Linux Security

Concept → Tooling

Michael Boelen
michael.boelen@cisofy.com

Utrecht, 16 January 2016

CISOFY
AUDITING-HARDENING-COMPLIANCE

Goals

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

Focus: Linux

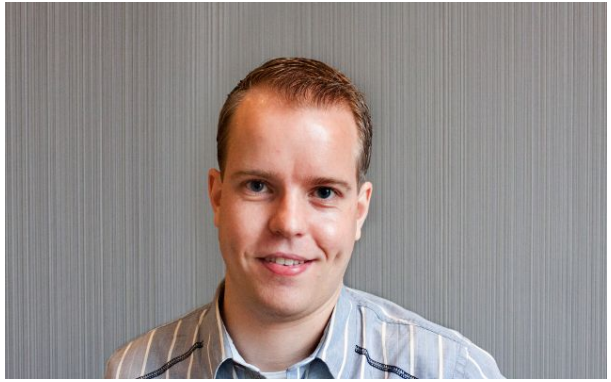
Agenda

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?


Dunland
Isengard
North-South Road
WESTFOLD Emnet
Emnet

Stranger hacks family's baby monitor and talks to child at night

By CHANTE OWENS January 7, 2016

source: http://sfglobe.com/

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

★8 ⑂0

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

Updated on 27 Dec 2009

Tools

Problem 3: Limited in their support

AdaLovelance/ **hardeningserverfromscratch**

Shell ★1 0

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


```
− <Group id="V-38581">
    <title>SRG-OS-999999</title>
    <description><GroupDescription></GroupDescription></description>
  − <Rule id="SV-50382r1_rule" severity="medium" weight="10.0">
      <version>RHEL-06-000066</version>
    − <title>
        The system boot loader configuration file(s) must be group-owned by root.
      </title>
    − <description>
        <VulnDiscussion>The "root" group is a highly-privileged group. Furthermore, the group-owner of this file should not have any access privileges anyway.</VulnDiscussion><FalsePositives></FalsePositives><FalseNegatives></FalseNegatives>
        <Documentable>false</Documentable><Mitigations></Mitigations><SeverityOverrideGuidance></SeverityOverrideGuidance><PotentialImpacts></PotentialImpacts><ThirdPartyTools></ThirdPartyTools><MitigationControl></MitigationControl><Responsibility>
        </Responsibility><IAControls></IAControls>
      </description>
    − <reference>
        <dc:title>DPMS Target Red Hat 6</dc:title>
        <dc:publisher>DISA FSO</dc:publisher>
        <dc:type>DPMS Target</dc:type>
        <dc:subject>Red Hat 6</dc:subject>
        <dc:identifier>2367</dc:identifier>
      </reference>
      <ident system="http://iase.disa.mil/cci">CCI-000366</ident>
    − <fixtext fixref="F-43529r1_fix">
        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 root /etc/grub.conf
      </fixtext>
      <fix id="F-43529r1_fix"/>
    − <check system="C-46139r1_chk">
        <check-content-ref href="DPMS_XCCDF_Benchmark_RHEL_6_STIG.xml" name="M"/>
      − <check-content>
          To check the group ownership of "/etc/grub.conf", run the command: $ ls -lL /etc/grub.conf If properly configured, the output should indicate the following group-owner. "root" If it does not, this is a finding.
        </check-content>
      </check>
    </Rule>
  </Group>
```

Tool 1: SCAP

SCAP

- **S**ecurity
- **C**ontent
- **A**utomation
- **P**rotocol

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))

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 chkgrp tool...                                   [ FOUND ]
  - Consistency check /etc/group file...                      [ OK ]
  - Test group files (grpck)...                               [ OK ]
  - Checking login shells...                                  [ WARNING ]
  - Checking non unique group ID's...                         [ OK ]
  - Checking non unique group names...                        [ OK ]
  - Checking LDAP authentication support                      [ NOT ENABLED ]
  - Check /etc/sudoers 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 (fstab)...            [ OK ]
  - Query swap partitions (fstab)...                          [ 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