

Forum:[Hack Forums](#)

Thread: [Post Exploitation & Privilege Escalation](#)

W1NK1LL3RX - August 22, 2025, 7:14 pm

POST-EXPLOITATION & PRIVILEGE ESCALATION

WHAT IS POST-EXPLOITATION

Post-exploitation is everything that happens after you've gained initial access. The goal is to maintain control, escalate privileges, move laterally, and gather valuable information, all without being detected.

It's not just about "getting in." It's about staying in, expanding your reach, and preparing for the bigger picture.

TOOLS FOR POST-EXPLOITATION

Some of the most useful tools for this phase:

- [Metasploit \(Meterpreter\)](#) – Provides persistence, privilege escalation modules, and lateral movement.
- [PowerSploit](#) – PowerShell scripts for privilege escalation and persistence on Windows.
- [JAWS](#) – Windows privilege escalation script.
- [LinEnum](#) – Linux privilege escalation and enumeration script.
- [PEASS-ng \(LinPEAS / WinPEAS\)](#) – Automated privilege escalation checkers.
- [GhostPack](#) – C# tools for Windows exploitation (SharpHound, Rubeus, etc.).
- [CrackMapExec](#) – Lateral movement, credential dumping, and privilege escalation.

These tools allow you to escalate from a low-privileged user to root/admin and establish persistence for long-term access.

COMMON PRIVILEGE ESCALATION METHODS

- Kernel Exploits – Exploiting vulnerabilities in outdated kernels.
- Misconfigurations – Abusing weak permissions, SUID binaries (Linux), or service misconfigurations.
- Password Reuse – Finding stored credentials or reusing cracked passwords.
- Token Impersonation – On Windows, stealing tokens to impersonate higher-privileged users.
- DLL Hijacking – Replacing DLLs that run with higher privileges.
- Scheduled Tasks & Services – Modifying or creating scheduled tasks/services to run as administrator.

- Exploiting Trusts – Moving laterally between machines with shared credentials or trusts. The idea is to transform “basic user” access into full system domination.

BEST PRACTICES

- Always enumerate before escalating, know your environment.
- Run automated tools like LinPEAS/WinPEAS, but also verify manually.
- Avoid unstable exploits that may crash the system.
- Use stealth, persistence methods should blend into normal activity.
- Rotate and encrypt backdoors to avoid detection.
- Document everything: credentials found, machines accessed, persistence set up.

A clean, careful operator leaves no unnecessary traces.

FINAL THOUGHT

Post-exploitation is the art of control. Once inside, you’re no longer just a visitor, you’re a hidden resident. Privilege escalation gives you the keys to the kingdom, and persistence ensures the door never truly closes.

This is where a hacker becomes more than an intruder, they become part of the system itself.