```
[ Lynis 3.1.5 ]

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

  2007-2024, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
␛[2C- Detecting OS... ␛[41C [ DONE ]
␛[2C- Checking profiles...␛[37C [ DONE ]

  ---------------------------------------------------
  Program version:           3.1.5
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  20.04
  End-of-life:               YES
  Kernel version:            5.15.0
  Hardware platform:         x86_64
  Hostname:                  gn-VirtualBox
  ---------------------------------------------------
  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:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
␛[2C- Program update status... ␛[32C [ NO UPDATE ]

[+] System tools
------------------------------------
␛[2C- Scanning available tools...␛[30C
␛[2C- Checking system binaries...␛[30C

[+] Plugins (phase 1)
------------------------------------
␛[0CNote: plugins have more extensive tests and may take several minutes to complete␛[0C
␛[0C ␛[0C
␛[2C- Plugins enabled␛[42C [ NONE ]

[+] Boot and services
------------------------------------
␛[2C- Service Manager␛[42C [ systemd ]
␛[2C- Checking UEFI boot␛[39C [ DISABLED ]
␛[2C- Checking presence GRUB2␛[34C [ FOUND ]
␛[4C- Checking for password protection␛[23C [ NONE ]
␛[2C- Check running services (systemctl)␛[23C [ DONE ]
␛[8CResult: found 31 running services␛[20C
␛[2C- Check enabled services at boot (systemctl)␛[15C [ DONE ]
␛[8CResult: found 63 enabled services␛[20C
␛[2C- Check startup files (permissions)␛[24C [ OK ]
␛[2C- Running 'systemd-analyze security'␛[23C
␛[6CUnit name (exposure value) and predicate␛[15C
␛[6C--------------------------------␛[23C
```

```
␛[4C- ModemManager.service (value=6.2)␛[23C [ MEDIUM ]
␛[4C- NetworkManager.service (value=7.8)␛[21C [ EXPOSED ]
␛[4C- accounts-daemon.service (value=9.6)␛[20C [ UNSAFE ]
␛[4C- acpid.service (value=9.6)␛[30C [ UNSAFE ]
␛[4C- alsa-state.service (value=9.6)␛[25C [ UNSAFE ]
␛[4C- anacron.service (value=9.6)␛[28C [ UNSAFE ]
␛[4C- apport.service (value=9.6)␛[29C [ UNSAFE ]
␛[4C- avahi-daemon.service (value=9.6)␛[23C [ UNSAFE ]
␛[4C- colord.service (value=8.8)␛[29C [ EXPOSED ]
␛[4C- cron.service (value=9.6)␛[31C [ UNSAFE ]
␛[4C- cups-browsed.service (value=9.6)␛[23C [ UNSAFE ]
␛[4C- cups.service (value=9.6)␛[31C [ UNSAFE ]
␛[4C- dbus.service (value=9.6)␛[31C [ UNSAFE ]
␛[4C- dmesg.service (value=9.6)␛[30C [ UNSAFE ]
␛[4C- emergency.service (value=9.5)␛[26C [ UNSAFE ]
␛[4C- fwupd.service (value=7.8)␛[30C [ EXPOSED ]
␛[4C- gdm.service (value=9.8)␛[32C [ UNSAFE ]
␛[4C- getty@tty1.service (value=9.6)␛[25C [ UNSAFE ]
␛[4C- irqbalance.service (value=6.1)␛[25C [ MEDIUM ]
␛[4C- kerneloops.service (value=9.2)␛[25C [ UNSAFE ]
␛[4C- networkd-dispatcher.service (value=9.6)␛[16C [ UNSAFE ]
␛[4C- ondemand.service (value=9.6)␛[27C [ UNSAFE ]
␛[4C- open-vm-tools.service (value=9.5)␛[22C [ UNSAFE ]
␛[4C- plymouth-start.service (value=9.5)␛[21C [ UNSAFE ]
␛[4C- polkit.service (value=9.6)␛[29C [ UNSAFE ]
␛[4C- rc-local.service (value=9.6)␛[27C [ UNSAFE ]
␛[4C- rescue.service (value=9.5)␛[29C [ UNSAFE ]
␛[4C- rsync.service (value=9.6)␛[30C [ UNSAFE ]
␛[4C- rsyslog.service (value=9.6)␛[28C [ UNSAFE ]
␛[4C- rtkit-daemon.service (value=7.1)␛[23C [ MEDIUM ]
␛[4C- snapd.service (value=9.8)␛[30C [ UNSAFE ]
␛[4C- switcheroo-control.service (value=7.5)␛[17C [ EXPOSED ]
␛[4C- systemd-ask-password-console.service (value=9.3)␛[7C [ UNSAFE ]
␛[4C- systemd-ask-password-plymouth.service (value=9.5)␛[6C [ UNSAFE ]
␛[4C- systemd-ask-password-wall.service (value=9.4)␛[10C [ UNSAFE ]
␛[4C- systemd-fsckd.service (value=9.5)␛[22C [ UNSAFE ]
␛[4C- systemd-initctl.service (value=9.3)␛[20C [ UNSAFE ]
␛[4C- systemd-journald.service (value=4.4)␛[19C [ PROTECTED ]
␛[4C- systemd-logind.service (value=2.8)␛[21C [ PROTECTED ]
␛[4C- systemd-networkd.service (value=3.1)␛[19C [ PROTECTED ]
␛[4C- systemd-resolved.service (value=2.2)␛[19C [ PROTECTED ]
␛[4C- systemd-rfkill.service (value=9.3)␛[21C [ UNSAFE ]
␛[4C- systemd-timesyncd.service (value=2.1)␛[18C [ PROTECTED ]
␛[4C- systemd-udevd.service (value=8.4)␛[22C [ EXPOSED ]
␛[4C- thermald.service (value=9.6)␛[27C [ UNSAFE ]
␛[4C- ubuntu-advantage.service (value=9.6)␛[19C [ UNSAFE ]
␛[4C- udisks2.service (value=9.6)␛[28C [ UNSAFE ]
␛[4C- unattended-upgrades.service (value=9.6)␛[16C [ UNSAFE ]
␛[4C- upower.service (value=2.3)␛[29C [ PROTECTED ]
␛[4C- user@1000.service (value=9.4)␛[26C [ UNSAFE ]
␛[4C- uuidd.service (value=4.5)␛[30C [ PROTECTED ]
␛[4C- vgauth.service (value=9.5)␛[29C [ UNSAFE ]
␛[4C- whoopsie.service (value=9.6)␛[27C [ UNSAFE ]
␛[4C- wpa_supplicant.service (value=9.6)␛[21C [ UNSAFE ]

[+] Kernel
------------------------------------
␛[2C- Checking default runlevel␛[32C [ runlevel 5 ]
␛[2C- Checking CPU support (NX/PAE)␛[28C
␛[4CCPU support: PAE and/or NoeXecute supported␛[14C [ FOUND ]
␛[2C- Checking kernel version and release␛[22C [ DONE ]
␛[2C- Checking kernel type␛[37C [ DONE ]
␛[2C- Checking loaded kernel modules␛[27C [ DONE ]
␛[6CFound 83 active modules␛[32C
␛[2C- Checking Linux kernel configuration file␛[17C [ FOUND ]
␛[2C- Checking default I/O kernel scheduler␛[20C [ NOT FOUND ]
```

```
␛[2C- Checking for available kernel update␛[21C [ OK ]
␛[2C- Checking core dumps configuration␛[24C
␛[4C- configuration in systemd conf files␛[20C [ DEFAULT ]
␛[4C- configuration in /etc/profile␛[26C [ DEFAULT ]
␛[4C- 'hard' configuration in /etc/security/limits.conf␛[6C [ DEFAULT ]
␛[4C- 'soft' configuration in /etc/security/limits.conf␛[6C [ DEFAULT ]
␛[4C- Checking setuid core dumps configuration␛[15C [ PROTECTED ]
␛[2C- Check if reboot is needed␛[32C [ NO ]

[+] Memory and Processes
------------------------------------
␛[2C- Checking /proc/meminfo␛[35C [ FOUND ]
␛[2C- Searching for dead/zombie processes␛[22C [ NOT FOUND ]
␛[2C- Searching for IO waiting processes␛[23C [ NOT FOUND ]
␛[2C- Search prelink tooling␛[35C [ NOT FOUND ]

[+] Users, Groups and Authentication
------------------------------------
␛[2C- Administrator accounts␛[35C [ OK ]
␛[2C- Unique UIDs␛[46C [ OK ]
␛[2C- Consistency of group files (grpck)␛[23C [ OK ]
␛[2C- Unique group IDs␛[41C [ OK ]
␛[2C- Unique group names␛[39C [ OK ]
␛[2C- Password file consistency␛[32C [ OK ]
␛[2C- Password hashing methods␛[33C [ SUGGESTION ]
␛[2C- Checking password hashing rounds␛[25C [ DISABLED ]
␛[2C- Query system users (non daemons)␛[25C [ DONE ]
␛[2C- NIS+ authentication support␛[30C [ NOT ENABLED ]
␛[2C- NIS authentication support␛[31C [ NOT ENABLED ]
␛[2C- Sudoers file(s)␛[42C [ FOUND ]
␛[4C- Permissions for directory: /etc/sudoers.d␛[14C [ WARNING ]
␛[4C- Permissions for: /etc/sudoers␛[26C [ OK ]
␛[4C- Permissions for: /etc/sudoers.d/README␛[17C [ OK ]
␛[2C- PAM password strength tools␛[30C [ SUGGESTION ]
␛[2C- PAM configuration files (pam.conf)␛[23C [ FOUND ]
␛[2C- PAM configuration files (pam.d)␛[26C [ FOUND ]
␛[2C- PAM modules␛[46C [ FOUND ]
␛[2C- LDAP module in PAM␛[39C [ NOT FOUND ]
␛[2C- Accounts without expire date␛[29C [ SUGGESTION ]
␛[2C- Accounts without password␛[32C [ OK ]
␛[2C- Locked accounts␛[42C [ OK ]
␛[2C- Checking user password aging (minimum)␛[19C [ DISABLED ]
␛[2C- User password aging (maximum)␛[28C [ DISABLED ]
␛[2C- Checking expired passwords␛[31C [ OK ]
␛[2C- Checking Linux single user mode authentication␛[11C [ OK ]
␛[2C- Determining default umask␛[32C
␛[4C- umask (/etc/profile)␛[35C [ NOT FOUND ]
␛[4C- umask (/etc/login.defs)␛[32C [ SUGGESTION ]
␛[2C- LDAP authentication support␛[30C [ NOT ENABLED ]
␛[2C- Logging failed login attempts␛[28C [ ENABLED ]

[+] Kerberos
------------------------------------
␛[2C- Check for Kerberos KDC and principals␛[20C [ NOT FOUND ]

[+] Shells
------------------------------------
␛[2C- Checking shells from /etc/shells␛[25C
␛[4CResult: found 7 shells (valid shells: 7).␛[16C
␛[4C- Session timeout settings/tools␛[25C [ NONE ]
␛[2C- Checking default umask values␛[28C
␛[4C- Checking default umask in /etc/bash.bashrc␛[13C [ NONE ]
␛[4C- Checking default umask in /etc/profile␛[17C [ NONE ]

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

```
␛[2C- Checking mount points␛[36C
␛[4C- Checking /home mount point␛[29C [ SUGGESTION ]
␛[4C- Checking /tmp mount point␛[30C [ SUGGESTION ]
␛[4C- Checking /var mount point␛[30C [ SUGGESTION ]
␛[2C- Query swap partitions (fstab)␛[28C [ OK ]
␛[2C- Testing swap partitions␛[34C [ OK ]
␛[2C- Testing /proc mount (hidepid)␛[28C [ SUGGESTION ]
␛[2C- Checking for old files in /tmp␛[27C [ OK ]
␛[2C- Checking /tmp sticky bit␛[33C [ OK ]
␛[2C- Checking /var/tmp sticky bit␛[29C [ OK ]
␛[2C- ACL support root file system␛[29C [ ENABLED ]
␛[2C- Mount options of /␛[39C [ NON DEFAULT ]
␛[2C- Mount options of /dev␛[36C [ HARDENED ]
␛[2C- Mount options of /dev/shm␛[32C [ PARTIALLY HARDENED ]
␛[2C- Mount options of /run␛[36C [ HARDENED ]
␛[2C- Total without nodev:7 noexec:17 nosuid:13 ro or noexec (W^X): 9 of total 48␛[0C
␛[2C- Disable kernel support of some filesystems␛[15C

[+] USB Devices
------------------------------------
␛[2C- Checking usb-storage driver (modprobe config)␛[12C [ NOT DISABLED ]
␛[2C- Checking USB devices authorization␛[23C [ ENABLED ]
␛[2C- Checking USBGuard␛[40C [ NOT FOUND ]

[+] Storage
------------------------------------
␛[2C- Checking firewire ohci driver (modprobe config)␛[10C [ DISABLED ]

[+] NFS
------------------------------------
␛[2C- Check running NFS daemon␛[33C [ NOT FOUND ]

[+] Name services
------------------------------------
␛[2C- Checking /etc/resolv.conf options␛[24C [ FOUND ]
␛[2C- Searching DNS domain name␛[32C [ UNKNOWN ]
␛[2C- Checking /etc/hosts␛[38C
␛[4C- Duplicate entries in hosts file␛[24C [ NONE ]
␛[4C- Presence of configured hostname in /etc/hosts␛[10C [ FOUND ]
␛[4C- Hostname mapped to localhost␛[27C [ NOT FOUND ]
␛[4C- Localhost mapping to IP address␛[24C [ OK ]

[+] Ports and packages
------------------------------------
␛[2C- Searching package managers␛[31C
␛[4C- Searching dpkg package manager␛[25C [ FOUND ]
␛[6C- Querying package manager␛[29C

  [WARNING]: Test PKGS-7345 had a long execution: 18.436642 seconds

␛[4C- Query unpurged packages␛[32C [ FOUND ]
␛[2C- Checking security repository in sources.list file␛[8C [ OK ]
␛[2C- Checking APT package database␛[28C [ OK ]

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

  Exception found!

  Function/test:  [PKGS-7392:1]
  Message:        Apt-check did not provide any result

  Help improving the Lynis community with your feedback!

  Steps:
  - Ensure you are running the latest version (/usr/local/bin/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!

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

␛[2C- Checking vulnerable packages (apt-get only)␛[14C [ DONE ]

  [WARNING]: Test PKGS-7392 had a long execution: 23.921180 seconds

␛[2C- Checking upgradeable packages␛[28C [ SKIPPED ]
␛[2C- Checking package audit tool␛[30C [ INSTALLED ]
␛[4CFound: apt-check␛[41C
␛[2C- Toolkit for automatic upgrades (unattended-upgrade)␛[6C [ FOUND ]

[+] Networking
------------------------------------
␛[2C- Checking IPv6 configuration␛[30C [ ENABLED ]
␛[6CConfiguration method␛[35C [ AUTO ]
␛[6CIPv6 only␛[46C [ NO ]
␛[2C- Checking configured nameservers␛[26C
␛[4C- Testing nameservers␛[36C
␛[8CNameserver: 127.0.0.53␛[31C [ OK ]
␛[4C- DNSSEC supported (systemd-resolved)␛[20C [ NO ]
␛[2C- Getting listening ports (TCP/UDP)␛[24C [ DONE ]
␛[2C- Checking promiscuous interfaces␛[26C [ OK ]
␛[2C- Checking status DHCP client␛[30C [ NOT ACTIVE ]
␛[2C- Checking for ARP monitoring software␛[21C [ NOT FOUND ]
␛[2C- Uncommon network protocols␛[31C [ 0 ]

[+] Printers and Spools
------------------------------------
␛[2C- Checking cups daemon␛[37C [ RUNNING ]
␛[2C- Checking CUPS configuration file␛[25C [ OK ]
␛[4C- File permissions␛[39C [ WARNING ]
␛[2C- Checking CUPS addresses/sockets␛[26C [ FOUND ]
␛[2C- Checking lp daemon␛[39C [ NOT RUNNING ]

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

[+] Software: firewalls
------------------------------------
␛[2C- Checking iptables kernel module␛[26C [ FOUND ]
␛[4C- Checking iptables policies of chains␛[19C [ FOUND ]
␛[6C- Chain INPUT (table: filter, target: ACCEPT)␛[10C [ ACCEPT ]
␛[6C- Chain INPUT (table: security, target: ACCEPT)␛[8C [ ACCEPT ]
␛[4C- Checking for empty ruleset␛[29C [ WARNING ]
␛[4C- Checking for unused rules␛[30C [ OK ]
␛[2C- Checking host based firewall␛[29C [ ACTIVE ]

[+] Software: webserver
------------------------------------
␛[2C- Checking Apache␛[42C [ NOT FOUND ]
␛[2C- Checking nginx␛[43C [ NOT FOUND ]

[+] SSH Support
------------------------------------
␛[2C- Checking running SSH daemon␛[30C [ NOT FOUND ]

[+] SNMP Support
------------------------------------
␛[2C- Checking running SNMP daemon␛[29C [ NOT FOUND ]

[+] Databases
------------------------------------
```

```
␛[4CNo database engines found␛[32C

[+] LDAP Services
------------------------------------
␛[2C- Checking OpenLDAP instance␛[31C [ NOT FOUND ]

[+] PHP
------------------------------------
␛[2C- Checking PHP␛[45C [ NOT FOUND ]

[+] Squid Support
------------------------------------
␛[2C- Checking running Squid daemon␛[28C [ NOT FOUND ]

[+] Logging and files
------------------------------------
␛[2C- Checking for a running log daemon␛[24C [ OK ]
␛[4C- Checking Syslog-NG status␛[30C [ NOT FOUND ]
␛[4C- Checking systemd journal status␛[24C [ FOUND ]
␛[4C- Checking Metalog status␛[32C [ NOT FOUND ]
␛[4C- Checking RSyslog status␛[32C [ FOUND ]
␛[4C- Checking RFC 3195 daemon status␛[24C [ NOT FOUND ]
␛[4C- Checking minilogd instances␛[28C [ NOT FOUND ]
␛[4C- Checking wazuh-agent daemon status␛[21C [ NOT FOUND ]
␛[2C- Checking logrotate presence␛[30C [ OK ]
␛[2C- Checking remote logging␛[34C [ NOT ENABLED ]
␛[2C- Checking log directories (static list)␛[19C [ DONE ]
␛[2C- Checking open log files␛[34C [ DONE ]
␛[2C- Checking deleted files in use␛[28C [ FILES FOUND ]

[+] Insecure services
------------------------------------
␛[2C- Installed inetd package␛[34C [ NOT FOUND ]
␛[2C- Installed xinetd package␛[33C [ OK ]
␛[4C- xinetd status␛[42C [ NOT ACTIVE ]
␛[2C- Installed rsh client package␛[29C [ OK ]
␛[2C- Installed rsh server package␛[29C [ OK ]
␛[2C- Installed telnet client package␛[26C [ OK ]
␛[2C- Installed telnet server package␛[26C [ NOT FOUND ]
␛[2C- Checking NIS client installation␛[25C [ OK ]
␛[2C- Checking NIS server installation␛[25C [ OK ]
␛[2C- Checking TFTP client installation␛[24C [ OK ]
␛[2C- Checking TFTP server installation␛[24C [ OK ]

[+] Banners and identification
------------------------------------
␛[2C- /etc/issue␛[47C [ FOUND ]
␛[4C- /etc/issue contents␛[36C [ WEAK ]
␛[2C- /etc/issue.net␛[43C [ FOUND ]
␛[4C- /etc/issue.net contents␛[32C [ WEAK ]

[+] Scheduled tasks
------------------------------------
␛[2C- Checking crontab and cronjob files␛[23C [ DONE ]

[+] Accounting
------------------------------------
␛[2C- Checking accounting information␛[26C [ NOT FOUND ]
␛[2C- Checking sysstat accounting data␛[25C [ NOT FOUND ]
␛[2C- Checking auditd␛[42C [ NOT FOUND ]

[+] Time and Synchronization
------------------------------------
␛[2C- NTP daemon found: systemd (timesyncd)␛[20C [ FOUND ]
␛[2C- Checking for a running NTP daemon or client␛[14C [ OK ]
␛[2C- Last time synchronization␛[32C [ 1871s ]
```

```
[+] Cryptography
------------------------------------
␛[2C- Checking for expired SSL certificates [0/151]␛[12C [ NONE ]

  [WARNING]: Test CRYP-7902 had a long execution: 24.338504 seconds

␛[2C- Kernel entropy is sufficient␛[29C [ YES ]
␛[2C- HW RNG & rngd␛[44C [ NO ]
␛[2C- SW prng␛[50C [ NO ]
␛[2C- MOR variable not found␛[35C [ WEAK ]

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

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

[+] Security frameworks
------------------------------------
␛[2C- Checking presence AppArmor␛[31C [ FOUND ]
␛[4C- Checking AppArmor status␛[31C [ ENABLED ]
␛[8CFound 131 unconfined processes␛[23C
␛[2C- Checking presence SELinux␛[32C [ NOT FOUND ]
␛[2C- Checking presence TOMOYO Linux␛[27C [ NOT FOUND ]
␛[2C- Checking presence grsecurity␛[29C [ NOT FOUND ]
␛[2C- Checking for implemented MAC framework␛[19C [ OK ]

[+] Software: file integrity
------------------------------------
␛[2C- Checking file integrity tools␛[28C
␛[2C- Checking presence integrity tool␛[25C [ NOT FOUND ]

[+] Software: System tooling
------------------------------------
␛[2C- Checking automation tooling␛[30C
␛[2C- Automation tooling␛[39C [ NOT FOUND ]
␛[2C- Checking for IDS/IPS tooling␛[29C [ NONE ]

[+] Software: Malware
------------------------------------
␛[2C- Malware software components␛[30C [ NOT FOUND ]

[+] File Permissions
------------------------------------
␛[2C- Starting file permissions check␛[26C
␛[4CFile: /boot/grub/grub.cfg␛[32C [ OK ]
␛[4CFile: /etc/crontab␛[39C [ SUGGESTION ]
␛[4CFile: /etc/group␛[41C [ OK ]
␛[4CFile: /etc/group-␛[40C [ OK ]
␛[4CFile: /etc/hosts.allow␛[35C [ OK ]
␛[4CFile: /etc/hosts.deny␛[36C [ OK ]
␛[4CFile: /etc/issue␛[41C [ OK ]
␛[4CFile: /etc/issue.net␛[37C [ OK ]
␛[4CFile: /etc/passwd␛[40C [ OK ]
␛[4CFile: /etc/passwd-␛[39C [ OK ]
␛[4CDirectory: /etc/cron.d␛[35C [ SUGGESTION ]
␛[4CDirectory: /etc/cron.daily␛[31C [ SUGGESTION ]
␛[4CDirectory: /etc/cron.hourly␛[30C [ SUGGESTION ]
␛[4CDirectory: /etc/cron.weekly␛[30C [ SUGGESTION ]
␛[4CDirectory: /etc/cron.monthly␛[29C [ SUGGESTION ]

[+] Home directories
------------------------------------
␛[2C- Permissions of home directories␛[26C [ WARNING ]
␛[2C- Ownership of home directories␛[28C [ OK ]
```

```
␛[2C- Checking shell history files␛[29C [ OK ]

[+] Kernel Hardening
------------------------------------
␛[2C- Comparing sysctl key pairs with scan profile␛[13C
␛[4C- dev.tty.ldisc_autoload (exp: 0)␛[24C [ DIFFERENT ]
␛[4C- fs.protected_fifos (exp: 2)␛[28C [ DIFFERENT ]
␛[4C- fs.protected_hardlinks (exp: 1)␛[24C [ OK ]
␛[4C- fs.protected_regular (exp: 2)␛[26C [ OK ]
␛[4C- fs.protected_symlinks (exp: 1)␛[25C [ OK ]
␛[4C- fs.suid_dumpable (exp: 0)␛[30C [ DIFFERENT ]
␛[4C- kernel.core_uses_pid (exp: 1)␛[26C [ DIFFERENT ]
␛[4C- kernel.ctrl-alt-del (exp: 0)␛[27C [ OK ]
␛[4C- kernel.dmesg_restrict (exp: 1)␛[25C [ DIFFERENT ]
␛[4C- kernel.kptr_restrict (exp: 2)␛[26C [ DIFFERENT ]
␛[4C- kernel.modules_disabled (exp: 1)␛[23C [ DIFFERENT ]
␛[4C- kernel.perf_event_paranoid (exp: 2 3 4)␛[16C [ OK ]
␛[4C- kernel.randomize_va_space (exp: 2)␛[21C [ OK ]
␛[4C- kernel.sysrq (exp: 0)␛[34C [ DIFFERENT ]
␛[4C- kernel.unprivileged_bpf_disabled (exp: 1)␛[14C [ DIFFERENT ]
␛[4C- kernel.yama.ptrace_scope (exp: 1 2 3)␛[18C [ OK ]
␛[4C- net.core.bpf_jit_harden (exp: 2)␛[23C [ DIFFERENT ]
␛[4C- net.ipv4.conf.all.accept_redirects (exp: 0)␛[12C [ DIFFERENT ]
␛[4C- net.ipv4.conf.all.accept_source_route (exp: 0)␛[9C [ OK ]
␛[4C- net.ipv4.conf.all.bootp_relay (exp: 0)␛[17C [ OK ]
␛[4C- net.ipv4.conf.all.forwarding (exp: 0)␛[18C [ OK ]
␛[4C- net.ipv4.conf.all.log_martians (exp: 1)␛[16C [ DIFFERENT ]
␛[4C- net.ipv4.conf.all.mc_forwarding (exp: 0)␛[15C [ OK ]
␛[4C- net.ipv4.conf.all.proxy_arp (exp: 0)␛[19C [ OK ]
␛[4C- net.ipv4.conf.all.rp_filter (exp: 1)␛[19C [ DIFFERENT ]
␛[4C- net.ipv4.conf.all.send_redirects (exp: 0)␛[14C [ DIFFERENT ]
␛[4C- net.ipv4.conf.default.accept_redirects (exp: 0)␛[8C [ DIFFERENT ]
␛[4C- net.ipv4.conf.default.accept_source_route (exp: 0)␛[5C [ DIFFERENT ]
␛[4C- net.ipv4.conf.default.log_martians (exp: 1)␛[12C [ DIFFERENT ]
␛[4C- net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)␛[10C [ OK ]
␛[4C- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1)␛[4C [ OK ]
␛[4C- net.ipv4.tcp_syncookies (exp: 1)␛[23C [ OK ]
␛[4C- net.ipv4.tcp_timestamps (exp: 0 1)␛[21C [ OK ]
␛[4C- net.ipv6.conf.all.accept_redirects (exp: 0)␛[12C [ DIFFERENT ]
␛[4C- net.ipv6.conf.all.accept_source_route (exp: 0)␛[9C [ OK ]
␛[4C- net.ipv6.conf.default.accept_redirects (exp: 0)␛[8C [ DIFFERENT ]
␛[4C- net.ipv6.conf.default.accept_source_route (exp: 0)␛[5C [ OK ]

[+] Hardening
------------------------------------
␛[4C- Installed compiler(s)␛[34C [ FOUND ]
␛[4C- Installed malware scanner␛[30C [ NOT FOUND ]
␛[4C- Non-native binary formats␛[30C [ NOT FOUND ]

[+] Custom tests
------------------------------------
␛[2C- Running custom tests... ␛[33C [ NONE ]

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

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

  -[ Lynis 3.1.5 Results ]-

  Warnings (2):
  ----------------------------
  ! This version 20.04 is marked end-of-life as of 2025-04-01 [GEN-0010]
      https://cisofy.com/lynis/controls/GEN-0010/

  ! iptables module(s) loaded, but no rules active [FIRE-4512]
```

```
      https://cisofy.com/lynis/controls/FIRE-4512/

  Suggestions (39):
  ----------------------------
  * This release is more than 4 months old. Check the website or GitHub to see if there
is an update available. [LYNIS]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/LYNIS/

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

  * 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/

  * 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/

  * Check PAM configuration, add rounds if applicable and expire passwords to encrypt
with new values [AUTH-9229]
    - 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-9229/

  * 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/

  * 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/

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

  * Purge old/removed packages (1 found) with aptitude purge or dpkg --purge command.
This will cleanup old configuration files, cron jobs and startup scripts. [PKGS-7346]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/PKGS-7346/

  * Install debsums utility for the verification of packages with known good database.
[PKGS-7370]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/PKGS-7370/

  * Check if system is up-to-date, security updates test (apt-check) gives an unexpected
result [PKGS-7392]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/PKGS-7392/

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

  * 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/

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

  * Check what deleted files are still in use and why. [LOGG-2190]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/LOGG-2190/

  * 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/

  * Double check the permissions of home directories as some might be not strict enough.
[HOME-9304]
    - Related resources
      * Website: 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>)
    - 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 compilers like restricting access to root user only [HRDN-7222]
    - Related resources
      * Article: Why remove compilers from your system?: https://linux-audit.com/software/-
why-remove-compilers-from-your-system/
      * Website: 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, 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:

  Hardening index : 64 [############        ]
  Tests performed : 245
  Plugins enabled : 0

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

  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

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

  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 3.1.5
  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2024, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

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

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