What are linPEAS and winPEAS?

linPEAS and winPEAS are open-source privilege-escalation enumeration scripts (part of the PEASS-ng project) that automatically check a Linux or Windows host for escalation paths, SUID binaries, sudo rules, capabilities, and writable files on Linux; privileges, services, and registry settings on Windows, and colour-highlight the most promising findings. They save an attacker hours of manual enumeration, and defenders run the same scripts to find and fix those paths first.

HOW IT WORKS

01 How they are used and payload

The attacker uploads and runs the script, then reads the highlighted output:

- Linux: `curl -L https://.../linpeas.sh | sh` or transfer and run `./linpeas.sh`
- Windows: run `winPEASx64.exe` or the batch version on the target.
- Findings flagged in red/yellow (for example a writable service, a dangerous capability, SeImpersonate enabled) point to the likely escalation.

The script does not exploit anything itself; it finds the path. The human confirms and exploits it. Shown for defensive context.

> RUN IT ON YOUR OWN HOSTS
>
> *Defenders should run linPEAS/winPEAS on their own systems exactly as an attacker would. Whatever it highlights is what a real intruder would target, so fix those findings first.*

HOW TO DEFEND

- Run linPEAS/winPEAS on your own hosts during hardening and after changes, and remediate the highlighted findings.
- Treat red/yellow flags as a prioritised work list (writable services, dangerous privileges, SUID binaries).
- Combine with patching so kernel and software CVEs are covered too.
- Detect the scripts running on production hosts, since an attacker would use them.
- Re-run periodically, as configuration drift introduces new paths.

SOURCES

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

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

[3] Microsoft: Privilege Constants (Windows)

Find the privilege-escalation paths before an attacker does.

securelayer7.net/learn/privilege-escalation/what-is-linpeas-and-winpeas

Open online