What is privilege escalation?

Privilege escalation is how an attacker turns limited access into powerful access, becoming an administrator or reaching resources they should not. Vertical escalation gains higher privileges; horizontal escalation moves sideways into other users' accounts at the same level. It usually exploits m isconfigurations, unpatched flaws, or excessive permissions. The defenses are least privilege, patching a nd hardening, removing excess permissions, and monitoring for privilege changes.

HOW IT WORKS

01 How attackers escalate

Escalation almost always abuses something already there:

- Misconfigurations: over-permissive sudo rules, weak file or service permissions, writable paths, exposed service accounts.
- Unpatched flaws: kernel or software vulnerabilities that hand out higher privileges.
- Excessive permissions: cloud IAM roles with far more than they need, so one compromised identity unlocks the account.
- Stolen tokens and credentials cached on a compromised host.
- Abuse of legitimate admin features that were never locked down.

In the cloud in particular, privilege escalation is usually an IAM problem: a role that can assume another role, or edit its own permissions.

02 Why it is the pivot of a breach

Almost no attack lands directly on the crown jewels. The chain is: get a foothold (often phishing or a stolen credential), escalate privileges, then move laterally to the data. Escalation is the hinge that turns a minor compromise into a major one.

This is exactly what a penetration test is built to find. The question is not whether one account is locked down, but whether an attacker who compromises a low-privilege user can climb to administrator and reach what matters.

HOW TO DEFEND

- Enforce least privilege everywhere, and review permissions regularly so they do not accumulate.
- Patch and harden operating systems, software, and cloud services promptly.
- Trim cloud IAM: remove unused permissions, avoid wildcard policies, and watch for roles that can escalate themselves.
- Separate admin accounts from everyday ones, and protect them with phishing-resistant multi-factor authentication.
- Monitor for privilege changes and new admin grants so escalation is visible.

SOURCES

[1] Privilege Escalation (Tactic TA0004)

[2] Cyber Threats and Advisories

[3] Computer Security Resource Center Glossary

See whether a low-privilege foothold can become domain admin.

securelayer7.net/learn/threats/privilege-escalation

Open online