HORIZONSHIELD

Securing Your Digital Future, Today.

INFRASTRUCTURE SERIES · BOOK 11 OF 16

Linux & Systems Security Guide

Hardening, Monitoring & Forensics — 2026

Comprehensive Linux security guide covering OS hardening, user and privilege management, file system security, kernel hardening via sysctl, auditd configuration, and incident investigation techniques.

CONTROLS	TOOLS	STANDARD	LEVEL
100+	30+	CIS RHEL/Ubuntu	Intermediate

Contents

LINUX & SYSTEMS SECURITY 2026

CHAPTER 01

Linux Hardening Fundamentals

A secure Linux system starts with a minimal installation and systematic hardening applied consistently.

CIS BENCHMARK | MINIMAL INSTALL | PATCHING | FIREWALL

Linux System Hardening

```
#!/bin/bash
# HorizonShield Linux Hardening Script
# Ubuntu/Debian — run as root

# 1. Update and upgrade all packages
apt update && apt upgrade -y && apt autoremove -y

# 2. Remove unnecessary packages
apt purge -y telnet rsh-client rsh-redone-client nis talk
apt purge -y xinetd inetd finger rlogind rshd

# 3. SSH hardening (see Chapter 03 for full config)
cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak
cat > /etc/ssh/sshd_config.d/99-hardening.conf << 'EOF'
PermitRootLogin no
PasswordAuthentication no
MaxAuthTries 3
MaxSessions 3
AllowUsers sysadmin
ClientAliveInterval 300
ClientAliveCountMax 2
Banner /etc/issue.net
LoginGraceTime 20
IgnoreRhosts yes
HostbasedAuthentication no
PermitEmptyPasswords no
X11Forwarding no
AllowTcpForwarding no
PrintLastLog yes
EOF
```

```
systemctl restart sshd

# 4. Configure UFW firewall
ufw default deny incoming
ufw default allow outgoing
ufw allow 22/tcp comment 'SSH'
ufw --force enable

# 5. Fail2ban
apt install -y fail2ban
systemctl enable fail2ban --now

# 6. Enable automatic security updates
apt install -y unattended-upgrades
dpkg-reconfigure --priority=low unattended-upgrades
```

CIS Control	Implementation	Command to Verify	Priority
Disable unused filesystems	blacklist cramfs,freevxfs,jffs2,hfs,hfsplus,squashfs,udf in /etc/modprobe.d/	lsmod | grep -E "cramfs|freevxfs|jffs2"	HIGH
Partition /tmp with noexec	Mount /tmp with noexec,nosuid,nodev options in /etc/fstab	mount | grep /tmp | grep -E "noexec|nosuid"	MEDIUM
Enable ASLR	kernel.randomize_va_space=2 in /etc/sysctl.d/	sysctl kernel.randomize_va_space	HIGH
Restrict core dumps	fs.suid_dumpable=0 AND * hard core 0 in /etc/security/limits.conf	ulimit -c (should be 0)	HIGH
Restrict su to wheel	pam_wheel.so auth required in /etc/pam.d/su	grep wheel /etc/pam.d/su	HIGH
Audit cron allowed users	Ensure /etc/cron.allow exists with only named users	ls /etc/cron.deny /etc/cron.allow	MEDIUM
Disable USB storage	blacklist usb-storage in /etc/modprobe.d/blacklist.conf	lsmod | grep usb-storage	Medium-High

CHAPTER 03

SSH Hardening

SSH is the primary remote administration attack surface on Linux systems. Harden it completely.

KEY AUTH | CONFIG | PORT KNOCKING | FAIL2BAN

SSH Security Configuration

```
# Complete /etc/ssh/sshd_config hardening
# Replace default config entirely:

# Protocol and listening
Port 22  # Consider changing to non-standard port (security by obscurity, low value)
AddressFamily inet  # IPv4 only unless you use IPv6
ListenAddress 0.0.0.0

# Authentication — password auth MUST be disabled
PermitRootLogin no
StrictModes yes
MaxAuthTries 3
MaxSessions 5
PasswordAuthentication no  # KEY AUTHENTICATION ONLY
ChallengeResponseAuthentication no
UsePAM yes
AllowUsers sysadmin deploy  # Explicit allowlist — not denylist
PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_keys

# Security restrictions
IgnoreRhosts yes
HostbasedAuthentication no
PermitEmptyPasswords no
X11Forwarding no  # Disable X11 forwarding
AllowTcpForwarding no
AllowAgentForwarding no
PermitTunnel no
PrintMotd yes
PrintLastLog yes
```

```
# Session timeout
ClientAliveInterval 300  # Disconnect inactive sessions after 5 minutes
ClientAliveCountMax 2    # 2 keepalives before disconnect
LoginGraceTime 20        # 20 seconds to authenticate

# Crypto configuration (exclude weak algorithms)
KexAlgorithms curve25519-sha256,diffie-hellman-group16-sha512
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com
HostKeyAlgorithms ssh-ed25519,rsa-sha2-512

# Verify config before restarting:
# sshd -t && systemctl restart sshd
```

SSH KEY MANAGEMENT BEST PRACTICES

(1) Unique key pair per user per server — never share private keys, (2) ED25519 preferred over RSA (shorter, faster, equally secure), (3) Passphrase-protect all private keys — add to ssh-agent for convenience, (4) Rotate SSH keys annually or when staff leave, (5) SSH certificate authority (SSH CA) for organisations with 10+ servers — avoids manual authorized_keys management.

CHAPTER 04

Kernel Hardening via sysctl

Kernel parameters significantly expand or restrict the Linux attack surface. Harden systematically.

SYSCTL | ASLR | NETWORK HARDENING | RESTRICT PTRACE

Kernel Hardening — sysctl Configuration

```
# /etc/sysctl.d/99-hs-hardening.conf
# HorizonShield kernel hardening parameters

# ── NETWORK HARDENING ──────────────────────────
# Disable IP forwarding (enable only if this is a router)
net.ipv4.ip_forward = 0
net.ipv6.conf.all.forwarding = 0

# Enable TCP SYN cookies (SYN flood protection)
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 2048

# Reject source-routed packets (IP spoofing)
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0

# Reject ICMP redirects (MITM prevention)
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv6.conf.all.accept_redirects = 0

# Enable reverse path filtering (anti-spoofing)
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1

# Disable ICMP broadcast responses (Smurf attack prevention)
net.ipv4.icmp_echo_ignore_broadcasts = 1

# ── KERNEL HARDENING ───────────────────────────
# Address Space Layout Randomisation (ASLR)
```

```
kernel.randomize_va_space = 2  # Full randomisation

# Restrict ptrace (prevents process injection)
kernel.yama.ptrace_scope = 1  # Parent processes only
# kernel.yama.ptrace_scope = 2  # Admin only (very restrictive)

# Restrict access to kernel logs
kernel.dmesg_restrict = 1
kernel.kptr_restrict = 2

# Disable core dumps (prevent credential extraction from memory)
fs.suid_dumpable = 0

# Restrict access to /proc/
kernel.perf_event_paranoid = 3

# Apply immediately:
sysctl -p /etc/sysctl.d/99-hs-hardening.conf
```

HS

H O R I Z O N S H I E L D

Securing Your Digital Future, Today.

Linux & Systems Security Guide 2026

Part of the HorizonShield Security Series — 16 comprehensive professional cybersecurity manuals covering every domain of modern enterprise security.