Lynis - Linux Auditing Report and Suggestions

Introduction

Lynis is an open-source security auditing tool for UNIX-based systems (Linux, macOS, BSD, and others). This report details the findings of a Lynis 3.1.5 security scan conducted in non-privileged mode on a Linux system running Ubuntu 22.04. The scan evaluates system security, identifies vulnerabilities, and provides recommendations for hardening.

License Information

System Overview

Scan Details

Parameter	Value
Program Version	3.1.5

Operating System	Linux
Operating System Name	REDACTED_HOST
Operating System Version	22.04
Kernel Version	5.15.0
Hardware Platform	x86_64
Hostname	REDACTED_HOST
Profiles	/home/REDACTED_USER/lynis/default.prf
Log File	/home/REDACTED_USER/lynis.log
Report File	/home/REDACTED_USER/lynis-report.dat
Report Version	1.0
Plugin Directory	./plugins
Auditor	Not Specified
Language	en
Test Category	all
Test Group	all

Program Update Status	**No Update**

Scan Mode

This scan was conducted in non-privileged mode. Some tests were skipped due to lack of root permissions, which may affect results compared to a privileged scan. Skipped tests include: BOOT-5108, BOOT-5109, BOOT-5116, BOOT-5140, AUTH-9216, AUTH-9229, AUTH-9252, AUTH-9288, FILE-6368, PKGS-7390, PKGS-7392, FIRE-4508, FIRE-4512, FIRE-4513, FIRE-4540, FIRE-4586, CRYP-7930, CRYP-7931.

Scan Results

System Tools

- Scanning available tools: **Completed**
- Checking system binaries: **Completed**

Plugins (Phase 1)

- Plugin: pam: **Executed**
- Plugin: systemd: **Executed**

Note: Plugins perform extensive tests and may take several minutes to complete.

Boot and Services

Check	Result

Service Manager	Systemd
GRUB2 Presence	**Found**
GRUB2 Password Protection	**None**
Running Services	24 found
Enabled Services at Boot	52 found
Startup Files Permissions	**OK**

Systemd Security Analysis

Service	Exposure Value	Status
ModemManager.service	6.3	**MEDIUM**
apport.service	9.6	**UNSAFE**
cloud-init-hotplugd.service	9.6	**UNSAFE**
cron.service	9.6	**UNSAFE**
dbus.service	9.5	**UNSAFE**
dm-event.service	9.5	**UNSAFE**
dmesg.service	9.6	**UNSAFE**

emergency.service	9.5	UNSAFE
fwupd.service	7.7	EXPOSED
getty@tty1.service	9.6	UNSAFE
irqbalance.service	6.2	MEDIUM
iscsid.service	9.5	UNSAFE
lvm2-lvmpolld.service	9.5	UNSAFE
lxd-agent.service	9.5	UNSAFE
multipathd.service	9.5	UNSAFE
networkd-dispatcher.service	9.6	UNSAFE
nmbd.service	9.6	UNSAFE
open-vm-tools.service	9.5	UNSAFE
plymouth-start.service	9.5	UNSAFE
polkit.service	9.6	UNSAFE
rc-local.service	9.6	UNSAFE
rescue.service	9.5	UNSAFE

rsyslog.service	9.6	UNSAFE
smbd.service	9.6	UNSAFE
snap.lxd.daemon.service	9.6	UNSAFE
snap.lxd.user-daemon.service	9.6	UNSAFE
snapd.aa-prompt-listener.service	9.6	UNSAFE
snapd.service	9.6	UNSAFE
ssh.service	9.6	UNSAFE
systemd-ask-password-console.service	9.4	UNSAFE
systemd-ask-password-plymouth.service	9.5	UNSAFE
systemd-ask-password-wall.service	9.4	UNSAFE
systemd-fsckd.service	9.5	UNSAFE
systemd-initctl.service	9.4	UNSAFE
systemd-journald.service	4.3	PROTECTED
systemd-logind.service	2.8	PROTECTED
systemd-networkd.service	2.9	PROTECTED

systemd-resolved.service	2.1	PROTECTED
systemd-rfkill.service	9.4	UNSAFE
systemd-timesyncd.service	2.1	PROTECTED
systemd-udevd.service	6.9	MEDIUM
thermald.service	9.6	UNSAFE
REDACTED_HOST-advantage.service	9.6	UNSAFE
udisks2.service	9.6	UNSAFE
unattended-upgrades.service	9.6	UNSAFE
upower.service	2.4	PROTECTED
user@1000.service	9.4	UNSAFE
uuidd.service	4.6	PROTECTED
vgauth.service	9.5	UNSAFE

Kernel

Check	Result

Default Runlevel	5
CPU Support	**PAE and/or NoExecute supported**
Kernel Version and Release	**Done**
Kernel Type	**Done**
Loaded Kernel Modules	88 active modules
Kernel Configuration File	**Found**
Default I/O Kernel Scheduler	**Not Found**
Kernel Update Availability	**OK**
Core Dumps Configuration (systemd)	**Default**
Core Dumps Configuration (/etc/profile)	**Default**
Core Dumps Configuration (hard, /etc/security/limits.conf)	**Default**
Core Dumps Configuration (soft, /etc/security/limits.conf)	**Default**
Setuid Core Dumps Configuration	**Protected**
Reboot Needed	**No**

Memory and Processes

Check	Result
/proc/meminfo	**Found**
Dead/Zombie Processes	**Not Found**
IO Waiting Processes	**Not Found**
Prelink Tooling	**Not Found**

Users, Groups, and Authentication

Check	Result
Administrator Accounts	**OK**
Unique UIDs	**OK**
Unique Group IDs	**OK**
Unique Group Names	**OK**
Password File Consistency	**Suggestion**
Password Hashing Rounds	**Disabled**
System Users (non-daemons)	**Done**
NIS+ Authentication Support	**Not Enabled**

NIS Authentication Support	**Not Enabled**
Sudoers File(s)	**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	**OK**
Accounts without Password	**OK**
Locked Accounts	**OK**
User Password Aging (Minimum)	**Disabled**
User Password Aging (Maximum)	**Disabled**
Single User Mode Authentication	**OK**
Default Umask (/etc/profile)	**Not Found**
Default Umask (/etc/login.defs)	**Suggestion**

LDAP Authentication Support	**Not Enabled**
Logging Failed Login Attempts	**Enabled**

Kerberos

Check	Result
Kerberos KDC and Principals	**Not Found**

Shells

Check	Result
Shells from /etc/shells	10 found (10 valid)
Session Timeout Settings/Tools	**None**
Default Umask in /etc/bash.bashrc	**None**
Default Umask in /etc/profile	**None**

File Systems

Check	Result
/home Mount Point	**Suggestion**

/tmp Mount Point	**Suggestion**
/var Mount Point	**Suggestion**
Swap Partitions (fstab)	**OK**
Swap Partitions	**OK**
/proc Mount (hidepid)	**Suggestion**
Old Files in /tmp	**OK**
/tmp Sticky Bit	**OK**
/var/tmp Sticky Bit	**OK**
Mount Options of /	**OK**
Mount Options of /dev	**Partially Hardened**
Mount Options of /dev/shm	**Partially Hardened**
Mount Options of /run	**Hardened**
Total Mounts (W^X)	7 of 30

USB Devices

Check	Result

USB-Storage Driver (modprobe config)	**Not Disabled**
USB Devices Authorization	**Enabled**
USBGuard	**Not Found**

Storage

Check	Result
Firewire OHCI Driver (modprobe config)	**Disabled**

NFS

Check	Result
NFS Daemon	**Not Found**

Name Services

Check	Result
Search Domains	**Found**
/etc/resolv.conf Options	**Found**
DNS Domain Name	**Unknown**

Duplicate Entries in /etc/hosts	**None**
Configured Hostname in /etc/hosts	**Found**
Hostname Mapped to REDACTED_HOST	**Not Found**
REDACTED_HOST Mapping to IP Address	**OK**

Ports and Packages

Check	Result
dpkg Package Manager	**Found**
Unpurged Packages	**None**
Security Repository in sources.list	**OK**
Upgradeable Packages	**Skipped**
Package Audit Tool	**None**
Unattended-Upgrade Toolkit	**Found**

Networking

Check	Result

IPv6 Configuration	**Enabled (Auto, not IPv6-only)**
Nameserver (127.0.0.53)	**OK**
DNSSEC (systemd-resolved)	**No**
Listening Ports (TCP/UDP)	**Done**
Promiscuous Interfaces	**OK**
DHCP Client Status	**Not Active**
ARP Monitoring Software	**Not Found**
Uncommon Network Protocols	0

Printers and Spools

Check	Result
CUPS Daemon	**Not Found**
LP Daemon	**Not Running**

Software: Firewalls

Check	Result

iptables Kernel Module	**Found**
Host-Based Firewall	**Active**

Software: Webserver

Check	Result
Apache	**Not Found**
Nginx	**Not Found**

SSH Support

Check	Result
SSH Daemon	**Found**
SSH Configuration	**Found**
OpenSSH Option: AllowUsers	**Not Found**
OpenSSH Option: AllowGroups	**Not Found**

SNMP Support

Check	Result

SNMP Daemon	Not Found

Databases

Check	Result
Database Engines	Not Found

LDAP Services

Check	Result
OpenLDAP Instance	Not Found

PHP

Check	Result
PHP	Not Found

Squid Support

Check	Result
Squid Daemon	Not Found

Logging and Files

Check	Result
Log Daemon	**OK**
Syslog-NG Status	**Not Found**
Systemd Journal Status	**Found**
Metalog Status	**Not Found**
RSyslog Status	**Found**
RFC 3195 Daemon Status	**Not Found**
Minilogd Instances	**Not Found**
Wazuh-Agent Daemon Status	**Not Found**
Logrotate Presence	**OK**
Remote Logging	**Not Enabled**
Log Directories (Static List)	**Done**
Open Log Files	**Done**
Deleted Files in Use	**Done**

Insecure Services

Check	Result
Inetd Package	**Not Found**
Xinetd Package	**OK**
Xinetd Status	**Not Active**
Rsh Client Package	**OK**
Rsh REDACTED_HOST Package	**OK**
Telnet Client Package	**OK**
Telnet REDACTED_HOST Package	**Not Found**
NIS Client Installation	**OK**
NIS REDACTED_HOST Installation	**OK**
TFTP Client Installation	**OK**
TFTP REDACTED_HOST Installation	**OK**

Banners and Identification

Check	Result

/etc/issue	Found
/etc/issue Contents	Weak
/etc/issue.net	Found
/etc/issue.net Contents	Weak

Scheduled Tasks

Check	Result
Crontab and Cronjob Files	Done

Accounting

Check	Result
Accounting Information	Not Found
Sysstat Accounting Data	Not Found
Auditd	Not Found

Time and Synchronization

Check	Result

NTP Daemon (systemd-timesyncd)	**Found**
Running NTP Daemon or Client	**OK**
Last Time Synchronization	414s

Cryptography

Check	Result
Expired SSL Certificates	**None (0/141)**
Kernel Entropy	**Sufficient**
HW RNG & rngd	**No**
SW PRNG	**No**
MOR Variable	**Weak**

Security Frameworks

Check	Result
AppArmor Presence	**Found**
AppArmor Status	**Unknown**

SELinux Presence	**Not Found**
TOMOYO Linux Presence	**Not Found**
Grsecurity Presence	**Not Found**
MAC Framework	**None**

Software: File Integrity

Check	Result
dm-integrity Status	**Disabled**
dm-verity Status	**Disabled**
Integrity Tool	**Not Found**

Software: System Tooling

Check	Result
Automation Tooling	**Not Found**
IDS/IPS Tooling	**None**

Software: Malware

Check	Result
Malware Software Components	Not Found

File Permissions

Check	Result
File: /boot/grub/grub.cfg	Suggestion
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/passwd	OK
File: /etc/passwd-	OK
File: /etc/ssh/sshd_config	Suggestion

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

Home Directories

Check	Result
Permissions of Home Directories	OK
Ownership of Home Directories	OK
Shell History Files	OK

Kernel Hardening

Check	Result
dev.tty.ldisc_autoload (exp: 0)	Different
fs.suid_dumpable (exp: 0)	Different

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.ipv4.conf.all.accept_redirects (exp: 0)	**Different**
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)	**OK**
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)	Different
net.ipv4.conf.default.accept_redirects (exp: 0)	Different
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

Hardening

Check	Result
Installed Compiler(s)	Found
Installed Malware Scanner	Not Found
Non-Native Binary Formats	Found

Custom Tests

Check	Result
Custom Tests	None

Plugins (Phase 2)

Check	Result
Plugins (Phase 2)	Done

Summary

Metric	Value
Hardening Index	62
Tests Performed	251
Plugins Enabled	2
Firewall	**Yes**
Malware Scanner	**No**
Scan Mode	Normal (Non-Privileged)
Compliance Status	Unknown
Security Audit	**Yes**
Vulnerability Scan	**Yes**

Warnings

Great, no warnings

Suggestions (35)

1. **This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]**
    - Website: https://cisofy.com/lynis/controls/LYNIS/

2. **Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]**
    - Website: https://cisofy.com/lynis/controls/BOOT-5122/
3. **Consider hardening system services [BOOT-5264]**

    Details: Run '/usr/bin/systemd-analyze security SERVICE' for each service
    - Article: Systemd features to secure service files: https://linux-audit.com/systemd/systemd-features-to-secure-units-and-services/
    - Website: https://cisofy.com/lynis/controls/BOOT-5264/
4. **If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]**
    - Article: Understand and configure core dumps on Linux: https://linux-audit.com/software/understand-and-configure-core-dumps-work-on-linux/
    - Website: https://cisofy.com/lynis/controls/KRNL-5820/
5. **Run pwck manually and correct any errors in the password file [AUTH-9228]**
    - Article: File integrity of password files: https://linux-audit.com/authentication/file-integrity-of-password-files/
    - Website: https://cisofy.com/lynis/controls/AUTH-9228/
6. **Configure password hashing rounds in /etc/login.defs [AUTH-9230]**
    - Article: Linux password security: hashing rounds: https://linux-audit.com/authentication/configure-the-minimum-password-length-on-linux-systems/
    - Website: https://cisofy.com/lynis/controls/AUTH-9230/
7. **Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc or libpam-passwdqc [AUTH-9262]**
    - Article: Configure minimum password length for Linux systems: https://linux-audit.com/configure-the-minimum-password-length-on-linux-systems/
    - Website: https://cisofy.com/lynis/controls/AUTH-9262/
8. **Configure minimum password age in /etc/login.defs [AUTH-9286]**

- Article: Configure minimum password length for Linux systems: https://linux-audit.com/configure-the-minimum-password-length-on-linux-systems/
- Website: https://cisofy.com/lynis/controls/AUTH-9286/

9. **Configure maximum password age in /etc/login.defs [AUTH-9286]**
   - Article: Configure minimum password length for Linux systems: https://linux-audit.com/configure-the-minimum-password-length-on-linux-systems/
   - Website: https://cisofy.com/lynis/controls/AUTH-9286/
10. **Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]**
    - Article: Set default file permissions on Linux with umask: https://linux-audit.com/filesystems/file-permissions/set-default-file-permissions-with-umask/
    - Website: https://cisofy.com/lynis/controls/AUTH-9328/
11. **To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]**
    - Website: https://cisofy.com/lynis/controls/FILE-6310/
12. **To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]**
    - Website: https://cisofy.com/lynis/controls/FILE-6310/
13. **To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]**
    - Website: https://cisofy.com/lynis/controls/FILE-6310/
14. **Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]**
    - Website: https://cisofy.com/lynis/controls/USB-1000/
15. **Check DNS configuration for the dns domain name [NAME-4028]**
    - Website: https://cisofy.com/lynis/controls/NAME-4028/
16. **Install debsums utility for the verification of packages with known good database. [PKGS-7370]**

    - Website: https://cisofy.com/lynis/controls/PKGS-7370/
17. **Install package apt-show-versions for patch management purposes [PKGS-7394]**
    - Website: https://cisofy.com/lynis/controls/PKGS-7394/
18. **Install a package audit tool to determine vulnerable packages [PKGS-7398]**
    - Website: https://cisofy.com/lynis/controls/PKGS-7398/
19. **Determine if protocol 'dccp' is really needed on this system [NETW-3200]**
    - Website: https://cisofy.com/lynis/controls/NETW-3200/
20. **Determine if protocol 'sctp' is really needed on this system [NETW-3200]**
    - Website: https://cisofy.com/lynis/controls/NETW-3200/
21. **Determine if protocol 'rds' is really needed on this system [NETW-3200]**
    - Website: https://cisofy.com/lynis/controls/NETW-3200/
22. **Determine if protocol 'tipc' is really needed on this system [NETW-3200]**
    - Website: https://cisofy.com/lynis/controls/NETW-3200/
23. **Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]**
    - Website: https://cisofy.com/lynis/controls/LOGG-2154/
24. **Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]**
    - Article: The real purpose of login banners: https://linux-audit.com/the-real-purpose-of-login-banners-on-linux/
    - Website: https://cisofy.com/lynis/controls/BANN-7126/
25. **Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]**
    - Article: The real purpose of login banners: https://linux-audit.com/the-real-purpose-of-login-banners-on-linux/
    - Website: https://cisofy.com/lynis/controls/BANN-7130/

26. **Enable process accounting [ACCT-9622]**
    - Website: https://cisofy.com/lynis/controls/ACCT-9622/
27. **Enable sysstat to collect accounting (no results) [ACCT-9626]**
    - Website: https://cisofy.com/lynis/controls/ACCT-9626/
28. **Enable auditd to collect audit information [ACCT-9628]**
    - Article: Linux audit framework 101: basic rules for configuration: https://linux-audit.com/linux-audit-framework/linux-audit-framework-101-basic-rules-for-configuration/
    - Article: Monitoring Linux file access, changes and data modifications: https://linux-audit.com/monitoring-linux-file-access-changes-and-modifications/
    - Website: https://cisofy.com/lynis/controls/ACCT-9628/
29. **Check output of aa-status [MACF-6208]**

    Details: /sys/kernel/security/apparmor/profiles

    Solution: Run aa-status
    - Article: AppArmor: https://linux-audit.com/security-frameworks/apparmor/
    - Website: https://cisofy.com/lynis/controls/MACF-6208/
30. **Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]**
    - Article: Monitoring Linux file access, changes and data modifications: https://linux-audit.com/monitoring-linux-file-access-changes-and-modifications/
    - Article: Monitor for file changes on Linux: https://linux-audit.com/monitor-for-file-system-changes-on-linux/
    - Website: https://cisofy.com/lynis/controls/FINT-4350/
31. **Determine if automation tools are present for system management [TOOL-5002]**
    - Website: https://cisofy.com/lynis/controls/TOOL-5002/

32. **Consider restricting file permissions [FILE-7524]**

    Details: See screen output or log file

    Solution: Use chmod to change file permissions

    - Website: https://cisofy.com/lynis/controls/FILE-7524/

33. **One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]**

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

    - Article: Linux hardening with sysctl settings: https://linux-audit.com/linux-hardening-with-sysctl/
    - Article: Overview of sysctl options and values: https://linux-audit.com/kernel/sysctl/
    - Website: https://cisofy.com/lynis/controls/KRNL-6000/

34. **Harden compilers like restricting access to root user only [HRDN-7222]**

    - Article: Why remove compilers from your system?: https://linux-audit.com/software/why-remove-compilers-from-your-system/
    - Website: https://cisofy.com/lynis/controls/HRDN-7222/

35. **Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]**

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

    - Article: Antivirus for Linux: is it really needed?: https://linux-audit.com/malware/antivirus-for-linux-really-needed/
    - Article: Monitoring Linux Systems for Rootkits: https://linux-audit.com/monitoring-linux-systems-for-rootkits/
    - Website: https://cisofy.com/lynis/controls/HRDN-7230/

Follow-up Actions

- Show details of a test: `lynis show details TEST-ID`
- Check the logfile for all details: `less /home/REDACTED_USER/lynis.log`
- Read security controls texts: https://cisofy.com

- Use `--upload` to upload data to central system (Lynis Enterprise users)

Files

File	Location
Test and Debug Information	/home/REDACTED_USER/lynis.log
Report Data	/home/REDACTED_USER/lynis-report.dat

Tip

Enhance Lynis audits by adding your settings to `custom.prf` (see `/home/REDACTED_USER/lynis/default.prf` for all settings).