What is a Linux kernel exploit?

A Linux kernel exploit is privilege escalation that abuses a vulnerability in the kernel (or a core system component) to gain root directly, regardless of how well the system is otherwise configured. Because the kernel runs with the highest privilege, a successful exploit grants full control. Famous examples include Dirty COW (CVE-2016-5195), PwnKit (CVE-2021-4034), and Dirty Pipe (CVE-2022-0847). The defence is straightforward but operationally hard: keep the kernel patched.

HOW IT WORKS

01 The abuse and payload

The attacker checks the kernel version, finds a matching public exploit, and runs it:

- Check the version and OS: `uname -a` and `cat /etc/os-release`
- Match against known vulnerabilities (for example Dirty Pipe affects certain 5.8 to 5.16 kernels).
- Compile and run the exploit: `gcc exploit.c -o exploit && ./exploit`, which typically drops a root shell.
- Examples: Dirty COW, PwnKit (a polkit pkexec bug exploited even without source on many distros), Dirty Pipe.

Kernel exploits can crash systems, so testers use them carefully. Shown for defensive context.

> LAST RESORT, HIGH IMPACT
>
> *Testers usually try misconfiguration paths first because kernel exploits risk instability. But an unpatched kernel is a single, reliable jump to root, which is exactly why patch latency matters.*

HOW TO DEFEND

- Patch the kernel and core packages promptly; this is the primary defence.
- Track your kernel version against known privilege-escalation CVEs.
- Use live-patching where available to reduce reboot delay.
- Apply defence in depth (least privilege, monitoring) so a foothold is harder to get in the first place.
- Retire end-of-life kernels and distributions that no longer receive security updates.

SOURCES

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

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

[3] Linux man-pages: setuid(2)

Find the privilege-escalation paths before an attacker does.

securelayer7.net/learn/privilege-escalation/what-is-a-linux-kernel-exploit

Open online