```
[ Lynis 3.0.9 ]

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

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


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

  ---------------------------------------------------
  Program version:           3.0.9
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  24.04
  Kernel version:            6.8.0
  Hardware platform:         x86_64
  Hostname:                  ip-172-31-81-209
  ---------------------------------------------------
  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 [ Installed and Enabled ]
- File System Checks:
- DM-Crypt, Cryptsetup & Cryptmount:
- Checking / on /dev/nvme0n1p1 [ NOT ENCRYPTED ]
- Checking /snap/amazon-ssm-agent/9881 on /var/lib/snapd/snaps/amazon-ssm-agent_9881.snap [ NOT ENCRYPTED ]
- Checking /snap/core22/1748 on /var/lib/snapd/snaps/core22_1748.snap [ NOT ENCRYPTED ]
- Checking /snap/core22/1802 on /var/lib/snapd/snaps/core22_1802.snap [ NOT ENCRYPTED ]
- Checking /snap/snapd/23545 on /var/lib/snapd/snaps/snapd_23545.snap [ NOT ENCRYPTED ]
- Checking /snap/snapd/23771 on /var/lib/snapd/snaps/snapd_23771.snap [ NOT ENCRYPTED ]
- Checking /boot on /dev/nvme0n1p16 [ NOT ENCRYPTED ]
- Checking /boot/efi on /dev/nvme0n1p15 [ NOT ENCRYPTED ]
- Software:
- apt-listbugs [ Not Installed ]
- apt-listchanges [ Installed and enabled for apt ]
- needrestart [ Installed ]
```

```
  - fail2ban [ Installed with jail.conf ]
  ]

  [+] Boot and services
  ------------------------------------
  - Service Manager [ systemd ]
  - Checking UEFI boot [ ENABLED ]
  - Checking Secure Boot [ DISABLED ]
  - Checking presence GRUB2 [ FOUND ]
  - Checking for password protection [ NONE ]
  - Check running services (systemctl) [ DONE ]
  Result: found 26 running services
  - Check enabled services at boot (systemctl) [ DONE ]
  Result: found 52 enabled services
  - Check startup files (permissions) [ OK ]
  - Running 'systemd-analyze security'
  - ModemManager.service: [ MEDIUM ]
  - acpid.service: [ UNSAFE ]
  - auditd.service: [ EXPOSED ]
  - chrony.service: [ PROTECTED ]
  - cron.service: [ UNSAFE ]
  - dbus.service: [ UNSAFE ]
  - dm-event.service: [ UNSAFE ]
  - dmesg.service: [ UNSAFE ]
  - emergency.service: [ UNSAFE ]
  - fail2ban.service: [ UNSAFE ]
  - getty@tty1.service: [ UNSAFE ]
  - hibinit-agent.service: [ UNSAFE ]
  - irqbalance.service: [ EXPOSED ]
  - iscsid.service: [ UNSAFE ]
  - lvm2-lvmpolld.service: [ UNSAFE ]
  - lynis.service: [ UNSAFE ]
  - multipathd.service: [ UNSAFE ]
  - networkd-dispatcher.service: [ UNSAFE ]
  - open-vm-tools.service: [ UNSAFE ]
  - packagekit.service: [ UNSAFE ]
  - plymouth-start.service: [ UNSAFE ]
  - polkit.service: [ PROTECTED ]
  - rc-local.service: [ UNSAFE ]
  - rescue.service: [ UNSAFE ]
  - rsyslog.service: [ MEDIUM ]
  - serial-getty@ttyS0.service: [ UNSAFE ]
  - snap.amazon-ssm-agent.amazon-ssm-agent.service: [ UNSAFE ]
  - snapd.service: [ UNSAFE ]
  - ssh.service: [ UNSAFE ]
  - systemd-ask-password-console.service: [ UNSAFE ]
  - systemd-ask-password-plymouth.service: [ UNSAFE ]
  - systemd-ask-password-wall.service: [ UNSAFE ]
  - systemd-bsod.service: [ UNSAFE ]
  - systemd-fsckd.service: [ UNSAFE ]
  - systemd-initctl.service: [ UNSAFE ]
  - systemd-journald.service: [ PROTECTED ]
  - systemd-logind.service: [ PROTECTED ]
  - systemd-networkd.service: [ PROTECTED ]
  - systemd-resolved.service: [ PROTECTED ]
  - systemd-rfkill.service: [ UNSAFE ]
  - systemd-udevd.service: [ MEDIUM ]
  - tpm-udev.service: [ UNSAFE ]
  - ubuntu-advantage.service: [ UNSAFE ]
  - udisks2.service: [ UNSAFE ]
  - unattended-upgrades.service: [ UNSAFE ]
  - user@1000.service: [ UNSAFE ]
  - uuidd.service: [ MEDIUM ]
  - vgauth.service: [ UNSAFE ]

  [+] 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 41 active modules
  - Checking Linux kernel configuration file [ FOUND ]
  - Checking default I/O kernel scheduler [ NOT FOUND ]
  - Checking for available kernel update [ OK ]
  - Checking core dumps configuration
  - configuration in systemd conf files [ DEFAULT ]
  - configuration in /etc/profile [ DEFAULT ]
  - 'hard' configuration in /etc/security/limits.conf [ DISABLED ]
  - 'soft' config in /etc/security/limits.conf (implicit) [ DISABLED ]
  - Checking setuid core dumps configuration [ DISABLED ]
  - Check if reboot is needed [ NO ]

  [+] Memory and Processes
  ------------------------------------
  - Checking /proc/meminfo [ FOUND ]
  - Searching for dead/zombie processes [ NOT FOUND ]
  - Searching for IO waiting processes [ NOT FOUND ]
  - Search prelink tooling [ NOT FOUND ]

  [+] Users, Groups and Authentication
  ------------------------------------
  - Administrator accounts [ OK ]
  - Unique UIDs [ OK ]
  - Consistency of group files (grpck) [ OK ]
  - Unique group IDs [ OK ]
  - Unique group names [ OK ]
  - Password file consistency [ OK ]
  - Password hashing methods [ OK ]
  - 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/90-cloud-init-users [ OK ]
  - Permissions for: /etc/sudoers.d/README [ OK ]
  - PAM password strength tools [ OK ]
  - 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 ]
  - 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 ]

  [+] Shells
  ------------------------------------
  - Checking shells from /etc/shells
  Result: found 9 shells (valid shells: 9).
  - 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) [ 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 / [ NON DEFAULT ]
  - Mount options of /boot [ DEFAULT ]
  - Mount options of /dev [ HARDENED ]
  - Mount options of /dev/shm [ PARTIALLY HARDENED ]
  - Mount options of /run [ HARDENED ]
  - Total without nodev:6 noexec:13 nosuid:9 ro or noexec (W^X): 8 of total 29
```

```
- Disable kernel support of some filesystems

 [+] USB Devices
------------------------------------
- Checking usb-storage driver (modprobe config) [ DISABLED ]
- Checking USB devices authorization [ DISABLED ]
- 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 [ FOUND ]
Domain name: ec2.internal
- Checking /etc/hosts
- Duplicate entries in hosts file [ NONE ]
- Presence of configured hostname in /etc/hosts [ NOT 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 ]
- debsums utility [ FOUND ]
- Cron job for debsums [ FOUND ]
- Checking security repository in sources.list.d directory [ OK ]
- Checking APT package database [ OK ]
- Checking vulnerable packages [ OK ]
- Checking upgradeable packages [ FOUND ]
- Checking package audit tool [ INSTALLED ]
Found: apt-check
- 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 ]
- DNSSEC supported (systemd-resolved) [ UNKNOWN ]
- Checking default gateway [ DONE ]
- Getting listening ports (TCP/UDP) [ DONE ]
- Checking promiscuous interfaces [ OK ]
- Checking waiting connections [ OK ]
- Checking status DHCP client
- Checking for ARP monitoring software [ NOT FOUND ]
- Uncommon network protocols [ NOT FOUND ]

 [+] Printers and Spools
------------------------------------
- Checking cups daemon [ NOT FOUND ]
- Checking lp daemon [ NOT RUNNING ]

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

 [+] Software: firewalls
------------------------------------
- Checking iptables kernel module [ FOUND ]
- Checking iptables policies of chains [ FOUND ]
- 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 [ OK ]
- OpenSSH option: ClientAliveInterval [ OK ]
- OpenSSH option: FingerprintHash [ OK ]
- OpenSSH option: GatewayPorts [ OK ]
- OpenSSH option: IgnoreRhosts [ OK ]
- OpenSSH option: LoginGraceTime [ OK ]
- OpenSSH option: LogLevel [ OK ]
- OpenSSH option: MaxAuthTries [ SUGGESTION ]
- OpenSSH option: MaxSessions [ SUGGESTION ]
- OpenSSH option: PermitRootLogin [ OK ]
- 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 [ OK ]
- OpenSSH option: AllowAgentForwarding [ SUGGESTION ]
- 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 [ DONE ]
- Checking deleted files in use [ DONE ]

[+] 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 [ OK ]
- /etc/issue.net [ FOUND ]
- /etc/issue.net contents [ OK ]

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

[+] Accounting
------------------------------------
- Checking accounting information [ OK ]
- Checking sysstat accounting data [ ENABLED ]
- Checking auditd [ ENABLED ]
- Checking audit rules [ SUGGESTION ]
- 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 [0/150] [ NONE ]
- Found 0 encrypted and 0 unencrypted swap devices in use. [ OK ]
- Kernel entropy is sufficient [ YES ]
- HW RNG & rngd [ NO ]
- SW prng [ NO ]
MOR-bit set [ YES ]

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

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

[+] Security frameworks
------------------------------------
- Checking presence AppArmor [ FOUND ]
- Checking AppArmor status [ ENABLED ]
Found 41 unconfined processes
- 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
- AIDE [ FOUND ]
- AIDE config file [ NOT FOUND ]
- dm-integrity (status) [ DISABLED ]
- dm-verity (status) [ DISABLED ]
- Checking presence integrity tool [ FOUND ]

[+] Software: System tooling
------------------------------------
- Checking automation tooling
- Ansible artifact [ FOUND ]
- Automation tooling [ FOUND ]
- Checking presence of Fail2ban [ FOUND ]
- Checking Fail2ban jails [ ENABLED ]
- Checking for IDS/IPS tooling [ FOUND ]

[+] Software: Malware
------------------------------------
- Checking Rootkit Hunter [ FOUND ]
- Malware software components [ FOUND ]
- Active agent [ NOT FOUND ]
- Rootkit scanner [ FOUND ]

[+] File Permissions
```

```
  ------------------------------------
  - Starting file permissions check
  File: /boot/grub/grub.cfg [ OK ]
  File: /etc/crontab [ OK ]
  File: /etc/group [ OK ]
  File: /etc/group- [ OK ]
  File: /etc/hosts.allow [ OK ]
  File: /etc/hosts.deny [ OK ]
  File: /etc/issue [ OK ]
  File: /etc/issue.net [ OK ]
  File: /etc/passwd [ OK ]
  File: /etc/passwd- [ OK ]
  File: /etc/ssh/sshd_config [ SUGGESTION ]
  Directory: /root/.ssh [ OK ]
  Directory: /etc/cron.d [ OK ]
  Directory: /etc/cron.daily [ OK ]
  Directory: /etc/cron.hourly [ OK ]
  Directory: /etc/cron.weekly [ OK ]
  Directory: /etc/cron.monthly [ OK ]

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

  [+] Kernel Hardening
  ------------------------------------
  - Comparing sysctl key pairs with scan profile
  - dev.tty.ldisc_autoload (exp: 0) [ DIFFERENT ]
  - fs.protected_fifos (exp: 2) [ DIFFERENT ]
  - fs.protected_hardlinks (exp: 1) [ OK ]
  - fs.protected_regular (exp: 2) [ OK ]
  - fs.protected_symlinks (exp: 1) [ OK ]
  - fs.suid_dumpable (exp: 0) [ OK ]
  - kernel.core_uses_pid (exp: 1) [ DIFFERENT ]
  - kernel.ctrl-alt-del (exp: 0) [ OK ]
  - kernel.dmesg_restrict (exp: 1) [ OK ]
  - 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) [ OK ]
  - kernel.unprivileged_bpf_disabled (exp: 1) [ DIFFERENT ]
  - kernel.yama.ptrace_scope (exp: 1 2 3) [ OK ]
  - net.core.bpf_jit_harden (exp: 2) [ 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) [ OK ]
  - net.ipv4.conf.all.log_martians (exp: 1) [ OK ]
  - 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) [ OK ]
  - 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) [ FOUND ]
  - Installed malware scanner [ FOUND ]
  - Non-native binary formats [ FOUND ]

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

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

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

    -[ Lynis 3.0.9 Results ]-

    Warnings (2):
    ----------------------------
    ! iptables module(s) loaded, but no rules active [FIRE-4512]
        https://cisofy.com/lynis/controls/FIRE-4512/

    ! No AIDE configuration file was found, needed for AIDE functionality [FINT-4315]
        https://cisofy.com/lynis/controls/FINT-4315/

    Suggestions (22):
    ----------------------------
    * This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [
        https://cisofy.com/lynis/controls/LYNIS/

    * Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
        https://cisofy.com/lynis/controls/DEB-0810/

    * Copy /etc/fail2ban/jail.conf to jail.local to prevent it being changed by updates. [DEB-0880]
        https://cisofy.com/lynis/controls/DEB-0880/

    * Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode wit
        https://cisofy.com/lynis/controls/BOOT-5122/

    * Consider hardening system services [BOOT-5264]
      - Details  : Run '/usr/bin/systemd-analyze security SERVICE' for each service
        https://cisofy.com/lynis/controls/BOOT-5264/

    * Look at the locked accounts and consider removing them [AUTH-9284]
        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]
        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/

    * Add the IP name and FQDN to /etc/hosts for proper name resolving [NAME-4404]
        https://cisofy.com/lynis/controls/NAME-4404/

    * 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  : MaxAuthTries (set 4 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  : 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  : 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/

    * Audit daemon is enabled with an empty ruleset. Disable the daemon or define rules [ACCT-9630]
        https://cisofy.com/lynis/controls/ACCT-9630/

    * 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/

    * Double check the permissions of home directories as some might be not strict enough. [HOME-9304]
        https://cisofy.com/lynis/controls/HOME-9304/

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

    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 : 79 [###############     ]
    Tests performed : 261
    Plugins enabled : 1

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

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

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

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

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

    Lynis 3.0.9

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

    2007-2021, 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)
```