Privilege Escalation

What is Privilege escalation ?

Privilege Escalation is the technique to gain higher-level permission on a system.

Types of Privilege escalation

1.Horizontal Privilege escalation
2.Vertical Privilege escalation

Horizontal Privilege escalation

Horizontal Privilege escalation is technique to gain the access of the data of same level privileges of the attacker as victim.

To make it clear think of a University application which has namely two users one is student and the second one is faculty.

The student can view his data such as marks, attendance. So susdent A can access only his data. If somehow a student B manage to access the data of student A then it is known as Horizontal privilege escalation.

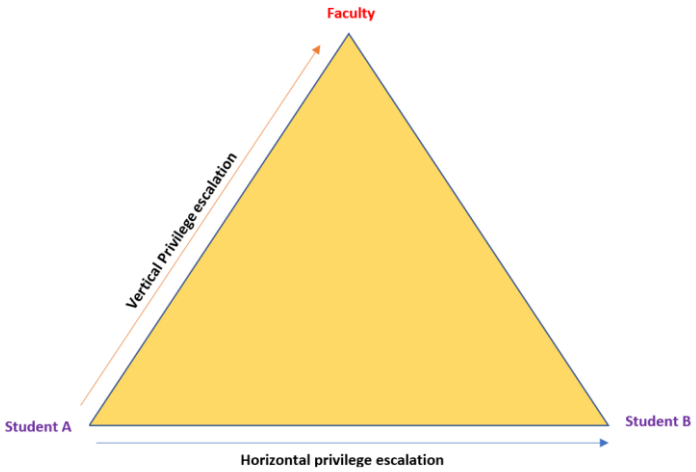
Here student A and Student B has same set of privileges on the application but student B escalated the his privilege to access data of the student A.

Vertical Privilege escalation

Vertical privilege escalation is a technique to gain higher privileges.

To make it clear think of the same university application in which there are two users one is faculty and the second one is student.

So, if a student can escalate his privilege to gain the privilege of the faculty then he can access all the functionality like viewing the student data, altering and adding new data in to the system.



Linux Privilege Escalation techniques

To find the kernel version

Command :- uname -a

cat /proc/version

cat /etc/issues

after getting the kernel version just search kernel version exploit in google you will be getting tons of exploits.

To check the process running in the system if any process run as root then you can execute the commands as root using those process.

Command :- ps aux

ps -ef

top

For example if mysql is running as root then use

Commend :- select sys_exec('any linux commands');

To find SUID bit set files

Command :- find / -perm -4000 2>/dev/null

To find GUID bit set files

Command :- find / -perm -2000 2>/dev/null

After getting the binaries whose suid or guid bits are set then search the exploit in GTFOBins.

Abusing Sudo rights

To check the sudo rights of the current user

Command :- sudo -l

It will display the binaries which can be run as root.

If you didn't find any thing interesting you can go with using a automation script to check carlospolop/privilege-escalation-awesome-scripts-suite: PEASS - Privilege Escalation Awesome Scripts SUITE (with colors) (github.com)