Privilege escalation, in plain terms.

Privilege escalation is the hinge between landing on a system and owning it. This section breaks the Linux and Windows paths into plain-language explainers with the real technical names a defender needs to recognise, each ending with how a penetration test surfaces that weakness in your own environment. Start with the foundations, then follow the Linux and Windows paths.

HOW IT WORKS

01 Key terms explained

Plain-language definitions of the techniques behind privilege escalation. Each page covers what it is, the attack, the payload, and how to defend.

Linux

- What is SUID and SGID?
- What is sudo abuse?
- What are Linux capabilities?
- What is cron job abuse?
- What is PATH hijacking?
- What is a Linux kernel exploit?
- What is GTFOBins?
- What is the writable /etc/passwd attack?

Windows

- What is SeImpersonatePrivilege?
- What are Potato attacks?
- What is an unquoted service path?
- What is AlwaysInstallElevated?
- What is DLL hijacking?
- What is a UAC bypass?
- What is weak service permissions?
- What are Windows privileges?

Enumeration

- What are linPEAS and winPEAS?

02 How to read this section

SOURCES

[1] MITRE ATT&CK: Privilege Escalation (TA0004)

[2] NIST SP 800-115 Technical Guide to Security Testing

[3] Microsoft: Privilege Constants (Windows)

The pages are ordered the way escalation actually works.

- Foundations first: what privilege escalation is, vertical and horizontal.
- Linux: the path to root, SUID, sudo, capabilities, cron, PATH, kernel.
- Windows: the path to SYSTEM, impersonation, services, install policy, UAC.
- Enumeration: the tooling that finds these paths automatically.

Each explainer ends with how a penetration test confirms the weakness in your own systems.

Find the privilege-escalation paths before an attacker does.

securelayer7.net/learn/privilege-escalation

Open online