

Мяу

Подготовил: One-nine9

Настройка

Добро пожаловать в Hack The Box!

Прежде чем мы начнем с вашей самой первой уязвимой машины, позвольте нам убедиться, что вы подключены к целевой сети и умеете обходиться с терминалом. При посещении страницы лаборатории Starting Point вам может быть предложено выбрать между подключением Pwnbox или файлом конфигурации VPN, который вы можете загрузить и запустить на своей виртуальной машине. Если вы еще не научились настраивать виртуальную машину, ознакомьтесь с [Сеттин граммВверх](#) модуль по Академии HTB.



Запустить Pwnbox очень просто, и вам не потребуется никаких дополнительных действий для подключения к целевой машине. Если вы загрузите новый экземпляр Pwnbox с параметром «Начальная точка», вы автоматически попадете в ту же сеть, что и цель. Вы можете узнать больше о Pwnbox [в этой статье](#).

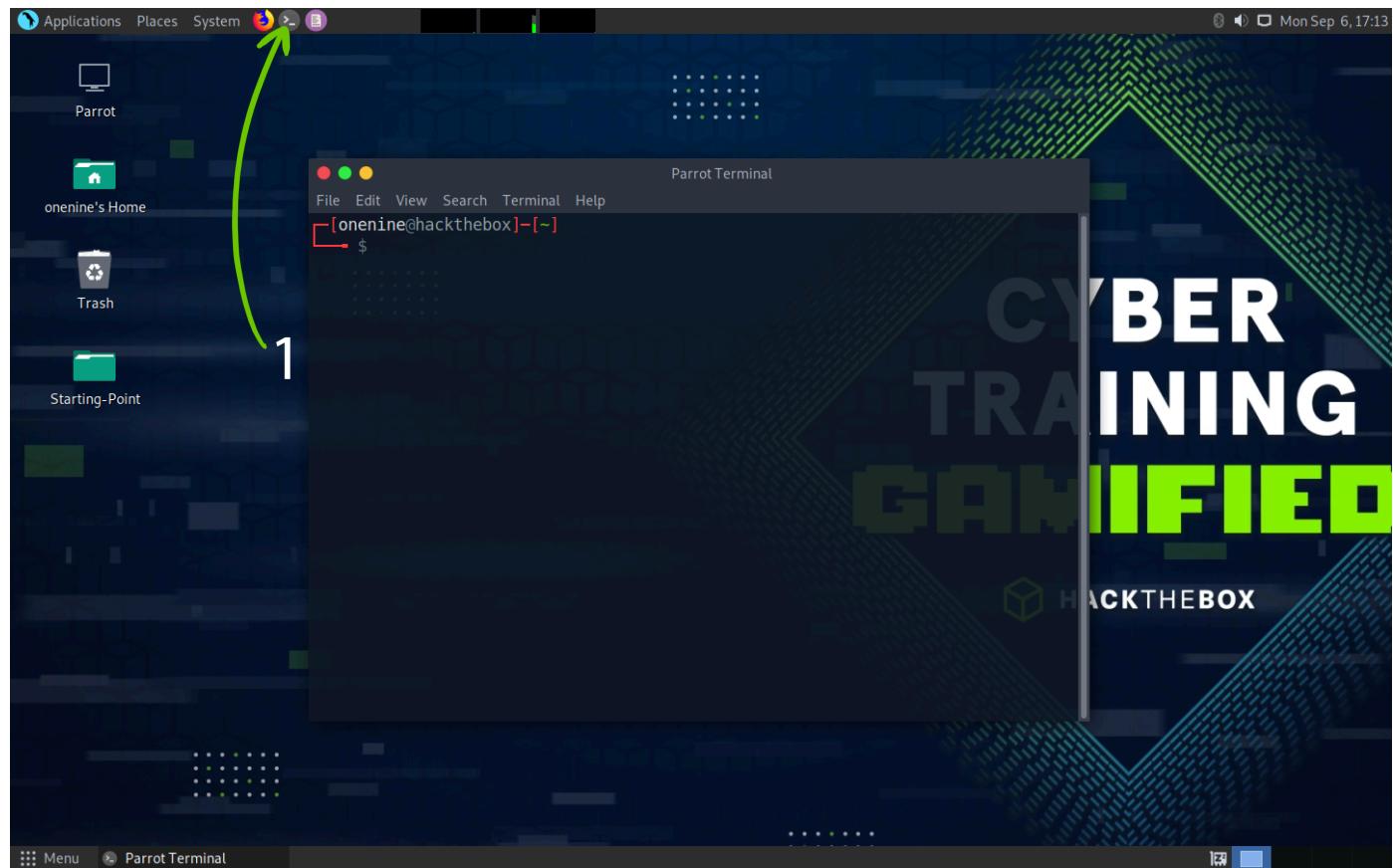


PWN BOX

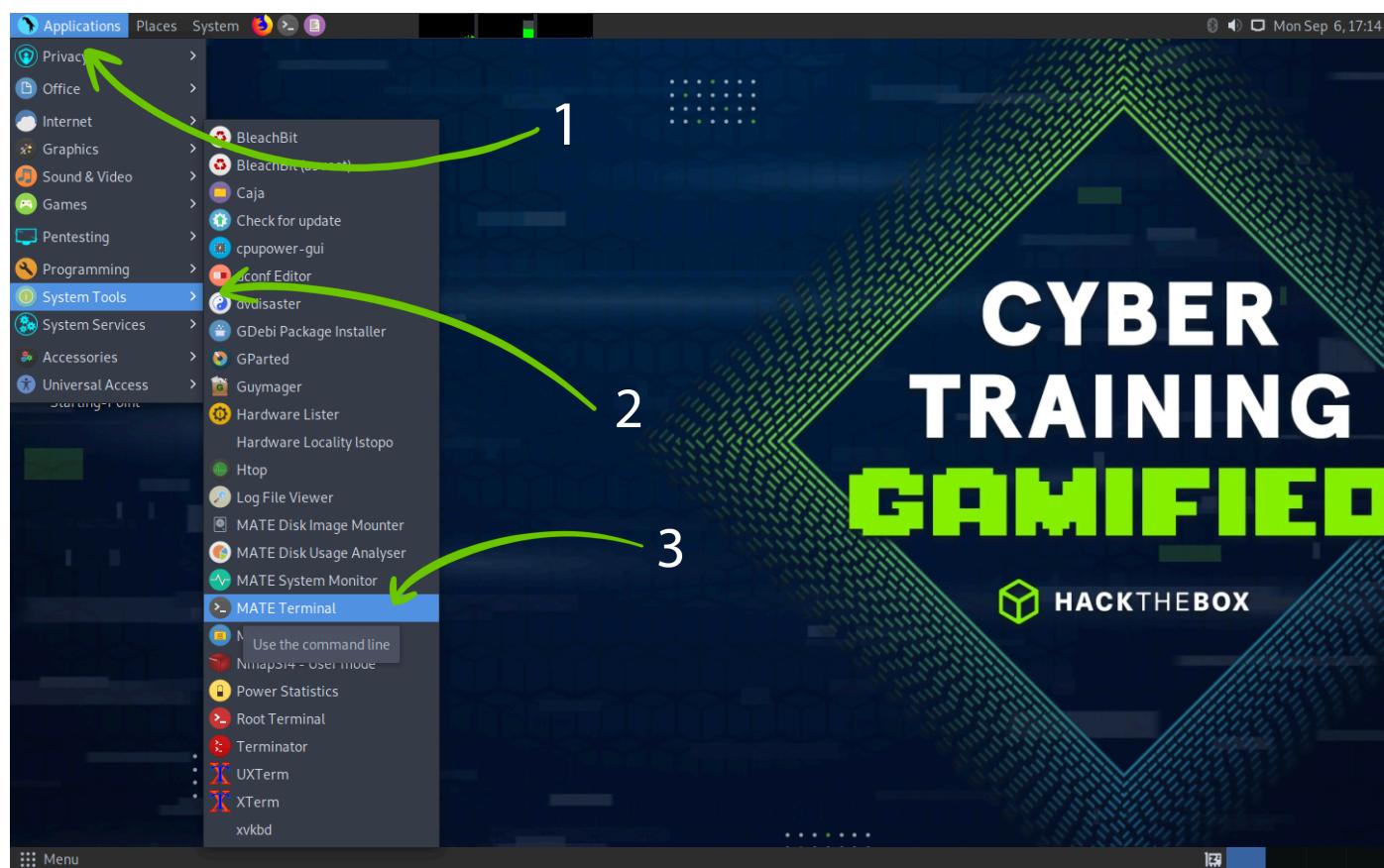
NOW AVAILABLE ON THE NEW PLATFORM!



Если вы решите загрузить файл конфигурации VPN (.ovpn) на свою виртуальную машину, то вот как использовать его для подключения к целевой сети. Чтобы открыть окно терминала, вы можете щелкнуть значок терминала на рабочем столе.



Кроме того, вы можете перейти в меню «Системные инструменты» и выбрать терминал оттуда. В этом случае мы используем терминал MATE. В конечном счете, неважно, какой терминал вы используете, главное, чтобы вы не заблудились. Наведя курсор на опцию терминала, можно увидеть описание инструмента: Используйте командную строку , что именно то, что мы будем делать дальше.



После выбора нашего окна терминала нам нужно будет указать, куда был загружен файл .ovpn. В большинстве случаев это находится в папке «Загрузки». Чтобы добраться туда правильно, давайте начнем с команды, которая означает изменить каталог , чтобы убедиться, что вы находитесь в своей домашней папке для текущего вошедшего в систему пользователя. Выполнение этой команды без указания местоположения для перехода просто поместит вас в ваш каталог. Таким образом мы можем убедиться, что все, кто читает это, находятся в правильной отправной точке (без каламбура). Следующая команда, которую мы можем ввести, это ls , который покажет нам папки домашнего каталога, некоторые из них Рабочий стол , Документы , Загрузки и более. Загрузки это то, что нас интересует, и мы используем cd Загрузки команда для навигации внутри него.

После перехода в каталог «Загрузки» введите ls чтобы убедиться, что файл .ovpn присутствует в системе, затем следует команда для запуска клиента OpenVPN и подключения к внутренней сети Hack The Box: sudo openvpn {имя файла}.ovpn , где {имя файла} следует заменить на имя вашего .ovpn для лаборатории Starting Point. Текст, отмеченный зеленым цветом и фигурными скобками {}, является заменой вашей собственной версии ввода. Это будет повторяться в рецензиях на «Отправную точку», так что имейте это в виду!

После запуска команды вам будет предложено ввести пароль суперпользователя, такой же, как текущий пароль для вашей учетной записи операционной системы. Не волнуйтесь, если вы не видите, что что-то вводится в терминал после ввода пароля. Это мера безопасности Linux, которая не позволяет другим лазить по вам через плечо. Завершите ввод пароля и нажмите клавишу Enter после завершения, чтобы инициализировать

OpenVPN-соединение.

Пусть сценарий конфигурации работает до тех пор, пока вы не увидите **Последовательность инициализации завершена сообщение на** самый конец вывода. После этого убедитесь, что в нем нет упоминаний о нескольких туннельных интерфейсах, таких как **тун1**, **тун2**, и так далее. Наличие нескольких туннельных интерфейсов может нарушить стабильность вашего подключения к цели и создать конфликты маршрутизации в вашей операционной системе, что только вызовет разочарование. Должно быть только **тун0** упоминается в выводе, как показано на изображении ниже.

```
$ cd
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
$ cd Downloads
$ ls
{filename}.ovpn
$ sudo openvpn {filename.ovpn}
[sudo] password for {username}: {your_VM_password}

2021-09-24 20:20:41 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2021-09-24 20:20:41 DEPRECATED OPTION: --cipher set to 'AES-128-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-GCM). Future OpenVPN version will ignore --cipher for cipher negotiations. Add 'AES-128-CBC' to --data-ciphers or change --cipher 'AES-128-CBC' to --data-ciphers-fallback 'AES-128-CBC' to silence this warning.
2021-09-24 20:20:41 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021

[...] Output omitted [...]

2021-09-24 20:20:41 net_addr_v6_add: {dead:beef:IPV6} dev tun0
2021-09-24 20:20:41 net_route_v4_add: 10.10.10.0/23 via 10.10.14.1 dev [NULL] table 0 metric -1
2021-09-24 20:20:41 net_route_v4_add: {IPV4} via 10.10.14.1 dev [NULL] table 0 metric -1
2021-09-24 20:20:41 add_route_ipv6(dead:beef::/64 -> {IPV6}) metric -1) dev tun0
2021-09-24 20:20:41 net_route_v6_add: dead:beef::/64 via :: dev tun0 table 0 metric -1
2021-09-24 20:20:41 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2021-09-24 20:20:41 Initialization Sequence Completed
```

Если вы чувствуете себя потерянным, вам, вероятно, нужно освежить свои навыки работы с Linux. Чтобы узнать больше о навигации и использовании Linux в качестве нового пользователя, вам следует проверить нашу [Основы Linux](#) модуль по Академии HTB. После его завершения вы окажетесь на правильном пути и сможете вернуться к отправной точке с новым набором навыков, которые снизят разочарование, которое испытывают многие новые пользователи, впервые приступая к пентесту без предварительного контакта. с Linux, интерфейсами командной строки и большими возможностями.



Убедившись, что все в выводе в порядке, вы можете открыть новую вкладку или окно терминала. Оставьте текущий работающим; в противном случае вы потеряете соединение с целью. Теперь вы готовы начать.

Введение

При первом запуске теста на проникновение или любой оценки безопасности на цели, первый шаг известен как **перечисление**. Этот шаг состоит из документирования текущего состояния цели, чтобы узнать как можно больше. можно об этом.

Поскольку теперь вы находитесь в той же виртуальной частной сети (VPN), что и цель, вы можете напрямую получить к ней доступ, как и любой другой пользователь. Если целью является веб-сервер, на котором запущена общедоступная веб-страница, вы можете перейти к ее IP-адресу, чтобы увидеть, что содержит страница. Если целью является сервер хранения, вы можете подключиться к нему, используя тот же IP-адрес, чтобы просмотреть файлы и папки, хранящиеся на нем, при условии, что у вас есть необходимые учетные данные. Вопрос в том, как вы находитите эти услуги? Вы не можете искать их вручную, потому что это займет много времени.

Каждый сервер использует **порты** для передачи данных другим клиентам. Первые шаги на этапе перечисления включают сканирование этих открытых портов, чтобы увидеть цель цели в сети и возможные уязвимости, которые могут появиться в службах, работающих в ней. Для быстрого сканирования портов мы можем использовать инструмент под названием **nmap**, о котором мы подробнее расскажем в главе «Перечисление» этой статьи.

Найдя открытые порты на цели, мы можем вручную получить доступ к каждому из них, используя различные инструменты, чтобы узнать, есть ли у нас доступ к их содержимому или нет. Для доступа к разным службам будут использоваться разные инструменты или сценарии. Их может обнаружить и изучить начинающий пентестер только со временем и практикой (и прилежным гуглением). Тестирование на проникновение на 90% состоит из исследований в Интернете о продукте, который вы тестируете. Поскольку технологическая экосистема постоянно развивается, невозможно знать все обо всем. Главное — уметь искать нужную информацию. Способность к

Эффективное исследование — это навык, который вам нужен, чтобы постоянно адаптироваться и развиваться до своего высшего качества.

Цель здесь не скорость, а дотошность. Если ресурс на цели будет упущен на этапе перечисления вашего теста, вы можете потерять жизненно важный вектор атаки, который потенциально сократил бы ваше рабочее время на цели вдвое или даже меньше.

перечисление

После того, как наше VPN-соединение успешно установлено, мы можем пропинговать IP-адрес цели, чтобы увидеть, достигают ли наши пакеты места назначения. Вы можете взять IP-адрес вашей текущей цели со страницы лаборатории Starting Point и вставить его в свой терминал после ввода **ping** команду, как показано ниже.

```
$ ping {target_IP}
PING {target_IP} ( {target_IP} ) 56(84) bytes of data.
64 bytes from {target_IP}: icmp_seq=1 ttl=63 time=20.4 ms
64 bytes from {target_IP}: icmp_seq=2 ttl=63 time=22.0 ms
64 bytes from {target_IP}: icmp_seq=3 ttl=63 time=20.2 ms
64 bytes from {target_IP}: icmp_seq=4 ttl=63 time=19.8 ms
^C
--- {target_IP} ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 19.788/20.603/22.026/0.849 ms
```

После четырех успешных ответов от цели мы можем определить, что наше соединение установлено и стабильно. Мы можем отменить команду ping, нажав кнопку **CTRL+C** комбинация на нашей клавиатуре, которая будет отображаться в терминале, как отмечено выше зеленым цветом. Это вернет нам контроль над вкладкой терминала, откуда мы сможем перейти к следующему шагу — сканированию всех открытых портов цели, чтобы определить запущенные на ней службы. Чтобы начать процесс сканирования, мы можем использовать следующую команду с **nmap** сценарием. **nmap** расшифровывается как Network Mapper, и он будет отправлять запросы к целевым портам в надежде получая ответ, тем самым определяя, открыт указанный порт или нет. Некоторые порты по умолчанию используются определенными службами. Другие могут быть нестандартными, поэтому мы будем использовать флаг обнаружения службы. **-СВ** К определить имя и описание идентифицированных услуг. Текст, выделенный зеленым цветом и фигурными скобками {} является заменой вашей собственной версии ввода. В этом случае вам нужно будет заменить {целевой_IP} часть IP-адресом вашей собственной цели.



```
$ sudo nmap -sV {target_IP}

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-24 20:36 BST
Nmap scan report for {target_IP}
Host is up (0.050s latency).
Not shown: 999 closed tcp ports (reset)

PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds
```

После завершения сканирования мы выявили

порт 23/TCP

в

открытым

государство, управляющее

телнет оказание услуг. Следующий [быстрая слизь граммLe Search](#) этого протокола мы узнаем, что telnet — это старый сервис, используемый для удаленного управления другими хостами в сети. Поскольку цель запускает эту службу, она может получать запросы на подключение через telnet от других хостов в сети (например, от нас самих). Обычно запросы на подключение через telnet настраиваются с комбинацией имени пользователя и пароля для повышения безопасности. Мы видим, что это относится и к нашей цели, поскольку нас встречает баннер Hack The Box и запрос от цели на аутентификацию, прежде чем нам будет разрешено продолжить удаленное управление целевым хостом.



```
$ telnet {target_IP}
```

```
Trying {target_IP}...
Connected to {target_IP}.
Escape character is '^]'.
```

Hack The Box

Meow login:

Нам нужно будет найти некоторые учетные данные, которые работают, чтобы продолжить, поскольку на цели нет других открытых портов, которые мы могли бы исследовать.

плацдарм

Иногда из-за ошибок конфигурации некоторые важные учетные записи могут быть оставлены с пустыми паролями для обеспечения доступности. Это серьезная проблема с некоторыми сетевыми устройствами или хостами, оставляющая их открытыми для простых атак методом перебора, когда злоумышленник может попытаться войти в систему последовательно, используя список имен пользователей без ввода пароля.

Некоторые типичные важные учетные записи имеют понятные имена, например:

- `администратор`
- `администратор`
- `корень`

Прямой способ попытаться войти в систему с этими учетными данными в надежде, что один из них существует и имеет пустой пароль, — это ввести их вручную в терминал, когда хосты запросят их. Если бы список был длиннее, мы могли бы использовать скрипт для автоматизации этого процесса, передав ему список слов для имен пользователей и один для паролей. Как правило, списки слов, используемые для этой задачи, состоят из типичных имен людей, сокращений или данных из предыдущих утечек из базы данных. На данный момент мы можем вручную попробовать эти три основных имени пользователя выше.



The screenshot shows a terminal window with a dark background and light-colored text. At the top, there are three small colored circles (red, yellow, green). The terminal output is as follows:

```
Meow login: admin
Password:
Login incorrect
Meow login: administrator
Password:
Login incorrect
Meow login:
```

Первые два нам не так повезло. Когда дела идут вниз, важно продолжать идти, быть настойчивым. Мы не сможем добиться успеха, если не испробуем все возможности. Попробуем последний.

```
Meow login: root
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Mon 06 Sep 2021 03:15:22 PM UTC

System load: 0.0          Processes: 195
Usage of /: 41.7% of 7.75GB Users logged in: 0
Memory usage: 4%          IPv4 address for eth0: {target_IP}
Swap usage: 0%

* Super-optimized for small spaces - read how we shrank the memory
  footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

72 updates can be applied immediately.
29 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Wed Jul 7 10:55:01 UTC 2021 on tty1
```

Успех! Мы вошли в целевую систему. Теперь мы можем пойти дальше и осмотреть каталог, в который мы попали, используя **команду**. Есть вероятность, что мы найдем то, что ищем.

```
# ls
flag.txt  snap

# cat flag.txt
b40abdf23665f766f9c61ecba8a4c19
```

The **флаг.txt** файл является нашей целью в этом случае. Большинство целей Hack The Box будут иметь один из этих файлов, который будет содержать хеш-значение, называемое **флаг**. Соглашение об именах для этих целевых файлов варьируется от лаборатории в лабораторию. Например, еженедельные и выведенные из эксплуатации машины будут иметь два флага, а **пользователь.txt** а также **корень.txt**. Именно цели CTF, а другие лаборатории будут иметь **флаг.txt**. Испытания в большинстве случаев не содержат фактического файла, а скорее предлагать вам фрагменты флага по мере его решения, соответствующие части которого более однородно встроены в задачу (текст, скрытый на изображении, или другие примеры).

Вы можете прочитать файл, чтобы значение хеш-функции отображалось в терминале, используя **кошка Команда. Копирование** флаг и вставку его на страницу лаборатории Starting Point предоставит вам право собственности на эту машину, выполняя вашу самую первую задачу.

Поздравляем!