Under the microscope:

Linux security tools

Lessons learned from 500+ projects

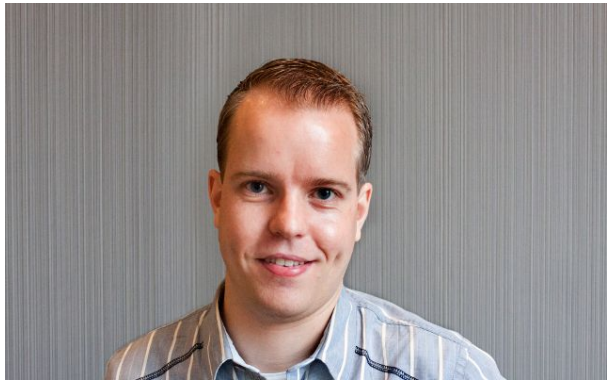
Michael Boelen

michael.boelen@cisofy.com

NLLGG, September 2018

CISOFY
AUDITING-HARDENING-COMPLIANCE

Michael Boelen



- **Open Source**
  - Lynis, Rootkit Hunter
- **Business**
  - Founder of CISOfy
- **Other**
  - Blogger at Linux-Audit.com
  - Board member NLUUG

The LSE project

Project: LSE

LinuxSecurity.Expert

- Library
- People
- Toolkit

Library

- Checklists →
- Guides
- Configuration
  - sysctl
  - systemd
  - SSH

People

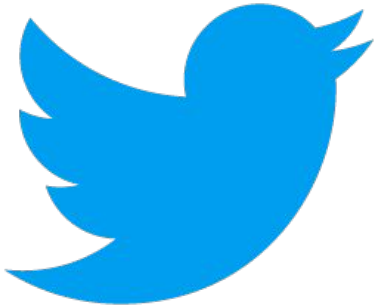
Profiles

- Specialists in our field
  - Person behind a tool
  - Interviews

Toolkit

- Tools
- Categories
- Snippets

Tools - Discovery



Tools - Discovery

Criteria

- Open source
- Security
- Runs on Linux, macOS, BSD

Tool analysis


PANEL NO.1

Tool analysis

Basics

Project description

Tool category

Typical user

License

Author

Language

Keywords

Latest release

Quality

Changelog

Popularity

Documentation

Code

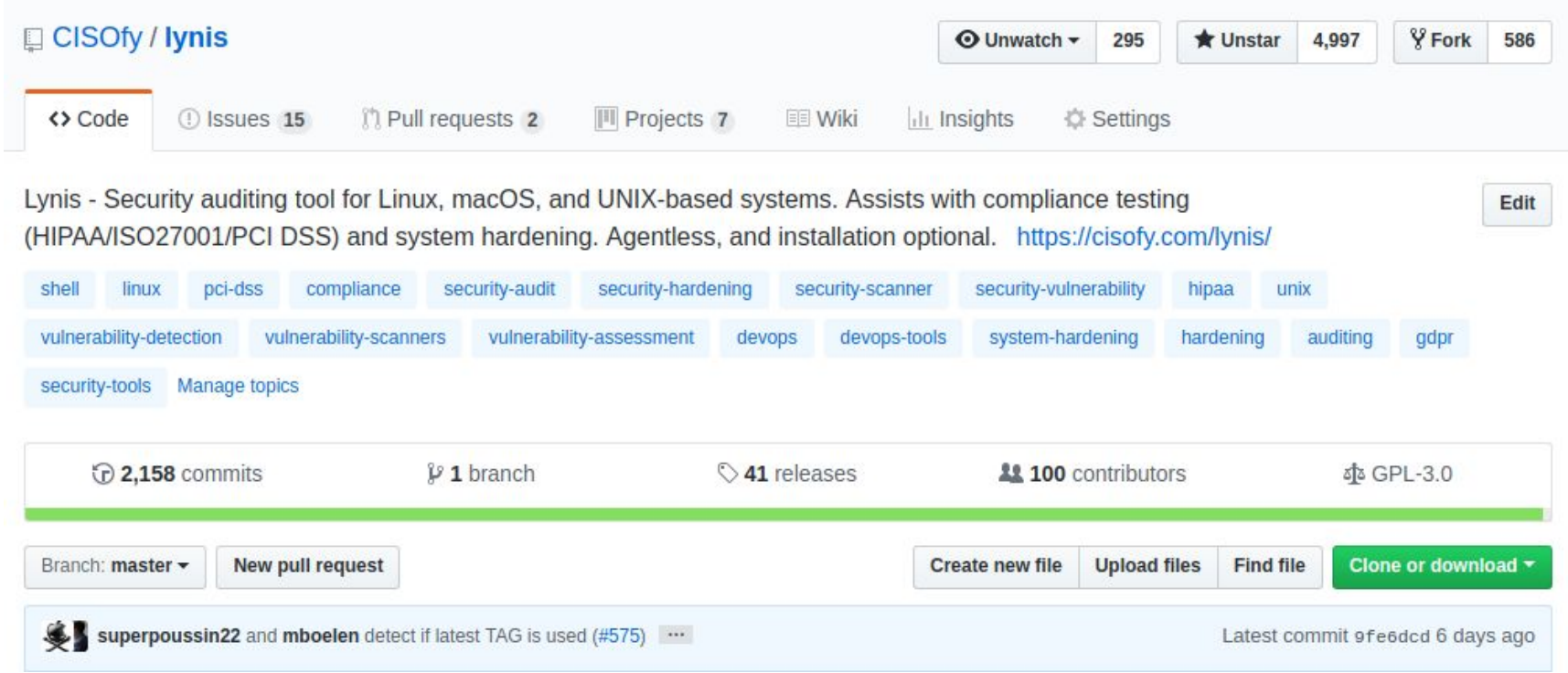
Releases

Usage

Installation

Ease of use

Tool analysis



Output

Tool review

- Introduction
- Typical tool usage
- How it works
- Background details
- Strengths and weaknesses
- Example output
- Author information
- Tool alternatives
- Categories
- Tags
- And more...

Tool review

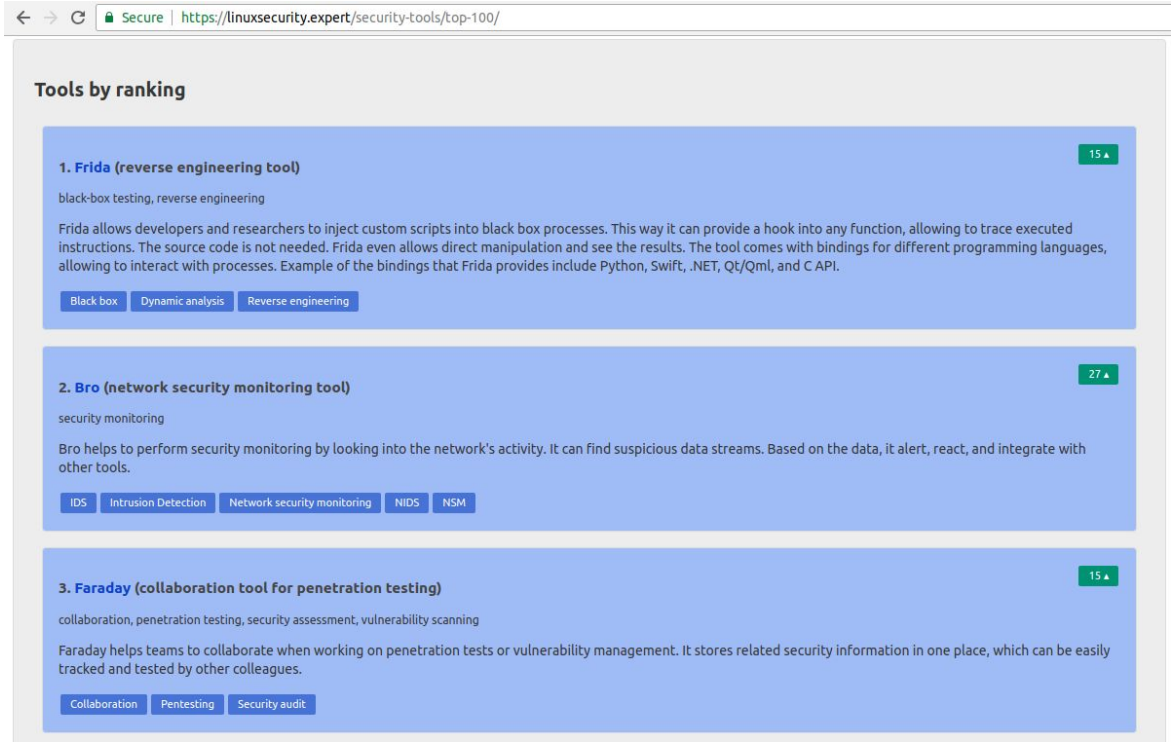
Tool and Usage

Project details	
Inception	2007
License	GPLv3
Programming language	shell script
Author	Michael Boelen
Latest release	2.6.8 [2018-08-23]

Project health

This score is calculated by different factors, like project age, last release date, etc.

Top 100: security tools



Tools by category

Lessons learned

Lessons learned - Basics

- Not really open source!
- Unclear goal
- Authorship
- Versioning
- Changelog missing

Lessons learned - Documentation

- Missing a basic description
- No ‘get started’ guide
- Lack of good examples

Lessons learned - Ease of use

- Complicated installation
- No sane defaults (e.g. --help missing)
- Parameters make no sense

What questions do you have?

Get connected

- Twitter (@mboelen and @LSELabs)
- LinkedIn (Michael Boelen)

More?

Related articles at **linux-audit.com**

- Why we use your open source project (or not)
- How to Promote your Open Source Project

Best Practices

--full-throttle-engine, -f

--help, -h, or help

--version, -V

Learn more: docopt.org

```
$ ./lynis show help
Lynis 2.4.1 - Help
==========================

Commands:
audit
show
update
upload-only

Use 'lynis show help <command>' to see details


Options:
--auditor
--check-all (-c)
--config
--cronjob (--cron)
--debug
--developer
--help (-h)
--license-key
--log-file
--manpage (--man)
--no-colors --no-log
--pentest
--profile
--plugins-dir
--quiet (-q)
--quick (-Q)
```

Best Practices

Keep a changelog

- History
- Trust
- Troubleshooting

Learn more: keepachangelog.com

Best Practices

Semantic versioning!

Major.Minor.Patch

Learn more: semver.org

Credits

Images

Where possible the origin of the used images are included in the slides. Some came without an origin from social media and therefore have no source. If you are the owner, let us know and we add the source.