

Lynis

Security auditing, hardening,
and compliance testing

Basics

Platforms

Linux, Mac OS X, *BSD, AIX,
HP-UX, Solaris

Devices

Desktops, servers, NAS, appliances

Language

Shell script

License

GPLv3

```
[+] Users, Groups and Authentication
-----
- Search administrator accounts... [ OK ]
- Checking UIDs... [ OK ]
- Checking chgrp tool... [ FOUND ]
- Consistency check /etc/group file... [ OK ]
- Test group files (grpck)... [ OK ]
- Checking login shells... [ WARNING ]
- Checking non unique group ID's... [ OK ]
- Checking non unique group names... [ OK ]
- Checking LDAP authentication support [ NOT ENABLED ]
- Check /etc/sudoers file [ NOT FOUND ]

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

[+] Shells
-----
- Checking console TTYS... [ WARNING ]
- Checking shells from /etc/shells...
  Result: found 6 shells (valid shells: 6).

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

[+] File systems
-----
- [FreeBSD] Querying UFS mount points (fstab)... [ OK ]
- Query swap partitions (fstab)... [ OK ]
- Testing swap partitions... [ OK ]
- Checking for old files in /tmp... [ WARNING ]
- Checking /tmp sticky bit... [ OK ]
```

Download

Website
GitHub

<https://cisofy.com/lynis/>
<https://github.com/CISOfy/lynis>

FAQ

Why should I use it?

Quickly test for security gaps, vulnerabilities, configuration issues, and required hardening efforts.

What makes it special?

Easy is the keyword: Easy to use, easy to understand, and easy to extend.

Why use Lynis instead of <other tool>?

- **Quick:** No installation required; no dependencies
- **Open source:** Freely available; GPLv3; commercial support available
- **Extensive:** Specifically focused on **Linux/UNIX systems**. Includes scanning of whole stack: **operating system + software components + configuration**

How can I help?

- **GitHub:** Report issues, create pull requests
- **Documentation:** Share tips to make it even easier to use
- **Features:** Request new options and/or tools to be supported
- **Promote:** Share the tool with others

What is next?

We have exciting plans, like Docker security scans, malware scanning, and kernel/system integrity monitoring.

Happy Hardening!

Michael Boelen

Author

Twitter: [@mboelen](https://twitter.com/mboelen)

