Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

Lynis

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

Lynis

Lynis est un outil d'audit de sécurité **open-source**, complet et extensible, conçu pour les systèmes d'exploitation basés sur UNIX (Linux, macOS, BSD, AIX, Solaris, etc.).

Type : Audit de sécurité "Host-based" (audit local) et Hardening (durcissement).

Langage : Écrit entièrement en **Shell Script (POSIX)**. Cela le rend totalement transparent (le code est lisible) et portable (pas de compilation nécessaire).

Installation : Aucune dépendance lourde requise. Peut s'exécuter en mode "portable" (depuis une clé USB ou un dossier local) ou être installé via les paquets (apt, yum, etc.).

Privilèges : Nécessite les droits **root** pour un audit complet (accès aux logs, configurations système, shadow file, etc.).

Contrairement à un scanner de vulnérabilités réseau (comme Nessus ou OpenVAS) qui scanne les ports de l'extérieur, Lynis s'exécute **sur** la machine. Il effectue des centaines de tests individuels basés sur :

- **L'analyse des fichiers de configuration** (SSH, Apache, Nginx, sysctl, systemd...).
- **La vérification des binaires** et de leurs versions.
- **L'analyse des permissions** de fichiers et répertoires.
- **La détection de logiciels malveillants** (rootkits) ou de traces d'intrusion.

Résultats et Rapports

- **Hardening Index :** Fournit un score global de sécurité (de 0 à 100).
- **Catégorisation :**
  - **Warnings :** Problèmes critiques à corriger immédiatement.
  - **Suggestions :** Recommandations pour durcir le système (bonnes pratiques CIS/NIST).
- **Logs :** Génère deux fichiers clés :
  - /var/log/lynis.log : Journal technique détaillé de tous les tests.
  - /var/log/lynis-report.dat : Fichier structuré pour l'intégration dans des outils de reporting ou des dashboards.

Download Lynis

```
admin@laptop:~$ wget -P /home/admin/Public/ https://downloads.cisofy.com/lynis/lynis-3.1.6.tar.gz
--2025-12-09 20:47:24--  https://downloads.cisofy.com/lynis/lynis-3.1.6.tar.gz
Resolving downloads.cisofy.com (downloads.cisofy.com)... 2a01:7c8:e001:1cb::c1d4, 89.41.171.41
Connecting to downloads.cisofy.com (downloads.cisofy.com)|2a01:7c8:e001:1cb::c1d4|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 354692 (346K) [application/octet-stream]
Saving to: ‘/home/admin/Public/lynis-3.1.6.tar.gz.1’

lynis-3.1.6.tar.gz.1                100%
[===================================================================>] 346.38K  --.-KB/s    in 0.1s

2025-12-09 20:47:25 (3.16 MB/s) - ‘/home/thomas/Public/lynis-3.1.6.tar.gz.1’ saved [354692/354692]
```

UnZIP

```
admin@laptop:~$ cd /home/admin/Public/
admin@laptop:~/Public$ tar -xzf lynis-3.1.6.tar.gz -C /home/admin/Public/
```

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

Lancement de l'audit système

```
admin@laptop:~$ cd /home/admin/Public/lynis/
admin@laptop:~/Public/lynis$ chmod +x lynis
```

```
admin@laptop:~/Public/lynis$ sudo ./lynis audit system
[sudo] password for admin:


[!] Change ownership of /home/admin/Public/lynis/include/functions to 'root' or similar (found: admin with UID
1000).

    Command:
      # chown 0:0 /home/admin/Public/lynis/include/functions

[X] Security check failed

    Why do I see this error?
    ------------------------------
    This is a protection mechanism to prevent the root user from executing user created files. The files may be
altered, or including malicious pieces of script.

    What can I do?
    ---------------------
    Option 1) Check if a trusted user created the files (e.g. due to using Git, Homebrew or similar).
              If you trust these files, you can decide to continue this run by pressing ENTER.

    Option 2) Change ownership of the related files (or full directory).

       Commands (full directory):
         # cd ..
         # chown -R 0:0 lynis
         # cd lynis
         # ./lynis audit system

[ Press ENTER to continue, or CTRL+C to cancel ]

[ Lynis 3.1.6 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

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


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

  ---------------------------------------------------
  Program version:           3.1.6
  Operating system:          Linux
  Operating system name:     Debian
  Operating system version:  13
  End-of-life:               UNKNOWN
  Kernel version:            6.12.57+deb13
  Hardware platform:         x86_64
  Hostname:                  laptop
  ---------------------------------------------------
  Profiles:                  /home/admin/Public/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          ./plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                                  [ NO UPDATE ]
```

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

```
[+] 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                                       [ ENABLED ]
  - Checking Secure Boot                                     [ DISABLED ]
  - Checking presence GRUB2                                  [ FOUND ]
    - Checking for password protection                       [ NONE ]
  - Check running services (systemctl)                       [ DONE ]
       Result: found 28 running services
  - Check enabled services at boot (systemctl)               [ DONE ]
       Result: found 39 enabled services
  - Check startup files (permissions)                        [ OK ]
  - Running 'systemd-analyze security'
    Unit name (exposure value) and predicate
    ---------------------------------
    - ModemManager.service (value=6.3)                       [ MEDIUM ]
    - NetworkManager.service (value=7.8)                     [ EXPOSED ]
    - accounts-daemon.service (value=5.5)                    [ MEDIUM ]
    - alsa-state.service (value=9.6)                         [ UNSAFE ]
    - anacron.service (value=9.6)                            [ UNSAFE ]
    - avahi-daemon.service (value=9.6)                       [ UNSAFE ]
    - blueman-mechanism.service (value=9.6)                  [ UNSAFE ]
    - bluetooth.service (value=6.0)                          [ MEDIUM ]
    - chrony.service (value=3.5)                             [ PROTECTED ]
    - colord.service (value=3.5)                             [ PROTECTED ]
    - cron.service (value=9.6)                               [ UNSAFE ]
    - cups-browsed.service (value=9.6)                       [ UNSAFE ]
    - cups.service (value=9.6)                               [ UNSAFE ]
    - dbus.service (value=9.3)                               [ UNSAFE ]
    - dm-event.service (value=9.5)                           [ UNSAFE ]
    - emergency.service (value=9.5)                          [ UNSAFE ]
    - getty@tty1.service (value=9.6)                         [ UNSAFE ]
    - iscsid.service (value=9.5)                             [ UNSAFE ]
    - libvirtd.service (value=9.6)                           [ UNSAFE ]
    - lightdm.service (value=9.6)                            [ UNSAFE ]
    - lvm2-lvmpolld.service (value=9.5)                      [ UNSAFE ]
    - plymouth-halt.service (value=9.5)                      [ UNSAFE ]
    - plymouth-kexec.service (value=9.5)                     [ UNSAFE ]
    - plymouth-poweroff.service (value=9.5)                  [ UNSAFE ]
    - plymouth-reboot.service (value=9.5)                    [ UNSAFE ]
    - plymouth-start.service (value=9.5)                     [ UNSAFE ]
    - polkit.service (value=1.2)                             [ PROTECTED ]
    - rc-local.service (value=9.6)                           [ UNSAFE ]
    - rescue.service (value=9.5)                             [ UNSAFE ]
    - resolvconf.service (value=9.5)                         [ UNSAFE ]
    - rtkit-daemon.service (value=7.2)                       [ MEDIUM ]
    - ssh.service (value=9.6)                                [ UNSAFE ]
    - sshd@sshd-keygen.service (value=9.6)                   [ UNSAFE ]
    - switcheroo-control.service (value=7.6)                 [ EXPOSED ]
    - systemd-ask-password-console.service (value=9.4)       [ UNSAFE ]
    - systemd-ask-password-plymouth.service (value=9.5)      [ UNSAFE ]
    - systemd-ask-password-wall.service (value=9.4)          [ UNSAFE ]
    - systemd-bsod.service (value=9.5)                       [ UNSAFE ]
    - systemd-hostnamed.service (value=1.7)                  [ PROTECTED ]
    - systemd-importd.service (value=5.0)                    [ MEDIUM ]
    - systemd-initctl.service (value=9.4)                    [ UNSAFE ]
    - systemd-journald.service (value=4.9)                   [ PROTECTED ]
    - systemd-logind.service (value=2.8)                     [ PROTECTED ]
    - systemd-machined.service (value=6.2)                   [ MEDIUM ]
    - systemd-networkd.service (value=2.9)                   [ PROTECTED ]
    - systemd-rfkill.service (value=9.4)                     [ UNSAFE ]
    - systemd-udevd.service (value=7.1)                      [ MEDIUM ]
    - udisks2.service (value=9.6)                            [ UNSAFE ]
    - upower.service (value=2.4)                             [ PROTECTED ]
    - user@1000.service (value=9.4)                          [ UNSAFE ]
    - virtlockd.service (value=9.6)                          [ UNSAFE ]
    - virtlogd.service (value=2.2)                           [ PROTECTED ]
    - wpa_supplicant.service (value=9.6)                     [ UNSAFE ]

[+] Kernel
```

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

```
------------------------------------
  - Checking default runlevel                               [ runlevel 5 ]
  - Checking CPU support (NX/PAE)
    CPU support: PAE and/or NoeXecute supported             [ FOUND ]
  - Checking kernel version and release                     [ DONE ]
  - Checking kernel type                                    [ DONE ]
  - Checking loaded kernel modules                          [ DONE ]
      Found 186 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     [ ENABLED ]
    - 'soft' configuration in /etc/security/limits.conf     [ 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                      [ FOUND ]
  - Search prelink tooling                                  [ NOT FOUND ]

[+] Users, Groups and Authentication
------------------------------------
  - Administrator accounts                                  [ OK ]
  - Unique UIDs                                             [ OK ]
  - Consistency of group files (grpck)                      [ OK ]
  - Unique group IDs                                        [ OK ]
  - Unique group names                                      [ OK ]
  - Password file consistency                               [ OK ]
  - Password hashing methods                                [ OK ]
  - Checking password hashing rounds                        [ DISABLED ]
  - Query system users (non daemons)                        [ DONE ]
  - NIS+ authentication support                             [ NOT ENABLED ]
  - NIS authentication support                              [ NOT ENABLED ]
  - Sudoers file(s)                                         [ FOUND ]
    - Permissions for directory: /etc/sudoers.d             [ WARNING ]
    - Permissions for: /etc/sudoers                         [ OK ]
    - Permissions for: /etc/sudoers.d/README                [ OK ]
  - PAM password strength tools                             [ SUGGESTION ]
  - PAM configuration files (pam.conf)                      [ FOUND ]
  - PAM configuration files (pam.d)                         [ FOUND ]
  - PAM modules                                             [ FOUND ]
  - LDAP module in PAM                                      [ NOT FOUND ]
  - Accounts without expire date                            [ SUGGESTION ]
  - Accounts without password                               [ OK ]
  - Locked accounts                                         [ FOUND ]
  - 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                           [ DISABLED ]

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

[+] 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                            [ OK ]
    - Checking /tmp mount point                             [ OK ]
    - Checking /var mount point                             [ SUGGESTION ]
  - Query swap partitions (fstab)                           [ OK ]
```

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

```
  - 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 /dev                                      [ PARTIALLY HARDENED ]
  - Mount options of /dev/shm                                  [ PARTIALLY HARDENED ]
  - Mount options of /home                                     [ DEFAULT ]
  - Mount options of /run                                      [ HARDENED ]
  - Mount options of /tmp                                      [ PARTIALLY HARDENED ]
  - Total without nodev:6 noexec:10 nosuid:4 ro or noexec (W^X): 10 of total 28
  - Disable kernel support of some filesystems

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

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

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

[+] Name services
------------------------------------
  - Checking search domains                                    [ FOUND ]
  - Searching DNS domain name                                  [ UNKNOWN ]
  - Checking /etc/hosts
    - Duplicate entries in hosts file                          [ NONE ]
    - Presence of configured hostname in /etc/hosts            [ FOUND ]
    - Hostname mapped to localhost                             [ NOT FOUND ]
    - Localhost mapping to IP address                          [ OK ]

[+] Ports and packages
------------------------------------
  - Searching package managers
    - Searching dpkg package manager                           [ FOUND ]
      - Querying package manager
    - Query unpurged packages                                  [ 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                             [ NOT FOUND ]

[+] Networking
------------------------------------
  - Checking IPv6 configuration                                [ ENABLED ]
      Configuration method                                     [ AUTO ]
      IPv6 only                                                [ NO ]
  - Checking configured nameservers
    - Testing nameservers
        Nameserver: 9.9.9.9                                    [ OK ]
        Nameserver: 192.168.139.254                            [ OK ]
        Nameserver: 2a01:cb19:900a:b700:1adf:26ff:fea7:9350    [ OK ]
        Nameserver: fe80::1adf:26ff:fea7:9350%enp5s0           [ OK ]
    - Minimal of 2 responsive nameservers                      [ OK ]
  - Checking default gateway                                   [ DONE ]
  - Getting listening ports (TCP/UDP)                          [ DONE ]
  - Checking promiscuous interfaces                            [ OK ]
  - Checking waiting connections                               [ OK ]
  - Checking status DHCP client                                [ NOT ACTIVE ]
  - Checking for ARP monitoring software                       [ NOT FOUND ]
  - Uncommon network protocols                                 [ 0 ]

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

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

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

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

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

[+] SSH Support
------------------------------------
  - Checking running SSH daemon                             [ FOUND ]
    - Searching SSH configuration                           [ FOUND ]
    - OpenSSH option: AllowTcpForwarding                    [ SUGGESTION ]
    - OpenSSH option: ClientAliveCountMax                   [ SUGGESTION ]
    - OpenSSH option: ClientAliveInterval                   [ OK ]
    - OpenSSH option: FingerprintHash                       [ OK ]
    - OpenSSH option: GatewayPorts                          [ OK ]
    - OpenSSH option: IgnoreRhosts                          [ OK ]
    - OpenSSH option: LoginGraceTime                        [ OK ]
    - OpenSSH option: LogLevel                              [ SUGGESTION ]
    - 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                         [ SUGGESTION ]
    - 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                               [ NOT FOUND ]
    - Checking RFC 3195 daemon status                       [ NOT FOUND ]
    - Checking minilogd instances                           [ NOT FOUND ]
    - Checking wazuh-agent daemon status                    [ NOT FOUND ]
  - Checking logrotate presence                             [ OK ]
  - Checking remote logging                                 [ NOT ENABLED ]
  - Checking log directories (static list)                  [ DONE ]
  - Checking open log files                                 [ DONE ]
  - Checking deleted files in use                           [ FILES FOUND ]
```

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

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

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

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

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

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

[+] Cryptography
------------------------------------
  - Checking for expired SSL certificates [0/152]           [ NONE ]

  [WARNING]: Test CRYP-7902 had a long execution: 13.474687 seconds

  - 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 104 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
  - 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
```

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

```
    File: /boot/grub/grub.cfg                                   [ 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                                  [ SUGGESTION ]
    Directory: /root/.ssh                                       [ 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
    - dev.tty.ldisc_autoload (exp: 0)                           [ DIFFERENT ]
    - fs.protected_fifos (exp: 2)                               [ DIFFERENT ]
    - fs.protected_hardlinks (exp: 1)                           [ OK ]
    - fs.protected_regular (exp: 2)                             [ OK ]
    - fs.protected_symlinks (exp: 1)                            [ OK ]
    - fs.suid_dumpable (exp: 0)                                 [ OK ]
    - kernel.core_uses_pid (exp: 1)                             [ OK ]
    - kernel.ctrl-alt-del (exp: 0)                              [ OK ]
    - kernel.dmesg_restrict (exp: 1)                            [ OK ]
    - kernel.kptr_restrict (exp: 2)                             [ DIFFERENT ]
    - kernel.modules_disabled (exp: 1)                          [ DIFFERENT ]
    - kernel.perf_event_paranoid (exp: 2 3 4)                   [ OK ]
    - kernel.randomize_va_space (exp: 2)                        [ OK ]
    - kernel.sysrq (exp: 0)                                     [ DIFFERENT ]
    - kernel.unprivileged_bpf_disabled (exp: 1)                 [ 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)               [ OK ]
    - net.ipv4.conf.all.accept_source_route (exp: 0)            [ OK ]
    - net.ipv4.conf.all.bootp_relay (exp: 0)                    [ OK ]
    - net.ipv4.conf.all.forwarding (exp: 0)                     [ DIFFERENT ]
    - net.ipv4.conf.all.log_martians (exp: 1)                   [ DIFFERENT ]
    - net.ipv4.conf.all.mc_forwarding (exp: 0)                  [ OK ]
    - net.ipv4.conf.all.proxy_arp (exp: 0)                      [ OK ]
    - net.ipv4.conf.all.rp_filter (exp: 1)                      [ DIFFERENT ]
    - net.ipv4.conf.all.send_redirects (exp: 0)                 [ DIFFERENT ]
    - net.ipv4.conf.default.accept_redirects (exp: 0)           [ DIFFERENT ]
    - net.ipv4.conf.default.accept_source_route (exp: 0)        [ OK ]
    - net.ipv4.conf.default.log_martians (exp: 1)               [ DIFFERENT ]
    - net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)             [ OK ]
    - net.ipv4.icmp_ignore_bogus_error_responses (exp: 1)       [ OK ]
    - net.ipv4.tcp_syncookies (exp: 1)                          [ OK ]
    - net.ipv4.tcp_timestamps (exp: 0 1)                        [ OK ]
    - net.ipv6.conf.all.accept_redirects (exp: 0)               [ DIFFERENT ]
    - net.ipv6.conf.all.accept_source_route (exp: 0)            [ OK ]
    - net.ipv6.conf.default.accept_redirects (exp: 0)           [ DIFFERENT ]
    - net.ipv6.conf.default.accept_source_route (exp: 0)        [ OK ]

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

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

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

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

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

```
  -[ Lynis 3.1.6 Results ]-

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

  Suggestions (48):
  ----------------------------
  * 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/

  * Determine runlevel and services at startup [BOOT-5180]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/BOOT-5180/

  * Consider hardening system services [BOOT-5264]
    - Details  : Run '/usr/bin/systemd-analyze security SERVICE' for each service
    - Related resources
      * Article: Systemd features to secure service files: https://linux-audit.com/systemd/systemd-features-to-
secure-units-and-services/
      * Website: https://cisofy.com/lynis/controls/BOOT-5264/

  * Check process listing for processes waiting for IO requests [PROC-3614]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/PROC-3614/

  * Configure password hashing rounds in /etc/login.defs [AUTH-9230]
    - Related resources
      * Article: Linux password security: hashing rounds: https://linux-audit.com/authentication/configure-the-
minimum-password-length-on-linux-systems/
      * Website: https://cisofy.com/lynis/controls/AUTH-9230/

  * Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc or libpam-passwdqc
[AUTH-9262]
    - Related resources
      * Article: Configure minimum password length for Linux systems: https://linux-audit.com/configure-the-
minimum-password-length-on-linux-systems/
      * Website: https://cisofy.com/lynis/controls/AUTH-9262/

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

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

  * Configure minimum password age in /etc/login.defs [AUTH-9286]
    - Related resources
      * Article: Configure minimum password length for Linux systems: https://linux-audit.com/configure-the-
minimum-password-length-on-linux-systems/
      * Website: https://cisofy.com/lynis/controls/AUTH-9286/

  * Configure maximum password age in /etc/login.defs [AUTH-9286]
    - Related resources
      * Article: Configure minimum password length for Linux systems: https://linux-audit.com/configure-the-
minimum-password-length-on-linux-systems/
      * Website: https://cisofy.com/lynis/controls/AUTH-9286/

  * Default umask in /etc/login.defs could not be found and defaults usually to 022, which 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 /var file system, place /var on a separate partition [FILE-6310]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/FILE-6310/

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

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

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

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

  * Purge old/removed packages (7 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/

  * Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or unattended-upgrades
[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/

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

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

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

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

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

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

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

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

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

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

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

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : MaxSessions (set 10 to 2)
```

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

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

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

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

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

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

  * 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/
```

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

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

  * One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
    - Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)
    - Related resources
      * Article: Linux hardening with sysctl settings: https://linux-audit.com/linux-hardening-with-sysctl/
      * Article: Overview of sysctl options and values: https://linux-audit.com/kernel/sysctl/
      * Website: https://cisofy.com/lynis/controls/KRNL-6000/

  * Harden 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:

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

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

  Details:
  Hardening index : 64 [#############        ]
  Tests performed : 254
  Plugins enabled : 0

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

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

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

  Notice: No OS entry was found in the end-of-life database

  What to do:
  Please submit a pull request on GitHub to include your OS version and the end date of this OS version is
being supported
  URL: https://github.com/CISOfy/lynis

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

  Lynis 3.1.6

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

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

Le contenu est disponible sous licence GNU Free Documentation License 1.3 ou ultérieure sauf mention contraire.

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

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

admin@laptop:~/Public/lynis$
```