What is sudo abuse?

Sudo abuse is privilege escalation through misconfigured `sudo` rules. The `sudoers` policy decides which users can run which commands as root. When a rule is too broad (allowing a program that can spawn a shell), uses NOPASSWD, or keeps a dangerous environment variable like LD_PRELOAD, a low-privileged user can turn their allowed command into a root shell. The first thing an attacker runs is `sudo -l`, and GTFOBins maps which sudo-allowed binaries escalate.

HOW IT WORKS

01 The common misconfigurations and payload

The attacker starts with `sudo -l` to see what they are allowed, then exploits it:

- A sudo-allowed editor or pager: `sudo vim -c ':!/bin/sh'` or `sudo less /etc/profile` then `!sh`
- Any sudo-allowed binary on GTFOBins (find, awk, python, tar with checkpoint, etc.)
- LD_PRELOAD kept via `env_keep`: compile a small library that calls `setuid(0)`, then `sudo LD_PRELOAD=/tmp/x.so <allowed-cmd>`
- A rule allowing `ALL` commands is an immediate `sudo /bin/bash`.

Documented techniques shown for defenders.

> START WITH SUDO -L
>
> *Run `sudo -l` as any user. It lists exactly what they can run as root. Cross-reference each allowed binary with GTFOBins; many escalate in one line.*

HOW TO DEFEND

- Grant the minimum: only the exact commands a user needs, never `ALL`, and avoid programs that can spawn shells or read arbitrary files.
- Avoid NOPASSWD except where truly necessary.
- Do not keep dangerous environment variables (remove `env_keep` entries like LD_PRELOAD; keep `env_reset` on).
- Use full paths in sudoers and avoid wildcards.
- Review sudoers regularly and test rules against GTFOBins-style abuse.

SOURCES

[1] Linux man-pages: sudoers(5)

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

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

Find the privilege-escalation paths before an attacker does.

securelayer7.net/learn/privilege-escalation/what-is-sudo-abuse

Open online