Trabajo Práctico Integrador: Introducción a la Ciberseguridad

Capturas/ Respuestas PARTE-1

En este apartado se van a encontrar todas las salidas de escaneo que fueron realizadas en la parte-1.

Índice

Salida 1: Escaneo inicial:

```
oot@linux-target:/opt/lynis# ./lynis audit system

[ Lynis 3.1.6 ]

################################################################################
  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.

  2007-2025, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                     [ DONE ]
  - Checking profiles...                                [ DONE ]

  ---------------------------------------------------
  Program version:           3.1.6
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  22.04
  End-of-life:               NO
  Kernel version:            6.12.38+kali
  Hardware platform:         x86_64
  Hostname:                  linux-target
  ---------------------------------------------------
```

```
  Profiles:               /opt/lynis/default.prf
  Log file:               /var/log/lynis.log
  Report file:             /var/log/lynis-report.dat
  Report version:           1.0
  Plugin directory:         ./plugins
  ---------------------------------------------------
  Auditor:                [Not Specified]
  Language:                 en
  Test category:            all
  Test group:               all
  ---------------------------------------------------
  - Program update status...                      [ SKIPPED ]

[+] 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: pam
    [..]
  - Plugin: systemd
    [.
  [WARNING]: Test PLGN-0010 had a long execution: 18.395515 seconds

System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
.....System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
..]

[+] Boot and services
------------------------------------
  - Service Manager                               [ upstart ]
  - Checking UEFI boot                             [ DISABLED ]
    - Boot loader                                [ NONE FOUND ]
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
  - Check running services (systemctl)                [ DONE ]
        Result: found 0 running services
  - Check enabled services at boot (systemctl)          [ DONE ]
        Result: found 11 enabled services
  - Check startup files (permissions)                 [ OK ]
  - Running 'systemd-analyze security'
      Unit name (exposure value) and predicate
      ------------------------------
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down

[+] 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 Linux kernel configuration file           [ NOT FOUND ]
/usr/bin/grep: /etc/kernel-img.conf: No such file or directory
  - Checking core dumps configuration
    - configuration in /etc/profile                    [ DEFAULT ]
    - 'hard' configuration in /etc/security/limits.conf  [ ENABLED ]
    - 'soft' configuration in /etc/security/limits.conf  [ ENABLED ]
    - Checking setuid core dumps configuration         [ DISABLED ]
  - Check if reboot is needed                          [ UNKNOWN ]

[+] 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                             [ WARNING ]
  - Unique UIDs                                        [ WARNING ]
  - 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                    [ WARNING ]
    - Permissions for: /etc/sudoers.d/README           [ 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                                    [ FOUND ]
  - 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                      [ ENABLED ]
```

```
[+] Kerberos
------------------------------------
  - Check for Kerberos KDC and principals                    [ NOT FOUND ]

[+] Shells
------------------------------------
  - Checking shells from /etc/shells
    Result: found 8 shells (valid shells: 8).
    - Session timeout settings/tools                         [ NONE ]
  - Checking default umask values
    - Checking default umask in /etc/bash.bashrc             [ WEAK ]
    - Checking default umask in /etc/profile                 [ NONE ]

[+] File systems
------------------------------------
  - Checking mount points
    - Checking /home mount point                             [ SUGGESTION ]
    - Checking /tmp mount point                              [ SUGGESTION ]
    - Checking /var mount point                              [ SUGGESTION ]
  - Query swap partitions (fstab)                            [ NONE ]
  - 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 /dev                                    [ PARTIALLY HARDENED ]
  - Mount options of /dev/shm                                [ HARDENED ]
  - Total without nodev:7 noexec:6 nosuid:5 ro or noexec (W^X): 6 of total 12

[+] 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
------------------------------------
  - Check running NFS daemon                                 [ NOT FOUND ]

[+] Name services
------------------------------------
  - Checking search domains                                  [ FOUND ]
  - Checking /etc/resolv.conf options                        [ FOUND ]
  - Searching DNS domain name                                [ UNKNOWN ]
  - 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 dpkg package manager                       [ FOUND ]
      - Querying package manager
    - Query unpurged packages                            [ NONE ]
  - Checking security repository in sources.list file      [ OK ]
  - Checking APT package database                          [ OK ]
  - Checking vulnerable packages (apt-get only)              [ DONE ]

  [WARNING]: Test PKGS-7392 had a long execution: 13.793921 seconds

  - Checking upgradeable packages                        [ SKIPPED ]
  - Checking package audit tool                        [ INSTALLED ]
    Found: apt-get

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

  Exception found!

  Function/test:  [PKGS-7410]
  Message:        Could not find any kernel packages via package manager

  Help improving the Lynis community with your feedback!

  Steps:
  - Ensure you are running the latest version (./lynis update check)
  - If so, create a GitHub issue at https://github.com/CISOfy/lynis
  - Include relevant parts of the log file or configuration file

  Thanks!

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

  - Toolkit for automatic upgrades                       [ NOT FOUND ]

[+] Networking
------------------------------------
  - Checking IPv6 configuration                          [ ENABLED ]
      Configuration method                             [ AUTO ]
      IPv6 only                                  [ NO ]
  - Checking configured nameservers
    - Testing nameservers
      Nameserver: 127.0.0.11                           [ SKIPPED ]
    - Minimal of 2 responsive nameservers                [ SKIPPED ]
    - DNSSEC supported (systemd-resolved)                  [ UNKNOWN ]
  - Checking default gateway                           [ DONE ]

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

  Exception found!
```

```
  Function/test:  [NETW-3004:1]
  Message:        No interfaces found on this system (OS=Linux)

  Help improving the Lynis community with your feedback!

  Steps:
  - Ensure you are running the latest version (./lynis update check)
  - If so, create a GitHub issue at https://github.com/CISOfy/lynis
  - Include relevant parts of the log file or configuration file

  Thanks!

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

  - Getting listening ports (TCP/UDP)                    [ DONE ]
  - Checking promiscuous interfaces                      [ UNKNOWN ]
  - 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
------------------------------------
  - Postfix status                                       [ RUNNING ]
    - Postfix configuration                              [ FOUND ]
      - Postfix configuration errors                     [ WARNING ]

[+] Software: firewalls
------------------------------------
  - Checking iptables support                            [ 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                                      [ NOT FOUND ]
  - Checking nginx                                       [ NOT FOUND ]

[+] SSH Support
------------------------------------
  - Checking running SSH daemon                          [ FOUND ]
    - Searching SSH configuration                        [ FOUND ]
    - OpenSSH option: AllowTcpForwarding                 [ SUGGESTION ]
    - OpenSSH option: ClientAliveCountMax                [ SUGGESTION ]
    - OpenSSH option: ClientAliveInterval                [ OK ]
```

```
   - OpenSSH option: FingerprintHash                [ OK ]
   - OpenSSH option: GatewayPorts                   [ SUGGESTION ]
   - OpenSSH option: IgnoreRhosts                   [ OK ]
   - OpenSSH option: LoginGraceTime                 [ OK ]
   - OpenSSH option: LogLevel                       [ SUGGESTION ]
   - OpenSSH option: MaxAuthTries                   [ SUGGESTION ]
   - OpenSSH option: MaxSessions                    [ SUGGESTION ]
   - OpenSSH option: PermitRootLogin                [ SUGGESTION ]
   - OpenSSH option: PermitUserEnvironment          [ SUGGESTION ]
   - OpenSSH option: PermitTunnel                   [ SUGGESTION ]
   - OpenSSH option: Port                           [ SUGGESTION ]
   - OpenSSH option: PrintLastLog                   [ OK ]
   - OpenSSH option: StrictModes                    [ SUGGESTION ]
   - OpenSSH option: TCPKeepAlive                   [ SUGGESTION ]
   - OpenSSH option: UseDNS                         [ OK ]
   - OpenSSH option: X11Forwarding                  [ SUGGESTION ]
   - OpenSSH option: AllowAgentForwarding           [ SUGGESTION ]
   - OpenSSH option: AllowUsers                     [ NOT FOUND ]
   - OpenSSH option: AllowGroups                    [ NOT FOUND ]

[+] SNMP Support
------------------------------------
  - Checking running SNMP daemon                    [ NOT FOUND ]

[+] Databases
------------------------------------
  - Redis (server) status                           [ FOUND ]
    - Redis (requirepass configured)                [ NOT FOUND ]
    - Redis (rename of CONFIG command)              [ NOT FOUND ]
    - Redis (bind on localhost)                     [ NOT FOUND ]

[+] LDAP Services
------------------------------------
  - Checking OpenLDAP instance                      [ NOT FOUND ]

[+] PHP
------------------------------------
  - Checking PHP                                    [ NOT FOUND ]

[+] Squid Support
------------------------------------
  - Checking running Squid daemon                   [ NOT FOUND ]

[+] Logging and files
------------------------------------
  - Checking for a running log daemon               [ WARNING ]
    - Checking Syslog-NG status                     [ NOT FOUND ]
    - Checking systemd journal status               [ NOT FOUND ]
    - Checking Metalog status                       [ NOT FOUND ]
    - Checking RSyslog status                       [ NOT FOUND ]
    - Checking RFC 3195 daemon status               [ NOT FOUND ]
    - Checking klogd                                [ NOT FOUND ]
    - Checking minilogd instances                   [ NOT FOUND ]
    - Checking wazuh-agent daemon status            [ NOT FOUND ]
```

```
  - Checking logrotate presence                        [ OK ]
  - Checking log directories (static list)             [ DONE ]
  - Checking open log files                            [ SKIPPED ]

[+] Insecure services
---------------------------------
  - Installed inetd package                            [ NOT FOUND ]
    - Checking enabled inetd services                      [ SUGGESTION ]
  - Installed xinetd package                           [ FOUND ]
    - xinetd status                                    [ NOT ACTIVE ]
      - Enabled xinetd.d services                      [ NOT FOUND ]
  - Installed rsh client package                       [ OK ]
  - Installed rsh server package                       [ OK ]
  - Installed telnet client package                    [ OK ]
  - Installed telnet server package                    [ FOUND ]
  - Checking NIS client installation                   [ OK ]
  - Checking NIS server installation                   [ OK ]
  - Checking TFTP client installation                  [ OK ]
  - Checking TFTP server installation                  [ OK ]

[+] Banners and identification
---------------------------------
  - /etc/issue                                         [ FOUND ]
    - /etc/issue contents                                  [ WEAK ]
  - /etc/issue.net                                     [ FOUND ]
    - /etc/issue.net contents                              [ WEAK ]

[+] Scheduled tasks
---------------------------------
  - Checking crontab and cronjobs files                    [ WARNING ]

[+] Accounting
---------------------------------
  - Checking accounting information                        [ NOT FOUND ]
  - Checking sysstat accounting data                       [ NOT FOUND ]
  - Checking auditd                                    [ NOT FOUND ]

[+] Time and Synchronization
---------------------------------

[+] Cryptography
---------------------------------
  - Checking for expired SSL certificates [0/149]          [ NONE ]

  [WARNING]: Test CRYP-7902 had a long execution: 14.170752 seconds

  - Kernel entropy is sufficient                           [ YES ]
  - HW RNG & rngd                                      [ NO ]
  - SW prng                                            [ NO ]
  - MOR variable not found                                 [ WEAK ]

[+] Virtualization
---------------------------------
```

```
[+] Containers
------------------------------------

[+] Security frameworks
------------------------------------
  - Checking presence AppArmor                     [ NOT FOUND ]
  - 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
  - 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: /etc/crontab                             [ SUGGESTION ]
    File: /etc/group                               [ SUGGESTION ]
    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                              [ SUGGESTION ]
    File: /etc/passwd-                             [ SUGGESTION ]
    File: /etc/ssh/sshd_config                     [ SUGGESTION ]
    Directory: /root/.ssh                          [ 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
------------------------------------
  - Permissions of home directories                [ OK ]
  - Ownership of home directories                  [ WARNING ]
  - 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)                  [ DIFFERENT ]
    - kernel.sysrq (exp: 0)                               [ DIFFERENT ]
    - kernel.unprivileged_bpf_disabled (exp: 1)           [ DIFFERENT ]
    - kernel.yama.ptrace_scope (exp: 1 2 3)               [ DIFFERENT ]
    - net.ipv4.conf.all.accept_redirects (exp: 0)         [ OK ]
    - net.ipv4.conf.all.accept_source_route (exp: 0)      [ OK ]
    - net.ipv4.conf.all.bootp_relay (exp: 0)              [ OK ]
    - net.ipv4.conf.all.forwarding (exp: 0)               [ DIFFERENT ]
    - net.ipv4.conf.all.log_martians (exp: 1)             [ DIFFERENT ]
    - net.ipv4.conf.all.mc_forwarding (exp: 0)            [ OK ]
    - net.ipv4.conf.all.proxy_arp (exp: 0)                [ OK ]
    - net.ipv4.conf.all.rp_filter (exp: 1)                [ DIFFERENT ]
    - net.ipv4.conf.all.send_redirects (exp: 0)           [ 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)                               [ NOT FOUND ]
    - Installed malware scanner                           [ NOT FOUND ]
    - Non-native binary formats                           [ NOT FOUND ]

[+] Custom tests
------------------------------------
  - Running custom tests...                               [ NONE ]

[+] Plugins (phase 2)
------------------------------------
  - Plugins (phase 2)                                     [ DONE ]

================================================================================
```

```
  -[ Lynis 3.1.6 Results ]-

  Warnings (6):
  ----------------------------
  ! Multiple users with UID 0 found in passwd file [AUTH-9204]
      https://cisofy.com/lynis/controls/AUTH-9204/

  ! Multiple accounts found with same UID [AUTH-9208]
      https://cisofy.com/lynis/controls/AUTH-9208/

  ! iptables module(s) loaded, but no rules active [FIRE-4512]
      https://cisofy.com/lynis/controls/FIRE-4512/

  ! Redis configuration file /etc/redis/redis.conf is world readable and might leak sensitive
details [DBS-1882]
    - Details  : /etc/redis/redis.conf
    - Solution : Use chmod 640 to change file permissions
      https://cisofy.com/lynis/controls/DBS-1882/

  ! klogd is not running, which could lead to missing kernel messages in log files
[LOGG-2138]
      https://cisofy.com/lynis/controls/LOGG-2138/

  ! Found one or more cronjob files with incorrect file permissions (see log for details)
[SCHD-7704]
      https://cisofy.com/lynis/controls/SCHD-7704/

  Suggestions (58):
  ----------------------------
  * 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/

  * Determine why /vmlinuz or /boot/vmlinuz is missing on this Debian/Ubuntu system.
[KRNL-5788]
    - Details  : /vmlinuz or /boot/vmlinuz
    - Related resources
      * Website: https://cisofy.com/lynis/controls/KRNL-5788/

  * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file
[KRNL-5820]
    - Related resources
      * 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/
```

* 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/

* Look at the locked accounts and consider removing them [AUTH-9284]
- Related resources
* Website: https://cisofy.com/lynis/controls/AUTH-9284/

* 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 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 /tmp file system, place /tmp 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/

  * 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 DNS configuration for the dns domain name [NAME-4028]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/NAME-4028/

  * 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/

  * 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/

  * Found a configuration error in Postfix [MAIL-8817]
    - Details  : /etc/postfix/main.cf
    - Solution : run postconf > /dev/null
    - Related resources
      * Article: Postfix Hardening Guide for Security and Privacy:
https://linux-audit.com/postfix-hardening-guide-for-security-and-privacy/
      * Website: https://cisofy.com/lynis/controls/MAIL-8817/

  * Disable the 'VRFY' command [MAIL-8820:disable_vrfy_command]
```

```
    - Details  : disable_vrfy_command=no
    - Solution : run postconf -e disable_vrfy_command=yes to change the value
    - Related resources
      * Article: Postfix Hardening Guide for Security and Privacy:
https://linux-audit.com/postfix-hardening-guide-for-security-and-privacy/
      * Website: https://cisofy.com/lynis/controls/MAIL-8820/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowTcpForwarding (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : ClientAliveCountMax (set 3 to 2)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : GatewayPorts (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : LogLevel (set INFO to VERBOSE)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxAuthTries (set 6 to 3)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxSessions (set 10 to 2)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitRootLogin (set YES to
(FORCED-COMMANDS-ONLY|NO|PROHIBIT-PASSWORD|WITHOUT-PASSWORD))
    - Related resources
      * Article: OpenSSH security and hardening:
```

https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details : PermitUserEnvironment (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details : PermitTunnel (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details : Port (set 22 to)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details : StrictModes (set NO to YES)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details : TCPKeepAlive (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details : X11Forwarding (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details : AllowAgentForwarding (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Configure the 'requirepass' setting for Redis [DBS-1884]
    - Details : /etc/redis/redis.conf

- Solution : configure 'requirepass' setting in /etc/redis/redis.conf
- Related resources
  * Website: https://cisofy.com/lynis/controls/DBS-1884/

* Use the 'rename-command CONFIG' setting for Redis [DBS-1886]
- Details : /etc/redis/redis.conf
- Solution : configure 'rename-command CONFIG' in /etc/redis/redis.conf
- Related resources
  * Website: https://cisofy.com/lynis/controls/DBS-1886/

* Use 'bind' setting to listen on localhost for Redis instance [DBS-1888]
- Details : /etc/redis/redis.conf
- Solution : configure 'bind localhost' in /etc/redis/redis.conf
- Related resources
  * Website: https://cisofy.com/lynis/controls/DBS-1888/

* Check if any syslog daemon is running and correctly configured. [LOGG-2130]
- Related resources
  * Website: https://cisofy.com/lynis/controls/LOGG-2130/

* Although inetd is not running, make sure no services are enabled in /etc/inetd.conf, or remove inetd service [INSE-8006]
- Related resources
  * Website: https://cisofy.com/lynis/controls/INSE-8006/

* If there are no xinetd services required, it is recommended that the daemon be removed [INSE-8100]
- Related resources
  * Website: https://cisofy.com/lynis/controls/INSE-8100/

* Removing the telnet server package and replace with SSH when possible [INSE-8322]
- Related resources
  * Website: https://cisofy.com/lynis/controls/INSE-8322/

* 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 (no results) [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-con
figuration/
      * 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 ownership of home directories as some might be incorrect.
[HOME-9306]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/HOME-9306/

  * 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 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/
      * 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:
  ----------------------------
  - 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:

  Scan mode:
  Normal [■]  Forensics [ ]  Integration [ ]  Pentest [ ]

  Lynis modules:
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]

  Details:
  Hardening index : 51 [###########          ]
  Tests performed : 254
  Plugins enabled : 2

  Software components:
  - Firewall               [V]
  - Intrusion software     [X]
  - Malware scanner        [X]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

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

  Exceptions found
  Some exceptional events or information was found!

  What to do:
  You can help by providing your log file (/var/log/lynis.log).
  Go to https://cisofy.com/contact/ and send your file to the e-mail address listed

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

  Lynis 3.1.6

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2025, 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
/opt/lynis/default.prf for all settings)
```

Salida 2: Escaneo solución AUTH-9204 y AUTH-9208 volver al indice

```
root@linux-target:/opt/lynis# ./lynis audit system

[ Lynis 3.1.6 ]

################################################################################
  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.

  2007-2025, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                     [ DONE ]
  - Checking profiles...                                [ DONE ]

  ---------------------------------------------------
  Program version:           3.1.6
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  22.04
  End-of-life:               NO
  Kernel version:            6.12.38+kali
  Hardware platform:         x86_64
  Hostname:                  linux-target
  ---------------------------------------------------
  Profiles:                  /opt/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          ./plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                            [ SKIPPED ]

[+] 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: pam
    [..]
  - Plugin: systemd
    [.
  [WARNING]: Test PLGN-0010 had a long execution: 15.730562 seconds

System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
.............System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
..]

[+] Boot and services
------------------------------------
  - Service Manager                                [ upstart ]
  - Checking UEFI boot                             [ DISABLED ]
    - Boot loader                                  [ NONE FOUND ]
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
  - Check running services (systemctl)             [ DONE ]
        Result: found 0 running services
  - Check enabled services at boot (systemctl)     [ DONE ]
        Result: found 11 enabled services
  - Check startup files (permissions)              [ OK ]
  - Running 'systemd-analyze security'
      Unit name (exposure value) and predicate
      --------------------------------
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down

[+] 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 Linux kernel configuration file       [ NOT FOUND ]
/usr/bin/grep: /etc/kernel-img.conf: No such file or directory
  - Checking core dumps configuration
    - configuration in /etc/profile                [ DEFAULT ]
    - 'hard' configuration in /etc/security/limits.conf  [ ENABLED ]
    - 'soft' configuration in /etc/security/limits.conf  [ ENABLED ]
    - Checking setuid core dumps configuration     [ DISABLED ]
  - Check if reboot is needed                      [ UNKNOWN ]

[+] 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                              [ SUGGESTION ]
  - 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                        [ WARNING ]
    - Permissions for: /etc/sudoers.d/README               [ 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                                        [ FOUND ]
  - 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                          [ ENABLED ]

[+] Kerberos
------------------------------------
  - Check for Kerberos KDC and principals                  [ NOT FOUND ]

[+] Shells
------------------------------------
  - Checking shells from /etc/shells
    Result: found 8 shells (valid shells: 8).
    - Session timeout settings/tools                       [ NONE ]
  - Checking default umask values
    - Checking default umask in /etc/bash.bashrc           [ WEAK ]
    - Checking default umask in /etc/profile               [ NONE ]

[+] File systems
------------------------------------
```

```
  - Checking mount points
    - Checking /home mount point                    [ SUGGESTION ]
    - Checking /tmp mount point                     [ SUGGESTION ]
    - Checking /var mount point                     [ SUGGESTION ]
  - Query swap partitions (fstab)                   [ NONE ]
  - 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 /dev                           [ PARTIALLY HARDENED ]
  - Mount options of /dev/shm                       [ HARDENED ]
  - Total without nodev:7 noexec:6 nosuid:5 ro or noexec (W^X): 6 of total 12

[+] 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
------------------------------------
  - Check running NFS daemon                        [ NOT FOUND ]

[+] Name services
------------------------------------
  - Checking search domains                         [ FOUND ]
  - Checking /etc/resolv.conf options               [ FOUND ]
  - Searching DNS domain name                       [ UNKNOWN ]
  - 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 dpkg package manager                [ FOUND ]
      - Querying package manager
    - Query unpurged packages                       [ NONE ]
  - Checking security repository in sources.list file  [ OK ]
  - Checking APT package database                   [ OK ]
  - Checking vulnerable packages (apt-get only)     [ DONE ]

  [WARNING]: Test PKGS-7392 had a long execution: 12.596901 seconds

  - Checking upgradeable packages                   [ SKIPPED ]
  - Checking package audit tool                     [ INSTALLED ]
```

```
   Found: apt-get

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

  Exception found!

  Function/test:  [PKGS-7410]
  Message:        Could not find any kernel packages via package manager

  Help improving the Lynis community with your feedback!

  Steps:
  - Ensure you are running the latest version (./lynis update check)
  - If so, create a GitHub issue at https://github.com/CISOfy/lynis
  - Include relevant parts of the log file or configuration file

  Thanks!

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

  - Toolkit for automatic upgrades                        [ NOT FOUND ]

[+] Networking
------------------------------------
  - Checking IPv6 configuration                           [ ENABLED ]
      Configuration method                              [ AUTO ]
      IPv6 only                                       [ NO ]
  - Checking configured nameservers
    - Testing nameservers
      Nameserver: 127.0.0.11                            [ SKIPPED ]
    - Minimal of 2 responsive nameservers                   [ SKIPPED ]
    - DNSSEC supported (systemd-resolved)                     [ UNKNOWN ]
  - Checking default gateway                              [ DONE ]

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

  Exception found!

  Function/test:  [NETW-3004:1]
  Message:        No interfaces found on this system (OS=Linux)

  Help improving the Lynis community with your feedback!

  Steps:
  - Ensure you are running the latest version (./lynis update check)
  - If so, create a GitHub issue at https://github.com/CISOfy/lynis
  - Include relevant parts of the log file or configuration file

  Thanks!

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

  - Getting listening ports (TCP/UDP)                     [ DONE ]
  - Checking promiscuous interfaces                       [ UNKNOWN ]
```

```
  - 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
------------------------------------
  - Postfix status                                  [ RUNNING ]
    - Postfix configuration                         [ FOUND ]
      - Postfix configuration errors                  [ WARNING ]

[+] Software: firewalls
------------------------------------
  - Checking iptables support                       [ 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                                 [ NOT FOUND ]
  - Checking nginx                                  [ NOT FOUND ]

[+] SSH Support
------------------------------------
  - Checking running SSH daemon                       [ FOUND ]
    - Searching SSH configuration                   [ FOUND ]
    - OpenSSH option: AllowTcpForwarding              [ SUGGESTION ]
    - OpenSSH option: ClientAliveCountMax             [ SUGGESTION ]
    - OpenSSH option: ClientAliveInterval           [ OK ]
    - OpenSSH option: FingerprintHash               [ OK ]
    - OpenSSH option: GatewayPorts                  [ SUGGESTION ]
    - OpenSSH option: IgnoreRhosts                  [ OK ]
    - OpenSSH option: LoginGraceTime                  [ OK ]
    - OpenSSH option: LogLevel                      [ SUGGESTION ]
    - OpenSSH option: MaxAuthTries                  [ SUGGESTION ]
    - OpenSSH option: MaxSessions                   [ SUGGESTION ]
    - OpenSSH option: PermitRootLogin                 [ SUGGESTION ]
    - OpenSSH option: PermitUserEnvironment             [ SUGGESTION ]
    - OpenSSH option: PermitTunnel                  [ SUGGESTION ]
    - OpenSSH option: Port                          [ SUGGESTION ]
    - OpenSSH option: PrintLastLog                    [ OK ]
    - OpenSSH option: StrictModes                   [ SUGGESTION ]
    - OpenSSH option: TCPKeepAlive                    [ SUGGESTION ]
    - OpenSSH option: UseDNS                        [ OK ]
    - OpenSSH option: X11Forwarding                   [ SUGGESTION ]
```

```
   - OpenSSH option: AllowAgentForwarding                [ SUGGESTION ]
   - OpenSSH option: AllowUsers                          [ NOT FOUND ]
   - OpenSSH option: AllowGroups                         [ NOT FOUND ]

[+] SNMP Support
------------------------------------
  - Checking running SNMP daemon                         [ NOT FOUND ]

[+] Databases
------------------------------------
  - Redis (server) status                                [ FOUND ]
    - Redis (requirepass configured)                     [ NOT FOUND ]
    - Redis (rename of CONFIG command)                   [ NOT FOUND ]
    - Redis (bind on localhost)                          [ NOT FOUND ]

[+] LDAP Services
------------------------------------
  - Checking OpenLDAP instance                           [ NOT FOUND ]

[+] PHP
------------------------------------
  - Checking PHP                                         [ NOT FOUND ]

[+] Squid Support
------------------------------------
  - Checking running Squid daemon                        [ NOT FOUND ]

[+] Logging and files
------------------------------------
  - Checking for a running log daemon                    [ WARNING ]
    - Checking Syslog-NG status                          [ NOT FOUND ]
    - Checking systemd journal status                    [ NOT FOUND ]
    - Checking Metalog status                            [ NOT FOUND ]
    - Checking RSyslog status                            [ NOT FOUND ]
    - Checking RFC 3195 daemon status                    [ NOT FOUND ]
    - Checking klogd                                     [ NOT FOUND ]
    - Checking minilogd instances                        [ NOT FOUND ]
    - Checking wazuh-agent daemon status                 [ NOT FOUND ]
  - Checking logrotate presence                          [ OK ]
  - Checking log directories (static list)               [ DONE ]
  - Checking open log files                              [ SKIPPED ]

[+] Insecure services
------------------------------------
  - Installed inetd package                              [ NOT FOUND ]
    - Checking enabled inetd services                    [ SUGGESTION ]
  - Installed xinetd package                             [ FOUND ]
    - xinetd status                                      [ NOT ACTIVE ]
      - Enabled xinetd.d services                        [ NOT FOUND ]
  - Installed rsh client package                         [ OK ]
  - Installed rsh server package                         [ OK ]
  - Installed telnet client package                      [ OK ]
  - Installed telnet server package                      [ FOUND ]
  - Checking NIS client installation                     [ OK ]
```

```
  - Checking NIS server installation                    [ OK ]
  - Checking TFTP client installation                   [ OK ]
  - Checking TFTP server installation                   [ OK ]

[+] Banners and identification
------------------------------------
  - /etc/issue                                  [ FOUND ]
    - /etc/issue contents                         [ WEAK ]
  - /etc/issue.net                              [ FOUND ]
    - /etc/issue.net contents                     [ WEAK ]

[+] Scheduled tasks
------------------------------------
  - Checking crontab and cronjobs files                 [ WARNING ]

[+] Accounting
------------------------------------
  - Checking accounting information                     [ NOT FOUND ]
  - Checking sysstat accounting data                    [ NOT FOUND ]
  - Checking auditd                                 [ NOT FOUND ]

[+] Time and Synchronization
------------------------------------

[+] Cryptography
------------------------------------
  - Checking for expired SSL certificates [0/149]           [ NONE ]

  [WARNING]: Test CRYP-7902 had a long execution: 21.908517 seconds

  - Kernel entropy is sufficient                        [ YES ]
  - HW RNG & rngd                                     [ NO ]
  - SW prng                                         [ NO ]
  - MOR variable not found                              [ WEAK ]

[+] Virtualization
------------------------------------

[+] Containers
------------------------------------

[+] Security frameworks
------------------------------------
  - Checking presence AppArmor                        [ NOT FOUND ]
  - 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
  - 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: /etc/crontab                                [ SUGGESTION ]
    File: /etc/group                                  [ SUGGESTION ]
    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                                 [ SUGGESTION ]
    File: /etc/passwd-                                [ SUGGESTION ]
    File: /etc/ssh/sshd_config                        [ SUGGESTION ]
    Directory: /root/.ssh                             [ 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
------------------------------------
  - Permissions of home directories                     [ OK ]
  - 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)                [ DIFFERENT ]
    - kernel.sysrq (exp: 0)                             [ DIFFERENT ]
    - kernel.unprivileged_bpf_disabled (exp: 1)         [ DIFFERENT ]
```

```
    - kernel.yama.ptrace_scope (exp: 1 2 3)                 [ DIFFERENT ]
    - net.ipv4.conf.all.accept_redirects (exp: 0)           [ OK ]
    - net.ipv4.conf.all.accept_source_route (exp: 0)        [ OK ]
    - net.ipv4.conf.all.bootp_relay (exp: 0)                [ OK ]
    - net.ipv4.conf.all.forwarding (exp: 0)                 [ DIFFERENT ]
    - net.ipv4.conf.all.log_martians (exp: 1)               [ DIFFERENT ]
    - net.ipv4.conf.all.mc_forwarding (exp: 0)              [ OK ]
    - net.ipv4.conf.all.proxy_arp (exp: 0)                  [ OK ]
    - net.ipv4.conf.all.rp_filter (exp: 1)                  [ DIFFERENT ]
    - net.ipv4.conf.all.send_redirects (exp: 0)             [ 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)                                 [ NOT FOUND ]
    - Installed malware scanner                             [ NOT FOUND ]
    - Non-native binary formats                             [ NOT FOUND ]

[+] Custom tests
------------------------------------
  - Running custom tests...                                 [ NONE ]

[+] Plugins (phase 2)
------------------------------------
  - Plugins (phase 2)                                       [ DONE ]

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

  -[ Lynis 3.1.6 Results ]-

  Warnings (4):
  ----------------------------
  ! iptables module(s) loaded, but no rules active [FIRE-4512]
      https://cisofy.com/lynis/controls/FIRE-4512/

  ! Redis configuration file /etc/redis/redis.conf is world readable and might leak sensitive
details [DBS-1882]
    - Details  : /etc/redis/redis.conf
    - Solution : Use chmod 640 to change file permissions
      https://cisofy.com/lynis/controls/DBS-1882/

  ! klogd is not running, which could lead to missing kernel messages in log files
[LOGG-2138]
```

```
      https://cisofy.com/lynis/controls/LOGG-2138/

  ! Found one or more cronjob files with incorrect file permissions (see log for details)
[SCHD-7704]
      https://cisofy.com/lynis/controls/SCHD-7704/

  Suggestions (58):
  ----------------------------
  * 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/

  * Determine why /vmlinuz or /boot/vmlinuz is missing on this Debian/Ubuntu system.
[KRNL-5788]
    - Details  : /vmlinuz or /boot/vmlinuz
    - Related resources
      * Website: https://cisofy.com/lynis/controls/KRNL-5788/

  * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file
[KRNL-5820]
    - Related resources
      * 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/

  * Run pwck manually and correct any errors in the password file [AUTH-9228]
    - Related resources
      * Article: File integrity of password files:
https://linux-audit.com/authentication/file-integrity-of-password-files/
      * Website: https://cisofy.com/lynis/controls/AUTH-9228/

  * 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-sy
stems/
      * 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/

  * Look at the locked accounts and consider removing them [AUTH-9284]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/AUTH-9284/

  * 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 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 /tmp file system, place /tmp 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/

  * 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 DNS configuration for the dns domain name [NAME-4028]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/NAME-4028/
```

```
  * 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/

  * 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/

  * Found a configuration error in Postfix [MAIL-8817]
    - Details  : /etc/postfix/main.cf
    - Solution : run postconf > /dev/null
    - Related resources
      * Article: Postfix Hardening Guide for Security and Privacy:
https://linux-audit.com/postfix-hardening-guide-for-security-and-privacy/
      * Website: https://cisofy.com/lynis/controls/MAIL-8817/

  * Disable the 'VRFY' command [MAIL-8820:disable_vrfy_command]
    - Details  : disable_vrfy_command=no
    - Solution : run postconf -e disable_vrfy_command=yes to change the value
    - Related resources
      * Article: Postfix Hardening Guide for Security and Privacy:
https://linux-audit.com/postfix-hardening-guide-for-security-and-privacy/
      * Website: https://cisofy.com/lynis/controls/MAIL-8820/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowTcpForwarding (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : ClientAliveCountMax (set 3 to 2)
```

```
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : GatewayPorts (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : LogLevel (set INFO to VERBOSE)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxAuthTries (set 6 to 3)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxSessions (set 10 to 2)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitRootLogin (set YES to
(FORCED-COMMANDS-ONLY|NO|PROHIBIT-PASSWORD|WITHOUT-PASSWORD))
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitUserEnvironment (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitTunnel (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/
```

```
  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Port (set 22 to )
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : StrictModes (set NO to YES)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : TCPKeepAlive (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : X11Forwarding (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowAgentForwarding (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Configure the 'requirepass' setting for Redis [DBS-1884]
    - Details  : /etc/redis/redis.conf
    - Solution : configure 'requirepass' setting in /etc/redis/redis.conf
    - Related resources
      * Website: https://cisofy.com/lynis/controls/DBS-1884/

  * Use the 'rename-command CONFIG' setting for Redis [DBS-1886]
    - Details  : /etc/redis/redis.conf
    - Solution : configure 'rename-command CONFIG' in /etc/redis/redis.conf
    - Related resources
      * Website: https://cisofy.com/lynis/controls/DBS-1886/

  * Use 'bind' setting to listen on localhost for Redis instance [DBS-1888]
    - Details  : /etc/redis/redis.conf
    - Solution : configure 'bind localhost' in /etc/redis/redis.conf
    - Related resources
      * Website: https://cisofy.com/lynis/controls/DBS-1888/
```

* Check if any syslog daemon is running and correctly configured. [LOGG-2130]
  - Related resources
    * Website: https://cisofy.com/lynis/controls/LOGG-2130/

* Although inetd is not running, make sure no services are enabled in /etc/inetd.conf, or remove inetd service [INSE-8006]
  - Related resources
    * Website: https://cisofy.com/lynis/controls/INSE-8006/

* If there are no xinetd services required, it is recommended that the daemon be removed [INSE-8100]
  - Related resources
    * Website: https://cisofy.com/lynis/controls/INSE-8100/

* Removing the telnet server package and replace with SSH when possible [INSE-8322]
  - Related resources
    * Website: https://cisofy.com/lynis/controls/INSE-8322/

* 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 (no results) [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/

  * 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 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/
      * 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:
  --------------------------
  - 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:

  Scan mode:
  Normal [■]  Forensics [ ]  Integration [ ]  Pentest [ ]

  Lynis modules:
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]

  Details:
  Hardening index : 50 [##########          ]
  Tests performed : 254
  Plugins enabled : 2
```

```
  Software components:
  - Firewall               [V]
  - Intrusion software     [X]
  - Malware scanner        [X]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

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

  Exceptions found
  Some exceptional events or information was found!

  What to do:
  You can help by providing your log file (/var/log/lynis.log).
  Go to https://cisofy.com/contact/ and send your file to the e-mail address listed

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

  Lynis 3.1.6

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2025, 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
/opt/lynis/default.prf for all settings)
```

Salida 3: intento 1 de solución a problemas de Firewall (FIRE-4512): volver al indice

```
[ Lynis 3.1.6 ]

################################################################################
  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.

  2007-2025, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################
```

```
[+] Initializing program
------------------------------------
  - Detecting OS...                                     [ DONE ]
  - Checking profiles...                                [ DONE ]

  ---------------------------------------------------
  Program version:           3.1.6
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  22.04
  End-of-life:               NO
  Kernel version:            6.12.38+kali
  Hardware platform:         x86_64
  Hostname:                  linux-target
  ---------------------------------------------------
  Profiles:                  /opt/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          ./plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                          [ SKIPPED ]

[+] 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: pam
    [..]
  - Plugin: systemd
    [.
  [WARNING]: Test PLGN-0010 had a long execution: 12.061681 seconds

System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
.....System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
..]

[+] Boot and services
------------------------------------
  - Service Manager                                   [ upstart ]
  - Checking UEFI boot                                  [ DISABLED ]
    - Boot loader                                     [ NONE FOUND ]
```

```
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
  - Check running services (systemctl)                    [ DONE ]
        Result: found 0 running services
  - Check enabled services at boot (systemctl)            [ DONE ]
        Result: found 11 enabled services
  - Check startup files (permissions)                     [ OK ]
  - Running 'systemd-analyze security'
      Unit name (exposure value) and predicate
      ------------------------------
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down

[+] 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 Linux kernel configuration file              [ NOT FOUND ]
/usr/bin/grep: /etc/kernel-img.conf: No such file or directory
  - Checking core dumps configuration
    - configuration in /etc/profile                       [ DEFAULT ]
    - 'hard' configuration in /etc/security/limits.conf   [ ENABLED ]
    - 'soft' configuration in /etc/security/limits.conf   [ ENABLED ]
    - Checking setuid core dumps configuration            [ DISABLED ]
  - Check if reboot is needed                             [ UNKNOWN ]

[+] 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                       [ WARNING ]
    - Permissions for: /etc/sudoers.d/README              [ 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                                    [ FOUND ]
  - 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                      [ ENABLED ]

[+] Kerberos
------------------------------------
  - Check for Kerberos KDC and principals              [ NOT FOUND ]

[+] Shells
------------------------------------
  - Checking shells from /etc/shells
    Result: found 8 shells (valid shells: 8).
    - Session timeout settings/tools                   [ NONE ]
  - Checking default umask values
    - Checking default umask in /etc/bash.bashrc       [ WEAK ]
    - Checking default umask in /etc/profile           [ NONE ]

[+] File systems
------------------------------------
  - Checking mount points
    - Checking /home mount point                       [ SUGGESTION ]
    - Checking /tmp mount point                        [ SUGGESTION ]
    - Checking /var mount point                        [ SUGGESTION ]
  - Query swap partitions (fstab)                      [ NONE ]
  - 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 /dev                              [ PARTIALLY HARDENED ]
  - Mount options of /dev/shm                          [ HARDENED ]
  - Total without nodev:7 noexec:6 nosuid:5 ro or noexec (W^X): 6 of total 12

[+] 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
------------------------------------
  - Check running NFS daemon                                 [ NOT FOUND ]

[+] Name services
------------------------------------
  - Checking search domains                                  [ FOUND ]
  - Checking /etc/resolv.conf options                        [ FOUND ]
  - Searching DNS domain name                                [ UNKNOWN ]
  - 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 dpkg package manager                         [ FOUND ]
      - Querying package manager
    - Query unpurged packages                                [ NONE ]
  - Checking security repository in sources.list file        [ OK ]
  - Checking APT package database                            [ OK ]
  - Checking vulnerable packages (apt-get only)              [ DONE ]

  [WARNING]: Test PKGS-7392 had a long execution: 11.168192 seconds

  - Checking upgradeable packages                            [ SKIPPED ]
  - Checking package audit tool                              [ INSTALLED ]
    Found: apt-get

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

  Exception found!

  Function/test:  [PKGS-7410]
  Message:        Could not find any kernel packages via package manager

  Help improving the Lynis community with your feedback!

  Steps:
  - Ensure you are running the latest version (./lynis update check)
  - If so, create a GitHub issue at https://github.com/CISOfy/lynis
  - Include relevant parts of the log file or configuration file

  Thanks!

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

  - Toolkit for automatic upgrades                           [ NOT FOUND ]

[+] Networking
```

```
------------------------------------
  - Checking IPv6 configuration                 [ ENABLED ]
      Configuration method                    [ AUTO ]
      IPv6 only                               [ NO ]
  - Checking configured nameservers
    - Testing nameservers
      Nameserver: 127.0.0.11                  [ SKIPPED ]
    - Minimal of 2 responsive nameservers     [ SKIPPED ]
    - DNSSEC supported (systemd-resolved)     [ UNKNOWN ]
  - Checking default gateway                  [ DONE ]

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

  Exception found!

  Function/test:  [NETW-3004:1]
  Message:        No interfaces found on this system (OS=Linux)

  Help improving the Lynis community with your feedback!

  Steps:
  - Ensure you are running the latest version (./lynis update check)
  - If so, create a GitHub issue at https://github.com/CISOfy/lynis
  - Include relevant parts of the log file or configuration file

  Thanks!

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

  - Getting listening ports (TCP/UDP)         [ DONE ]
  - Checking promiscuous interfaces           [ UNKNOWN ]
  - 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
------------------------------------
  - Postfix status                            [ RUNNING ]
    - Postfix configuration                   [ FOUND ]
      - Postfix configuration errors          [ WARNING ]

[+] Software: firewalls
------------------------------------
  - Checking iptables support                 [ FOUND ]
    - Checking iptables policies of chains    [ FOUND ]
      - Chain INPUT (table: filter, target: ACCEPT)    [ ACCEPT ]
      - Chain INPUT (table: filter, target: DROP)      [ DROP ]
      - Chain INPUT (table: security, target: ACCEPT)  [ ACCEPT ]
```

```
   - Checking for empty ruleset                    [ WARNING ]
   - Checking for unused rules                     [ FOUND ]
  - Checking host based firewall                   [ ACTIVE ]

[+] Software: webserver
------------------------------------
  - Checking Apache                              [ NOT FOUND ]
  - Checking nginx                               [ NOT FOUND ]

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

[+] SNMP Support
------------------------------------
  - Checking running SNMP daemon                   [ NOT FOUND ]

[+] Databases
------------------------------------
  - Redis (server) status                        [ FOUND ]
    - Redis (requirepass configured)               [ NOT FOUND ]
    - Redis (rename of CONFIG command)             [ NOT FOUND ]
    - Redis (bind on localhost)                  [ NOT FOUND ]

[+] LDAP Services
------------------------------------
  - Checking OpenLDAP instance                     [ NOT FOUND ]

[+] PHP
------------------------------------
  - Checking PHP                                 [ NOT FOUND ]
```

```
[+] Squid Support
------------------------------------
  - Checking running Squid daemon                       [ NOT FOUND ]

[+] Logging and files
------------------------------------
  - Checking for a running log daemon                   [ WARNING ]
    - Checking Syslog-NG status                         [ NOT FOUND ]
    - Checking systemd journal status                   [ NOT FOUND ]
    - Checking Metalog status                           [ NOT FOUND ]
    - Checking RSyslog status                           [ NOT FOUND ]
    - Checking RFC 3195 daemon status                   [ NOT FOUND ]
    - Checking klogd                                    [ NOT FOUND ]
    - Checking minilogd instances                       [ NOT FOUND ]
    - Checking wazuh-agent daemon status                [ NOT FOUND ]
  - Checking logrotate presence                         [ OK ]
  - Checking log directories (static list)              [ DONE ]
  - Checking open log files                             [ SKIPPED ]

[+] Insecure services
------------------------------------
  - Installed inetd package                             [ NOT FOUND ]
    - Checking enabled inetd services                   [ SUGGESTION ]
  - Installed xinetd package                            [ FOUND ]
    - xinetd status                                     [ NOT ACTIVE ]
      - Enabled xinetd.d services                       [ NOT FOUND ]
  - Installed rsh client package                        [ OK ]
  - Installed rsh server package                        [ OK ]
  - Installed telnet client package                     [ OK ]
  - Installed telnet server package                     [ FOUND ]
  - Checking NIS client installation                    [ OK ]
  - Checking NIS server installation                    [ OK ]
  - Checking TFTP client installation                   [ OK ]
  - Checking TFTP server installation                   [ OK ]

[+] Banners and identification
------------------------------------
  - /etc/issue                                          [ FOUND ]
    - /etc/issue contents                               [ WEAK ]
  - /etc/issue.net                                      [ FOUND ]
    - /etc/issue.net contents                           [ WEAK ]

[+] Scheduled tasks
------------------------------------
  - Checking crontab and cronjobs files                 [ WARNING ]

[+] Accounting
------------------------------------
  - Checking accounting information                     [ NOT FOUND ]
  - Checking sysstat accounting data                    [ NOT FOUND ]
  - Checking auditd                                     [ NOT FOUND ]

[+] Time and Synchronization
```

```
---------------------------------

[+] Cryptography
---------------------------------
  - Checking for expired SSL certificates [0/149]            [ NONE ]

  [WARNING]: Test CRYP-7902 had a long execution: 14.495226 seconds

  - Kernel entropy is sufficient                             [ YES ]
  - HW RNG & rngd                                            [ NO ]
  - SW prng                                                  [ NO ]
  - MOR variable not found                                   [ WEAK ]

[+] Virtualization
---------------------------------

[+] Containers
---------------------------------

[+] Security frameworks
---------------------------------
  - Checking presence AppArmor                               [ NOT FOUND ]
  - 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
  - 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: /etc/crontab                                       [ SUGGESTION ]
    File: /etc/group                                         [ SUGGESTION ]
    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                                        [ SUGGESTION ]
    File: /etc/passwd-                                       [ SUGGESTION ]
```

```
   File: /etc/ssh/sshd_config                          [ SUGGESTION ]
   Directory: /root/.ssh                             [ 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
------------------------------------
  - Permissions of home directories                  [ OK ]
  - 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)             [ DIFFERENT ]
    - kernel.sysrq (exp: 0)                          [ DIFFERENT ]
    - kernel.unprivileged_bpf_disabled (exp: 1)      [ DIFFERENT ]
    - kernel.yama.ptrace_scope (exp: 1 2 3)          [ DIFFERENT ]
    - net.ipv4.conf.all.accept_redirects (exp: 0)    [ OK ]
    - net.ipv4.conf.all.accept_source_route (exp: 0) [ OK ]
    - net.ipv4.conf.all.bootp_relay (exp: 0)         [ OK ]
    - net.ipv4.conf.all.forwarding (exp: 0)          [ DIFFERENT ]
    - net.ipv4.conf.all.log_martians (exp: 1)        [ DIFFERENT ]
    - net.ipv4.conf.all.mc_forwarding (exp: 0)       [ OK ]
    - net.ipv4.conf.all.proxy_arp (exp: 0)           [ OK ]
    - net.ipv4.conf.all.rp_filter (exp: 1)           [ DIFFERENT ]
    - net.ipv4.conf.all.send_redirects (exp: 0)      [ 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)                       [ NOT FOUND ]
   - Installed malware scanner                     [ NOT FOUND ]
   - Non-native binary formats                     [ NOT FOUND ]

[+] Custom tests
------------------------------------
  - Running custom tests...                      [ NONE ]

[+] Plugins (phase 2)
------------------------------------
  - Plugins (phase 2)                            [ DONE ]

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

  -[ Lynis 3.1.6 Results ]-

  Warnings (4):
  ----------------------------
  ! iptables module(s) loaded, but no rules active [FIRE-4512]
      https://cisofy.com/lynis/controls/FIRE-4512/

  ! Redis configuration file /etc/redis/redis.conf is world readable and might leak sensitive details [DBS-1882]
    - Details  : /etc/redis/redis.conf
    - Solution : Use chmod 640 to change file permissions
      https://cisofy.com/lynis/controls/DBS-1882/

  ! klogd is not running, which could lead to missing kernel messages in log files [LOGG-2138]
      https://cisofy.com/lynis/controls/LOGG-2138/

  ! Found one or more cronjob files with incorrect file permissions (see log for details) [SCHD-7704]
      https://cisofy.com/lynis/controls/SCHD-7704/

  Suggestions (58):
  ----------------------------
  * 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/

  * Determine why /vmlinuz or /boot/vmlinuz is missing on this Debian/Ubuntu system. [KRNL-5788]
    - Details  : /vmlinuz or /boot/vmlinuz
```

- Related resources
* Website: https://cisofy.com/lynis/controls/KRNL-5788/

* If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
- Related resources
* 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/

* 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/

* Look at the locked accounts and consider removing them [AUTH-9284]
- Related resources
* Website: https://cisofy.com/lynis/controls/AUTH-9284/

* 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 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 /tmp file system, place /tmp 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/

  * 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 DNS configuration for the dns domain name [NAME-4028]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/NAME-4028/

  * 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/

  * 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/
```

```
  * Found a configuration error in Postfix [MAIL-8817]
    - Details  : /etc/postfix/main.cf
    - Solution : run postconf > /dev/null
    - Related resources
      * Article: Postfix Hardening Guide for Security and Privacy:
https://linux-audit.com/postfix-hardening-guide-for-security-and-privacy/
      * Website: https://cisofy.com/lynis/controls/MAIL-8817/

  * Disable the 'VRFY' command [MAIL-8820:disable_vrfy_command]
    - Details  : disable_vrfy_command=no
    - Solution : run postconf -e disable_vrfy_command=yes to change the value
    - Related resources
      * Article: Postfix Hardening Guide for Security and Privacy:
https://linux-audit.com/postfix-hardening-guide-for-security-and-privacy/
      * Website: https://cisofy.com/lynis/controls/MAIL-8820/

  * Check iptables rules to see which rules are currently not used [FIRE-4513]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/FIRE-4513/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowTcpForwarding (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : ClientAliveCountMax (set 3 to 2)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : GatewayPorts (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : LogLevel (set INFO to VERBOSE)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxAuthTries (set 6 to 3)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
```

```
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxSessions (set 10 to 2)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitRootLogin (set YES to
(FORCED-COMMANDS-ONLY|NO|PROHIBIT-PASSWORD|WITHOUT-PASSWORD))
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitUserEnvironment (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitTunnel (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Port (set 22 to )
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : StrictModes (set NO to YES)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : TCPKeepAlive (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : X11Forwarding (set YES to NO)
```

- Related resources
  * Article: OpenSSH security and hardening: https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
  * Website: https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details : AllowAgentForwarding (set YES to NO)
  - Related resources
    * Article: OpenSSH security and hardening: https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
    * Website: https://cisofy.com/lynis/controls/SSH-7408/

* Configure the 'requirepass' setting for Redis [DBS-1884]
  - Details : /etc/redis/redis.conf
  - Solution : configure 'requirepass' setting in /etc/redis/redis.conf
  - Related resources
    * Website: https://cisofy.com/lynis/controls/DBS-1884/

* Use the 'rename-command CONFIG' setting for Redis [DBS-1886]
  - Details : /etc/redis/redis.conf
  - Solution : configure 'rename-command CONFIG' in /etc/redis/redis.conf
  - Related resources
    * Website: https://cisofy.com/lynis/controls/DBS-1886/

* Use 'bind' setting to listen on localhost for Redis instance [DBS-1888]
  - Details : /etc/redis/redis.conf
  - Solution : configure 'bind localhost' in /etc/redis/redis.conf
  - Related resources
    * Website: https://cisofy.com/lynis/controls/DBS-1888/

* Check if any syslog daemon is running and correctly configured. [LOGG-2130]
  - Related resources
    * Website: https://cisofy.com/lynis/controls/LOGG-2130/

* Although inetd is not running, make sure no services are enabled in /etc/inetd.conf, or remove inetd service [INSE-8006]
  - Related resources
    * Website: https://cisofy.com/lynis/controls/INSE-8006/

* If there are no xinetd services required, it is recommended that the daemon be removed [INSE-8100]
  - Related resources
    * Website: https://cisofy.com/lynis/controls/INSE-8100/

* Removing the telnet server package and replace with SSH when possible [INSE-8322]
  - Related resources
    * Website: https://cisofy.com/lynis/controls/INSE-8322/

* 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 (no results) [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-con
figuration/
      * 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/

  * 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 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/
    * 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:
  ----------------------------
  - 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:

  Scan mode:
  Normal [■]  Forensics [ ]  Integration [ ]  Pentest [ ]

  Lynis modules:
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]

  Details:
  Hardening index : 51 [##########          ]
  Tests performed : 254
  Plugins enabled : 2

  Software components:
  - Firewall               [V]
  - Intrusion software     [X]
  - Malware scanner        [X]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

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

  Exceptions found
  Some exceptional events or information was found!

  What to do:
  You can help by providing your log file (/var/log/lynis.log).
  Go to https://cisofy.com/contact/ and send your file to the e-mail address listed

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

  Lynis 3.1.6
```

```
  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2025, 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
/opt/lynis/default.prf for all settings)
```

Salida 4: intento 2 de solución a problemas de Firewall (FIRE-4512): volver al indice

```
root@linux-target:/opt/lynis# ./lynis audit system

[ Lynis 3.1.6 ]

################################################################################
  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.

  2007-2025, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                     [ DONE ]
  - Checking profiles...                                [ DONE ]

  ---------------------------------------------------
  Program version:           3.1.6
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  22.04
  End-of-life:               NO
  Kernel version:            6.12.38+kali
  Hardware platform:         x86_64
  Hostname:                  linux-target
  ---------------------------------------------------
  Profiles:                  /opt/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          ./plugins
  ---------------------------------------------------
```

```
  Auditor:                 [Not Specified]
  Language:                en
  Test category:           all
  Test group:              all
  ------------------------------------------------
  - Program update status...                     [ SKIPPED ]

[+] 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: pam
    [..]
  - Plugin: systemd
    [.
  [WARNING]: Test PLGN-0010 had a long execution: 11.751637 seconds

System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
.............System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
..]

[+] Boot and services
------------------------------------
  - Service Manager                            [ upstart ]
  - Checking UEFI boot                         [ DISABLED ]
    - Boot loader                            [ NONE FOUND ]
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
  - Check running services (systemctl)             [ DONE ]
        Result: found 0 running services
  - Check enabled services at boot (systemctl)     [ DONE ]
        Result: found 11 enabled services
  - Check startup files (permissions)          [ OK ]
  - Running 'systemd-analyze security'
      Unit name (exposure value) and predicate
      --------------------------------
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down

[+] 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 Linux kernel configuration file   [ NOT FOUND ]
/usr/bin/grep: /etc/kernel-img.conf: No such file or directory
```

```
  - Checking core dumps configuration
    - configuration in /etc/profile                    [ DEFAULT ]
    - 'hard' configuration in /etc/security/limits.conf    [ ENABLED ]
    - 'soft' configuration in /etc/security/limits.conf    [ ENABLED ]
    - Checking setuid core dumps configuration          [ DISABLED ]
  - Check if reboot is needed                          [ UNKNOWN ]

[+] 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                    [ WARNING ]
    - Permissions for: /etc/sudoers.d/README           [ 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                                    [ FOUND ]
  - 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                      [ ENABLED ]

[+] Kerberos
------------------------------------
  - Check for Kerberos KDC and principals              [ NOT FOUND ]

[+] Shells
```

```
---------------------------------
  - Checking shells from /etc/shells
    Result: found 8 shells (valid shells: 8).
    - Session timeout settings/tools                [ NONE ]
  - Checking default umask values
    - Checking default umask in /etc/bash.bashrc      [ WEAK ]
    - Checking default umask in /etc/profile          [ NONE ]

[+] File systems
---------------------------------
  - Checking mount points
    - Checking /home mount point                    [ SUGGESTION ]
    - Checking /tmp mount point                     [ SUGGESTION ]
    - Checking /var mount point                     [ SUGGESTION ]
  - Query swap partitions (fstab)                   [ NONE ]
  - 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 /dev                           [ PARTIALLY HARDENED ]
  - Mount options of /dev/shm                       [ HARDENED ]
  - Total without nodev:7 noexec:6 nosuid:5 ro or noexec (W^X): 6 of total 12

[+] 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
---------------------------------
  - Check running NFS daemon                        [ NOT FOUND ]

[+] Name services
---------------------------------
  - Checking search domains                         [ FOUND ]
  - Checking /etc/resolv.conf options               [ FOUND ]
  - Searching DNS domain name                       [ UNKNOWN ]
  - 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 dpkg package manager                [ FOUND ]
```

```
    - Querying package manager
   - Query unpurged packages                      [ NONE ]
  - Checking security repository in sources.list file      [ OK ]
  - Checking APT package database                  [ OK ]
  - Checking vulnerable packages (apt-get only)          [ DONE ]
  - Checking upgradeable packages                [ SKIPPED ]
  - Checking package audit tool                  [ INSTALLED ]
    Found: apt-get

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

  Exception found!

  Function/test:  [PKGS-7410]
  Message:        Could not find any kernel packages via package manager

  Help improving the Lynis community with your feedback!

  Steps:
  - Ensure you are running the latest version (./lynis update check)
  - If so, create a GitHub issue at https://github.com/CISOfy/lynis
  - Include relevant parts of the log file or configuration file

  Thanks!

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

  - Toolkit for automatic upgrades                 [ NOT FOUND ]

[+] Networking
------------------------------------
  - Checking IPv6 configuration                    [ ENABLED ]
      Configuration method                       [ AUTO ]
      IPv6 only                                  [ NO ]
  - Checking configured nameservers
    - Testing nameservers
      Nameserver: 127.0.0.11                     [ SKIPPED ]
    - Minimal of 2 responsive nameservers            [ SKIPPED ]
    - DNSSEC supported (systemd-resolved)            [ UNKNOWN ]
  - Checking default gateway                       [ DONE ]

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

  Exception found!

  Function/test:  [NETW-3004:1]
  Message:        No interfaces found on this system (OS=Linux)

  Help improving the Lynis community with your feedback!

  Steps:
  - Ensure you are running the latest version (./lynis update check)
  - If so, create a GitHub issue at https://github.com/CISOfy/lynis
  - Include relevant parts of the log file or configuration file
```

```
  Thanks!

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

  - Getting listening ports (TCP/UDP)                [ DONE ]
  - Checking promiscuous interfaces                  [ UNKNOWN ]
  - 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
------------------------------------
  - Postfix status                                   [ RUNNING ]
    - Postfix configuration                          [ FOUND ]
      - Postfix configuration errors                 [ WARNING ]

[+] Software: firewalls
------------------------------------
  - Checking iptables support                        [ FOUND ]
    - Checking iptables policies of chains           [ FOUND ]
      - Chain INPUT (table: filter, target: ACCEPT)  [ ACCEPT ]
      - Chain INPUT (table: filter, target: DROP)    [ DROP ]
      - Chain INPUT (table: security, target: ACCEPT) [ ACCEPT ]
    - Checking for empty ruleset                     [ WARNING ]
    - Checking for unused rules                      [ FOUND ]
  - Checking host based firewall                     [ ACTIVE ]

[+] Software: webserver
------------------------------------
  - Checking Apache                                  [ NOT FOUND ]
  - Checking nginx                                   [ NOT FOUND ]

[+] SSH Support
------------------------------------
  - Checking running SSH daemon                      [ FOUND ]
    - Searching SSH configuration                    [ FOUND ]
    - OpenSSH option: AllowTcpForwarding             [ SUGGESTION ]
    - OpenSSH option: ClientAliveCountMax            [ SUGGESTION ]
    - OpenSSH option: ClientAliveInterval            [ OK ]
    - OpenSSH option: FingerprintHash                [ OK ]
    - OpenSSH option: GatewayPorts                   [ SUGGESTION ]
    - OpenSSH option: IgnoreRhosts                   [ OK ]
    - OpenSSH option: LoginGraceTime                 [ OK ]
    - OpenSSH option: LogLevel                       [ SUGGESTION ]
    - OpenSSH option: MaxAuthTries                   [ SUGGESTION ]
    - OpenSSH option: MaxSessions                    [ SUGGESTION ]
    - OpenSSH option: PermitRootLogin                [ SUGGESTION ]
```

```
   - OpenSSH option: PermitUserEnvironment                [ SUGGESTION ]
   - OpenSSH option: PermitTunnel                         [ SUGGESTION ]
   - OpenSSH option: Port                                 [ SUGGESTION ]
   - OpenSSH option: PrintLastLog                         [ OK ]
   - OpenSSH option: StrictModes                          [ SUGGESTION ]
   - OpenSSH option: TCPKeepAlive                         [ SUGGESTION ]
   - OpenSSH option: UseDNS                               [ OK ]
   - OpenSSH option: X11Forwarding                        [ SUGGESTION ]
   - OpenSSH option: AllowAgentForwarding                 [ SUGGESTION ]
   - OpenSSH option: AllowUsers                           [ NOT FOUND ]
   - OpenSSH option: AllowGroups                          [ NOT FOUND ]

[+] SNMP Support
------------------------------------
  - Checking running SNMP daemon                          [ NOT FOUND ]

[+] Databases
------------------------------------
  - Redis (server) status                                 [ FOUND ]
    - Redis (requirepass configured)                      [ NOT FOUND ]
    - Redis (rename of CONFIG command)                    [ NOT FOUND ]
    - Redis (bind on localhost)                           [ NOT FOUND ]

[+] LDAP Services
------------------------------------
  - Checking OpenLDAP instance                            [ NOT FOUND ]

[+] PHP
------------------------------------
  - Checking PHP                                          [ NOT FOUND ]

[+] Squid Support
------------------------------------
  - Checking running Squid daemon                         [ NOT FOUND ]

[+] Logging and files
------------------------------------
  - Checking for a running log daemon                     [ WARNING ]
    - Checking Syslog-NG status                           [ NOT FOUND ]
    - Checking systemd journal status                     [ NOT FOUND ]
    - Checking Metalog status                             [ NOT FOUND ]
    - Checking RSyslog status                             [ NOT FOUND ]
    - Checking RFC 3195 daemon status                     [ NOT FOUND ]
    - Checking klogd                                      [ NOT FOUND ]
    - Checking minilogd instances                         [ NOT FOUND ]
    - Checking wazuh-agent daemon status                  [ NOT FOUND ]
  - Checking logrotate presence                           [ OK ]
  - Checking log directories (static list)                [ DONE ]
  - Checking open log files                               [ SKIPPED ]

[+] Insecure services
------------------------------------
  - Installed inetd package                               [ NOT FOUND ]
    - Checking enabled inetd services                     [ SUGGESTION ]
```

```
  - Installed xinetd package                      [ FOUND ]
    - xinetd status                             [ NOT ACTIVE ]
      - Enabled xinetd.d services                 [ NOT FOUND ]
  - Installed rsh client package                  [ OK ]
  - Installed rsh server package                   [ OK ]
  - Installed telnet client package                [ OK ]
  - Installed telnet server package                 [ FOUND ]
  - Checking NIS client installation                [ OK ]
  - Checking NIS server installation                 [ OK ]
  - Checking TFTP client installation                [ OK ]
  - Checking TFTP server installation                 [ OK ]

[+] Banners and identification
------------------------------------
  - /etc/issue                                  [ FOUND ]
    - /etc/issue contents                         [ WEAK ]
  - /etc/issue.net                               [ FOUND ]
    - /etc/issue.net contents                     [ WEAK ]

[+] Scheduled tasks
------------------------------------
  - Checking crontab and cronjobs files              [ WARNING ]

[+] Accounting
------------------------------------
  - Checking accounting information                  [ NOT FOUND ]
  - Checking sysstat accounting data                 [ NOT FOUND ]
  - Checking auditd                               [ NOT FOUND ]

[+] Time and Synchronization
------------------------------------

[+] Cryptography
------------------------------------
  - Checking for expired SSL certificates [0/149]          [ NONE ]

  [WARNING]: Test CRYP-7902 had a long execution: 13.323990 seconds

  - Kernel entropy is sufficient                   [ YES ]
  - HW RNG & rngd                                 [ NO ]
  - SW prng                                     [ NO ]
  - MOR variable not found                         [ WEAK ]

[+] Virtualization
------------------------------------

[+] Containers
------------------------------------

[+] Security frameworks
------------------------------------
  - Checking presence AppArmor                     [ NOT FOUND ]
  - 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
  - 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: /etc/crontab                                    [ SUGGESTION ]
    File: /etc/group                                      [ SUGGESTION ]
    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                                     [ SUGGESTION ]
    File: /etc/passwd-                                    [ SUGGESTION ]
    File: /etc/ssh/sshd_config                                [ SUGGESTION ]
    Directory: /root/.ssh                                 [ 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
------------------------------------
  - Permissions of home directories                           [ OK ]
  - 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)              [ DIFFERENT ]
   - kernel.sysrq (exp: 0)                           [ DIFFERENT ]
   - kernel.unprivileged_bpf_disabled (exp: 1)       [ DIFFERENT ]
   - kernel.yama.ptrace_scope (exp: 1 2 3)           [ DIFFERENT ]
   - net.ipv4.conf.all.accept_redirects (exp: 0)     [ OK ]
   - net.ipv4.conf.all.accept_source_route (exp: 0)  [ OK ]
   - net.ipv4.conf.all.bootp_relay (exp: 0)          [ OK ]
   - net.ipv4.conf.all.forwarding (exp: 0)           [ DIFFERENT ]
   - net.ipv4.conf.all.log_martians (exp: 1)         [ DIFFERENT ]
   - net.ipv4.conf.all.mc_forwarding (exp: 0)        [ OK ]
   - net.ipv4.conf.all.proxy_arp (exp: 0)            [ OK ]
   - net.ipv4.conf.all.rp_filter (exp: 1)            [ DIFFERENT ]
   - net.ipv4.conf.all.send_redirects (exp: 0)       [ 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)                           [ NOT FOUND ]
   - Installed malware scanner                       [ NOT FOUND ]
   - Non-native binary formats                       [ NOT FOUND ]

[+] Custom tests
------------------------------------
  - Running custom tests...                          [ NONE ]

[+] Plugins (phase 2)
------------------------------------
  - Plugins (phase 2)                                [ DONE ]

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

  -[ Lynis 3.1.6 Results ]-

  Warnings (4):
  ----------------------------
  ! iptables module(s) loaded, but no rules active [FIRE-4512]
      https://cisofy.com/lynis/controls/FIRE-4512/
```

```
  ! Redis configuration file /etc/redis/redis.conf is world readable and might leak sensitive
details [DBS-1882]
    - Details  : /etc/redis/redis.conf
    - Solution : Use chmod 640 to change file permissions
      https://cisofy.com/lynis/controls/DBS-1882/

  ! klogd is not running, which could lead to missing kernel messages in log files
[LOGG-2138]
      https://cisofy.com/lynis/controls/LOGG-2138/

  ! Found one or more cronjob files with incorrect file permissions (see log for details)
[SCHD-7704]
      https://cisofy.com/lynis/controls/SCHD-7704/

  Suggestions (58):
  ----------------------------
  * 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/

  * Determine why /vmlinuz or /boot/vmlinuz is missing on this Debian/Ubuntu system.
[KRNL-5788]
    - Details  : /vmlinuz or /boot/vmlinuz
    - Related resources
      * Website: https://cisofy.com/lynis/controls/KRNL-5788/

  * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file
[KRNL-5820]
    - Related resources
      * 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/

  * 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-sys
tems/
      * 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/

  * Look at the locked accounts and consider removing them [AUTH-9284]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/AUTH-9284/

  * 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 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 /tmp file system, place /tmp 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/

  * 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 DNS configuration for the dns domain name [NAME-4028]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/NAME-4028/
```

```
  * 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/

  * 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/

  * Found a configuration error in Postfix [MAIL-8817]
    - Details  : /etc/postfix/main.cf
    - Solution : run postconf > /dev/null
    - Related resources
      * Article: Postfix Hardening Guide for Security and Privacy:
https://linux-audit.com/postfix-hardening-guide-for-security-and-privacy/
      * Website: https://cisofy.com/lynis/controls/MAIL-8817/

  * Disable the 'VRFY' command [MAIL-8820:disable_vrfy_command]
    - Details  : disable_vrfy_command=no
    - Solution : run postconf -e disable_vrfy_command=yes to change the value
    - Related resources
      * Article: Postfix Hardening Guide for Security and Privacy:
https://linux-audit.com/postfix-hardening-guide-for-security-and-privacy/
      * Website: https://cisofy.com/lynis/controls/MAIL-8820/

  * Check iptables rules to see which rules are currently not used [FIRE-4513]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/FIRE-4513/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowTcpForwarding (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
```

https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details : ClientAliveCountMax (set 3 to 2)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details : GatewayPorts (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details : LogLevel (set INFO to VERBOSE)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details : MaxAuthTries (set 6 to 3)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details : MaxSessions (set 10 to 2)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details : PermitRootLogin (set YES to
(FORCED-COMMANDS-ONLY|NO|PROHIBIT-PASSWORD|WITHOUT-PASSWORD))
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details : PermitUserEnvironment (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]

- Details : PermitTunnel (set YES to NO)
- Related resources
* Article: OpenSSH security and hardening: https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
* Website: https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : Port (set 22 to)
- Related resources
* Article: OpenSSH security and hardening: https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
* Website: https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : StrictModes (set NO to YES)
- Related resources
* Article: OpenSSH security and hardening: https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
* Website: https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : TCPKeepAlive (set YES to NO)
- Related resources
* Article: OpenSSH security and hardening: https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
* Website: https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : X11Forwarding (set YES to NO)
- Related resources
* Article: OpenSSH security and hardening: https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
* Website: https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : AllowAgentForwarding (set YES to NO)
- Related resources
* Article: OpenSSH security and hardening: https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
* Website: https://cisofy.com/lynis/controls/SSH-7408/

* Configure the 'requirepass' setting for Redis [DBS-1884]
- Details : /etc/redis/redis.conf
- Solution : configure 'requirepass' setting in /etc/redis/redis.conf
- Related resources
* Website: https://cisofy.com/lynis/controls/DBS-1884/

* Use the 'rename-command CONFIG' setting for Redis [DBS-1886]
- Details : /etc/redis/redis.conf
- Solution : configure 'rename-command CONFIG' in /etc/redis/redis.conf
- Related resources
* Website: https://cisofy.com/lynis/controls/DBS-1886/

* Use 'bind' setting to listen on localhost for Redis instance [DBS-1888]

- Details : /etc/redis/redis.conf
- Solution : configure 'bind localhost' in /etc/redis/redis.conf
- Related resources
  * Website: https://cisofy.com/lynis/controls/DBS-1888/

* Check if any syslog daemon is running and correctly configured. [LOGG-2130]
- Related resources
  * Website: https://cisofy.com/lynis/controls/LOGG-2130/

* Although inetd is not running, make sure no services are enabled in /etc/inetd.conf, or remove inetd service [INSE-8006]
- Related resources
  * Website: https://cisofy.com/lynis/controls/INSE-8006/

* If there are no xinetd services required, it is recommended that the daemon be removed [INSE-8100]
- Related resources
  * Website: https://cisofy.com/lynis/controls/INSE-8100/

* Removing the telnet server package and replace with SSH when possible [INSE-8322]
- Related resources
  * Website: https://cisofy.com/lynis/controls/INSE-8322/

* 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 (no results) [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/

  * 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 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/
      * 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:
  ---------------------------
  - 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:

  Scan mode:
  Normal [■]  Forensics [ ]  Integration [ ]  Pentest [ ]

  Lynis modules:
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]
```

```
  Details:
  Hardening index : 51 [##########          ]
  Tests performed : 254
  Plugins enabled : 2

  Software components:
  - Firewall               [V]
  - Intrusion software     [X]
  - Malware scanner        [X]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

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

  Exceptions found
  Some exceptional events or information was found!

  What to do:
  You can help by providing your log file (/var/log/lynis.log).
  Go to https://cisofy.com/contact/ and send your file to the e-mail address listed

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

  Lynis 3.1.6

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2025, 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
/opt/lynis/default.prf for all settings)
```

Salida 5: intento 3 de solución a problemas de Firewall (FIRE-4512): volver al indice

```
root@linux-target:/opt/lynis# ./lynis audit system

[ Lynis 3.1.6 ]

################################################################################
  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.
```

```
  2007-2025, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################
########


[+] Initializing program
------------------------------------
  - Detecting OS...                                     [ DONE ]
  - Checking profiles...                                [ DONE ]

  ---------------------------------------------------
  Program version:           3.1.6
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  22.04
  End-of-life:               NO
  Kernel version:            6.12.38+kali
  Hardware platform:         x86_64
  Hostname:                  linux-target
  ---------------------------------------------------
  Profiles:                  /opt/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          ./plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                          [ SKIPPED ]

[+] 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: pam
    [..]
  - Plugin: systemd
    [.
  [WARNING]: Test PLGN-0010 had a long execution: 11.097920 seconds

System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
.............System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
```

```
..]

[+] Boot and services
------------------------------------
  - Service Manager                                [ upstart ]
  - Checking UEFI boot                             [ DISABLED ]
    - Boot loader                                  [ NONE FOUND ]
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
  - Check running services (systemctl)             [ DONE ]
        Result: found 0 running services
  - Check enabled services at boot (systemctl)     [ DONE ]
        Result: found 11 enabled services
  - Check startup files (permissions)              [ OK ]
  - Running 'systemd-analyze security'
      Unit name (exposure value) and predicate
      ------------------------------
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down

[+] 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 Linux kernel configuration file       [ NOT FOUND ]
/usr/bin/grep: /etc/kernel-img.conf: No such file or directory
  - Checking core dumps configuration
    - configuration in /etc/profile                [ DEFAULT ]
    - 'hard' configuration in /etc/security/limits.conf  [ ENABLED ]
    - 'soft' configuration in /etc/security/limits.conf  [ ENABLED ]
    - Checking setuid core dumps configuration     [ DISABLED ]
  - Check if reboot is needed                      [ UNKNOWN ]

[+] 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                   [ WARNING ]
    - Permissions for: /etc/sudoers.d/README            [ 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                                 [ FOUND ]
  - 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                     [ ENABLED ]

[+] Kerberos
------------------------------------
  - Check for Kerberos KDC and principals             [ NOT FOUND ]

[+] Shells
------------------------------------
  - Checking shells from /etc/shells
    Result: found 8 shells (valid shells: 8).
    - Session timeout settings/tools                  [ NONE ]
  - Checking default umask values
    - Checking default umask in /etc/bash.bashrc        [ WEAK ]
    - Checking default umask in /etc/profile          [ NONE ]

[+] File systems
------------------------------------
  - Checking mount points
    - Checking /home mount point                      [ SUGGESTION ]
    - Checking /tmp mount point                       [ SUGGESTION ]
    - Checking /var mount point                       [ SUGGESTION ]
  - Query swap partitions (fstab)                     [ NONE ]
  - 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 /dev                             [ PARTIALLY HARDENED ]
  - Mount options of /dev/shm                         [ HARDENED ]
  - Total without nodev:7 noexec:6 nosuid:5 ro or noexec (W^X): 6 of total 12

[+] 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
------------------------------------
  - Check running NFS daemon                                [ NOT FOUND ]

[+] Name services
------------------------------------
  - Checking search domains                                 [ FOUND ]
  - Checking /etc/resolv.conf options                       [ FOUND ]
  - Searching DNS domain name                               [ UNKNOWN ]
  - 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 dpkg package manager                        [ FOUND ]
      - Querying package manager
    - Query unpurged packages                               [ NONE ]
  - Checking security repository in sources.list file       [ OK ]
  - Checking APT package database                           [ OK ]
  - Checking vulnerable packages (apt-get only)             [ DONE ]
  - Checking upgradeable packages                           [ SKIPPED ]
  - Checking package audit tool                             [ INSTALLED ]
    Found: apt-get

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

  Exception found!

  Function/test:  [PKGS-7410]
  Message:        Could not find any kernel packages via package manager

  Help improving the Lynis community with your feedback!

  Steps:
  - Ensure you are running the latest version (./lynis update check)
  - If so, create a GitHub issue at https://github.com/CISOfy/lynis
  - Include relevant parts of the log file or configuration file

  Thanks!

================================================================
```

```
  - Toolkit for automatic upgrades                        [ NOT FOUND ]

[+] Networking
------------------------------------
  - Checking IPv6 configuration                           [ ENABLED ]
      Configuration method                              [ AUTO ]
      IPv6 only                                     [ NO ]
  - Checking configured nameservers
    - Testing nameservers
      Nameserver: 127.0.0.11                            [ SKIPPED ]
    - Minimal of 2 responsive nameservers                   [ SKIPPED ]
    - DNSSEC supported (systemd-resolved)                     [ UNKNOWN ]
  - Checking default gateway                              [ DONE ]

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

  Exception found!

  Function/test:  [NETW-3004:1]
  Message:        No interfaces found on this system (OS=Linux)

  Help improving the Lynis community with your feedback!

  Steps:
  - Ensure you are running the latest version (./lynis update check)
  - If so, create a GitHub issue at https://github.com/CISOfy/lynis
  - Include relevant parts of the log file or configuration file

  Thanks!

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

  - Getting listening ports (TCP/UDP)                     [ DONE ]
  - Checking promiscuous interfaces                       [ UNKNOWN ]
  - 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
------------------------------------
  - Postfix status                                    [ RUNNING ]
    - Postfix configuration                             [ FOUND ]
      - Postfix configuration errors                        [ WARNING ]

[+] Software: firewalls
------------------------------------
  - Checking iptables support                             [ FOUND ]
```

```
   - Checking iptables policies of chains              [ FOUND ]
     - Chain INPUT (table: filter, target: DROP)       [ DROP ]
     - Chain INPUT (table: security, target: ACCEPT)   [ ACCEPT ]
   - Checking for empty ruleset                        [ OK ]
   - Checking for unused rules                         [ FOUND ]
  - Checking host based firewall                       [ ACTIVE ]

[+] Software: webserver
------------------------------------
  - Checking Apache                                   [ NOT FOUND ]
  - Checking nginx                                    [ NOT FOUND ]

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

[+] SNMP Support
------------------------------------
  - Checking running SNMP daemon                      [ NOT FOUND ]

[+] Databases
------------------------------------
  - Redis (server) status                             [ FOUND ]
    - Redis (requirepass configured)                  [ NOT FOUND ]
    - Redis (rename of CONFIG command)                [ NOT FOUND ]
    - Redis (bind on localhost)                       [ NOT FOUND ]

[+] LDAP Services
------------------------------------
  - Checking OpenLDAP instance                        [ NOT FOUND ]
```

```
[+] PHP
------------------------------------
  - Checking PHP                                [ NOT FOUND ]

[+] Squid Support
------------------------------------
  - Checking running Squid daemon                       [ NOT FOUND ]

[+] Logging and files
------------------------------------
  - Checking for a running log daemon                   [ WARNING ]
    - Checking Syslog-NG status                         [ NOT FOUND ]
    - Checking systemd journal status                   [ NOT FOUND ]
    - Checking Metalog status                           [ NOT FOUND ]
    - Checking RSyslog status                           [ NOT FOUND ]
    - Checking RFC 3195 daemon status                   [ NOT FOUND ]
    - Checking klogd                                    [ NOT FOUND ]
    - Checking minilogd instances                       [ NOT FOUND ]
    - Checking wazuh-agent daemon status                [ NOT FOUND ]
  - Checking logrotate presence                         [ OK ]
  - Checking log directories (static list)              [ DONE ]
  - Checking open log files                             [ SKIPPED ]

[+] Insecure services
------------------------------------
  - Installed inetd package                             [ NOT FOUND ]
    - Checking enabled inetd services                   [ SUGGESTION ]
  - Installed xinetd package                            [ FOUND ]
    - xinetd status                                     [ NOT ACTIVE ]
      - Enabled xinetd.d services                       [ NOT FOUND ]
  - Installed rsh client package                        [ OK ]
  - Installed rsh server package                        [ OK ]
  - Installed telnet client package                     [ OK ]
  - Installed telnet server package                     [ FOUND ]
  - Checking NIS client installation                    [ OK ]
  - Checking NIS server installation                    [ OK ]
  - Checking TFTP client installation                   [ OK ]
  - Checking TFTP server installation                   [ OK ]

[+] Banners and identification
------------------------------------
  - /etc/issue                                          [ FOUND ]
    - /etc/issue contents                               [ WEAK ]
  - /etc/issue.net                                      [ FOUND ]
    - /etc/issue.net contents                           [ WEAK ]

[+] Scheduled tasks
------------------------------------
  - Checking crontab and cronjobs files                 [ WARNING ]

[+] Accounting
------------------------------------
  - Checking accounting information                     [ NOT FOUND ]
  - Checking sysstat accounting data                    [ NOT FOUND ]
```

```
  - Checking auditd                                   [ NOT FOUND ]

[+] Time and Synchronization
---------------------------------

[+] Cryptography
---------------------------------
  - Checking for expired SSL certificates [0/149]          [ NONE ]

  [WARNING]: Test CRYP-7902 had a long execution: 11.377515 seconds

  - Kernel entropy is sufficient                           [ YES ]
  - HW RNG & rngd                                          [ NO ]
  - SW prng                                              [ NO ]
  - MOR variable not found                                 [ WEAK ]

[+] Virtualization
---------------------------------

[+] Containers
---------------------------------

[+] Security frameworks
---------------------------------
  - Checking presence AppArmor                           [ NOT FOUND ]
  - 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
  - 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: /etc/crontab                                   [ SUGGESTION ]
    File: /etc/group                                     [ SUGGESTION ]
    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                                   [ SUGGESTION ]
    File: /etc/passwd-                                  [ SUGGESTION ]
    File: /etc/ssh/sshd_config                          [ SUGGESTION ]
    Directory: /root/.ssh                               [ 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
------------------------------------
  - Permissions of home directories                     [ OK ]
  - 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)                [ DIFFERENT ]
    - kernel.sysrq (exp: 0)                             [ DIFFERENT ]
    - kernel.unprivileged_bpf_disabled (exp: 1)         [ DIFFERENT ]
    - kernel.yama.ptrace_scope (exp: 1 2 3)             [ DIFFERENT ]
    - net.ipv4.conf.all.accept_redirects (exp: 0)       [ OK ]
    - net.ipv4.conf.all.accept_source_route (exp: 0)    [ OK ]
    - net.ipv4.conf.all.bootp_relay (exp: 0)            [ OK ]
    - net.ipv4.conf.all.forwarding (exp: 0)             [ DIFFERENT ]
    - net.ipv4.conf.all.log_martians (exp: 1)           [ DIFFERENT ]
    - net.ipv4.conf.all.mc_forwarding (exp: 0)          [ OK ]
    - net.ipv4.conf.all.proxy_arp (exp: 0)              [ OK ]
    - net.ipv4.conf.all.rp_filter (exp: 1)              [ DIFFERENT ]
    - net.ipv4.conf.all.send_redirects (exp: 0)         [ DIFFERENT ]
    - net.ipv4.conf.default.accept_redirects (exp: 0)   [ OK ]
    - net.ipv4.conf.default.accept_source_route (exp: 0)  [ OK ]
    - net.ipv4.conf.default.log_martians (exp: 1)       [ DIFFERENT ]
    - net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)     [ OK ]
    - net.ipv4.icmp_ignore_bogus_error_responses (exp: 1)  [ OK ]
    - net.ipv4.tcp_syncookies (exp: 1)                  [ OK ]
    - net.ipv4.tcp_timestamps (exp: 0 1)                [ OK ]
    - net.ipv6.conf.all.accept_redirects (exp: 0)       [ OK ]
    - net.ipv6.conf.all.accept_source_route (exp: 0)    [ OK ]
```

```
   - net.ipv6.conf.default.accept_redirects (exp: 0)        [ OK ]
   - net.ipv6.conf.default.accept_source_route (exp: 0)     [ OK ]

[+] Hardening
----------------------------------
   - Installed compiler(s)                          [ NOT FOUND ]
   - Installed malware scanner                        [ NOT FOUND ]
   - Non-native binary formats                        [ NOT FOUND ]

[+] Custom tests
----------------------------------
  - Running custom tests...                          [ NONE ]

[+] Plugins (phase 2)
----------------------------------
  - Plugins (phase 2)                               [ DONE ]

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

  -[ Lynis 3.1.6 Results ]-

  Warnings (3):
  ----------------------------
  ! Redis configuration file /etc/redis/redis.conf is world readable and might leak sensitive
details [DBS-1882]
    - Details  : /etc/redis/redis.conf
    - Solution : Use chmod 640 to change file permissions
      https://cisofy.com/lynis/controls/DBS-1882/

  ! klogd is not running, which could lead to missing kernel messages in log files
[LOGG-2138]
      https://cisofy.com/lynis/controls/LOGG-2138/

  ! Found one or more cronjob files with incorrect file permissions (see log for details)
[SCHD-7704]
      https://cisofy.com/lynis/controls/SCHD-7704/

  Suggestions (58):
  ----------------------------
  * 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/

  * Determine why /vmlinuz or /boot/vmlinuz is missing on this Debian/Ubuntu system.
[KRNL-5788]
    - Details  : /vmlinuz or /boot/vmlinuz
```

- Related resources
* Website: https://cisofy.com/lynis/controls/KRNL-5788/

* If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
- Related resources
* 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/

* 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/

* Look at the locked accounts and consider removing them [AUTH-9284]
- Related resources
* Website: https://cisofy.com/lynis/controls/AUTH-9284/

* 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 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 /tmp file system, place /tmp 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/

  * 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 DNS configuration for the dns domain name [NAME-4028]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/NAME-4028/

  * 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/

  * 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/
```

```
  * Found a configuration error in Postfix [MAIL-8817]
    - Details  : /etc/postfix/main.cf
    - Solution : run postconf > /dev/null
    - Related resources
      * Article: Postfix Hardening Guide for Security and Privacy:
https://linux-audit.com/postfix-hardening-guide-for-security-and-privacy/
      * Website: https://cisofy.com/lynis/controls/MAIL-8817/

  * Disable the 'VRFY' command [MAIL-8820:disable_vrfy_command]
    - Details  : disable_vrfy_command=no
    - Solution : run postconf -e disable_vrfy_command=yes to change the value
    - Related resources
      * Article: Postfix Hardening Guide for Security and Privacy:
https://linux-audit.com/postfix-hardening-guide-for-security-and-privacy/
      * Website: https://cisofy.com/lynis/controls/MAIL-8820/

  * Check iptables rules to see which rules are currently not used [FIRE-4513]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/FIRE-4513/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowTcpForwarding (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : ClientAliveCountMax (set 3 to 2)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : GatewayPorts (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : LogLevel (set INFO to VERBOSE)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxAuthTries (set 6 to 3)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
```

```
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxSessions (set 10 to 2)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitRootLogin (set YES to
(FORCED-COMMANDS-ONLY|NO|PROHIBIT-PASSWORD|WITHOUT-PASSWORD))
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitUserEnvironment (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitTunnel (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Port (set 22 to )
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : StrictModes (set NO to YES)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : TCPKeepAlive (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : X11Forwarding (set YES to NO)
```

- Related resources
  * Article: OpenSSH security and hardening: https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
  * Website: https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
  - Details : AllowAgentForwarding (set YES to NO)
  - Related resources
    * Article: OpenSSH security and hardening: https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
    * Website: https://cisofy.com/lynis/controls/SSH-7408/

* Configure the 'requirepass' setting for Redis [DBS-1884]
  - Details : /etc/redis/redis.conf
  - Solution : configure 'requirepass' setting in /etc/redis/redis.conf
  - Related resources
    * Website: https://cisofy.com/lynis/controls/DBS-1884/

* Use the 'rename-command CONFIG' setting for Redis [DBS-1886]
  - Details : /etc/redis/redis.conf
  - Solution : configure 'rename-command CONFIG' in /etc/redis/redis.conf
  - Related resources
    * Website: https://cisofy.com/lynis/controls/DBS-1886/

* Use 'bind' setting to listen on localhost for Redis instance [DBS-1888]
  - Details : /etc/redis/redis.conf
  - Solution : configure 'bind localhost' in /etc/redis/redis.conf
  - Related resources
    * Website: https://cisofy.com/lynis/controls/DBS-1888/

* Check if any syslog daemon is running and correctly configured. [LOGG-2130]
  - Related resources
    * Website: https://cisofy.com/lynis/controls/LOGG-2130/

* Although inetd is not running, make sure no services are enabled in /etc/inetd.conf, or remove inetd service [INSE-8006]
  - Related resources
    * Website: https://cisofy.com/lynis/controls/INSE-8006/

* If there are no xinetd services required, it is recommended that the daemon be removed [INSE-8100]
  - Related resources
    * Website: https://cisofy.com/lynis/controls/INSE-8100/

* Removing the telnet server package and replace with SSH when possible [INSE-8322]
  - Related resources
    * Website: https://cisofy.com/lynis/controls/INSE-8322/

* 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 (no results) [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-con
figuration/
      * 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/

  * 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 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/
    * 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:
  ----------------------------
  - 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:

  Scan mode:
  Normal [■]  Forensics [ ]  Integration [ ]  Pentest [ ]

  Lynis modules:
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]

  Details:
  Hardening index : 52 [##########          ]
  Tests performed : 254
  Plugins enabled : 2

  Software components:
  - Firewall               [V]
  - Intrusion software     [X]
  - Malware scanner        [X]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

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

  Exceptions found
  Some exceptional events or information was found!

  What to do:
  You can help by providing your log file (/var/log/lynis.log).
  Go to https://cisofy.com/contact/ and send your file to the e-mail address listed

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

  Lynis 3.1.6
```

```
  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2025, 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
/opt/lynis/default.prf for all settings)
```

Salida 6: Escaneo final de warngins volver al indice

```
root@linux-target:/opt/lynis# ./lynis audit system

[ Lynis 3.1.6 ]

################################################################################
  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.

  2007-2025, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                     [ DONE ]
  - Checking profiles...                                [ DONE ]

  ---------------------------------------------------
  Program version:           3.1.6
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  22.04
  End-of-life:               NO
  Kernel version:            6.12.38+kali
  Hardware platform:         x86_64
  Hostname:                  linux-target
  ---------------------------------------------------
  Profiles:                  /opt/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          ./plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
```

```
  Language:                en
  Test category:           all
  Test group:              all
  ---------------------------------------------------
  - Program update status...                          [ SKIPPED ]

[+] 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: pam
    [..]
  - Plugin: systemd
    [.System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
.............System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
..]

[+] Boot and services
------------------------------------
  - Service Manager                                   [ upstart ]
  - Checking UEFI boot                                [ DISABLED ]
    - Boot loader                                     [ NONE FOUND ]
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
  - Check running services (systemctl)                [ DONE ]
        Result: found 0 running services
  - Check enabled services at boot (systemctl)        [ DONE ]
        Result: found 11 enabled services
  - Check startup files (permissions)                 [ OK ]
  - Running 'systemd-analyze security'
      Unit name (exposure value) and predicate
      ------------------------------
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down

[+] 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 Linux kernel configuration file          [ NOT FOUND ]
/usr/bin/grep: /etc/kernel-img.conf: No such file or directory
  - Checking core dumps configuration
    - configuration in /etc/profile                   [ DEFAULT ]
    - 'hard' configuration in /etc/security/limits.conf  [ ENABLED ]
    - 'soft' configuration in /etc/security/limits.conf  [ ENABLED ]
```

```
    - Checking setuid core dumps configuration               [ DISABLED ]
  - Check if reboot is needed                              [ UNKNOWN ]

[+] 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                        [ WARNING ]
    - Permissions for: /etc/sudoers.d/README               [ 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                                        [ FOUND ]
  - 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                          [ ENABLED ]

[+] Kerberos
------------------------------------
  - Check for Kerberos KDC and principals                  [ NOT FOUND ]

[+] Shells
------------------------------------
  - Checking shells from /etc/shells
    Result: found 8 shells (valid shells: 8).
    - Session timeout settings/tools                       [ NONE ]
```

```
  - Checking default umask values
    - Checking default umask in /etc/bash.bashrc              [ WEAK ]
    - Checking default umask in /etc/profile                  [ NONE ]

[+] File systems
------------------------------------
  - Checking mount points
    - Checking /home mount point                              [ SUGGESTION ]
    - Checking /tmp mount point                               [ SUGGESTION ]
    - Checking /var mount point                               [ SUGGESTION ]
  - Query swap partitions (fstab)                             [ NONE ]
  - 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 /dev                                     [ PARTIALLY HARDENED ]
  - Mount options of /dev/shm                                 [ HARDENED ]
  - Total without nodev:7 noexec:6 nosuid:5 ro or noexec (W^X): 6 of total 12

[+] 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
------------------------------------
  - Check running NFS daemon                                  [ NOT FOUND ]

[+] Name services
------------------------------------
  - Checking search domains                                   [ FOUND ]
  - Checking /etc/resolv.conf options                         [ FOUND ]
  - Searching DNS domain name                                 [ UNKNOWN ]
  - 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 dpkg package manager                          [ FOUND ]
      - Querying package manager
    - Query unpurged packages                                 [ NONE ]
  - Checking security repository in sources.list file         [ OK ]
  - Checking APT package database                             [ OK ]
```

```
  - Checking vulnerable packages (apt-get only)               [ DONE ]
  - Checking upgradeable packages                           [ SKIPPED ]
  - Checking package audit tool                           [ INSTALLED ]
    Found: apt-get

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

  Exception found!

  Function/test:  [PKGS-7410]
  Message:        Could not find any kernel packages via package manager

  Help improving the Lynis community with your feedback!

  Steps:
  - Ensure you are running the latest version (./lynis update check)
  - If so, create a GitHub issue at https://github.com/CISOfy/lynis
  - Include relevant parts of the log file or configuration file

  Thanks!

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

  - Toolkit for automatic upgrades                        [ NOT FOUND ]

[+] Networking
------------------------------------
  - Checking IPv6 configuration                           [ ENABLED ]
      Configuration method                              [ AUTO ]
      IPv6 only                                   [ NO ]
  - Checking configured nameservers
    - Testing nameservers
      Nameserver: 127.0.0.11                          [ SKIPPED ]
    - Minimal of 2 responsive nameservers                 [ SKIPPED ]
    - DNSSEC supported (systemd-resolved)                   [ UNKNOWN ]
  - Checking default gateway                            [ DONE ]

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

  Exception found!

  Function/test:  [NETW-3004:1]
  Message:        No interfaces found on this system (OS=Linux)

  Help improving the Lynis community with your feedback!

  Steps:
  - Ensure you are running the latest version (./lynis update check)
  - If so, create a GitHub issue at https://github.com/CISOfy/lynis
  - Include relevant parts of the log file or configuration file

  Thanks!

================================================================
```

```
  - Getting listening ports (TCP/UDP)                    [ DONE ]
  - Checking promiscuous interfaces                      [ UNKNOWN ]
  - 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
------------------------------------
  - Postfix status                                       [ RUNNING ]
    - Postfix configuration                              [ FOUND ]
      - Postfix configuration errors                     [ WARNING ]

[+] Software: firewalls
------------------------------------
  - Checking iptables support                            [ FOUND ]
    - Checking iptables policies of chains               [ FOUND ]
      - Chain INPUT (table: filter, target: DROP)        [ DROP ]
      - Chain INPUT (table: security, target: ACCEPT)    [ ACCEPT ]
    - Checking for empty ruleset                         [ OK ]
    - Checking for unused rules                          [ FOUND ]
  - Checking host based firewall                         [ ACTIVE ]

[+] Software: webserver
------------------------------------
  - Checking Apache                                      [ NOT FOUND ]
  - Checking nginx                                       [ NOT FOUND ]

[+] SSH Support
------------------------------------
  - Checking running SSH daemon                          [ FOUND ]
    - Searching SSH configuration                        [ FOUND ]
    - OpenSSH option: AllowTcpForwarding                 [ SUGGESTION ]
    - OpenSSH option: ClientAliveCountMax                [ SUGGESTION ]
    - OpenSSH option: ClientAliveInterval                [ OK ]
    - OpenSSH option: FingerprintHash                    [ OK ]
    - OpenSSH option: GatewayPorts                       [ SUGGESTION ]
    - OpenSSH option: IgnoreRhosts                       [ OK ]
    - OpenSSH option: LoginGraceTime                     [ OK ]
    - OpenSSH option: LogLevel                           [ SUGGESTION ]
    - OpenSSH option: MaxAuthTries                       [ SUGGESTION ]
    - OpenSSH option: MaxSessions                        [ SUGGESTION ]
    - OpenSSH option: PermitRootLogin                    [ SUGGESTION ]
    - OpenSSH option: PermitUserEnvironment              [ SUGGESTION ]
    - OpenSSH option: PermitTunnel                       [ SUGGESTION ]
    - OpenSSH option: Port                               [ SUGGESTION ]
    - OpenSSH option: PrintLastLog                       [ OK ]
    - OpenSSH option: StrictModes                        [ SUGGESTION ]
```

```
   - OpenSSH option: TCPKeepAlive                    [ SUGGESTION ]
   - OpenSSH option: UseDNS                          [ OK ]
   - OpenSSH option: X11Forwarding                   [ SUGGESTION ]
   - OpenSSH option: AllowAgentForwarding            [ SUGGESTION ]
   - OpenSSH option: AllowUsers                      [ NOT FOUND ]
   - OpenSSH option: AllowGroups                     [ NOT FOUND ]

[+] SNMP Support
------------------------------------
  - Checking running SNMP daemon                     [ NOT FOUND ]

[+] Databases
------------------------------------
  - Redis (server) status                            [ FOUND ]
    - Redis (requirepass configured)                 [ NOT FOUND ]
    - Redis (rename of CONFIG command)               [ NOT FOUND ]
    - Redis (bind on localhost)                      [ NOT FOUND ]

[+] LDAP Services
------------------------------------
  - Checking OpenLDAP instance                       [ NOT FOUND ]

[+] PHP
------------------------------------
  - Checking PHP                                     [ NOT FOUND ]

[+] 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                [ NOT FOUND ]
    - Checking Metalog status                        [ NOT FOUND ]
    - Checking RSyslog status                        [ FOUND ]
    - Checking RFC 3195 daemon status                [ NOT FOUND ]
    - Checking minilogd instances                    [ NOT FOUND ]
    - Checking wazuh-agent daemon status             [ NOT FOUND ]
  - Checking logrotate presence                      [ OK ]
  - Checking remote logging                          [ NOT ENABLED ]
  - Checking log directories (static list)           [ DONE ]
  - Checking open log files                          [ SKIPPED ]

[+] Insecure services
------------------------------------
  - Installed inetd package                          [ NOT FOUND ]
    - Checking enabled inetd services                [ SUGGESTION ]
  - Installed xinetd package                         [ FOUND ]
    - xinetd status                                  [ NOT ACTIVE ]
      - Enabled xinetd.d services                    [ NOT FOUND ]
  - Installed rsh client package                     [ OK ]
  - Installed rsh server package                     [ OK ]
```

```
  - Installed telnet client package                [ OK ]
  - Installed telnet server package                [ FOUND ]
  - Checking NIS client installation               [ OK ]
  - Checking NIS server installation               [ OK ]
  - Checking TFTP client installation              [ OK ]
  - Checking TFTP server installation              [ OK ]

[+] 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               [ NOT FOUND ]
  - Checking auditd                                [ NOT FOUND ]

[+] Time and Synchronization
-----------------------------------

[+] Cryptography
-----------------------------------
  - Checking for expired SSL certificates [0/149]  [ NONE ]

  [WARNING]: Test CRYP-7902 had a long execution: 10.831699 seconds

  - Kernel entropy is sufficient                   [ YES ]
  - HW RNG & rngd                                  [ NO ]
  - SW prng                                        [ NO ]
  - MOR variable not found                         [ WEAK ]

[+] Virtualization
-----------------------------------

[+] Containers
-----------------------------------

[+] Security frameworks
-----------------------------------
  - Checking presence AppArmor                     [ NOT FOUND ]
  - 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
  - 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: /etc/crontab                              [ OK ]
    File: /etc/group                                [ SUGGESTION ]
    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                               [ SUGGESTION ]
    File: /etc/passwd-                              [ SUGGESTION ]
    File: /etc/ssh/sshd_config                      [ SUGGESTION ]
    Directory: /root/.ssh                           [ 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
------------------------------------
  - Permissions of home directories                     [ OK ]
  - 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)                    [ DIFFERENT ]
   - kernel.sysrq (exp: 0)                                 [ DIFFERENT ]
   - kernel.unprivileged_bpf_disabled (exp: 1)             [ DIFFERENT ]
   - kernel.yama.ptrace_scope (exp: 1 2 3)                 [ DIFFERENT ]
   - net.ipv4.conf.all.accept_redirects (exp: 0)           [ OK ]
   - net.ipv4.conf.all.accept_source_route (exp: 0)        [ OK ]
   - net.ipv4.conf.all.bootp_relay (exp: 0)                [ OK ]
   - net.ipv4.conf.all.forwarding (exp: 0)                 [ DIFFERENT ]
   - net.ipv4.conf.all.log_martians (exp: 1)               [ DIFFERENT ]
   - net.ipv4.conf.all.mc_forwarding (exp: 0)              [ OK ]
   - net.ipv4.conf.all.proxy_arp (exp: 0)                  [ OK ]
   - net.ipv4.conf.all.rp_filter (exp: 1)                  [ DIFFERENT ]
   - net.ipv4.conf.all.send_redirects (exp: 0)             [ DIFFERENT ]
   - net.ipv4.conf.default.accept_redirects (exp: 0)       [ OK ]
   - net.ipv4.conf.default.accept_source_route (exp: 0)    [ OK ]
   - net.ipv4.conf.default.log_martians (exp: 1)           [ DIFFERENT ]
   - net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)         [ OK ]
   - net.ipv4.icmp_ignore_bogus_error_responses (exp: 1)   [ OK ]
   - net.ipv4.tcp_syncookies (exp: 1)                      [ OK ]
   - net.ipv4.tcp_timestamps (exp: 0 1)                    [ OK ]
   - net.ipv6.conf.all.accept_redirects (exp: 0)           [ OK ]
   - net.ipv6.conf.all.accept_source_route (exp: 0)        [ OK ]
   - net.ipv6.conf.default.accept_redirects (exp: 0)       [ OK ]
   - net.ipv6.conf.default.accept_source_route (exp: 0)    [ OK ]

[+] Hardening
------------------------------------
   - Installed compiler(s)                                 [ NOT FOUND ]
   - Installed malware scanner                             [ NOT FOUND ]
   - Non-native binary formats                             [ NOT FOUND ]

[+] Custom tests
------------------------------------
  - Running custom tests...                                [ NONE ]

[+] Plugins (phase 2)
------------------------------------
  - Plugins (phase 2)                                      [ DONE ]

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

  -[ Lynis 3.1.6 Results ]-

  Great, no warnings

  Suggestions (58):
  -----------------------------
  * 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/

* Determine why /vmlinuz or /boot/vmlinuz is missing on this Debian/Ubuntu system. [KRNL-5788]
- Details : /vmlinuz or /boot/vmlinuz
- Related resources
* Website: https://cisofy.com/lynis/controls/KRNL-5788/

* If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
- Related resources
* 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/

* 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/

* Look at the locked accounts and consider removing them [AUTH-9284]
- Related resources
* Website: https://cisofy.com/lynis/controls/AUTH-9284/

* 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 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 /tmp file system, place /tmp 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/

* 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 DNS configuration for the dns domain name [NAME-4028]
- Related resources
* Website: https://cisofy.com/lynis/controls/NAME-4028/

* 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/

* 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/

  * Found a configuration error in Postfix [MAIL-8817]
    - Details  : /etc/postfix/main.cf
    - Solution : run postconf > /dev/null
    - Related resources
      * Article: Postfix Hardening Guide for Security and Privacy:
https://linux-audit.com/postfix-hardening-guide-for-security-and-privacy/
      * Website: https://cisofy.com/lynis/controls/MAIL-8817/

  * Disable the 'VRFY' command [MAIL-8820:disable_vrfy_command]
    - Details  : disable_vrfy_command=no
    - Solution : run postconf -e disable_vrfy_command=yes to change the value
    - Related resources
      * Article: Postfix Hardening Guide for Security and Privacy:
https://linux-audit.com/postfix-hardening-guide-for-security-and-privacy/
      * Website: https://cisofy.com/lynis/controls/MAIL-8820/

  * Check iptables rules to see which rules are currently not used [FIRE-4513]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/FIRE-4513/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowTcpForwarding (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : ClientAliveCountMax (set 3 to 2)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : GatewayPorts (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : LogLevel (set INFO to VERBOSE)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
```

```
     * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxAuthTries (set 6 to 3)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxSessions (set 10 to 2)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitRootLogin (set YES to
(FORCED-COMMANDS-ONLY|NO|PROHIBIT-PASSWORD|WITHOUT-PASSWORD))
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitUserEnvironment (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitTunnel (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Port (set 22 to )
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : StrictModes (set NO to YES)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : TCPKeepAlive (set YES to NO)
```

- Related resources
* Article: OpenSSH security and hardening: https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
* Website: https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : X11Forwarding (set YES to NO)
- Related resources
* Article: OpenSSH security and hardening: https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
* Website: https://cisofy.com/lynis/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : AllowAgentForwarding (set YES to NO)
- Related resources
* Article: OpenSSH security and hardening: https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
* Website: https://cisofy.com/lynis/controls/SSH-7408/

* Configure the 'requirepass' setting for Redis [DBS-1884]
- Details : /etc/redis/redis.conf
- Solution : configure 'requirepass' setting in /etc/redis/redis.conf
- Related resources
* Website: https://cisofy.com/lynis/controls/DBS-1884/

* Use the 'rename-command CONFIG' setting for Redis [DBS-1886]
- Details : /etc/redis/redis.conf
- Solution : configure 'rename-command CONFIG' in /etc/redis/redis.conf
- Related resources
* Website: https://cisofy.com/lynis/controls/DBS-1886/

* Use 'bind' setting to listen on localhost for Redis instance [DBS-1888]
- Details : /etc/redis/redis.conf
- Solution : configure 'bind localhost' in /etc/redis/redis.conf
- Related resources
* Website: https://cisofy.com/lynis/controls/DBS-1888/

* 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/

* Although inetd is not running, make sure no services are enabled in /etc/inetd.conf, or remove inetd service [INSE-8006]
- Related resources
* Website: https://cisofy.com/lynis/controls/INSE-8006/

* If there are no xinetd services required, it is recommended that the daemon be removed [INSE-8100]
- Related resources
* Website: https://cisofy.com/lynis/controls/INSE-8100/

* Removing the telnet server package and replace with SSH when possible [INSE-8322]
- Related resources

```
      * Website: https://cisofy.com/lynis/controls/INSE-8322/

  * 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 (no results) [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-con
figuration/
      * 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/

  * 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 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/
      * 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:
  ----------------------------
  - 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:

  Scan mode:
  Normal [■]  Forensics [ ]  Integration [ ]  Pentest [ ]

  Lynis modules:
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]

  Details:
  Hardening index : 54 [###########          ]
  Tests performed : 255
  Plugins enabled : 2

  Software components:
  - Firewall               [V]
  - Intrusion software     [X]
  - Malware scanner        [X]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

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

  Exceptions found
  Some exceptional events or information was found!
```

```
  What to do:
  You can help by providing your log file (/var/log/lynis.log).
  Go to https://cisofy.com/contact/ and send your file to the e-mail address listed

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

  Lynis 3.1.6

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2025, 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
/opt/lynis/default.prf for all settings)
```

Salida 7: Escaneo arreglando sugerencias volver al indice

```
root@linux-target:/opt/lynis# ./lynis audit system

[ Lynis 3.1.6 ]

################################################################################
  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.

  2007-2025, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                     [ DONE ]
  - Checking profiles...                                [ DONE ]

  ---------------------------------------------------
  Program version:           3.1.6
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  22.04
  End-of-life:               NO
  Kernel version:            6.12.38+kali
  Hardware platform:         x86_64
  Hostname:                  linux-target
```

```
  ---------------------------------------------------
  Profiles:               /opt/lynis/default.prf
  Log file:               /var/log/lynis.log
  Report file:             /var/log/lynis-report.dat
  Report version:           1.0
  Plugin directory:         ./plugins
  ---------------------------------------------------
  Auditor:                [Not Specified]
  Language:                 en
  Test category:            all
  Test group:               all
  ---------------------------------------------------
  - Program update status...                      [ SKIPPED ]

[+] 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: pam
    [..]
  - Plugin: systemd
    [.System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
.............System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
..]

[+] Boot and services
------------------------------------
  - Service Manager                               [ upstart ]
  - Checking UEFI boot                             [ DISABLED ]
    - Boot loader                                [ NONE FOUND ]
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
  - Check running services (systemctl)                [ DONE ]
        Result: found 0 running services
  - Check enabled services at boot (systemctl)          [ DONE ]
        Result: found 11 enabled services
  - Check startup files (permissions)                 [ OK ]
  - Running 'systemd-analyze security'
      Unit name (exposure value) and predicate
      ------------------------------
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down

[+] 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 Linux kernel configuration file                 [ NOT FOUND ]
/usr/bin/grep: /etc/kernel-img.conf: No such file or directory
  - Checking core dumps configuration
    - configuration in /etc/profile                          [ DEFAULT ]
    - 'hard' configuration in /etc/security/limits.conf      [ ENABLED ]
    - 'soft' configuration in /etc/security/limits.conf      [ ENABLED ]
    - Checking setuid core dumps configuration               [ DISABLED ]
  - Check if reboot is needed                                [ UNKNOWN ]

[+] 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 ]
  - Password hashing rounds (minimum)                        [ CONFIGURED ]
  - 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              [ OK ]
    - Permissions for: /etc/sudoers                          [ OK ]
    - Permissions for: /etc/sudoers.d/README                 [ 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                                          [ FOUND ]
  - User password aging (minimum)                            [ CONFIGURED ]
  - User password aging (maximum)                            [ CONFIGURED ]
  - 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                            [ ENABLED ]

[+] Kerberos
```

```
---------------------------------
  - Check for Kerberos KDC and principals                    [ NOT FOUND ]

[+] Shells
---------------------------------
  - Checking shells from /etc/shells
    Result: found 8 shells (valid shells: 8).
    - Session timeout settings/tools                         [ NONE ]
  - Checking default umask values
    - Checking default umask in /etc/bash.bashrc             [ WEAK ]
    - Checking default umask in /etc/profile                 [ NONE ]

[+] File systems
---------------------------------
  - Checking mount points
    - Checking /home mount point                             [ SUGGESTION ]
    - Checking /tmp mount point                              [ SUGGESTION ]
    - Checking /var mount point                              [ SUGGESTION ]
  - Query swap partitions (fstab)                            [ NONE ]
  - 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 /dev                                    [ PARTIALLY HARDENED ]
  - Mount options of /dev/shm                                [ HARDENED ]
  - Total without nodev:7 noexec:6 nosuid:5 ro or noexec (W^X): 6 of total 12

[+] 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
---------------------------------
  - Check running NFS daemon                                 [ NOT FOUND ]

[+] Name services
---------------------------------
  - Checking search domains                                  [ FOUND ]
  - Checking /etc/resolv.conf options                        [ FOUND ]
  - Searching DNS domain name                                [ UNKNOWN ]
  - 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 dpkg package manager                [ FOUND ]
      - Querying package manager
    - Query unpurged packages                       [ NONE ]
  - Checking security repository in sources.list file  [ OK ]
  - Checking APT package database                   [ OK ]
  - Checking vulnerable packages (apt-get only)       [ DONE ]
  - Checking upgradeable packages                   [ SKIPPED ]
  - Checking package audit tool                     [ INSTALLED ]
    Found: apt-get

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

  Exception found!

  Function/test:  [PKGS-7410]
  Message:        Could not find any kernel packages via package manager

  Help improving the Lynis community with your feedback!

  Steps:
  - Ensure you are running the latest version (./lynis update check)
  - If so, create a GitHub issue at https://github.com/CISOfy/lynis
  - Include relevant parts of the log file or configuration file

  Thanks!

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

  - Toolkit for automatic upgrades                  [ NOT FOUND ]

[+] Networking
------------------------------------
  - Checking IPv6 configuration                     [ ENABLED ]
      Configuration method                        [ AUTO ]
      IPv6 only                                 [ NO ]
  - Checking configured nameservers
    - Testing nameservers
      Nameserver: 127.0.0.11                    [ SKIPPED ]
    - Minimal of 2 responsive nameservers           [ SKIPPED ]
    - DNSSEC supported (systemd-resolved)             [ UNKNOWN ]
  - Checking default gateway                    [ DONE ]

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

  Exception found!

  Function/test:  [NETW-3004:1]
  Message:        No interfaces found on this system (OS=Linux)

  Help improving the Lynis community with your feedback!
```

```
  Steps:
  - Ensure you are running the latest version (./lynis update check)
  - If so, create a GitHub issue at https://github.com/CISOfy/lynis
  - Include relevant parts of the log file or configuration file

  Thanks!

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

  - Getting listening ports (TCP/UDP)                    [ DONE ]
  - Checking promiscuous interfaces                      [ UNKNOWN ]
  - 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
------------------------------------
  - Postfix status                                       [ RUNNING ]
    - Postfix configuration                              [ FOUND ]
      - Postfix configuration errors                     [ WARNING ]

[+] Software: firewalls
------------------------------------
  - Checking iptables support                            [ FOUND ]
    - Checking iptables policies of chains               [ FOUND ]
      - Chain INPUT (table: filter, target: DROP)        [ DROP ]
      - Chain INPUT (table: security, target: ACCEPT)    [ ACCEPT ]
    - Checking for empty ruleset                         [ OK ]
    - Checking for unused rules                          [ FOUND ]
  - Checking host based firewall                         [ ACTIVE ]

[+] Software: webserver
------------------------------------
  - Checking Apache                                      [ NOT FOUND ]
  - Checking nginx                                       [ NOT FOUND ]

[+] SSH Support
------------------------------------
  - Checking running SSH daemon                          [ FOUND ]
    - Searching SSH configuration                        [ FOUND ]
    - OpenSSH option: AllowTcpForwarding                 [ SUGGESTION ]
    - OpenSSH option: ClientAliveCountMax                [ SUGGESTION ]
    - OpenSSH option: ClientAliveInterval                [ OK ]
    - OpenSSH option: FingerprintHash                    [ OK ]
    - OpenSSH option: GatewayPorts                       [ SUGGESTION ]
    - OpenSSH option: IgnoreRhosts                       [ OK ]
    - OpenSSH option: LoginGraceTime                     [ OK ]
    - OpenSSH option: LogLevel                           [ SUGGESTION ]
```

```
   - OpenSSH option: MaxAuthTries                    [ SUGGESTION ]
   - OpenSSH option: MaxSessions                     [ SUGGESTION ]
   - OpenSSH option: PermitRootLogin                 [ SUGGESTION ]
   - OpenSSH option: PermitUserEnvironment           [ SUGGESTION ]
   - OpenSSH option: PermitTunnel                    [ SUGGESTION ]
   - OpenSSH option: Port                            [ SUGGESTION ]
   - OpenSSH option: PrintLastLog                    [ OK ]
   - OpenSSH option: StrictModes                     [ SUGGESTION ]
   - OpenSSH option: TCPKeepAlive                    [ SUGGESTION ]
   - OpenSSH option: UseDNS                          [ OK ]
   - OpenSSH option: X11Forwarding                   [ SUGGESTION ]
   - OpenSSH option: AllowAgentForwarding            [ SUGGESTION ]
   - OpenSSH option: AllowUsers                      [ NOT FOUND ]
   - OpenSSH option: AllowGroups                     [ NOT FOUND ]

[+] SNMP Support
------------------------------------
  - Checking running SNMP daemon                     [ NOT FOUND ]

[+] Databases
------------------------------------
  - Redis (server) status                           [ FOUND ]
    - Redis (requirepass configured)                [ NOT FOUND ]
    - Redis (rename of CONFIG command)              [ NOT FOUND ]
    - Redis (bind on localhost)                     [ NOT FOUND ]

[+] LDAP Services
------------------------------------
  - Checking OpenLDAP instance                      [ NOT FOUND ]

[+] PHP
------------------------------------
  - Checking PHP                                    [ NOT FOUND ]

[+] 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               [ NOT FOUND ]
    - Checking Metalog status                       [ NOT FOUND ]
    - Checking RSyslog status                       [ FOUND ]
    - Checking RFC 3195 daemon status               [ NOT FOUND ]
    - Checking minilogd instances                   [ NOT FOUND ]
    - Checking wazuh-agent daemon status            [ NOT FOUND ]
  - Checking logrotate presence                     [ OK ]
  - Checking remote logging                         [ NOT ENABLED ]
  - Checking log directories (static list)          [ DONE ]
  - Checking open log files                         [ SKIPPED ]

[+] Insecure services
```

```
------------------------------------
  - Installed inetd package                 [ NOT FOUND ]
    - Checking enabled inetd services          [ SUGGESTION ]
  - Installed xinetd package                [ FOUND ]
    - xinetd status                       [ NOT ACTIVE ]
      - Enabled xinetd.d services          [ NOT FOUND ]
  - Installed rsh client package            [ OK ]
  - Installed rsh server package            [ OK ]
  - Installed telnet client package         [ OK ]
  - Installed telnet server package          [ FOUND ]
  - Checking NIS client installation         [ OK ]
  - Checking NIS server installation          [ OK ]
  - Checking TFTP client installation         [ OK ]
  - Checking TFTP server installation          [ OK ]

[+] 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          [ NOT FOUND ]
  - Checking auditd                        [ NOT FOUND ]

[+] Time and Synchronization
------------------------------------

[+] Cryptography
------------------------------------
  - Checking for expired SSL certificates [0/149]      [ NONE ]

  [WARNING]: Test CRYP-7902 had a long execution: 12.011810 seconds

  - Kernel entropy is sufficient            [ YES ]
  - HW RNG & rngd                          [ NO ]
  - SW prng                             [ NO ]
  - MOR variable not found                  [ WEAK ]

[+] Virtualization
------------------------------------

[+] Containers
------------------------------------

[+] Security frameworks
------------------------------------
```

```
  - Checking presence AppArmor                          [ NOT FOUND ]
  - 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
  - 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: /etc/crontab                                  [ OK ]
    File: /etc/group                                    [ SUGGESTION ]
    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                                   [ SUGGESTION ]
    File: /etc/passwd-                                  [ SUGGESTION ]
    File: /etc/ssh/sshd_config                          [ SUGGESTION ]
    Directory: /root/.ssh                               [ 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
------------------------------------
  - Permissions of home directories                     [ OK ]
  - 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)                [ DIFFERENT ]
   - kernel.sysrq (exp: 0)                             [ DIFFERENT ]
   - kernel.unprivileged_bpf_disabled (exp: 1)         [ DIFFERENT ]
   - kernel.yama.ptrace_scope (exp: 1 2 3)             [ DIFFERENT ]
   - net.ipv4.conf.all.accept_redirects (exp: 0)       [ OK ]
   - net.ipv4.conf.all.accept_source_route (exp: 0)    [ OK ]
   - net.ipv4.conf.all.bootp_relay (exp: 0)            [ OK ]
   - net.ipv4.conf.all.forwarding (exp: 0)             [ DIFFERENT ]
   - net.ipv4.conf.all.log_martians (exp: 1)           [ DIFFERENT ]
   - net.ipv4.conf.all.mc_forwarding (exp: 0)          [ OK ]
   - net.ipv4.conf.all.proxy_arp (exp: 0)              [ OK ]
   - net.ipv4.conf.all.rp_filter (exp: 1)              [ DIFFERENT ]
   - net.ipv4.conf.all.send_redirects (exp: 0)         [ DIFFERENT ]
   - net.ipv4.conf.default.accept_redirects (exp: 0)   [ OK ]
   - net.ipv4.conf.default.accept_source_route (exp: 0)  [ OK ]
   - net.ipv4.conf.default.log_martians (exp: 1)       [ DIFFERENT ]
   - net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)     [ OK ]
   - net.ipv4.icmp_ignore_bogus_error_responses (exp: 1)  [ OK ]
   - net.ipv4.tcp_syncookies (exp: 1)                  [ OK ]
   - net.ipv4.tcp_timestamps (exp: 0 1)                [ OK ]
   - net.ipv6.conf.all.accept_redirects (exp: 0)       [ OK ]
   - net.ipv6.conf.all.accept_source_route (exp: 0)    [ OK ]
   - net.ipv6.conf.default.accept_redirects (exp: 0)   [ OK ]
   - net.ipv6.conf.default.accept_source_route (exp: 0)  [ OK ]

[+] Hardening
------------------------------------
   - Installed compiler(s)                             [ NOT FOUND ]
   - Installed malware scanner                         [ NOT FOUND ]
   - Non-native binary formats                         [ NOT FOUND ]

[+] Custom tests
------------------------------------
  - Running custom tests...                            [ NONE ]

[+] Plugins (phase 2)
------------------------------------
  - Plugins (phase 2)                                  [ DONE ]

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

  -[ Lynis 3.1.6 Results ]-

  Great, no warnings
```

```
  Suggestions (55):
  ----------------------------
  * 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/

  * Determine why /vmlinuz or /boot/vmlinuz is missing on this Debian/Ubuntu system.
[KRNL-5788]
    - Details  : /vmlinuz or /boot/vmlinuz
    - Related resources
      * Website: https://cisofy.com/lynis/controls/KRNL-5788/

  * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file
[KRNL-5820]
    - Related resources
      * 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/

  * 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/

  * Look at the locked accounts and consider removing them [AUTH-9284]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/AUTH-9284/

  * Default umask in /etc/login.defs 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 /tmp file system, place /tmp 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/

  * 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 DNS configuration for the dns domain name [NAME-4028]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/NAME-4028/

  * 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/

  * 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/

  * Found a configuration error in Postfix [MAIL-8817]
    - Details : /etc/postfix/main.cf

```
    - Solution : run postconf > /dev/null
    - Related resources
      * Article: Postfix Hardening Guide for Security and Privacy:
https://linux-audit.com/postfix-hardening-guide-for-security-and-privacy/
      * Website: https://cisofy.com/lynis/controls/MAIL-8817/

  * Disable the 'VRFY' command [MAIL-8820:disable_vrfy_command]
    - Details  : disable_vrfy_command=no
    - Solution : run postconf -e disable_vrfy_command=yes to change the value
    - Related resources
      * Article: Postfix Hardening Guide for Security and Privacy:
https://linux-audit.com/postfix-hardening-guide-for-security-and-privacy/
      * Website: https://cisofy.com/lynis/controls/MAIL-8820/

  * Check iptables rules to see which rules are currently not used [FIRE-4513]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/FIRE-4513/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowTcpForwarding (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : ClientAliveCountMax (set 3 to 2)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : GatewayPorts (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : LogLevel (set INFO to VERBOSE)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxAuthTries (set 6 to 3)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
```

```
    - Details  : MaxSessions (set 10 to 2)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitRootLogin (set YES to
(FORCED-COMMANDS-ONLY|NO|PROHIBIT-PASSWORD|WITHOUT-PASSWORD))
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitUserEnvironment (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitTunnel (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Port (set 22 to )
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : StrictModes (set NO to YES)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : TCPKeepAlive (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : X11Forwarding (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
```

```
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowAgentForwarding (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Configure the 'requirepass' setting for Redis [DBS-1884]
    - Details  : /etc/redis/redis.conf
    - Solution : configure 'requirepass' setting in /etc/redis/redis.conf
    - Related resources
      * Website: https://cisofy.com/lynis/controls/DBS-1884/

  * Use the 'rename-command CONFIG' setting for Redis [DBS-1886]
    - Details  : /etc/redis/redis.conf
    - Solution : configure 'rename-command CONFIG' in /etc/redis/redis.conf
    - Related resources
      * Website: https://cisofy.com/lynis/controls/DBS-1886/

  * Use 'bind' setting to listen on localhost for Redis instance [DBS-1888]
    - Details  : /etc/redis/redis.conf
    - Solution : configure 'bind localhost' in /etc/redis/redis.conf
    - Related resources
      * Website: https://cisofy.com/lynis/controls/DBS-1888/

  * 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/

  * Although inetd is not running, make sure no services are enabled in /etc/inetd.conf, or
remove inetd service [INSE-8006]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/INSE-8006/

  * If there are no xinetd services required, it is recommended that the daemon be
removed [INSE-8100]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/INSE-8100/

  * Removing the telnet server package and replace with SSH when possible [INSE-8322]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/INSE-8322/

  * 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 (no results) [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-con
figuration/
      * 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/

  * 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 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/
```

```
    * 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:
  ----------------------------
  - 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:

  Scan mode:
  Normal [■]  Forensics [ ]  Integration [ ]  Pentest [ ]

  Lynis modules:
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]

  Details:
  Hardening index : 56 [###########         ]
  Tests performed : 255
  Plugins enabled : 2

  Software components:
  - Firewall               [V]
  - Intrusion software     [X]
  - Malware scanner        [X]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

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

  Exceptions found
  Some exceptional events or information was found!

  What to do:
  You can help by providing your log file (/var/log/lynis.log).
  Go to https://cisofy.com/contact/ and send your file to the e-mail address listed

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

  Lynis 3.1.6

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

```
  (Linux, macOS, BSD, and others)

  2007-2025, 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
/opt/lynis/default.prf for all settings)
```

Salida 8 Solucionando sugerencias: volver al indice

```
root@linux-target:/opt/lynis# ./lynis audit system

[ Lynis 3.1.6 ]

################################################################################
  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.

  2007-2025, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                     [ DONE ]
  - Checking profiles...                                [ DONE ]

  ---------------------------------------------------
  Program version:           3.1.6
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  22.04
  End-of-life:               NO
  Kernel version:            6.12.38+kali
  Hardware platform:         x86_64
  Hostname:                  linux-target
  ---------------------------------------------------
  Profiles:                  /opt/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          ./plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
```

```
  Test category:            all
  Test group:               all
  ------------------------------------------------
  - Program update status...                      [ SKIPPED ]

[+] 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: pam
    [..]
  - Plugin: systemd
    [.
  [WARNING]: Test PLGN-0010 had a long execution: 11.124423 seconds

System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
.............System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
..]

[+] Boot and services
------------------------------------
  - Service Manager                             [ upstart ]
  - Checking UEFI boot                          [ DISABLED ]
    - Boot loader                               [ NONE FOUND ]
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down
  - Check running services (systemctl)          [ DONE ]
        Result: found 0 running services
  - Check enabled services at boot (systemctl)  [ DONE ]
        Result: found 11 enabled services
  - Check startup files (permissions)           [ OK ]
  - Running 'systemd-analyze security'
      Unit name (exposure value) and predicate
      ------------------------------
System has not been booted with systemd as init system (PID 1). Can't operate.
Failed to connect to bus: Host is down

[+] 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 Linux kernel configuration file    [ NOT FOUND ]
/usr/bin/grep: /etc/kernel-img.conf: No such file or directory
  - Checking core dumps configuration
    - configuration in /etc/profile             [ DEFAULT ]
```

```
    - 'hard' configuration in /etc/security/limits.conf       [ ENABLED ]
    - 'soft' configuration in /etc/security/limits.conf       [ ENABLED ]
    - Checking setuid core dumps configuration                [ DISABLED ]
  - Check if reboot is needed                                 [ UNKNOWN ]

[+] 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 ]
  - Password hashing rounds (minimum)                         [ CONFIGURED ]
  - 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               [ OK ]
    - Permissions for: /etc/sudoers                           [ OK ]
    - Permissions for: /etc/sudoers.d/README                  [ 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                                           [ FOUND ]
  - User password aging (minimum)                             [ CONFIGURED ]
  - User password aging (maximum)                             [ CONFIGURED ]
  - Checking expired passwords                                [ OK ]
  - Checking Linux single user mode authentication            [ OK ]
  - Determining default umask
    - umask (/etc/profile)                                    [ NOT FOUND ]
    - umask (/etc/login.defs)                                 [ OK ]
  - LDAP authentication support                               [ NOT ENABLED ]
  - Logging failed login attempts                             [ ENABLED ]

[+] Kerberos
------------------------------------
  - Check for Kerberos KDC and principals                     [ NOT FOUND ]

[+] Shells
------------------------------------
  - Checking shells from /etc/shells
```

```
    Result: found 8 shells (valid shells: 8).
    - Session timeout settings/tools                    [ NONE ]
  - Checking default umask values
    - Checking default umask in /etc/bash.bashrc        [ WEAK ]
    - Checking default umask in /etc/profile            [ NONE ]

[+] File systems
------------------------------------
  - Checking mount points
    - Checking /home mount point                        [ SUGGESTION ]
    - Checking /tmp mount point                         [ SUGGESTION ]
    - Checking /var mount point                         [ SUGGESTION ]
  - Query swap partitions (fstab)                       [ NONE ]
  - 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 /dev                               [ PARTIALLY HARDENED ]
  - Mount options of /dev/shm                           [ HARDENED ]
  - Total without nodev:7 noexec:6 nosuid:5 ro or noexec (W^X): 6 of total 12

[+] 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
------------------------------------
  - Check running NFS daemon                            [ NOT FOUND ]

[+] Name services
------------------------------------
  - Checking search domains                             [ FOUND ]
  - Checking /etc/resolv.conf options                   [ FOUND ]
  - Searching DNS domain name                           [ UNKNOWN ]
  - 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 dpkg package manager                    [ FOUND ]
      - Querying package manager
    - Query unpurged packages                           [ NONE ]
```

```
  - Checking security repository in sources.list file         [ OK ]
  - Checking APT package database                             [ OK ]
  - Checking vulnerable packages (apt-get only)               [ DONE ]
  - Checking upgradeable packages                             [ SKIPPED ]
  - Checking package audit tool                               [ INSTALLED ]
    Found: apt-get

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

  Exception found!

  Function/test:  [PKGS-7410]
  Message:        Could not find any kernel packages via package manager

  Help improving the Lynis community with your feedback!

  Steps:
  - Ensure you are running the latest version (./lynis update check)
  - If so, create a GitHub issue at https://github.com/CISOfy/lynis
  - Include relevant parts of the log file or configuration file

  Thanks!

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

  - Toolkit for automatic upgrades                            [ NOT FOUND ]

[+] Networking
------------------------------------
  - Checking IPv6 configuration                               [ ENABLED ]
      Configuration method                                    [ AUTO ]
      IPv6 only                                               [ NO ]
  - Checking configured nameservers
    - Testing nameservers
      Nameserver: 127.0.0.11                                  [ SKIPPED ]
    - Minimal of 2 responsive nameservers                     [ SKIPPED ]
    - DNSSEC supported (systemd-resolved)                     [ UNKNOWN ]
  - Checking default gateway                                  [ DONE ]

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

  Exception found!

  Function/test:  [NETW-3004:1]
  Message:        No interfaces found on this system (OS=Linux)

  Help improving the Lynis community with your feedback!

  Steps:
  - Ensure you are running the latest version (./lynis update check)
  - If so, create a GitHub issue at https://github.com/CISOfy/lynis
  - Include relevant parts of the log file or configuration file

  Thanks!
```

```
================================================================

  - Getting listening ports (TCP/UDP)                [ DONE ]
  - Checking promiscuous interfaces                  [ UNKNOWN ]
  - 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
------------------------------------
  - Postfix status                                   [ RUNNING ]
    - Postfix configuration                          [ FOUND ]
      - Postfix configuration errors                 [ WARNING ]

[+] Software: firewalls
------------------------------------
  - Checking iptables support                        [ FOUND ]
    - Checking iptables policies of chains           [ FOUND ]
      - Chain INPUT (table: filter, target: DROP)    [ DROP ]
      - Chain INPUT (table: security, target: ACCEPT)  [ ACCEPT ]
    - Checking for empty ruleset                     [ OK ]
    - Checking for unused rules                      [ FOUND ]
  - Checking host based firewall                     [ ACTIVE ]

[+] Software: webserver
------------------------------------
  - Checking Apache                                  [ NOT FOUND ]
  - Checking nginx                                   [ NOT FOUND ]

[+] SSH Support
------------------------------------
  - Checking running SSH daemon                      [ FOUND ]
    - Searching SSH configuration                    [ FOUND ]
    - OpenSSH option: AllowTcpForwarding             [ OK ]
    - OpenSSH option: ClientAliveCountMax            [ SUGGESTION ]
    - OpenSSH option: ClientAliveInterval            [ OK ]
    - OpenSSH option: FingerprintHash                [ OK ]
    - OpenSSH option: GatewayPorts                   [ SUGGESTION ]
    - OpenSSH option: IgnoreRhosts                   [ OK ]
    - OpenSSH option: LoginGraceTime                 [ OK ]
    - OpenSSH option: LogLevel                       [ OK ]
    - OpenSSH option: MaxAuthTries                   [ OK ]
    - OpenSSH option: MaxSessions                    [ OK ]
    - OpenSSH option: PermitRootLogin                [ SUGGESTION ]
    - OpenSSH option: PermitUserEnvironment          [ SUGGESTION ]
    - OpenSSH option: PermitTunnel                   [ SUGGESTION ]
    - OpenSSH option: Port                           [ SUGGESTION ]
```

```
   - OpenSSH option: PrintLastLog                    [ OK ]
   - OpenSSH option: StrictModes                     [ OK ]
   - OpenSSH option: TCPKeepAlive                    [ OK ]
   - OpenSSH option: UseDNS                          [ OK ]
   - OpenSSH option: X11Forwarding                   [ OK ]
   - OpenSSH option: AllowAgentForwarding            [ OK ]
   - OpenSSH option: AllowUsers                      [ NOT FOUND ]
   - OpenSSH option: AllowGroups                     [ NOT FOUND ]

[+] SNMP Support
------------------------------------
  - Checking running SNMP daemon                     [ NOT FOUND ]

[+] Databases
------------------------------------
  - Redis (server) status                           [ FOUND ]
    - Redis (requirepass configured)                [ NOT FOUND ]
    - Redis (rename of CONFIG command)              [ NOT FOUND ]
    - Redis (bind on localhost)                     [ FOUND ]

[+] LDAP Services
------------------------------------
  - Checking OpenLDAP instance                      [ NOT FOUND ]

[+] PHP
------------------------------------
  - Checking PHP                                    [ NOT FOUND ]

[+] 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               [ NOT FOUND ]
    - Checking Metalog status                       [ NOT FOUND ]
    - Checking RSyslog status                       [ FOUND ]
    - Checking RFC 3195 daemon status               [ NOT FOUND ]
    - Checking minilogd instances                   [ NOT FOUND ]
    - Checking wazuh-agent daemon status            [ NOT FOUND ]
  - Checking logrotate presence                     [ OK ]
  - Checking remote logging                         [ NOT ENABLED ]
  - Checking log directories (static list)          [ DONE ]
  - Checking open log files                         [ SKIPPED ]

[+] Insecure services
------------------------------------
  - Installed inetd package                         [ NOT FOUND ]
    - Checking enabled inetd services               [ SUGGESTION ]
  - Installed xinetd package                        [ FOUND ]
    - xinetd status                                 [ NOT ACTIVE ]
      - Enabled xinetd.d services                   [ NOT FOUND ]
```

```
  - Installed rsh client package                [ OK ]
  - Installed rsh server package                [ OK ]
  - Installed telnet client package             [ OK ]
  - Installed telnet server package             [ FOUND ]
  - Checking NIS client installation            [ OK ]
  - Checking NIS server installation            [ OK ]
  - Checking TFTP client installation           [ OK ]
  - Checking TFTP server installation           [ OK ]

[+] 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            [ NOT FOUND ]
  - Checking auditd                             [ NOT FOUND ]

[+] Time and Synchronization
-----------------------------------

[+] Cryptography
-----------------------------------
  - Checking for expired SSL certificates [0/149]  [ NONE ]

  [WARNING]: Test CRYP-7902 had a long execution: 13.271809 seconds

  - Kernel entropy is sufficient                [ YES ]
  - HW RNG & rngd                               [ NO ]
  - SW prng                                     [ NO ]
  - MOR variable not found                      [ WEAK ]

[+] Virtualization
-----------------------------------

[+] Containers
-----------------------------------

[+] Security frameworks
-----------------------------------
  - Checking presence AppArmor                  [ NOT FOUND ]
  - 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
  - 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: /etc/crontab                                  [ OK ]
    File: /etc/group                                    [ SUGGESTION ]
    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                                   [ SUGGESTION ]
    File: /etc/passwd-                                  [ SUGGESTION ]
    File: /etc/ssh/sshd_config                          [ SUGGESTION ]
    Directory: /root/.ssh                               [ 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
------------------------------------
  - Permissions of home directories                     [ OK ]
  - 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)                  [ DIFFERENT ]
  - kernel.sysrq (exp: 0)                               [ DIFFERENT ]
  - kernel.unprivileged_bpf_disabled (exp: 1)           [ DIFFERENT ]
  - kernel.yama.ptrace_scope (exp: 1 2 3)               [ DIFFERENT ]
  - net.ipv4.conf.all.accept_redirects (exp: 0)         [ OK ]
  - net.ipv4.conf.all.accept_source_route (exp: 0)      [ OK ]
  - net.ipv4.conf.all.bootp_relay (exp: 0)              [ OK ]
  - net.ipv4.conf.all.forwarding (exp: 0)               [ DIFFERENT ]
  - net.ipv4.conf.all.log_martians (exp: 1)             [ DIFFERENT ]
  - net.ipv4.conf.all.mc_forwarding (exp: 0)            [ OK ]
  - net.ipv4.conf.all.proxy_arp (exp: 0)                [ OK ]
  - net.ipv4.conf.all.rp_filter (exp: 1)                [ DIFFERENT ]
  - net.ipv4.conf.all.send_redirects (exp: 0)           [ DIFFERENT ]
  - net.ipv4.conf.default.accept_redirects (exp: 0)     [ OK ]
  - net.ipv4.conf.default.accept_source_route (exp: 0)  [ OK ]
  - net.ipv4.conf.default.log_martians (exp: 1)         [ DIFFERENT ]
  - net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)       [ OK ]
  - net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [ OK ]
  - net.ipv4.tcp_syncookies (exp: 1)                    [ OK ]
  - net.ipv4.tcp_timestamps (exp: 0 1)                  [ OK ]
  - net.ipv6.conf.all.accept_redirects (exp: 0)         [ OK ]
  - net.ipv6.conf.all.accept_source_route (exp: 0)      [ OK ]
  - net.ipv6.conf.default.accept_redirects (exp: 0)     [ OK ]
  - net.ipv6.conf.default.accept_source_route (exp: 0)  [ OK ]

[+] Hardening
------------------------------------
  - Installed compiler(s)                               [ NOT FOUND ]
  - Installed malware scanner                           [ NOT FOUND ]
  - Non-native binary formats                           [ NOT FOUND ]

[+] Custom tests
------------------------------------
  - Running custom tests...                             [ NONE ]

[+] Plugins (phase 2)
------------------------------------
  - Plugins (phase 2)                                   [ DONE ]

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

  -[ Lynis 3.1.6 Results ]-

  Great, no warnings

  Suggestions (44):
  -----------------------------
  * 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/

  * Determine why /vmlinuz or /boot/vmlinuz is missing on this Debian/Ubuntu system.
[KRNL-5788]
    - Details  : /vmlinuz or /boot/vmlinuz
    - Related resources
      * Website: https://cisofy.com/lynis/controls/KRNL-5788/

  * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file
[KRNL-5820]
    - Related resources
      * 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/

  * 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/

  * Look at the locked accounts and consider removing them [AUTH-9284]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/AUTH-9284/

  * 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 /tmp file system, place /tmp 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/

  * 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 DNS configuration for the dns domain name [NAME-4028]
  - Related resources
    * Website: https://cisofy.com/lynis/controls/NAME-4028/

* 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/

* 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/

* Found a configuration error in Postfix [MAIL-8817]
  - Details : /etc/postfix/main.cf
  - Solution : run postconf > /dev/null
  - Related resources
    * Article: Postfix Hardening Guide for Security and Privacy: https://linux-audit.com/postfix-hardening-guide-for-security-and-privacy/
    * Website: https://cisofy.com/lynis/controls/MAIL-8817/

* Check iptables rules to see which rules are currently not used [FIRE-4513]
  - Related resources
    * Website: https://cisofy.com/lynis/controls/FIRE-4513/

* Consider hardening SSH configuration [SSH-7408]
  - Details : ClientAliveCountMax (set 3 to 2)
  - Related resources

```
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : GatewayPorts (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitRootLogin (set YES to
(FORCED-COMMANDS-ONLY|NO|PROHIBIT-PASSWORD|WITHOUT-PASSWORD))
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitUserEnvironment (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : PermitTunnel (set YES to NO)
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Port (set 22 to )
    - Related resources
      * Article: OpenSSH security and hardening:
https://linux-audit.com/ssh/audit-and-harden-your-ssh-configuration/
      * Website: https://cisofy.com/lynis/controls/SSH-7408/

  * Configure the 'requirepass' setting for Redis [DBS-1884]
    - Details  : /etc/redis/redis.conf
    - Solution : configure 'requirepass' setting in /etc/redis/redis.conf
    - Related resources
      * Website: https://cisofy.com/lynis/controls/DBS-1884/

  * Use the 'rename-command CONFIG' setting for Redis [DBS-1886]
    - Details  : /etc/redis/redis.conf
    - Solution : configure 'rename-command CONFIG' in /etc/redis/redis.conf
    - Related resources
      * Website: https://cisofy.com/lynis/controls/DBS-1886/

  * 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/

* Although inetd is not running, make sure no services are enabled in /etc/inetd.conf, or remove inetd service [INSE-8006]
- Related resources
* Website: https://cisofy.com/lynis/controls/INSE-8006/

* If there are no xinetd services required, it is recommended that the daemon be removed [INSE-8100]
- Related resources
* Website: https://cisofy.com/lynis/controls/INSE-8100/

* Removing the telnet server package and replace with SSH when possible [INSE-8322]
- Related resources
* Website: https://cisofy.com/lynis/controls/INSE-8322/

* 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 (no results) [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/

  * 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 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/
      * 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:
  ----------------------------
  - 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:

  Scan mode:
  Normal [■]  Forensics [ ]  Integration [ ]  Pentest [ ]

  Lynis modules:
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]

  Details:
  Hardening index : 66 [##############       ]
  Tests performed : 255
  Plugins enabled : 2
```

```
  Software components:
  - Firewall               [V]
  - Intrusion software     [X]
  - Malware scanner        [X]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

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

  Exceptions found
  Some exceptional events or information was found!

  What to do:
  You can help by providing your log file (/var/log/lynis.log).
  Go to https://cisofy.com/contact/ and send your file to the e-mail address listed

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

  Lynis 3.1.6

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2025, 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
/opt/lynis/default.prf for all settings)
```