



Scan to visit

Linux Security Commands

Use this when: you check a Linux box for who has access, what is running and listening, what changed, and how to lock it down.

Security+ · Linux+
Sheet v1.0 · Oct 2026

Read a permission line

$r = 4 \cdot w = 2 \cdot x = 1$, add them up

- type	rwx owner = 7	r-x group = 5	--- others = 0	alice ops script.sh
chmod 750 script.sh sets exactly that. Type: - file, d directory, l link.				
chmod u+x adds execute for the owner. chown alice:ops sets owner and group.				

SAFE DEFAULTS

644	Normal files
755	Directories, scripts
600	Private keys, secrets
700	~/ .ssh
4000	SUID: runs as the file owner

Who has access?

id · whoami	My user, groups
sudo -l	What can I sudo?
w · last	Who is on, logins
sudo lastb	Failed logins
awk -F: '\$3==0' /etc/passwd	UID 0 (root) users

What is running and listening?

ss -tulpn	Ports, PIDs
sudo lsof -i :22	Port 22 owner
ps aux --sort=-%cpu head	Top CPU
systemctl --state=running	Running units

What changed? Find risky files

find / -xdev -perm -4000 -type f	SUID files
find / -xdev -perm -0002 -type f	World-writable
find /etc -mtime -1	Changed in 24 h
sha256sum file.iso	Hash to compare

Read the logs

journalctl -u ssh --since today	SSH log
journalctl -p err -b	Errors, boot
grep "Failed password" /var/log/auth.log	SSH guessing
Ubuntu and Debian shown. RHEL: /var/log/secure, unit sshd.	

Lock it down

```
# keys first, from your PC
ssh-keygen -t ed25519
ssh-copy-id admin@192.0.2.10
# firewall (Ubuntu ufw)
sudo ufw default deny incoming
sudo ufw limit 22/tcp # SSH, rate-limited
sudo ufw enable && sudo ufw status verbose
# /etc/ssh/sshd_config
PermitRootLogin no
PasswordAuthentication no # keys only
sudo sshd -t && sudo systemctl reload ssh
# patches (RHEL: sudo dnf upgrade)
sudo apt update && sudo apt upgrade
```

Before you press Enter

DANGER chmod -R 777 and rm -rf on the wrong path can't be undone.

CAUTION Allow SSH before ufw enable, or a remote session locks you out.

CAUTION Set up SSH keys and keep a second session open before you turn off passwords.

LEGAL Run these only on systems you administer.



Use sudo per command, not a root shell

sshd -t before every reload

Patch on a schedule, not when you remember