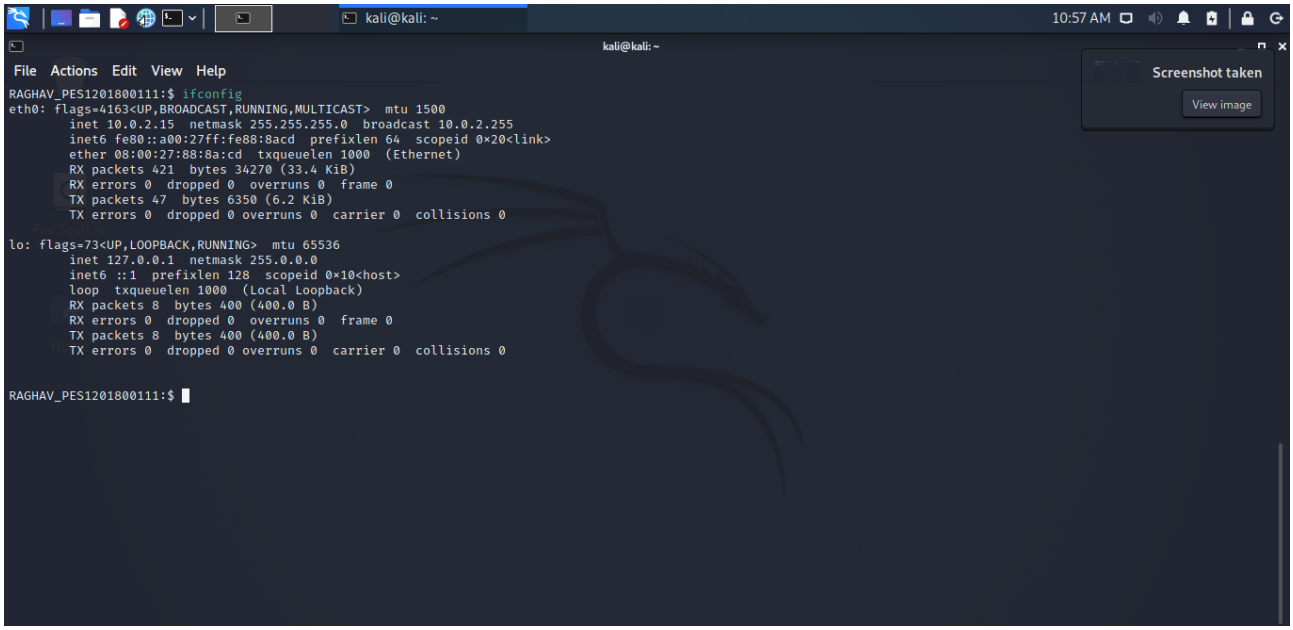
Ethical Hacking
Assigment-2

By:
Raghav Goyal,
PES1201800111,
Section-D,
Roll No: 7

Configuration

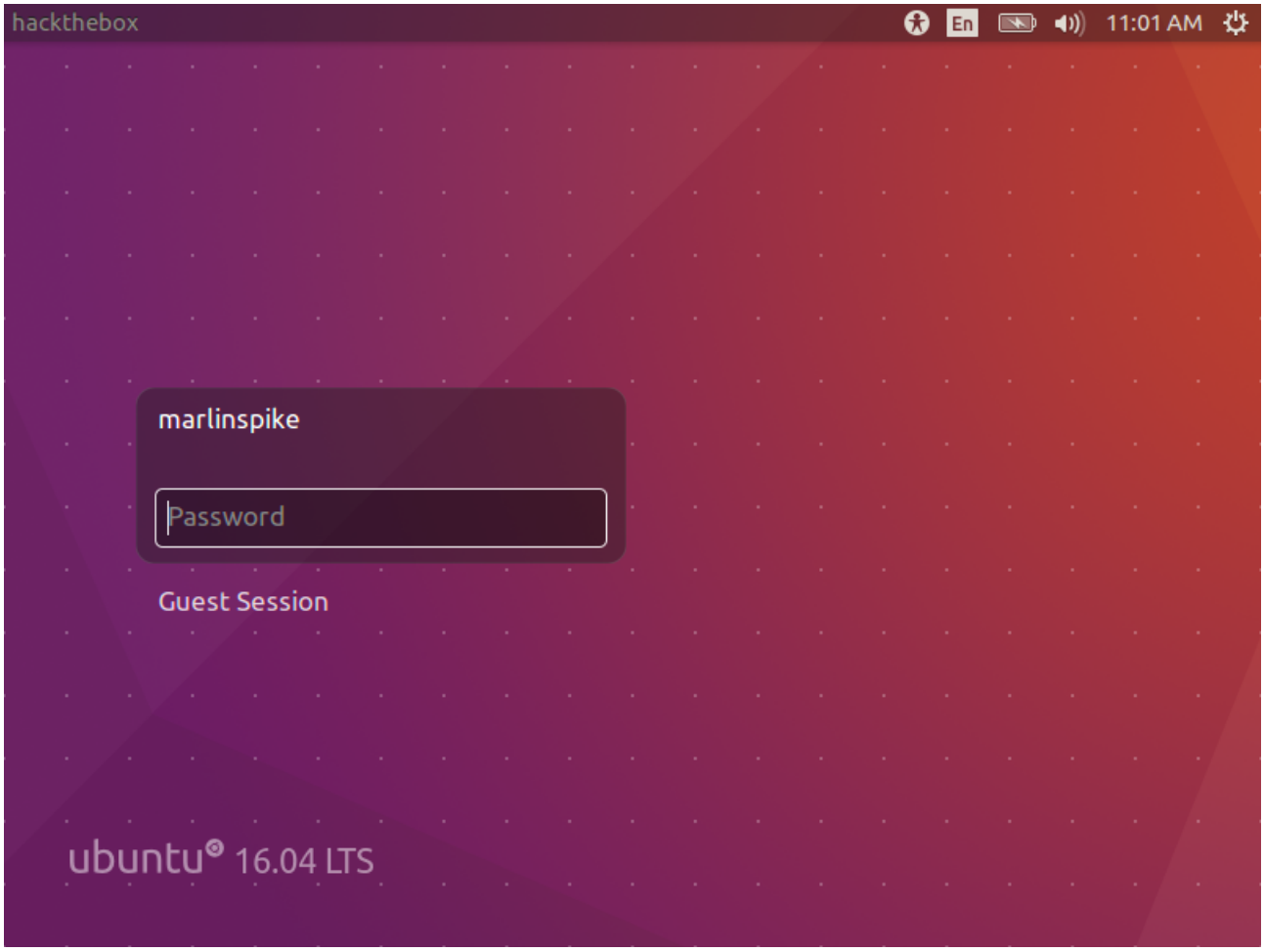
Kali machine (Attacker):



Terminal prompt: RAGHAV_PES1201800111:$
IP Adress: 10.0.2.15

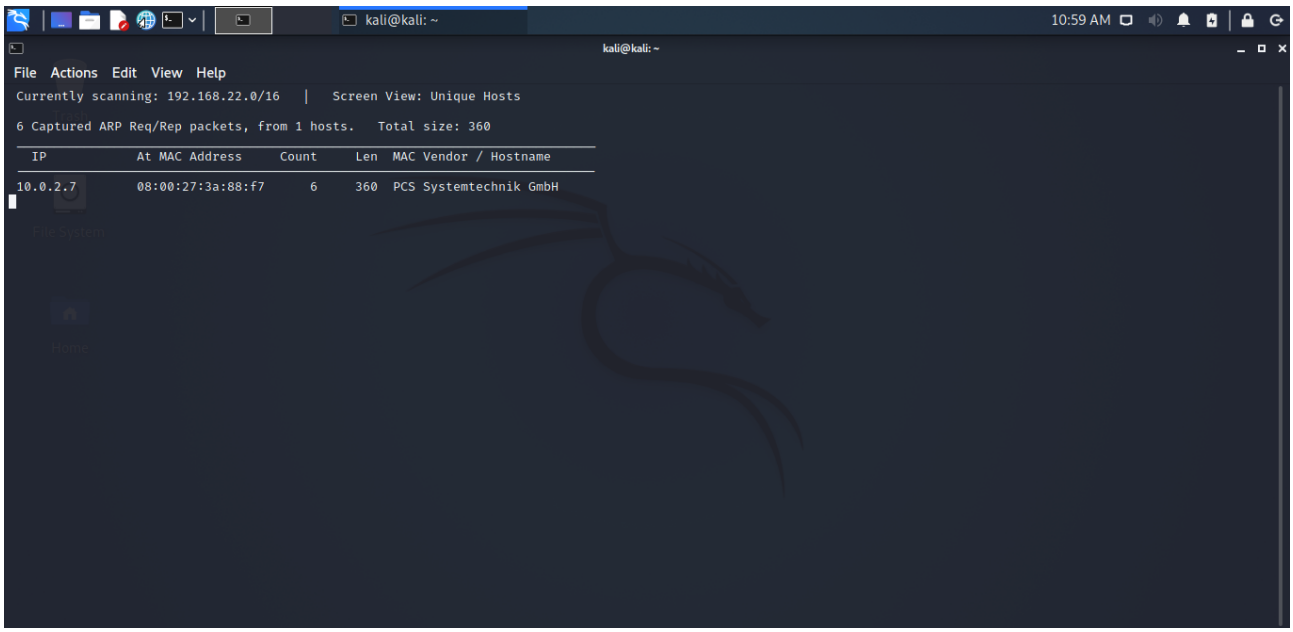
Hackthebox-1

1. Open the hackthebox VM



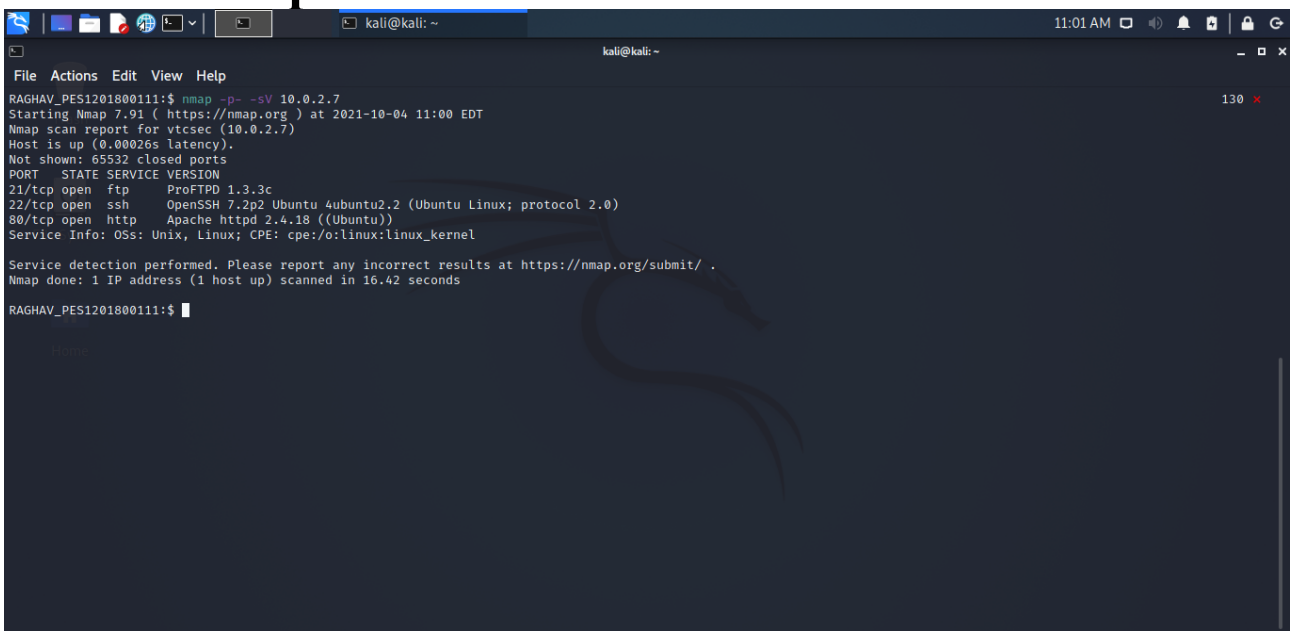
2. Keep the machine on login screen. Do not login as Guest. As logging in as guest will not allow root access.

3. Scan for machines on Kali using netdiscover
Command: sudo netdiscover



Output: The victim's IP address as 10.0.2.7

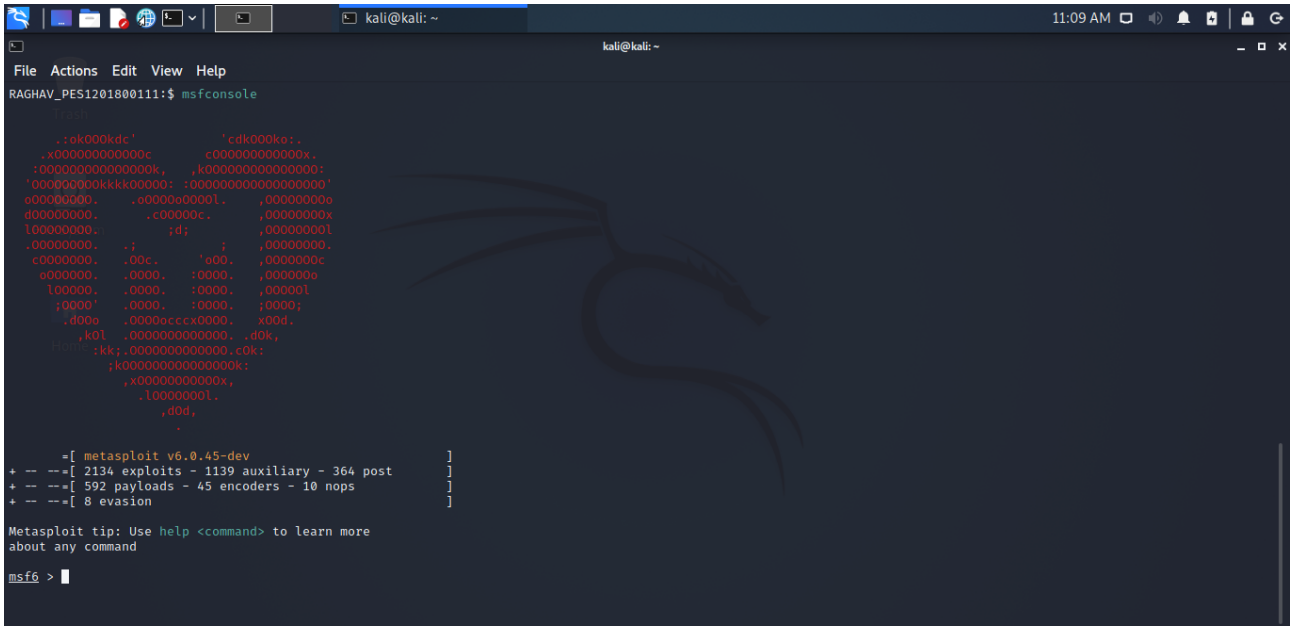
4. Scan for open services on the victim's machine.



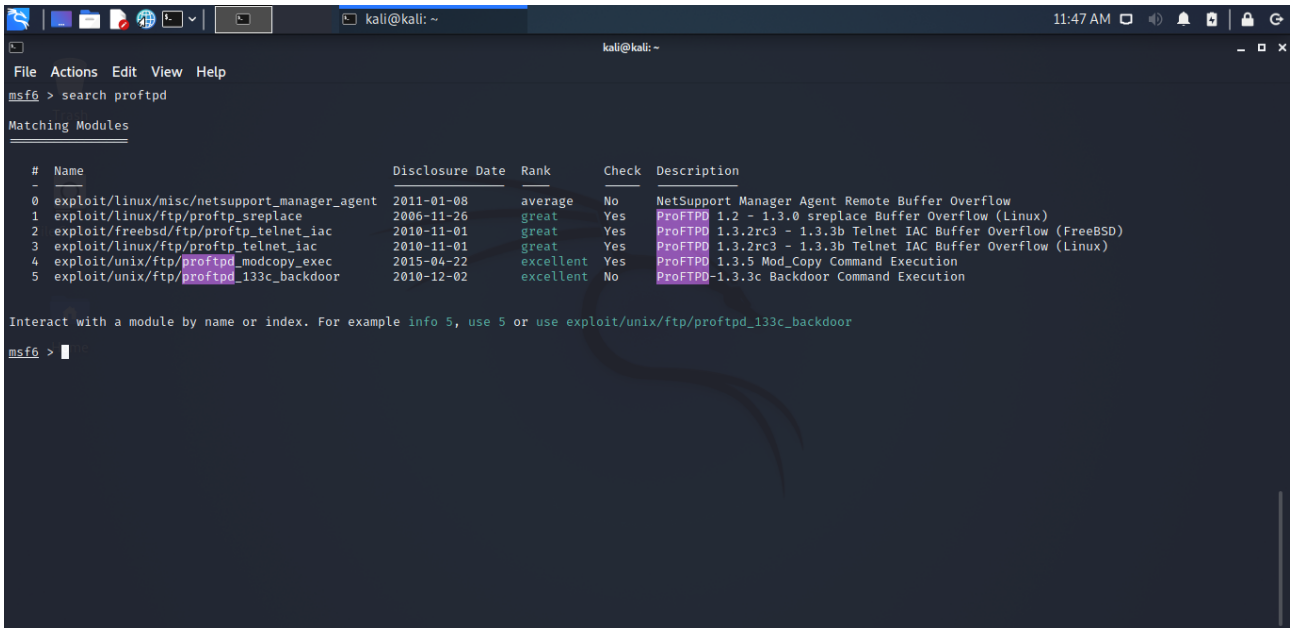
Command: nmap -p- -sV 10.0.2.7

Ouput: The victim has following open services; ftp (ProFTPD), ssh (OpenSSH) and http (Apache).

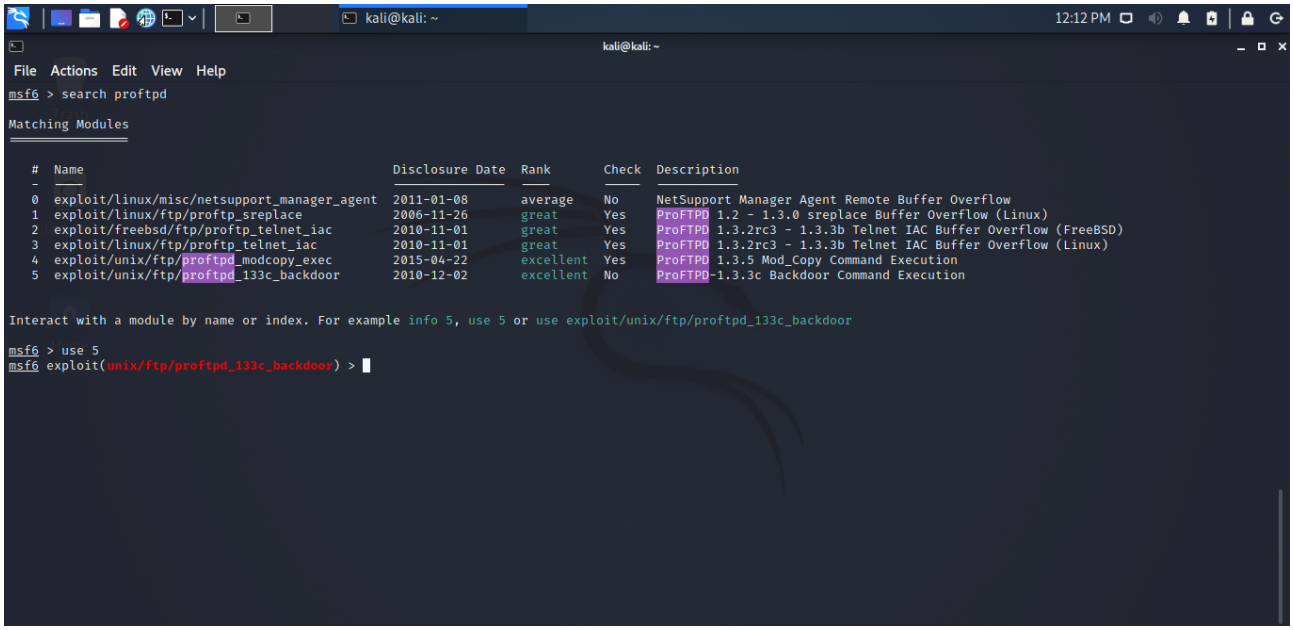
5. Open msfconsole to utilise the metasploitable framework on Kali.



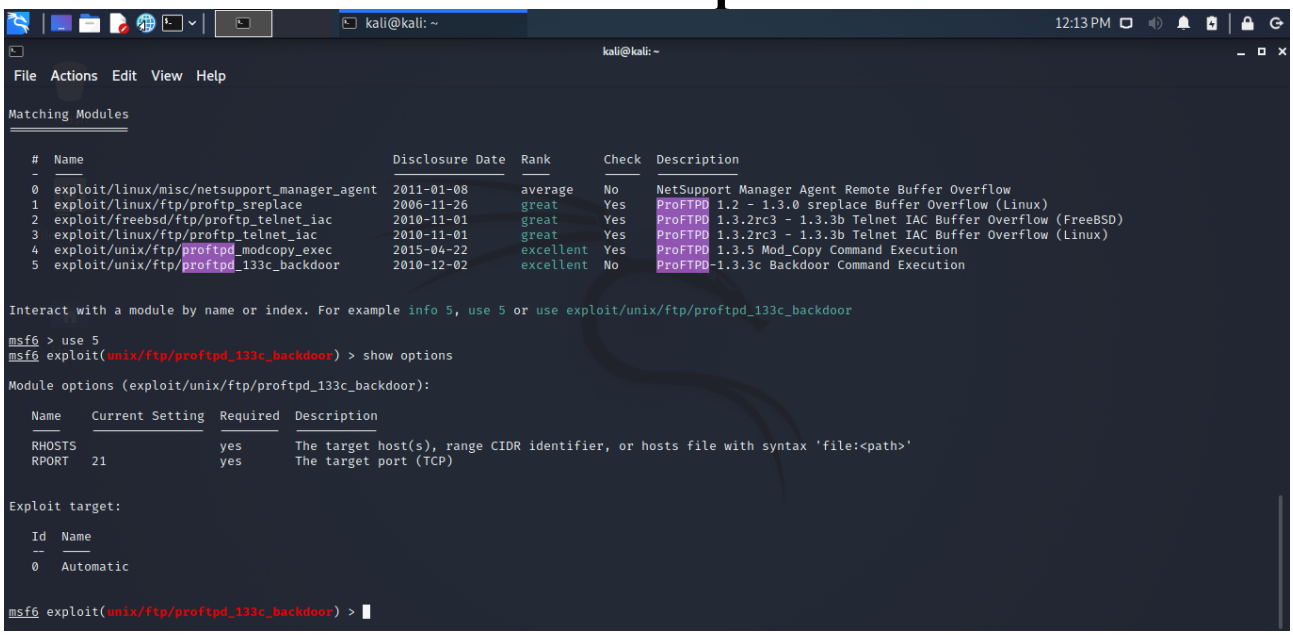
6. To exploit the ftp service, search proftpd.

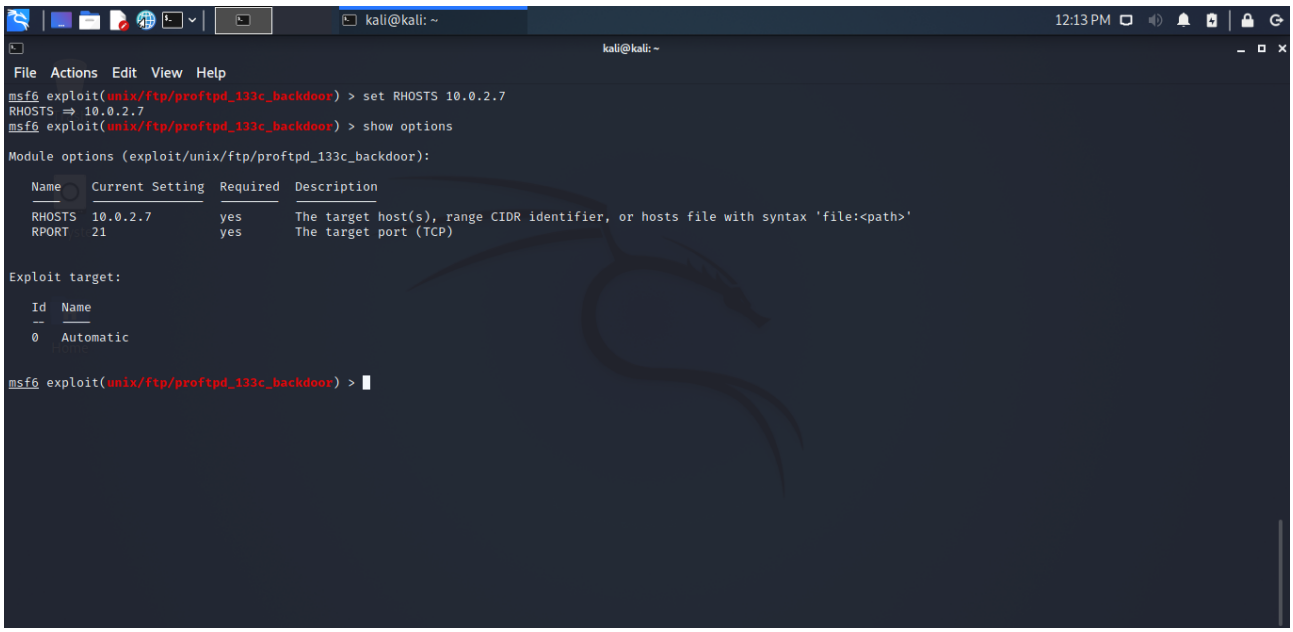


7. Use one of the available exploits. Eg: exploit 5

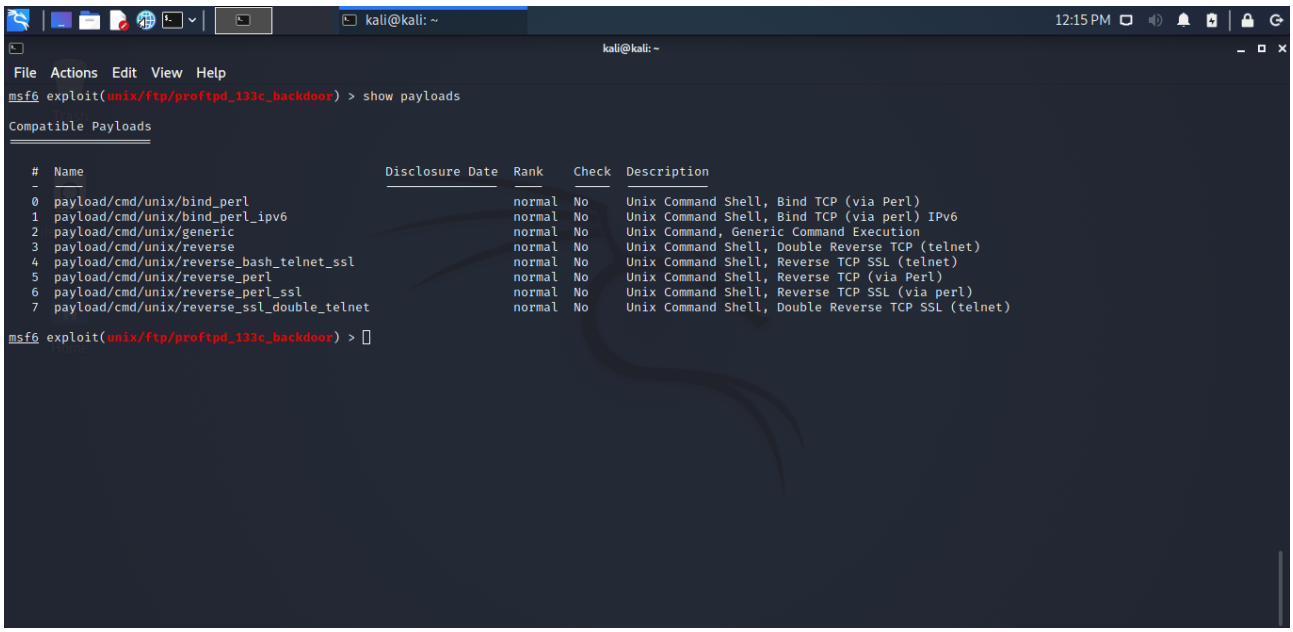


8. View and Set the attributes options.

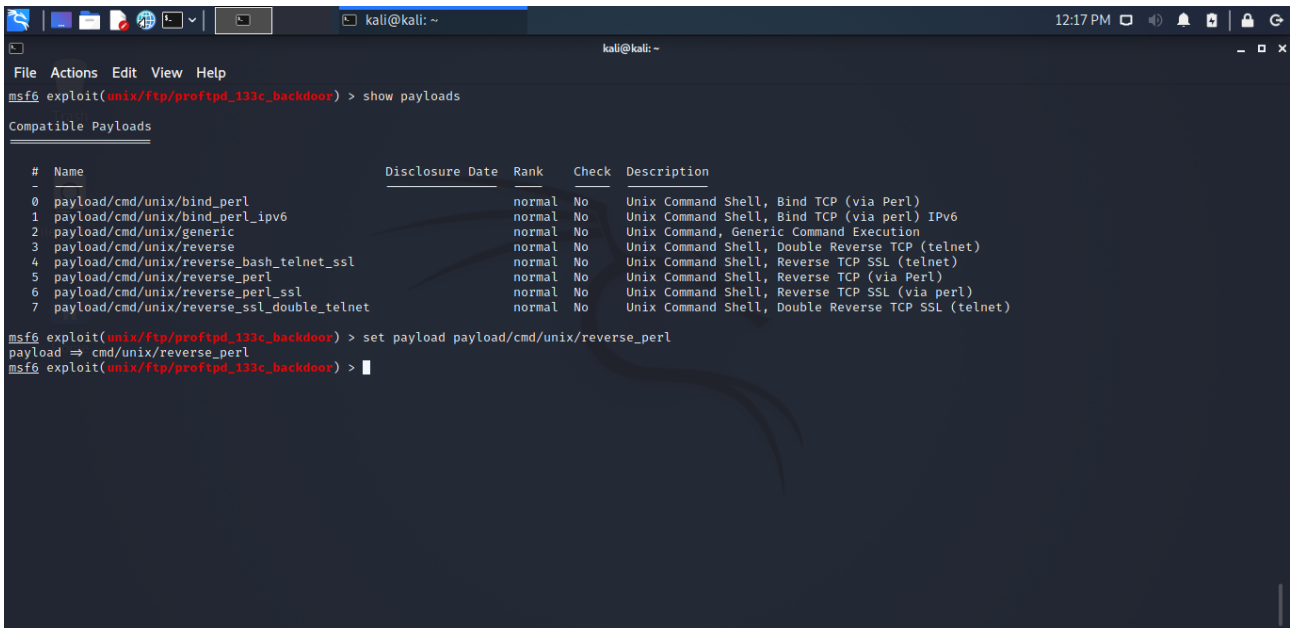




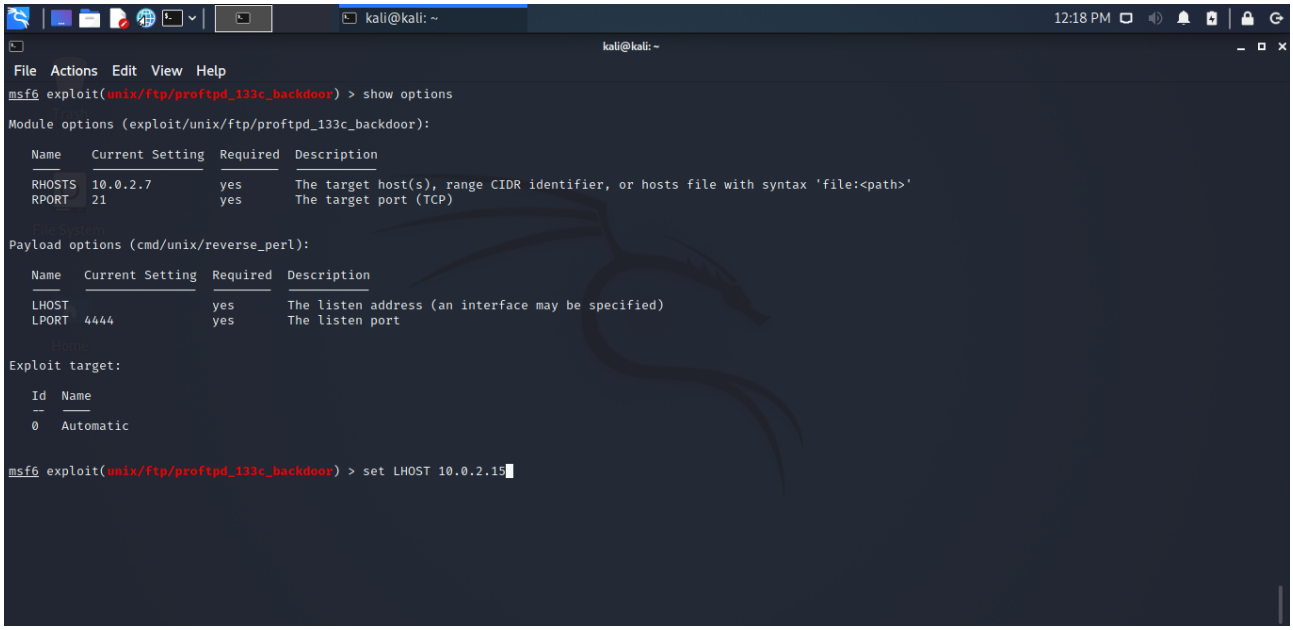
9. List out available payloads. These payloads are the code/data that will be sent/run on victim's machine.



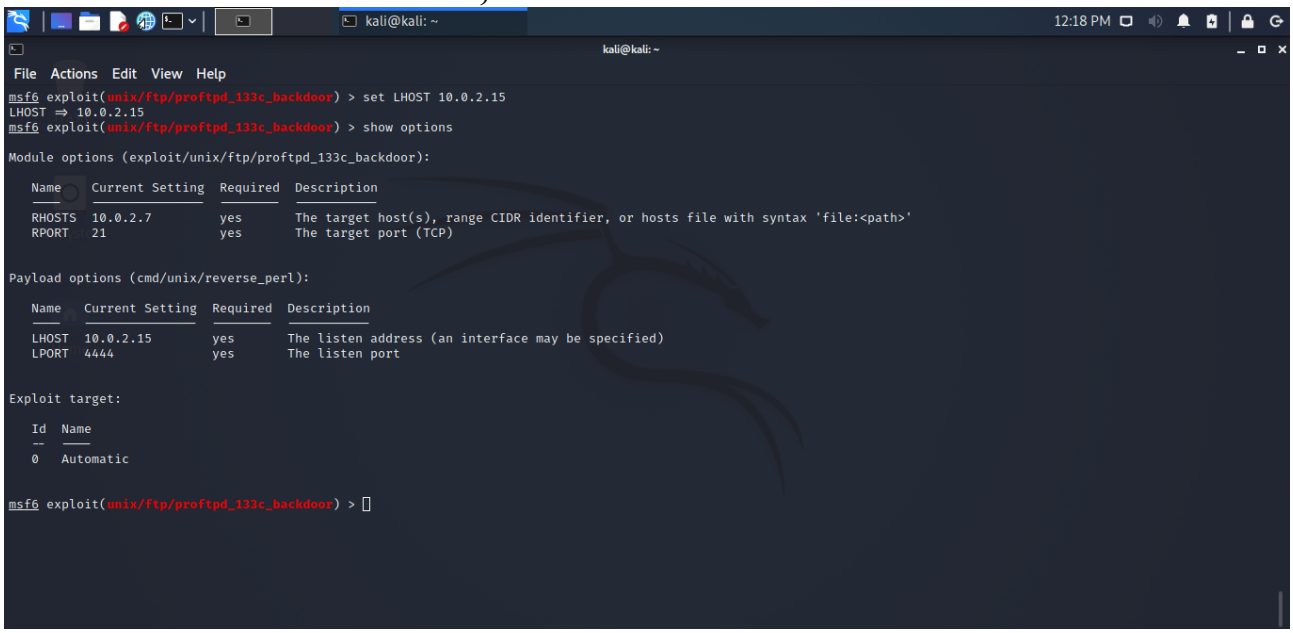
10. Set payload from among the list. Eg: 5th payload



11. Set the new options.

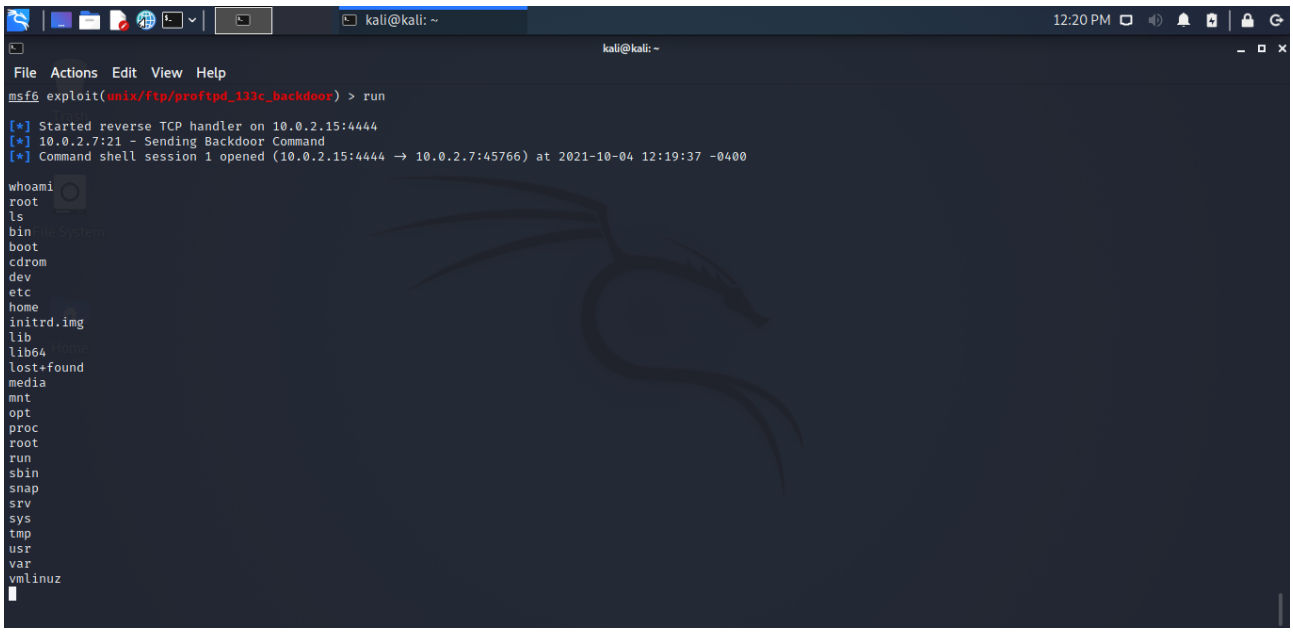


LHOST is set to local host, i.e Kali machine's IP address.



12. Exploit the machine.

Command: run

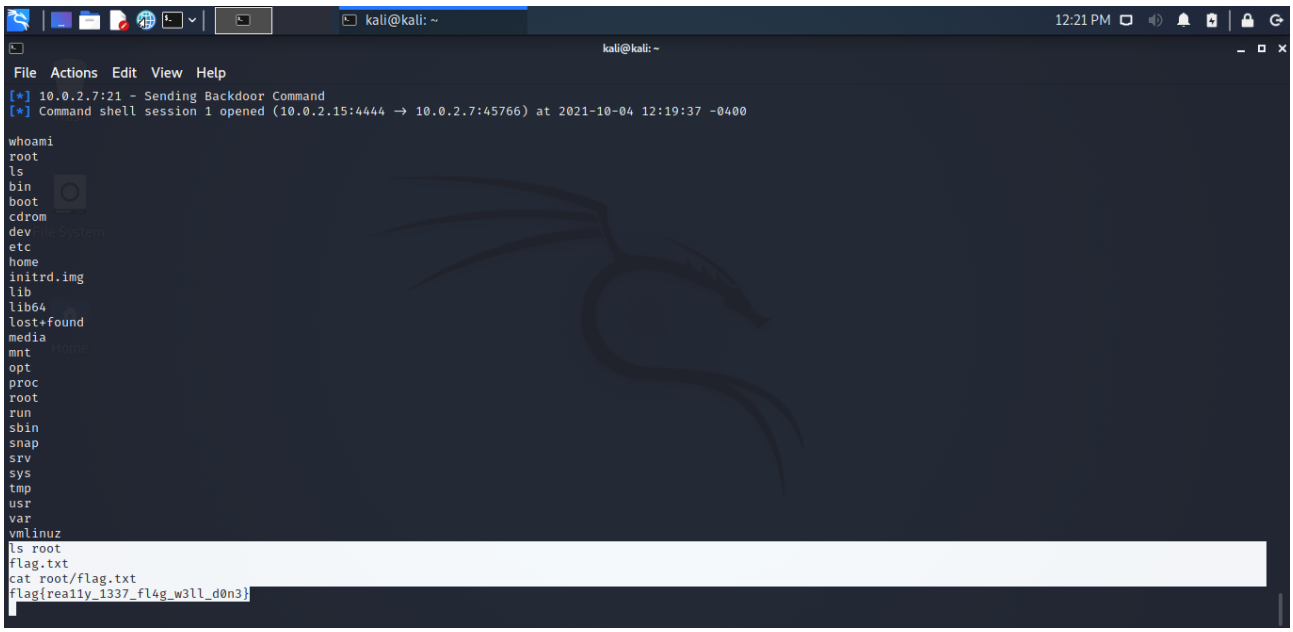


Output: Terminal session is opened on the victim machine.

13. Flag finding

Flag-1:

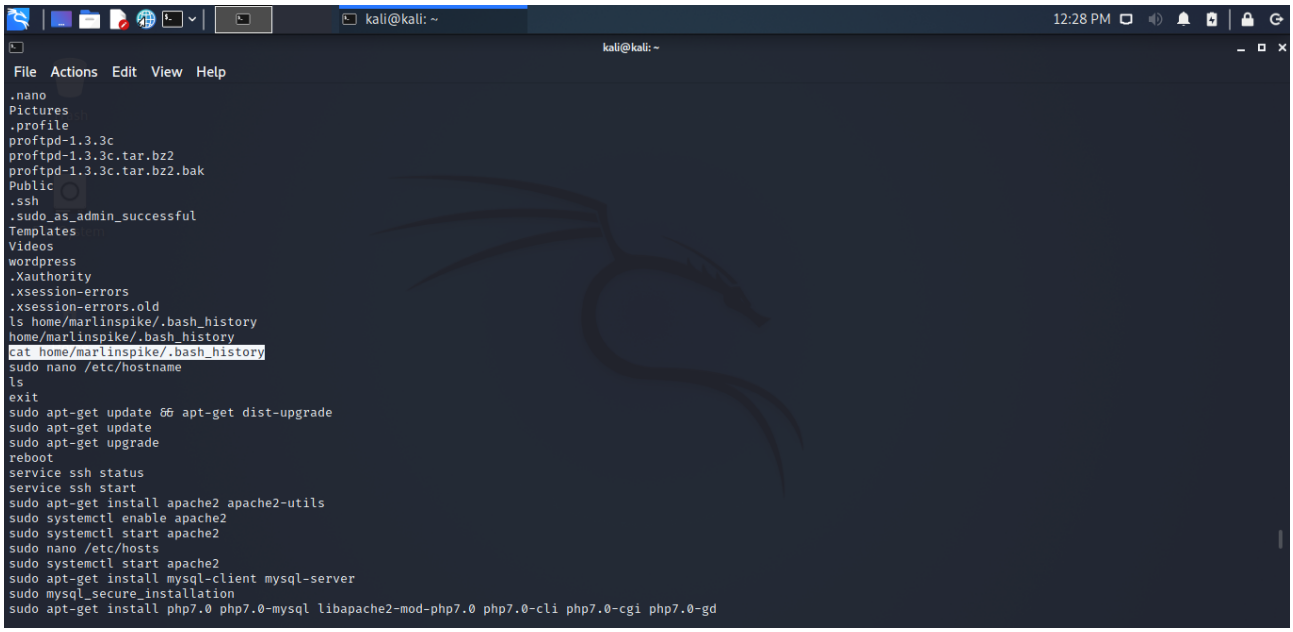
1st flag was present in a file named flag.txt present inside root directory.
Flag value: *flag{really_1337_fl4g_w3ll_d0n3}*

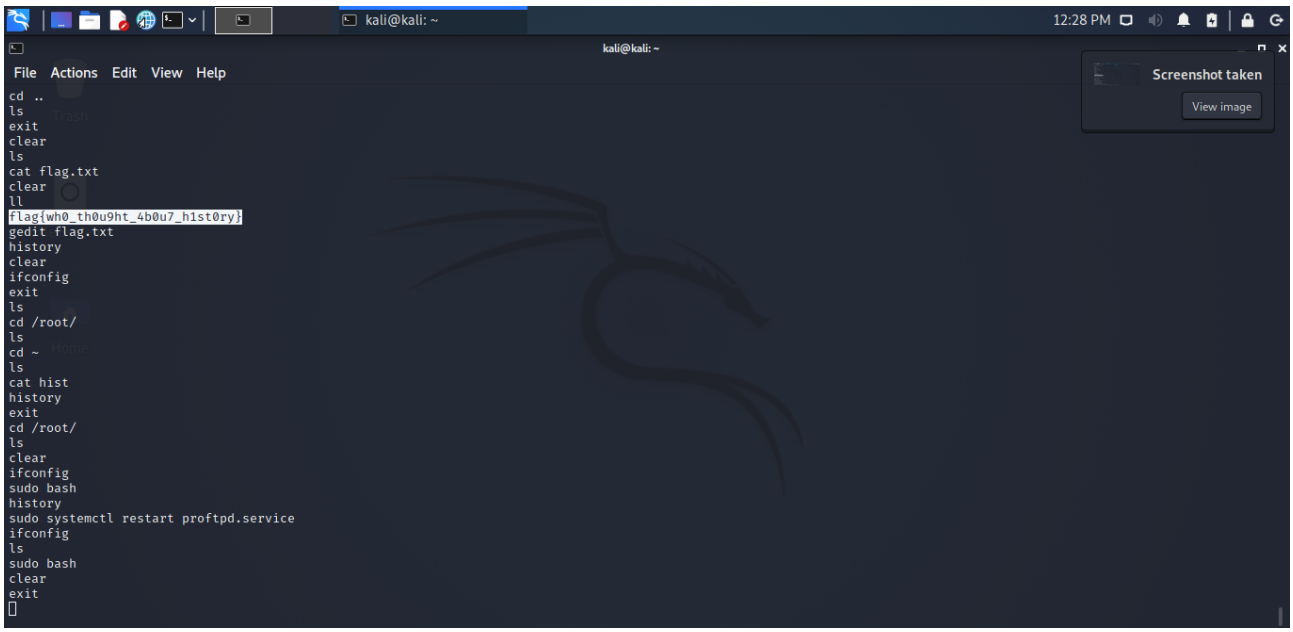


Flag-2:

2nd flag was present in the .bash_history file present inside /home/marlinspike directory.

Flag value: *flag{wh0_th0u9ht_4b0u7_h1st0ry}*

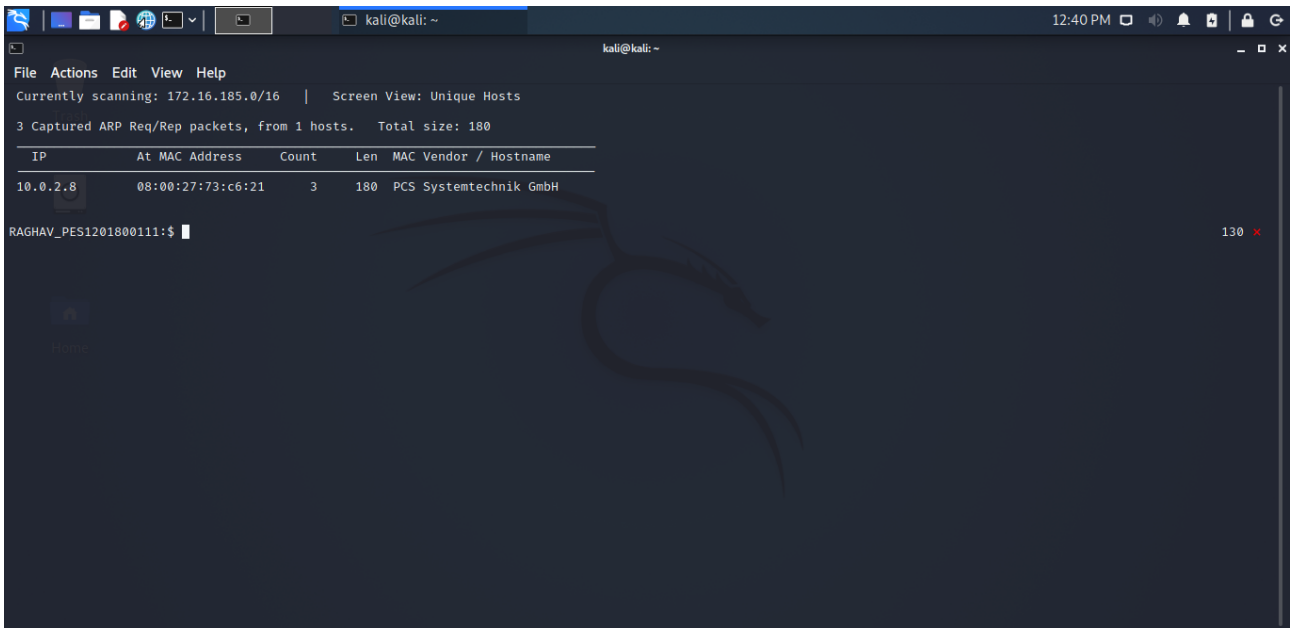




Hackthebox – 2

1. Scan for IP address of machine

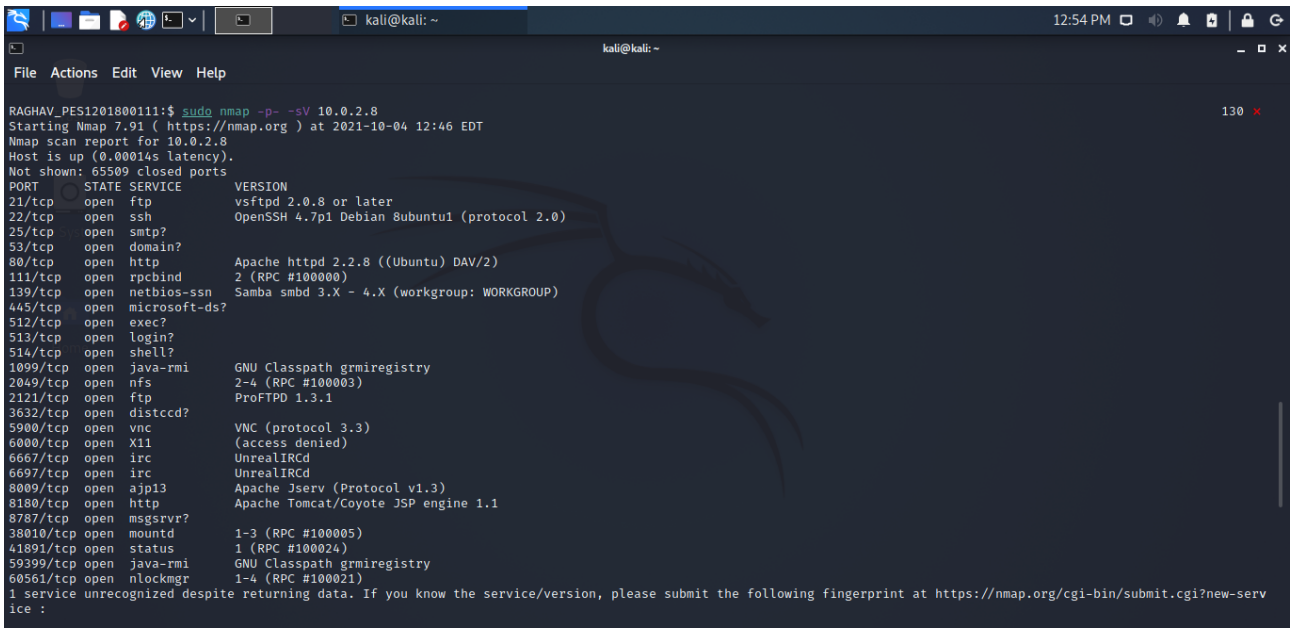
Command: sudo netdiscover



Output: The victim's IP is found to be 10.0.2.8

2. Scan for open ports on victim machine.

Command: sudo nmap -p- -sV 10.0.2.8

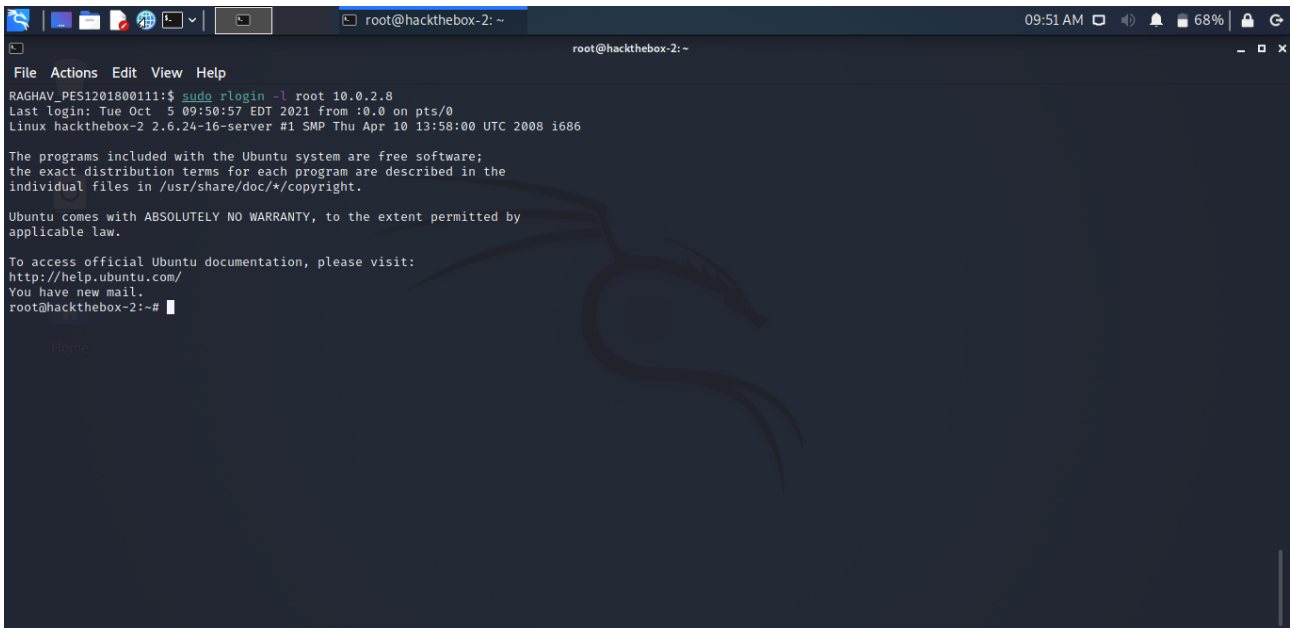


3. Install rsh-client

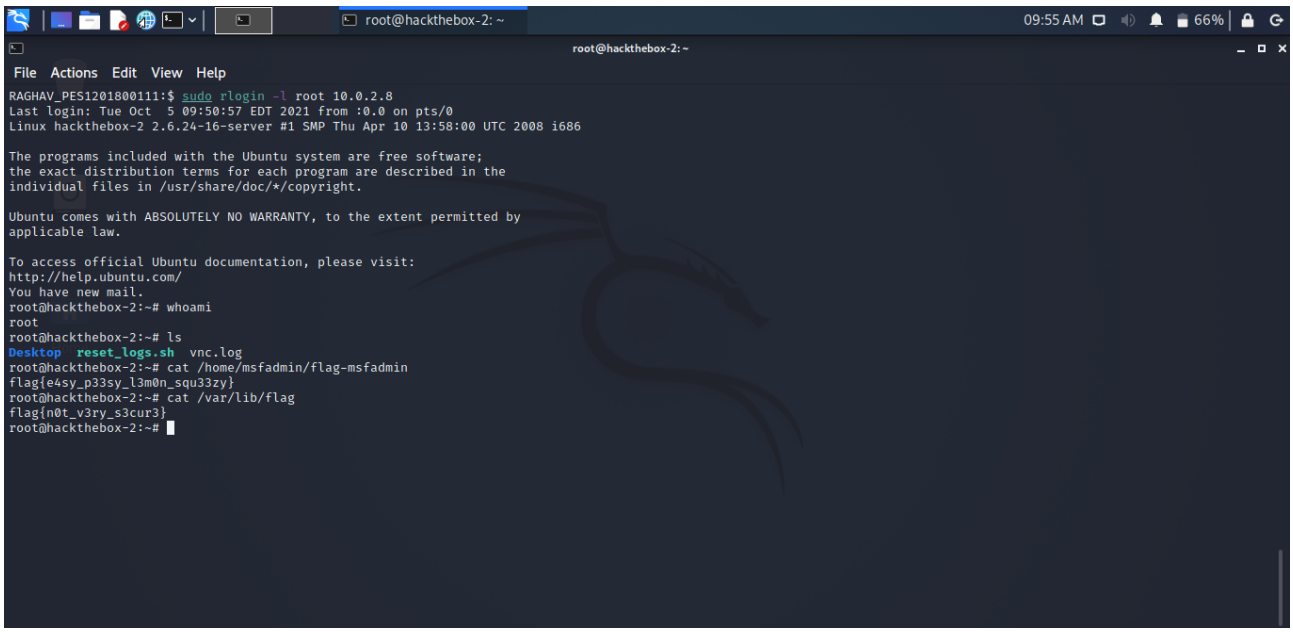
Command: sudo apt install rsh-client

4. Remote login the victim machine.

Command: sudo rlong -l root 10.0.2.8



Output: Now we have access to victim machine remotely.
Note: the terminal prompt changed to hacthebox-2~$



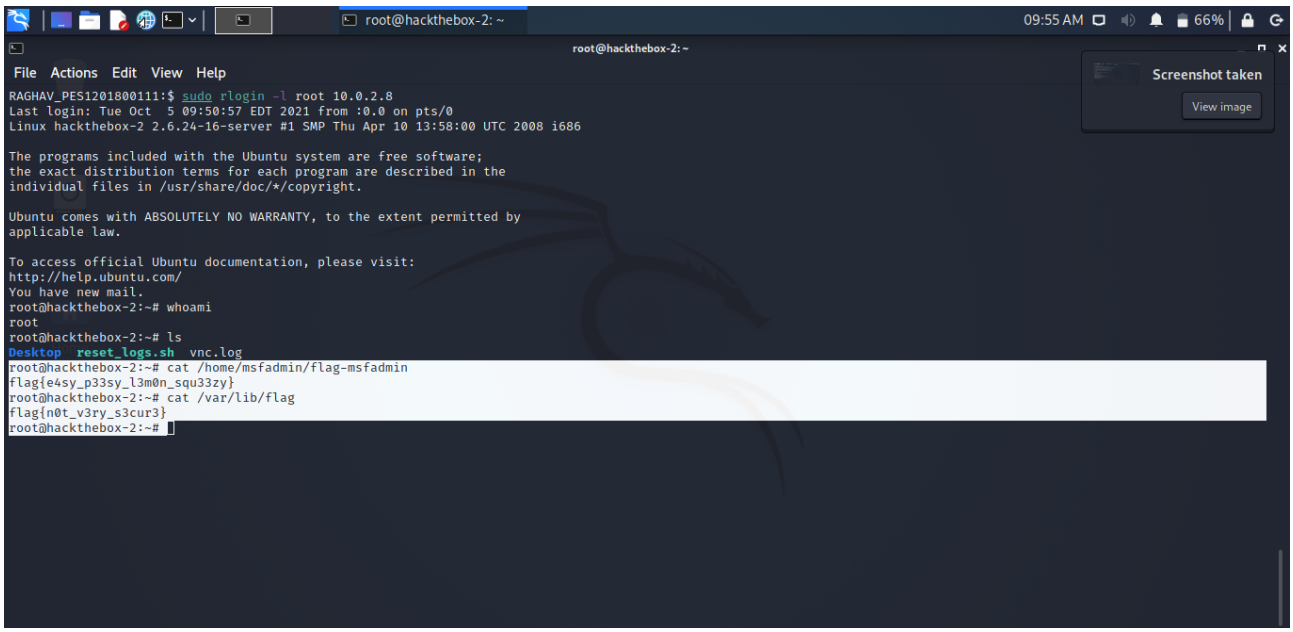
5. Flag finding

Flag-1:

1st flag was found in *flag-msfadmin* file located at /home/msfadmin/
Flag value: *flag{ea4y_p33sy_l3m0n_squ33zy}*

Flag-2:

2nd flag was in a file named *flag* located /var/lib directory.


root@hackthebox-2: ~
09:55 AM
66%
root@hackthebox-2: ~
File Actions Edit View Help
RAGHAV_PES1201800111:$ sudo rlogin -l root 10.0.2.8
Last login: Tue Oct 5 09:50:57 EDT 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:~# whoami
root
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:~#
Screenshot taken
View image

========== END ==========