Linux Security

Concept → Tooling
Goals

1. Learn **what** to protect
2. Know some **strategies**
3. Learn about **tooling**

**Focus**: Linux
Agenda

Today
1. Hardening
2. Auditing
3. Guides and Tools

Bonus: Lynis demo
Michael Boelen

- Open Source Security
  - Rootkit Hunter (malware scan)
  - Lynis (security audit)
- 150+ blog posts at Linux-Audit.com
- Founder of CISOfy
Hardening
Q: What is Hardening?
Q: Why Hardening?
Stranger hacks family's baby monitor and talks to child at night

By CHANTE OWENS  January 7, 2016
Hardening

- New defenses
- Existing defenses
- Reduce weaknesses (attack surface)

Photo Credits: http://commons.wikimedia.org/wiki/User:Wilson44691
Myth

After hardening I’m done

Server Shield v1.1.5

Server Shield is a lightweight method of protecting and hardening your Linux server. It is easy to install, hard to mess up, and makes your server instantly and effortlessly resistant to many basic and advanced attacks.

All IP addresses will be automatically detected and used for the firewall configuration. Automatic security updates are enabled by default.

No maintenance required—just set it and forget it!
Fact

● Security should be an ongoing process
● Which means it is never finished
● New attacks = more hardening
  ○ POODLE
  ○ Hearthbleed
Hardening

What to harden?

- Operating System
- Software + Configuration
- Access controls
Hardening

Operating System

● Services

● Users

● Permissions
Hardening

Software

● Minimal installation

● Configuration

● Tuning
Hardening

Users and Access Controls

- Who can access what
- Password policies
- Accountability
Hardening

Encryption

● **Good**: Encryption solves a lot

● **Bad**: Knowledge required

● **Ugly**: Easy to forget
Technical Auditing
Auditing

Why audit?

- Checking defenses
- Assurance
- Quality Control
Common Strategy

1. Audit
2. Get a lot of findings
3. Start hardening
4. .......
5. Quit
Improved Strategy

1. Focus
2. Audit
3. Focus
4. Harden
5. Repeat!
Guides and Tools
Options

- Benchmarks and Guides
- SCAP
- Other resources
- Tools
Benchmarks / Guides

- Center for Internet Security (CIS)
- NIST / NSA
- OWASP
- Vendors
Benchmarks / Guides

**Pros**
- Free to use
- Detailed
- You are in control

**Cons**
- Time intensive
- Usually no tooling
- Limited distributions
- Delayed releases
Tooling
Tools

Tools make life easier, right?

Not always...
Tools

Problem 1: There aren’t many
Tools

Problem 2: Usually outdated

eglimi/linux_hardening

A report describing how to harden a Linux System. This work has been done as a semester project at university. It is no longer maintained and kept for reference only.

Updated on 27 Dec 2009
Tools

Problem 3: Limited in their support

AdaLovelance/hardeningserverfromscratch

Este repositorio es un conjunto de scripts para proveer seguridad en un servidor GNU/Linux

Updated 22 days ago
Tools

Problem 4: Hard to use

The system boot loader configuration file(s) must be group-owned by root.

The file "/etc/grub.conf" should be group-owned by the "root" group to prevent destruction or modification of the file. To properly set the group owner of "/etc/grub.conf", run the command: $ chgrp -R root /etc/grub.conf

To check the group ownership of "/etc/grub.conf", run the command: $ ls -l /etc/grub.conf If properly configured, the output should indicate the following group ownership. "root" If it does not, this is a finding.
Tool 1: SCAP
SCAP

- **Security**
- **Content**
- **Automation**
- **Protocol**
SCAP

Combination of:

- Markup
- Rules
- Tooling
- Scripts
SCAP features

- Common Vulnerabilities and Exposures (CVE)
- Common Configuration Enumeration (CCE)
- Common Platform Enumeration (CPE)
- Common Vulnerability Scoring System (CVSS)
- Extensible Configuration Checklist Description Format (XCCDF)
- Open Vulnerability and Assessment Language (OVAL)

Starting with SCAP version 1.1
- Open Checklist Interactive Language (OCIL) Version 2.0

Starting with SCAP version 1.2
- Asset Identification
- Asset Reporting Format (ARF)
- Common Configuration Scoring System (CCSS)
- Trust Model for Security Automation Data (TMSAD)
List of Tables (Common Configuration Scoring System (CCSS))
Table 1. Access Vector Scoring Evaluation ................................................................. 8
Table 2. Authentication Scoring Evaluation ............................................................... 9
Table 3. Access Complexity Scoring Evaluation ....................................................... 10
Table 4. Confidentiality Impact Scoring Evaluation ................................................. 11
Table 5. Integrity Impact Scoring Evaluation ............................................................ 12
Table 6. Availability Impact Scoring Evaluation ....................................................... 12
Table 7. General Exploit Level Scoring Evaluation ............................................... 13
Table 8. General Remediation Level Scoring Evaluation ....................................... 14
Table 9. Local Vulnerability Prevalence Scoring Evaluation ............................... 15
Table 10. Perceived Target Value Scoring Evaluation ........................................... 15
Table 11. Local Remediation Level Scoring Evaluation ........................................ 16
Table 12. Collateral Damage Potential Scoring Evaluation .................................... 17
SCAP Overview

**Pros**
- Free to use
- Focused on automation

**Cons**
- Limited distributions
- Complexity
- Hard to customize
Tool 2: Lynis
Lynis

[+] Users, Groups and Authentication
--------------------------------------------------
- Search administrator accounts... [ OK ]
- CheckingUIDs... [ OK ]
- Checking chgrp tool... [ FOUND ]
- Consistency check /etc/group file... [ OK ]
- Test group files (grep/k)... [ OK ]
- Checking login shells... [ WARNING ]
- Checking non unique group ID's... [ OK ]
- Checking non unique group names... [ OK ]
- Checking LLP authentication support
- Check /etc/ Buckley file [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] Shells
-------------------
- Checking console TTY's... [ WARNING ]
- Checking shells from /etc/shells...
  Result: Found 6 shells (valid shells: 6).

[ Press [ENTER] to continue, or [CTRL]+C to stop ]

[+] File systems
-----------------
- [FreeBSS] Querying BFS mount points /stab)... [ OK ]
- Query swap partitions /stab)... [ OK ]
- Testing swap partitions... [ OK ]
- Checking for old files in /tmp... [ WARNING ]
- Checking /tmp sticky bit... [ OK ]
Lynis

Goals

● Perform a quick security scan
● Collect data
● Define next hardening steps
Lynis

Background

● Since 2007

● Goals
  ○ Flexible
  ○ Portable
Lynis

Open Source Software

● GPLv3
● Shell
● Community
Lynis

Simple

● No installation needed
● Run with just one parameter
● No configuration needed
Lynis

Flexibility

● No dependencies*
● Option to extend easily
● Custom tests

* Besides common tools like awk, grep, ps
Lynis

Portability

- Run on all Unix platforms
- Detect and use “on the go”
- Usable after OS version upgrade
How it works

1. Initialise
2. OS detection
3. Detect binaries
4. Run helpers/plugins/tests
5. Show report
Running

1. lynis
2. lynis audit system
3. lynis audit system --quick
4. lynis audit system --quick --quiet
Demo?
Conclusions

● Protect your precious
● Hardening
● Do regular checks
Success!

You finished this presentation
Learn more?

Follow

- Blog Linux Audit (linux-audit.com)
- Twitter @mboelen