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 <u>CISOfy</u>
 - Board member and program committee NLUUG



Blog: Linux-Audit.com

Linux Audit

Linux Security: Auditing, Hardening and Compliance

<u>Home</u>	Lynis	Contact	About	
<u>iii</u> <u>2016</u>	<u>-11-23</u>	Michael Boe	elen 🏲 Firewa	ll 🗭 Leave a comment

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?









Core Infrastructure Initiative

- Badge program
- Census project
- Education
- Tooling



Core Infrastructure Initiative Fortifying our future.



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 selfcertify 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

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 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



100%

The Future

Some Thoughts for 2017

- Docker
- Nftables
- Frameworks
- Kernel patching
- Auditing





Questions?

Connect

- Twitter (<u>@mboelen</u>)
- LinkedIn (Michael Boelen)

