**B.E SecureIT**

AUDITORIA E COMPLIANCE DE SEGURANÇA

# Relatório
# Auditoria de Segurança

**[ Lynis 3.0.8 ]**

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


  --------------------------------------------------
  Program version:          3.0.8
  Operating system:         Linux
  Operating system name:    CentOS Linux
  Operating system version: 7
  Kernel version:           3.10.0
  Hardware platform:        x86_64
  Hostname:                 centos
  --------------------------------------------------
  Profiles:                 /etc/lynis/default.prf
  Log file:                 /var/log/lynis.log
  Report file:              /var/log/lynis-report.dat
  Report version:           1.0
  Plugin directory:         /usr/share/lynis/plugins
  --------------------------------------------------
  Auditor:                  B.E SecureIT
  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

- Plugins enabled [ **NONE** ]

[+] **Boot and services**
------------------------------------
- Service Manager [ **systemd** ]
- Checking UEFI boot [ **DISABLED** ]
- Checking presence GRUB2 [ **FOUND** ]
- Checking for password protection [ **OK** ]
- Check running services (systemctl) [ **DONE** ]
Result: found 17 running services
- Check enabled services at boot (systemctl) [ **DONE** ]
Result: found 29 enabled services
- Check startup files (permissions) [ **OK** ]

[+] **Kernel**
------------------------------------
- Checking default runlevel [ **runlevel 3** ]
- Checking CPU support (NX/PAE)
CPU support: PAE and/or NoeXecute supported [ **FOUND** ]
- Checking kernel version and release [ **DONE** ]
- Checking kernel type [ **DONE** ]
- Checking loaded kernel modules [ **DONE** ]
Found 44 active modules
- Checking Linux kernel configuration file [ **FOUND** ]
- Checking default I/O kernel scheduler [ **FOUND** ]
- Checking core dumps configuration
- configuration in systemd conf files [ **DEFAULT** ]
- configuration in /etc/profile [ **DEFAULT** ]
- 'hard' configuration in /etc/security/limits.conf [ **DEFAULT** ]
- 'soft' configuration in /etc/security/limits.conf [ **DEFAULT** ]
- Checking setuid core dumps configuration [ **DISABLED** ]
- Check if reboot is needed [ **YES** ]

[+] **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 [ SUGGESTION ]
- 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 [ OK ]
- Permissions for: /etc/sudoers [ OK ]
- Permissions for: /etc/sudoers.d/vagrant [ OK ]
- PAM password strength tools [ OK ]
- PAM configuration file (pam.conf) [ NOT FOUND ]
- PAM configuration files (pam.d) [ FOUND ]
- PAM modules [ FOUND ]
- LDAP module in PAM [ NOT FOUND ]
- Accounts without expire date [ SUGGESTION ]
- Accounts without password [ OK ]
- Locked accounts [ OK ]
- Checking user password aging (minimum) [ DISABLED ]
- User password aging (maximum) [ DISABLED ]
- Checking expired passwords [ OK ]
- Checking Linux single user mode authentication [ OK ]
- Determining default umask
- umask (/etc/profile and /etc/profile.d) [ SUGGESTION ]
- umask (/etc/login.defs) [ OK ]
- umask (/etc/init.d/functions) [ SUGGESTION ]
- LDAP authentication support [ NOT ENABLED ]
- Logging failed login attempts [ DISABLED ]

[+] Shells
  -------------------------------------
- Checking shells from /etc/shells
  Result: found 4 shells (valid shells: 4).
- Session timeout settings/tools [ NONE ]
- Checking default umask values
- Checking default umask in /etc/bashrc [ WEAK ]
- Checking default umask in /etc/csh.cshrc [ WEAK ]
- Checking default umask in /etc/profile [ WEAK ]

[+] File systems
  -------------------------------------
- Checking mount points
- Checking /home mount point [ SUGGESTION ]
- Checking /tmp mount point [ SUGGESTION ]
- Checking /var mount point [ SUGGESTION ]
- Query swap partitions (fstab) [ OK ]
- Testing swap partitions [ OK ]
- Testing /proc mount (hidepid) [ SUGGESTION ]
- Checking for old files in /tmp [ OK ]
- Checking /tmp sticky bit [ OK ]
- Checking /var/tmp sticky bit [ OK ]
- ACL support root file system [ ENABLED ]
- Mount options of / [ OK ]
- Mount options of /dev [ PARTIALLY HARDENED ]
- Mount options of /dev/shm [ PARTIALLY HARDENED ]
- Mount options of /run [ HARDENED ]
- Total without nodev:11 noexec:13 nosuid:9 ro or noexec (W^X): 13 of total 30
- Disable kernel support of some filesystems

[+] USB Devices
  -------------------------------------
- Checking usb-storage driver (modprobe config) [ NOT DISABLED ]
- Checking USB devices authorization [ DISABLED ]
- Checking USBGuard [ NOT FOUND ]

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

[+] NFS
```

```
--------------------------------------
- Query rpc registered programs [ DONE ]
- Query NFS versions [ DONE ]
- Query NFS protocols [ DONE ]
- Check running NFS daemon [ NOT FOUND ]

[+] Name services
--------------------------------------
- Checking search domains [ FOUND ]
- Searching DNS domain name [ UNKNOWN ]
- Checking /etc/hosts
- Duplicate entries in hosts file [ FOUND ]
- Presence of configured hostname in /etc/hosts [ FOUND ]
- Hostname mapped to localhost [ NOT FOUND ]
- Localhost mapping to IP address [ OK ]

[+] Ports and packages
--------------------------------------
- Searching package managers
- Searching RPM package manager [ FOUND ]
- Querying RPM package manager

   [WARNING]: Test PKGS-7308 had a long execution: 10.213769 seconds

- YUM package management consistency [ OK ]
- Checking package database duplicates [ OK ]
- Checking package database for problems [ OK ]
- Checking missing security packages [ OK ]

   [WARNING]: Test PKGS-7386 had a long execution: 12.073945 seconds

- Checking GPG checks (yum.conf) [ OK ]
- Checking package audit tool [ INSTALLED ]
Found: yum-security
- Toolkit for automatic upgrades [ NOT FOUND ]

[+] Networking
--------------------------------------
- Checking IPv6 configuration [ ENABLED ]
Configuration method [ AUTO ]
IPv6 only [ NO ]
- Checking configured nameservers
- Testing nameservers
Nameserver: 10.0.2.3 [ SKIPPED ]
- Minimal of 2 responsive nameservers [ SKIPPED ]
- Getting listening ports (TCP/UDP) [ DONE ]
- Checking promiscuous interfaces [ OK ]
- Checking status DHCP client [ RUNNING ]
- 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 banner [ WARNING ]

[+] Software: firewalls
--------------------------------------
- Checking iptables kernel module [ FOUND ]
- Checking iptables policies of chains [ FOUND ]
- Checking chain INPUT (table:
filter, policy 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: Compression [ SUGGESTION ]
- OpenSSH option: FingerprintHash [ OK ]
- OpenSSH option: GatewayPorts [ OK ]
- 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 [ OK ]
- OpenSSH option: PermitTunnel [ OK ]
- OpenSSH option: Port [ SUGGESTION ]
- OpenSSH option: PrintLastLog [ OK ]
- OpenSSH option: StrictModes [ OK ]
- OpenSSH option: TCPKeepAlive [ SUGGESTION ]
- OpenSSH option: UseDNS [ OK ]
- OpenSSH option: X11Forwarding [ SUGGESTION ]
- OpenSSH option: AllowAgentForwarding [ SUGGESTION ]
- OpenSSH option: UsePrivilegeSeparation [ OK ]
- OpenSSH option: AllowUsers [ NOT FOUND ]
- OpenSSH option: AllowGroups [ NOT FOUND ]

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

[+] Databases
------------------------------------
No database engines found

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

[+] PHP
------------------------------------
- Checking PHP [ 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 [ FOUND ]
- Checking Metalog status [ NOT FOUND ]
- Checking RSyslog status [ FOUND ]
- Checking RFC 3195 daemon status [ NOT FOUND ]
- Checking minilogd instances [ 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 ]
- Installed xinetd package [ OK ]
- xinetd status
- Installed rsh client package [ OK ]
- Installed rsh server package [ OK ]
- Installed telnet client package [ OK ]
- Installed telnet server package [ NOT FOUND ]
- Checking NIS client installation [ OK ]
- Checking NIS server installation [ OK ]
- Checking TFTP client installation [ OK ]
- Checking TFTP server installation [ OK ]

[+] 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 [ ENABLED ]
  - Checking audit rules [ OK ]
  - Checking audit configuration file [ OK ]
  - Checking auditd log file [ FOUND ]

[+] Time and Synchronization
    ------------------------------------
- NTP daemon found: chronyd [ FOUND ]
- Checking for a running NTP daemon or client [ OK ]

[+] Cryptography
    ------------------------------------
- Checking for expired SSL certificates [0/4] [ NONE ]
- 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 [ FOUND ]
- Checking SELinux status [ ENABLED ]
- Checking current mode and config file [ OK ]
Current SELinux mode: enforcing
Found 0 permissive SELinux object types
Found 16 unconfined and 0 initrc_t processes
- Checking presence TOMOYO Linux [ NOT FOUND ]
- Checking presence grsecurity [ NOT FOUND ]
- Checking for implemented MAC framework [ OK ]

[+] 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: /boot/grub2/grub.cfg [ SUGGESTION ]
File: /etc/cron.deny [ OK ]
File: /etc/crontab [ SUGGESTION ]
File: /etc/group [ OK ]
File: /etc/group- [ OK ]
File: /etc/hosts.allow [ OK ]
File: /etc/hosts.deny [ OK ]
File: /etc/issue [ OK ]
File: /etc/issue.net [ OK ]
File: /etc/motd [ OK ]
File: /etc/passwd [ OK ]
File: /etc/passwd- [ OK ]
File: /etc/ssh/sshd_config [ OK ]
Directory: /etc/cron.d [ SUGGESTION ]
Directory: /etc/cron.daily [ SUGGESTION ]
Directory: /etc/cron.hourly [ SUGGESTION ]
Directory: /etc/cron.weekly [ SUGGESTION ]
Directory: /etc/cron.monthly [ SUGGESTION ]

[+] Home directories
    ------------------------------------
- Permissions of home directories [ OK ]
- Ownership of home directories [ OK ]
- Checking shell history files [ OK ]
```

```
[+] Kernel Hardening
------------------------------------
 - Comparing sysctl key pairs with scan profile
 - fs.protected_hardlinks (exp: 1) [ 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: 3) [ DIFFERENT ]
 - kernel.randomize_va_space (exp: 2) [ OK ]
 - kernel.sysrq (exp: 0) [ DIFFERENT ]
 - kernel.yama.ptrace_scope (exp: 1 2 3) [ DIFFERENT ]
 - net.core.bpf_jit_harden (exp: 2) [ DIFFERENT ]
 - net.ipv4.conf.all.accept_redirects (exp: 0) [ DIFFERENT ]
 - net.ipv4.conf.all.accept_source_route (exp: 0) [ OK ]
 - net.ipv4.conf.all.bootp_relay (exp: 0) [ OK ]
 - net.ipv4.conf.all.forwarding (exp: 0) [ OK ]
 - net.ipv4.conf.all.log_martians (exp: 1) [ DIFFERENT ]
 - net.ipv4.conf.all.mc_forwarding (exp: 0) [ OK ]
 - net.ipv4.conf.all.proxy_arp (exp: 0) [ OK ]
 - net.ipv4.conf.all.rp_filter (exp: 1) [ OK ]
 - net.ipv4.conf.all.send_redirects (exp: 0) [ DIFFERENT ]
 - net.ipv4.conf.default.accept_redirects (exp: 0) [ DIFFERENT ]
 - net.ipv4.conf.default.accept_source_route (exp: 0) [ OK ]
 - net.ipv4.conf.default.log_martians (exp: 1) [ DIFFERENT ]
 - net.ipv4.icmp_echo_ignore_broadcasts (exp: 1) [ OK ]
 - net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [ OK ]
 - net.ipv4.tcp_syncookies (exp: 1) [ OK ]
 - net.ipv4.tcp_timestamps (exp: 0 1) [ OK ]
 - net.ipv6.conf.all.accept_redirects (exp: 0) [ DIFFERENT ]
 - net.ipv6.conf.all.accept_source_route (exp: 0) [ OK ]
 - net.ipv6.conf.default.accept_redirects (exp: 0) [ DIFFERENT ]
 - net.ipv6.conf.default.accept_source_route (exp: 0) [ OK ]

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

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

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

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

  -[ Lynis 3.0.8 Results ]-

  Warnings (3):
  ----------------------------
  ! Reboot of system is most likely needed [KRNL-5830]
     - Solution : reboot
       https://cisofy.com/lynis/controls/KRNL-5830/

  ! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]
       https://cisofy.com/lynis/controls/MAIL-8818/

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

  Suggestions (43):
  ----------------------------
  * This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
       https://cisofy.com/lynis/controls/LYNIS/

  * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
       https://cisofy.com/lynis/controls/KRNL-5820/

  * Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229]
       https://cisofy.com/lynis/controls/AUTH-9229/

  * Configure password hashing rounds in /etc/login.defs [AUTH-9230]
       https://cisofy.com/lynis/controls/AUTH-9230/

  * When possible set expire dates for all password protected accounts [AUTH-9282]
       https://cisofy.com/lynis/controls/AUTH-9282/
```

```
  * Configure minimum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/lynis/controls/AUTH-9286/

  * Configure maximum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/lynis/controls/AUTH-9286/

  * Default umask in /etc/profile or /etc/profile.d/custom.sh could be more strict (e.g. 027) [AUTH-9328]
      https://cisofy.com/lynis/controls/AUTH-9328/

  * To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]
      https://cisofy.com/lynis/controls/FILE-6310/

  * To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]
      https://cisofy.com/lynis/controls/FILE-6310/

  * To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]
      https://cisofy.com/lynis/controls/FILE-6310/

  * Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]
      https://cisofy.com/lynis/controls/USB-1000/

  * Disable drivers like firewire storage when not used, to prevent unauthorized storage or data theft [STRG-1846]
      https://cisofy.com/lynis/controls/STRG-1846/

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

  * Remove duplicate lines in /etc/hosts [NAME-4402]
      https://cisofy.com/lynis/controls/NAME-4402/

  * Consider using a tool to automatically apply upgrades [PKGS-7420]
      https://cisofy.com/lynis/controls/PKGS-7420/

  * Determine if protocol 'dccp' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * Determine if protocol 'sctp' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * Determine if protocol 'rds' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * Determine if protocol 'tipc' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * You are advised to hide the mail_name (option: smtpd_banner) from your postfix configuration. Use postconf -e or change
your main.cf file (/etc/postfix/main.cf) [MAIL-8818]
      https://cisofy.com/lynis/controls/MAIL-8818/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowTcpForwarding (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : ClientAliveCountMax (set 3 to 2)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Compression (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : LogLevel (set INFO to VERBOSE)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxAuthTries (set 6 to 3)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxSessions (set 10 to 2)
      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))
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Port (set 22 to )
      https://cisofy.com/lynis/controls/SSH-7408/

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

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

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : X11Forwarding (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowAgentForwarding (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]
      https://cisofy.com/lynis/controls/LOGG-2154/

  * Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
      https://cisofy.com/lynis/controls/BANN-7126/

  * Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
      https://cisofy.com/lynis/controls/BANN-7130/

  * Enable process accounting [ACCT-9622]
      https://cisofy.com/lynis/controls/ACCT-9622/

  * Enable sysstat to collect accounting (no results) [ACCT-9626]
      https://cisofy.com/lynis/controls/ACCT-9626/

  * Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]
      https://cisofy.com/lynis/controls/FINT-4350/

  * Determine if automation tools are present for system management [TOOL-5002]
      https://cisofy.com/lynis/controls/TOOL-5002/

  * Consider restricting file permissions [FILE-7524]
    - Details  : See screen output or log file
    - Solution : Use chmod to change file permissions
      https://cisofy.com/lynis/controls/FILE-7524/

  * One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
    - Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)
      https://cisofy.com/lynis/controls/KRNL-6000/

  * Harden compilers like restricting access to root user only [HRDN-7222]
      https://cisofy.com/lynis/controls/HRDN-7222/

  * Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]
    - Solution : Install a tool like rkhunter, chkrootkit, OSSEC
      https://cisofy.com/lynis/controls/HRDN-7230/

  Follow-up:
  --------------------------
  - Show details of a test (lynis show details TEST-ID)
  - Check the logfile for all details (less /var/log/lynis.log)
  - Read security controls texts (https://cisofy.com)
  - Use --upload to upload data to central system (Lynis Enterprise users)

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

  Lynis security scan details:

  Hardening index : 65 [############        ]
  Tests performed : 242
  Plugins enabled : 0

  Components:
  - Firewall               [V]
  - Malware scanner        [X]

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

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

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

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

  Lynis 3.0.8

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

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