Security Audit Report

ProxMenux Monitor - Lynis System Audit

Date: 2/5/2026, 11:13:40
Auditor: Lynis 3.1.6
ID: PMXA-M004JVHB

1. EXECUTIVE SUMMARY

71
GOOD

System Hardening Assessment (Proxmox Adjusted)

Audit of **amd** running **Debian 13** (Proxmox VE). 277 tests executed. **3 actionable warning(s)** and **40 actionable suggestion(s)**. 11 findings are expected behavior in Proxmox VE.

Lynis raw: 66/100 — **PVE adjusted: 71/100**

0 - Critical | 50 - Moderate | 70 - Good | 100

2. SYSTEM INFORMATION

HOSTNAME	OPERATING SYSTEM	KERNEL
amd	Debian 13	6.17.13-2-pve

LYNIS VERSION	REPORT DATE	TESTS PERFORMED
3.1.6	2026-05-02 11:13	277

3. SECURITY POSTURE OVERVIEW

71/100	3	40	277
PVE SCORE (GOOD)	ACTIONABLE WARNINGS	ACTIONABLE SUGGESTIONS	TESTS PERFORMED
Lynis raw: 66	+3 PVE expected	+8 PVE expected	

FIREWALL	MALWARE SCANNER	INSTALLED PACKAGES
Active	Not Found	938

4. WARNINGS (6 - 3 ACTIONABLE)

Issues that require attention and may represent security vulnerabilities.

#1 `PKGS-7392` WARNING

Found one or more vulnerable packages.

Proxmox: Package updates should be applied regularly. Check if the 'vulnerable' packages are Proxmox-specific packages pending a PVE update.

#2 `NETW-2705` Low Risk

Couldn't find 2 responsive nameservers

Proxmox: Single DNS server is common in home/lab environments. Add a secondary DNS in /etc/resolv.conf if possible.

#3 `NETW-3015` PVE Expected

Found promiscuous interface

Proxmox: Network bridges (vmbr*) operate in promiscuous mode by design to forward traffic between VMs/containers.

#4 `NETW-3015` PVE Expected

Found promiscuous interface

Proxmox: Network bridges (vmbr*) operate in promiscuous mode by design to forward traffic between VMs/containers.

#5 `MAIL-8818` Low Risk

Found some information disclosure in SMTP banner (OS or software name)

Proxmox: Postfix is used by Proxmox for system notifications. The SMTP banner can be customized but is low risk on an internal server.

#6 `FIRE-4512` PVE Expected

iptables module(s) loaded, but no rules active

Proxmox: Proxmox uses pve-firewall which manages iptables/nftables rules dynamically. Direct iptables rules are not used.

5. SUGGESTIONS (48 - 40 ACTIONABLE)

Recommended improvements to strengthen your system's security posture. 8 items are expected behavior in Proxmox VE.

#1 `BOOT-5122` Low Priority

Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password)

Proxmox: GRUB password is recommended for physical servers but less critical for headless/remote Proxmox nodes.

#2 `BOOT-5180`

Determine runlevel and services at startup

#3 `BOOT-5264` PVE Expected

Consider hardening system services

Proxmox: Many Proxmox core services (pve-*, corosync, spiceproxy, etc.) run without systemd hardening. This is by design as they need broad system access.

```
Run '/usr/bin/systemd-analyze security SERVICE' for each service
```

#4 `KRNL-5788` PVE Expected

Determine why /vmlinuz or /boot/vmlinuz is missing on this Debian/Ubuntu system.

Proxmox: Proxmox uses its own kernel (pve-kernel) which may not place vmlinuz in the standard location.

```
/vmlinuz or /boot/vmlinuz
```

#5 `AUTH-9230`

Configure password hashing rounds in /etc/login.defs

#6 `AUTH-9262`

Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc or libpam-passwdqc

#7 `AUTH-9282` PVE Expected

When possible set expire dates for all password protected accounts

Proxmox: Proxmox system accounts (www-data, backup, etc.) don't use password expiry. Only applies to interactive user accounts.

#8 `AUTH-9284` PVE Expected

Look at the locked accounts and consider removing them

Proxmox: Locked system accounts are normal in Proxmox (daemon, nobody, etc.).

#9 `AUTH-9286`

Configure minimum password age in /etc/login.defs

#10 `AUTH-9286`

Configure maximum password age in /etc/login.defs

#11 `AUTH-9328`

Default umask in /etc/login.defs could not be found and defaults usually to 022, which could be more strict like 027

#12 `FILE-6310` PVE Expected

To decrease the impact of a full /home file system, place /home on a separate partition

Proxmox: Separate partitions for /home and /var are best practice but Proxmox typically uses a simple partition layout with LVM-thin for VM storage.

#13 `FILE-6310` PVE Expected

To decrease the impact of a full /var file system, place /var on a separate partition

Proxmox: Separate partitions for /home and /var are best practice but Proxmox typically uses a simple partition layout with LVM-thin for VM storage.

#14 `USB-1000` Low Priority

Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft

Proxmox: USB passthrough to VMs may require USB drivers. Disable only if USB passthrough is not needed.

#15 `STRG-1846` Low Priority

Disable drivers like firewire storage when not used, to prevent unauthorized storage or data theft

Proxmox: FireWire is typically not used in modern servers. Safe to disable.

#16 `PKGS-7346`

Purge old/removed packages (1 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron jobs and startup scripts.

#17 `PKGS-7370`

Install debsums utility for the verification of packages with known good database.

#18 `PKGS-7392`

Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or unattended-upgrades

#19 `PKGS-7394`

Install package apt-show-versions for patch management purposes

#20 `PKGS-7420`

Consider using a tool to automatically apply upgrades

#21 `NETW-2705`

Check your resolv.conf file and fill in a backup nameserver if possible

#22 `NETW-3200`

Determine if protocol 'dccp' is really needed on this system

Proxmox: Protocols dccp, sctp, rds, tipc are typically not needed. Can be disabled via modprobe blacklist.

#23 `NETW-3200`

Determine if protocol 'sctp' is really needed on this system

Proxmox: Protocols dccp, sctp, rds, tipc are typically not needed. Can be disabled via modprobe blacklist.

#24 **NETW-3200**

Determine if protocol 'rds' is really needed on this system

Proxmox: Protocols dccp, sctp, rds, tipc are typically not needed. Can be disabled via modprobe blacklist.

#25 **NETW-3200**

Determine if protocol 'tipc' is really needed on this system

Proxmox: Protocols dccp, sctp, rds, tipc are typically not needed. Can be disabled via modprobe blacklist.

#26 **MAIL-8818**

You are advised to hide the mail_name (option: smtpd_banner) from your postfix configuration. Use postconf -e or change your main.cf file (/etc/postfix/main.cf)

#27 **SSH-7408**

Consider hardening SSH configuration

Proxmox: SSH hardening is recommended but PermitRootLogin is required for Proxmox API/CLI management. Other SSH settings can be tuned.

```
AllowTcpForwarding (set YES to NO)
```

#28 **SSH-7408**

Consider hardening SSH configuration

Proxmox: SSH hardening is recommended but PermitRootLogin is required for Proxmox API/CLI management. Other SSH settings can be tuned.

```
ClientAliveCountMax (set 3 to 2)
```

#29 **SSH-7408**

Consider hardening SSH configuration

Proxmox: SSH hardening is recommended but PermitRootLogin is required for Proxmox API/CLI management. Other SSH settings can be tuned.

```
LogLevel (set INFO to VERBOSE)
```

#30 **SSH-7408**

Consider hardening SSH configuration

Proxmox: SSH hardening is recommended but PermitRootLogin is required for Proxmox API/CLI management. Other SSH settings can be tuned.

```
MaxSessions (set 10 to 2)
```

#31 **SSH-7408**

Consider hardening SSH configuration

Proxmox: SSH hardening is recommended but PermitRootLogin is required for Proxmox API/CLI management. Other SSH settings can be tuned.

```
PermitRootLogin (set YES to (FORCED-COMMANDS-ONLY|NO|PROHIBIT-PASSWORD|WITHOUT-PASSWORD))
```

#32 **SSH-7408**

Consider hardening SSH configuration

Proxmox: SSH hardening is recommended but PermitRootLogin is required for Proxmox API/CLI management. Other SSH settings can be tuned.

```
Port (set 22 to )
```

#33 SSH-7408

Consider hardening SSH configuration

Proxmox: SSH hardening is recommended but PermitRootLogin is required for Proxmox API/CLI management. Other SSH settings can be tuned.

`TCPKeepAlive (set YES to NO)`

#34 SSH-7408

Consider hardening SSH configuration

Proxmox: SSH hardening is recommended but PermitRootLogin is required for Proxmox API/CLI management. Other SSH settings can be tuned.

`X11Forwarding (set YES to NO)`

#35 SSH-7408

Consider hardening SSH configuration

Proxmox: SSH hardening is recommended but PermitRootLogin is required for Proxmox API/CLI management. Other SSH settings can be tuned.

`AllowAgentForwarding (set YES to NO)`

#36 LOGG-2154 Low Priority

Enable logging to an external logging host for archiving purposes and additional protection

Proxmox: External logging is recommended for production but optional for single-node environments.

#37 LOGG-2190

Check what deleted files are still in use and why.

#38 BANN-7126 Low Priority

Add a legal banner to /etc/issue, to warn unauthorized users

Proxmox: Legal banners in /etc/issue are recommended for compliance but not a security risk.

#39 BANN-7130 Low Priority

Add legal banner to /etc/issue.net, to warn unauthorized users

Proxmox: Legal banners in /etc/issue.net are recommended for compliance but not a security risk.

#40 ACCT-9622 Low Priority

Enable process accounting

Proxmox: Process accounting is useful for forensics but not required for a hypervisor.

#41 ACCT-9626 Low Priority

Enable sysstat to collect accounting (no results)

Proxmox: Sysstat is useful for performance monitoring but not a security requirement.

#42 ACCT-9628 Low Priority

Enable auditd to collect audit information

Proxmox: Auditd provides detailed audit logging. Recommended for production, optional for home/lab.

#43 FINT-4350 Low Priority

Install a file integrity tool to monitor changes to critical and sensitive files

Proxmox: File integrity monitoring (AIDE, Tripwire) is recommended for production but optional for home/lab environments.

#44 TOOL-5002 PVE Expected

Determine if automation tools are present for system management

Proxmox: Automation tools (Ansible, Puppet) are useful for multi-node clusters but not required for single-node setups.

#45 FILE-7524

Consider restricting file permissions

Recommendation: Use chmod to change file permissions

```
See screen output or log file
```

#46 KRNL-6000 PVE Expected

One or more sysctl values differ from the scan profile and could be tweaked

Proxmox: Some sysctl values differ because Proxmox needs IP forwarding, bridge-nf-call, and relaxed kernel settings for VM/container networking.

Recommendation: Change sysctl value or disable test (skip-test=KRNL-6000:)

#47 HRDN-7222 Low Priority

Harden compilers like restricting access to root user only

Proxmox: Restricting compiler access is good practice on production servers. Less critical on a hypervisor where only root has access.

#48 HRDN-7230 Low Priority

Harden the system by installing at least one malware scanner, to perform periodic file system scans

Proxmox: A malware scanner (rkhunter, ClamAV) is recommended but optional for a dedicated hypervisor.

Recommendation: Install a tool like rkhunter, chkrootkit, OSSEC, Wazuh

6. DETAILED SECURITY CHECKS (38 CATEGORIES)

Complete list of all security checks performed during the audit, organized by category.

1 Boot and services — 73 checks

Check	Status
Service Manager	systemd
Checking UEFI boot	ENABLED
Checking Secure Boot	DISABLED
Checking presence GRUB2	FOUND
Checking for password protection	NONE
Check running services (systemctl) (found 42 running services)	DONE
Check enabled services at boot (systemctl) (found 65 enabled services)	DONE
Check startup files (permissions)	OK
chrony.service (value=3.5)	PROTECTED
console-getty.service (value=9.6)	UNSAFE
corosync.service (value=9.2)	UNSAFE
cron.service (value=9.6)	UNSAFE
dbus.service (value=9.3)	UNSAFE
dm-event.service (value=9.5)	UNSAFE
emergency.service (value=9.5)	UNSAFE
fail2ban.service (value=9.6)	UNSAFE
frr.service (value=9.8)	UNSAFE
getty@tty1.service (value=9.6)	UNSAFE
haveged.service (value=3.2)	PROTECTED
iperf3.service (value=9.2)	UNSAFE
iscsid.service (value=9.5)	UNSAFE
ksmtuned.service (value=9.6)	UNSAFE
log2ram-daily.service (value=9.6)	UNSAFE
lvm2-lvmpolld.service (value=9.5)	UNSAFE
lxc-monitord.service (value=9.6)	UNSAFE
lxcfs.service (value=9.6)	UNSAFE
netavark-dhcp-proxy.service (value=9.6)	UNSAFE
nfs-blkmap.service (value=9.5)	UNSAFE
postfix.service (value=3.9)	PROTECTED
postfix@-.service (value=3.9)	PROTECTED
proxmenux-monitor.service (value=9.6)	UNSAFE
proxmox-auth-logger.service (value=9.6)	UNSAFE
proxmox-firewall.service (value=9.6)	UNSAFE
pve-cluster.service (value=9.5)	UNSAFE
pve-container@101.service (value=9.6)	UNSAFE
pve-container@103.service (value=9.6)	UNSAFE
pve-container@111.service (value=9.6)	UNSAFE

pve-firewall.service (value=9.5)	UNSAFE
pve-ha-crm.service (value=9.6)	UNSAFE
pve-ha-lrm.service (value=9.6)	UNSAFE
pve-lxc-syscalld.service (value=9.6)	UNSAFE
pvedaemon.service (value=9.6)	UNSAFE
pvefw-logger.service (value=9.5)	UNSAFE
pveproxy.service (value=9.6)	UNSAFE
pvescheduler.service (value=9.6)	UNSAFE
pvestatd.service (value=9.6)	UNSAFE
qmeventd.service (value=9.6)	UNSAFE
rc-local.service (value=9.6)	UNSAFE
rescue.service (value=9.5)	UNSAFE
rpc-gssd.service (value=9.5)	UNSAFE
rpc-statd-notify.service (value=9.5)	UNSAFE
rpc-svcgssd.service (value=9.5)	UNSAFE
rpcbind.service (value=9.5)	UNSAFE
rrdcached.service (value=9.6)	UNSAFE
smartmontools.service (value=9.6)	UNSAFE
spiceproxy.service (value=9.6)	UNSAFE
ssh-auth-logger.service (value=9.6)	UNSAFE
ssh.service (value=9.6)	UNSAFE
sshd@sshd-keygen.service (value=9.6)	UNSAFE
systemd-ask-password-console.service (value=9.4)	UNSAFE
systemd-ask-password-wall.service (value=9.4)	UNSAFE
systemd-bsod.service (value=9.5)	UNSAFE
systemd-hostnamed.service (value=1.7)	PROTECTED
systemd-initctl.service (value=9.4)	UNSAFE
systemd-journald.service (value=4.9)	PROTECTED
systemd-logind.service (value=2.8)	PROTECTED
systemd-networkd.service (value=2.9)	PROTECTED
systemd-rfkill.service (value=9.4)	UNSAFE
systemd-udevd.service (value=7.1)	MEDIUM
user@0.service (value=9.8)	UNSAFE
uuidd.service (value=5.8)	MEDIUM
watchdog-mux.service (value=9.6)	UNSAFE
zfs-zed.service (value=9.6)	UNSAFE

2 Kernel

13 checks

Check	Status
Checking default runlevel	runlevel 5
CPU support: PAE and/or NoeXecute supported	FOUND
Checking kernel version and release	DONE
Checking kernel type	DONE
Checking loaded kernel modules	DONE
Checking Linux kernel configuration file	FOUND
Checking default I/O kernel scheduler	NOT FOUND
configuration in systemd conf files	DEFAULT
configuration in /etc/profile	DEFAULT
'hard' configuration in /etc/security/limits.conf	ENABLED
'soft' configuration in /etc/security/limits.conf	DISABLED
Checking setuid core dumps configuration	DISABLED
Check if reboot is needed	NO

3 Memory and Processes

4 checks

Check	Status
Checking /proc/meminfo	FOUND
Searching for dead/zombie processes	NOT FOUND
Searching for IO waiting processes	NOT FOUND
Search prelink tooling	NOT FOUND

4 Users, Groups and Authentication

28 checks

Check	Status
Administrator accounts	OK
Unique UIDs	OK
Consistency of group files (grpck)	OK
Unique group IDs	OK
Unique group names	OK
Password file consistency	OK
Password hashing methods	OK
Checking password hashing rounds	DISABLED
Query system users (non daemons)	DONE
NIS+ authentication support	NOT ENABLED
NIS authentication support	NOT ENABLED
Sudoers file	NOT FOUND
PAM password strength tools	SUGGESTION
PAM configuration files (pam.conf)	FOUND
PAM configuration files (pam.d)	FOUND
PAM modules	FOUND
LDAP module in PAM	NOT FOUND
Accounts without expire date	SUGGESTION
Accounts without password	OK
Locked accounts	FOUND
Checking user password aging (minimum)	DISABLED
User password aging (maximum)	DISABLED
Checking expired passwords	OK
Checking Linux single user mode authentication	OK
umask (/etc/profile)	NOT FOUND
umask (/etc/login.defs)	SUGGESTION
LDAP authentication support	NOT ENABLED
Logging failed login attempts	DISABLED

5 Kerberos

1 checks

Check	Status
Check for Kerberos KDC and principals	NOT FOUND

6 Shells

3 checks

Check	Status
Session timeout settings/tools	NONE
Checking default umask in /etc/bash.bashrc	NONE
Checking default umask in /etc/profile	NONE

7 File systems

18 checks

Check	Status
Checking /home mount point	SUGGESTION
Checking /tmp mount point	OK
Checking /var mount point	SUGGESTION
Checking LVM volume groups	FOUND
Checking LVM volumes	FOUND
Query swap partitions (fstab)	OK
Testing swap partitions	OK
Testing /proc mount (hidepid)	SUGGESTION
Checking for old files in /tmp	OK
Checking /tmp sticky bit	OK
Checking /var/tmp sticky bit	OK
ACL support root file system	ENABLED
Mount options of /	NON DEFAULT
Mount options of /dev	PARTIALLY HARDENED
Mount options of /dev/shm	PARTIALLY HARDENED
Mount options of /run	HARDENED
Mount options of /tmp	PARTIALLY HARDENED
Mount options of /var/log	HARDENED

8 USB Devices

3 checks

Check	Status
Checking usb-storage driver (modprobe config)	NOT DISABLED
Checking USB devices authorization	ENABLED
Checking USBGuard	NOT FOUND

9 Storage

1 checks

Check	Status
Checking firewire ohci driver (modprobe config)	NOT DISABLED

10 NFS

4 checks

Check	Status
Query rpc registered programs	DONE
Query NFS versions	DONE
Query NFS protocols	DONE
Check running NFS daemon	NOT FOUND

11 Name services

6 checks

Check	Status
Checking search domains	FOUND
Searching DNS domain name	FOUND
Duplicate entries in hosts file	NONE
Presence of configured hostname in /etc/hosts	FOUND
Hostname mapped to localhost	NOT FOUND
Localhost mapping to IP address	OK

12 Ports and packages

8 checks

Check	Status
Searching dpkg package manager	FOUND
Query unpurged packages	FOUND
Checking security repository in sources.list.d directory	OK
Checking APT package database	OK
Checking vulnerable packages	WARNING
Checking upgradeable packages	SKIPPED
Checking package audit tool	INSTALLED
Toolkit for automatic upgrades	NOT FOUND

13 Networking

10 checks

Check	Status
Checking IPv6 configuration	ENABLED
Configuration method	AUTO
IPv6 only	NO
Nameserver: 1.1.1.1	OK
Minimal of 2 responsive nameservers	WARNING
Getting listening ports (TCP/UDP)	DONE
Checking promiscuous interfaces	WARNING
Checking status DHCP client	RUNNING
Checking for ARP monitoring software	NOT FOUND
Uncommon network protocols	0

14 Printers and Spools

2 checks

Check	Status
Checking cups daemon	NOT FOUND
Checking lp daemon	NOT RUNNING

15 Software: e-mail and messaging

3 checks

Check	Status
Postfix status	RUNNING
Postfix configuration	FOUND
Postfix banner	WARNING

16 Software: firewalls

7 checks

Check	Status
Checking iptables kernel module	FOUND
Checking iptables policies of chains	FOUND
Chain INPUT (table: filter, target: ACCEPT)	ACCEPT
Chain INPUT (table: security, target: ACCEPT)	ACCEPT
Checking for empty ruleset	WARNING
Checking for unused rules	OK
Checking host based firewall	ACTIVE

17 Software: webserver

2 checks

Check	Status
Checking Apache	NOT FOUND
Checking nginx	NOT FOUND

18 SSH Support

24 checks

Check	Status
Checking running SSH daemon	FOUND
Searching SSH configuration	FOUND
OpenSSH option: AllowTcpForwarding	SUGGESTION
OpenSSH option: ClientAliveCountMax	SUGGESTION
OpenSSH option: ClientAliveInterval	OK
OpenSSH option: FingerprintHash	OK
OpenSSH option: GatewayPorts	OK
OpenSSH option: IgnoreRhosts	OK
OpenSSH option: LoginGraceTime	OK
OpenSSH option: LogLevel	SUGGESTION
OpenSSH option: MaxAuthTries	OK
OpenSSH option: MaxSessions	SUGGESTION
OpenSSH option: PermitRootLogin	SUGGESTION
OpenSSH option: PermitUserEnvironment	OK
OpenSSH option: PermitTunnel	OK
OpenSSH option: Port	SUGGESTION
OpenSSH option: PrintLastLog	OK
OpenSSH option: StrictModes	OK
OpenSSH option: TCPKeepAlive	SUGGESTION
OpenSSH option: UseDNS	OK
OpenSSH option: X11Forwarding	SUGGESTION
OpenSSH option: AllowAgentForwarding	SUGGESTION
OpenSSH option: AllowUsers	NOT FOUND
OpenSSH option: AllowGroups	NOT FOUND

19 SNMP Support

1 checks

Check	Status
Checking running SNMP daemon	NOT FOUND

20 LDAP Services

1 checks

Check	Status
Checking OpenLDAP instance	NOT FOUND

21 PHP

1 checks

Check	Status
Checking PHP	NOT FOUND

22 Squid Support

1 checks

Check	Status
Checking running Squid daemon	NOT FOUND

23 Logging and files

13 checks

Check	Status
Checking for a running log daemon	OK
Checking Syslog-NG status	NOT FOUND
Checking systemd journal status	FOUND
Checking Metalog status	NOT FOUND
Checking RSyslog status	FOUND
Checking RFC 3195 daemon status	NOT FOUND
Checking minilogd instances	NOT FOUND
Checking wazuh-agent daemon status	NOT FOUND
Checking logrotate presence	OK
Checking remote logging	NOT ENABLED
Checking log directories (static list)	DONE
Checking open log files	DONE
Checking deleted files in use	FILES FOUND

24 Insecure services

11 checks

Check	Status
Installed inetd package	NOT FOUND
Installed xinetd package	OK
xinetd status	NOT ACTIVE
Installed rsh client package	OK
Installed rsh server package	OK
Installed telnet client package	OK
Installed telnet server package	NOT FOUND
Checking NIS client installation	OK
Checking NIS server installation	OK
Checking TFTP client installation	OK
Checking TFTP server installation	OK

25 Banners and identification

4 checks

Check	Status
/etc/issue	FOUND
/etc/issue contents	WEAK
/etc/issue.net	FOUND
/etc/issue.net contents	WEAK

26 Scheduled tasks — 1 checks

Check	Status
Checking crontab and cronjob files	DONE

27 Accounting — 3 checks

Check	Status
Checking accounting information	NOT FOUND
Checking sysstat accounting data	NOT FOUND
Checking auditd	NOT FOUND

28 Time and Synchronization — 2 checks

Check	Status
NTP daemon found: chronyd	FOUND
Checking for a running NTP daemon or client	OK

29 Cryptography — 6 checks

Check	Status
Checking for expired SSL certificates [0/151]	NONE
Found 0 encrypted and 1 unencrypted swap devices in use.	OK
Kernel entropy is sufficient	YES
HW RNG & rngd	NO
SW prng	YES
MOR-bit set	YES

30 Security frameworks — 6 checks

Check	Status
Checking presence AppArmor	FOUND
Checking AppArmor status	ENABLED
Checking presence SELinux	NOT FOUND
Checking presence TOMOYO Linux	NOT FOUND
Checking presence grsecurity	NOT FOUND
Checking for implemented MAC framework	OK

31 Software: file integrity — 3 checks

Check	Status
dm-integrity (status)	DISABLED
dm-verity (status)	DISABLED
Checking presence integrity tool	NOT FOUND

32 Software: System tooling

4 checks

Check	Status
Automation tooling	NOT FOUND
Checking presence of Fail2ban	FOUND
Checking Fail2ban jails	ENABLED
Checking for IDS/IPS tooling	FOUND

33 Software: Malware

1 checks

Check	Status
Malware software components	NOT FOUND

34 File Permissions

18 checks

Check	Status
File: /boot/grub/grub.cfg	OK
File: /etc/crontab	SUGGESTION
File: /etc/group	OK
File: /etc/group-	OK
File: /etc/hosts.allow	OK
File: /etc/hosts.deny	OK
File: /etc/issue	OK
File: /etc/issue.net	OK
File: /etc/motd	OK
File: /etc/passwd	OK
File: /etc/passwd-	OK
File: /etc/ssh/sshd_config	SUGGESTION
Directory: /root/.ssh	OK
Directory: /etc/cron.d	SUGGESTION
Directory: /etc/cron.daily	SUGGESTION
Directory: /etc/cron.hourly	SUGGESTION
Directory: /etc/cron.weekly	SUGGESTION
Directory: /etc/cron.monthly	SUGGESTION

35 Home directories

3 checks

Check	Status
Permissions of home directories	OK
Ownership of home directories	OK
Checking shell history files	OK

36 Kernel Hardening

37 checks

Check	Status
dev.tty.ldisc_autoload (exp: 0)	DIFFERENT
fs.protected_fifos (exp: 2)	DIFFERENT
fs.protected_hardlinks (exp: 1)	OK
fs.protected_regular (exp: 2)	OK
fs.protected_symlinks (exp: 1)	OK
fs.suid_dumpable (exp: 0)	OK
kernel.core_uses_pid (exp: 1)	OK
kernel.ctrl-alt-del (exp: 0)	OK
kernel.dmesg_restrict (exp: 1)	OK
kernel.kptr_restrict (exp: 2)	DIFFERENT
kernel.modules_disabled (exp: 1)	DIFFERENT
kernel.perf_event_paranoid (exp: 2 3 4)	OK
kernel.randomize_va_space (exp: 2)	OK
kernel.sysrq (exp: 0)	DIFFERENT
kernel.unprivileged_bpf_disabled (exp: 1)	DIFFERENT
kernel.yama.ptrace_scope (exp: 1 2 3)	OK
net.core.bpf_jit_harden (exp: 2)	DIFFERENT
net.ipv4.conf.all.accept_redirects (exp: 0)	OK
net.ipv4.conf.all.accept_source_route (exp: 0)	OK
net.ipv4.conf.all.bootp_relay (exp: 0)	OK
net.ipv4.conf.all.forwarding (exp: 0)	DIFFERENT
net.ipv4.conf.all.log_martians (exp: 1)	DIFFERENT
net.ipv4.conf.all.mc_forwarding (exp: 0)	OK
net.ipv4.conf.all.proxy_arp (exp: 0)	OK
net.ipv4.conf.all.rp_filter (exp: 1)	DIFFERENT
net.ipv4.conf.all.send_redirects (exp: 0)	OK
net.ipv4.conf.default.accept_redirects (exp: 0)	OK
net.ipv4.conf.default.accept_source_route (exp: 0)	OK
net.ipv4.conf.default.log_martians (exp: 1)	DIFFERENT
net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)	OK
net.ipv4.icmp_ignore_bogus_error_responses (exp: 1)	OK
net.ipv4.tcp_syncookies (exp: 1)	OK
net.ipv4.tcp_timestamps (exp: 0 1)	OK
net.ipv6.conf.all.accept_redirects (exp: 0)	DIFFERENT
net.ipv6.conf.all.accept_source_route (exp: 0)	OK
net.ipv6.conf.default.accept_redirects (exp: 0)	DIFFERENT
net.ipv6.conf.default.accept_source_route (exp: 0)	OK

37 Hardening

3 checks

Check	Status
Installed compiler(s)	FOUND
Installed malware scanner	NOT FOUND
Non-native binary formats	FOUND

38 Custom tests

1 checks

Check	Status
Running custom tests...	NONE