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
System Hardening
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:

1BaLBdomt2DhibCKsmLXaxKCy467QB4DzF

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.
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

<table>
<thead>
<tr>
<th>Areas</th>
<th>Core</th>
<th>Resources</th>
<th>Services</th>
<th>Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Hardening</strong></td>
<td>Boot Process</td>
<td>Accounting</td>
<td>Database</td>
<td>Forensics</td>
</tr>
<tr>
<td></td>
<td>Containers</td>
<td>Authentication</td>
<td>Mail</td>
<td>Incident Response</td>
</tr>
<tr>
<td></td>
<td>Frameworks</td>
<td>Cgroups</td>
<td>Middleware</td>
<td>Malware</td>
</tr>
<tr>
<td></td>
<td>Kernel</td>
<td>Cryptography</td>
<td>Monitoring</td>
<td>Risks</td>
</tr>
<tr>
<td></td>
<td>Service Manager</td>
<td>Logging</td>
<td>Printing</td>
<td>Security Monitoring</td>
</tr>
<tr>
<td></td>
<td>Virtualization</td>
<td>Namespaces</td>
<td>Shell</td>
<td>System Integrity</td>
</tr>
<tr>
<td><strong>Security Auditing</strong></td>
<td>Accounting</td>
<td>Network</td>
<td>Web</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td>Software</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cgroups</td>
<td>Storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cryptography</td>
<td>Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td>Accounting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cgroups</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cryptography</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Logging</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Namespaces</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Storage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 chgrp tool... [ FOUND ]
- Consistency check /etc/group file... [ OK ]
- Test group files (group)... [ OK ]
- Checking login shells... [ WARNING ]
- Checking non unique group ID's... [ OK ]
- Checking non unique group names... [ OK ]
- Checking SSLP authentication support [ NOT ENABLED ]
- Check /etc/swcour 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 /mnt... [ OK ]
- Query swap partitions /swap... [ 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

```bash
# 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
  audit system
  audit dockerfile <file>
  : Perform security scan
  : Analyze Dockerfile

show
  show
  show version
  show help
  : Show all options
  : Show Lynis version
  : Show help

update
  update info
  update release
  : Show update details
  : 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

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/](https://cisofy.com/lynis/) — Edit
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 (linux-audit.com)
- Twitter @mboelen

This presentation can be found on michaelboelen.com