PSP0201

Week 3

Writeup

Group Name: ikun no 1

Members

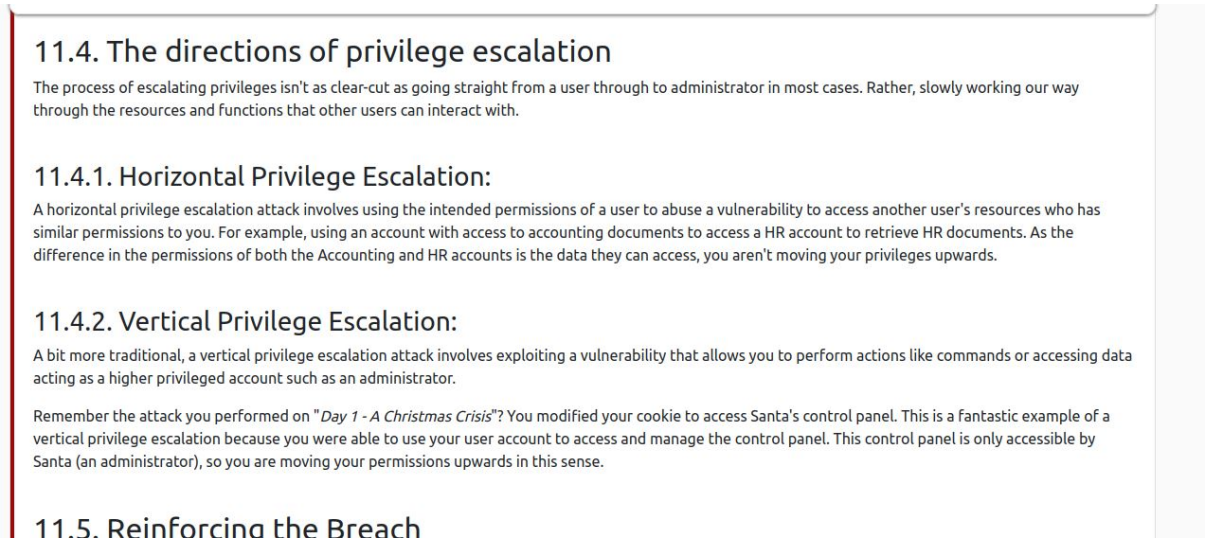
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 11 - Networking The Rogue Gnome

Tool Used: Kali Linux, firefox, GTFObins, LinEnum, Nmap, Netcat

Solution/walkthrough:

Q1



11.4. The directions of privilege escalation

The process of escalating privileges isn't as clear-cut as going straight from a user through to administrator in most cases. Rather, slowly working our way through the resources and functions that other users can interact with.

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.

11.5. Reinforcing the Breach

Study from Try Hack Me.

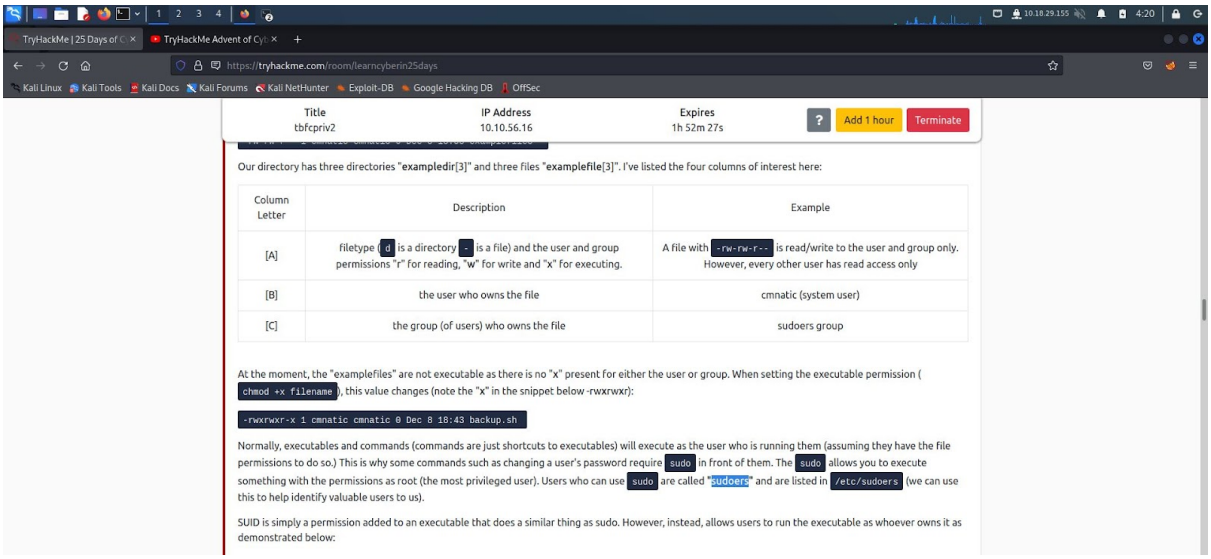
Q2

In this case, it means I have access as a higher privileged account.

Q3

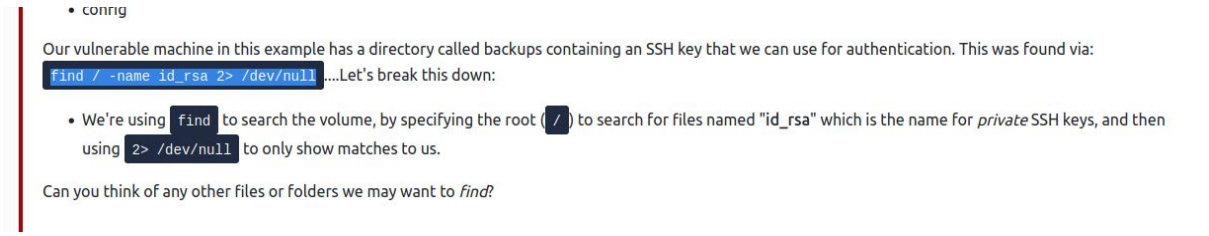
In this case, I have access to another user's resources who has similar privileges.

Q4



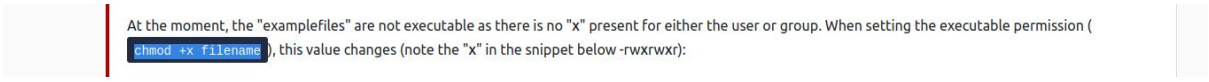
Study from Try Hack Me.

Q5



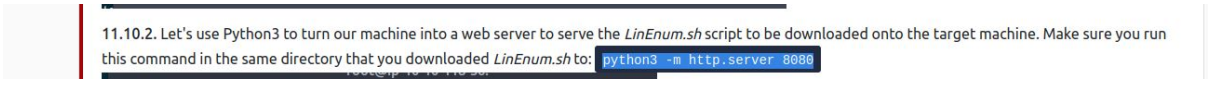
Study from Try Hack Me.

Q6



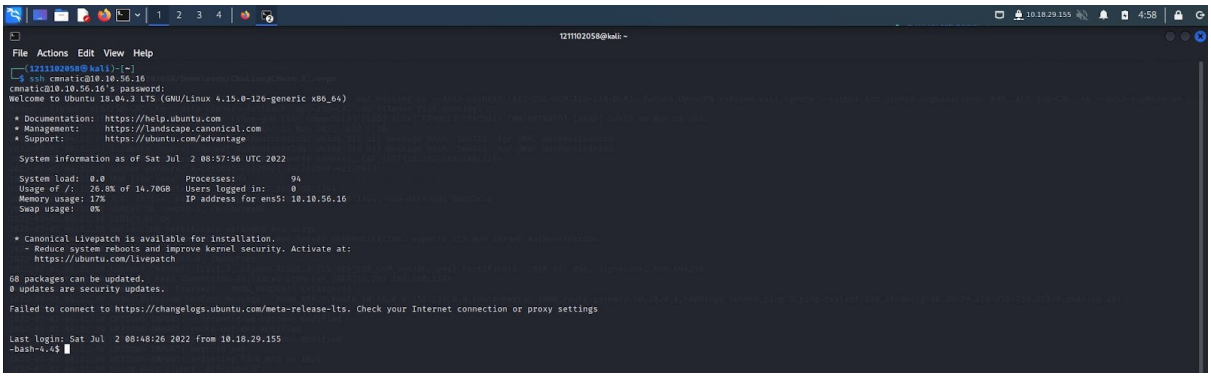
To execute an executable file, use the [chmod +x {filename}] command and replace the [filename] with the name of the executable file.

Q7

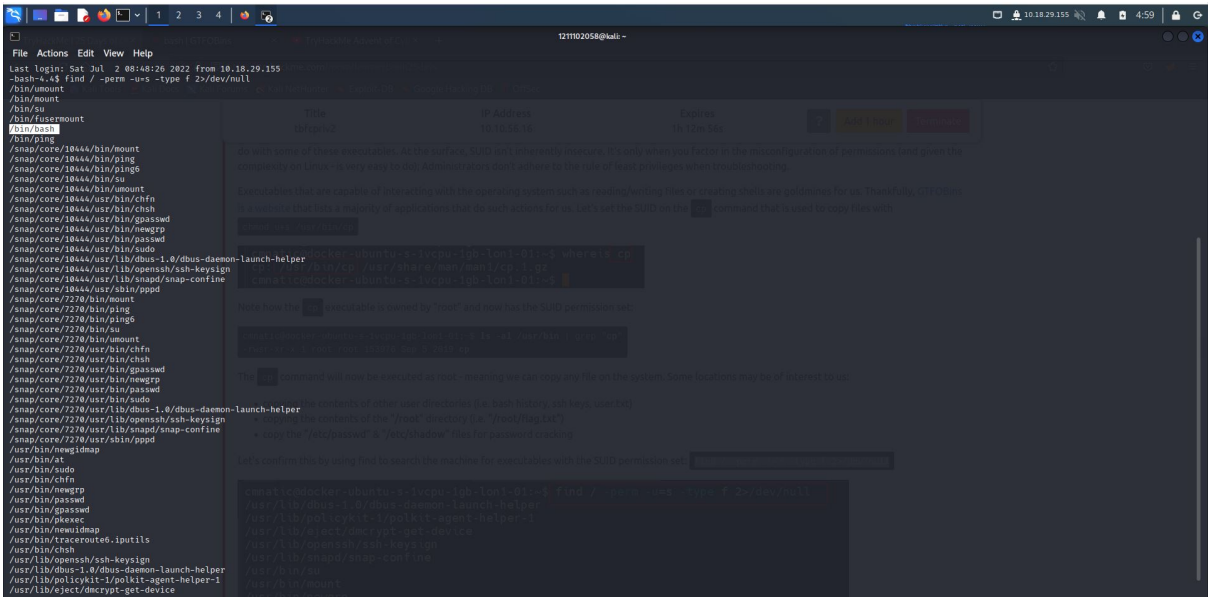


To host a server using python3 that can use wget, use the similar command as learned from Try Hack Me [python3 -m http.server {port number}]and replace the {port number} with the port number required.

Q8



Use SSH to login.



Use find command to search for all executables with the SUID set. The command used is [find / -perm -u=s -type f 2>/dev/null].

SUID

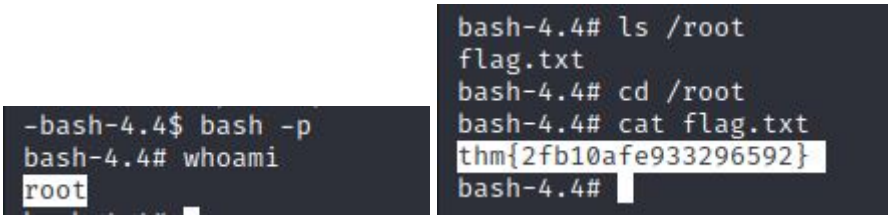
If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which bash) .

./bash -p
```

A command name [/bash] is found that is executed as root. Try to execute it with another version from GTFObins for misconfiguration of permission.



After executing the command, misconfiguration occurs. Look into the file inside the root directory. A .txt file name flag is found. Read the file and capture the flag.