cyber.encse

CIS DISTRIBUTION INDEPENDENT LINUX BENCHMARK — ALIGNED

Linux Server Hardening (Ubuntu / RHEL)

SSH hardening, filesystem permissions, auditd configuration, sysctl tuning, PAM lockout, and firewalld/ufw setup.

This guide provides hardening rationale and verification commands for a security baseline. Always test in a non-production environment first — some settings can break application compatibility or legacy integrations. Not every control applies to every environment; assess against your own risk tolerance.

Published by eNeoteric Consultancy Services · cyber.encse.com · v1.0, August 2026

1. SSH Hardening

1.1 /etc/ssh/sshd_config baseline

```
PermitRootLogin no
PasswordAuthentication no
PubkeyAuthentication yes
Protocol 2
X11Forwarding no
MaxAuthTries 3
ClientAliveInterval 300
ClientAliveCountMax 2
AllowTcpForwarding no
LoginGraceTime 30
```

Disabling root login and password authentication forces attackers to compromise a private key rather than brute-force credentials — by far the most common initial-access vector against internet-facing Linux hosts.

1.2 Apply and verify

```
sudo sshd -t # validate config syntax before reload
sudo systemctl reload sshd
sudo ss -tlnp | grep :22
```

2. Filesystem Permissions & Mounts

Path	Recommended Mount Options	Why
/tmp	nodev,nosuid,noexec	Prevents execution of malicious binaries dropped in world-writable temp space
/var/tmp	nodev,nosuid,noexec	Same rationale as /tmp
/home	nodev,nosuid	User directories should never need device files or SUID execution
/dev/shm	nodev,nosuid,noexec	Shared memory is a common in-memory malware staging area

```
# /etc/fstab example line for /tmp
tmpfs /tmp tmpfs defaults,nodev,nosuid,noexec 0 0
```

2.1 Key permission checks

```
# World-writable files not owned by root (review each hit)
find / -xdev -type f -perm -0002 -not -path '/proc/*' 2>/dev/null

# Unauthorised SUID/SGID binaries — compare against a known-good baseline
find / -xdev \( -perm -4000 -o -perm -2000 \) -type f 2>/dev/null
```

3. Auditd Configuration

The Linux Audit daemon (auditd) provides tamper-evident logging of security-relevant kernel events. At minimum, monitor:

- Changes to /etc/passwd, /etc/shadow, /etc/group, /etc/sudoers
- Use of privilege-escalation commands (sudo, su)
- Changes to system time (clock manipulation can hide attacker activity in logs)
- Loading/unloading of kernel modules
- Failed login attempts and use of the faillock/pam_tally2 mechanism

```
# /etc/audit/rules.d/hardening.rules
-w /etc/passwd -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/sudoers -p wa -k identity
-w /etc/sudoers.d/ -p wa -k identity
-a always,exit -F arch=b64 -S execve -F euid=0 -k rootcmd
-w /sbin/insmod -p x -k modules
-w /sbin/modprobe -p x -k modules

sudo augenrules --load
sudo systemctl enable --now auditd
```

4. Kernel & Network Hardening (sysctl)

```
# /etc/sysctl.d/99-hardening.conf
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.tcp_syncookies = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.icmp_echo_ignore_broadcasts = 1
kernel.randomize_va_space = 2
fs.suid_dumpable = 0

sudo sysctl --system
```

rp_filter=1 enables reverse-path filtering to drop spoofed-source packets; randomize_va_space=2 enables full ASLR, raising the bar for memory-corruption exploits.

5. PAM Account Lockout

```
# /etc/security/faillock.conf (RHEL/pam_faillock) or /etc/pam.d/common-auth (Ubuntu/pam_tally2)
deny = 5
unlock_time = 900
fail_interval = 900
```

Locks an account for 15 minutes after 5 failed login attempts, slowing online brute-force attacks. Ensure this does not create a trivial denial-of-service against critical break-glass accounts — pair with monitoring and an out-of-band unlock procedure.

6. Host Firewall

6.1 Ubuntu (ufw)

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow from 10.0.0.0/8 to any port 22 proto tcp
sudo ufw enable
```

6.2 RHEL / CentOS (firewalld)

```
sudo firewall-cmd --set-default-zone=drop
sudo firewall-cmd --zone=trusted --add-source=10.0.0.0/8 --permanent
sudo firewall-cmd --zone=drop --add-service=ssh --permanent
sudo firewall-cmd --reload
```

7. Package & Patch Management

- Enable automatic security updates: `unattended-upgrades` (Ubuntu) or `dnf-automatic` (RHEL) for security-classified packages at minimum.
- Apply critical/actively-exploited CVE patches within 14 days; high-severity within 30 days.
- Remove unused packages and disable unused services to reduce attack surface: `systemctl list-unit-files --state=enabled`.
- Subscribe to your distribution's security advisory feed (USN for Ubuntu, RHSA for RHEL) and CISA's KEV catalog.

8. Verification Checklist

Control	Verified
Root SSH login and password auth disabled	
/tmp, /var/tmp, /dev/shm mounted noexec,nodev,nosuid	
No unauthorised SUID/SGID binaries or world-writable files	
auditd running with identity/sudoers/module watch rules	
sysctl hardening applied (rp_filter, ASLR, no redirects)	
PAM account lockout configured (5 attempts / 15 min)	
Host firewall default-deny inbound, only required ports open	
Automatic security updates enabled	
Patch SLA defined and tracked (14d critical / 30d high)	

Based on the CIS Distribution Independent Linux Benchmark. This guide is a starting baseline, not a complete hardening programme — validate against the full CIS Benchmark for your specific distribution and version.