Преимущества и недостатки системы Qubes

Арс Либрев 18.12.2024

После публикации видео о возможности достижения безопасности на компьютере, в котором в том числе, говорилось о том, что одним из наиболее надежных инструментов безопасности является виртуализация, мне задавали много вопросов о системе Qubes, которая как раз и построена полностью на использовании виртуализации. Действительно, почему я ни словом ее не упомянул? Я решил пояснить преимущества и недостатки данной системы, чтобы пользователи могли сами решить, подходит им она или нет.

Сразу скажу, что я не упомянул в видео об этой системе, потому что просто не нашел ей места. Попытка упомянуть ее разрывала повествование и нарушалась последовательность. Поэтому решил не трогать ее. Теперь конкретно о некоторых моментах данной системы.

Для начала напомню, что собой представляет Qubes. Эта система, в которой вся активность разделена по виртуальным машинам — то есть отдельным операционным системам. Таким образом имеет место высокая изоляция разных процессов, и сбои в одном не влияют на другой. Если будет взломана одна ОС, это не повлечет компрометацию всей системы. При этом виртуальные машины имеют только необходимые пакеты, что делает их более легковесными, чем полноценные виртуалки в иных системах, а также снижает поверхность атаки. При этом реализован механизм зависимости виртуалок от шаблона, за счет чего обновление каждой ОС происходит за счет обновления шаблона — не нужно обновлять каждую виртуалку по отдельности. Изоляция подключения к Интернету осуществляется не только за счет вынесения подключения в отдельную ОС, но также и за счет реализации механизмов фильтрации на уровне взаимодействия ОС, что создает дополнительную безопасность при компрометации виртуалки, подключаемой к Интернету.

В Qubes интегрированы инструменты Whonix, что позволяет осуществлять приватный Интернет-серфинг, будучи защищенным даже от активного деанона. Напомню, Whonix состоит из двух виртуальных машин, одна из которых все соединения производит через сеть Tor, анонимизируя их, а другая из которой и осуществляется Интернет-активность, подключается к ней по виртуальной локальной сети. Таким образом, система из-под которой и происходит обращение к ресурсам не знает ни реальный ip-адрес, ни MAC-адрес, поскольку не связана с сетевым адаптером, а имеет лишь виртуально эмулированный. Если такая система будет взломана, или если в ней будет выполнен вредоносный java-скрипт, или в браузере в ней будет активирован WebRTC, ip-

адрес не будет слит, поскольку система его не знает, она имеет лишь ip в виртуальной локальной сети, который является стандартным, и по которому невозможно провести никакую идентификацию.
К преимуществам Qubes можно также отнести вынесение в отдельный интерфейс подключений USB-устройств. Таким образом, эта потенциально опасная составляющая имеют серьезную изоляцию, что препятствует вредоносному ПО, находящемуся на USB-носителях, причинять системе ущерб. Также стоит отметить двухуровневый буфер обмена, который облегчает перенос файлов между системами, и в то же время препятствует эксплуатации дыр, связанных с общим буфером обмена, поскольку каждая ОС обладает своим буфером, и уже они связаны между собой. Еще отдельный уровень изоляции имеет микрофон. Таким образом, система Qubes является одним из самых надежных инструментов безопасности.
Теперь о минусах Qubes. Во-первых, система Qubes очень прихотлива к железу. Не на каждый компьютер ее возможно установить, не на каждом оборудовании ее получится использовать. Это уже губит возможность рекомендовать эту систему широкому кругу пользователей.
Во-вторых, эта система весьма специфическая, и если у пользователя нет достаточного опыта в работе с системами GNU/Linux, он может просто запутаться. Многие настройки усложнены. В общем, по уровню удобства, она даже рядом не стояла с Debian или Devuan и уж тем более с Linux Mint, даже при использовании в них самих виртуализации, например с помощью Менеджера виртуальных машин.
В-третьих, версия Whonix для Qubes не имеет многих функций безопасности, которые реализованы в версиях для других систем. А это уже минус именно безопасности, причем в наиболее ключевом моменте — приватной Интернет-активности. Таким образом, использование Whonix в той же Linux Mint или Debian, в некоторых аспектах, может быть даже более безопасно. Конечно важно, что лишь в некоторых аспектах, поскольку тот уровень изоляции компонентов и функций системы, который реализован в этой системе, даже близко не сравнится с тем, что можно сделать в иных системах.
Если вам повезло иметь устройство, которое не имеет проблем с установкой Qubes, вы обладаете достаточным опытом или просто не боитесь трудностей, а также если недостатки безопасности версии Whonix в этой системе вам не кажутся серьезными — например, поскольку ее достоинства для вас важнее — то можете смело ее использовать.
Таким образом система Qubes при всех своих достоинствах, подойдет далеко не всем. Она, увы, остается уделом узких энтузиастов.