```
[ Lynis 2.7.5 ]

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

  2007-2019, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


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

  ---------------------------------------------------
  Program version:           2.7.5
  Operating system:          Linux
  Operating system name:     Ubuntu Linux
  Operating system version:  18.04
  Kernel version:            4.15.0
  Hardware platform:         x86_64
  Hostname:                  pc07
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /etc/lynis/plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                                  [ NO UPDATE ]

[+] System Tools
------------------------------------
  - Scanning available tools...
  - Checking system binaries...

[+] Plugins (phase 1)
------------------------------------
 Note: plugins have more extensive tests and may take several minutes to complete

  - Plugin: debian
    [
[+] Debian Tests
------------------------------------
  - Checking for system binaries that are required by Debian Tests...
    - Checking /bin...                                        [ FOUND ]
    - Checking /sbin...                                       [ FOUND ]
    - Checking /usr/bin...                                    [ FOUND ]
    - Checking /usr/sbin...                                   [ FOUND ]
    - Checking /usr/local/bin...                              [ FOUND ]
    - Checking /usr/local/sbin...                             [ FOUND ]
  - Authentication:
    - PAM (Pluggable Authentication Modules):
      - libpam-tmpdir                                         [ Not Installed ]
      - libpam-usb                                            [ Not Installed ]
  - File System Checks:
    - DM-Crypt, Cryptsetup & Cryptmount:
  - Software:
    - apt-listbugs                                            [ Not Installed ]
    - apt-listchanges                                         [ Not Installed ]
    - checkrestart                                            [ Not Installed ]
    - needrestart                                             [ Not Installed ]
    - debsecan                                                [ Installed and enabled for
cron ]
    - debsums                                                 [ Installed and enabled for
cron ]
    - fail2ban                                                [ Not Installed ]
]

[+] Boot and services
------------------------------------
  - Service Manager                                           [ systemd ]
  - Checking UEFI boot                                        [ DISABLED ]
  - Checking presence GRUB2                                   [ FOUND ]
    - Checking for password protection                        [ NONE ]
  - Check running services (systemctl)                        [ DONE ]
        Result: found 44 running services
  - Check enabled services at boot (systemctl)                [ DONE ]
        Result: found 71 enabled services
  - Check startup files (permissions)                         [ OK ]

[+] Kernel
------------------------------------
  - Checking default run level                                [ RUNLEVEL 5 ]
  - Checking CPU support (NX/PAE)
    CPU support: PAE and/or NoeXecute supported               [ FOUND ]
  - Checking kernel version and release                       [ DONE ]
  - Checking kernel type                                      [ DONE ]
  - Checking loaded kernel modules                            [ DONE ]
      Found 126 active modules
  - Checking Linux kernel configuration file                  [ FOUND ]
  - Checking default I/O kernel scheduler                     [ FOUND ]
  - Checking for available kernel update                      [ OK ]
  - Checking core dumps configuration                         [ DISABLED ]
    - Checking setuid core dumps configuration                [ PROTECTED ]
  - Check if reboot is needed                                 [ NO ]

[+] Memory and Processes
------------------------------------
  - Checking /proc/meminfo                                    [ FOUND ]
  - Searching for dead/zombie processes                       [ OK ]
  - Searching for IO waiting processes                        [ OK ]

[+] 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 ]
  - Query system users (non daemons)                          [ DONE ]
  - NIS+ authentication support                               [ NOT ENABLED ]
  - NIS authentication support                                [ NOT ENABLED ]
  - sudoers file                                              [ FOUND ]
    - Permissions for directory: /etc/sudoers.d               [ WARNING ]
    - 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                              [ OK ]
  - Accounts without password                                 [ OK ]
  - Checking user password aging (minimum)                    [ DISABLED ]
  - User password aging (maximum)                             [ DISABLED ]
  - Checking expired passwords                                [ OK ]
  - Checking Linux single user mode authentication            [ OK ]
  - Determining default umask
    - umask (/etc/profile)                                    [ NOT FOUND ]
    - umask (/etc/login.defs)                                 [ SUGGESTION ]
  - LDAP authentication support                               [ NOT ENABLED ]
  - Logging failed login attempts                             [ ENABLED ]

[+] Shells
------------------------------------
  - Checking shells from /etc/shells
    Result: found 7 shells (valid shells: 7).
    - Session timeout settings/tools                          [ NONE ]
  - Checking default umask values
    - Checking default umask in /etc/bash.bashrc              [ NONE ]
    - Checking default umask in /etc/profile                  [ NONE ]

[+] File systems
------------------------------------
  - Checking mount points
    - Checking /home mount point                              [ SUGGESTION ]
    - Checking /tmp mount point                               [ 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 /                                        [ NON DEFAULT ]
  - Checking Locate database                                  [ FOUND ]
  - Disable kernel support of some filesystems
    - Discovered kernel modules: cramfs freevxfs hfs hfsplus jffs2 udf

[+] 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)           [ 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
    - Checking /etc/hosts (duplicates)                        [ OK ]
    - Checking /etc/hosts (hostname)                          [ OK ]
    - Checking /etc/hosts (localhost)                         [ OK ]
    - Checking /etc/hosts (localhost to IP)                   [ OK ]

[+] Ports and packages
------------------------------------
  - Searching package managers
    - Searching dpkg package manager                          [ FOUND ]
      - Querying package manager
    - Query unpurged packages                                 [ FOUND ]
    - debsums utility                                         [ FOUND ]
      - Cron job for debsums                                  [ FOUND ]
  - Checking security repository in sources.list file         [ OK ]
  - Checking APT package database                             [ OK ]
  - Checking vulnerable packages                              [ WARNING ]
  - Checking upgradeable packages                             [ SKIPPED ]
  - Checking package audit tool                               [ INSTALLED ]
    Found: apt-get
  - Toolkit for automatic upgrades (unattended-upgrade)       [ FOUND ]

[+] Networking
------------------------------------
  - Checking IPv6 configuration                               [ ENABLED ]
      Configuration method                                    [ AUTO ]
      IPv6 only                                               [ NO ]
  - Checking configured nameservers
    - Testing nameservers
        Nameserver: 127.0.0.53                                [ OK ]
  - Checking default gateway                                  [ DONE ]
  - Getting listening ports (TCP/UDP)                         [ DONE ]
  - Checking promiscuous interfaces                           [ OK ]
  - Checking waiting connections                              [ OK ]
  - Checking status DHCP client                               [ RUNNING ]
  - Checking for ARP monitoring software                      [ NOT FOUND ]

[+] Printers and Spools
------------------------------------
  - Checking cups daemon                                      [ RUNNING ]
  - Checking CUPS configuration file                          [ OK ]
    - File permissions                                        [ WARNING ]
  - Checking CUPS addresses/sockets                           [ FOUND ]
  - Checking lp daemon                                        [ NOT RUNNING ]

[+] Software: e-mail and messaging
------------------------------------


[+] Software: firewalls
------------------------------------
  - Checking iptables kernel module                           [ FOUND ]
    - Checking iptables policies of chains                    [ FOUND ]
    - Checking for empty ruleset                              [ OK ]
    - Checking for unused rules                               [ FOUND ]
  - Checking host based firewall                              [ ACTIVE ]

[+] Software: webserver
------------------------------------
  - Checking Apache (binary /usr/sbin/apache2)                [ FOUND ]
      Info: Configuration file found (/etc/apache2/apache2.conf)
      Info: No virtual hosts found
    * Loadable modules                                        [ FOUND (114) ]
        - Found 114 loadable modules
          mod_evasive: anti-DoS/brute force                   [ NOT FOUND ]
          mod_reqtimeout/mod_qos                              [ FOUND ]
          ModSecurity: web application firewall               [ NOT FOUND ]
  - Checking nginx                                            [ NOT FOUND ]

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

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

[+] Databases
------------------------------------
  - MySQL process status                                      [ FOUND ]
  - 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                                              [ FOUND ]
    - Checking PHP disabled functions                         [ FOUND ]
    - Checking expose_php option                              [ ON ]
    - Checking enable_dl option                               [ OFF ]
    - Checking allow_url_fopen option                         [ ON ]
    - Checking allow_url_include option                       [ OFF ]

[+] 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 log directories (static list)                    [ DONE ]
  - Checking open log files                                   [ DONE ]
  - Checking deleted files in use                             [ FILES FOUND ]

[+] Insecure services
------------------------------------
  - Installed inetd package                                   [ NOT FOUND ]
  - Installed xinetd package                                  [ OK ]
    - xinetd status                                           [ NOT ACTIVE ]
  - Installed rsh client package                              [ OK ]
  - Installed rsh server package                              [ OK ]
  - Installed telnet client package                           [ OK ]
  - Installed telnet server package                           [ NOT FOUND ]

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

[+] Scheduled tasks
------------------------------------
  - Checking crontab and cronjob files                        [ DONE ]

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

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

[+] Cryptography
------------------------------------
  - Checking for expired SSL certificates [3/9]               [ FOUND ]

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

[+] Containers
------------------------------------
    - Docker
      - Docker daemon                                         [ RUNNING ]
        - Docker info output (warnings)                       [ 1 ]
      - Containers
        - Total containers                                    [ 6 ]
          - Running containers                                [ 3 ]
        - Unused containers                                   [ 3 ]
    - File permissions                                        [ OK ]

[+] Security frameworks
------------------------------------
  - Checking presence AppArmor                                [ FOUND ]
    - Checking AppArmor status                                [ ENABLED ]
  - Checking presence SELinux                                 [ NOT FOUND ]
  - 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
------------------------------------

[+] File Permissions
------------------------------------
  - Starting file permissions check

[+] Home directories
------------------------------------
  - 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)                               [ DIFFERENT ]
    - kernel.core_uses_pid (exp: 1)                           [ DIFFERENT ]
    - kernel.ctrl-alt-del (exp: 0)                            [ OK ]
    - kernel.dmesg_restrict (exp: 1)                          [ DIFFERENT ]
    - kernel.kptr_restrict (exp: 2)                           [ DIFFERENT ]
    - kernel.randomize_va_space (exp: 2)                      [ OK ]
    - kernel.sysrq (exp: 0)                                   [ DIFFERENT ]
    - kernel.yama.ptrace_scope (exp: 1 2 3)                   [ OK ]
    - 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)                    [ 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)      [ DIFFERENT ]
    - 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 ]

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

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

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

  -[ Lynis 2.7.5 Results ]-

  Warnings (1):
  ----------------------------
  ! Found one or more vulnerable packages. [PKGS-7392]
      https://cisofy.com/lynis/controls/PKGS-7392/

  Suggestions (43):
  ----------------------------
  * Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [CUST-0280]
      https://your-domain.example.org/controls/CUST-0280/

  * Install libpam-usb to enable multi-factor authentication for PAM sessions [CUST-0285]
      https://your-domain.example.org/controls/CUST-0285/

  * Install apt-listbugs to display a list of critical bugs prior to each APT
installation. [CUST-0810]
      https://your-domain.example.org/controls/CUST-0810/

  * Install apt-listchanges to display any significant changes prior to any upgrade via
APT. [CUST-0811]
      https://your-domain.example.org/controls/CUST-0811/

  * Install debian-goodies so that you can run checkrestart after upgrades to determine
which services are using old versions of libraries and need restarting. [CUST-0830]
      https://your-domain.example.org/controls/CUST-0830/

  * Install needrestart, alternatively to debian-goodies, so that you can run needrestart
after upgrades to determine which daemons are using old versions of libraries and need
restarting. [CUST-0831]
      https://your-domain.example.org/controls/CUST-0831/

  * Install fail2ban to automatically ban hosts that commit multiple authentication
errors. [DEB-0880]
      https://cisofy.com/lynis/controls/DEB-0880/

  * Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot
in single user mode without password) [BOOT-5122]
      https://cisofy.com/lynis/controls/BOOT-5122/

  * Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc
[AUTH-9262]
      https://cisofy.com/lynis/controls/AUTH-9262/

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

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

  * Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
      https://cisofy.com/lynis/controls/AUTH-9328/

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

```
      https://cisofy.com/lynis/controls/FILE-6310/

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

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

  * Disable drivers like USB storage when not used, to prevent unauthorized storage or
data theft [STRG-1840]
      https://cisofy.com/lynis/controls/STRG-1840/

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

  * Purge old/removed packages (76 found) with aptitude purge or dpkg --purge command.
This will cleanup old configuration files, cron jobs and startup scripts. [PKGS-7346]
      https://cisofy.com/lynis/controls/PKGS-7346/

  * Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or
unattended-upgrades [PKGS-7392]
      https://cisofy.com/lynis/controls/PKGS-7392/

  * Install package apt-show-versions for patch management purposes [PKGS-7394]
      https://cisofy.com/lynis/controls/PKGS-7394/

  * Remove any unneeded kernel packages [PKGS-7410]
    - Details  : 27 kernels
    - Solution : validate dpkg -l output and perform cleanup with apt autoremove
      https://cisofy.com/lynis/controls/PKGS-7410/

  * Consider running ARP monitoring software (arpwatch,arpon) [NETW-3032]
      https://cisofy.com/lynis/controls/NETW-3032/

  * Access to CUPS configuration could be more strict. [PRNT-2307]
      https://cisofy.com/lynis/controls/PRNT-2307/

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

  * Install Apache mod_evasive to guard webserver against DoS/brute force attempts [HTTP-
6640]
      https://cisofy.com/lynis/controls/HTTP-6640/

  * Install Apache modsecurity to guard webserver against web application attacks [HTTP-
6643]
      https://cisofy.com/lynis/controls/HTTP-6643/

  * Configure the 'requirepass' setting for Redis [DBS-1884]
    - Details  : /etc/redis/redis.conf
    - Solution : configure 'requirepass' setting in /etc/redis/redis.conf
      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
      https://cisofy.com/lynis/controls/DBS-1886/

  * Turn off PHP information exposure [PHP-2372]
    - Details  : expose_php = Off
      https://cisofy.com/lynis/controls/PHP-2372/

  * Change the allow_url_fopen line to: allow_url_fopen = Off, to disable downloads via
PHP [PHP-2376]
      https://cisofy.com/lynis/controls/PHP-2376/

  * Check what deleted files are still in use and why. [LOGG-2190]
      https://cisofy.com/lynis/controls/LOGG-2190/
  * Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
      https://cisofy.com/lynis/controls/BANN-7126/

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

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

  * Enable sysstat to collect accounting (disabled) [ACCT-9626]
      https://cisofy.com/lynis/controls/ACCT-9626/

  * Enable auditd to collect audit information [ACCT-9628]
      https://cisofy.com/lynis/controls/ACCT-9628/

  * Check available certificates for expiration [CRYP-7902]
      https://cisofy.com/lynis/controls/CRYP-7902/

  * Run 'docker info' to see warnings applicable to Docker daemon [CONT-8104]
      https://cisofy.com/lynis/controls/CONT-8104/

  * 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/

  * 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 : 58 [###########          ]
  Tests performed : 247
  Plugins enabled : 1

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

  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 2.7.5

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

  2007-2019, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

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

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