Linux Security

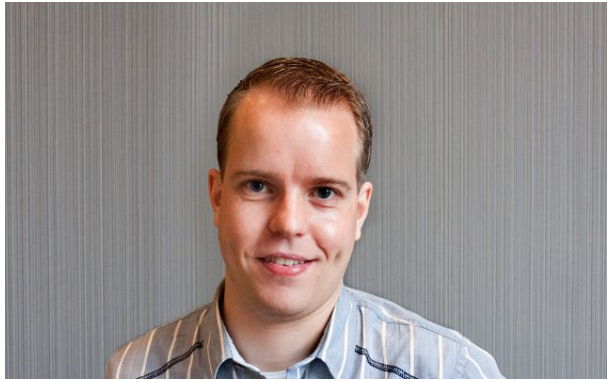
State of Linux Security in 2016

Michael Boelen
michael.boelen@cisofy.com

DBLUG, 7 December 2016

CISOFY
AUDITING-HARDENING-COMPLIANCE

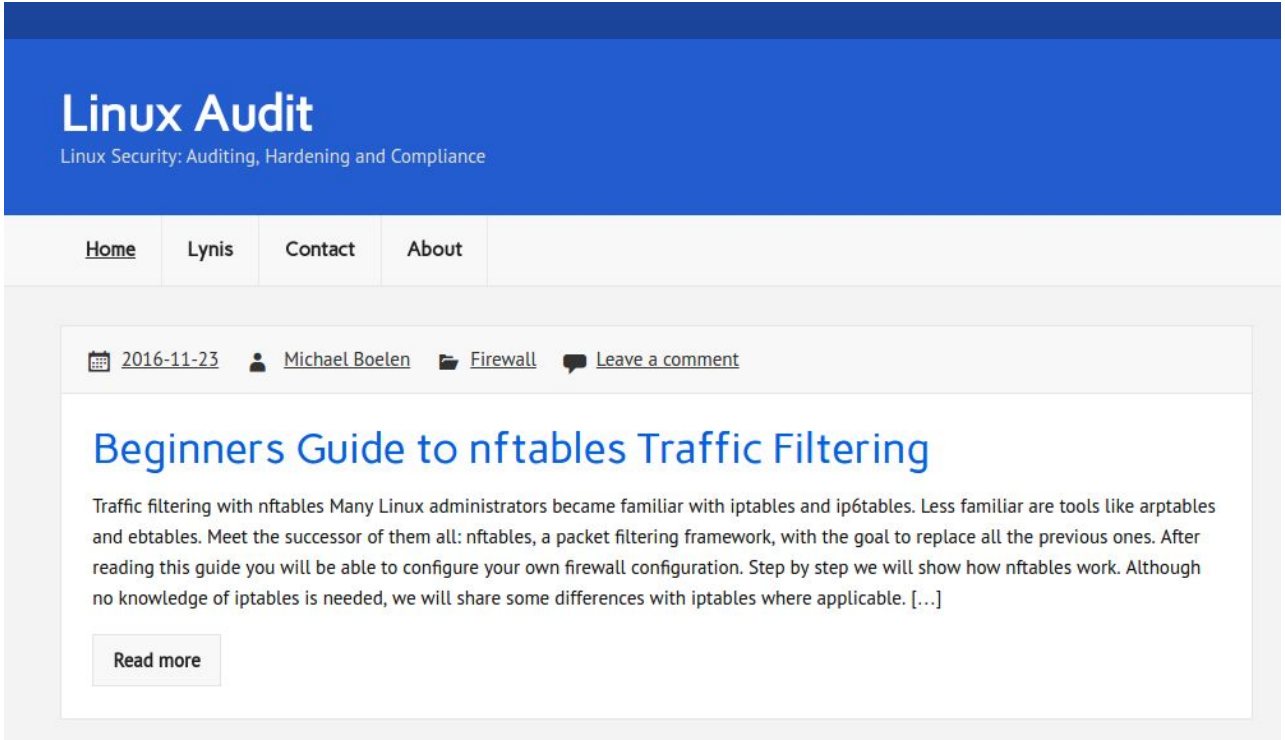
Michael Boelen



- **Open Source**
  - Lynis, Rootkit Hunter

- **Business and Community**
  - Founder of CISOfy
  - 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?

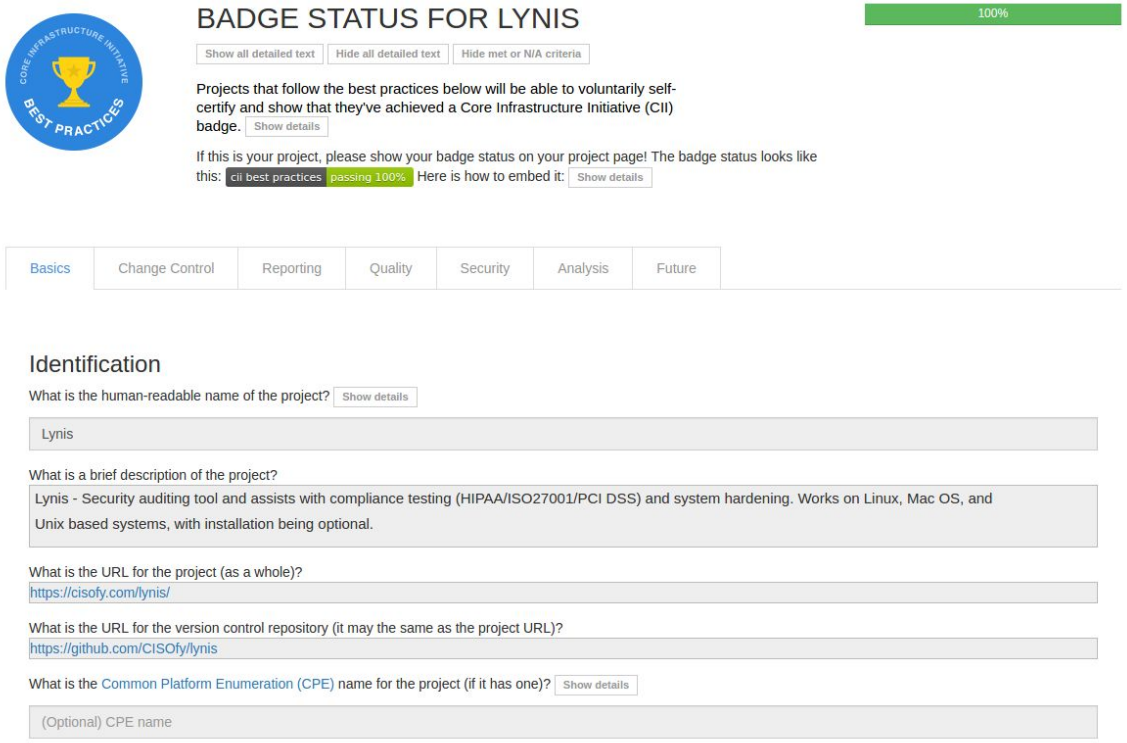
Conferences

Core Infrastructure Initiative

- Badge program
- Census project
- Education
- Tooling

CII Example

- Questions
- Proof
- Score



The Future

Some Thoughts for 2017

- Docker
- Nftables
- Frameworks
- Kernel patching
- Auditing

Questions?

Connect

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