

Linux Security

State of Linux Security in 2016

Michael Boelen

michael.boelen@cisofy.com

DBLUG, 7 December 2016

Michael Boelen

- **Open Source**

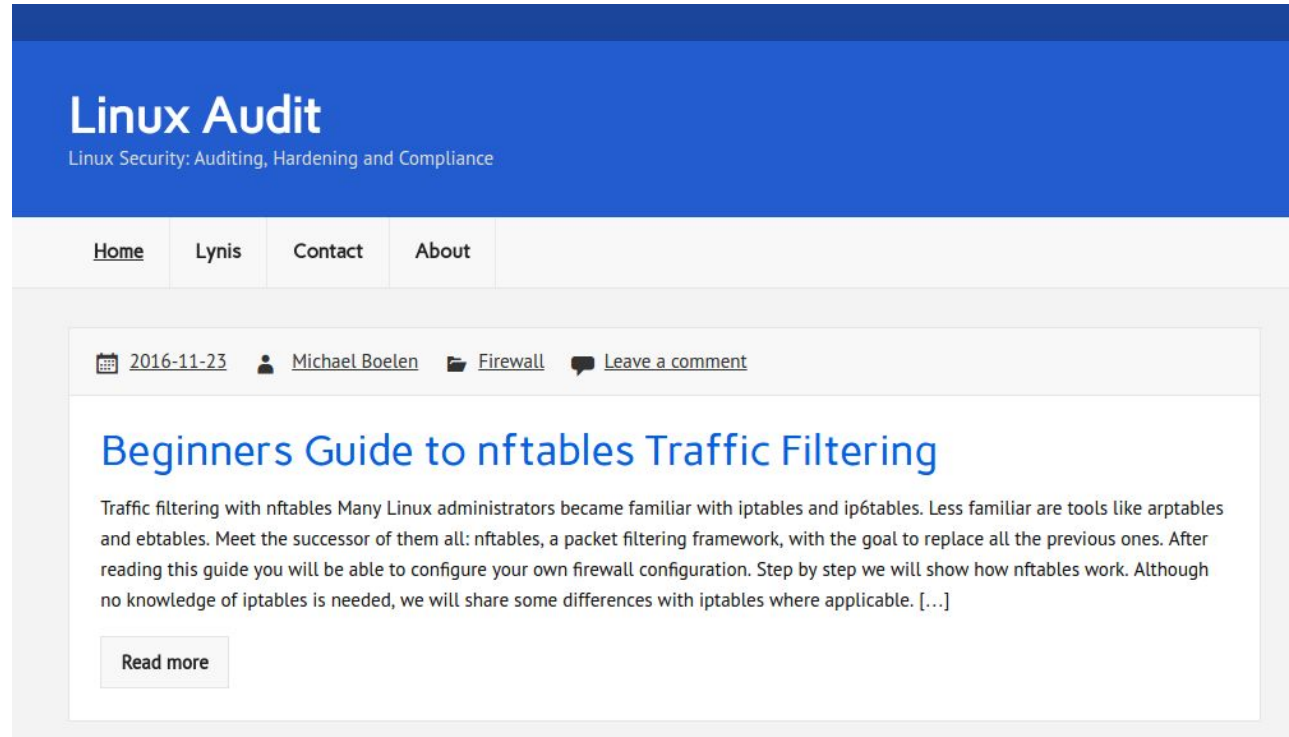
- Lynis, Rootkit Hunter



- **Business and Community**

- Founder of [CISOfy](https://www.cisofy.nl)
- Board member and program committee NLUUG

Blog: Linux-Audit.com



Agenda

Topics

- Highlights
- Future
- Discussion



Highlights

The Past: Services

- Telnet
- “r” services
- Finger



The Past: Tooling



2016

Kernel security

- Vulnerabilities
- Linus himself
- Grsecurity



2016

- Drown attack
- Dirty COW
- Cryptsetup initrd (root shell)



Compromise

- Linux.PNScan (routers)
- Linux.Rex.1 (p2p botnet)



What about good things?

Conferences



Core Infrastructure Initiative

- Badge program
- Census project
- Education
- Tooling



CII Example

- Questions
- Proof
- Score



BADGE STATUS FOR LYNIS

[Show all detailed text](#) [Hide all detailed text](#) [Hide met or N/A criteria](#)

Projects that follow the best practices below will be able to voluntarily self-certify and show that they've achieved a Core Infrastructure Initiative (CII) badge. [Show details](#)

If this is your project, please show your badge status on your project page! The badge status looks like this: **cii best practices** **passing 100%** Here is how to embed it: [Show details](#)

100%

Basics

Change Control

Reporting

Quality

Security

Analysis

Future

Identification

What is the human-readable name of the project? [Show details](#)

Lynis

What is a brief description of the project?

Lynis - Security auditing tool and assists with compliance testing (HIPAA/ISO27001/PCI DSS) and system hardening. Works on Linux, Mac OS, and Unix based systems, with installation being optional.

What is the URL for the project (as a whole)?

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

What is the URL for the version control repository (it may be the same as the project URL)?

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

What is the **Common Platform Enumeration (CPE)** name for the project (if it has one)? [Show details](#)

(Optional) CPE name

The Future

Some Thoughts for 2017

- Docker
- Nftables
- Frameworks
- Kernel patching
- Auditing



Questions?

Connect

- Twitter ([@mboelen](#))
- LinkedIn ([Michael Boelen](#))

