PSP0201

Week 4

Writeup

Group Name: Undecided

Members

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha Binti Muhd Firdaus	Member

Day 11: Networking – The Rogue Gnome

Tools used: AttackBox, Firefox

Solution/walkthrough:

Question 1

Read and find the type of privilege escalation based on the definition of it.

> 11.4.2. Vertical Privilege Escalation:
>
> A bit more traditional, a vertical privilege escalation attack involves exploiting a vulnerability that allows you to perform actions like commands or accessing data acting as a higher privileged account such as an administrator.

Question 2

Read and find the suitable privilege escalation based on its definition relating to the given statement.

> 11.4.1. Horizontal Privilege Escalation:
>
> A horizontal privilege escalation attack involves using the intended permissions of a user to abuse a vulnerability to access another user's resources who has similar permissions to you. For example, using an account with access to accounting documents to access a HR account to retrieve HR documents. As the difference in the permissions of both the Accounting and HR accounts is the data they can access, you aren't moving your privileges upwards.
>
> 11.4.2. Vertical Privilege Escalation:
>
> A bit more traditional, a vertical privilege escalation attack involves exploiting a vulnerability that allows you to perform actions like commands or accessing data acting as a higher privileged account such as an administrator.
>
> Remember the attack you performed on "*Day 1 - A Christmas Crisis*"? You modified your cookie to access Santa's control panel. This is a fantastic example of a vertical privilege escalation because you were able to use your user account to access and manage the control panel. This control panel is only accessible by Santa (an administrator), so you are moving your permissions upwards in this sense.

Question 3

Read and find the suitable privilege escalation based on its definition relating to the given statement.

> 11.4.1. Horizontal Privilege Escalation:
>
> A horizontal privilege escalation attack involves using the intended permissions of a user to abuse a vulnerability to access another user's resources who has similar permissions to you. For example, using an account with access to accounting documents to access a HR account to retrieve HR documents. As the difference in the permissions of both the Accounting and HR accounts is the data they can access, you aren't moving your privileges upwards.
>
> 11.4.2. Vertical Privilege Escalation:
>
> A bit more traditional, a vertical privilege escalation attack involves exploiting a vulnerability that allows you to perform actions like commands or accessing data acting as a higher privileged account such as an administrator.
>
> Remember the attack you performed on "*Day 1 - A Christmas Crisis*"? You modified your cookie to access Santa's control panel. This is a fantastic example of a vertical privilege escalation because you were able to use your user account to access and manage the control panel. This control panel is only accessible by Santa (an administrator), so you are moving your permissions upwards in this sense.

Question 4

Read and find the name of the file that contains a list of users who are a part of the sudo group. Then, copy it.

Normally, executables and commands (commands are just shortcuts to executables) will execute as the user who is running them (assuming they have the file permissions to do so.) This is why some commands such as changing a user's password require `sudo` in front of them. The `sudo` allows you to execute something with the permissions as root (the most privileged user). Users who can use `sudo` are called **"sudoers"** and are listed in `/etc/sudoers` (we can use this to help identify valuable users to us).

Question 5

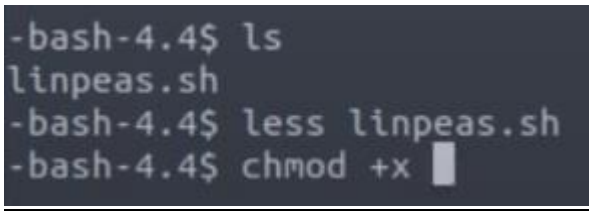
Read and find the Linux Command that is used to enumerate the key for SSH. Then, copy it.

Our vulnerable machine in this example has a directory called backups containing an SSH key that we can use for authentication. This was found via: `find / -name id_rsa 2> /dev/null` ....Let's break this down:

- We're using `find` to search the volume, by specifying the root (`/`) to search for files named "**id_rsa**" which is the name for *private* SSH keys, and then using `2> /dev/null` to only show matches to us.

Question 6

In the cmnatics home directory through the ssh log in, follow the command starting with chmod +x “filename”. Include the given file name in the command line to make it be able to execute.

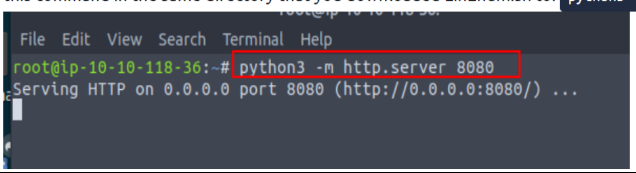


At the moment, the "examplefiles" are not executable as there is no "**x**" present for either the user or group. When setting the executable permission (`chmod +x filename`), this value changes (note the "**x**" in the snippet below -rw**x**rw**x**r):

Question 7

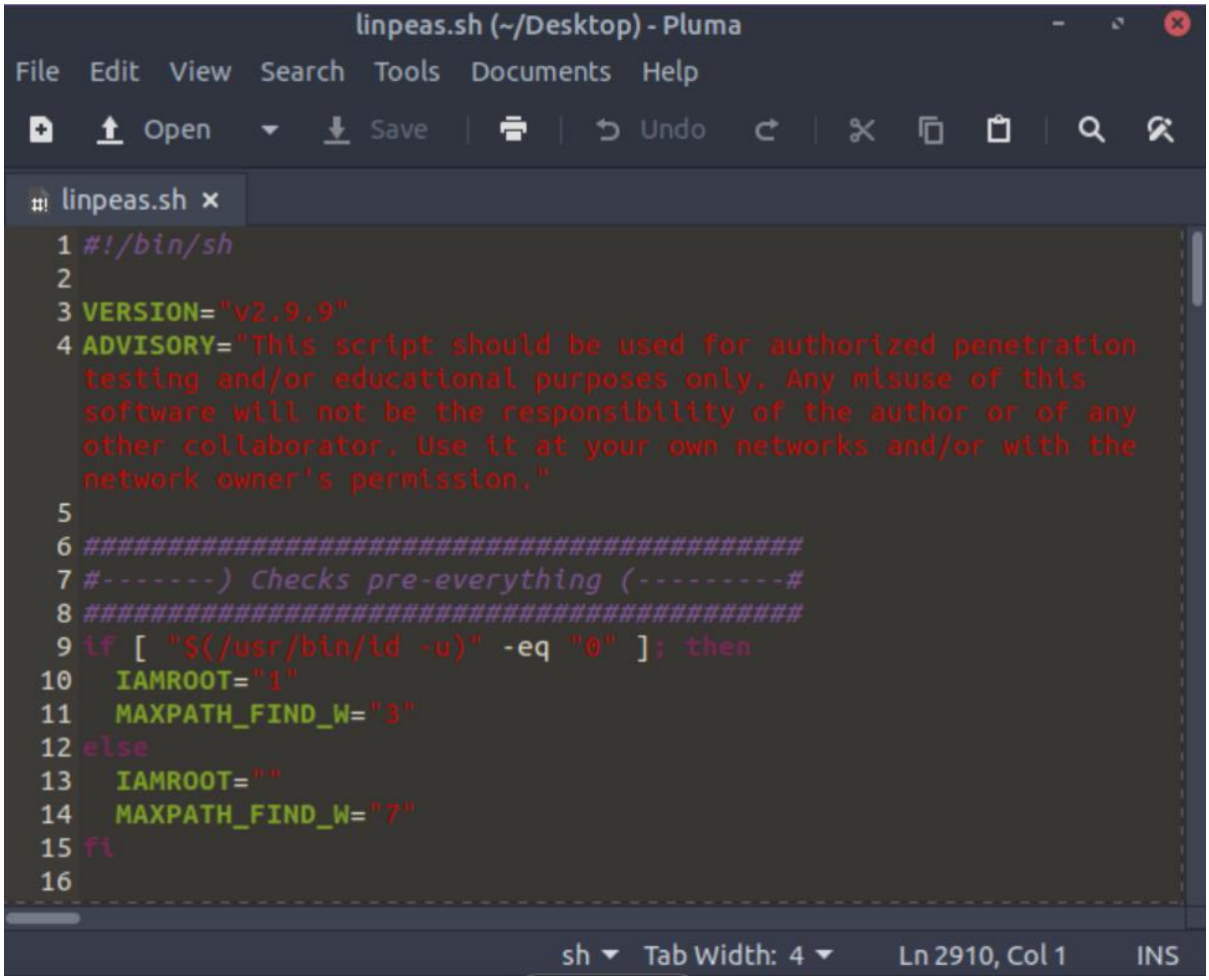
Read and find the correct command to be used under the Enumeration Scripts Category, in order to host a http server using python3 on port 9999. Include the command line from python3 -m http.server “port number” and insert the port number at the end.

11.10.2. Let's use Python3 to turn our machine into a web server to serve the *LinEnum.sh* script to be downloaded onto the target machine. Make sure you run this command in the same directory that you downloaded *LinEnum.sh* to: `python3 -m http.server 8080`



Question 8

We used linpeas on our target machine and copied the raw script into our local computer and then transferred it over by naming it “linpeas.sh”.



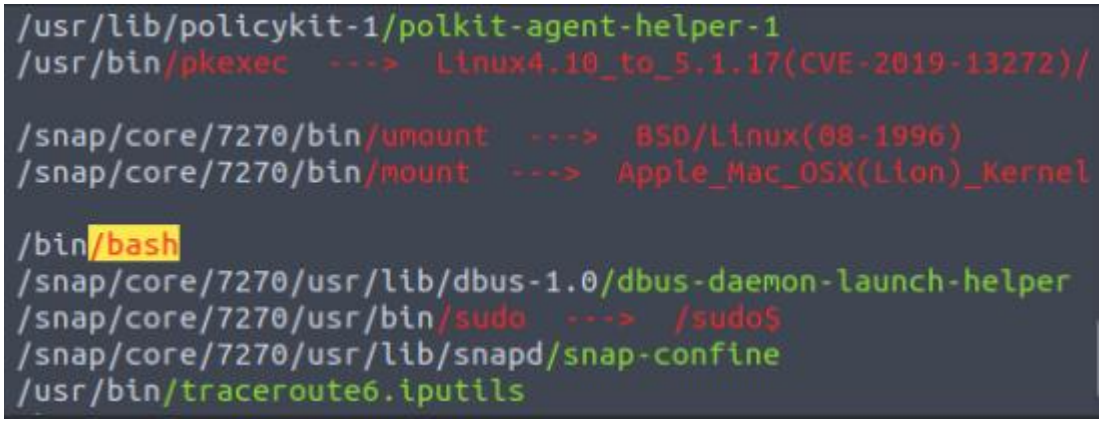
We then created a server on our local machine to transfer it in the same directory where we saved our file.

```
root@ip-10-10-136-247:~/Desktop# python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

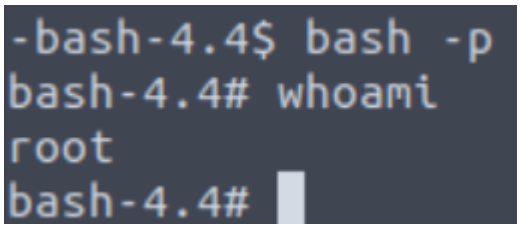
Back over at the SSH connection, we grabbed the file from the server we just created by using our IP address. From here, we could list the files to ensure it is transferred correctly and then changed the permissions to make it executable.

```
-bash-4.4$ ls
linpeas.sh  wget-log
-bash-4.4$ chmod +x linpeas.sh
-bash-4.4$
```

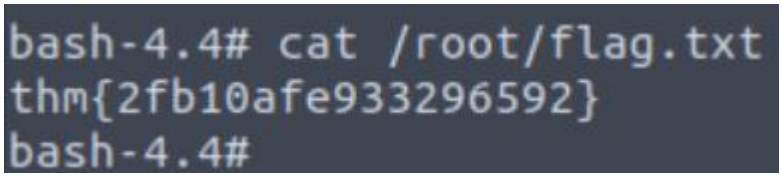
We were then able to execute linpeas.



We then used the following command to gain root privileges.



Lastly, find the contents of the file by typing in "/root/flag.txt" and copy the flag.



Thought Process/Methodology:

Firstly, we started by reading and understanding the overall networking of Day 11 to be able to find answers from questions 1-7. We proceeded on finding the types of privilege escalation regarding questions 1-3. Next, we found the name of the file which contains a list of users who were part of the sudo group under the Vulnerability section. We then found the suitable Linux Command to enumerate the key for SSH which we could use for authentication. Later, we were able to find the command to execute an executable file named "find.sh". After, we moved on to find the command we would use to host a http server using python3 on port 9999. The port number was different from the one we were about to use for the last question. Lastly, we started by enumerating the machine for executables that have had the SUID permission set. The materials did mention an enumeration script that we could use for this, called LInEnum but I did not need to use it as GTFOBins worked fine. Thus, we used linpeas on our target machine and copied the raw script into our local computer and then transferred it over by naming it "linpeas.sh". This enabled us to then create a server on our local machine to transfer it in the same directory where we saved our file. Once done, we moved back to the SSH connection to grab the file from the server we had created by using our IP address. From here, we could list the files to ensure it is transferred correctly and then changed the permissions to make it executable. We were then able to execute linpeas. Finally, in order to receive

the flag, we proceeded by following the right command to gain privileges and typed in “/root/flag.txt”. This then gave us the flag to the contents of the file.