What is privilege escalation?

Privilege escalation is the step where an attacker who has gained limited access to a system raises their privileges to do more than they should, typically from a standard user to root (Linux) or SYSTEM/Administrator (Windows). There are two kinds: vertical (gaining higher privileges) and horizontal (taking over another account at the same level). It usually exploits a misconfiguration, a weak permission, a vulnerable program, or an unpatched kernel, rather than a single dramatic bug, which is why thorough host enumeration is the core skill.

HOW IT WORKS

01 Vertical vs horizontal

There are two directions:

- Vertical privilege escalation: gaining higher privileges than you started with, for example a normal user becoming root. This is the classic meaning and the more dangerous one.
- Horizontal privilege escalation: taking over another account at the same privilege level, for example reading another user's files or acting as a different standard user. It often sets up a later vertical jump.

Most real attacks chain both: move sideways to an account with more useful access, then escalate vertically to root.

02 How attackers actually do it

Privilege escalation is mostly about enumeration: methodically listing everything about the host until a weak spot appears. Common categories:

- Misconfigured permissions: SUID binaries, writable files owned by root, weak service permissions.
- Excessive rights: overly broad `sudo` rules, dangerous Windows privileges like SeImpersonate.
- Vulnerable software: an unpatched kernel or a privileged program with a known exploit.
- Predictable behaviour: scheduled jobs (cron) or services that run as root and trust attacker-controlled input.

SOURCES

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

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

[3] Microsoft: Privilege Constants (Windows)

Tools like the PEAS scripts automate the enumeration, but the judgement of which finding actually leads to root is the human skill.

03 How a pentest tests for it

A penetration test starts from a realistic low-privileged position and tries to reach root or SYSTEM the way an intruder would, then maps every viable path. The deliverable is not a list of theoretical risks. It is the exact chain from "limited user" to "full control," with the specific misconfiguration or vulnerability behind each step and a fix for each one.

> THE MENTAL MODEL
>
> *Privilege escalation is rarely one big hole. It is a chain of small ones: a writable file here, an over-broad sudo rule there. Defenders win by removing the rungs, not just patching the kernel.*

Find the privilege-escalation paths before an attacker does.
securelayer7.net/learn/privilege-escalation/what-is-privilege-escalation

Open online