Первый шаг к безопасности

Раз вы тут, значит вы в какой то степени решили поменять свою жизнь. Перемены это всегда хорошо, а особенно взвешенные.

Этот курс безопасности является универсальным и не заточен под какой-то какую-то конкретную сферу работы. Я считаю, что безопасность должна строиться на понимании человеком её принципов, а не на бессознательном копировании каких-то настроек. Поэтому в этом курсе я постараюсь максимально раскрыть принципы на которые безопасность полагается. Хотя чтобы рассказать всё в деталях и года не хватит, поэтому иногда я буду давать уже готовые настройки и программы. По окончанию курса у вас получится защищенная среда для безопасного продолжения работы в любой сфере. А чтобы больше погрузиться в детали, следите за каналом Hacker Place, там публикуется полезная информация.

Ко мне часто обращаются с вопросом люди, которые хотят обезопасить свой бизнес, увести на сервера бухгалтерии, надёжно сохранить файлы, спрятав их от чужих глаз. В общем, вопросы абсолютно разные. Но даже получая конкретный ответ люди, которые чаще всего не знают о подводных камнях, но пытаются настроить безопасность, встречаются со многими проблемами: сегодня увели бухгалтерию на далекие сервера, завтра доступы к серверам у 3-их лиц – почему? Что за ошибки были допущены?

Ответы на подобные вопросы о ***мнимой*** безопасности будут даны в рамках этого курса. Потому что чувствовать себя в безопасности и быть в безопасности – две совершенно разные вещи. И на этом курсе мы будем рассматривать и разбирать связки безопасности, а так же будем прорабатывать и продумывать свои связки безопасности под основные потребности.

Структура

У нас будет следующая концепция: сначала идёт теория без практики. Тут будут приводиться примеры из жизни, социальные ошибки, на чём люди обычно попадаются и прокалываются, а также теоретические моменты технической части вопроса: разберем как и для чего использовать сервера, в каких рамках тор безопасен, изолированные сети и прочее.

А после теории мы будем переходить к практике. Это непосредственная настройка рабочей машины с разбором того, что необходимо для повышения уровня анонимности.

Поскольку университет – это не просто сборник хорошо проработанного, но статичного материала, а интерактивная площадка, помимо лекций в подобном формате будут беседы в онлайн чате в более свободной форме, на них мы будем решать возникающие проблемы, и там будет даваться дополнительный материал. Причём дополнительные лекции не заканчиваются с прохождением курса, обновления продолжаются и после.

Так же доступна приватная поддержка в форме вопрос-ответ, тикет можно создать к любой лекции.

Туда можно обращаться по любым вопросам, лучше перестраховаться, но быть уверенным, что непонятных моментов нет.

Начнём мы с двух важных правил:

Я думаю вы все смотрели боевики, и там у киллеров и мошенников были свои неписаные правила, к примеру: не трогать женщин и детей. Так и в нашем мире тоже

есть такие правила. Только они уже не только морально-этические, а ещё и практические.

Первое правило
Не работать по РУ и странам СНГ. На то есть несколько причин:

- Мы живем на одной земле, так сказать. Ведь вам никому бы не хотелось чтоб у его бабушки украли пенсионные накопления с карты?
- Тесная связь между странами – тесная связь между их правоохранительными органами. И если накосячить и наследить где-то, то шанс быть пойманным сильно возрастает при работе по СНГ. Для наглядности: на Красной площади безопаснее топтать флаг США, а не России. Тогда вас мало того, что может и не арестуют, так ещё и поддержат и помочь могут.

Лучше основными целями выбирать страны Европы и Америки, у них страховые работают гораздо лучше чем в СНГ. Если вдруг со счета пропадут средства, они оформляют такую операцию как Charge Back, и им деньги возвращают, так что переживать не стоит. И морально спокойно, и для безопасности хорошо. Поэтому про работу по СНГ забываем пока не наберёмся опыта и не начнём чётко понимать, что мы делаем.

Тут есть грань, например, если ваша жертва - русскоговорящий наркоторговец, то никому не станет плохо, если вы его ограбите. Я думаю все понимают, что моральные границы – вещь тонкая. Но помните, что работая по РУ надо убедиться, что безопасности настроена как надо. Я думаю это никому ненужно по ошибке сесть надолго. А работая по USA, вас никто трогать не будет.

И хочу подчеркнуть в этой лекции, которая на половину вводная: как бы строго вы не соблюдали инструкции, всегда нужно думать своей головой перед тем, как что-то делать. Даже если вы уже не новичок и ваши практические навыки на уровне профи, а у вас в руках оказался онлайн-магазин с кредитными картами общей стоимостью товара на 50.000$, остановитесь на минуту и подумайте, посоветуйтесь если есть время. Эмоции надо откидывать и действовать взвешенно. Ведь в работе, самим того не заметив, можно нечаянно слить информацию о себе. И перед совершением действий надо вспоминать, а не оставили ли вы лишнюю информацию где-то.

Приведу дурацкий пример: на сайте запросило почту и была машинально введена своя настоящая. Тогда сразу после слива базы на кураже, вашей безопасности настаёт конец вне зависимости сколько нод тора использовалось и сколько уровней VPN стоит. Вас найдут при беглом анализе лога. Это не пример из реальной жизни, деанонимизируются обычно на более сложных связях, и умение их видеть, прогнозировать и избегать как раз и есть тот навык безопасности, который мы будем отрабатывать тут.

Второе правило
Это скорей не правило, а обычай, рекомендация. Работая в любой чёрной или серой сфере лучше купить отдельный ноутбук для этого дела и использовать эту машину только для работы по одной тематике. Другие действия на нем совершать запрещено. К примеру, работаете вы по своей теневой сфере и тут вам в голову пришло проверить свою личную электронную почту. Ну это, естественно, большая ошибка. Звучит очевидно, но это одна из популярных ошибок *мнимой* безопасности. До основной машины лезть лень, и создаётся впечатление, что войдя один раз в белую почту ничего не случится, но не надо забывать, что помимо очевидных следов, таких как сохранённые пароли в браузере, которые вы конечно не сделаете, в системе могут остаться более незаметные флаги, такие как части кеша. Поэтому никаких белых дел на этом ноутбуке. Под белыми делами я имею ввиду: социальные сети, почта,

мессенджеры, вообще ничего. Ничего того, что может связать ваш рабочий ПК с вашей реальной личностью. Запомните этот важный момент: Рабочий ПК - только рабочие дела. Другой пк или смартфон - белые дела и ваша реальная жизнь.

Практический совет по переносу данных: если рабочяя машина докупается по пути, то, скорее всего, на момент её у вас будут данные по работе, которые вы захотите туда перенести. Самым безопасным способом будет перекидывание через зашифрованное хранилище типа mega.nz. И помните, что некоторые программы оставляют следы. Например, Microsoft Word пишет данные об авторе в файл. Пропустить таким образом свои данные - уже более реальный пример из жизни, и это встречается в реальной работе, становясь причиной деанонимизации людей.

В простых текстовых файлах txt подобной информации нет. Поэтому при переносе данных постарайтесь переносить всё в базовых форматах.

Социальная безопасность

Выше я упомянул некоторые социальные ошибки. Это не ошибки, связанные с настройками сети или конфигурацией компьютера, а ошибки самого человека. Но самое забавное или даже печальное, что самые громкие хакеры и мошенники попадаются именно на таких тупых проколах.

Из реального примера, был такой хакер, под никнеймом Fly. Он держал крупный ботнет в Европе, у него было куча ботов, зарабатывал он огромные деньги. Его искали все, кто можно, включая независимого эксперта Браина Кребса. Fly был просто неуловим, но проебался он на тупости своей же. Данный персонаж приревновал свою подругу, закинул ей троя, который использовал для всей ботсети в качестве прогруза. Это наверное самый тупой поступок который он мог совершить. Как дальше раскручивали связку, остается только догадываться, но спалился он именно на этом. Казалось бы…

Лидера группы "Шалтай-Болтай" выдала шляпа. Он давал личное интервью свободному журналисту в одной азиатской стране. Репортер надежный был, не он его сдал. Но для своей статьи он сфотографировал шляпу, в которой пришел хакер. Немного об этот есть тут

http://www.rosbalt.ru/moscow/2017/06/19/1624238.html

Подняли ли они записи с камер видеонаблюдения или только по соц. сетям действовали достоверно не известно. Потому что такие дела засекречиваются, чтобы остальные не знали, на чём соседи по делу прокалываются, и не учились на чужих ошибках. Но большинство методов работы органов мне известно и материал курса на них опирается.

Социальная анонимность, это как раз таки подобные ошибки как из примеров выше. Приводить примеров можно просто море. Даже элементарно – наркокороль, владелец маркетплейса Silk Road с много миллионными оборотами, да под него плясал весь мир наркобизнеса. А спалился на чем? Потому что со своей личной почты писал на форуме сообщения в виде "Заходите на silk road, там заебись" Ну и дальше уже связка начала рваться и собираться доказательная база. Тупизм, больше ничего не сказать.

Да и вообще еще что главное… Главное скорей ваш язык. Меньше стоит рассказывать людям о том, чем вы занимаетесь. Это лично ваше, и никому до этого дела не должно быть. Девушке, другу, маме, папе, не надо никому об этом знать. Условно сегодня-завтра вы заработаете приличную сумму денег, купите себе машину дорогую. Вам обязательно начнут завидовать, у кого-то разрыв шаблона случиться и вас сдадут к чертям. Доверять нельзя никому. Помните, все люди женятся или выходят за муж

потому что уверенны, что с этим человеком они хотят связать всю оставшуюся жизнь, но каждый год в России более полумиллиона разводов. Не надо думать, что вы сможете доверять кому-то от начала и до конца, доверять можно только гайду по безопасности.

Еще важный момент про общение в сети. Спустя время у вас в контактах появится много много людей. Всевозможных продавцов, покупателей и так далее. Тут тоже нужно учитывать важный факт, не надо никому в сети рассказывать о себе, как вас зовут, сколько вам лет, где вы живете и тд. Даже если вас посетят мысли, я же с ним работаю уже больше года, почему бы мне с ним не выпить пивка и поболтать о жизни? Не вздумайте. Этого делать категорически нельзя. Думаю вы догадываетесь почему… Вне зависимости, как давно вы знаете этого партнера и сколько лет вы с ним работаете, это может быть человек из органов. А может он прокололся, его нашли и сейчас через него подельников раскручивают, чтобы их тоже задержать. Некоторые из них будут возражать и говорить, что вы с ним через столько прошли! Я не спорю, но стоит учитывать, что на подобном пиздеже уже словили кучу киберпреступников. Сначала идет разработка и полный сбор данных, а потом уже задержание с обвинением, так что молчание – золото.

Для близких людей и семьи придумайте легенду и ее толкайте. Например, разработка сайтов и реклама, платят хорошо. Кто-то из семьи, конечно, вряд ли вас сдаст, но на них надавить могут и вынудить выступить против вас, в органах отуплять классно умеют.

А тем более девушка или жена, с этим тоже надо быть осторожным. Чуть что и она на зло сдаст мусорам всю инфу, такое тоже бывает. Фильтруем и дозируем информацию.

Друзья - друзей не бывает, инфу тоже им лучше не стоит знать, купить можно каждого, вопрос только в цене.

Если рассмотреть это все, так сказать, на "бытовом" уровне, то могу привести пару примеров того, чего делать не надо:

- НЕ надо оплачивать модем для доступа в интернет для рабочей машины со своей банковской карты.
- НЕ надо оформлять модем на свое имя.
- НЕ надо заходить в социальные сети, проверять свою почту с рабочего пк.
- НЕ надо рассказывать жене, что украл биткоины у богатенького студента.
- НЕ надо встречаться попить пива с давнишнем подельником.

Это не полный список, но надо в голове у себя уложить эту информацию и не повторять чужих ошибок. Я только подчеркну, что социальная безопасность важнее чем вы думаете. Компьютер мы с вами настроим, все схемы я дам. Но если вы не понимаете основ соц. безопасности, то я ничем уже вам помочь не могу. Поэтому просто начинаем думать головой и не связываем работу и личную жизнь. Если соблюдать эти 2 правила, то социальных ошибок не будет, и будете вы как неуловимый Джо.

Технический аспект

Это более обширная тема, и я раскрою её намного глубже, чем социальную безопасность, которая для многих никаких пояснений и не требовала. В этой лекции я только начну это делать и расскажу про несколько шагов.

Вы будете использовать для всей своей деятельности интернет, сейчас вы наверняка подключены к своему роутеру который оформлен на ваше имя, первое время возможно это использовать, в дальнейшем необходимо будет купить модем который

оформленный на другое лицо, который раздает вай-фай, купить его на радио рынке допустим, симкарту там же, оформленную на другое лицо. Либо если не заморачиватся с модемом, будут даны инструкции как возможно взломать соседский вайфай и подключится к нему и использовать его точку доступа для работы.

Главное то, что по умолчанию на основной машине трафик будет шифроваться, днс запросы будут шифроваться тором, провайдер не сможет определить природу и маршут трафика, тем не менее будут даны рекомендации по взлому соседского вайфая.

На этом я закончу первую лекцию. Тут была не очень сложная информация, скорее настрой на дальнейшее обучение. *Кто будет переустанавливать систему, не спешите это делать. Это лучше отложить до шифрования жёсткого диска, о котором будет в следующих лекциях.*