Linux Security

State of Linux Security in 2016
Michael Boelen

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

- **Business and Community**
  - Founder of [CISOfy](#)
  - Board member and program committee NLUUG
Beginners Guide to nftables Traffic Filtering

Traffic filtering with nftables Many Linux administrators became familiar with iptables and ip6tables. Less familiar are tools like arptables and ebtables. Meet the successor of them all: nftables, a packet filtering framework, with the goal to replace all the previous ones. After reading this guide you will be able to configure your own firewall configuration. Step by step we will show how nftables work. Although no knowledge of iptables is needed, we will share some differences with iptables where applicable. [...]

Read more
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)