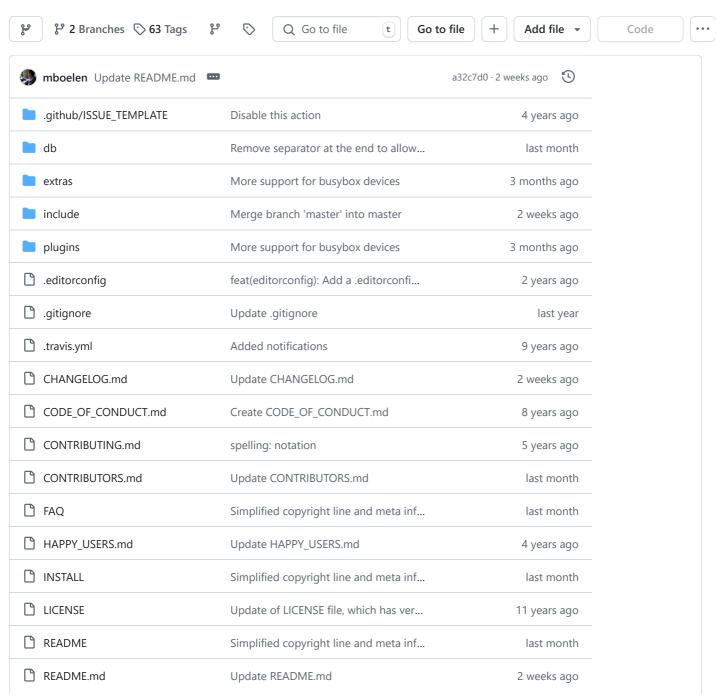


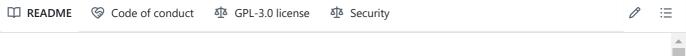
⊙ १ 🕏

Lynis - Security auditing tool for Linux, macOS, and UNIX-based systems. Assists with compliance testing (HIPAA/ISO27001/PCI DSS) and system hardening. Agentless, and installation optional.

- ₲ GPL-3.0 license
- Code of conduct
- Security policy
- ☆ 13.8k stars 💡 1.5k forks ⊙ 342 watching 🐉 Branches Activity 🖃 Custom properties 🕒 Tags
- Public repository



SECURITY.md	Create SECURITY.md file	6 years ago
TODO.md	Updated rationale related to egrep (li	4 years ago
default.prf	Added initial version of a Kerberos pl	9 months ago
developer.prf	Run non-interactive by default, use	6 years ago
lynis	Update lynis	last month
🗋 lynis.8	Fix quote syntax error in manpage	5 years ago



LSE top 10 Lynis (7) build unknown openssf best practices passing Documentation

Do you like this software? Star the project and become a stargazer.

lynis

Lynis - Security auditing and hardening tool, for UNIX-based systems.

Lynis is a security auditing tool for systems based on UNIX like Linux, macOS, BSD, and others. It performs an indepth security scan and runs on the system itself. The primary goal is to test security defenses and provide tips for further system hardening. It will also scan for general system information, vulnerable software packages, and possible configuration issues. Lynis was commonly used by system administrators and auditors to assess the security defenses of their systems. Besides the "blue team," nowadays penetration testers also have Lynis in their toolkit.

We believe software should be **simple**, **updated on a regular basis**, and **open**. You should be able to trust, understand, and have the option to change the software. Many agree with us, as the software is being used by thousands every day to protect their systems.

Goals

The main goals of Lynis include:

- · Automated security auditing
- Compliance testing (e.g. ISO27001, PCI-DSS, HIPAA)
- Vulnerability detection

The software (also) assists with:

- Configuration and asset management
- Software patch management
- System hardening
- Penetration testing (privilege escalation)
- Intrusion detection

Audience

Typical users of the software:

- System administrators
- Auditors
- · Security officers
- Penetration testers
- Security professionals

Installation

There are multiple options available to install Lynis.

Software package

For systems running Linux, BSD, and macOS, there is typically a package available. This is the preferred method of obtaining Lynis, as it is quick to install and easy to update. The Lynis project itself also provides <u>packages</u> in RPM or DEB format suitable for systems systems running: CentOS, Debian, Fedora, OEL, openSUSE, RHEL, Ubuntu, and others.

Some distributions may also have Lynis in their software repository: in repositories 23

Note: Some distributions don't provide an up-to-date version. In that case it is better to use the CISOfy software repository, download the tarball from the website, or download the latest GitHub release.

Git

The very latest developments can be obtained via git.

1. Clone or download the project files (no compilation nor installation is required);

git clone https://github.com/CISOfy/lynis

Q

2. Execute:

cd lynis && ./lynis audit system

Q

If you want to run the software as root (or sudo), we suggest changing the ownership of the files. Use chown - R 0:0 to recursively alter the owner and group and set it to user ID 0 (root). Otherwise Lynis will warn you about the file permissions. After all, you are executing files owned by a non-privileged user.

Documentation

Have a look at the <u>Lynis documentation</u> to learn more about the configuration and usage of Lynis. When you are interested in reading more articles about Linux security, then check out the <u>Linux security blog</u> named Linux Audit. For some suggestions by Lynis, this is also the source used to learn more about specific findings.

Customization

If you want to create your own tests, have a look at the Lynis software development kit.

Security

We participate in the CII best <u>practices</u> badge program of the Linux Foundation.

Media and Awards

Lynis is collecting some awards along the way and we are proud of that.

- 2016
 - Best of Open Source Software Awards 2016.
 - Article by TechRepublic, considering Lynis a "must-have" tool: <u>How to quickly audit a Linux system from</u> the command line
 - o ToolsWatch Best Tools (top 10)
- 2015
 - o ToolsWatch Best Tools (second place)
 - o Best of Open Source Software Awards 2015 (mirror).
- 2014
 - o ToolsWatch Best Tools (third place)
- 2013
 - o ToolsWatch Best Tools (sixth place)

Contribute

We love contributors.

Do you have something to share? Want to help out with translating Lynis into your own language? Create an issue or pull request on GitHub, or send us an e-mail: lynis-dev@cisofy.com.

More details can be found in the Contributors Guide.

You can also simply contribute to the project by *starring* the project and show your appreciation that way.

Thanks!

License

GPLv3

Enterprise version for companies

This software component is also part of an enterprise solution and focuses on companies. Same quality, yet with more functionality.

Focus areas include compliance (PCI DSS , HIPAA , ISO27001 , and others). The Enterprise version comes with:

- a web interface;
- · dashboard and reporting;
- hardening snippets;
- improvement plan (based on risk);
- commercial support.

Releases 63



+ 62 releases

Contributors 230





























+ 216 contributors

Languages

• Shell 99.6%

Other 0.4%