Lynis Package Description

Lynis is an open source security auditing tool. Its main goal is to audit and harden Unix and Linux based systems. It scans the system by performing many security control checks. Examples include searching for installed software and determine possible configuration flaws.

Many tests are part of common security guidelines and standards, with on top additional security tests. After the scan a report will be displayed with all discovered findings. To provide you with initial guidance, a link is shared to the related Lynis control.

Source: https://cisofy.com/lynis/
Lynis Homepage

- Author: Michael Boelen
- License: GPLv3

Tools included in the lynis package

lynis – Open source security auditing tool

root@kali:~# lynis -h

[Lynis 2.6.2]

```
################################################################################
  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.

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################
```

[+] Initializing program

  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:

--no-log   : Don't create a log file
--pentest   : Non-privileged scan (useful for pentest)
--profile <profile>   : Scan the system with the given profile file
--quick (-Q)   : Quick mode, don't wait for user input

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

Misc options
--debug   : Debug logging to screen
--view-manpage (--man)   : View man page
--verbose   : Show more details on screen
--version (-V)   : Display version number and quit

Enterprise options
--plugin-dir "<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.

lynis Usage Example

Scan the system in quiet mode *(-Q)* and output in cronjob format *(–cronjob)*:

root@kali:~# lynis -Q --cronjob

[Lynis 2.6.2]

###
  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.

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
###

[+] Initializing program

- Detecting OS... [DONE]
- Checking profiles... [DONE]

  Program version: 2.6.2
  Operating system: Linux
  Operating system name: Debian
  Operating system version: kali-rolling
  Kernel version: 4.18.0
  Hardware platform: x86_64
  Hostname: kali

  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

  ...

**Become a Certified
Penetration Tester**

Enroll in Penetration Testing with
Kali Linux, the course required to
become an Offensive Security
Certified Professional (OSCP)