

# Linux Security Scanning

Learn your weaknesses with Lynis

**Michael Boelen**

michael.boelen@cisofy.com

**Nijmegen, 2016-05-10**

Meetup: [Linux Usergroup Nijmegen](#)

# Goals

1. Perform a **security audit**
2. Learn **what** to protect
3. Determine **why**



# Agenda

## Today

1. System Hardening
2. Security Auditing
3. Lynis



# Michael Boelen

- Open Source Security
  - **rkhunter** (malware scan)
  - **Lynis** (security audit)
- 170+ blog posts at **Linux-Audit.com**
- Founder of [CISOfy](https://www.cisofy.com)



# System Hardening





Scheveningen Zeeruststraat

03-01-2016 12:26:58

**SANITRONICS**  
INTERNATIONAL B.V.



NOT STARTED

MACHINE OK

Cleaning

Units

Toilet

1 2



Door



Log on 0



### 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, you will never be able to decrypt your files and they will be lost forever



Tin cans within the structural columns in the Weiguan Jinlong apartment complex in Taiwan (via China Foto Press)

# Hardening Basics

# Hardening 101

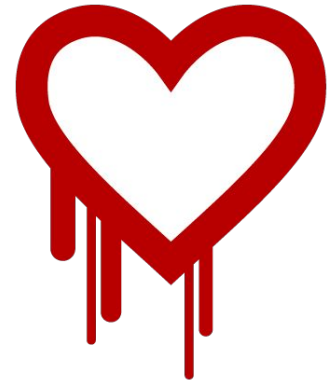
- New defenses
- Existing defenses
- Reduce weaknesses  
(= attack surface)



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

# Hardening 101

- Security is an **ongoing process**
- It is **never finished**
- New attacks = **more hardening**
  - [POODLE](#)
  - [Hearthbleed](#)



# Hardening 101

## Operating System

- Packages
- Processes
- Configuration

# Linux Security

Areas	Core	Resources	Services	Environment
System Hardening	Boot Process Containers Frameworks Kernel Service Manager Virtualization	Accounting Authentication Cgroups Cryptography Logging Namespaces Network Software Storage Time	Database Mail Middleware Monitoring Printing Shell Web	Forensics Incident Response Malware Risks Security Monitoring System Integrity
Security Auditing				
Compliance				

# Technical Auditing

# Auditing

## Why audit?

- Checking defenses
- Assurance
- Quality Control



# Auditing

## Who?

- Auditors
- Security Professionals
- System Engineers

# Auditing

## How?

1. Focus
2. Audit
3. Focus
4. Harden
- 5. Repeat!**

# Resources

## Guides

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

# Guides

## Pros

Free to use

Detailed

You are in control

## Cons

Time intensive

Usually no tooling

Limited distributions

Delayed releases

No follow-up

# **Audit Tool: 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

## 2007

# Lynis

## GPL v3

# Lynis

## Shell script

# Lynis

## Goal 1

In-depth security scan

# Lynis

## Goal 2

Quick and easy to use

# Lynis

## Goal 3

Define the next (hardening) step

## **Differences with other tools**

# Lynis

## Simple

- No installation needed
- Run with simple commands
- 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

# Running Lynis

# How it works

- Initialise → OS detection → Read profiles  
→ Detect binaries
- Run helpers / plugins / tests
- Show audit results

# Running Lynis

1. `lynis`
2. `lynis audit system`
3. `lynis audit system --quick`
4. `lynis audit system --quick --quiet`

# Lynis Profiles

## Optional configuration

- Default profile (default.prf)
- Custom profile (custom.prf)
- Other profiles with --profile

# Lynis Profiles

## Example: developer

```
# This profile is useful when creating your own tests, or debugging tests
# lynis audit system --profile developer.prf

debug=yes
developer-mode=yes
quick=yes
```

# Plugins

## An extension to Lynis

Plugins are mostly for gathering facts

***Customization: include/tests\_custom or custom plugin***

**Demo?**

# Lessons Learned

# Lessons Learned

## Simplicity

- Keep it simple
- First impression
- Next step

**Usage:** lynis `command` [options]

**Command:**

`audit`

<code>audit system</code>	: Perform security scan
<code>audit dockerfile &lt;file&gt;</code>	: Analyze Dockerfile

`show`

<code>show</code>	: Show all options
<code>show version</code>	: Show Lynis version
<code>show help</code>	: Show help

`update`

<code>update info</code>	: Show update details
<code>update release</code>	: Update Lynis release

More options available. Run '`./lynis show options`', or use the man page.

# Lessons Learned

## Less is better

- Dependencies
- Program arguments
- Screen output

# Lessons Learned

## Documentation

- Understand its power
- Focus on new users
- Separate properly

### Documentation

#### » Lynis

- [Get Started with Lynis](#)
- [Lynis - Configuration](#)
- [Lynis - Features](#)
- [Lynis - Usage guide](#)
- [Upgrading Lynis](#)

#### » Lynis Enterprise

- [Lynis Collector](#)
- [Lynis Enterprise - Modules](#)
- [Lynis Enterprise - Software Architecture](#)
- [Lynis Enterprise - On-premise Guide](#)

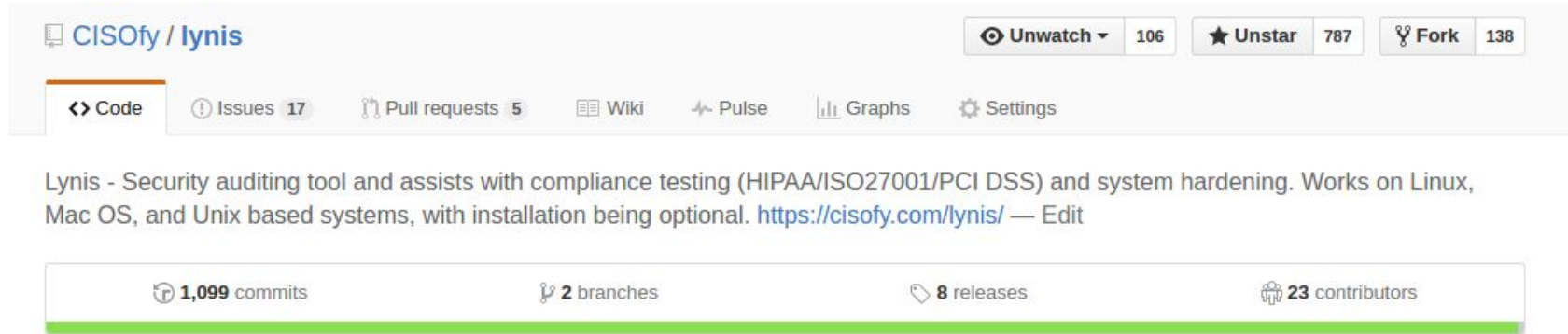
#### » Lynis Development

- [Lynis Plugins - Development Guide](#)

# Lessons Learned

## GitHub

**Stats:** issues / pulls / stars / watchers



The screenshot shows the GitHub repository page for CISOFy / lynis. The repository name is displayed at the top left. On the top right, there are buttons for 'Unwatch' (106), 'Unstar' (787), and 'Fork' (138). Below these, a navigation bar includes links for 'Code', 'Issues' (17), 'Pull requests' (5), 'Wiki', 'Pulse', 'Graphs', and 'Settings'. The repository description states: '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. <https://cisofy.com/lynis/> — Edit'. At the bottom, a statistics bar shows '1,099 commits', '2 branches', '8 releases', and '23 contributors'.

CISOFy / lynis

Unwatch 106 Unstar 787 Fork 138

Code Issues 17 Pull requests 5 Wiki Pulse Graphs Settings

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. <https://cisofy.com/lynis/> — Edit

1,099 commits 2 branches 8 releases 23 contributors

# Lessons Learned

## Open Source = Business

It needs PR, blog posts, attention  
(like a business)

**Future**

# Future

- Packages
- More tests
- Quality control
- Linting
- Unit tests
- Software Development Kit

# Future

## Want to help?

- Submit patches
- Provide feedback
- Deploy Lynis

**Success!**

**You finished this presentation**

# Learn more?

## Follow

- Blog      [Linux Audit](https://linux-audit.com) (linux-audit.com)
- Twitter    [@mboelen](https://twitter.com/mboelen)

This presentation can be found on [michaelboelen.com](https://michaelboelen.com)

