Windows privilege escalation.

Windows privilege escalation is how an attacker goes from a standard user to SYSTEM or local Administrator. The frequent paths are token-impersonation privileges (SeImpersonate) abused through Potato attacks, weak service permissions, unquoted service paths, the AlwaysInstallElevated policy, DLL hijacking, and UAC bypasses. As on Linux, it is mostly enumeration: list privileges, services, and writable locations until a path to SYSTEM appears. Scripts like winpeas automate the sweep.

HOW IT WORKS

01 The common escalation paths

The recurring Windows privesc vectors, each with its own page:

- SeImpersonatePrivilege: a privilege common on service accounts. Details.
- Potato attacks: tools that turn SeImpersonate into SYSTEM. Details.
- Weak service permissions: a service you can reconfigure. Details.
- Unquoted service paths: a path with spaces that lets you plant an executable. Details.
- AlwaysInstallElevated: MSI packages that install as SYSTEM. Details.
- DLL hijacking: a program loading a DLL from a writable path. Details.
- UAC bypass: elevating without a prompt. Details.
- Dangerous privileges: SeBackup, SeRestore, SeDebug and more. Details.

02 Enumeration: where it starts

Windows escalation starts by listing privileges, services, and writable spots. Common first commands:

- `whoami /priv` to list the current token's privileges
- `whoami /groups` for group membership
- `wmic service get name,pathname,startmode` to find service paths
- `systeminfo` to check the patch level

SOURCES

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

[2] Microsoft: Privilege Constants (Windows)

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

- check writable service binaries and `HKLM`/`HKCU` install policy

The PEAS script winpeas automates this. The skill is spotting which privilege or service actually reaches SYSTEM.

> WATCH FOR SEIMPERSONATE
>
> *If* `whoami /priv` *shows SeImpersonatePrivilege enabled (common on IIS and SQL service accounts), a Potato attack usually grants SYSTEM directly. It is the first thing to check on Windows.*