

# Table des matières

- LYNIS (Audit System Tools) ..... 2**
- Installation* ..... 2**
- Manuel* ..... 2**
- Audit System* ..... 3**
- Score* ..... 4**
- Report* ..... 5**
- Remédiation* ..... 6**



# LYNIS (Audit System Tools)

---

## Installation

```
sudo apt update && sudo apt install lynis
```

## Manuel

```
lynis
```

```
Usage: lynis command [options]

Command:

audit
  audit system           : Perform local security scan
  audit system remote <host> : Remote security scan
  audit dockerfile <file> : Analyze Dockerfile

show
  show                   : Show all commands
  show version           : Show Lynis version
  show help              : Show help

update
  update info           : Show update details

Options:

Alternative system audit modes
--forensics           : Perform forensics on a running or mounted system
--pentest             : Non-privileged, show points of interest for pentesting

Layout options
--no-colors           : Don't use colors in output
--quiet (-q)          : No output
--reverse-colors      : Optimize color display for light backgrounds
--reverse-colours     : Optimize colour display for light backgrounds

Misc options
--debug               : Debug logging to screen
--no-log              : Don't create a log file
--profile <profile>   : Scan the system with the given profile file
--view-manpage (--man) : View man page
--verbose             : Show more details on screen
--version (-V)        : Display version number and quit
--wait                : Wait between a set of tests
--slow-warning <seconds> : Threshold for slow test warning in seconds (default 10)

Enterprise options
--plugindir <path>    : Define path of available plugins
--upload              : Upload data to central node

More options available. Run '/usr/sbin/lynis show options', or use the man page.

No command provided. Exiting..
```

## Audit System

```
lynis audit system
```

```
[+] Initializing program
-----
#####
#                                     #
#  NON-PRIVILEGED SCAN MODE          #
#                                     #
#####

NOTES:
-----
* Some tests will be skipped (as they require root permissions)
* Some tests might fail silently or give different results

- Detecting OS... [ DONE ]
- Checking profiles... [ DONE ]
- Detecting language and localization [ fr ]

-----
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:             Latitude-7410

-----
Profiles:             /etc/lynis/default.prf
Log file:              /home/sylvain/lynis.log
Report file:          /home/sylvain/lynis-report.dat
Report version:       1.0
Plugin directory:    /etc/lynis/plugins

-----
Auditor:              [Not Specified]
Language:             fr
Test category:       all
Test group:          all

-----
- Program update status... [ PAS DE MISE A JOUR ]

[+] Outils système
-----
- Scanning available tools...
- Checking system binaries...

[+] Plugins (phase 1)
-----
Note : Les plugins ont des tests plus poussés qui peuvent prendre plusieurs minutes

- Plugin: debian
  [
[+] Debian Tests
```

## Score

```

Lynis security scan details:

Hardening index : 49 [##### ]
Tests performed : 239
Plugins enabled : 1

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

Scan mode:
Normal [ ] Forensics [ ] Integration [ ] Pentest [V] (running non-privileged)

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

Files:
- Test and debug information : /home/[redacted]/lynis.log
- Report data : /home/[redacted]/lynis-report.dat

```

# Report

```

Great, no warnings

Suggestions (44):
-----
* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
  https://cisofy.com/lynis/controls/LYNIS/

* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]
  https://cisofy.com/lynis/controls/DEB-0280/

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

* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]
  https://cisofy.com/lynis/controls/DEB-0811/

* Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using o
EB-0831]
  https://cisofy.com/lynis/controls/DEB-0831/

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

* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
  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/

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

* Check the output of ps for dead or zombie processes [PROC-3612]
  https://cisofy.com/lynis/controls/PROC-3612/

* Run pwck manually and correct any errors in the password file [AUTH-9228]
  https://cisofy.com/lynis/controls/AUTH-9228/

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

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

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

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

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

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

```

# Remédiation

lynis show details DEB-0280

```
2025-08-20 20:04:35 Performing test ID DEB-0280 (Checking if libpam-tmpdir is installed and enabled.)
2025-08-20 20:04:35 - libpam-tmpdir is not installed.
2025-08-20 20:04:35 Hardening: assigned partial number of hardening points (0 of 2). Currently having 0 points (out of 2)
2025-08-20 20:04:35 Suggestion: Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [test:DEB-0280] [details:-] [solution:-]
2025-08-20 20:04:35 Status: Starting file system checks...
2025-08-20 20:04:35 Status: Starting file system checks for dm-crypt, cryptsetup & cryptmount...
2025-08-20 20:04:35 ===
```

 **En cours de Rédaction !!**

From:  
<https://wiki.mazinger.fr/wiki/> - **My Personal Wiki**

Permanent link:  
<https://wiki.mazinger.fr/wiki/doku.php?id=securite:system:lynis:index>

Last update: **2025/08/20 20:49**

