


PRIVILEGE ESCALATION

Privilege escalation in Linux refers to the process of gaining higher levels of access or permissions beyond what is initially granted to a user.



COMMON METHODS FOR PRIVILEGE ESCALATION

Exploiting Vulnerabilities: Attackers may exploit vulnerabilities in the operating system, kernel, or installed software to gain elevated privileges.

Exploiting Misconfigured Permissions: Improperly configured file and directory permissions can allow an attacker to escalate privileges.

Exploiting Weak User Passwords: If a user account has a weak or easily guessable password, an attacker can gain access to the account and then escalate privileges.

Exploiting Sudo Misconfigurations: Improperly configured sudo rules or insecure sudoers file entries can enable an attacker to execute arbitrary commands with root privileges.

Exploiting Kernel Vulnerabilities: Vulnerabilities in the Linux kernel can allow attackers to gain elevated privileges.

Mitigating privilege escalation

- Regularly update the operating system and installed software to apply security patches.
- Use strong passwords and enforce password complexity requirements.
- Employ the principle of least privilege by only granting necessary permissions to users and limiting the use of root access.
- Review and update sudo configuration to ensure proper command restrictions.
- Regularly monitor and log system activities to detect any suspicious or unauthorized activities.
- Use file and directory permissions correctly, limiting access to sensitive files and directories.
- Stay informed about security vulnerabilities and apply relevant security advisories.