Курс по анонимности и безопасности Linux

Установка и настройка Linux

Смена DNS Linux Mint

Установка и настройка VPN для Linux Mint

Установка и настройка VPN для Whonix Workstation

Создаем цепочку VPN-Tor-VPN

Ставим в автозапуск VPN

Установка и настройка Whonix Workstation и Whonix Gateway на виртуальной машине

Настройка браузера на Whonix Workstation

Взлом Wi Fi

Дополнительный материал

Ссылка на образ ISO

Руководство пользователя Linux Mint 18

Выбор и покупка виртуального сервера (VPS)
[spoiler]
В обучении данный сервер настраивается для использования перед TOP на хост машине, а основная работа уже будет с виртуальной машины Хуникс воркстейшен на которой будет еще один впн, это очень важный момент. Впн здесь нужен даже не для нужд анонимности, а для того, чтобы надежно зашифровать траффик и скрыть от провайдера использование TOP.

1. Регистрируем саморег яндекс денег при помощи сервиса sms-activate.ru (стоит 1 рубль). Выпускаем при помощи этой же вирт

смс виртуальную карту и аварийныые коды.

2.Регистрируем аккаунт пейпал. Нужен более менее свежий скан паспорта, инн можно узнать на сайте Госуслуг https://www.gosuslugi.ru/pgu/fns/findInn

3.Привязываем к пейпал карту яндекс.

4. Анонимно пополнить яндекс можно с тех же биткоинов используя обменники

5. Регистрируем аккаунт Didgital Ocean. Указываем имя и фамилию нашего скана.

6. Учетку желательно регистрировать на зарубежную почту вроде gmail.com и по возможности делать это с айпи адреса который не принаддежит датацентру (сокс5 прокси, дед). Если такой возможности нет, то можно использовать браузерный впн Zenmate

7.Зачастую аккаунт морозится после первой оплаты (если регили с впн), нам нужно написать админам, что мы собираемся использовать их сервер исключительно для благих целей вроде хостинга сайта с котиками и если необходимо готовы предоставить скан паспорта. Как правило проверка всегда проходит успешно. Именно Didgital Ocean не принципиально брать можно воспользоваться сайтом poiskvps.ru

Нам подойдет даже самый дещевый сервер с 256 мб оперативной памяти, главное обрати внимание, чтобы не было ограничений по скорости из стран бери Европу – Нидерланды, Германию, Австрию, Францию и т. д.
[/spoiler]

Установка и настройка VPN

[spoiler]
Далее идет сам подъем сервера.

1.Создаем дроплет дебиан в нашей учетке ДО, страну выбираем Германию или Нидерланды (самая лучшая скорость к России).

2.На почту придут данные для рут доступа на сервер.

3.Логинимся на наш сервер при помощи команды ssh root@айписервера

Соглашаемся добавить сервер в список известных хостов вбив yes

4. Вводим наш пароль от root,который пришел на почту. В терминале crtl +v не работаем вставляейте правой кнопкой мыши.

5. Нам автоматически предлагают сменить пароль.

6. Вводим опять пароль от root после чего нужно два раза ввести новый пароль.

Устанавливайте сложный пароль около 15-20 символов с разным регистром, цифрами и символами][=-?><_, желательно при использовании генератора паролей. Это должно обезопасить нас от любого брута.

В терминале вводимые символы не отображаются знаком *, ничего страшного, все равно вводим и жмем enter

Обновляем систему деда apt-get update && apt-get dist-upgrade

Далее идет подъем впн. Тут два вариана, делать все долго вручную либо использовать автоматизированный скрипт с гитхаба. Ученик здесь решает самостоятельно, что ему нужно. Для примера здесь напишу вариант со скриптом.

Заходим на гитхаб, обращаем внимание, что данный скрипт на сайте уже достаточно давно, регулярно обновляется и у него большой рейтинг, при особом желании можно даже ознакомиться с иходным кодом.

https://github.com/Nyr/openvpn-install

Скачивается и запускается скрипт командой

wget https://git.io/vpn -O openvpn-install.sh && bash openvpn-install.sh

Нам показывает айпи нашего сервера жмем интер

Предлагает выбрать порт, можно оставить 1194 либо указать какой-нибудь экзотический.
в имени клиента убираем client и вводим любое имя конфига

Ждем пока скрипт сгенирирует все необходимые сертификаты и закончит работу, новоиспеченный конфиг появится в папке /root/нашеимя.ovpn

Открываем новый терминал (терминал с консолью сервера не трогаем) и скачиваем конфиг
sudo scp root@айпинашегосервера:~/имянашеговпн.ovpn /home/user/Downloads

После этого файл можно найти в папке /home/user/Downloads

Запускаем наш конфиг командой

sudo openvpn /home/user/Downloads/имяконфига.ovpn

Если клиент Openvpn не стоит то устанавливаем его командой

sudo apt-get install openvpn

Заходим на чекер анонимности 2ip.ru видим, что впн работает, но сервис видит наличие двухсторонего туннеля и даже выдает vpn fingerprint.

Нам такой фигни естественно не надо, поэтому продолжим настройку сервера и конфигов.

Заходим снова в терминал с сервером.

1.Отключаем ведение любых системных логов удаляя системную утилиту rsyslog

apt-get remove rsyslog

2. открываем наш серверный конфиг

nano /etc/openvpn/server.conf

если консольный текстовый редактор не установлен, то устанавливаем

apt-get install nano

в конфиге нам необходимо добавить строчку mssfix 0

также убедимся что отключены логи впн и есть строка verb 0

жмем ctrl+ o для сохранения изменений и ctrl + x для выхода

3. Настраиваем файрвол который блокирует любые подключения к нашему серверу кроме портов ssh и порта опенвпн (по дефолту 1194)

ставим файрвол ufw

sudo apt-get install ufw

разрешаем подключения по ssh

ufw allow ssh

Разрешаем подключения к порту openvpn

ufw allow 1194/udp (если создавали конфиг с tcp, то указываем tcp вместо udp)

Залаем правило перенаправления пакетов ufw

nano /etc/default/ufw

в строке DEFAULT_FORWARD_POLICY=»DROP». Дроп меняем на ACCEPT, чтобы вышло
DEFAULT_FORWARD_POLICY=»ACCEPT»

Сохраняемся и выходим

Решаем проблему с определением двухстороннего пинга

g
nano /etc/ufw/before.rules

нужно закомментить строку поставив перед ней знак #
-A ufw-before-input -p icmp –icmp-type echo-request -j ACCEPT

Должно получиться так

ok icmp codes
-A ufw-before-input -p icmp –icmp-type destination-unreachable -j ACCEPT
-A ufw-before-input -p icmp –icmp-type source-quench -j ACCEPT
-A ufw-before-input -p icmp –icmp-type time-exceeded -j ACCEPT
-A ufw-before-input -p icmp –icmp-type parameter-problem -j ACCEPT
#-A ufw-before-input -p icmp –icmp-type echo-request -j ACCEPT

Сохраняемся и выходим

Включаем наш файрвол ufw enable

Открываем наш клиентский конфиг на хост машине и дописываем строчку
mssfix 0

Сохраняемся и выходим
[/spoiler]

Установка и настройка Whonix Workstation и Whonix Gateway на виртуальной машине

[spoiler]
Скрипт vpnfw.sh
[/spoiler]

4.Настройка браузера на Whonix Workstation

[spoiler]
Настройка браузера

1. Открываем чекер whoer.net

2. Необходимо удостовериться что выключен flash и java (не путать с java script). Выключается в графе addons>plugins, все

пункты должны быть отключены. Если нам нужны сайты, которые требуют данные технологии, то можно включить (на свой страх и риск)

3. Ставим нужные нам плагины

No Script (отключает java script на сайтах. ВАЖНО! Джава скрипт необходим для нормальной работы большинства сайтов, но также может использоваться злоумышленником для сбора информации и даже эксплойтирования уязвимостей в браузере. Разрешаем в плагине только те сайты, которым мы доверяем. Жизненный пример: злоумышленник размещает безобидную статью на форуме, где есть ссылка на его ресурс, переходя по ссылке мы переходим на сайт, где срабатывают вредоносные скрипты, при этом мы как правило не замечаем ничего подозрительного).

https everywhere (данный плагин принуждает сайты использовать зашифрованное соединение по протоколу https, если на сайте есть поддержка данной технологии, также в плагине можно указать опцию, которая блокирует любой http траффик в принципе. Жизненный пример: Злодей пишет траффик на выходной ноде тора и может свободно анализировать наш http траффик, т.к. он никак не зашифрован).

Self destructed cookies (кукисы – это вспомогательные файлы, которые хрянят настройки сайтов на нашем компьютере, могут быть как безобидными так и вредоносными см. evercookies, также наличие кукисов может быть доказательством, что нам принадлежит определенная учетка на форуме\соцсети. Данный плагин удаляет все кукисы сразу после закрытия вкладки\окна браузера)

Privacy settings (в данном плагине можно сразу указать опцию privacy and security по желанию, но самое важное – это отключить webrtc в пункте media peer connections enable)

Random agent spoofer (данный плагин позволяет подделывать нашу операционную систему\разрешение экрана\user agent и многое другое, при этом даже джаваскрипт не определяет нашу

настоящую систему)
[/spoiler]

Настройка виртуалки для взлома Wi-Fi

[spoiler]
1. Нужно сказать extension pack для VirtualBox http://download.virtualbox.org/virtualbox/5.1.14/Oracle_VM_VirtualBox_Extension_Pack-5.1.14-112924.vbox-extpack
Он нужен для того чтобы подключить USB Wi-Fi адаптер к виртуалке

2. Потом нужно скачать ISO дистрибутива wifislax
http://www.wifislax.com/category/download/nuevas-versiones/

Там будет 3 ссылки. Это один и тот же файл.

Устанавливаем пак для виртуалбокс

Создаем виртуалку с ISO wifislax. Жесткий диск ненужно крепить к нему.

При установке на виртуалбокс ISO wifislax название ОС указываем debian 64 bit
Запускаем (от имени администратора) ISO в live режиме. Т.е после рестарта виртуалбокса все данные на нем сотрутся.

При запуске выбираем язык

Non-ES Language selection-russion
[/spoiler]

Взлом Wi-Fi

[spoiler]
Предупреждение! Использование чужих точек – не панацея и само по себе является лишь небольшим ДОПОЛНЕНИЕМ к виртуальным машинам Whonix. Ни в коем случае нельзя использовать одно только подключение к чужой точке без других куда более важных мер, особенно, если эта точка находится неподалеку от вашего

основного места жительства.

Крайне рекомендуется при взломе использовать внешний usb wi-fi адаптер, это повышает эффективность процедуры на 50-70%. Также в последствии можно будет подключить к адаптеру более мощную направленную антену.

Недорогой и надежный вариант tp link TL-WN722N (около 1000 р.) http://www.tp-link.com/en/products/details/TL-WN722N.html

Ни в коем случае не покупайте другие модели тплинк.

Данное обучение можно проходить и со встроенным адаптером ноутбука, принцип не меняется.

Есть три основных способа взлома чужих сетей вайфай, которые нужно применять последовательно, т.е. если не сработал первый, переходить ко второму, если не сработал второй то к третьему и т.д.

1. Pixie script – самый быстрый (буквально 2-3 минуты) и простой способ получить пароль к чужой точке доступа. Используется уязвимость wps определенных моделей роутеров.

2. Отлов хендшейков (пакеты в которых роутер и устройство обмениваются зашифрованными пакетами с паролем) и дальнейшая расфшифрока данных пакетов.

3. Брут пинкодов WPS (reaver). Занимает от 4 до 8 часов, у роутера должен быть включен WPS. Подробней про впс здесь https://ru.wikipedia.org/wiki/Wi-Fi_Protected_Setup

Помимо данных трех есть еще способ с блокировкой чужой точки доступа и созданием ее фейка. Для него нужно иметь два вайфайадаптера. В виду сложности в обучении его не рассматриваю.

Инстукция по применению wifislax.

Загружаемся с флешки. При запуске не нужно ничего выбирать,

везде жмем enter.

ПЕРВЫЙ СПОСОБ

1.Включаем пикси

Стартменю (K) » Wifislax» Wpa-wps» Pixie Script

2.Выбираем наш сетевой адаптер (wlan0 или wlan1) и переводим адаптер в режим мониторинга MODO MONITOR, далее сканировать точки доступа INICIAR ESCANEO.

3.Выбираем нужную нам точку и жмем INICIAR ATAQUE.

При успехе рядом с точкой появится желтая звезда, и пароль затем можно найти на рабочем столе в папке Wireless-keys.

ВТОРОЙ СПОСОБ

Можно ловить хендщейки выборочно, но я рекомендую использовать команду besside-ng

1.Убиваем процессы, которые используют нашу сетевую карту

```
sudo kill 1623
sudo kill 1718
```

2.Включаем нашу карточку в режим мониторинга.

```
sudo airmon-ng start wlan0
```

3.Запускаем команду besside-ng

```
sudo besside-ng wlan0
```

В разделе TO OWN [сети которые мы пытаемся нагнуть]
В разделе OWNED [сети чьи хендщейки мы уже получили]

Скрипт рекомендуется оставить работающим на 5-12 часов для макс. результата.

4.Открываем на рабочем столе ярлык HOME и смотрим сожержимое

папки /root/
файл besside.log это лог результата работы програмы

SSID -имя сети
BSSID -макадрес сети вида

43:o3:d3:vb:d5:56

Первая половина данного мака
43:o3:d3 – это общий идентификатор произоводителя устройства, например, тп-линк, д-линк и т.д.

Вторая половина
vb:d5:56 – уникальный идентификатор конкретного устройства.

Файл, который содержит сами хендшейки это wpa.cap

Т.к. все данные при загрузки с лайв-флешки не сохраняются имеет смысл сохранить файлы wpa.cap и besside.log на другой носитель.

5. Редактируем файл с хендшейками

Запускаем wireshark

sudo wireshark

открываем наш файл wpa.cap

Каждый отдельный хендшейк здесь – это три последовательных пронумерованных пакета.

Так как в файле все хендшейки идут подряд, нам нужно разделить этот файл, чтобы каждой точке доступа соответствовал один конкретный хендшейк (три пакета)

Для этого смотри раздел Source видим, что там уже отображается производель роутера (програма автоматически прочитала первую половину значения макадреса) и уникальный идентификатор. Далее см. в файле бессайд.лог какой-именно сети соответствует данный макдрес.

Linux, [30.01.17 16:15]

Нажимаем File » Export Specified Packets » выбираем Specify a packet range » вводим в поле номера первых трех пакетов 1-3

Имя файла вводим такое же как у точки доступа (см. файл бессайд лог) и жмем Save.

Затем нам нужно повторить данную операцию со всеми остальными пакетами, для этого вбиваем в поле Specify a packet range

4-6
7-9
10-12
13-15
16-18
и т.д. пока не закончим

Как только мы закончим нужно переименовать расширения всех файлов с имяточкидоступа.pcap на имяточкидоступа.cap Это нужно для сервиса.

Заходим на сайт http://wpa-sec.stanev.org регистрируемся, получаем на почту ключ.
Начинаем заливать наши хендшейки в разделе Submit

Как правило пароль подбирается за 10-15 минут, если процедура затягивается то скорей всего фейл. Все слабые пароли до восьми символов ломаются, сложные нет. Средняя статистика успеха где-то 20%.

ТРЕТИЙ СПОСОБ

Брутим wps. От 5 до 10 часов на точку

Основная программа для этого reaver, но в wifislax существует огромное кол-во автоматизированных скриптов для него, я покажу на примере одного из них.

Стартменю (K) » Wifislax» Wpa-wps» Goyscript wps

1.Выбираем номер нашего сетевого устройства и жмем enter

2.Ждем секунд 30-40 пока идет сканирование точек с ВПС,
после чего останавливаем процесс нажатием ctrl+c.

3.Выбираем порядковый номер нужной нам точки и жмем enter.

4.Далее непосредственно идет процесс брута. Если роутер почти сразу блокирует попытки, то врядли что-то выйдет.

На современных моделях роутеров данный способ практически не действует.

По фай вай скажу ряд моментов

1. Если злоумышленник получает доступ к твоей основной системе, то он получает доступ и к твоей сетевой карточке вайфай и видит все имена и макадреса всех точек, которые она ловит, а также твой личный мак адрес, а это скорей всего уже деанон. Можешь открыть например данный сервис https://wigle.net/ и посмотреть есть по твоему адресу точки, которые у тебя ловят.

2 .У твоего сетевого адаптера есть макадрес по которому тебя можно великолепно вычислять не важно к какой именно точке ты подключен. Даже если мак меняешь, то это не панацея (по последним исследованиям). Также никакой особой роли не играет, что подключаешься к точке за несколько км, вычислят по маку на ура, причем чем мощней антена, тем проще вычислять.

3. Если ты настраиваешь нормальную цепочку с использованием TOP + туннели или впн + виртуальная машина, то непонятна вообще роль соседского вайфай в данной истории. Сдеанонить TOp это задача уровня американского агентства нац. безопасности, да и то не факт что они смогут. А если злоумышленник получает доступ к машине то см. п.1
[/spoiler]

Sshuttle

[spoiler]
Начнем с того что автор не рекомендует использовать этот метод для анонимности если у нас есть впн.

Но несмотря на это ниже будет мини мануал поэтому поводу.

Сначала мы должны установить sshuttle на свой линукс минт

Команды:

```
pip install sshuttle
sudo apt-get install pip
sudo pip install sshuttle
```

На ВПС ничего устанавливать ненужно

Команда для подключение к серверу

```
sshuttle -r user@remoteserver 0.0.0.0/0 –vv
```

где username – логин на удаленном виртуальном сервере, sshserver – его IP-адрес или доменное имя, параметр 0.0.0.0/0 означает, что мы собираемся добавить в нашу таблицу маршрутизации правило, благодаря которому весь исходящий трафик будет отправляться на удалённый сервер, за исключением DNS-запросов. Разработчик намеренно не включает по умолчанию этот функционал для DNS, потому что у некоторых пользователей для выхода в интернет должны использоваться провайдерские серверы разрешения имен. Если мы можем пользоваться любыми DNS-серверами, то и запросы к ним можем “завернуть” в наш шифрованный SSH-туннель
[/spoiler]

Whonix

[spoiler]
Whonix – это две виртуальные машины Линукс Debian запущенные в программе Virtual Box, настроенные для максимальной безы\анонимности. Первый образ шлюз – Whonix Gateway, заворачивает весь наш траффик в сеть TOR, а второй рабочая

станция – Whoinix Workstation, с которой мы уже заходим в интернет\запускаем софт. Причем, рабочая станция настроена таким образом, что вообще не может принимать никакого траффика кроме сети TOR. Это полностью исключает любую возможную утечку нашего айпи адреса или днс. Более того, даже если злоумышленнику удастся получить удаленный доступ к нашей машине хуникс, единственное что он сможет получить это локальный айпиадрес, который абсолютно бесполезен.

На рабочей станции хуиникса легко настраивается впн, что избавляет нас от постоянного ввода предельно тупорылой капчи и защищает нас от недобросовестных выходных нод тора, которые могут сниффать траффик. При желании можно подключить к нашему шлюзу Хуиникс любую другую виртуалку\несколько виртуалок. Можете даже Виндоус подключить, только учитывайте при этом его дырявость.

1.Смена пароля.

В системе на обоих виртуальных машинах у нас два пользователя root и user, пароли для них по-умолчанию changeme. Для смены вводим:

```
sudo passwd user
sudo passwd root
```

2. Обновляется система командой sudo apt-get update && sudo apt-get dist-upgrade

3. Для установки чего либо вбиваем sudo apt-get install имяпрограммы

pidgin – джаббер
pidgin-otr – плагин otr шифрования для пиджина
keepassx- менеджер паролей
libreoffice – офисный пакет

Также можно устанавливать скаченные с сайтов проги вручную через sudo dpkg -i /путь/имя

или устанавливать через скрипты sudo sh /путь/имя
Обычно инструкции можно найти на этих же сайтах.

4. Для экономии оперативной памяти в настройках хуникс гетвей можно умеьшить ползунок до 150 мб. Тогда машина запустится в консольном виде. Если обратно увеличим – то снова будет графическая среда. Сэкономленую память можно выделить Хуникс Воркстейшен.
Обычно гетвей мы пользуемся только для обновления системы sudo apt-get update && sudo apt-get dist-upgrade
Также в случае проблем соединения с тор, можно перезапустить сервис sudo service tor restart

5. Графическая среда KDE не самая приятная, поэтому при желании ее можно сменить на более быструю xfce4 или mate

для этого вбиваем в консоли

sudo apt-get install mate
sudo apt-get install xfce4

После перезагрузки все должно работать.
[/spoiler]

Обфускация (маскировка) траффика

[spoiler]
Этот способ нужно использовать только если ваш провайдер блокирует VPN или TOR подключение

Команды

sudo apt-get install python2.7 python-pip python-dev build-essential libgmp-dev
pip install obfsproxy
sudo pip install setuptools

после этого мы можем выполнить команду запуска obfs и запустить openvpn:

/etc/init.d/obfs start
[/spoiler]

Флешка ключ

[spoiler]
Для того чтобы наш минт не запускался без флешки раздел boot нужно создать на этом флешке. Вспоминаем урок 1.Установка и настройка Linux Mint. Там начиная с 05:53 он объясняет как это сделать. Только там он создает раздел там куда будет установлен минт
Но мы должны выбрать и создать этот раздел на флешке.
[/spoiler]

Эффективные приемы сокрытия вашего рабочего траффика

[spoiler]
Самый простой способ сокрытия вашего рабочего траффика (Защита от сравнения слепков траффика и эффективное сокрытие от вашего провайдера анонимной зашифрованной сессии)
это использовать transmission торрент клиент https://transmissionbt.com/
Ставим его на наш минт и начинаем скачивать любой файл через торрент, штук 10-20 и ставить на раздачу. Как только закончится скачка снова запускаем его и так по кругу
Пока не закончим свои дела. Самое главное, все это нужно делать не под ВПН
Этот способ подойдет только для параноиков.
[/spoiler]