Виртуальная система

Та операционная система, в которой запущен браузер и с которой читается эта лекция -- это хост система. Она так называется потому что **является платформой для всех запускаемых в ней приложений**. Запускать всё в одной системе удобно, но у этого есть один большой минус: если все приложения используют одно систему, то они могут влиять друг на друга, смотреть системные настройки, пытаться отслеживать систему по её уникальным параметрам. А если попадает вирус на хост, то последствия её более масштабные: всей безопасности наступает конец. Потому что из хоста можно управлять всем, и никакие настройки безопасности тут не помогут.

Поэтому критически важно не устанавливать на хост ничего лишнего и подозрительного. Системе с вирусами настройки безопасности и виртуальные машины не помогут.

Кстати, не только вирусы занимаются отслеживанием системы, выявлением её уникальных идентификаторов и т.п. Функции телеметрии в той или иной степени присутствуют в любой системе, а главное они часто встречаются в проприетарных ПО(хотя бывают в абсолютно любых программах и даже open source). Поэтому есть необходимость в максимальной виртуализации, чтобы на хост системе был только надёжный минимум, а всё остальное работало в виртуальных машинах, в которых вопрос защиты системы не стоит.

Начнём с начала. **Что такое виртуальная машина?** -- это система, которая работает в специальной программе для виртуализации. Причём в виртуальной среде с полной виртуализацией можно запустить любую систему, даже отличного типа от хост системы. Например, на linux развернуть windows или на оборот. В общем инструмент очень мощный. И ещё один важный момент, можно построить виртуальную внутреннюю сеть, которая будет жить по своим правилам.

Вообще локальных сетей есть много. Например, если подключение осуществляется через роутер, то все устройства, подключённые к роутеру, состоят в локальной сети. Главные отличительные черты локальной сети: её участники обмениваться данными между собой через специальное устройство(маршрутизатор), которое поддерживает эту сеть. Через него идут все запросы, и оно доступно из внешней сети. В сети с роутером эту функцию берёт на себя непосредственно сам роутер. Устройство, которое обрабатывает все запросы в локальной сети указывается в настройках как гейт или шлюз. В обычной домашней локальной сети роутер ещё обеспечивает доступ к внешнему миру, направляя запросы в интернет. Если вы представили у себя в голове эту картину, значит вы уже понимаете, что такое локальная сеть.

Переходим ко второму этапу

Сюда добавляется OpenVPN. Он создаёт в системе виртуальный адаптер, на который переключаются все соединения в системе. Это виртуальный компонент, его не существует в виде оборудования. Если до этого у вас был один адаптер, то это ethernet адаптр, которые установлен на материнской плате компьютера. Работу нового TAP адапра поддерживает программа OpenVPN. Возникает вопрос, а как же он подключается к интернету тогда, если не его не существует? - Он использует имеющийся реальный адаптер. То есть openvpn оборачивает весь интернет трафик и направляет его на vpn сервер через реальный адаптер, он выступает виртуальным слоем. Помимо этого **у openvpn есть ещё одна важная функция - шифрование всего**

проходящего через него трафика, чтобы даже если его перехватили, передаваемые данные были в нечитабельном виде.

Многие сайты работают на https, это протокол обмена данными с шифрованием. Но даже его не достаточно, потому что при перехвате https пакета видно сервер, куда он направляется. Это случается потому что шифрование делается на разных уровнях. Есть модель OSI по которой всё, что есть в системе, делится на 7 уровней. Чем ниже уровень, тем меньше абстракция данных. Суть в том, что на каждом уровне храниться своя информация о данных. ssl работает на 4 уровне - транспортном уровне. А данные о конечном сервере храняться на 3 уровне и ssl с ними ничего не делает. Поэтому роль VPN в системе важна, он работает на 3 уровне(сетевом) и защищяет информацию о назначении пакета и его содержании(даже если он был уже зашифрован ssl).

Следующий шаг

Добавление нового слоя безопасности - виртуализации систем. Это делается при помощи VirtualBox, который поддерживает полную виртуализацию в том числе компонентов. Его альтернатива: VMware. Он может быть удобнее при одновременной работе с большим числом машин, но на первое время надо пробовать работать с VirtualBox, потому что это проверенное временем open source решение.

С помощью whonix gateway будет создана новая внутривенная сеть, она работает поверх текущего подключения. Если в системе стоит VPN, то трафик с виртуалок через gateway так же пойдёт через VPN.

Схема подключения виртуалки через gateway: Виртуалка - Whonix Gateway - основной адаптер в системе(виртуальный TAP, если работает OpenVPN) - сеть.

И роль whonix gateway тут обернуть трафик и направить его через tor. Он работает по принципу: либо данные с него идут через тор, либо не идут вообще никак.

Первым делом скачиваем и устанавливаем VirtualBox последней версии. Найти его можно на странице загрузок на официальном сайте. Нам нужна версия для Windows hosts.

Для настройки работы через TOR надо создать защищенную внутреннюю сеть. Для этих целей используется Whonix. Лучшим способом установки является не установка exe версии для windows, а **прямой импорт в виртуальную машину**. Найти образы для импорта можно на официальном сайте whonix. Нам потребуется только Gateway. Его надо загрузить по ссылке Whonix with XFCE.

После окончания загрузки достаточно будет открыть загруженный файл двойным кликом, запустится меню импорта VirtualBox. Единственное, что надо будет изменить в параметрах машины -- **перегенерировать MAC адрес**. Для этого надо будет поставить соответствующую галочку внизу(Reinitialize the MAC address of all network cards)

После импорта в меню VirtualBox появится новая виртуальная машина Whonix-Gateway. Если её запустить, то запустится копия linux, которая обеспечивает работу gateway. Но лучше сразу изменить настройки и отключить графический интерфейс, который gateway не так нужен. Для этого выбираем виртуальную машину одинарным кликом и нажимаем кнопку **Settings(Настройки)** вверху. Затем переходим в пункт **Display(Дисплей)** и уменьшаем объём **Video Memory(видео память)** до **4MB**. В пункте **System(Система)** в первой вкладке **Mother board(Материнская плата)** устанавливаем объём **Base memory(Основная память)** значение **256 MB(МБ)**. После этого жмём ок и можно запустить машину, чтобы убедиться, что она работает.

После загрузки, которая длится около минуты, запустится консольный linux с меню входа в систему. Настройки по умолчанию:

Имя пользователя: **root**

Пароль: **changeme**

пароль в процессе ввода не отображается

Основные команды для управление gateway:

- service tor restart -- перезапустить тор, это принудительно закроет все текущие соединения.
- poweroff -- выключить gateway
- passwd -- установить новый пароль текущему пользователю
- killall -HUP tor -- обновить tor. Все новые соединения будут под новым адресом, но если есть активные соединения, они продолжат работать.

В последующих практических материалах будет непосредственная установка виртуальных операционных систем. **Чтобы интернет на них работал виртуальная машина whonix gateway должна быть постоянно запущена в фоне.** Без этого интернет на виртуальной машине будет отсутствовать.

На некоторых системах функция Virtualization Technology(VT) для Intel или AMD-V для and не включены по умолчанию. Без них не получится установить 64 битные системы. windows и linux, которые мы будем устанавливать, есть и в 32 битном варианте, но если основная система x64, а в VirtualBox при дальнейших установках 64bit не будет доступен, **зайдите в BIOS и включите соответствующую технологию**.