**REPORT FILE FOR TASK 3**

# ELEVATELABS-CYBERSECURITY-INTERNSHIP-TASK-3-vulnerability Scan

**TASK 3:- PERFORM A BASIC VULNERABILITY SCAN ON YOUR PC.**

**⚙️ Objective:**

Use free tools available in Kali Linux to identify common vulnerabilities on your computer.

**🖥️ Scan Target:**

127.0.0.1 (Localhost)

**🧰 Tools Used:**

**nmap –** for port and vulnerability scanning.

**nikto –** for scanning web servers.

**lynis –** for full system security auditing.

**✅Step 1:** Update Kali Linux

Open the terminal and run:

sudo apt update && sudo apt upgrade -y

**✅ Step 2:** Scan with Nmap for Open Ports & Vulnerabilities

Nmap is pre-installed in Kali. Run:

sudo nmap --script vuln 127.0.0.1

This uses nmap's built-in vulnerability detection scripts.

**✅ Step 3**: Scan Web Server with Nikto (if running a local web server)

sudo nikto -h http://127.0.0.1

This will test for common vulnerabilities like outdated software, default files, etc.

**✅ Step 4:** Perform System Security Audit with Lynis

Install if not available:

sudo apt install lynis -y

Run audit:

sudo lynis audit system

Lynis will give a detailed security audit with suggestions.

**✅ Step 5:** Analyze Results

Nmap: Look at open ports and detected vulnerabilities.

Nikto: Note insecure configurations or outdated software.

Lynis: Check the score and review suggested actions.

🔍SHORT SUMMARY ...........................................................................

✅ 1. Updated Kali Linux

sudo apt update && sudo apt upgrade -y

✅ 2. Nmap Scan for Open Ports and Services

sudo nmap -sS -sV -T4 -O -v 127.0.0.1

✅ 3. Nmap Vulnerability Scan

sudo nmap --script vuln 127.0.0.1

✅ 4. Web Server Scan Using Nikto

sudo nikto -h http://127.0.0.1

✅ 5. System Audit Using Lynis

sudo apt install lynis -y

sudo lynis audit system

**📊 Summary of VULNURABILITIES FINDINGS** ..............-----------------------------------------------------

Tool Result Summary

Nmap Detected open ports: [e.g., 22, 80]. Services: SSH, HTTP

Nikto Found potential issues: outdated Apache version, directory listing enabled

Lynis Audit Score: 68/100. Suggestions: update firewall rules, disable unused services

⚠️ Critical Vulnerabilities Identified:

Open SSH port (22) – Exposed to brute force attacks.

Directory listing enabled – Reveals sensitive file structure.

Outdated services – May contain unpatched vulnerabilities.

🛡️ Suggested Fixes/Mitigations:

Configure firewall using ufw:

sudo apt install ufw

sudo ufw enable

sudo ufw allow only required ports

Disable directory listing in web server config.

**RESULT**

**NMAP**

──(simpoli㉿simpoli)-[~]

└─$ sudo nmap --script vuln 127.0.0.1

[sudo] password for simpoli:

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-07 13:50 EDT

Nmap scan report for localhost (127.0.0.1)

Host is up (0.0000060s latency).

All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.

Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 11.37 seconds

**NIKTO**

──(simpoli㉿simpoli)-[~]

└─$ sudo nikto -h http://127.0.0.1

[sudo] password for simpoli:

- Nikto v2.5.0

---------------------------------------------------------------------------

---------------------------------------------------------------------------

+ 0 host(s) tested

**LYNIS**

┌──(simpoli㉿simpoli)-[~]

└─$ sudo lynis audit system

[ Lynis 3.1.4 ]

################################################################################

Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are

welcome to redistribute it under the terms of the GNU General Public License.

See the LICENSE file for details about using this software.

2007-2024, CISOfy - https://cisofy.com/lynis/

Enterprise support available (compliance, plugins, interface and tools)

################################################################################

[+] Initializing program

------------------------------------

- Detecting OS... [ DONE ]

- Checking profiles... [ DONE ]

---------------------------------------------------

Program version: 3.1.4

Operating system: Linux

Operating system name: Kali Linux

Operating system version: Rolling release

Kernel version: 6.12.25

Hardware platform: x86\_64

Hostname: simpoli

---------------------------------------------------

Profiles: /etc/lynis/default.prf

Log file: /var/log/lynis.log

Report file: /var/log/lynis-report.dat

Report version: 1.0

Plugin directory: /etc/lynis/plugins

---------------------------------------------------

Auditor: [Not Specified]

Language: en

Test category: all

Test group: all

---------------------------------------------------

- Program update status... [ NO UPDATE ]

[+] System tools

------------------------------------

- Scanning available tools...

- Checking system binaries...

[+] Plugins (phase 1)

------------------------------------

Note: plugins have more extensive tests and may take several minutes to complete

- Plugin: debian

[

[+] Debian Tests

------------------------------------

- Checking for system binaries that are required by Debian Tests...

- Checking /bin... [ FOUND ]

- Checking /sbin... [ FOUND ]

- Checking /usr/bin... [ FOUND ]

- Checking /usr/sbin... [ FOUND ]

- Checking /usr/local/bin... [ FOUND ]

- Checking /usr/local/sbin... [ FOUND ]

- Authentication:

- PAM (Pluggable Authentication Modules):

[WARNING]: Test DEB-0001 had a long execution: 63.234000 seconds

- libpam-tmpdir [ Not Installed ]

- File System Checks:

- DM-Crypt, Cryptsetup & Cryptmount:

[WARNING]: Test DEB-0280 had a long execution: 18.668133 seconds

- Software:

- apt-listbugs [ Not Installed ]

- apt-listchanges [ Not Installed ]

- needrestart [ Not Installed ]

- fail2ban [ Not Installed ]

]

[+] Boot and services

------------------------------------

- Service Manager [ systemd ]

- Checking UEFI boot [ DISABLED ]

- Checking presence GRUB2 [ FOUND ]

- Checking for password protection [ NONE ]

- Check running services (systemctl) [ DONE ]

Result: found 19 running services

- Check enabled services at boot (systemctl) [ DONE ]

Result: found 17 enabled services

- Check startup files (permissions) [ OK ]

- Running 'systemd-analyze security'

Unit name (exposure value) and predicate

--------------------------------

- ModemManager.service (value=6.3) [ MEDIUM ]

- NetworkManager.service (value=7.8) [ EXPOSED ]

- accounts-daemon.service (value=5.5) [ MEDIUM ]

- colord.service (value=3.5) [ PROTECTED ]

- cron.service (value=9.6) [ UNSAFE ]

- dbus.service (value=9.3) [ UNSAFE ]

- emergency.service (value=9.5) [ UNSAFE ]

- getty@tty1.service (value=9.6) [ UNSAFE ]

- haveged.service (value=3.2) [ PROTECTED ]

- lightdm.service (value=9.6) [ UNSAFE ]

- lynis.service (value=9.6) [ UNSAFE ]

- open-vm-tools.service (value=9.5) [ UNSAFE ]

- pcscd.service (value=2.1) [ PROTECTED ]

- plymouth-start.service (value=9.5) [ UNSAFE ]

- polkit.service (value=1.2) [ PROTECTED ]

- 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 ]

- rtkit-daemon.service (value=7.2) [ MEDIUM ]

- smartmontools.service (value=9.6) [ UNSAFE ]

- ssh.service (value=9.6) [ UNSAFE ]

- systemd-ask-password-console.service (value=9.4) [ UNSAFE ]

- systemd-ask-password-plymouth.service (value=9.5) [ 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-timesyncd.service (value=2.1) [ PROTECTED ]

- systemd-udevd.service (value=7.1) [ MEDIUM ]

- udisks2.service (value=9.6) [ UNSAFE ]

- upower.service (value=2.4) [ PROTECTED ]

- user@1000.service (value=9.4) [ UNSAFE ]

- vgauth.service (value=9.5) [ UNSAFE ]

[+] Kernel

------------------------------------

- Checking default runlevel [ runlevel 5 ]

- Checking CPU support (NX/PAE)

CPU support: PAE and/or NoeXecute supported [ FOUND ]

- Checking kernel version and release [ DONE ]

- Checking kernel type [ DONE ]

- Checking loaded kernel modules [ DONE ]

Found 94 active modules

- Checking Linux kernel configuration file [ FOUND ]

- Checking default I/O kernel scheduler [ NOT FOUND ]

- Checking for available kernel update [ OK ]

- Checking core dumps configuration

- 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 ]

[+] Memory and Processes

------------------------------------

- Checking /proc/meminfo [ FOUND ]

- Searching for dead/zombie processes [ NOT FOUND ]

- Searching for IO waiting processes [ NOT FOUND ]

- Search prelink tooling [ NOT FOUND ]

[+] Users, Groups and Authentication

------------------------------------

- 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(s) [ FOUND ]

- Permissions for directory: /etc/sudoers.d [ WARNING ]

- Permissions for: /etc/sudoers [ OK ]

- Permissions for: /etc/sudoers.d/ospd-openvas [ OK ]

- Permissions for: /etc/sudoers.d/README [ OK ]

- Permissions for: /etc/sudoers.d/kali-grant-root [ OK ]

- 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 [ OK ]

- Checking user password aging (minimum) [ DISABLED ]

- User password aging (maximum) [ DISABLED ]

- Checking expired passwords [ OK ]

- Checking Linux single user mode authentication [ OK ]

- Determining default umask

- umask (/etc/profile) [ NOT FOUND ]

- umask (/etc/login.defs) [ SUGGESTION ]

- LDAP authentication support [ NOT ENABLED ]

- Logging failed login attempts [ DISABLED ]

[+] Kerberos

------------------------------------

- Check for Kerberos KDC and principals [ NOT FOUND ]

[+] Shells

------------------------------------

- Checking shells from /etc/shells

Result: found 13 shells (valid shells: 13).

- Session timeout settings/tools [ NONE ]

- Checking default umask values

- Checking default umask in /etc/bash.bashrc [ NONE ]

- Checking default umask in /etc/profile [ NONE ]

[+] File systems

------------------------------------

- Checking mount points

- Checking /home mount point [ SUGGESTION ]

- Checking /tmp mount point [ OK ]

- Checking /var mount point [ SUGGESTION ]

- 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 ]

- Total without nodev:6 noexec:11 nosuid:4 ro or noexec (W^X): 11 of total 28

- Checking Locate database [ NOT FOUND ]

- Disable kernel support of some filesystems

[+] USB Devices

------------------------------------

- Checking usb-storage driver (modprobe config) [ NOT DISABLED ]

- Checking USB devices authorization [ ENABLED ]

- Checking USBGuard [ NOT FOUND ]

[+] Storage

------------------------------------

- Checking firewire ohci driver (modprobe config) [ NOT DISABLED ]

[+] NFS

------------------------------------

- Query rpc registered programs [ DONE ]

- Query NFS versions [ DONE ]

- Query NFS protocols [ DONE ]

- Check running NFS daemon [ NOT FOUND ]

[+] Name services

------------------------------------

- Checking search domains [ FOUND ]

- Searching DNS domain name [ FOUND ]

Domain name: simpoli

- Checking /etc/hosts

- 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 ]

[+] Ports and packages

------------------------------------

- Searching package managers

- Searching RPM package manager [ FOUND ]

- Querying RPM package manager

- Searching dpkg package manager [ FOUND ]

- Querying package manager

[WARNING]: Test PKGS-7345 had a long execution: 44.648236 seconds

- Query unpurged packages [ NONE ]

- Checking APT package database [ OK ]

- Checking vulnerable packages (apt-get only) [ DONE ]

[WARNING]: Test PKGS-7392 had a long execution: 31.096735 seconds

- Checking upgradeable packages [ SKIPPED ]

- Checking package audit tool [ INSTALLED ]

Found: apt-get

- Toolkit for automatic upgrades [ NOT FOUND ]

[+] Networking

------------------------------------

- Checking IPv6 configuration [ ENABLED ]

Configuration method [ AUTO ]

IPv6 only [ NO ]

- Checking configured nameservers

- Testing nameservers

Nameserver: 192.168.213.2 [ OK ]

- Minimal of 2 responsive nameservers [ WARNING ]

- Checking default gateway [ DONE ]

- Getting listening ports (TCP/UDP) [ SKIPPED ]

- Checking promiscuous interfaces [ OK ]

- Checking waiting connections [ OK ]

- Checking status DHCP client [ NOT ACTIVE ]

- Checking for ARP monitoring software [ NOT FOUND ]

- Uncommon network protocols [ 0 ]

[+] Printers and Spools

------------------------------------

- Checking cups daemon [ NOT FOUND ]

- Checking lp daemon [ NOT RUNNING ]

[+] Software: e-mail and messaging

------------------------------------

[+] Software: firewalls

------------------------------------

- 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 ]

[+] Software: webserver

------------------------------------

- Checking Apache (binary /usr/sbin/apache2) [ FOUND ]

Info: Configuration file found (/etc/apache2/apache2.conf)

Info: No virtual hosts found

\* Loadable modules [ FOUND (118) ]

- Found 118 loadable modules

mod\_evasive: anti-DoS/brute force [ NOT FOUND ]

mod\_reqtimeout/mod\_qos [ FOUND ]

ModSecurity: web application firewall [ NOT FOUND ]

- Checking TraceEnable setting in:

/etc/apache2/sites-available/000-default.conf [ NOT FOUND ]

/etc/apache2/sites-available/default-ssl.conf [ NOT FOUND ]

/etc/apache2/conf-enabled/serve-cgi-bin.conf [ NOT FOUND ]

/etc/apache2/conf-enabled/security.conf [ FOUND ]

/etc/apache2/conf-enabled/other-vhosts-access-log.conf [ NOT FOUND ]

/etc/apache2/conf-enabled/javascript-common.conf [ NOT FOUND ]

/etc/apache2/conf-enabled/localized-error-pages.conf [ NOT FOUND ]

/etc/apache2/conf-enabled/charset.conf [ NOT FOUND ]

/etc/apache2/ports.conf [ NOT FOUND ]

/etc/apache2/sites-enabled/000-default.conf [ NOT FOUND ]

/etc/apache2/mods-enabled/status.conf [ NOT FOUND ]

/etc/apache2/mods-enabled/autoindex.conf [ NOT FOUND ]

/etc/apache2/mods-enabled/reqtimeout.conf [ NOT FOUND ]

/etc/apache2/mods-enabled/mpm\_prefork.conf [ NOT FOUND ]

/etc/apache2/mods-enabled/php8.4.conf [ NOT FOUND ]

/etc/apache2/mods-enabled/alias.conf [ NOT FOUND ]

/etc/apache2/mods-enabled/setenvif.conf [ NOT FOUND ]

/etc/apache2/mods-enabled/mime.conf [ NOT FOUND ]

/etc/apache2/mods-enabled/deflate.conf [ NOT FOUND ]

/etc/apache2/mods-enabled/negotiation.conf [ NOT FOUND ]

/etc/apache2/mods-enabled/dir.conf [ NOT FOUND ]

/etc/apache2/conf-available/serve-cgi-bin.conf [ NOT FOUND ]

/etc/apache2/conf-available/security.conf [ FOUND ]

/etc/apache2/conf-available/other-vhosts-access-log.conf [ NOT FOUND ]

/etc/apache2/conf-available/javascript-common.conf [ NOT FOUND ]

/etc/apache2/conf-available/localized-error-pages.conf [ NOT FOUND ]

/etc/apache2/conf-available/charset.conf [ NOT FOUND ]

/etc/apache2/apache2.conf [ NOT FOUND ]

/etc/apache2/mods-available/userdir.conf [ NOT FOUND ]

/etc/apache2/mods-available/proxy\_html.conf [ NOT FOUND ]

/etc/apache2/mods-available/cgid.conf [ NOT FOUND ]

/etc/apache2/mods-available/proxy.conf [ NOT FOUND ]

/etc/apache2/mods-available/status.conf [ NOT FOUND ]

/etc/apache2/mods-available/autoindex.conf [ NOT FOUND ]

/etc/apache2/mods-available/http2.conf [ NOT FOUND ]

/etc/apache2/mods-available/reqtimeout.conf [ NOT FOUND ]

/etc/apache2/mods-available/ssl.conf [ NOT FOUND ]

/etc/apache2/mods-available/proxy\_connect.conf [ NOT FOUND ]

/etc/apache2/mods-available/info.conf [ NOT FOUND ]

/etc/apache2/mods-available/mpm\_prefork.conf [ NOT FOUND ]

/etc/apache2/mods-available/proxy\_ftp.conf [ NOT FOUND ]

/etc/apache2/mods-available/ldap.conf [ NOT FOUND ]

/etc/apache2/mods-available/php8.4.conf [ NOT FOUND ]

/etc/apache2/mods-available/proxy\_balancer.conf [ NOT FOUND ]

/etc/apache2/mods-available/mpm\_worker.conf [ NOT FOUND ]

/etc/apache2/mods-available/actions.conf [ NOT FOUND ]

/etc/apache2/mods-available/alias.conf [ NOT FOUND ]

/etc/apache2/mods-available/setenvif.conf [ NOT FOUND ]

/etc/apache2/mods-available/mime.conf [ NOT FOUND ]

/etc/apache2/mods-available/mime\_magic.conf [ NOT FOUND ]

/etc/apache2/mods-available/dav\_fs.conf [ NOT FOUND ]

/etc/apache2/mods-available/deflate.conf [ NOT FOUND ]

/etc/apache2/mods-available/negotiation.conf [ NOT FOUND ]

/etc/apache2/mods-available/dir.conf [ NOT FOUND ]

/etc/apache2/mods-available/cache\_disk.conf [ NOT FOUND ]

/etc/apache2/mods-available/mpm\_event.conf [ NOT FOUND ]

- Checking nginx [ NOT FOUND ]

[+] SSH Support

------------------------------------

- Checking running SSH daemon [ NOT FOUND ]

[+] SNMP Support

------------------------------------

- Checking running SNMP daemon [ NOT FOUND ]

[+] Databases

------------------------------------

No database engines found

[+] LDAP Services

------------------------------------

- Checking OpenLDAP instance [ NOT FOUND ]

[+] PHP

------------------------------------

- Checking PHP [ FOUND ]

- Checking PHP disabled functions [ FOUND ]

- Checking expose\_php option [ OFF ]

- Checking enable\_dl option [ OFF ]

- Checking allow\_url\_fopen option [ ON ]

- Checking allow\_url\_include option [ OFF ]

- Checking listen option [ OK ]

[+] Squid Support

------------------------------------

- Checking running Squid daemon [ NOT FOUND ]

[+] Logging and files

------------------------------------

- 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 [ NOT 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 ]

[+] Insecure services

------------------------------------

- Installed inetd package [ NOT FOUND ]

- Installed xinetd package [ OK ]

- xinetd status [ NOT ACTIVE ]

- Installed rsh client package [ SUGGESTION ]

- 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 [ SUGGESTION ]

- Checking TFTP server installation [ SUGGESTION ]

[+] Banners and identification

------------------------------------

- /etc/issue [ FOUND ]

- /etc/issue contents [ WEAK ]

- /etc/issue.net [ FOUND ]

- /etc/issue.net contents [ WEAK ]

[+] Scheduled tasks

------------------------------------

- Checking crontab and cronjob files [ DONE ]

[+] Accounting

------------------------------------

- Checking accounting information [ NOT FOUND ]

- Checking sysstat accounting data [ DISABLED ]

- Checking auditd [ NOT FOUND ]

[+] Time and Synchronization

------------------------------------

- NTP daemon found: systemd (timesyncd) [ FOUND ]

- Checking for a running NTP daemon or client [ OK ]

- Last time synchronization [ 303s ]

[+] Cryptography

------------------------------------

- Checking for expired SSL certificates [0/152] [ NONE ]

[WARNING]: Test CRYP-7902 had a long execution: 78.031742 seconds

- Found 0 encrypted and 1 unencrypted swap devices in use. [ OK ]

- Kernel entropy is sufficient [ YES ]

- HW RNG & rngd [ NO ]

- SW prng [ YES ]

- MOR variable not found [ WEAK ]

[+] Virtualization

------------------------------------

[+] Containers

------------------------------------

[+] Security frameworks

------------------------------------

- Checking presence AppArmor [ FOUND ]

- Checking AppArmor status [ DISABLED ]

- Checking presence SELinux [ NOT FOUND ]

- Checking presence TOMOYO Linux [ NOT FOUND ]

- Checking presence grsecurity [ NOT FOUND ]

- Checking for implemented MAC framework [ NONE ]

[+] Software: file integrity

------------------------------------

- Checking file integrity tools

- dm-integrity (status) [ DISABLED ]

- dm-verity (status) [ DISABLED ]

- Checking presence integrity tool [ NOT FOUND ]

[+] Software: System tooling

------------------------------------

- Checking automation tooling

- Automation tooling [ NOT FOUND ]

- Checking for IDS/IPS tooling [ NONE ]

[+] Software: Malware

------------------------------------

- Malware software components [ NOT FOUND ]

[+] File Permissions

------------------------------------

- Starting file permissions check

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 ]

[+] Home directories

------------------------------------

- Permissions of home directories [ WARNING ]

- Ownership of home directories [ OK ]

- Checking shell history files [ OK ]

[+] Kernel Hardening

------------------------------------

- Comparing sysctl key pairs with scan profile

- 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) [ DIFFERENT ]

- 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) [ DIFFERENT ]

- net.core.bpf\_jit\_harden (exp: 2) [ DIFFERENT ]

- 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

------------------------------------

- Installed compiler(s) [ FOUND ]

- Installed malware scanner [ NOT FOUND ]

- Non-native binary formats [ FOUND ]

[+] Custom tests

------------------------------------

- Running custom tests... [ NONE ]

[+] Plugins (phase 2)

------------------------------------

================================================================================

-[ Lynis 3.1.4 Results ]-

Warnings (2):

----------------------------

! Couldn't find 2 responsive nameservers [NETW-2705]

https://cisofy.com/lynis/controls/NETW-2705/

! iptables module(s) loaded, but no rules active [FIRE-4512]

https://cisofy.com/lynis/controls/FIRE-4512/

Suggestions (49):

----------------------------

\* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]

- Related resources

\* Website: https://cisofy.com/lynis/controls/LYNIS/

\* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]

- Related resources

\* Website: https://cisofy.com/lynis/controls/DEB-0280/

\* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]

- Related resources

\* Website: https://cisofy.com/lynis/controls/DEB-0810/

\* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]

- Related resources

\* Website: https://cisofy.com/lynis/controls/DEB-0811/

\* Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [DEB-0831]

- Related resources

\* Website: https://cisofy.com/lynis/controls/DEB-0831/

\* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]

- Related resources

\* Website: https://cisofy.com/lynis/controls/DEB-0880/

\* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]

- Related resources

\* Website: https://cisofy.com/lynis/controls/BOOT-5122/

\* Determine runlevel and services at startup [BOOT-5180]

- Related resources

\* Website: https://cisofy.com/lynis/controls/BOOT-5180/

\* Consider hardening system services [BOOT-5264]

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

- Related resources

\* 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/

\* Configure password hashing rounds in /etc/login.defs [AUTH-9230]

- Related resources

\* 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/

\* Install a PAM module for password strength testing like pam\_cracklib or pam\_passwdqc or libpam-passwdqc [AUTH-9262]

- Related resources

\* 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/

\* When possible set expire dates for all password protected accounts [AUTH-9282]

- Related resources

\* Website: https://cisofy.com/lynis/controls/AUTH-9282/

\* Configure minimum password age in /etc/login.defs [AUTH-9286]

- Related resources

\* 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/

\* Configure maximum password age in /etc/login.defs [AUTH-9286]

- Related resources

\* 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/

\* Default umask in /etc/login.defs could not be found and defaults usually to 022, which could be more strict like 027 [AUTH-9328]

- Related resources

\* 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/

\* To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]

- Related resources

\* Website: https://cisofy.com/lynis/controls/FILE-6310/

\* To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]

- Related resources

\* Website: https://cisofy.com/lynis/controls/FILE-6310/

\* The database required for 'locate' could not be found. Run 'updatedb' or 'locate.updatedb' to create this file. [FILE-6410]

- Related resources

\* Website: https://cisofy.com/lynis/controls/FILE-6410/

\* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]

- Related resources

\* Website: https://cisofy.com/lynis/controls/USB-1000/

\* Disable drivers like firewire storage when not used, to prevent unauthorized storage or data theft [STRG-1846]

- Related resources

\* Website: https://cisofy.com/lynis/controls/STRG-1846/

\* Check RPM database as RPM binary available but does not reveal any packages [PKGS-7308]

- Related resources

\* Website: https://cisofy.com/lynis/controls/PKGS-7308/

\* Install debsums utility for the verification of packages with known good database. [PKGS-7370]

- Related resources

\* Website: https://cisofy.com/lynis/controls/PKGS-7370/

\* Install package apt-show-versions for patch management purposes [PKGS-7394]

- Related resources

\* Website: https://cisofy.com/lynis/controls/PKGS-7394/

\* Consider using a tool to automatically apply upgrades [PKGS-7420]

- Related resources

\* Website: https://cisofy.com/lynis/controls/PKGS-7420/

\* Check your resolv.conf file and fill in a backup nameserver if possible [NETW-2705]

- Related resources

\* Website: https://cisofy.com/lynis/controls/NETW-2705/

\* Determine if protocol 'dccp' is really needed on this system [NETW-3200]

- Related resources

\* Website: https://cisofy.com/lynis/controls/NETW-3200/

\* Determine if protocol 'sctp' is really needed on this system [NETW-3200]

- Related resources

\* Website: https://cisofy.com/lynis/controls/NETW-3200/

\* Determine if protocol 'rds' is really needed on this system [NETW-3200]

- Related resources

\* Website: https://cisofy.com/lynis/controls/NETW-3200/

\* Determine if protocol 'tipc' is really needed on this system [NETW-3200]

- Related resources

\* Website: https://cisofy.com/lynis/controls/NETW-3200/

\* Install Apache mod\_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]

- Related resources

\* Website: https://cisofy.com/lynis/controls/HTTP-6640/

\* Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]

- Related resources

\* Website: https://cisofy.com/lynis/controls/HTTP-6643/

\* Change the allow\_url\_fopen line to: allow\_url\_fopen = Off, to disable downloads via PHP [PHP-2376]

- Related resources

\* Website: https://cisofy.com/lynis/controls/PHP-2376/

\* Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]

- Related resources

\* Website: https://cisofy.com/lynis/controls/LOGG-2154/

\* Check what deleted files are still in use and why. [LOGG-2190]

- Related resources

\* Website: https://cisofy.com/lynis/controls/LOGG-2190/

\* Remove rsh client when it is not in use or replace with the more secure SSH package [INSE-8300]

- Related resources

\* Website: https://cisofy.com/lynis/controls/INSE-8300/

\* It is recommended that TFTP be removed, unless there is a specific need for TFTP (such as a boot server) [INSE-8318]

- Related resources

\* Website: https://cisofy.com/lynis/controls/INSE-8318/

\* Removing the atftpd package decreases the risk of the accidental (or intentional) activation of tftp services [INSE-8320]

- Related resources

\* Website: https://cisofy.com/lynis/controls/INSE-8320/

\* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]

- Related resources

\* 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/

\* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]

- Related resources

\* 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/

\* Enable process accounting [ACCT-9622]

- Related resources

\* Website: https://cisofy.com/lynis/controls/ACCT-9622/

\* Enable sysstat to collect accounting (disabled) [ACCT-9626]

- Related resources

\* Website: https://cisofy.com/lynis/controls/ACCT-9626/

\* Enable auditd to collect audit information [ACCT-9628]

- Related resources

\* 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/

\* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]

- Related resources

\* 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/

\* Determine if automation tools are present for system management [TOOL-5002]

- Related resources

\* Website: https://cisofy.com/lynis/controls/TOOL-5002/

\* Consider restricting file permissions [FILE-7524]

- Details : See screen output or log file

- Solution : Use chmod to change file permissions

- Related resources

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

\* Double check the permissions of home directories as some might be not strict enough. [HOME-9304]

- Related resources

\* Website: https://cisofy.com/lynis/controls/HOME-9304/

\* 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:<sysctl-key>)

- Related resources

\* 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/

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

- Related resources

\* 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/

\* 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

- Related resources

\* Article: Antivirus for Linux: is it really needed?: https://linux-audit.com/malware/antivirus-for-linux-really-needed/

ssaudit.com/monitoring-linux-systems-for-rootkits/

\* Website: https://cisofy.com/lynis/controls/HRDN-7230/

Follow-up:

----------------------------

- Show details of a test (lynis show details TEST-ID)

- Check the logfile for all details (less /var/log/lynis.log)

- Read security controls texts (https://cisofy.com)

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

================================================================================

Lynis security scan details:

Hardening index : 62 [############ ]

Tests performed : 273

Plugins enabled : 1

Components:

- Firewall [V]

- Malware scanner [X]

Scan mode:

Normal [V] Forensics [ ] Integration [ ] Pentest [ ]

Lynis modules:

- Compliance status [?]

- Security audit [V]

- Vulnerability scan [V]

Files:

- Test and debug information : /var/log/lynis.log

- Report data : /var/log/lynis-report.dat

================================================================================

Lynis 3.1.4

Auditing, system hardening, and compliance for UNIX-based systems

(Linux, macOS, BSD, and others)

2007-2024, CISOfy - https://cisofy.com/lynis/

Enterprise support available (compliance, plugins, interface and tools)

================================================================================

[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)