

SYSTEM HARDENING LAB01

1 Revision

Revision	Date	Author	Description
01	06/05/2018	F. Coppo	System Hardening Report LAB01

2 Summary

1	Revision.....	2
2	Summary.....	3
3	Preparation.....	4
4	Perform an audit (Es1).....	4
5	Package Warning Analysis	5
6	Component checklist (Es2)	7
6.1	Firewall	7
6.2	Malware scanner	8
7	Unprivileged user test run (Es3)	9
	In the picture below is reported not privileged scan mode result:.....	9
8	Warning elimination (Es4)	9
8.1	Kernel Hardening warning (Es4)	9
9	Password Hardening (Es5)	10
10	Tests removing (Es6).....	12
11	SSH server hardening (Es7).....	13
11.1	SSH Users and Groups	15
11.2	SSH Port	16
12	USB storage hardening (Es8)	17
13	Increase Hardening index (Es9)	18
13.1	Kernel.....	18
13.2	Password robustness	19
13.3	Compilers	20
13.4	File integrity tool	20

3 Preparation

The exercises proposed in this laboratory aim to find some possible vulnerabilities of a Linux system using **Lynis** tool and explaining how is possible to solve it. In order to prepare the environment, following step has been executed:

- Install UBUNTU-16-04.4 desktop on Virtual Machine support
- Install Lynis tool on target machine

```
root@ubuntu:/home/coppo# lynis show version
2.6.4
```

Lynis is a security auditing tool that checks the system and the software configuration, to see if there is any point of improvement the security defenses.

4 Perform an audit (Es1)

It has been done an audit on the system distribution performing a system scan as root user:

```
root@ubuntu:/home/coppo# lynis audit system
```

```
Program version: 2.6.4
Operating system: Linux
Operating system name: Ubuntu Linux
Operating system version: 16.04
Kernel version: 4.13.0
Hardware platform: x86_64
Hostname: ubuntu
```

The report, displayed at the end of the scan, contains warnings, suggestions and other info like the number of security tests performed. The *Hardening index* displayed in the report resume, reported in the next figure, gives the auditor an impression on how well a system is configured for hardening. This number is not the percentage of how much a system is “safe”, but just an indicator of taken measures and configuration performed. The goal of Hardening Index flag is to encourage the auditor to check if the system is well hardened.

```

root@ubuntu:/home/coppo
https://cisofy.com/controls/TOOL-5002/

* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
- Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)
https://cisofy.com/controls/KRNL-6000/

* Harden compilers like restricting access to root user only [HRDN-7222]
https://cisofy.com/controls/HRDN-7222/

* Harden the system by installing at least one malware scanner, to perform periodic sy
sten scans [HRDN-7230]
- Solution : Install a tool like rkhunter, chkrootkit, OSSEC
https://cisofy.com/controls/HRDN-7230/

Follow-up:
-----
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)

=====
Lynis security scan details:
Hardening index : 56 [#####]
Tests performed : 203
Plugins enabled : 0

Components:
- Firewall [X]
- 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

=====

```

Additionally in the scan resume is reported the location of two files generated by the tool:

- **lynis.log** : is a log file, a trace with a time stamp, containing information about test performed, test result, test skipped, action performed by the tool etc.
- **lynis-report**: report data, contain few info about the software version under auditing.

5 Package Warning Analysis

The tool tests for the presence of vulnerable packages and when it finds something, the warning is reported. In our case is present the following packet warning (PKGS):

Warnings (1):

! Found one or more vulnerable packages. [PKGS-7392]

<https://cisofy.com/controls/PKGS-7392/>

It is marked as high impact, as each vulnerable package can be exploited by attackers: the solution is to install security updates.

Here below is reported a detail of the test performed by the tool about this specific warning.

```

root@ubuntu:/home/coppo# sudo lynis show details PKGS-7392
2018-05-04 05:39:06 Performing test ID PKGS-7392 (Check for Debian/Ubuntu security updates)
2018-05-04 05:39:06 Action: updating package repository with apt-get
2018-05-04 05:39:09 Result: apt-get finished
2018-05-04 05:39:09 Test: Checking if /usr/lib/update-notifier/apt-check exists

```

```

2018-05-04 05:39:09 Result: found /usr/lib/update-notifier/apt-check
2018-05-04 05:39:09 Test: checking if any of the updates contain security updates
2018-05-04 05:39:11 Result: found 45 security updates via apt-check
2018-05-04 05:39:11 Hardening: assigned partial number of hardening points (0 of 25). Currently having 89 points (out of 153)
2018-05-04 05:39:14 Result: found vulnerable package(s) via apt-get (-security channel)
2018-05-04 05:39:14 Found vulnerable package: firefox
2018-05-04 05:39:14 Found vulnerable package: ghostscript
2018-05-04 05:39:14 Found vulnerable package: ghostscript-x
2018-05-04 05:39:14 Found vulnerable package: libcurl3
2018-05-04 05:39:14 Found vulnerable package: libcurl3-gnutls
2018-05-04 05:39:14 Found vulnerable package: libgs9
2018-05-04 05:39:14 Found vulnerable package: libgs9-common
2018-05-04 05:39:14 Found vulnerable package: libicu55
2018-05-04 05:39:14 Found vulnerable package: libperl5.22
2018-05-04 05:39:14 Found vulnerable package: libraw15
2018-05-04 05:39:14 Found vulnerable package: libsmclient
2018-05-04 05:39:14 Found vulnerable package: libssl1.0.0
2018-05-04 05:39:14 Found vulnerable package: libtiff5
2018-05-04 05:39:14 Found vulnerable package: libvncclient1
2018-05-04 05:39:14 Found vulnerable package: libvorbis0a
2018-05-04 05:39:14 Found vulnerable package: libvorbisenc2
2018-05-04 05:39:14 Found vulnerable package: libvorbisfile3
2018-05-04 05:39:14 Found vulnerable package: libwayland-client0
2018-05-04 05:39:14 Found vulnerable package: libwayland-cursor0
2018-05-04 05:39:14 Found vulnerable package: libwayland-server0
2018-05-04 05:39:14 Found vulnerable package: libwbclient0
2018-05-04 05:39:14 Found vulnerable package: openssl
2018-05-04 05:39:14 Found vulnerable package: patch
2018-05-04 05:39:14 Found vulnerable package: perl
2018-05-04 05:39:14 Found vulnerable package: perl-base
2018-05-04 05:39:14 Found vulnerable package: perl-modules-5.22
2018-05-04 05:39:14 Found vulnerable package: python3-distupgrader
2018-05-04 05:39:14 Found vulnerable package: samba-ls
2018-05-04 05:39:14 Found vulnerable package: ubuntu-release-upgrader-core
2018-05-04 05:39:14 Found vulnerable package: ubuntu-release-upgrader-gtk
2018-05-04 05:39:14 Warning: Found one or more vulnerable packages. [test:PKGS-7392] [details:-] [solution:-]
2018-05-04 05:39:14 Suggestion: Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or unattended-upgrades
[test:PKGS-7392] [details:-] [solution:-]
2018-05-04 05:39:14 =====

```

The auditor, is also advised to watch default configuration and pay attention to not-configured setting. Here below is reported an example of configuration setting captured by the tool:

```

root@ubuntu:/home/coppo# lynis show settings
# Colored screen output
colors=1

# Compressed uploads
compressed-uploads=0

# Use non-zero exit code if one or more warnings were found
error-on-warnings=0

# Language
language=en

# License key
license-key=[not configured]

# Logging of tests that have a different OS
log-tests-incorrect-os=1

# Machine role (personal, workstation or server)
machine-role=server

# Pause between tests (in seconds)
pause-between-tests=0

# Quick mode (non-interactive)
quick=0

# Refresh repositories (for vulnerable package detection)
refresh-repositories=1

# Show more details in report (solution)
show-report-solution=1

```

```
# Show tool tips
show-tool-tips=1

# Skip plugins
skip-plugins=0

# Skip upgrade test
skip-upgrade-test=0

# Paths for SSL certificates
ssl-certificate-paths=/etc/apache2:/etc/dovecot:/etc/httpd:/etc/letsencrypt:/etc/pki:/etc/postfix:/etc/ssl:/opt/psa/var/certificates:/usr/local/psa/var/certificates:/usr/local/share/ca-certificates:/var/www:/srv/www

# Perform strict code test of scripts
strict=0

# Scan mode
test-scan-mode=full

# Upload options
upload-options=[not configured]

# Upload server (ip or hostname)
upload-server=[not configured]

# Data upload after scanning
upload=no

# Verbose output
verbose=0
```

6 Component checklist (Es2)

After the first scan, the component checklist reports that Firewall and Malware Scanner components are missed.

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

6.1 Firewall

Also into the specific firewall section of the report is mark the missing of this component:

```
[+] Software: firewalls
-----
- Checking iptables kernel module [ NOT FOUND ]
- Checking host based firewall [ NOT ACTIVE ]
```

And in the *Suggestion* section of the report it is marked some advice to address the warning (FIRE-4590).

```
* Configure a firewall/packet filter to filter incoming and outgoing traffic [FIRE-4590]
https://cisofy.com/controls/FIRE-4590/
```

From log file *lynis.log* a similar advice is reported

```
2018-05-04 05:39:16 =====
2018-05-04 05:39:16 Performing test ID FIRE-4590 (Check firewall status)
2018-05-04 05:39:16 Result: no host based firewall/packet filter found or configured
2018-05-04 05:39:16 Suggestion: Configure a firewall/packet filter to filter incoming and outgoing traffic [test:FIRE-4590] [details:-] [solution:-]
2018-05-04 05:39:16 Hardening: assigned partial number of hardening points (0 of 5). Currently having 96 points (out of 166)
2018-05-04 05:39:16 =====
```

The auditor, to solve this vulnerability shall enable the firewall with following command.

```
sudo ufw enable
```

6.2 Malware scanner

As reported into *Hardening* section of the report and into *Suggestion* section , a Malware scanner is not present on that distribution and shall be installed.

```
[+] Hardening
-----
- Installed compiler(s)           [ FOUND ]
- Installed malware scanner      [ NOT FOUND ]
```

```
* Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]
- Solution : Install a tool like rkhunter, chkrootkit, OSSEC
https://cisofy.com/controls/HRDN-7230/
```

From log file *lynis.log* a similar advice is reported

```
2018-05-04 05:39:25 =====
2018-05-04 05:39:25 Performing test ID HRDN-7230 (Check for malware scanner)
2018-05-04 05:39:25 Test: Check if a malware scanner is installed
2018-05-04 05:39:25 Result: no malware scanner found
2018-05-04 05:39:25 Suggestion: Harden the system by installing at least one malware scanner, to perform periodic file system scans [test:HRDN-7230] [details:-] [solution:Install a tool like rkhunter, chkrootkit, OSSEC]
2018-05-04 05:39:25 Hardening: assigned partial number of hardening points (1 of 3). Currently having 133 points (out of 236)
2018-05-04 05:39:25 Result: no malware scanner found
2018-05-04 05:39:25 =====
```

The auditor, to solve this vulnerability shall install a Malware Scanner:

```
sudo apt-get install rkhunter
```

After enabling and installing of firewall and Malware Scanner, a greater number of test is performed, and the Hardening Index has been increased.

```
root@ubuntu:/# lynis show details HRDN-7230
2018-05-04 09:38:06 Performing test ID HRDN-7230 (Check for malware scanner)
2018-05-04 09:38:06 Test: Check if a malware scanner is installed
2018-05-04 09:38:06 Result: found at least one malware scanner
2018-05-04 09:38:06 Hardening: assigned maximum number of hardening points for this item (3). Currently having 188 points (out of 283)
2018-05-04 09:38:06 =====
root@ubuntu:/# lynis show details FIRE-4590
2018-05-04 09:37:54 Performing test ID FIRE-4590 (Check firewall status)
2018-05-04 09:37:54 Result: host based firewall or packet filter is active
2018-05-04 09:37:54 Hardening: assigned maximum number of hardening points for this item (5). Currently having 104 points (out of 141)
2018-05-04 09:37:54 =====
```

The component list after countermeasures is updated, as reported in the next screenshot.


```

=====
Lynis security scan details:
Hardening Index : 67 [##### ]
Tests performed : 210
Plugins enabled : 0

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

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
=====

```

7 Unprivileged user test run (Es3)

Running not privileged scan mode, some tests will be skipped (as they require root permissions) and some tests might fail silently or give different results.

```

root@ubuntu:/home/coppo# su coppo
coppo@ubuntu:~$ lynis audit system

```

In the picture below is reported not privileged scan mode result:

```

coppo@ubuntu:~$ lynis audit system
=====
Lynis security scan details:
Hardening Index : 62 [##### ]
Tests performed : 199
Plugins enabled : 0

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

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

Files:
- Test and debug information : /tmp/lynis.log
- Report data : /tmp/lynis-report.dat
=====

```

The hardening index and the number of test performed decrease.

8 Warning elimination (Es4)

The NETW-2705 warning has been checked and seems not applicable on that distribution:

```

2018-05-04 05:39:15 =====
2018-05-04 05:39:15 Skipped test NETW-2705 (Check availability two nameservers)
2018-05-04 05:39:15 Reason to skip: Prerequisites not met (ie missing tool, other type of Linux distribution)
2018-05-04 05:39:15 Result: Test most likely skipped due having local resolver in /etc/resolv.conf
2018-05-04 05:39:15 =====

```

8.1 Kernel Hardening warning (Es4)

In order to address kernel hardening warning, has been modify some kernel parameter as reported below.

[+] Kernel Hardening

```

- Comparing sysctl key pairs with scan profile
- fs.protected_hardlinks (exp: 1) [ OK ]
- fs.protected_symlinks (exp: 1) [ OK ]
- fs.suid_dumpable (exp: 0) [ DIFFERENT ]
- kernel.core_uses_pid (exp: 1) [ DIFFERENT ]

```

```
- kernel.ctrl-alt-del (exp: 0) [ OK ]
- kernel.dmesg_restrict (exp: 1) [ DIFFERENT ]
- kernel.kptr_restrict (exp: 2) [ DIFFERENT ]
```

```
root@ubuntu:/# sysctl kernel.kptr_restrict=2
kernel.kptr_restrict = 2
```

```
root@ubuntu:/# sysctl kernel.dmesg_restrict=1
kernel.dmesg_restrict = 1
```

Meaning of the configuration parameters:

- The parameter *dmesg_restrict* set to "1", allow only users with *CAP_SYS_ADMIN* read the kernel syslog via *dmesg(8)* or other mechanisms;
- If *kptr_restrict* is set to 2, kernel pointers using %pK are printed as 0's regardless of privileges.

After a news scan this warning is fixed

[+] Kernel Hardening

```
- Comparing sysctl key pairs with scan profile
- fs.protected_hardlinks (exp: 1) [ OK ]
- fs.protected_symlinks (exp: 1) [ OK ]
- fs.suid_dumpable (exp: 0) [ DIFFERENT ]
- kernel.core_uses_pid (exp: 1) [ OK ]
- kernel.ctrl-alt-del (exp: 0) [ OK ]
- kernel.dmesg_restrict (exp: 1) [ OK ]
- kernel.kptr_restrict (exp: 2) [ OK ]
- kernel.randomize_va_space (exp: 2) [ OK ]
```

and the *Hardening index* increases:

```
root@ubuntu: /home/coppo
https://cisofy.com/controls/HRDN-7222/

Follow-up:
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)

=====
Lynis security scan details:
Hardening index : 69 [#####]
Tests performed : 210
Plugins enabled : 0

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

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

Files:
- Test and debug information : /var/log/lynis.log
```

9 Password Hardening (Es5)

The AUTH-9286 suggestion has been analyzed; it requires the setup of expire date and proper aging for users' passwords.

```
lynis show details AUTH-9286
root@ubuntu:/home/coppo# lynis show details AUTH-9286
2018-05-04 07:12:24 Performing test ID AUTH-9286 (Checking user password aging)
2018-05-04 07:12:24 Test: Checking PASS_MIN_DAYS option in /etc/login.defs
2018-05-04 07:12:24 Result: password minimum age is not configured
2018-05-04 07:12:24 Suggestion: Configure minimum password age in /etc/login.defs [test:AUTH-9286] [details:-] [solution:-]
```

```

2018-05-04 07:12:24 Hardening: assigned partial number of hardening points (0 of 1). Currently having 14 points (out of 20)
2018-05-04 07:12:24 Test: Checking PASS_MAX_DAYS option in /etc/login.defs
2018-05-04 07:12:24 Result: password aging limits are not configured
2018-05-04 07:12:24 Suggestion: Configure maximum password age in /etc/login.defs [test:AUTH-9286] [details:-] [solution:-]
2018-05-04 07:12:24 Hardening: assigned partial number of hardening points (0 of 1). Currently having 14 points (out of 21)
2018-05-04 07:12:24 =====

```

Using *chage* command is possible to change password aging configuration

```

Minimum Password Age [10]: 10
Maximum Password Age [17]: 5
Last Password Change (YYYY-MM-DD) [2018-05-04]: 2018-04-04
Password Expiration Warning [2]: 2
Password Inactive [-1]: -1
Account Expiration Date (YYYY-MM-DD) [-1]: -1

```

Since the modification seems not persistent, the aging password configuration has been directly changed into login file: */etc/login.defs*

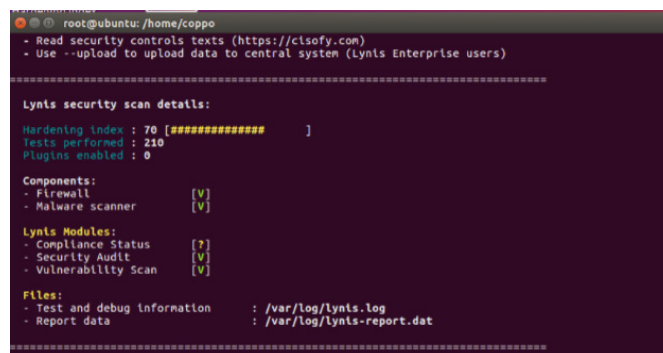
The result after password aging modification on AUTH-9282 is the following:

```

root@ubuntu:/home/coppo# lynis show details AUTH-9286
2018-05-04 08:04:47 Performing test ID AUTH-9286 (Checking user password aging)
2018-05-04 08:04:47 Test: Checking PASS_MIN_DAYS option in /etc/login.defs
2018-05-04 08:04:47 Result: password needs to be at least 5 days old
2018-05-04 08:04:47 Hardening: assigned maximum number of hardening points for this item (3). Currently having 17 points (out of 22)
2018-05-04 08:04:47 Test: Checking PASS_MAX_DAYS option in /etc/login.defs
2018-05-04 08:04:47 Result: max password age is 10 days
2018-05-04 08:04:47 Hardening: assigned maximum number of hardening points for this item (3). Currently having 20 points (out of 25)
2018-05-04 08:04:47 =====

```

As expected, the *Hardening index* has been increased after this warning fixed.



```

root@ubuntu:/home/coppo
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)

=====
Lynis security scan details:
Hardening index : 70 [#####]
Tests performed : 210
Plugins enabled : 0

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

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
=====

```

About AUTH-9282 suggestion, we can see that all account seems to have an expire date, so there is nothing to fix:

```

root@ubuntu:/# lynis show details AUTH-9282
2018-05-05 01:57:27 Performing test ID AUTH-9282 (Checking password protected account without expire date)
2018-05-05 01:57:27 Test: Checking Linux version and password expire date status
2018-05-05 01:57:27 Result: all accounts seem to have an expire date
2018-05-05 01:57:27 =====

```

10 Tests removing (Es6)

The auditor had to remove any test related to CUPS printing service. It has been checked the tests related to this service as reported below

```
root@ubuntu:/home/coppo# lynis show tests
.
.
.
PRNT-2304      Check cupsd status (security)
PRNT-2306      Check CUPSd configuration file (security)
PRNT-2307      Check CUPSd configuration file permissions (security)
PRNT-2308      Check CUPSd network configuration (security)
.
.
.
```

Before removing test the *Printers and Spools* session appears like following:

```
[+] Printers and Spools
-----
- Checking cups daemon           [ RUNNING ]
- Checking CUPS configuration file [ OK ]
- File permissions              [ WARNING ]
- Checking CUPS addresses/sockets [ FOUND ]
- Checking lp daemon            [ NOT RUNNING ]
```

It has been edited the path of current profile in order to add skip directive to each specific test as reported below:

```
root@ubuntu:/home/coppo# lynis show profiles
/etc/lynis/default.prf

root@ubuntu:/# nano /etc/lynis/default.prf

root@ubuntu: /home/coppo
GNU nano 2.5.3 File: /etc/lynis/default.prf
pause-between-tests=0
# Enable quick mode (no waiting for keypresses, same as --quick option)
quick=no
# Refresh software repositories to help detecting vulnerable packages
refresh-repositories=yes
# Show solution for findings
show-report-solution=yes
# Show inline tips about the tool
show-tool-tips=yes
# Skip plugins
skip-plugins=no
# Skip a test (one per line)
#skip-test=SSH-7408
skip-test=PRNT-2304
skip-test=PRNT-2306
skip-test=PRNT-2307
skip-test=PRNT-2308
```

It has been performed a new scan test and it has been checked that tool has skipped four tests. The *Printers and Spools* section result like following:

```
[+] Printers and Spools
-----
- Checking lp daemon            [ NOT RUNNING ]
```

11 SSH server hardening (Es7)

It has been installed ssh server; after installation a scan has been launched with following revealing results:

[+] SSH Support

```

- Checking running SSH daemon          [ FOUND ]
- Searching SSH configuration          [ FOUND ]
- SSH option: AllowTcpForwarding       [ SUGGESTION ]
- SSH option: ClientAliveCountMax     [ SUGGESTION ]
- SSH option: ClientAliveInterval     [ OK ]
- SSH option: Compression             [ SUGGESTION ]
- SSH option: FingerprintHash         [ OK ]
- SSH option: GatewayPorts            [ OK ]
- SSH option: IgnoreRhosts            [ OK ]
- SSH option: LoginGraceTime          [ OK ]
- SSH option: LogLevel                [ SUGGESTION ]
- SSH option: MaxAuthTries            [ SUGGESTION ]
- SSH option: MaxSessions             [ SUGGESTION ]
- SSH option: PermitRootLogin         [ SUGGESTION ]
- SSH option: PermitUserEnvironment   [ OK ]
- SSH option: PermitTunnel            [ OK ]
- SSH option: Port                    [ SUGGESTION ]
- SSH option: PrintLastLog            [ OK ]
- SSH option: Protocol                [ OK ]
- SSH option: StrictModes             [ OK ]
- SSH option: TCPKeepAlive            [ SUGGESTION ]
- SSH option: UseDNS                  [ OK ]
- SSH option: UsePrivilegeSeparation   [ SUGGESTION ]
- SSH option: VerifyReverseMapping     [ NOT FOUND ]
- SSH option: X11Forwarding           [ SUGGESTION ]
- SSH option: AllowAgentForwarding    [ SUGGESTION ]
- SSH option: AllowUsers               [ NOT FOUND ]
- SSH option: AllowGroups              [ NOT FOUND ]

```

After SSH installation, the hardening index has been decreased: this means that with this software we have increased the attack surface, and now we have to “harden” this surface.

From suggestion session has been taken in charge this following four suggestion:

```

* Consider hardening SSH configuration [SSH-7408]
- Details : Compression (YES --> NO)
  https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : LogLevel (INFO --> VERBOSE)
  https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : MaxAuthTries (6 --> 2)
  https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : MaxSessions (10 --> 2)
  https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : PermitRootLogin (WITHOUT-PASSWORD --> NO)
  https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : Port (22 --> )
  https://cisofy.com/controls/SSH-7408/

```

```

* Consider hardening SSH configuration [SSH-7408]
- Details : TCPKeepAlive (YES --> NO)
https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : UsePrivilegeSeparation (YES --> SANDBOX)
https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : X11Forwarding (YES --> NO)
https://cisofy.com/controls/SSH-7408/

* Consider hardening SSH configuration [SSH-7408]
- Details : AllowAgentForwarding (YES --> NO)

```

It has been changed configuration under `/etc/ssh/sshd_config` file for following parameters:

- *LogLevel*: the parameter equal "VERBOSE" allows to log more information, needed to monitor malicious SSH traffic;
- *x11Forwarding*: the X11 protocol is not secure and it is avoided;
- *tcpKeepAlive*: this option only uses TCP keep-alives (as opposed to using ssh level keep-alives). Even if seems that there's no exploitable vulnerability at now using TCP keep-alives, the parameter has been set in order to use ssh keep-alives level;
- *UsePrivilegeSeparation*: the sandbox mode does a jail environment. It is more secure to prevent escalation privilege, attack other host or kernel attack surface .

The new configuration, after `sshd_config` file manipulation is reported in green color.

```

root@ubuntu:/# sshd -T
port 22
protocol 2
addressfamily any
listenaddress [::]:22
listenaddress 0.0.0.0:22
usepam yes
serverkeybits 1024
loggingrctime 120
keyregenerationinterval 3600
x11displayoffset 10
maxauthtries 6
maxsessions 10
clientaliveinterval 0
clientalivecountmax 3
streamlocalbindmask 0177
permitrootlogin without-password
ignorerhosts yes
ignoreuserknownhosts no
rhostsauthentication no
hostbasedauthentication no
hostbasedusesnamefrompacketonly no
rsaauthentication yes
pubkeyauthentication yes
kerberosauthentication no
kerberosorlocalpasswd yes
kerberosticketcleanup yes
gssapiauthentication no
gssapikeyexchange no
gssapicleanupcredentials yes
gssapistrictacceptorcheck yes
gssapistorecredentialsonekey no
passwordauthentication yes
kbdinteractiveauthentication no
challengeresponseauthentication no
printmotd no
printlastlog yes
x11forwarding no
x11uselocalhost yes
permittty yes
permitusercc yes
strictmodes yes
tcpkeepalive no
permitemptypasswords no

```

```

permituserenvironment no
useloglein no
compression yes
gatewayports no
usedns no
allowtcpforwarding yes
allowagentforwarding yes
allowstreamlocalforwarding yes
useprivilegeseparation sandbox
fingerprinthash SHA256
pidfile /var/run/sshd.pid
xauthlocation /usr/bin/xauth
ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
macs umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-
etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
versionaddendum none
kexalgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-
group14-sha1
hostbasedacceptedkeytypes ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-
v01@openssh.com,ssh-ed25519-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-
ed25519,rsa-sha2-512,rsa-sha2-256,ssh-rsa
hostkeyalgorithms ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-
ed25519-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-ed25519,rsa-sha2-512,rsa-sha2-
256,ssh-rsa
pubkeyacceptedkeytypes ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-
ed25519-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-ed25519,rsa-sha2-512,rsa-sha2-
256,ssh-rsa
loglevel VERBOSE
syslogfacility AUTH
authorizedkeysfile .ssh/authorized_keys .ssh/authorized_keys2
hostkey /etc/ssh/ssh_host_rsa_key
hostkey /etc/ssh/ssh_host_dsa_key
hostkey /etc/ssh/ssh_host_ecdsa_key
hostkey /etc/ssh/ssh_host_ed25519_key
acceptenv LANG
acceptenv LC_*
subsystem sftp /usr/lib/openssh/sftp-server
maxstartups 10:30:100
permittunnel no
ipqos lowdelay throughput
rekeylimit 0 0
permitopen any

```

11.1 SSH Users and Groups

From test session are still preset some suggestion like the red-one in the following table.

SSH-7402	Check for running SSH daemon (security)
SSH-7404	Check SSH daemon file location (security)
SSH-7408	Check SSH specific defined options (security)
SSH-7440	AllowUsers and AllowGroups (security)

The SSH-7440 suggestion shows how it is necessary to limit SSH access to specific users as part of server hardening. We can easily accomplish this suggestion, by editing SSH configuration file `sshd_config` and adding the option **AllowUsers** followed by the user names. Only the listed users will have access to server. Also you can limit access to specific group by adding **AllowGroups** followed by group names. The procedure is showed in the following table.

```

PrintLastLog yes
TCPKeepAlive no
#UseLogin no

#MaxStartups 10:30:60
#Banner /etc/issue.net

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

Subsystem sftp /usr/lib/openssh/sftp-server

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes

AllowUsers user1
AllowGroups group1

```

After a new scan, the *SSH Support* session has been improved as showed below:

```

[+] SSH Support
-----
- Checking running SSH daemon           [ FOUND ]
- Searching SSH configuration           [ FOUND ]
- SSH option: AllowUsers                 [ FOUND ]
- SSH option: AllowGroups               [ FOUND ]

```

The test details shows that this item has been hardened:

```

root@ubuntu:/# sudo lynis show details SSH-7440
2018-05-05 03:10:53 Performing test ID SSH-7440 (Check SSH option: AllowUsers and AllowGroups)
2018-05-05 03:10:53 Result: AllowUsers set, with value user1
user2
2018-05-05 03:10:53 Result: AllowUsers set group1
group2
2018-05-05 03:10:54 Result: SSH is limited to a specific set of users, which is good
2018-05-05 03:10:54 Hardening: assigned maximum number of hardening points for this item (2). Currently having 106 points (out of 143)
2018-05-05 03:10:54 Checking permissions of /usr/share/lynis/include/tests_snmp
2018-05-05 03:10:54 File permissions are OK
2018-05-05 03:10:54 ===-----=====

```

NOTE:

Instead of allowing specific users, the auditor can block them: for this option the entry label to SSH configuration file is **DenyUsers**.

11.2 SSH Port

The SSH uses port 22 as default. In order to prevent automated attacks and improve system hardening, a best practice is to change the default port. Once it has been changed, it is more difficult for malicious agent address the port you are using for SSH service.

```

root@ubuntu:/
GNU nano 2.5.3 File: /etc/ssh/sshd_config

# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation SANSBOX

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

```


NOTE: *Protocol* supported is just version 2, so vulnerability of version 1 protocol are already fixed.

12 USB storage hardening (Es8)

USB storage is available and enabled:

```
[+] USB Devices
-----
- Checking usb-storage driver (modprobe config)      [ NOT DISABLED ]
- Checking USB devices authorization                  [ ENABLED ]
- Checking USBGuard                                  [ NOT FOUND ]
```

Lynis tool suggestion (STRG-1840) claims that this capability shall be removed if unnecessary.

* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [STRG-1840]
<https://cisofy.com/controls/STRG-1840/>

```
root@ubuntu:/# sudo lynis show details STRG-1840
2018-05-05 04:25:13 Performing test ID STRG-1840 (Check if USB storage is disabled)
2018-05-05 04:25:13 Test: Checking USB storage driver in directory /etc/modprobe.d and configuration file /etc/modprobe.conf
2018-05-05 04:25:13 Result: usb-storage driver is not explicitly disabled
2018-05-05 04:25:13 Suggestion: Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [test:STRG-1840] [details:-] [solution:-]
2018-05-05 04:25:13 Hardening: assigned partial number of hardening points (2 of 3). Currently having 89 points (out of 113)
2018-05-05 04:25:13 ===-----=====
```

Once disabled this capability

```
root@ubuntu:/# echo "blacklist usb-storage" | sudo tee -a /etc/modprobe.d/blacklist.conf
blacklist usb-storage
```

It has been check that the module is not loaded any more:

```
root@ubuntu:/# sudo lynis show details STRG-1840
2018-05-05 04:54:39 Performing test ID STRG-1840 (Check if USB storage is disabled)
2018-05-05 04:54:39 Test: Checking USB storage driver in directory /etc/modprobe.d and configuration file /etc/modprobe.conf
2018-05-05 04:54:39 Result: found usb-storage driver in disabled state (blacklisted)
2018-05-05 04:54:39 Result: usb-storage driver is disabled
2018-05-05 04:54:39 Hardening: assigned maximum number of hardening points for this item (3). Currently having 90 points (out of 113)
2018-05-05 04:54:39 ===-----=====
root@ubuntu:/#
```

```
[+] USB Devices
-----
- Checking usb-storage driver (modprobe config)      [ DISABLED ]
```

In the meantime the *Hardening Index* has been increased:

```
root@ubuntu: /

Hardening index : 72 [#####          ]
Tests performed : 208
Plugins enabled  : 0

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

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

=====
```

13 Increase Hardening index (Es9)

13.1 Kernel

It has been addressed others kernel configuration issues detected in the Kernel hardening section of the report, using *sysctl* commands:

```
root@ubuntu:/# sysctl net.ipv4.conf.all.log_martians=1
net.ipv4.conf.all.log_martians = 1
root@ubuntu:/# sysctl net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.all.send_redirects = 0
root@ubuntu:/# sysctl net.ipv4.conf.default.log_martians=1
net.ipv4.conf.default.log_martians = 1
root@ubuntu:/# sysctl net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
root@ubuntu:/# sysctl kernel.sysrq=0
kernel.sysrq = 0
root@ubuntu:/# sysctl fs.suid_dumpable=0
```

Where:

- *net.ipv4.conf.all.log_martians* is a label to used manage the logging into kernel log of packets with “impossible addresses” (Martian packet is IP packet which specifies a source or destination address that is reserved for special-use). Setting this label equal 1 it allows to log packet with suspicious source address;
- *kernel.sysrq* configured equal 0 disable completely *sysrq* control (where *sysrq* functionality allow user to perform low level command regardless machine state: is a sort of debugging functionality of the kernel);
- *net.ipv4.conf.all.send_redirects* equal 0 disable send redirects;
- *net.ipv4.tcp_syncookies* configured equal 1 enable the controls the use of TCP syncookies (that is a technique used to resist SYN flood attacks);
- *fs.suid_dumpable* configured equal 0 disable core dumps functionality.

Here below is reported *Kernel Hardening* session resume:

```
[+] Kernel Hardening
-----
- Comparing sysctl key pairs with scan profile
- fs.protected_hardlinks (exp: 1) [ OK ]
- fs.protected_symlinks (exp: 1) [ OK ]
- fs.suid_dumpable (exp: 0) [ OK ]
- kernel.core_uses_pid (exp: 1) [ OK ]
- kernel.ctrl-alt-del (exp: 0) [ OK ]
- kernel.dmesg_restrict (exp: 1) [ OK ]
- kernel.kptr_restrict (exp: 2) [ OK ]
- kernel.randomize_va_space (exp: 2) [ OK ]
- kernel.sysrq (exp: 0) [ OK ]
- kernel.yama.ptrace_scope (exp: 1 2 3) [ OK ]
- net.ipv4.conf.all.accept_redirects (exp: 0) [ OK ]
- net.ipv4.conf.all.accept_source_route (exp: 0) [ OK ]
- net.ipv4.conf.all.bootp_relay (exp: 0) [ OK ]
- net.ipv4.conf.all.forwarding (exp: 0) [ OK ]
- net.ipv4.conf.all.log_martians (exp: 1) [ OK ]
- net.ipv4.conf.all.mc_forwarding (exp: 0) [ OK ]
- net.ipv4.conf.all.proxy_arp (exp: 0) [ OK ]
- net.ipv4.conf.all.rp_filter (exp: 1) [ OK ]
- net.ipv4.conf.all.send_redirects (exp: 0) [ OK ]
- net.ipv4.conf.default.accept_redirects (exp: 0) [ OK ]
- net.ipv4.conf.default.accept_source_route (exp: 0) [ OK ]
- net.ipv4.conf.default.log_martians (exp: 1) [ OK ]
- net.ipv4.tcp_echo_ignore_broadcasts (exp: 1) [ OK ]
- net.ipv4.tcp_ignore_bogus_error_responses (exp: 1) [ OK ]
- net.ipv4.tcp_syncookies (exp: 1) [ OK ]
- net.ipv4.tcp_timestamps (exp: 0 1) [ OK ]
- net.ipv4.conf.all.accept_redirects (exp: 0) [ OK ]
- net.ipv6.conf.all.accept_source_route (exp: 0) [ OK ]
- net.ipv6.conf.default.accept_redirects (exp: 0) [ OK ]
- net.ipv6.conf.default.accept_source_route (exp: 0) [ OK ]
```

The hardening Index has been improved.

```

root@ubuntu: /
-----
- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (https://cisofy.com)
- Use --upload to upload data to central system (Lynis Enterprise users)
-----

Lynis security scan details:

Hardening index : 74 [#####          ]
Tests performed : 208
Plugins enabled : 0

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

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
-----

```

13.2 Password robustness

Some modules within the PAM framework can help restricting access to facilities to only authorized people, including limitations as a strong password. Passwords should be protected and strengthened where possible.

The system detect that is missing a MAP module for password strength checking:

```

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

2018-05-05 05:50:11 Performing test ID AUTH-9262 (Checking presence password strength testing tools (PAM))
2018-05-05 05:50:11 Searching PAM password testing modules (cracklib, passwdqc, pwquality)
2018-05-05 05:50:11 Result: pam_cracklib.so NOT found (crack library PAM)
2018-05-05 05:50:11 Result: pam_passwdqc.so NOT found (passwd quality control PAM)
2018-05-05 05:50:11 Result: pam_pwquality.so NOT found (pwquality control PAM)
2018-05-05 05:50:11 Result: no PAM modules for password strength testing found
2018-05-05 05:50:11 Suggestion: Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [test:AUTH-9262] [details:-] [solution:-]
2018-05-05 05:50:11 Hardening: assigned partial number of hardening points (0 of 3). Currently having 14 points (out of 19)
2018-05-05 05:50:11 ===-----=====

```

In this example has been included tools like *passwdqc* (password quality control) and *cracklib* (password cracking library).

```
sudo apt-get install libpam-cracklib
```

After new scan:

```

root@ubuntu:/# lynis show details AUTH-9262
2018-05-05 06:26:27 Performing test ID AUTH-9262 (Checking presence password strength testing tools (PAM))
2018-05-05 06:26:27 Searching PAM password testing modules (cracklib, passwdqc, pwquality)
2018-05-05 06:26:27 Result: found pam_cracklib.so (crack library PAM) in /lib/x86_64-linux-gnu/security
2018-05-05 06:26:27 Result: pam_cracklib.so found
2018-05-05 06:26:27 Result: pam_passwdqc.so NOT found (passwd quality control PAM)
2018-05-05 06:26:27 Result: pam_pwquality.so NOT found (pwquality control PAM)
2018-05-05 06:26:27 Result: found at least one PAM module for password strength testing
2018-05-05 06:26:27 Hardening: assigned maximum number of hardening points for this item (3). Currently having 17 points (out of 19)
2018-05-05 06:26:27 ===-----=====

```

Hardening Index has been increased

```
Hardening index : 76 [#####          ]
```

13.3 Compilers

Following suggestion has been fixed

```
* Harden compilers like restricting access to root user only [HRDN-7222]
https://cisofy.com/controls/HRDN-7222/
```

When possible, the removal of any unused compilers is the best option. In this example compilers has been hardened restricting access to root user only. The result has been reported below

```
root@ubuntu:/# lynis show details HRDN-7222
2018-05-05 06:48:50 Performing test ID HRDN-7222 (Check compiler permissions)
2018-05-05 06:48:50 Test: Check if one or more compilers can be found on the system
2018-05-05 06:48:50 Test: Check file permissions for /usr/bin/as
2018-05-05 06:48:50 Action: checking symlink for file /usr/bin/as
2018-05-05 06:48:50 Note: Using real readlink binary to determine symlink on /usr/bin/as
2018-05-05 06:48:50 Result: readlink shows /usr/bin/x86_64-linux-gnu-as as output
2018-05-05 06:48:50 Result: symlink found, pointing to file /usr/bin/x86_64-linux-gnu-as
2018-05-05 06:48:50 Hardening: assigned maximum number of hardening points for this item (3). Currently having 160 points (out of 209)
2018-05-05 06:48:50 Test: Check file permissions for /usr/bin/gcc
2018-05-05 06:48:50 Action: checking symlink for file /usr/bin/gcc
2018-05-05 06:48:50 Note: Using real readlink binary to determine symlink on /usr/bin/gcc
2018-05-05 06:48:50 Result: readlink shows /usr/bin/gcc-5 as output
2018-05-05 06:48:50 Result: symlink found, pointing to file /usr/bin/gcc-5
2018-05-05 06:48:50 Hardening: assigned maximum number of hardening points for this item (3). Currently having 163 points (out of 212)
2018-05-05 06:48:50 ===-----===
```

Hardening index has been increase to 77.

```
Hardening index : 77 [##### ]
```

13.4 File integrity tool

The following test case do not detect any file integrity tool.

```
root@ubuntu:/# lynis show details FINT-4350
2018-05-05 07:30:49 Performing test ID FINT-4350 (File integrity software installed)
2018-05-05 07:30:49 Test: Check if at least on file integrity tool is available/installed
2018-05-05 07:30:49 Result: No file integrity tools found
2018-05-05 07:30:49 Suggestion: Install a file integrity tool to monitor changes to critical and sensitive files [test:FINT-4350] [details:-] [solution:-]
2018-05-05 07:30:49 Hardening: assigned partial number of hardening points (0 of 5). Currently having 125 points (out of 166)
2018-05-05 07:30:49 Checking permissions of /usr/share/lynis/include/tests_tooling
2018-05-05 07:30:49 File permissions are OK
2018-05-05 07:30:49 ===-----===
```

To fix this suggestion it has been installed AIDE file integrity tool.

```
root@ubuntu:/# apt install aide

root@ubuntu:/# aide -v
Aide 0.16a2-19-g16ed855

Compiled with the following options:

WITH_MMAP
WITH_POSIX_ACL
WITH_SELINUX
WITH_XATTR
WITH_E2FSATTRS
WITH_LSTAT64
WITH_READDIR64
WITH_ZLIB
WITH_MHASH
WITH_AUDIT
CONFIG_FILE = "/dev/null"
```

