LAB 07: **Access control vulnerabilities - Privilege escalation**

Part 1: Answer the following questions

1. In the context of privilege escalation, what is the difference between vertical and horizontal privilege escalation, and can you give an example of each?

The difference between vertical and horizontal privilege escalation lies in the level of access the attacker gains:

Vertical Privilege Escalation:

- Moves the attacker from their current (low) level of access to a higher level. ○ Goal is to gain administrator-level or root access to the entire system.

Examples:

Exploiting a vulnerability in a program to get admin rights on a computer.

Stealing a supervisor's login credentials to access privileged data.

Using a backdoor planted in the system to bypass security measures.

Horizontal Privilege Escalation:

- Involves gaining access to another account with the same level of privilege as the current account.
- Doesn't necessarily need to be a high-privileged account. ○ The goal is to move laterally within the system and potentially compromise other accounts or data.

Examples:

Stealing a coworker's credentials to access shared files or send unauthorized emails.

Exploiting a misconfiguration in a database to access another user's records.

Using a compromised service account to gain access to other systems on the network.

2. What are some effective strategies or practices that can be implemented to prevent privilege escalation vulnerabilities in a system?

Preventing privilege escalation vulnerabilities requires a multi-layered approach, addressing both technical and human aspects. There are some effective strategies and practices can implement:

- Security Awareness Training ○ Separation of Duties ○ Least Privilege
- Patch Management ○ Vulnerability Scanning ○ Secure Configuration ○ Application Hardening ○ Network Segmentation ○ Strong Authentication ○ Log Monitoring ○ Incident Response Planning