Linux Hardening

Locking Down Linux To Increase Security

Michael Boelen
michael.boelen@cisofy.com

‘s-Hertogenbosch, 1 March 2016
Meetup: Den Bosch Linux User Group
Goals

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

**Focus:** Linux
Agenda

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

Bonus: Lynis demo
Michael Boelen

- Open Source Security
  - *rkhunter* (malware scan)
  - *Lynis* (security audit)
- 150+ blog posts at Linux-Audit.com
- Founder of [CISOfy](https://www.cisofy.com)
System Hardening
Q: What is Hardening?
Q: Why Hardening?
Q: What if we don’t?
ALL YOUR PERSONAL FILES HAS BEEN ENCRYPTED

All your data (photos, documents, databases, etc) have been encrypted with a private and unique key generated for this computer. This means that you will not be able to access your files anymore until they are decrypted. The private key is stored in our servers and the only way to receive your key to decrypt your files is making a payment.

The payment has to be done in Bitcoins to a unique address that we generated for you. Bitcoins are a virtual currency to make online payments. If you don’t know how to get Bitcoins, you can click the button “How to buy Bitcoins” below and follow the instructions.

You only have 4 days to submit the payment. When the provided time ends, the payment will increase to 1 Bitcoins ($350 aprox.). Also, if you don’t pay in 7 days, your unique key will be destroyed and you won’t be able to recover your files anymore.

Payment raise
3 days, 23:59:43

Final destruction
6 days, 23:59:43

To recover your files and unlock your computer, you must send 0.1 Bitcoins ($35 aprox.) to the next Bitcoin address:

1BaLBdomt2DhibCXsmLXaxKCy467QB4DzF

Check payment How to buy Bitcoins

If you try to remove this payment platform, your will never be able to decrypt your files and they will be lost forever.
Stranger hacks family's baby monitor and talks to child at night

By CHANTE OWENS  January 7, 2016

source: http://sfglobe.com/
Tin cans within the structural columns in the Weiguan Jinlong apartment complex in Taiwan (via China Foto Press)
TOUR OF ACCOUNTING

OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.

NINE NINE NINE NINE

ARE YOU SURE THAT’S RANDOM?

THAT’S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.
Hardening Basics
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 is an **ongoing process**
- It is **never finished**
- New attacks = **more hardening**
  - POODLE
  - Hearthbleed
Hardening

What to harden?

● Operating System
● Software + Configuration
● Access controls
Hardening

Operating System

● Packages
● Services
● Configuration
Hardening

Software

● Minimal installation
● Configuration
● Permissions
Hardening

Access Controls

- Who can access what
- Password policies
- Accountability
Hardening

Encryption

● **Good:** Encryption solves a lot
● **Bad:** Knowledge required
● **Ugly:** Easy to forget, or do it incorrectly
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!
Hardening Resources
Options

● Guides
● Tools (SCAP / Lynis)
● Other resources
Hardening Guides

● Center for Internet Security (CIS)
● NIST / NSA
● OWASP
● Vendors
Hardening Guides

Pros
Free to use
Detailed
You are in control

Cons
Time intensive
Usually no tooling
Limited distributions
Delayed releases
Missing follow-up
Tooling
Tools

Tools make life easier, right?

Not always...
Tools

Problem:

There aren’t many good tools
Tools

Cause 1: Usually outdated

eglmi/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

Cause 2: 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

Cause 3: Hard to use
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)
Complexity?

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 ]
- Checking UIDs...  [ OK ]
- Checking chgrp tool...  [ FOUND ]
- Consistency check /etc/group file...  [ OK ]
- Test group files (grent)...  [ OK ]
- Checking login shells...  [ WARNING ]
- Checking non unique group ID's...  [ OK ]
- Checking non unique group names...  [ OK ]
- Checking LIAP authentication support  [ NOT ENABLED ]
- Check /etc/sockets file  [ NOT FOUND ]

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

[+] Shells

- Checking console TTYs...  [ WARNING ]
- Checking shells from /etc/shells...
  Result: Found 6 shells (valid shells: 6).

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

[+] File systems

  [FreeBSD] Querying UFS mount points /fsstab)...  [ OK ]
  - Query swap partitions /fsstab)...  [ OK ]
  - Testing swap partitions...  [ OK ]
  - Checking for old files in /tmp...  [ WARNING ]
  - Checking /tmp sticky bit...  [ OK ]
Lynis

Goals

● In-depth security scan
● Quick and easy to use
● 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*
● Can be easily extended
● 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

1. Know your crown jewels (properly)
2. Determine hardening level
3. Perform regular checks
Success!

You finished this presentation
Learn more?

Follow

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

This presentation can be found on michaelboelen.com