БРОШЮРА
ДЛЯ КЛИЕНТОВ СЕРВИСА

VEKTOR T13

www.VektorT13.pro

ОБО МНЕ И МОЕЙ КОМАНДЕ

Я — Vektor T13, специалист в области информационной безопасности. Специализации: организация сохранения анонимности пользователей в сети, способы деанонимизации пользователей и криминалистический анализ компьютерной техники. Последние два года активно изучаю вопрос безопасности сетей SS7 и мобильных девайсов.

Проживаю на Украине. Могу консультировать на русском, украинском, чешском и английском языках. Программирую на TurboPascal, QBasic, Delphi, C++. В совершенстве знаю архитектуру основных современных ОС. Участвую в международных конференциях, посвященных IT-безопасности и компьютерной криминалистике.

Имею квалификацию пентестера компьютерных систем. Свободно работаю с Kali Linux и могу обучать работе с этой ОС. Имею опыт тестирования на возможность проникновения и наличие уязвимостей в корпоративных сетях. Обладаю передовым криминалистическим софтом для проведения комплексного криминалистического анализа систем.

В моей команде есть специалист по сетевым решениям и организации сетевой архитектуры. Именно он занимается разработкой и настройкой профессиональных сетевых решений, таких как VPN, VoIP, Mail, Cloud solutions и др. Он всегда готов взяться за сложные индивидуальные решения как для компаний, так и для частных лиц.

Для удобства клиентов у меня работает профессиональный саппорт, который каждый день на связи, и будет рад помочь Вам по любому организационному вопросу.

> “
>
> Более 7 лет я занимаюсь изучением вопросов анонимной и безопасной работы в сети, вопросами активной и пассивной деанонимизации. Каждое свое утро я начинаю с чтения специализированных изданий на английском языке, приобретаю и изучаю всю литературу по данной тематике, участвую в профессиональных конференциях, делюсь опытом с коллегами, приобретаю топовый криминалистический софт. Я готов поделиться своими знаниями и опытом с Вами.
>
> *Vektor T13*

ОТЗЫВЫ О ВЕБИНАРАХ И КОНСУЛЬТАЦИЯХ Vektor T13

“
Только что провели двухчасовую лекцию с вектором — объясняет так, что поняла бы, наверное, даже моя бабушка! Доходчиво, понятно, не перескакивает с темы на тему, в общем было приятно слушать, как будто я на лекции или на семинаре в вузе и ведет у меня грамотный препод.
Peace

Юзал double vpn. Превосходно. И скорость, и пинг, и тех поддержка. Ещё было очень подробно всё объяснено. Рекомендую ”
TheillusiveMan

“
Пользуюсь данным сервисом. Хочу сказать что оператор отзывчивый, все грамотно и подробно объясняет. Может доступно разжевав донести до любых персонажей суть того что он делает. Сами его услуги оказались очень полезны. Цены немного высоковаты на мой взгляд, но сфера деятельности немного специфична и некоторым просто необходима. Были небольшие трудности, но ТС их разрешил и на данный момент впечатление и отношение к сервису только положительное. Надеюсь селлер будет продолжать оказывать данные услуги на высоком уровне и радовать нас без устали!
Misterproper

Больше узнал на вебинарах Вектора о безопасности чем за все время учебы в университете на факультете информационной безопасности)) Всем советую! ”
Armagedec

“
Отличные уроки! Смотрю каждый ваш вебинар, не жалею ни одной минуты потраченного времени
HelloWorld

“

Спасибо, Vektor, за твои прекрасные вебинары, твой тяжелый труд и уйму потраченного времени на организацию проведения. Очень много в них полезной и актуальной информации как для новичков, так и для продвинутых. Все твои вебинары это бомба.

Activate

Вебинар был суперским, Vektor T13 все классно объяснил и дал ответы на все интересные вопросы, не упустил ни единого вопроса, всем советую его вебинары, он знает что говорит!!!!

Sh4aa ”

“

Очень крутые вебинары, спасибо. Уже давно интересуюсь безопасностью, но на ваших вебинарах узнал столько инфы, что если бы искал её самостоятельно, то на это потребовался бы наверно не один год.

Spectrx

Вектор как всегда был на высоте!!! Про логи я вообще в осадок выпал. Всем крайне советую внимательно слушать и впитывать инфу которую Вектор нам бесплатно вещает, за что ему конечно же огромное СПАСИБО.

Abuza ”

“

Вектор дает реально познавательный материал в информационной безопасности. Думаю, что таких учителей, которые смогут сложные вещи объяснить доходчиво, а затем закрепить на практике — единицы.

HoRRy

ВАРИАНТЫ ОБУЧЕНИЯ И СТОИМОСТЬ

Индивидуальные консультации.

Проводятся голосом и текстом или только текстом. Время бронируется у саппорта, согласовывается индивидуально. На консультации Вы будете одни, и специалист будет работать с Вами индивидуально, решая только Ваши задачи.

Есть три категории людей: первые приходят с конкретными проблемами и вопросами, вторые хотят настроить защиту от каких-то категорий угроз, третьи проходят полноценное обучение от А до Я. Вы сами можете выбрать свой путь.

Комплексное обучение включает шесть компонентов: теорию, интерактив, настройку, практику, тестирование и углубленное изучение.

Теория — изучение теоретических вопросов, посвященных анонимности и безопасности в сети.

Интерактив — практическая демонстрация какого-либо материала, например, демонстрация атаки, деанонимизации пользователя или заражения системы.

Настройка — настройка Вашей системы и девайсов для анонимной и безопасной работы в сети.

Практика — использование полученных знаний и навыков на практике. Например, после обучения аудиту сетевой активности Вы будете на практике проводить аудит своего сетевого трафика и разбирать полученные результаты со специалистом. Проводится Вами при поддержке нашего специалиста.

Тестирование — проверка полученных Вами знаний и навыков на практике.

Углубленное изучение — расширение изучения темы по желанию пользователя. Если Вас заинтересовала тема, Вы можете выделить часы для дополнительного изучения материалов. По некоторым темам мы предоставим Вам литературу, аудио и видео материалы для углубленного изучения темы.

Стоимость: **50 $/час**
Минимальная оплата для первоначальной записи: **3 часа**

ПРАВИЛА ОБУЧЕНИЯ

Мы не обучаем преступников. Если до консультации или в ее процессе выяснится, что Ваша деятельность связана с нарушением закона, мы будем вынуждены прервать консультацию без возможности возобновления.

Мы не обучаем совершать преступления. Не надо просить нас обучить взлому, осуществлению DDoS-атак, флуду мессенджеров или телефонов, кибершпионажу за пользователями и другим видам деятельности, нарушающим закон.

Проблемные ситуации. Мы не продаем решений под ключ. Иногда в процессе настройки возникают проблемы, решение которых занимает время. Просим отнестись с пониманием, что это время будет засчитано Вам как консультационное. Если Ваша техника не позволяет реализовать какое-то из стандартных решений, нам придется искать причины проблемы или альтернативные решения, это может занять время. Например, на некоторых ноутбуках возникают проблемы при создании виртуальной ОС, либо проблемы могут возникнуть с приобретенной вами USB-флешкой, на которую будет устанавливаться ОС.

Индивидуальные решения. Если Вы хотите получить какое-то индивидуальное решение, например, прошивку для Вашего телефона или хотите, чтобы специалист изучил какой-либо вопрос для дальнейшей консультации Вас, необходимо забронировать часы у саппорта. Любой индивидуальный вопрос требует времени, к сожалению, все рабочее время у нас расписано.

Срочные консультации. Обычно из-за большого количества клиентов запись к нам происходит заранее. Но специалист всегда оставляет часы по утрам и вечерам для консультирования срочных клиентов. Если Вам надо срочно записаться

на ближайшее время, это всегда можно сделать у саппорта. Срочные консультации оплачиваются по двойному тарифу.

Прогулы и опоздания. О невозможности посетить консультацию надо сообщать минимум за 12 часов до ее начала. Если Вы не явитесь на консультацию без предупреждения, наш специалист будет вынужден этот час сидеть и ждать Вас. Час ожидания будет вычтен с Вас как консультационный.

Проблемы со связью. Вы должны самостоятельно организовать качественный уровень связи на время обучения. Если Вы не сможете заниматься по причине проблем со связью, и об этом не будет сообщено заранее (не позднее 12 часов до начала), мы вынуждены будем вычесть с Вас час консультаций.

Есть два способа консультации. Предпочтительный — голос (Вы можете только слушать) и текст, второй — только текст, для тех, у кого проблемы с качеством связи.

Проблемы с TeamViewer. Для консультации используется специализированное программное обеспечение для оказания дистанционной технической поддержки TeamViewer. Вам необходимо до начала консультации скачать его с официального сайта https://www.teamviewer.com и проверить работоспособность на Вашем устройстве. Если при проверке TeamViewer возникнут проблемы, обратитесь в службу поддержки нашего сервиса.

ОПИСАНИЕ УГРОЗ, ПОСЛЕДСТВИЙ И РЕШЕНИЙ

Угроза: заражение вашего персонального компьютера, кража данных.

Последствия.

Получение злоумышленниками доступа к любым Вашим файлам, возможность проведения любых действий с Вашими файлами и папками, включая изменение, удаление и шифрование. Получение доступа ко всем Вашим паролям, любым Вашим аккаунтам. Контроль всех Ваших переписок в мессенджерах и социальных сетях, запись и прослушивание всех Ваших звонков с мобильного и компьютера, например, при помощи Skype или VoIP. При этом абсолютно не важно, используете вы шифрование или нет.

Незаметная подмена реквизитов при отправке банковских переводов, автоматическая подмена выдаваемых сайтами платежных реквизитов, включая кошельки биткоин. Возможность кибершпионажа за Вами при помощи просмотра и записи видео с Вашего экрана, видеонаблюдение за Вами при помощи веб-камеры

и прослушка помещения при помощи микрофона. Использование Вашего компьютера для рассылки спама, DDoS-атак и майнинга биткоинов. Уничтожение операционной системы или конкретных файлов без возможности восстановления.

Решение.

Наивно полагать, что своевременное обновление системы, антивирус или файрвол защитят Вас от вредоносного программного обеспечения (далее — вредоносное ПО). В этом случае вредоносного ПО просто бы не было, статистика зараженных устройств не била бы все рекорды, а разработчики троянов не зарабатывали бы миллиарды долларов ежегодно.

В своем курсе мы познакомим Вас с механизмом работы антивируса и файрвола, а также с тем, как киберпреступники обходят защиту. Это важно, поскольку невозможно защититься от врага, не зная его ресурсы и возможности. Знания — это первый барьер защиты.

В процессе обучения на удаленных компьютерах мы будем разбирать работу вредоносного ПО, знакомиться с реальными троянами и шифровальщиками, изучать принцип их работы и возможности.

Кроме самого вредоносного ПО, мы будем изучать и пути заражения: от «склейки» программы с файлом или документом до заражения через веб-сайты.

Второй барьер защиты — операционная система на основе Linux. Мы установим и настроим операционную систему на основе Linux, для которой на сегодняшний день крайне мало эффективного вредоносного ПО. Заразить компьютер с ОС на основе Linux — это трудная задача даже для опытного специалиста. 95% вирусов и троянов в сети будут не способны нанести Вам какой-либо вред.

Мы научим Вас использовать Linux в повседневной жизни, перенести туда работу и отдых, запускать приложения, разработанные под Windows.

Отдельным блоком мы хотим предложить Вам обучение работе с терминалом.

Терминал (консоль) — командная строка в системах на основе Linux, позволяющая управлять системой, файлами и процессами. Именно она часто пугает новичков, но обучившись работе с ней, Вы расширите свои возможности по защите данных и анонимизации в сети.

Пройдя несколько занятий, Вы будете в совершенстве владеть всем основным функционалом консоли, сможете как опытные пользователи работать с Linux-системами, не используя графического интерфейса.

Мы можем помочь Вам настроить защищенный компьютер и на основе ОС Windows (7, 8, 10), однако возможности Windows во много раз скромнее возможностей Linux.

Мы никогда не сможем достичь на Windows уровня защиты от вредоносного ПО и угроз заражения, какой возможен на Linux. Мы настоятельно рекомендуем использовать ОС Windows только в качестве виртуальной операционной системы.

Mac OS X в плане безопасности значительно лучше Windows, и мы можем настроить высокий уровень безопасности системы.

Мы настроим Вам безопасную виртуальную среду. Все ссылки и файлы Вы будете открывать только в виртуальной операционной системе. В процессе обучения мы будем проводить в ней анализ файлов и сайтов, находить вредоносные программы и угрозы нашей безопасности.

Мы научим Вас проводить аудит портов и анализ трафика. Эти навыки помогут обнаружить вредоносное ПО, проанализировать, куда и как часто оно «стучит», а также закрыть все открытые порты, что сделает атаки на Вас еще сложнее.

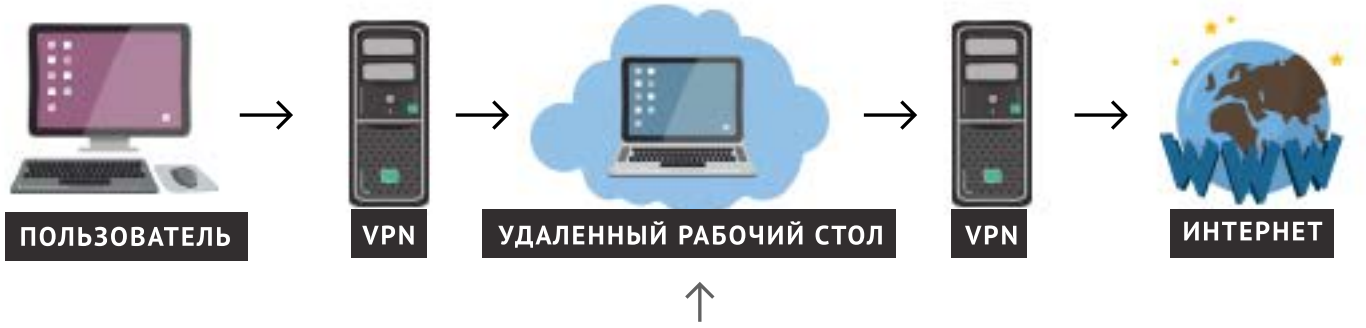
Мы поможем Вам научиться анализировать процессы, запущенные в системе, находить активность «нежелательного» программного обеспечения и блокировать его.

Теоретическую часть обучения мы закончим практикой, предоставив Вам удаленный доступ к зараженному различными вредоносными программами компьютеру. Вы должны будете применить полученные знания, путем аудита трафика и процессов обнаружить и ликвидировать все вредоносное ПО.

Для защиты от «шифровальщиков» мы настроим систему резервного копирования Ваших данных в Ваше персональное облачное хранилище. Даже если вредоносная программа каким-то образом попадет на Ваш компьютер и зашифрует все данные, Вы восстановите их, не платя выкуп злоумышленникам.

Если Вам будет необходим особый уровень защиты от вредоносного ПО, рассмотрите наше решение с защищенным удаленным столом. При использовании данной схемы Вы подключаетесь к удаленному серверу, где установлена Ваша рабочая операционная система на основе Linux, настроенная по всем канонам защиты. В ней установлено ПО виртуализации и хорошо настроен файрвол.

Защищенный удаленный рабочий стол, настроенный профессионалами, будет служить непреодолимым барьером для вредоносного ПО.



Здесь вы фактически будете работать, открывать ссылки, файлы, запускать программы

Угроза: заражение вашего мобильного девайса (телефона/планшета), кража данных.

Последствия.

Получение злоумышленниками доступа ко всем данным на Вашем мобильном телефоне, включая видеофайлы и фотографии, возможность читать, перехватывать и отправлять SMS-сообщения, возможность похитить деньги с Ваших счетов, к которым привязан мобильный банкинг (как правило, это основная цель заражения). Злоумышленники смогут отправлять с Вашего телефона СМС на платные номера, оформлять подписки с абонентской платой, осуществлять перевод денег с номера на номер.

Получив доступ к камере, микрофону и GPS-навигатору, злоумышленники смогут слушать Вас, наблюдать через веб-камеру, следить за Вашими перемещениями. Они смогут получить доступ ко всем Вашим приложениям и сайтам, читать переписку в мессенджерах и социальных сетях. Злоумышленники могут загружать Вам на телефон новые приложения, а также рассылать вредоносное программное обеспечение по Вашему списку контактов.

Решение.

Решить эту проблему может комплексная настройка безопасности вашего телефона, и доступно это только на телефонах с ОС Android. В процессе работы мы установим Вам альтернативную прошивку CyanogenMod. Это популярная во всем мире прошивка с открытым исходным кодом, позволяющая качественно настроить безопасность данных Вашего мобильного устройства.

Сегодня защита Android-устройства не сильно отличается от защиты компьютера и включает в себя обучение анализу процессов и сетевой активности, аудиту портов и прав приложений.

На устройствах под управлением iOS возможна лишь частичная настройка безопасности данных.

Угроза: эксплуатирование 0day уязвимостей в операционных системах и программном обеспечении.

Последствия.
Заражение устройства со всеми вытекающими результатами, описанными выше. Однако данный тип угроз вынесен в отдельный пункт ввиду того, что для защиты от 0day уязвимостей (уязвимостей, которые еще не известны или от которых еще не разработана защита), нужны особые средства и подходы.

Решение.
Многие «специалисты» по безопасности для защиты от данного типа угроз ограничиваются рекомендациями своевременно обновлять программное обеспечение. К сожалению, своевременное обновление ПО абсолютно не работает против 0day уязвимостей. Здесь необходима адресная работа с самыми потенциально уязвимыми местами.

Одно из самых уязвимых ПО на компьютере — браузер. По несколько раз в год в различных браузерах обнаруживаются критические 0day уязвимости, и именно атаки на браузер чаще всего используются для адресных и массовых атак. Обновления закрывают только часть уязвимостей, а другая часть остается необнаруженной и активно эксплуатируется злоумышленниками. В рамках обучения для защиты от 0day уязвимостей мы будем запускать браузер в виртуальной среде, что исключит возможность занесения вредоносного программного обеспечения на Ваш компьютер.

Угроза: деанонимизация (получение данных о Вас и Вашем местонахождении, получение информации о Ваших учетных записях на веб-сайтах).

Последствия.
В зависимости от возможностей и задач недоброжелателя — это установление Вашей личности и точного местонахождения, получение истории посещения веб-сайтов, отслеживание Вашей активности в сети, принадлежащих Вам страничек в социальных сетях и аккаунтов на форумах.

Кроме этого, злоумышленник может организовать атаку на Ваш IP-адрес и тем самым лишить Вас интернета в заданный момент. Если Вы используете Wi-Fi роутер, и злоумышленник получит Ваш IP-адрес, он может взломать роутер и получить доступ к Вашему трафику. Последствия взлома Wi-Fi роутера мы опишем в следующей части.

Одним из самых опасных последствий может быть использование злоумышленником Вашего IP-адреса для атаки на правительственные ресурсы (ip spoofing).

Последствия подобной атаки могут привести к визиту в Ваш дом правоохранительных органов, аресту техники и обыску.

Решение.
Защиту от деанонимизации мы начнем с сокрытия Вашего подлинного IP-адреса. Здесь нам поможет VPN (Double VPN и выше). У Вас будут свои личные VPN-сервера с отключенным логом. Это не позволит сайтам получить Ваш подлинный IP-адрес.

Все подключения будут идти только через зашифрованный канал VPN.
Мы заблокируем любые подключения в обход Вашего личного VPN, исключив случайные утечки данных при обрыве VPN или ошибках в системе. Случайные утечки данных и ситуации «ой, я кажется забыл включить VPN» являются одной из самых распространенных причин деанонимизации.

Вместе с VPN-сервером у Вас будет и свой DNS-сервер, шифрующий DNS-запросы, и на котором будет отключено логгирование. Защита DNS исключит Вашу деанонимизацию путем подмены IP-адресов сайтов, а также отслеживание Вашей активности в сети по DNS-запросам.

VPN обеспечит анонимность на достаточно хорошем уровне. Но, используя только VPN, Вы будете иметь один-единственный IP-адрес, а следовательно, будет возможность отследить, какие социальные сети, аккаунты на ресурсах, сайты посещаются с данного IP. При наличии необходимого административного ресурса, проанализировав эту информацию, можно будет установить Вашу личность и отследить Вашу активность.

Это большой минус Вашей безопасности и для его нейтрализации мы научим Вас создавать и использовать proxy-сервера. Поднятие и настройка прокси занимает всего несколько минут и позволит Вам использовать различные IP-адреса для различных направлений активности в сети.

По окончании обучения у Вас будет несколько профилей в браузере с привязанными прокси, которые Вы будете периодически менять. Например, один профиль с IP в Нидерландах Вы будете использовать для социальных сетей, другой, с IP

Германии, — для веб-серфинга, третий, с IP Швейцарии, — для форумов. Сколько IP-адресов использовать и для каких целей — решать Вам.

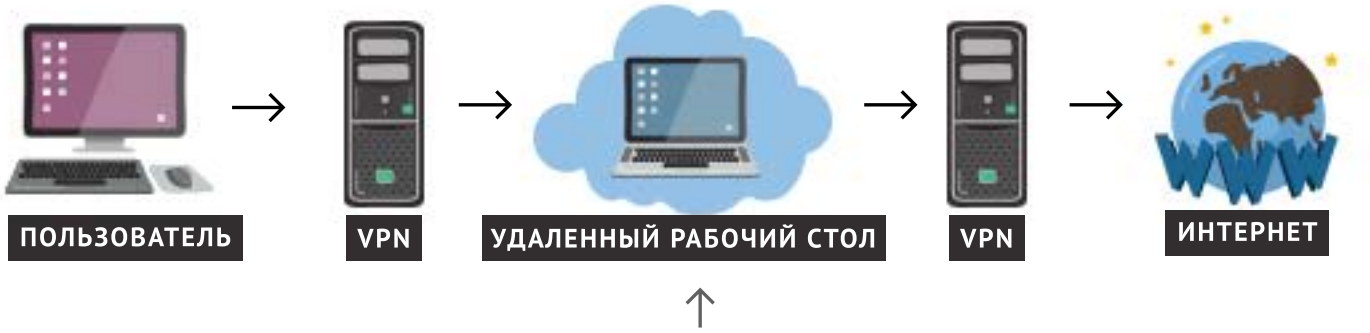
Для защиты от «раскрутки*» мы при необходимости будем дополнять схему включением в нее Тора. Это большой минус к скорости и качеству интернета, но большой плюс к анонимности. Вы будете добавлять Tor, когда Вам необходима максимальная анонимность, и оставаться только на VPN, когда Вам нужен анонимный и безопасный интернет без потери качества.

А для максимального уровня анонимности мы добавим в схему защищенный удаленный рабочий стол, к которому Вы будете подключаться через VPN. Добавление удаленного рабочего стола в схему сразу выведет Вашу анонимность на принципиально иной уровень.

Дело в том, что все программы, которые установлены на Вашем компьютере, имеют прямой доступ к Вашему IP-адресу. Это и браузер, и мессенджеры, и любые программы, проводящие автоматическое обновление. Ни Tor, ни VPN, ни proxy им не помеха: если они уже на Вашем компьютере, то знают Ваш подлинный IP-адрес.

Подобным образом работают и системы активной деанонимизации. Попадая под видом файла, документа или картинки на компьютер жертвы, они получают IP-адрес с компьютера в обход систем анонимизации (VPN, Tor, proxy).

В случае, когда в Вашей системе используется защищенный удаленный рабочий стол, все установленые на нем программы могут получить только его IP-адрес. Как правило, удаленный рабочий стол расположен в другой стране и даже не «знает» Вашего подлинного IP-адреса благодаря VPN, который используется для подключения к нему.



Удаленный рабочий стол, именно его IP-адрес будут видеть программы и софт для активной деанонимизации

Для предотвращения деанонимизации путем тайминг-атак* на Вашем VPN-сервере будет размещена специальная система, сжимающая трафик и надежно защищающая Вас от любых видов тайминг-атак.

Деанонимизацию Вас по MAC-адресу сетевой карты мы предотвратим, установив Вам специальное ПО. Данное ПО будет менять MAC-адрес Вашей сетевой карты после каждой перезагрузки компьютера.

Для защиты от деанонимизации путем использования против Вас вредоносных скриптов (JS) на сайте, мы проведем Вам комплексную настройку браузера, по умолчанию отключив исполнение JS на неизвестных сайтах. Помимо этого, мы научим Вас проводить аудит сайта на наличие опасных скриптов

Для тестирования полученных знаний Вам будет дано несколько сайтов; Вашей задачей будет провести анализ JS и постараться определить, какую информацию они запрашивают о Вас. Полученные результаты будут детально разобраны.

Во втором тесте Вы научитесь пользоваться сайтом с развернутой системой для заражения и деанонимизации пользователей, а затем попробуете деанонимизировать сами себя. В рамках этого теста Вы на практике увидите, как сайты могут деанонимизировать Вас, и проверите свой браузер на наличие уязвимостей.

Одним из самых эффективных методов деанонимизации являются файлы с вредоносным ПО. К сожалению, если такой файл попадет на Ваш компьютер, он легко сможет получить ваш подлинный IP-адрес на уровне ПК.

В рамках третьего теста мы попробуем атаковать Вас с помощью специального ПО для активной деанонимизации и проверим Вашу анонимность «в бою».

*Раскрутка — метод деанонимизации, при котором раскручивают структуру подключений. Например, узнают у интернет-провайдера, кто подключался к серверу. Если связь шла через VPN, то идет запрос к интернет-провайдеру VPN-сервера с вопросом, кто в определенный временной промежуток к нему подключался. Если подключался другой VPN, то обращаются к провайдеру первого VPN и запрашивают, кто подключался к нему в тот же временной промежуток. Таким образом выходят на первичный IP-адрес.

**Тайминг-атаки — атаки, направленные на вычисление конечного пользователя в сети путем модификации или искажения трафика. Конечный узел (сайт, сервис), к которому через инструменты деанонимизации подключилось разыскиваемое лицо, отправляет пакет необычного размера или с необычной задержкой. Затем система контроля интернет-трафика, например СОРМ, отслеживает, к кому в итоге придет этот пакет. Система позволяет пробивать связки любой длины и содержания.

VPN, Tor, удаленный компьютер, SSH, proxy легко вскрываются тайминг-атакой.

Угроза: взлом Wi-Fi роутера / 3G модема

Последствия.
Взлом Wi-Fi роутера может привести к подмене DNS и, как следствие, подмене сайтов (IP-адресов сайтов) для показа Вам вредоносной рекламы, перехвата Ваших данных, получения доступа к Вашим банковским счетам, аккаунтам на веб-ресурсах, шпионажа за Вами, блокировки Вам доступа в интернет, заражения Ваших устройств и, само собой, для вашей полной деанонимизации. И не только Вас, а всех, кто подключается ко взломанному Wi-Fi роутеру.

Решение.
К сожалению, сегодня большинство роутеров имеют уязвимости и подвержены риску взлома. Для комплексной защиты устройства мы предлагаем следующий план работ.

- Тестирование Вашего Wi-Fi роутера на наличие уязвимостей. При желании мы можем обучить Вас самостоятельно тестировать роутер на наличие уязвимостей. Обращаем Ваше внимание, что это — знания двойного назначения, и предупреждаем Вас, что использовать их допустимо только для тестирования безопасности Ваших устройств.
- При необходимости мы подберем безопасные модели Wi-Fi роутеров/3G модемов, для которых нет публично известных уязвимостей.
- Проверим актуальность прошивки Вашего роутера/модема, при необходимости обновим прошивку.
- Сменим стандартные заводские пароли на уникальные и защищенные от брутфорса.
- Проводим «переброс портов» веб-панели роутера.
- По возможности блокируем доступ в панель веб-управления роутером (оставляем только в зависимости от модели ssh или telnet).
- Настроим Вам VPN-туннель для защиты от перехвата данных при использовании публичных Wi-Fi роутеров.

При желании в процессе обучения мы проведем наглядную демонстрацию значимости защиты Wi-Fi роутера. Вам будет дан IP-адрес роутера модели, содержащей

уязвимость. Вашей задачей будет получить доступ к роутеру, перехватить трафик и выдернуть оттуда логины и пароли к различным ресурсам, включая социальные сети и популярные почтовые клиенты. Предварительно Вы будете обучены проводить тестирование роутеров на наличие уязвимостей, перехватывать и анализировать трафик.

Этот позволит Вам понять, насколько важно заботиться о безопасности Wi-Fi роутера и шифровать трафик при помощи VPN.

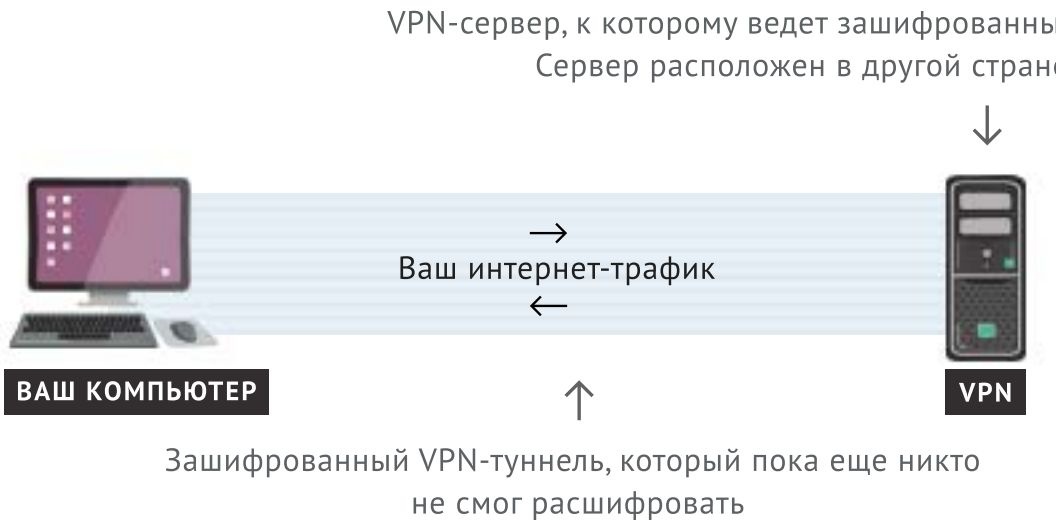
Угроза: перехват и изменение интернет-трафика.

Последствия.

Получение информации о посещенных Вами сайтах, просмотренных фото и видео, об аккаунтах на сайтах и социальных сетях, об используемых Вами программах, перехват логинов и паролей, кража электронных кошельков. В случае изменения интернет-трафика возможна загрузка на устройство пользователя вредоносного ПО, подмена сайтов.

Решение.

Для защиты от перехвата и изменения интернет-трафика мы будем использовать технологию VPN. VPN позволит надежно зашифровать трафик и исключить перехват отправляемой информации на уровне Вашего модема, Wi-Fi роутера, интернет-кабеля (физический доступ) и интернет-провайдера.



Вы не только поднимете свой VPN-сервер или цепочку серверов, но также мы разберем принцип работы VPN. Именно понимание процессов — залог эффективной защиты данных.

В то же время мы рассмотрим риски использования «публичных» VPN сервисов. Для этого Вы в онлайн режиме сможете посмотреть перехват данных на уровне VPN-сервера и при желании лично повторить это. Мы расскажем Вам, как VPN-провайдеры ведут лог и анализируют трафик, это поможет оценить важность персонального VPN.

В качестве итогового теста Вам будет предложено самостоятельно перехватить Ваш трафик и убедиться, что он надежно зашифрован. Предварительно мы научим Вас перехватывать и анализировать трафик.

Угроза: перехват и изменение интернет-трафика на инструментах анонимизации в сети.

Последствия.
Все последствия перехвата и изменения трафика, описанные в предыдущем блоке, угроза выдачи собранной информации недоброжелателям, продажа собранной о Вас информации (логов).

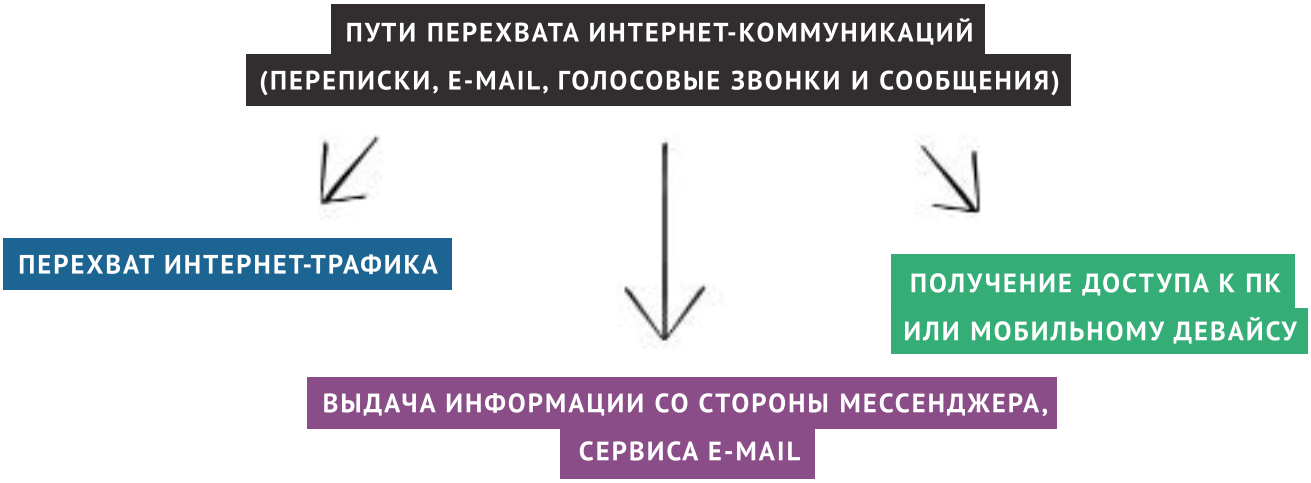
Решение.
К сожалению, если Вы используете публичные VPN-сервисы, выходные ноды Tor, удаленные рабочие столы и прокси-сервера, то подвергаетесь серьезному риску перехвата интернет-трафика со стороны владельца ресурса. Это сплошь и рядом применяется на бесплатных или бюджетных ресурсах. Защита тут может быть только одна — поднятие своих ресурсов, чем мы и будем заниматься с Вами в процессе обучения.

Угроза: перехват интернет-коммуникаций (email, мессенджеры, голосовые звонки в сети).

Последствия.
Получение недоброжелателями доступа к Вашей переписке, голосовым звонкам, сообщениям и передаваемым файлам, а также установление списка Ваших

собеседников с их IP-адресами. Кроме того, возможно получение Вашего подлинного IP-адреса, к которому есть доступ у мессенджеров, устанавливаемых на компьютер или мобильный девайс, даже при использовании средств анонимизации вроде VPN, Tor и proxy.

Решение.
Первым делом стоит разделить пути перехвата интернет-коммуникаций.



Угрозу перехвата интернет-трафика мы решим использованием VPN. Угрозу перехвата трафика на уровне VPN, чем часто злоупотребляют владельцы сервисов, мы решим использованием своих ресурсов.

Проблему получения несанкционированного доступа к персональному компьютеру или мобильному девайсу для перехвата интернет-коммуникаций мы решим комплексной настройкой безопасности, о которой говорили в начале материала.

А вот решение вопроса защиты от выдачи данных заслуживает отдельного внимания. Первым делом мы откажемся от:

- использования публичных сервисов электронной почты (Gmail, почта Яндекса, Mail.ru, Yahoo и др.),
- мессенджеров (Skype, ICQ, WhatsApp и др.),
- сервисов голосовых звонков (Skype, Viber, Line и др.).

Эти сервисы хранят Ваши метаданные, переданные файлы, звонки и имеют возможность передать их 3-ей стороне. Они ведут лог IP-адресов всех Ваших подключений, а установленные Вами на ПК/телефон программы имеют возможность получить доступ к Вашему настоящему IP-адресу даже при использовании VPN, Tor или других средств для анонимизации.

Email

Вместо использования «публичных» почтовых серверов мы поднимем собственный почтовый сервер, где Вы всегда сможете безвозвратно удалять полученные

и отправленные письма, файлы и документы. Ваш собственный сервис не будет хранить письма и, разумеется, никому ничего не выдаст «по запросу».

Помимо этого, мы научимся шифровать письма при помощи PGP. Мы лично будем обмениваться с Вами в процессе обучения зашифрованными письмами.

Кроме этого, мы покажем Вам еще несколько интересных моментов, которые могут быть для Вас полезны при использовании электронной почты. Например, как узнать IP-адрес отправителя письма или как отправить письмо с подменой почтового адреса и как распознать подмену.

Мессенджер

В качестве мессенджера мы будем использовать Jabber. В процессе обучения мы развернем свой XMPP-сервер, где отключим логгирование. Подключение к нему будет только через VPN, а все сообщения будут зашифрованы OTR/PGP.
На сегодняшний день PGP считается неприступным методом шифрования данных даже для спецслужб.

Голосовое общение в сети

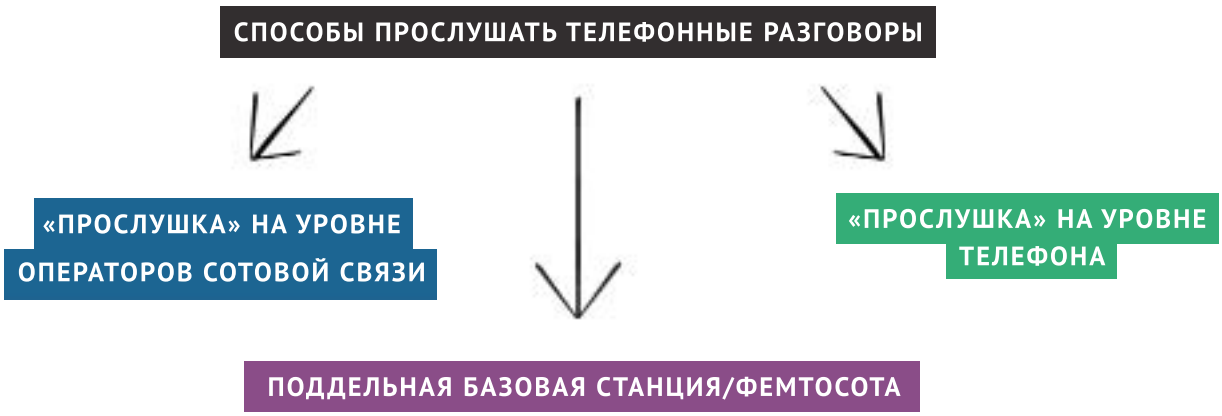
Для защищенного голосового общения в сети мы развернем персональный VoIP-сервер. Все разговоры будут надежно зашифрованы, на Вашем VoIP-сервере будет отключено логгирование. Подключение к своему VoIP-серверу будет только через VPN, что гарантирует максимальный уровень защиты данных, а также исключит возможность определить наличие подключения к VoIP-серверу на уровне интернет-провайдера.

Качество своего VoIP-сервера превосходит публичные сервисы, такие как Skype и Viber. Для сокрытия Вашего подлинного голоса можно использовать модуляцию — программное или аппаратное изменение голоса.

Угроза: прослушивание телефонных переговоров.

Последствия.
Получение доступа ко всем Вашим звонкам, запись звонков, получение доступа к Вашим SMS, перехват SMS.

Решение.
Для начала рассмотрим способы прослушать телефонные звонки.



От прослушивания на уровне оператора связи Вас ничто не защитит. Просто смиритесь с этим. Для прослушивания необходимо знать Ваш номер телефона и обладать соответствующим административным ресурсом. Помните, что прослушивать могут не только Вас, но и номер Вашего собеседника. Единственным решением тут является отказ от использования GSM связи для звонков и общение с партнерами, коллегами и друзьями через персональный VoIP.

Для защиты от прослушивания переговоров мы поднимем собственный VoIP-сервер и настроим звонки через него. Это будет Ваш личный VoIP, мы научим Вас управлять им, проверять отсутствие лога, менять root-доступы.

Все разговоры будут надежно зашифрованы, никто не сможет их прослушать. Поверх шифрования VoIP-канала трафик будет шифровать VPN-туннель. Такую связку не под силу расшифровать ни одному специалисту в мире.

Если Вам необходимо будет звонить на сотовые или городские номера, к серверу будет привязан виртуальный номер, но Вы должны помнить, что эти звонки уже не будут защищены.

От перехвата сотового сигнала при помощи фемтосоты или аналогов Вас надежно защитит свой VoIP с шифрованием трафика и VPN-туннель, шифрующий трафик поверх VoIP. Даже если Ваш трафик смогут перехватить, расшифровать его не будет

возможности.

Остается вероятность прослушки разговоров, если Ваш телефон будет заражен вредоносным программным обеспечением, получившим доступ к камере и микрофону. Для защиты от данного способа прослушки мы настроим комплексную безопасность телефона, которая описана в отдельном блоке.

Угроза: защита от идентификации и установления личности звонящего.

Последствия.
Определение личности звонящего и его местоположения.

Решение.
Для защиты от установления личности по отпечатку голоса* мы настроим Вам модуляцию (изменение) голоса. Модуляция может быть встроена на уровне VoIP, когда Ваш голос будет изменяться на сервере, либо производиться при помощи специального программного обеспечения. В этом случае определить звонящего по голосу не сможет ни человек, ни система.

Для защиты от пеленга** Вы будете совершать звонки только через Ваш VoIP-сервер, к которому мы привяжем один или несколько виртуальных номеров. Подключение к серверу будет происходить через один или несколько VPN-серверов. При такой связке произвести пеленгацию номера и определить местоположение звонящего невозможно. При этом у Вас всегда будет отличное качество связи, даже при 3G интернете.

Поскольку звонок происходит через VoIP, деанонимизация звонящего по IMEI или данным сим-карты невозможна.

*Отпечаток голоса — набор уникальных показателей голоса, по которым система может идентифицировать человека. Точность современных систем идентификации голоса стремится к ста процентам.

**Пеленгация — определение местоположения телефона в мобильной сети.

Угроза: взлом ваших аккаунтов.

Последствия.
Получение доступа к различными аккаунтам, кража денег, персональной информации, иной нематериальный ценности. Использование Ваших аккаунтов в преступных схемах, например, почтовых ящиков и страниц в социальных сетях для рассылки СПАМа.

Решение.
Мы перенесем все пароли в менеджер паролей KeePassX, где они будут храниться в зашифрованном виде. Все пароли будут генерироваться автоматически, содержать буквы верхнего и нижнего регистра, цифры и специальные символы. Длина пароля будет превышать 25 символов, что защитит Вас от подбора пароля.

Все пароли будут уникальны, и если злоумышленник получит один из Ваших паролей, это не приведет ко взлому других аккаунтов. Для дополнительной защиты пароли будут регулярно меняться.

В рамках обучения будут рассмотрены все основные способы кражи паролей: от фишинговых страниц до кражи сессий из браузера. Кражу паролей из браузера мы будем разбирать детально, и в процессе обучения Вы сможете потренироваться красть пароли, сохраненные в Вашем браузере.

Угроза: криминалистический анализ (извлечение информации при наличии физического доступа к устройству).

Последствия.
Получение доступа ко всей информации на Вашем жестком диске и в оперативной памяти, анализ полученной информации и извлечение ценных для недоброжелателя артефактов.

Решение.
Все данные на Вашем компьютере будут надежно зашифрованы.

Первым барьером для доступа к Вашим файлам будет комплексное шифрование Вашей операционной системы, жестких дисков и внешних носителей.

Вторым барьером будут криптоконтейнеры, в которых будут храниться Ваши данные. На случай, если Вам придется выдать пароли, криптоконтейнеры будут иметь "двойное дно". В скрытой части криптоконтейнера Вы будете хранить самые ценные файлы. При правильном использовании обнаружить наличие "двойного дна" не способен ни человек, ни специальные программы, используемые специалистами по криминалистическому анализу.

Сами криптоконтейнеры не будут размещены в открытом виде, а будут надежно замаскированы. Маскировка криптоконтейнеров — комплекс мер, направленных на изменение криптоконтейнера таким образом, чтобы он, не теряя при этом своих свойств, не распознавался ни человеком, ни программой как криптоконтейнер. Это означает, что недоброжелатели не найдут на Вашем компьютере зашифрованзашифрованных файлов, если Вы сами им их не выдадите.

Многие знают, что при обычном удалении файлов специалисты легко смогут их восстановить. Это касается всех файлов, включая историю браузера, логи переписок, ключи шифрования. Вы можете ввести в поисковой системе «восстановление удаленных файлов» и увидите множество предложений от специализирующихся на данном виде деятельности компаний.

В рамках обучения мы научим Вас удалять файлы при помощи Метода Гутмана — алгоритма удаления данных с жесткого диска и внешних носителей, после которого восстановление данных невозможно ни с помощью специального программного обеспечения, ни в лабораториях.

Помимо жесткого диска и внешних носителей информации у компьютера имеется еще одно звено, из которого возможно извлечь ценную информацию, — это оперативная память (ОЗУ, энергозависимая память компьютера). В основном анализ оперативной памяти используют для получения ключей шифрования криптоконтейнеров.

Программы для работы с криптоконтейнерами хранят ключи в оперативной памяти, откуда их и извлекают специалисты. Для предотвращения атаки на ОЗУ мы будем использовать специальное программное обеспечение — «Красную кнопку».

Если у Вас будет желание, в рамках курса мы можем сделать слепок Вашей оперативной памяти и провести его анализ. Это поможет Вам оценить и возможности профессионального криминалистического софта, и уровень Вашей защищенности.

КОНТАКТЫ ДЛЯ ЗАПИСИ НА ОБУЧЕНИЕ

help@VektorT13.pro

help@VektorT13.pro