Linux Security
+ de APK voor systemen

Michael Boelen
michael.boelen@cisoty.com

www.denhack.nl
Agenda

Linux security

1. System hardening
2. Technical audits
3. Automation
# 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>System Hardening</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>Security Auditing</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>Compliance</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>

---

*Note: The table above outlines various areas of Linux security, including system hardening, security auditing, and compliance. Each area is further broken down into core components and resources, with related services and environmental considerations. This framework is designed to provide a comprehensive overview of the critical aspects of Linux security.*
System Hardening
Security 101

● Ongoing process
● Prevention || Detection
● React and mitigate:
  ○ Hearthbleed
  ○ Spectre and Meltdown
All your personal files have been encrypted. 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 approx.). 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 approx.) to the next Bitcoin address:

1BaLBdomt2DhibC2xsmLxaxKCy467QB4DzF

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.
Hardening 101

Defenses

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

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

Resources

● Center for Internet Security (CIS)
● NSA → NIST
● OWASP
● Vendors
● *The Internet*
Auditing
Auditing

Why?

- Quality
- Assurance
Audit (or some pentests)

Typically:

10 Run vulnerability scanner
20 Apply fix
30 goto 10
Audit

Better:
10 Select target(s)
20 Perform audit
30 Risk analysis
40 Define automation steps
50 Implement hardening
60 goto 10
Automation
### Networking

- Checking IPv6 configuration
  - Configuration method: [ENABLED]
  - IPv6 only: [AUTO]
- Checking configured nameservers
  - Testing nameservers
    - Nameserver: 192.168.1.1 [OK]
    - Nameserver: 8.8.8.8 [OK]
    - Nameserver: 8.8.4.4 [OK]
- Minimal of 2 responsive nameservers: [OK]
- Checking default gateway: [DONE]
- Getting listening ports (TCP/UDP)
  * Found 15 ports
- Checking promiscuous interfaces: [OK]
- Checking waiting connections: [OK]
- Checking status DHCP client: [NOT ACTIVE]
- Checking for ARP monitoring software: [NOT FOUND]

### Printers and Spools

- Checking cups daemon: [NOT FOUND]
- Checking lp daemon: [NOT RUNNING]

### Software: e-mail and messaging

- Postfix status
  - Postfix configuration: [RUNNING]
  - Postfix banner: [FOUND]

### Software: firewalls

- Checking iptables kernel module: [FOUND]
- Checking iptables policies of chains: [FOUND]
- Checking for empty ruleset: [OK]
- Checking for unused rules: [FOUND]
- Checking host based firewall: [ACTIVE]
How it works

● Initialization

● Run
  ○ Helpers
  ○ Plugins
  ○ Tests

● Show audit results
Warnings (2):
------------------------
! Reboot of system is most likely needed [KRNL-5830]
   - solution: reboot
      https://cisofy.com/controls/KRNL-5830/

! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]
   https://cisofy.com/controls/MAIL-8818/

Suggestions (41):
------------------------
* Version of Lynis outdated, consider upgrading to the latest version [LYNIS]
      https://cisofy.com/controls/LYNIS/

* Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user
      https://cisofy.com/controls/BOOT-5122/

* Install a PAM module for password strength testing like pan_cracklib or pan_passwdqc [AUTH-9262]
      https://cisofy.com/controls/AUTH-9262/

* Configure minimum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/controls/AUTH-9286/

* Configure maximum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/controls/AUTH-9286/

* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
      https://cisofy.com/controls/AUTH-9328/
Lynis security scan details:

Hardening index : 62 [############################]
Tests performed : 266
Plugins enabled : 18

Components:
- Firewall [V]
- Malware scanner [X]

Lynis Modules:
- Compliance Status [?]
- Security Audit [V]
- Vulnerability Scan [V]

Files:
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat
Why Lynis?

Flexibility

- No dependencies*
- Understandable
- Create your own tests

* Besides common tools like awk, grep, ps
Why Lynis?

Three pillars
1. First impression
2. Keep it simple
3. Next step
Why Lynis?

Next step:

Lynis update available

Current version : 262   Latest version : 264

Please update to the latest version.
New releases include additional features, bug fixes, tests, and baselines.

Download the latest version:

Packages (DEB/RPM) - https://packages.cisofy.com
Website (TAR) - https://cisofy.com/downloads/
GitHub (source) - https://github.com/CISOfy/lynis
Running Lynis

- lynis
- lynis audit system
- lynis show
- lynis show commands
 lynis show categories  (display test categories)
 lynis show changelog [version]  (release details)
 lynis show commands  (all available commands)
 lynis show dbdir  (database directory)
 lynis show details  (display test details from log file)
 lynis show environment  (hardware, virtual machine, or container type)
 lynis show groups  (test groups)
 lynis show help  (detailed information about arguments)
 lynis show hostids  (unique IDs for this system)
 lynis show includedir  (include directory for tests and functions)
 lynis show language  (configured or detected language)
 lynis show license  (license details)
 lynis show logfile  (location of logfile)
 lynis show man  (show help)
 lynis show options  (available flags and options)
 lynis show os  (operating system and version)
 lynis show pidfile  (active file to stored process ID)
 lynis show pluginindir  (directory with plugins)
 lynis show profiles  (discovered profiles)
 lynis show release  (version)
 lynis show releasedate  (date of release)
 lynis show report  (location of report data)
 lynis show settings  (display configured settings, options: --brief --nocolors)
 lynis show tests [test]  (display information about one or more tests)
 lynis show tests skipped  (which tests to skip according profile)
 lynis show version  (Lynis version)
 lynis show workdir  (work directory)
Lynis Profiles

Optional configuration

- Default.prf
- Custom.prf
- Other profiles
Automation

Dealing with findings

- Log + website
- Create hardening snippet
- Automate via Chef, Puppet, Salt, etc.
Let’s summarize
Summary

Take action:

1. Perform regular scans
2. Get that low-hanging fruit
3. Automate the outcome
Success!

You finished this presentation
Questions?

Connect

- Twitter: @mboelen
- LinkedIn: Michael Boelen

Relevant project: https://LinuxSecurity.Expert
(security tools, checklists, guides)
D3NH4CK
Hét security-event van Nederland

www.denhack.nl