What is SUID and SGID?

SUID (Set User ID) and SGID (Set Group ID) are special Linux permission bits that make an executable run with the privileges of its owner or group, not the user who launched it. A SUID-root binary therefore runs as root for any user. That is intended for tools like `passwd`, but if a SUID binary can be made to run arbitrary commands (directly or via a known trick), any user gets a root shell. Finding and minimising SUID binaries is a core Linux hardening step.

HOW IT WORKS

01 The abuse and payload

The attacker lists SUID binaries and checks each against known abuse techniques:

- Find them: `find / -perm -4000 -type f 2>/dev/null` (SUID) or `-perm -2000` (SGID)
- Look the binary up on GTFOBins. Many standard tools escalate trivially, for example a SUID `find`: `find . -exec /bin/sh -p \; -quit`
- Custom SUID programs that call other binaries by name are abusable via PATH hijacking.

The `-p` flag keeps the elevated privileges in the spawned shell. Documented techniques shown for defenders.

> THE ONE COMMAND
>
> *Run* `find / -perm -4000 -type f 2>/dev/null` *on any Linux host. Every result is a SUID binary worth checking against GTFOBins. Unexpected entries are red flags.*

HOW TO DEFEND

- Inventory SUID/SGID binaries and remove the bit from anything that does not need it: `chmod u-s <file>`.
- Avoid SUID on custom or scripting binaries (interpreters and tools that can run commands are especially dangerous).
- Patch system binaries so known SUID exploits do not apply.
- Mount untrusted filesystems with `nosuid` so SUID bits there are ignored.
- Monitor for new SUID files appearing, a common persistence and escalation sign.

SOURCES

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

[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-suid-sgid

Open online