INFORME LYNIS

[Lynis 3.1.3]
[Lynis 3.1.3]
##
 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

 ##
 # #
 # NON-PRIVILEGED SCAN MODE #
 # #
 ##
 NOTES:
 ----
 * Some tests will be skipped (as they require root permissions)
 * Some tests might fail silently or give different results
 - Detecting OS... [DONE]
 - Checking profiles... [DONE]
 - Detecting language and localization [es]
Translation file (db/languages/es) needs an update [OUTDATED]
==
Help other users and translate the missing lines:
1) Go to: https://github.com/CISOfy/lynis/edit/master/db/languages/es
2) Translate (some of) the lines starting with a hash (#) and remove the leading hash
3) Commit the changes
Thank you!
Note: no lines with a hash? Look if the file recently has been changed by another translator.
==

 Program version: 3.1.3
 Operating system: Linux
 Operating system name: Ubuntu
 Operating system version: 24.04
 Kernel version: 6.8.0
 Hardware platform: x86_64
 Hostname: aaron-VirtualBox

 Profiles: /home/aaron/lynis/default.prf
 Log file: /home/aaron/lynis.log
 Report file: /home/aaron/lynis-report.dat
 Report version: 1.0
 Plugin directory: ./plugins

```
 Auditor: [Not Specified]
 Language: es
 Test category: all
 Test group: all
 ------------------------------------------------
 - Program update status... [ SIN ACTUALIZACIÓN ]
[+] Herramientas del sistema
------------------------------------
 - Scanning available tools...
 - Checking system binaries...
[+] Plugins (fase 1)
------------------------------------
 Nota: los plugins contienen pruebas más extensivas y toman más tiempo
 - Plugin: pam
[..]
 - Plugin: systemd
[.................]
[+] Arranque y servicios
------------------------------------
 - Service Manager [ systemd ]
 - Checking presence GRUB2 [ ENCONTRADO ]
- Checking for password protection [ NINGUNO ]
 - Check running services (systemctl) [ HECHO ]
 Result: found 29 running services
 - Check enabled services at boot (systemctl) [ HECHO ]
 Result: found 55 enabled services
 - Check startup files (permissions) [ OK ]
 - Running 'systemd-analyze security'
 - ModemManager.service: [ MEDIO ]
 - NetworkManager.service: [ EXPUESTO ]
 - accounts-daemon.service: [ MEDIO ]
 - alsa-state.service: [ INSEGURO ]
 - anacron.service: [ INSEGURO ]
 - avahi-daemon.service: [ INSEGURO ]
 - colord.service: [ PROTEGIDO ]
 - cron.service: [ INSEGURO ]
 - cups-browsed.service: [ INSEGURO ]
 - cups.service: [ INSEGURO ]
 - dbus.service: [ INSEGURO ]
 - dmesg.service: [ INSEGURO ]
 - emergency.service: [ INSEGURO ]
 - gdm.service: [ INSEGURO ]
 - getty@tty1.service: [ INSEGURO ]
 - gnome-remote-desktop.service: [ INSEGURO ]
 - kerneloops.service: [ INSEGURO ]
 - networkd-dispatcher.service: [ INSEGURO ]
 - plymouth-start.service: [ INSEGURO ]
 - polkit.service: [ PROTEGIDO ]
 - power-profiles-daemon.service: [ MEDIO ]
 - rc-local.service: [ INSEGURO ]
 - rescue.service: [ INSEGURO ]
 - rsyslog.service: [ MEDIO ]
```

- rtkit-daemon.service: [MEDIO]
- snapd.service: [INSEGURO]
- sssd-autofs.service: [INSEGURO]
- sssd-nss.service: [INSEGURO]
- sssd-pac.service: [INSEGURO]
- sssd-pam.service: [INSEGURO]
- sssd-ssh.service: [INSEGURO]
- sssd-sudo.service: [INSEGURO]
- sssd.service: [EXPUESTO]
- switcheroo-control.service: [EXPUESTO]
- systemd-ask-password-console.service: [INSEGURO]
- systemd-ask-password-plymouth.service: [INSEGURO]
- systemd-ask-password-wall.service: [INSEGURO]
- systemd-bsod.service: [INSEGURO]
- systemd-fsckd.service: [INSEGURO]
- systemd-initctl.service: [INSEGURO]
- systemd-journald.service: [PROTEGIDO]
- systemd-logind.service: [PROTEGIDO]
- systemd-networkd.service: [PROTEGIDO]
- systemd-oomd.service: [PROTEGIDO]
- systemd-resolved.service: [PROTEGIDO]
- systemd-rfkill.service: [INSEGURO]
- systemd-timesyncd.service: [PROTEGIDO]
- systemd-udevd.service: [MEDIO]
- thermald.service: [INSEGURO]
- tpm-udev.service: [INSEGURO]
- ubuntu-advantage.service: [INSEGURO]
- udisks2.service: [INSEGURO]
- unattended-upgrades.service: [INSEGURO]
- upower.service: [PROTEGIDO]
- user@1000.service: [INSEGURO]
- uuidd.service: [MEDIO]
- whoopsie.service: [INSEGURO]
- wpa_supplicant.service: [INSEGURO]

[+] Kernel

- Checking default runlevel [runlevel 5]
- Checking CPU support (NX/PAE)

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

- Checking kernel version and release [HECHO]
- Checking kernel type [HECHO]
- Checking loaded kernel modules [HECHO]

Found 68 active modules

- Checking Linux kernel configuration file [ENCONTRADO]
- Checking default I/O kernel scheduler [NO ENCONTRADO]
- Checking for available kernel update [OK]
- Checking core dumps configuration

- configuration in systemd conf files [POR DEFECTO]
- configuration in /etc/profile [POR DEFECTO]
- 'hard' configuration in /etc/security/limits.conf [POR DEFECTO]
- 'soft' configuration in /etc/security/limits.conf [POR DEFECTO]
- Checking setuid core dumps configuration [PROTEGIDO]

 - Check if reboot is needed [NO]
[+] Memoria y procesos

 - Checking /proc/meminfo [ENCONTRADO]
 - Searching for dead/zombie processes [NO ENCONTRADO]
 - Searching for IO waiting processes [NO ENCONTRADO]
 - Search prelink tooling [NO ENCONTRADO]
[+] Usuarios, grupos y autenticación

 - Administrator accounts [OK]
 - Unique UIDs [OK]
 - Unique group IDs [OK]
 - Unique group names [OK]
 - Password file consistency [SUGERENCIA]
 - Checking password hashing rounds [DESHABILITADO]
 - Query system users (non daemons) [HECHO]
 - NIS+ authentication support [NO HABILITADO]
 - NIS authentication support [NO HABILITADO]
 - Sudoers file(s) [ENCONTRADO]
 - PAM password strength tools [OK]
 - PAM configuration files (pam.conf) [ENCONTRADO]
 - PAM configuration files (pam.d) [ENCONTRADO]
 - PAM modules [ENCONTRADO]
 - LDAP module in PAM [NO ENCONTRADO]
 - Accounts without expire date [OK]
 - Accounts without password [OK]
 - Locked accounts [OK]
 - Checking user password aging (minimum) [DESHABILITADO]
 - User password aging (maximum) [DESHABILITADO]
 - Checking Linux single user mode authentication [OK]
 - Determining default umask
- umask (/etc/profile) [NO ENCONTRADO]
- umask (/etc/login.defs) [SUGERENCIA]
 - LDAP authentication support [NO HABILITADO]
 - Logging failed login attempts [HABILITADO]
[+] Kerberos

 - Check for Kerberos KDC and principals [NO ENCONTRADO]
[+] Shells

 - Checking shells from /etc/shells
Result: found 7 shells (valid shells: 7).
- Session timeout settings/tools [NINGUNO]
 - Checking default umask values
- Checking default umask in /etc/bash.bashrc [NINGUNO]
- Checking default umask in /etc/profile [NINGUNO]
[+] Sistemas de ficheros

 - Checking mount points
- Checking /home mount point [SUGERENCIA]
- Checking /tmp mount point [SUGERENCIA]
- Checking /var mount point [SUGERENCIA]

- Query swap partitions (fstab) [OK]
- Testing swap partitions [OK]
- Testing /proc mount (hidepid) [SUGERENCIA]
- Checking for old files in /tmp [OK]
- Checking /tmp sticky bit [OK]
- Checking /var/tmp sticky bit [OK]
- Mount options of / [OK]
- Mount options of /dev [PARCIALMENTE BASTIONADO]
- Mount options of /dev/shm [PARCIALMENTE BASTIONADO]
- Mount options of /run [BASTIONADO]
- Total without nodev:6 noexec:21 nosuid:15 ro or noexec (W^X): 10 of total 37
- JBD driver is not loaded [NECESITA VERIFICACIÓN]
- Disable kernel support of some filesystems

[+] Dispositivos USB

- Checking usb-storage driver (modprobe config) [NO DESHABILITADO]
- Checking USB devices authorization [HABILITADO]
- Checking USBGuard [NO ENCONTRADO]

[+] Almacenamiento

- Checking firewire ohci driver (modprobe config) [DESHABILITADO]

[+] NFS

- Check running NFS daemon [NO ENCONTRADO]

[+] Servicios de nombres

- Checking search domains [ENCONTRADO]
- Checking /etc/resolv.conf options [ENCONTRADO]
- Searching DNS domain name [DESCONOCIDO]
- Checking /etc/hosts
- Duplicate entries in hosts file [NINGUNO]
- Presence of configured hostname in /etc/hosts [ENCONTRADO]
- Hostname mapped to localhost [NO ENCONTRADO]
- Localhost mapping to IP address [OK]

[+] Puertos y paquetes

- Searching package managers
- Searching dpkg package manager [ENCONTRADO]
- Querying package manager
- Query unpurged packages [NINGUNO]
- Checking security repository in sources.list.d directory [OK]
- Checking upgradeable packages [OMITIDO]
- Checking package audit tool [NINGUNO]
- Toolkit for automatic upgrades (unattended-upgrade) [ENCONTRADO]

[+] Conectividad

- Checking IPv6 configuration [HABILITADO]
Configuration method [AUTO]
IPv6 only [NO]
- Checking configured nameservers
- Testing nameservers
Nameserver: 127.0.0.53 [OK]

- DNSSEC supported (systemd-resolved) [DESCONOCIDO]
 - Getting listening ports (TCP/UDP) [HECHO]
 - Checking promiscuous interfaces [OK]
 - Checking status DHCP client [NOT ACTIVE]
 - Checking for ARP monitoring software [NO ENCONTRADO]
 - Uncommon network protocols [0]
[+] Impresoras y spools

 - Checking cups daemon [CORRIENDO]
 - Checking CUPS configuration file [OK]
- File permissions [PELIGRO]
 - Checking CUPS addresses/sockets [ENCONTRADO]
 - Checking lp daemon [NO ESTÁ CORRIENDO]
[+] Software: correo electrónico y mensajería

[+] Software: firewalls

 - Checking iptables kernel module [ENCONTRADO]
 - Checking host based firewall [ACTIVO]
[+] Software: servidor web

 - Checking Apache [NO ENCONTRADO]
 - Checking nginx [NO ENCONTRADO]
[+] Soporte SSH

 - Checking running SSH daemon [NO ENCONTRADO]
[+] Soporte SNMP

 - Checking running SNMP daemon [NO ENCONTRADO]
[+] Bases de datos

No database engines found
[+] Servicios LDAP

 - Checking OpenLDAP instance [NO ENCONTRADO]
[+] PHP

 - Checking PHP [NO ENCONTRADO]
[+] Soporte Squid

 - Checking running Squid daemon [NO ENCONTRADO]
[+] Logging y ficheros

 - Checking for a running log daemon [OK]
- Checking Syslog-NG status [NO ENCONTRADO]
- Checking systemd journal status [ENCONTRADO]
- Checking Metalog status [NO ENCONTRADO]
- Checking RSyslog status [ENCONTRADO]
- Checking RFC 3195 daemon status [NO ENCONTRADO]
- Checking minilogd instances [NO ENCONTRADO]
- Checking wazuh-agent daemon status [NO ENCONTRADO]
 - Checking logrotate presence [OK]

- Checking remote logging [NO HABILITADO]
- Checking log directories (static list) [HECHO]
- Checking open log files [HECHO]
- Checking deleted files in use [ARCHIVOS ENCONTRADOS]

[+] Servicios inseguros

- Installed inetd package [NO ENCONTRADO]
- 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 [NO ENCONTRADO]
- Checking NIS client installation [OK]
- Checking NIS server installation [OK]
- Checking TFTP client installation [OK]
- Checking TFTP server installation [OK]

[+] Banners e identificación

- /etc/issue [ENCONTRADO]
- /etc/issue contents [DÉBIL]
- /etc/issue.net [ENCONTRADO]
- /etc/issue.net contents [DÉBIL]

[+] Tareas programadas

- Checking crontab and cronjob files [HECHO]

[+] Contabilidad

- Checking accounting information [NO ENCONTRADO]
- Checking sysstat accounting data [DESHABILITADO]
- Checking auditd [NO ENCONTRADO]

[+] Tiempo y sincronización

- NTP daemon found: systemd (timesyncd) [ENCONTRADO]
- Checking for a running NTP daemon or client [OK]
- Last time synchronization [426s]

[+] Criptografía

- Checking for expired SSL certificates [0/151] [NINGUNO]
- Kernel entropy is sufficient [SÍ]
- HW RNG & rngd [NO]
- SW prng [NO]
- MOR variable not found [DÉBIL]

[+] Virtualización

[+] Contenedores

[+] Frameworks de seguridad

- Checking presence AppArmor [ENCONTRADO]
- Checking AppArmor status [DESCONOCIDO]
- Checking presence SELinux [NO ENCONTRADO]

 - Checking presence TOMOYO Linux [NO ENCONTRADO]
 - Checking presence grsecurity [NO ENCONTRADO]
 - Checking for implemented MAC framework [NINGUNO]
[+] Software: integridad de ficheros

 - Checking file integrity tools
 - Checking presence integrity tool [NO ENCONTRADO]
[+] Software: Herramientas del sistema

 - Checking automation tooling
 - Automation tooling [NO ENCONTRADO]
 - Checking for IDS/IPS tooling [NINGUNO]
[+] Software: Malware

 - Malware software components [NO ENCONTRADO]
[+] Permisos de ficheros

 - Starting file permissions check
File: /boot/grub/grub.cfg [OK]
File: /etc/crontab [SUGERENCIA]
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]
Directory: /etc/cron.d [SUGERENCIA]
Directory: /etc/cron.daily [SUGERENCIA]
Directory: /etc/cron.hourly [SUGERENCIA]
Directory: /etc/cron.weekly [SUGERENCIA]
Directory: /etc/cron.monthly [SUGERENCIA]
[+] Directorios de inicio

 - Permissions of home directories [OK]
 - Ownership of home directories [OK]
 - Checking shell history files [OK]
[+] Bastionado del kernel

 - Comparing sysctl key pairs with scan profile
- dev.tty.ldisc_autoload (exp: 0) [DIFERENTE]
- fs.protected_fifos (exp: 2) [DIFERENTE]
- fs.protected_hardlinks (exp: 1) [OK]
- fs.protected_regular (exp: 2) [OK]
- fs.protected_symlinks (exp: 1) [OK]
- fs.suid_dumpable (exp: 0) [DIFERENTE]
- kernel.core_uses_pid (exp: 1) [DIFERENTE]
- kernel.ctrl-alt-del (exp: 0) [OK]
- kernel.dmesg_restrict (exp: 1) [OK]
- kernel.kptr_restrict (exp: 2) [DIFERENTE]
- kernel.modules_disabled (exp: 1) [DIFERENTE]

- kernel.perf_event_paranoid (exp: 2 3 4) [OK]
- kernel.randomize_va_space (exp: 2) [OK]
- kernel.sysrq (exp: 0) [DIFERENTE]
- kernel.unprivileged_bpf_disabled (exp: 1) [DIFERENTE]
- kernel.yama.ptrace_scope (exp: 1 2 3) [OK]
- net.ipv4.conf.all.accept_redirects (exp: 0) [DIFERENTE]
- 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) [DIFERENTE]
- 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) [DIFERENTE]
- net.ipv4.conf.all.send_redirects (exp: 0) [DIFERENTE]
- net.ipv4.conf.default.accept_redirects (exp: 0) [DIFERENTE]
- net.ipv4.conf.default.accept_source_route (exp: 0) [DIFERENTE]
- net.ipv4.conf.default.log_martians (exp: 1) [DIFERENTE]
- 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) [DIFERENTE]
- net.ipv6.conf.all.accept_source_route (exp: 0) [OK]
- net.ipv6.conf.default.accept_redirects (exp: 0) [DIFERENTE]
- net.ipv6.conf.default.accept_source_route (exp: 0) [OK]
[+] Bastionado

- Installed compiler(s) [NO ENCONTRADO]
- Installed malware scanner [NO ENCONTRADO]
- Non-native binary formats [ENCONTRADO]
[+] Pruebas personalizadas

 - Running custom tests... [NINGUNO]
[+] Plugins (fase 2)

 - Plugins (phase 2) [HECHO]
==========
 -[Lynis 3.1.3 Results]-
 Great, no warnings
 Suggestions (35):
 ---
 * Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
 https://cisofy.com/lynis/controls/BOOT-5122/
 * Consider hardening system services [BOOT-5264]
- Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service
 https://cisofy.com/lynis/controls/BOOT-5264/
 * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL#5820]
 https://cisofy.com/lynis/controls/KRNL-5820/
 * Run pwck manually and correct any errors in the password file [AUTH-9228]

https://cisofy.com/lynis/controls/AUTH-9228/
* Configure password hashing rounds in /etc/login.defs [AUTH-9230]
https://cisofy.com/lynis/controls/AUTH-9230/
* Configure minimum password age in /etc/login.defs [AUTH-9286]
https://cisofy.com/lynis/controls/AUTH-9286/
* Configure maximum password age in /etc/login.defs [AUTH-9286]
https://cisofy.com/lynis/controls/AUTH-9286/
* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
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]
https://cisofy.com/lynis/controls/FILE-6310/
* To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]
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]
https://cisofy.com/lynis/controls/FILE-6310/
* The JBD (Journal Block Device) driver is not loaded. [FILE-6398]
- Details : Since boot-time, you have not been using any filesystems with journaling. Alternatively, reason could be driver is blacklisted.
https://cisofy.com/lynis/controls/FILE-6398/
* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]
https://cisofy.com/lynis/controls/USB-1000/
* Check DNS configuration for the dns domain name [NAME-4028]
https://cisofy.com/lynis/controls/NAME-4028/
* Install debsums utility for the verification of packages with known good database. [PKGS-7370]
https://cisofy.com/lynis/controls/PKGS-7370/
* Install package apt-show-versions for patch management purposes [PKGS-7394]
https://cisofy.com/lynis/controls/PKGS-7394/
* Install a package audit tool to determine vulnerable packages [PKGS-7398]
https://cisofy.com/lynis/controls/PKGS-7398/
* Determine if protocol 'dccp' is really needed on this system [NETW-3200]
https://cisofy.com/lynis/controls/NETW-3200/
* Determine if protocol 'sctp' is really needed on this system [NETW-3200]
https://cisofy.com/lynis/controls/NETW-3200/
* Determine if protocol 'rds' is really needed on this system [NETW-3200]
https://cisofy.com/lynis/controls/NETW-3200/
* Determine if protocol 'tipc' is really needed on this system [NETW-3200]
https://cisofy.com/lynis/controls/NETW-3200/
* Access to CUPS configuration could be more strict. [PRNT-2307]
https://cisofy.com/lynis/controls/PRNT-2307/
* Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]
https://cisofy.com/lynis/controls/LOGG-2154/
* Check what deleted files are still in use and why. [LOGG-2190]
https://cisofy.com/lynis/controls/LOGG-2190/
* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
https://cisofy.com/lynis/controls/BANN-7126/
* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
https://cisofy.com/lynis/controls/BANN-7130/
* Enable process accounting [ACCT-9622]
https://cisofy.com/lynis/controls/ACCT-9622/

```
 * Enable sysstat to collect accounting (disabled) [ACCT-9626]
 https://cisofy.com/lynis/controls/ACCT-9626/
 * Enable auditd to collect audit information [ACCT-9628]
 https://cisofy.com/lynis/controls/ACCT-9628/
 * Check output of aa-status [MACF-6208]
- Details : /sys/kernel/security/apparmor/profiles
- Solution : Run aa-status
 https://cisofy.com/lynis/controls/MACF-6208/
 * Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]
 https://cisofy.com/lynis/controls/FINT-4350/
 * Determine if automation tools are present for system management [TOOL-5002]
 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
 https://cisofy.com/lynis/controls/FILE-7524/
 * 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>)
 https://cisofy.com/lynis/controls/KRNL-6000/
 * 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
 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 /home/aaron/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 : 64 [############ ]
 Tests performed : 250
 Plugins enabled : 2
 Components:
 - Firewall [V]
 - Malware scanner [X]
 Scan mode:
 Normal [ ] Forensics [ ] Integration [ ] Pentest [V] (running non-privileged)
 Lynis modules:
 - Compliance status [?]
 - Security audit [V]
 - Vulnerability scan [V]
 Files:
 - Test and debug information : /home/aaron/lynis.log
 - Report data : /home/aaron/lynis-report.dat
================================================================================
 Pruebas omitidas, debido a que el modo no privilegiado está activo
BOOT-5108 - Check Syslinux as bootloader
BOOT-5109 - Check rEFInd as bootloader
```

BOOT-5116 - Check if system is booted in UEFI mode
BOOT-5140 - Check for ELILO boot loader presence
AUTH-9216 - Check group and shadow group files
AUTH-9229 - Check password hashing methods
AUTH-9252 - Check ownership and permissions for sudo configuration files
AUTH-9288 - Checking for expired passwords
FILE-6368 - Checking ACL support on root file system
PKGS-7390 - Check Ubuntu database consistency
PKGS-7392 - Check for Debian/Ubuntu security updates
FIRE-4508 - Check used policies of iptables chains
FIRE-4512 - Check iptables for empty ruleset
FIRE-4513 - Check iptables for unused rules
FIRE-4540 - Check for empty nftables configuration
FIRE-4586 - Check firewall logging
CRYP-7930 - Determine if system uses LUKS block device encryption
==

 Lynis 3.1.3
 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
/home/aaron/lynis/default.prf for all settings)
##
 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

 ##
 # #
 # NON-PRIVILEGED SCAN MODE #
 # #
 ##
 NOTES:
 ----
 * Some tests will be skipped (as they require root permissions)
 * Some tests might fail silently or give different results
 - Detecting OS... [DONE]
 - Checking profiles... [DONE]
 - Detecting language and localization [es]
Translation file (db/languages/es) needs an update [OUTDATED]
==
Help other users and translate the missing lines:
1) Go to: https://github.com/CISOfy/lynis/edit/master/db/languages/es
2) Translate (some of) the lines starting with a hash (#) and remove the leading hash

3) Commit the changes
Thank you!
Note: no lines with a hash? Look if the file recently has been changed by another translator.
==

 Program version: 3.1.3
 Operating system: Linux
 Operating system name: Ubuntu
 Operating system version: 24.04
 Kernel version: 6.8.0
 Hardware platform: x86_64
 Hostname: aaron-VirtualBox

 Profiles: /home/aaron/lynis/default.prf
 Log file: /home/aaron/lynis.log
 Report file: /home/aaron/lynis-report.dat
 Report version: 1.0
 Plugin directory: ./plugins

 Auditor: [Not Specified]
 Language: es
 Test category: all
 Test group: all

 - Program update status... [SIN ACTUALIZACIÓN]
[+] Herramientas del sistema

 - Scanning available tools...
 - Checking system binaries...
[+] Plugins (fase 1)

 Nota: los plugins contienen pruebas más extensivas y toman más tiempo
 - Plugin: pam
[..]
 - Plugin: systemd
[.....]
[+] Arranque y servicios

 - Service Manager [systemd]
 - Checking presence GRUB2 [ENCONTRADO]
- Checking for password protection [NINGUNO]
 - Check running services (systemctl) [HECHO]
 Result: found 29 running services
 - Check enabled services at boot (systemctl) [HECHO]
 Result: found 55 enabled services
 - Check startup files (permissions) [OK]
 - Running 'systemd-analyze security'
 - ModemManager.service: [MEDIO]
 - NetworkManager.service: [EXPUESTO]
 - accounts-daemon.service: [MEDIO]
 - alsa-state.service: [INSEGURO]
 - anacron.service: [INSEGURO]

- avahi-daemon.service: [INSEGURO]
- colord.service: [PROTEGIDO]
- cron.service: [INSEGURO]
- cups-browsed.service: [INSEGURO]
- cups.service: [INSEGURO]
- dbus.service: [INSEGURO]
- dmesg.service: [INSEGURO]
- emergency.service: [INSEGURO]
- gdm.service: [INSEGURO]
- getty@tty1.service: [INSEGURO]
- gnome-remote-desktop.service: [INSEGURO]
- kerneloops.service: [INSEGURO]
- networkd-dispatcher.service: [INSEGURO]
- plymouth-start.service: [INSEGURO]
- polkit.service: [PROTEGIDO]
- power-profiles-daemon.service: [MEDIO]
- rc-local.service: [INSEGURO]
- rescue.service: [INSEGURO]
- rsyslog.service: [MEDIO]
- rtkit-daemon.service: [MEDIO]
- snapd.service: [INSEGURO]
- sssd-autofs.service: [INSEGURO]
- sssd-nss.service: [INSEGURO]
- sssd-pac.service: [INSEGURO]
- sssd-pam.service: [INSEGURO]
- sssd-ssh.service: [INSEGURO]
- sssd-sudo.service: [INSEGURO]
- sssd.service: [EXPUESTO]
- switcheroo-control.service: [EXPUESTO]
- systemd-ask-password-console.service: [INSEGURO]
- systemd-ask-password-plymouth.service: [INSEGURO]
- systemd-ask-password-wall.service: [INSEGURO]
- systemd-bsod.service: [INSEGURO]
- systemd-fsckd.service: [INSEGURO]
- systemd-initctl.service: [INSEGURO]
- systemd-journald.service: [PROTEGIDO]
- systemd-logind.service: [PROTEGIDO]
- systemd-networkd.service: [PROTEGIDO]
- systemd-oomd.service: [PROTEGIDO]
- systemd-resolved.service: [PROTEGIDO]
- systemd-rfkill.service: [INSEGURO]
- systemd-timesyncd.service: [PROTEGIDO]
- systemd-udevd.service: [MEDIO]
- thermald.service: [INSEGURO]
- tpm-udev.service: [INSEGURO]
- ubuntu-advantage.service: [INSEGURO]
- udisks2.service: [INSEGURO]
- unattended-upgrades.service: [INSEGURO]
- upower.service: [PROTEGIDO]
- user@1000.service: [INSEGURO]
- uuidd.service: [MEDIO]
- whoopsie.service: [INSEGURO]

 - wpa_supplicant.service: [INSEGURO]
[+] Kernel

 - Checking default runlevel [runlevel 5]
 - Checking CPU support (NX/PAE)
CPU support: PAE and/or NoeXecute supported [ENCONTRADO]
 - Checking kernel version and release [HECHO]
 - Checking kernel type [HECHO]
 - Checking loaded kernel modules [HECHO]
 Found 68 active modules
 - Checking Linux kernel configuration file [ENCONTRADO]
 - Checking default I/O kernel scheduler [NO ENCONTRADO]
 - Checking for available kernel update [OK]
 - Checking core dumps configuration
- configuration in systemd conf files [POR DEFECTO]
- configuration in /etc/profile [POR DEFECTO]
- 'hard' configuration in /etc/security/limits.conf [POR DEFECTO]
- 'soft' configuration in /etc/security/limits.conf [POR DEFECTO]
- Checking setuid core dumps configuration [PROTEGIDO]
 - Check if reboot is needed [NO]
[+] Memoria y procesos

 - Checking /proc/meminfo [ENCONTRADO]
 - Searching for dead/zombie processes [NO ENCONTRADO]
 - Searching for IO waiting processes [NO ENCONTRADO]
 - Search prelink tooling [NO ENCONTRADO]
[+] Usuarios, grupos y autenticación

 - Administrator accounts [OK]
 - Unique UIDs [OK]
 - Unique group IDs [OK]
 - Unique group names [OK]
 - Password file consistency [SUGERENCIA]
 - Checking password hashing rounds [DESHABILITADO]
 - Query system users (non daemons) [HECHO]
 - NIS+ authentication support [NO HABILITADO]
 - NIS authentication support [NO HABILITADO]
 - Sudoers file(s) [ENCONTRADO]
 - PAM password strength tools [OK]
 - PAM configuration files (pam.conf) [ENCONTRADO]
 - PAM configuration files (pam.d) [ENCONTRADO]
 - PAM modules [ENCONTRADO]
 - LDAP module in PAM [NO ENCONTRADO]
 - Accounts without expire date [OK]
 - Accounts without password [OK]
 - Locked accounts [OK]
 - Checking user password aging (minimum) [DESHABILITADO]
 - User password aging (maximum) [DESHABILITADO]
 - Checking Linux single user mode authentication [OK]
 - Determining default umask
- umask (/etc/profile) [NO ENCONTRADO]
- umask (/etc/login.defs) [SUGERENCIA]

 - LDAP authentication support [NO HABILITADO]
 - Logging failed login attempts [HABILITADO]
[+] Kerberos

 - Check for Kerberos KDC and principals [NO ENCONTRADO]
[+] Shells

 - Checking shells from /etc/shells
Result: found 7 shells (valid shells: 7).
- Session timeout settings/tools [NINGUNO]
 - Checking default umask values
- Checking default umask in /etc/bash.bashrc [NINGUNO]
- Checking default umask in /etc/profile [NINGUNO]
[+] Sistemas de ficheros

 - Checking mount points
- Checking /home mount point [SUGERENCIA]
- Checking /tmp mount point [SUGERENCIA]
- Checking /var mount point [SUGERENCIA]
 - Query swap partitions (fstab) [OK]
 - Testing swap partitions [OK]
 - Testing /proc mount (hidepid) [SUGERENCIA]
 - Checking for old files in /tmp [OK]
 - Checking /tmp sticky bit [OK]
 - Checking /var/tmp sticky bit [OK]
 - Mount options of / [OK]
 - Mount options of /dev [PARCIALMENTE BASTIONADO]
 - Mount options of /dev/shm [PARCIALMENTE BASTIONADO]
 - Mount options of /run [BASTIONADO]
 - Total without nodev:6 noexec:21 nosuid:15 ro or noexec (W^X): 10 of total 37
 - JBD driver is not loaded [NECESITA VERIFICACIÓN]
 - Disable kernel support of some filesystems
[+] Dispositivos USB

 - Checking usb-storage driver (modprobe config) [NO DESHABILITADO]
 - Checking USB devices authorization [HABILITADO]
 - Checking USBGuard [NO ENCONTRADO]
[+] Almacenamiento

 - Checking firewire ohci driver (modprobe config) [DESHABILITADO]
[+] NFS

 - Check running NFS daemon [NO ENCONTRADO]
[+] Servicios de nombres

 - Checking search domains [ENCONTRADO]
 - Checking /etc/resolv.conf options [ENCONTRADO]
 - Searching DNS domain name [DESCONOCIDO]
 - Checking /etc/hosts
- Duplicate entries in hosts file [NINGUNO]
- Presence of configured hostname in /etc/hosts [ENCONTRADO]
- Hostname mapped to localhost [NO ENCONTRADO]

- Localhost mapping to IP address [OK]
[+] Puertos y paquetes

 - Searching package managers
- Searching dpkg package manager [ENCONTRADO]
 - Querying package manager
- Query unpurged packages [NINGUNO]
 - Checking security repository in sources.list.d directory [OK]
 - Checking upgradeable packages [OMITIDO]
 - Checking package audit tool [NINGUNO]
 - Toolkit for automatic upgrades (unattended-upgrade) [ENCONTRADO]
[+] Conectividad

 - Checking IPv6 configuration [HABILITADO]
 Configuration method [AUTO]
 IPv6 only [NO]
 - Checking configured nameservers
- Testing nameservers
 Nameserver: 127.0.0.53 [OK]
- DNSSEC supported (systemd-resolved) [DESCONOCIDO]
 - Getting listening ports (TCP/UDP) [HECHO]
 - Checking promiscuous interfaces [OK]
 - Checking status DHCP client [NOT ACTIVE]
 - Checking for ARP monitoring software [NO ENCONTRADO]
 - Uncommon network protocols [0]
[+] Impresoras y spools

 - Checking cups daemon [CORRIENDO]
 - Checking CUPS configuration file [OK]
- File permissions [PELIGRO]
 - Checking CUPS addresses/sockets [ENCONTRADO]
 - Checking lp daemon [NO ESTÁ CORRIENDO]
[+] Software: correo electrónico y mensajería

[+] Software: firewalls

 - Checking iptables kernel module [ENCONTRADO]
 - Checking host based firewall [ACTIVO]
[+] Software: servidor web

 - Checking Apache [NO ENCONTRADO]
 - Checking nginx [NO ENCONTRADO]
[+] Soporte SSH

 - Checking running SSH daemon [NO ENCONTRADO]
[+] Soporte SNMP

 - Checking running SNMP daemon [NO ENCONTRADO]
[+] Bases de datos

No database engines found
[+] Servicios LDAP

 - Checking OpenLDAP instance [NO ENCONTRADO]
[+] PHP

 - Checking PHP [NO ENCONTRADO]
[+] Soporte Squid

 - Checking running Squid daemon [NO ENCONTRADO]
[+] Logging y ficheros

 - Checking for a running log daemon [OK]
- Checking Syslog-NG status [NO ENCONTRADO]
- Checking systemd journal status [ENCONTRADO]
- Checking Metalog status [NO ENCONTRADO]
- Checking RSyslog status [ENCONTRADO]
- Checking RFC 3195 daemon status [NO ENCONTRADO]
- Checking minilogd instances [NO ENCONTRADO]
- Checking wazuh-agent daemon status [NO ENCONTRADO]
 - Checking logrotate presence [OK]
 - Checking remote logging [NO HABILITADO]
 - Checking log directories (static list) [HECHO]
 - Checking open log files [HECHO]
 - Checking deleted files in use [ARCHIVOS ENCONTRADOS]
[+] Servicios inseguros

 - Installed inetd package [NO ENCONTRADO]
 - 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 [NO ENCONTRADO]
 - Checking NIS client installation [OK]
 - Checking NIS server installation [OK]
 - Checking TFTP client installation [OK]
 - Checking TFTP server installation [OK]
[+] Banners e identificación

 - /etc/issue [ENCONTRADO]
- /etc/issue contents [DÉBIL]
 - /etc/issue.net [ENCONTRADO]
- /etc/issue.net contents [DÉBIL]
[+] Tareas programadas

 - Checking crontab and cronjob files [HECHO]
[+] Contabilidad

 - Checking accounting information [NO ENCONTRADO]
 - Checking sysstat accounting data [DESHABILITADO]
 - Checking auditd [NO ENCONTRADO]
[+] Tiempo y sincronización

- NTP daemon found: systemd (timesyncd) [ENCONTRADO]
- Checking for a running NTP daemon or client [OK]
- Last time synchronization [426s]

[+] Criptografía

- Checking for expired SSL certificates [0/151] [NINGUNO]
- Kernel entropy is sufficient [SÍ]
- HW RNG & rngd [NO]
- SW prng [NO]
- MOR variable not found [DÉBIL]

[+] Virtualización

[+] Contenedores

[+] Frameworks de seguridad

- Checking presence AppArmor [ENCONTRADO]
- Checking AppArmor status [DESCONOCIDO]
- Checking presence SELinux [NO ENCONTRADO]
- Checking presence TOMOYO Linux [NO ENCONTRADO]
- Checking presence grsecurity [NO ENCONTRADO]
- Checking for implemented MAC framework [NINGUNO]

[+] Software: integridad de ficheros

- Checking file integrity tools
- Checking presence integrity tool [NO ENCONTRADO]

[+] Software: Herramientas del sistema

- Checking automation tooling
- Automation tooling [NO ENCONTRADO]
- Checking for IDS/IPS tooling [NINGUNO]

[+] Software: Malware

- Malware software components [NO ENCONTRADO]

[+] Permisos de ficheros

- Starting file permissions check

File: /boot/grub/grub.cfg [OK]
File: /etc/crontab [SUGERENCIA]
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]
Directory: /etc/cron.d [SUGERENCIA]
Directory: /etc/cron.daily [SUGERENCIA]
Directory: /etc/cron.hourly [SUGERENCIA]
Directory: /etc/cron.weekly [SUGERENCIA]
Directory: /etc/cron.monthly [SUGERENCIA]

[+] Directorios de inicio

 - Permissions of home directories [OK]
 - Ownership of home directories [OK]
 - Checking shell history files [OK]
[+] Bastionado del kernel

 - Comparing sysctl key pairs with scan profile
- dev.tty.ldisc_autoload (exp: 0) [DIFERENTE]
- fs.protected_fifos (exp: 2) [DIFERENTE]
- fs.protected_hardlinks (exp: 1) [OK]
- fs.protected_regular (exp: 2) [OK]
- fs.protected_symlinks (exp: 1) [OK]
- fs.suid_dumpable (exp: 0) [DIFERENTE]
- kernel.core_uses_pid (exp: 1) [DIFERENTE]
- kernel.ctrl-alt-del (exp: 0) [OK]
- kernel.dmesg_restrict (exp: 1) [OK]
- kernel.kptr_restrict (exp: 2) [DIFERENTE]
- kernel.modules_disabled (exp: 1) [DIFERENTE]
- kernel.perf_event_paranoid (exp: 2 3 4) [OK]
- kernel.randomize_va_space (exp: 2) [OK]
- kernel.sysrq (exp: 0) [DIFERENTE]
- kernel.unprivileged_bpf_disabled (exp: 1) [DIFERENTE]
- kernel.yama.ptrace_scope (exp: 1 2 3) [OK]
- net.ipv4.conf.all.accept_redirects (exp: 0) [DIFERENTE]
- 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) [DIFERENTE]
- 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) [DIFERENTE]
- net.ipv4.conf.all.send_redirects (exp: 0) [DIFERENTE]
- net.ipv4.conf.default.accept_redirects (exp: 0) [DIFERENTE]
- net.ipv4.conf.default.accept_source_route (exp: 0) [DIFERENTE]
- net.ipv4.conf.default.log_martians (exp: 1) [DIFERENTE]
- 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) [DIFERENTE]
- net.ipv6.conf.all.accept_source_route (exp: 0) [OK]
- net.ipv6.conf.default.accept_redirects (exp: 0) [DIFERENTE]
- net.ipv6.conf.default.accept_source_route (exp: 0) [OK]
[+] Bastionado

- Installed compiler(s) [NO ENCONTRADO]
- Installed malware scanner [NO ENCONTRADO]
- Non-native binary formats [ENCONTRADO]
[+] Pruebas personalizadas

 - Running custom tests... [NINGUNO]

[+] Plugins (fase 2)

 - Plugins (phase 2) [HECHO]
==========
 -[Lynis 3.1.3 Results]-
 Great, no warnings
 Suggestions (35):
 ---
 * Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
 https://cisofy.com/lynis/controls/BOOT-5122/
 * Consider hardening system services [BOOT-5264]
- Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service
 https://cisofy.com/lynis/controls/BOOT-5264/
 * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL#5820]
 https://cisofy.com/lynis/controls/KRNL-5820/
 * Run pwck manually and correct any errors in the password file [AUTH-9228]
 https://cisofy.com/lynis/controls/AUTH-9228/
 * Configure password hashing rounds in /etc/login.defs [AUTH-9230]
 https://cisofy.com/lynis/controls/AUTH-9230/
 * Configure minimum password age in /etc/login.defs [AUTH-9286]
 https://cisofy.com/lynis/controls/AUTH-9286/
 * Configure maximum password age in /etc/login.defs [AUTH-9286]
 https://cisofy.com/lynis/controls/AUTH-9286/
 * Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
 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]
 https://cisofy.com/lynis/controls/FILE-6310/
 * To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]
 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]
 https://cisofy.com/lynis/controls/FILE-6310/
 * The JBD (Journal Block Device) driver is not loaded. [FILE-6398]
- Details : Since boot-time, you have not been using any filesystems with journaling. Alternatively, reason could be driver is blacklisted.
 https://cisofy.com/lynis/controls/FILE-6398/
 * Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]
 https://cisofy.com/lynis/controls/USB-1000/
 * Check DNS configuration for the dns domain name [NAME-4028]
 https://cisofy.com/lynis/controls/NAME-4028/
 * Install debsums utility for the verification of packages with known good database. [PKGS-7370]
 https://cisofy.com/lynis/controls/PKGS-7370/
 * Install package apt-show-versions for patch management purposes [PKGS-7394]
 https://cisofy.com/lynis/controls/PKGS-7394/
 * Install a package audit tool to determine vulnerable packages [PKGS-7398]
 https://cisofy.com/lynis/controls/PKGS-7398/
 * Determine if protocol 'dccp' is really needed on this system [NETW-3200]
 https://cisofy.com/lynis/controls/NETW-3200/

```
 * Determine if protocol 'sctp' is really needed on this system [NETW-3200]
 https://cisofy.com/lynis/controls/NETW-3200/
 * Determine if protocol 'rds' is really needed on this system [NETW-3200]
 https://cisofy.com/lynis/controls/NETW-3200/
 * Determine if protocol 'tipc' is really needed on this system [NETW-3200]
 https://cisofy.com/lynis/controls/NETW-3200/
 * Access to CUPS configuration could be more strict. [PRNT-2307]
 https://cisofy.com/lynis/controls/PRNT-2307/
 * Enable logging to an external logging host for archiving purposes and additional protection
[LOGG-2154]
 https://cisofy.com/lynis/controls/LOGG-2154/
 * Check what deleted files are still in use and why. [LOGG-2190]
 https://cisofy.com/lynis/controls/LOGG-2190/
 * Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
 https://cisofy.com/lynis/controls/BANN-7126/
 * Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
 https://cisofy.com/lynis/controls/BANN-7130/
 * Enable process accounting [ACCT-9622]
 https://cisofy.com/lynis/controls/ACCT-9622/
 * Enable sysstat to collect accounting (disabled) [ACCT-9626]
 https://cisofy.com/lynis/controls/ACCT-9626/
 * Enable auditd to collect audit information [ACCT-9628]
 https://cisofy.com/lynis/controls/ACCT-9628/
 * Check output of aa-status [MACF-6208]
- Details : /sys/kernel/security/apparmor/profiles
- Solution : Run aa-status
 https://cisofy.com/lynis/controls/MACF-6208/
 * Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]
 https://cisofy.com/lynis/controls/FINT-4350/
 * Determine if automation tools are present for system management [TOOL-5002]
 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
 https://cisofy.com/lynis/controls/FILE-7524/
 * 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>)
 https://cisofy.com/lynis/controls/KRNL-6000/
 * 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
 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 /home/aaron/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 : 64 [############ ]
```

Tests performed : 250
Plugins enabled : 2
Components:
- Firewall [V]
- Malware scanner [X]
Scan mode:
Normal [ ] Forensics [ ] Integration [ ] Pentest [V] (running non-privileged)
Lynis modules:
- Compliance status [?]
- Security audit [V]
- Vulnerability scan [V]
Files:
- Test and debug information : /home/aaron/lynis.log
- Report data : /home/aaron/lynis-report.dat
==

Pruebas omitidas, debido a que el modo no privilegiado está activo
BOOT-5108 - Check Syslinux as bootloader
BOOT-5109 - Check rEFInd as bootloader
BOOT-5116 - Check if system is booted in UEFI mode
BOOT-5140 - Check for ELILO boot loader presence
AUTH-9216 - Check group and shadow group files
AUTH-9229 - Check password hashing methods
AUTH-9252 - Check ownership and permissions for sudo configuration files
AUTH-9288 - Checking for expired passwords
FILE-6368 - Checking ACL support on root file system
PKGS-7390 - Check Ubuntu database consistency
PKGS-7392 - Check for Debian/Ubuntu security updates
FIRE-4508 - Check used policies of iptables chains
FIRE-4512 - Check iptables for empty ruleset
FIRE-4513 - Check iptables for unused rules
FIRE-4540 - Check for empty nftables configuration
FIRE-4586 - Check firewall logging
CRYP-7930 - Determine if system uses LUKS block device encryption
==

Lynis 3.1.3
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
/home/aaron/lynis/default.prf for all settings)