h, 2023		npliance Report a Randall Seymore

Table of Contents

Statement of Objective	
Theory	
Description of Experimental Setup	
Procedure	1
Data	2
Analysis of Data	12
Discussion of Results	12
Conclusion	12
Appendices	13
Initial Lynis Vulnerability Scan Results	13
Post-Hardening Lynis Vulnerability Scan Results	24

Statement of Objective

The objective of this lab report is to determine the effectiveness of steps to harden an Ubuntu Server 22.04 system by implementing configuration changes recommended by the Center for Internet Security (CIS) Benchmark for Ubuntu Linux 22.04 (v1.0.0). Efficacy of changes will be measured by performing a baseline vulnerability scan before hardening the system, then comparing those results to a subsequent scan performed after all configuration changes have been applied.

Theory

Ubuntu is a widely used Linux distribution. Like any other operating system, default configurations introduce numerous vulnerabilities. By implementing recommended hardening measures derived from CIS benchmarks, we anticipate a notable improvement in the post-configuration scan Lynis Hardening Index over the initial value of 63. This improvement would signify a more robust and resilient system configuration to better protect against potential threats.

Description of Experimental Setup

All hardening configurations were applied to a single Virtual Machine (VM) created from the latest Ubuntu Server 22.04 LTS image available on the Ubuntu Download page. The VM was run on an ESXi Hypervisor and was allocated 2 vCPUs, 4 GB RAM, and 50 GB of storage. The VM was assigned a single NIC, receiving IP assignment and internal DNS lookup address from DHCP, allowing connectivity to a virtual network with outbound internet access only.

Procedure

After downloading the Ubuntu Server 22.04.03 LTS image from https://ubuntu.com/download/server, a virtual machine with specifications described in the section above was deployed in a lab environment. The installation steps were followed to create a non root user and include a default ssh server configuration.

Following deployment, administrators connected to the VM remotely and performed apt package update and upgrade steps. The Lynis scanner was downloaded directly to the VM from https://github.com/CISOfy/Lynis and run as root to generate the Initial Lynis Vulnerability Scan Results.

Recommendations from the initial scan were taken and identified on the <u>Ubuntu 22.04 CIS Benchmark</u>. Each set of guidance was combined to identify an appropriate configuration to harden the system accordingly. Testers performed each assigned test first on a replicated VM to validate feasibility and make any adjustments for final implementation on the primary VM.

After applying hardening configurations for 15 items on the primary VM, a second scan was run and compared with the initial scan to determine if the Lynis Hardening Index value increased.

Data

Step	Guidance	Configuration Applied	Evidence
1	Lynis Scan Recommendation Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122] CIS Benchmark Recommendation 1.4.1 - Ensure bootloader password is set	1. Create an encrypted password: cybr510-dbaba# grub-mkpasswd-pbkdf2 2. Add the following lines into the '/etc/grub.d/ <uniquenum>-custo m' configuration file: cat <<eof <username="" password_pbkdf2="" set="" superusers="<username>"> <encrypted-password> EOF 3. Update the grub2 configuration: cybr510-dbaba# update-grub</encrypted-password></eof></uniquenum>	Audit: root@cybr510-dbaba:/home/rbarber# grep "^set superusers" /boot/grub/grub.cfg root@cybr510-dbaba:/home/rbarber# grub-mkpasswd-pbkdf2 Enter password: Reenter password: Reenter password: Reenter password: Revord
2	Lynis Scan Recommendation Configure maximum password age in /etc/login.defs [AUTH-9286]	Set the PASS_MAX_DAYS parameter to conform to site policy in /etc/login.defs: PASS_MAX_DAYS 365	Audit: root@cybr510-dbaba:-# cat /etc/login.defs grep PASS_MAX_DAYS # PASS_MAX_DAYS Maximum number of days a password may be used. PASS_NAX_DAYS 99999
	CIS Benchmark Recommendation 5.5.1.2 - Ensure password expiration is 365 days or less	2. Modify user parameters for all users with a password set to match: cybr510-dbaba# chagemaxdays 365 <user></user>	Result: [root@cybr510-dbaba:~# chage -l rbarber Last password change : Sep 30, 2023 Password expires : Sep 29, 2024 Password inactive : never Account expires : never Hinimum number of days between password change : 0 Maximum number of days between password change : 365 Number of days of warning before password expires : 7

Lynis Scan Recommendation

Consider hardening SSH configuration [SSH-7408]

2. Then sudo nano

CIS Benchmark Recommendation

3

5.2.4 Configure SSH Server

1. Firstly run sudo sshd -T -C user=root -C host="\$(hostname)" -C addr="\$(grep \$(hostname) /etc/hosts | awk '{print \$1}')" | grep -Pi '^\h*(allow|deny)(users|groups)\ h+\H+(\h+.*)?\$'

/etc/ssh/sshd_config

3. Added the phrase "AllowUsers lumi"

4. Re-ran sudo sshd -T -C user=root -C host="\$(hostname)" -C addr="\$(grep \$(hostname) /etc/hosts | awk '{print \$1}')" | grep -Pi '^\h*(allow|deny)(users|groups)\ h+\H+(\h+.*)?\$'

Audit:

Remediation:

Results:

Lynis Scan Recommendation Configure password hashing rounds in 1. Edit the /etc/login.defs `/etc/pam.d/common-password` [AUTH-9230] file and update line 25 of the `pam_unix.so` to include the following: password [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass Audit: remember=5 2. Edit '/etc/login.defs' and ensure 4 that `ENCRYPT_METHOD` is set to 'yescrypt'. Remediation/Results: ENCRYPT_METHOD yescrypt **CIS Benchmark** Recommendation 3. Force each user on the system 5.4.4 Ensure to reset password at next login password hashing in order to force hashing with algorithm is up to updated algorithm. date with the latest standards. passwd --expire <username> 5.4.5 Ensure all current passwords uses the configured hashing algorithm.

1. Remove or modify the 'umask' of any files returned by the following command: Lynis Scan Recommendation cybr510-dbaba# grep -RPi Audit: '(^|^[^#]*)\s*umask\s+([0-7][0-7][01][0-7 Default umask in (root@cybr510-dbaba:~# cat /etc/login.defs | grep UMASK # UMASK Default "umask" value. # UMASK is the default umask value for pam_umask and is # 022 is the "historical" value in Debian for UMASK # If USERGROUPS_ENAB is set to "yes", that will modify]\b|[0-7][0-7][0-6]\b|[0-7][01][0-7]\b| /etc/login.defs could [0-7][0-7][0-6]\b|(u=[rwx]{0,3},)?(g=[rwx] be more strict like [0,3], ?o=[rwx]+\b|(u=[rwx]{1,3},)?g=[^ 027 [AUTH-9328] $rx]{1,3}(,o=[rwx]{0,3})?b)'$ /etc/login.defs /etc/profile* aba:~# cat /etc/login.defs | grep USERGROUPS_ENAB _ENAB is set to "yes", that will modify this UMASK default valu /etc/bash.bashrc* 5 Remediation/Results: 2. Edit '/etc/login.defs' and edit the root@cybr510-dbaba:-# vi /etc/login.defs root@cybr510-dbaba:-# cat /etc/login.defs | grep UMASK # UMVASK # UMVASK # UMVASK is the default umask value for pam umask and is used by # UZL is the "historical" value in Debian for IMVASK # 1F USERGROUPS_ENAB is set to "yes", that will modify this UMVASK default value UMVASK # 1F USERGROUPS_ENAB is not set, the value of UMVASK is used to create the mode. root@cybr510-dbaba:-# cat /etc/login.defs | grep USERGROUPS_ENAB # 1F USERGROUPS_ENAB is set to "yes", that will modify this UMVASK default value USERGROUPS_ENAB no **`UMASK`** and **`USERGROUPS_ENAB` lines as CIS Benchmark** follows: Recommendation UMASK 027 5.5.4 Ensure default user umask is 027 or more restrictive. USERGROUPS ENAB no Audit: Lynis Scan Audit Result: ** FAIL ** – Reason(s) for audit ailure: Recommendation module: "usb-storage" is loadable: nsmod /lib/modules/5.4.0-164-generic/kernel/drivers/usb/storage/usb-storage.ko module: "usb-storage" is not deny listed Disable drivers like USB storage when not used, to prevent module: "usb-storage" is not loaded unauthorized dina@mainserver:~/Projects\$ storage or data theft Remediation: 1. Run bash script provided by the zmedina@mainserver:~/Projects\$ sudo ./fix.sh — setting module: "usb–storage" to be not loadable — deny listing "usb–storage" zmedina@mainserver:~/Projects\$ _ 6 benchmark to disable usb-storage Results: **CIS Benchmark** zmedina@mainserver:~/Projects\$ sudo ./audit.sh Recommendation Audit Result: 1.1.10 Disable USB ** PASS ** Storage – module: "usb–storage" is not loadable: install /bin/false - module: "usb-storage" is not loaded - module: "usb-storage" is deny listed in: '/etc/modprobe.d/usb-storage.conf"

7	Lynis Scan Recommendation Add a legal banner to /etc/issue, to warn unauthorized users CIS Benchmark Recommendation 1.7.2 Ensure local login warning banner is configured	1.	Enter command: sudo bash -c "echo 'Authorized users only. All activity may be monitored and reported.' >> /etc/issue"	Audit: zmedino@mainserver:"\$ cat /etc/issue doubrit 20.04.6 LTS vn 1 zmedino@mainserver:"\$ grep -E -1 "(\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
8	Lynis Scan Recommendation Install a file integrity tool to monitor changes to critical and sensitive files CIS Benchmark Recommendation 1.3.1 Ensure AIDE is installed	1. 2. 3.	Enter command: sudo apt install aide aide-common Enter command: sudo aideinit Configure mail server for sending logs	Audit: International Interver: "\$ dpkg-query = H = f= {\frac{1}{1}} \text{binary: Fackage} \ta{\frac{1}{1}} \ta{\frac{1}{1}} \tatus = \tatus \tau \tau \tau \tau \tau \tau \tau \tau

9	Lynis Scan Recommendation Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc	 Enter command: sudo apt instal libpam-pwquality Edit the /etc/security/pwquality.conf file and set the value of minlen to 14, d-/u-/l-/o-credit to -1, and minclass to 4. 	dcredit = -1 The maximum credit for having uppercase characters in the new password. If less than 0 it is the minimum number of uppercase characters in the new password. ucredit = -1 The maximum credit for having lowercase characters in the new password. If less than 0 it is the minimum number of lowercase characters in the new password. lcredit = -1 The maximum credit for having other characters in the new password. If less than 0 it is the minimum number of other characters in the new password. If less than 0 it is the minimum number of other characters in the new password.
	CIS Benchmark Recommendation 5.4.1 Ensure password creation requirements are configured		orredit = -1 The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others). Results: zmedina@mainserver:~\$ grep 'minlen' /etc/security/pwquality.conf # minlen = 14 zmedina@mainserver:~\$ grep 'minclass' /etc/security/pwquality.conf # minclass = 4
	Lynis Scan Recommendation Enable auditd to collect audit information		Audit: zmedinadmainserver:"\$ dpkg-query -N -f='\$ibinary:Package\\\$iStatus\\t\$idb:Status-Status\\n' audito' audispd-plugins dpkg-query: no packages found matching audito' dpkg-query: no packages found matching audispd-plugins Remediation: zmedina@mainserver:"\$ sudo apt install audito audispd-plugins Reading package lists Done Building dependency tree Reading state information Done The following additional packages will be installed: libauparse0 libprelude28 prelude-utils The following NEW packages will be installed: audispd-plugins auditol libauparse0 libprelude28 prelude-utils
10	CIS Benchmark Recommendation 4.1.1.2 Ensure auditd is enabled	Enter command: sudo apt instal auditd audispd-plugins	O upgraded, 5 newly installed, 0 to remove and 0 not upgraded. Need to get 570 kB of archives. After this operation, 3,139 kB of additional disk space will be used. Results: Zmedina@mainserver:~\$ dpkg-query -W -f='\${binary:Pa audispd-plugins audispd-plugins install ok installed installed auditd install ok installed zmedina@mainserver:~\$ sudo systemctl is-enabled auditd enabled Zmedina@mainserver:~\$ sudo systemctl is-active auditd active

Lynis Scan Recommendation

! systemd-timesyncd did not synchronize the time recently. [TIME-3185]

- 1. Enter command: apt install chrony
- 2. Enter command: systemctl stop systemd-timesyncd.service
- 3. Enter command: systemctl --now mask systemd-timesyncd.service
- 4. Enter command: apt purge ntp

CIS Benchmark Recommendation

11

2.1.1 Ensure time synchronization is in use.

Audit:

```
File Actions Edit View Help
    File Actions Edit View Help

ontablabutuserver:/# {

output-" \ _tsd-" \ _sdtd-" \ _chrony-" \ _tntp-"

dpkg-query - w \ _chrony > /dev/null \ _251 \ _65 \ _chrony-"y"

dpkg-query - w \ _ntp > /dev/null \ _251 \ _65 \ _chrony-"y"

dpkg-query - w \ _ntp > /dev/null \ _251 \ _65 \ _chrony-"y"

| l \ _ntp-" \ _systemet\ _list-units - all \ _-types-service \ _grep - q \ _systemd'Btimesyncd.service \ _66 \ _system \
! i \ _s-mabled \ _systemd-!inesyncd.service \ _grep \ _q \ _enabled \ _65 \ _sstemt\ _s-mabled \ _systemd-timesyncd.service \ _grep - q \ _enabled \ _66 \ _sstemt\ _s-mabled \ _70 \ _10 \ _sstemt\ _10 \ _sstemt\ _70 \ _70 \ _60 \ _51 \ _ntp' \ _70 \ _70 \ _60 \ _51 \ _stdd \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 \ _70 
      satu
'$output\n- systemd-timesyncd is in use on the system"
                se 
"$\frac{1}{2} \chrony" = "y" 56 "$\frac{1}{2} \ntp" = "y" ]] 56 output="$output\n- both 
rony and atp are in use on the system" ]
"$\frac{1}{2} \chrony" = "y" 56 "$\frac{1}{2} \std" = "y" ]] 56 output="$output\n- both 
rony and systemd-timesyncd are in use on the system 
"$\frac{1}{2} \text{Clntp" "}" 56 "$\frac{1}{2} \text{Clntp" "}" 10 output="$output\n- both 
ntp 
d systemd-timesyncd are in use on the system 
"$\frac{1}{2} \text{Clntp" "}" 10 output="$output\n- both 
ntp 
d systemd-timesyncd are in use on the system "
      echo -e "\n- FAIL:\n$output\n"
echo -e "\n- FAIL:\n$output\n"
}
Command 'q' not found, but can be installed with:
snap install q
apt install python3-q-text-as-data # version 1.6.3-1, or
spe 'snap info q' for additional versions.
Eq: command not found
```

Remediation:

root@ubuntuserver:/# apt install chrony Reading package lists... Done Building dependency tree ... Done Reading state information... Done The following packages will be REMOVED: systemd-timesyncd The following NEW packages will be installed: chrony

Results:

```
Resulfs:

rotabuluntuserver:/# { output="\_tsd="\_sdtd="\_chrony="\_lntp-"; dpkg-query = \width{W} chrony=\width{W} chrony=\width{W}; dpkg-query = \width{W} chrony=\width{W}; dpkg-query = \width{W}; d
```

12	Lynis Scan Recommendation Configure minimum password age in /etc/login.defs [AUTH-9286] CIS Benchmark Recommendation 5.5.1.1 Ensure minimum days between password changes is configured.	 Enter command: sudo nano /etc/login.defs Change PASS_MIN_DAYS value from 0 to 1. Press: Ctrl + x Enter value: Y Press enter to save changes. 	Audit: root@ubuntuserver:/# rep PASS_MIN_DAYS /etc/login.defs # PASS_MIN_DAYS Minimum number of days allowed between password changes. PASS_MIN_DAYS 0 root@ubuntuserver:/# awk -F: '(/^{^:}+:[^!*]/ 56 \$4 < 1){print \$1 * * \$4}' /etc/shadow rseymore 0 Remediation: # PASS_MAX_DAYS Maximum number of days a password may be used. # PASS_MIN_DAYS Minimum number of days allowed between password changes. # PASS_MIN_DAYS Minimum number of days allowed between password expires. # PASS_MIN_DAYS 1 PASS_MAX_DAYS 99999 PASS_MIN_DAYS 1 PASS_MAN_AGE 7 Results: root@ubuntuserver:/# grep PASS_MIN_DAYS /etc/login.defs # PASS_MIN_DAYS 1 Minimum number of days allowed between password changes. Minimum number of days allowed between password changes.
13	Lynis Scan Recommendation Consider hardening SSH configuration [SSH-7408] Details: AllowTcpForwarding (set YES to NO) CIS Benchmark Recommendation 5.2.16 Ensure SSH AllowTcpForwarding is disabled	1. Enter the command: sudo nano /etc/ssh/sshd_config 2. Modify or add the line: "AllowTcpForwarding no"	Audit: Interchase Section Sec

Lynis Scan Recommendation If not required, consider explicit disabling of core dump in /etc/security/limits.co nf file [KRNL-5820] Audit: 1. Enter command: sudo nano /etc/security/limits.conf 2. Modify or add the line: " hard 2 "\$ sudo grep "fs.suid_dumpable" /etc/sysctl.conf /etc/sysctl.d/* ;"\$ sudo systemctl is-enabled coredump.service file state for coredump.service: No such file or directory core 0" 3. Enter command: sudo nano Remediation: /etc/sysctl.conf <type> <item> 4. Modify or add the line: "fs.suid_dumpable = 0" hard core 14 5. Enter command: sudo sysctl -w s.suid_dumpable = 0 fs.suid_dumpable=0 zmedina@mainserver:~\$ sudo sysctl –w fs.suid_dumpable=0 6. Enter command: sudo nano fs.suid_dumpable = 0 /etc/systemd/coredump.conf /etc/systemd/coredump.conf GNU nano 6.2 torage=none rocessSizeMax=0 7. Modify or add the line: **CIS Benchmark** "Storage=none" Recommendation Results: Modify or add the line: 1.5.4 Ensure core "ProcessSizeMax=0" s.conf:* hard core ~\$ sudo sysctl fs.suid_dumpable O ~\$ sudo grep "fs.suid_dumpable" /etc/sysctl.conf /etc/sysctl.d/* .suid_dumpable = O sctl.conf:fs.suid_dumpable = O dumps are restricted

Lynis Scan Recommendation To decrease the Audit: impact of a full /tmp zmedina@mainserver:~\$ sudo findmnt --kernel /tmp zmedina@mainserver:~\$ _ file system, place /tmp on a separate partition [FILE-6310] 1. Copy tmp.mount file to the /etc Remediation: directory with command: sudo /usr/share/systemd/tmp.mount /etc/systemd/system/ √hat=tmpfs Nhere=/tmp 2. Modify the tmp.mount file using ype=tmpfs ptions=mode=1777,strictatime,nosuid,nodev,noexec command: sudo nano /etc/systemd/system/tmp.mount 15 medina@mainserver:/\$ sudo systemctl daemon–reload 3. Edit the options at the bottom to zmedina@mainserver:/\$ equal: nument can be roll or, Treadestin, systemal, manage-unit-files Puthentication is required to manage system service or unit files. Authenticating as: Zoe (zmedina) 1777, strictatime, nosuid, nodev, n oexec **CIS Benchmark** Recommendation 4. Reload the service using command: sudo systemctl Results: 1.1.2.1 Ensure /tmp daemon-reload zmedina@mainserver:/\$ sudo findmnt ––kernel /tmp is a separate TARGET SOURCE FSTYPE OPTIONS partition. /tmp tmpfs tmpfs rw,nosuid,nodev,noexec,inode64 zmedina@mainserver:/\$ edina@mainserver:/\$ sudo systemctl is–enabled tmp.mount

Analysis of Data

To visualize the delta in hardening index value between the initial scan and the scan performed once all hardening configurations were applied, screenshots of each scan result for comparison are provided below.

The screenshot on the left shows the initial Hardening Index value of 63. The screenshot on the right shows the recalculated Hardening Index value of 67 from the second Lynis scan.

Discussion of Results

Based on results from running configurations detailed in the <u>Data</u> section, the system's security posture was generally improved. The increase of the Hardening Index Value demonstrates an immediate return on implementation of hardening configurations prescribed within the CIS Benchmark for Ubuntu 22.04.

Conclusion

While changes to the primary VM resulted in a positive increase to the Hardening Index value (62 to 67), the overall security posture of the system stands to benefit from additional hardening. In a scenario where the particular system under test is deployed in a Production environment, other factors must be considered that are external to the scope of this report. For this reason, the Lynis Hardening Index should not be accepted as the overall representation of a system's security posture. Instead, our results support our theory that taking steps to implement secure configurations on a system will result in stronger protections against threats. Using the Lynis scanner to identify vulnerabilities on a target test system, then cross-referencing results with recommendations from the applicable blueprint to make changes on that system directly resulted in a higher Hardening Index value.

Appendices

Initial Lynis Vulnerability Scan Results

[Lynis 3.0.9]	
Lynis comes with ABSOLUTELY NO WARRAN welcome to redistribute it under the terms of the See the LICENSE file for details about using this	e GNU General Public License.
2007-2021, CISOfy - https://cisofy.com/lynis/ Enterprise support available (compliance, plugir	ns, interface and tools)
[+] Initializing program	
- Detecting OS Checking profiles	[DONE]
Program version: 3.0.9 Operating system: Linux Operating system name: Ubuntu Operating system version: 22.04 Kernel version: 5.15.0 Hardware platform: x86_64 Hostname: cybr510-dbaba	
Profiles: /home/rbarber/lynis/default.p Log file: /var/log/lynis.log Report file: /var/log/lynis-report.dat Report version: 1.0 Plugin directory: ./plugins	orf
Auditor: [Not Specified] Language: en Test category: all Test group: all	
- Program update status	[NO UPDATE]
[+] System tools	
- Scanning available tools - Checking system binaries	
[+] Plugins (phase 1)	
Note: plugins have more extensive tests and ma	ay take several minutes to complete
- Plugin: pam [] - Plugin: systemd []	
[+] Boot and services	
- Service Manager - Checking UEFI boot - Checking presence GRUB2 - Checking for password protection	[systemd] [DISABLED] [FOUND] [NONE]

```
- Check running services (systemctl)
                                             [DONE]
         Result: found 24 running services
 - Check enabled services at boot (systemctl)
                                             [DONE]
         Result: found 50 enabled services
- Check startup files (permissions)
                                               [ OK ]
- Running 'systemd-analyze security'
         - ModemManager.service:
                                               [ MEDIUM ]
         - apport.service:
                                               [UNSAFE]
         - cloud-init-hotplugd.service:
                                              [UNSAFE]
                                               [UNSAFE]
         - cron.service:
         - dbus.service:
                                                UNSAFE 1
                                                UNSAFE ]
         dm-event.service:
         - dmesg.service:
                                               [UNSAFE]
         - emergency.service:
                                              [UNSAFE]
         getty@ttv1.service:
                                               [UNSAFE]
         - irqbalance.service:
                                               [ MEDIUM ]
         - iscsid.service:
                                               [UNSAFE]
         - lvm2-lvmpolld.service:
                                               [ UNSAFE ]
         - lxd-agent.service:
                                                UNSAFE ]
         - multipathd.service:
                                               [UNSAFE]
         - networkd-dispatcher.service:
                                             [UNSAFE]
         - open-vm-tools.service:
                                              [UNSAFE]
         - packagekit.service:
                                               UNSAFE]
                                              [UNSAFE]
         plymouth-start.service:
         - polkit.service:
                                               [UNSAFE]
         - rc-local.service:
                                                UNSAFE]
         - rescue.service:
                                                UNSAFE ]
         - rsyslog.service:
                                               [UNSAFE]
         - snap.lxd.daemon.service:
                                              [UNSAFE]
                                               UNSAFE 1
         - snap.lxd.user-daemon.service:
         - snapd.aa-prompt-listener.service:
                                              [UNSAFE]
         - snapd.service:
                                               UNSAFÉ 1
         - ssh.service:
                                               [UNSAFE]
                                                        [UNSAFE]
         - systemd-ask-password-console.service:
         - systemd-ask-password-plymouth.service:
                                                        [UNSAFE]
         - systemd-ask-password-wall.service: [ UNSAFE ]
         - systemd-fsckd.service:
                                             [UNSAFE]
         - systemd-initctl.service:
                                               [UNSAFĒ]
         systemd-journald.service:
                                              [PROTECTED]
         - systemd-logind.service:
                                             [PROTECTED]
         systemd-networkd.service:
                                             [PROTECTED]
         - systemd-resolved.service:
                                             [PROTECTED]
         systemd-rfkill.service:
                                               [UNSAFE]
         - systemd-timesyncd.service:
                                             [PROTECTED]
         systemd-udevd.service:
                                             [ MEDIUM ]
         - thermald.service:
                                               [UNSAFĒ]
                                             [ UNSAFE ]
         - ubuntu-advantage.service:
         - udisks2.service:
                                               [UNSAFE]
         - unattended-upgrades.service:
                                             [UNSAFE]
                                               [PROTECTED]
         - upower.service:
         - user@1000.service:
                                             [UNSAFE]
         - uuidd.service:
                                               [PROTECTED]
         - vgauth.service:
                                               [UNSAFE]
[+] Kernel
- Checking default run level
                                               [RUNLEVEL 5]
 - Checking CPU support (NX/PAE)
         CPU support: PAE and/or NoeXecute supported
                                                                 [FOUND]
 - Checking kernel version and release
                                              [DONE]
- Checking kernel type
                                               [DONE]
 - Checking loaded kernel modules
                                               [DONE]
         Found 73 active modules
 - Checking Linux kernel configuration file
                                               [FOUND]
                                                        NOT FOUND ]
- Checking default I/O kernel scheduler
 - Checking for available kernel update
                                               [OK]
 - Checking core dumps configuration
```

```
- configuration in systemd conf files
                                                         [DEFAULT]
         - configuration in /etc/profile
                                                         [DEFAULT]
                                                          DEFAULT ]
         - 'hard' configuration in /etc/security/limits.conf
         - 'soft' configuration in /etc/security/limits.conf
                                                         [ DEFAULT ]
         - Checking setuid core dumps configuration
                                                        [PROTECTED]
 - Check if reboot is needed
                                               [YES]
[+] Memory and Processes
                                               [FOUND]
 - Checking /proc/meminfo
 - Searching for dead/zombie processes
                                              [ NOT FOUND ]
 - Searching for IO waiting processes
                                             [ NOT FOUND ]
 - Search prelink tooling
                                               [NOT FOUND]
[+] Users, Groups and Authentication
 - Administrator accounts
                                               [ OK ]
                                                OK 1
- Unique UIDs
 - Consistency of group files (grpck)
                                                OK į
 - Unique group IDs
                                                OK ]
 - Unique group names
                                                OKI
- Password file consistency
                                                OK]
- Password hashing methods
                                                SUGGESTION 1
- Checking password hashing rounds
                                             [DISABLED]
 - Query system users (non daemons)
                                              [DONE]
- NIS+ authentication support
                                                [ NOT ENABLED ]
 - NIS authentication support
                                                NOT ENABLED ]
- Sudoers file(s)
                                               FOUND
         - Permissions for directory: /etc/sudoers.d
                                                         [ WARNING ]
         - Permissions for: /etc/sudoers
                                                         [OK]
                                                        [OK]
         - Permissions for: /etc/sudoers.d/README
- PAM password strength tools
                                               [ SUGGESTION ]
                                                [FOUND]
- PAM configuration files (pam.conf)
- PAM configuration files (pam.d)
                                                FOUND 1
 - PAM modules
                                                FOUND ]
- LDAP module in PAM
                                                NOT FOUND 1
- Accounts without expire date
                                                [SUGGESTION]
                                                ίοκ]
- Accounts without password
- Locked accounts
                                               [ OK ]
- Checking user password aging (minimum)
                                                         [DISABLED]
- User password aging (maximum)
                                                         [DISABLED]
 - Checking expired passwords
                                               [OK]
 - Checking Linux single user mode authentication
                                                         [ OK ]
 - Determining default umask
                                               [NOT FOUND]
         - umask (/etc/profile)
         - umask (/etc/login.defs)
                                              SUGGESTION
 - LDAP authentication support
                                               [ NOT ENABLED ]
- Logging failed login attempts
                                               [ENABLED]
[+] Shells
- Checking shells from /etc/shells
         Result: found 10 shells (valid shells: 10).
         - Session timeout settings/tools
                                                         [ NONE ]
 - Checking default umask values
         - Checking default umask in /etc/bash.bashrc
                                                        [NONE]
         - Checking default umask in /etc/profile
                                                         [NONE]
[+] File systems
- Checking mount points
                                                         [SUGGESTION]
         - Checking /home mount point
                                                         [ SUGGESTION I
         - Checking /tmp mount point
         - Checking /var mount point
                                                          SUGGESTION ]
 - Checking LVM volume groups
                                               [FOUND ]
         - Checking LVM volumes
                                                [FOUND]
 - Query swap partitions (fstab)
                                               [OK]
```

```
- Testing swap partitions
 - Testing /proc mount (hidepid)
                                                SUGGESTION ]
                                                OK]
 - Checking for old files in /tmp
 - Checking /tmp sticky bit
                                                OK]
 - Checking /var/tmp sticky bit
                                                OK 1
 - ACL support root file system
                                               [ENABLED]
 - Mount options of /
                                                OK]
 - Mount options of /boot
                                                DEFAULT ]
                                               PARTIALLÝ HARDENED )
 - Mount options of /dev
 - Mount options of /dev/shm
                                               [ PARTIALLY HARDENED ]
 - Mount options of /run
                                               [HARDENED]
 - Total without nodev:7 noexec:13 nosuid:10 ro or noexec (W^X): 8 of total 30
 - Disable kernel support of some filesystems
[+] USB Devices
 - Checking usb-storage driver (modprobe config)
                                                         [NOT DISABLED]
 - Checking USB devices authorization
                                                         [DISABLED]
                                               [NOT FOUND]
 - Checking USBGuard
[+] Storage
                                                        [DISABLED]
 - Checking firewire ohci driver (modprobe config)
[+] NFS
 - Check running NFS daemon
                                               [ NOT FOUND ]
[+] Name services
 - Checking search domains
                                               [FOUND]
 - Checking /etc/resolv.conf options
                                               [ FOUND ]
 - Searching DNS domain name
                                               [UNKNOWN]
 - Checking /etc/hosts
         - Duplicate entries in hosts file
                                                         [NONE]
         - Presence of configured hostname in /etc/hosts [FOUND]
         - Hostname mapped to localhost
                                                        [ NOT FOUND ]
         - Localhost mapping to IP address
                                                         [OK]
[+] Ports and packages
 - Searching package managers
                                                        [FOUND]

    Searching dpkg package manager

         - Querying package manager
         - Query unpurged packages
                                                         [NONE]
 - Checking security repository in sources.list file
                                                         [OK]
                                               [OK]
 - Checking APT package database
 - Checking vulnerable packages
                                               [ OK ]
                                              [SKIPPED]
 - Checking upgradeable packages
                                               [INSTALLÉD]
 - Checking package audit tool
         Found: apt-check
 - Toolkit for automatic upgrades (unattended-upgrade)
                                                        [FOUND]
[+] Networking
 - Checking IPv6 configuration
                                               [ENABLED]
         Configuration method
                                                        [AUTO]
         IPv6 only
                                               [ NO ]
 - Checking configured nameservers

    Testing nameservers

         Nameserver: 127.0.0.53
                                                        [OK]
         - DNSSEC supported (systemd-resolved)
                                                                  [ NO ]
 - Getting listening ports (TCP/UDP)
                                               [DONE]
 - Checking promiscuous interfaces
                                              [OK]
 - Checking status DHCP client
                                               [ NOT ACTIVE ]
 - Checking for ARP monitoring software
                                              [NOT FOUND]
 - Uncommon network protocols
                                              [0]
```

```
[+] Printers and Spools
                                             [NOT FOUND]
 - Checking cups daemon
                                             [ NOT RUNNING ]
 - Checking Ip daemon
[+] Software: e-mail and messaging
[+] Software: firewalls
                                             [FOUND]
- Checking iptables kernel module
         - Checking iptables policies of chains
                                            [FOUND]
                                            [WARNING]
         - Checking for empty ruleset
         - Checking for unused rules
                                            [OK]
                                             [ACTIVE]
 - Checking host based firewall
[+] Software: webserver
                                             [NOT FOUND]
- Checking Apache
                                             [ NOT FOUND ]
 - Checking nginx
[+] SSH Support
- Checking running SSH daemon
                                                       [FOUND]
                                                       [ FOUND ]
         - Searching SSH configuration
         - OpenSSH option: AllowTcpForwarding
                                                      [SUGGESTION]
         - OpenSSH option: ClientAliveCountMax
                                                       [SUGGESTION]
         - OpenSSH option: ClientAliveInterval
                                                       [OK]
         - OpenSSH option: FingerprintHash
                                                       OK]
         - OpenSSH option: GatewayPorts
                                                        OK]
         - OpenSSH option: IgnoreRhosts
                                                       OK j

    OpenSSH option: LoginGraceTime

                                                        SUGGESTION ]
         - OpenSSH option: LogLevel

    OpenSSH option: MaxAuthTries

                                                        SUGGESTION
         - OpenSSH option: MaxSessions
                                                       SUGGESTION ]
         - OpenSSH option: PermitRootLogin
                                                       OK]
         - OpenSSH option: PermitUserEnvironment
                                                       [ OK ]

    OpenSSH option: PermitTunnel

                                                       [OK]
         - OpenSSH option: Port
                                                        SUGGESTION ]
         - OpenSSH option: PrintLastLog
                                                        OK]
         - OpenSSH option: StrictModes
                                                        OK ]
                                                        SUGGESTION ]

    OpenSSH option: TCPKeepAlive

         - OpenSSH option: UseDNS
                                                        OK]

    OpenSSH option: X11Forwarding

                                                       [SUGGESTION]
         - OpenSSH option: AllowAgentForwarding
                                                     [SUGGESTION]
                                                       [ NOT FOUND ]

    OpenSSH option: AllowUsers

         - OpenSSH option: AllowGroups
                                                       [NOT FOUND]
[+] SNMP Support
                                                      [NOT FOUND]
- Checking running SNMP daemon
[+] Databases
         No database engines found
[+] LDAP Services
- Checking OpenLDAP instance
                                             [NOT FOUND]
[+] PHP
- Checking PHP
                                             [NOT FOUND]
[+] Squid Support
```

- Checking running Squid daemon	[NOT FOUND]
[+] Logging and files	
- Checking for a running log daemon - Checking Syslog-NG status - Checking systemd journal status - Checking Metalog status - Checking RSyslog status - Checking RFC 3195 daemon status - Checking minilogd instances - Checking logrotate presence - Checking remote logging - Checking log directories (static list) - Checking open log files - Checking deleted files in use	[OK] [NOT FOUND] [FOUND] [NOT FOUND] [NOT FOUND] [NOT FOUND] [NOT FOUND] [OK] [NOT ENABLED] [DONE] [DONE]
[+] Insecure services	
- Installed inetd package - Installed xinetd package - xinetd status - Installed rsh client package - Installed rsh server package - Installed telnet client package - Installed telnet server package - Installed telnet server package - Checking NIS client installation - Checking TFTP client installation - Checking TFTP server installation	[NOT FOUND] [OK] [NOT ACTIVE] [OK] [OK] [OK] [OK] [NOT FOUND] [OK] [OK] [OK]
[+] Banners and identification	
- /etc/issue [FOUNI - /etc/issue contents - /etc/issue.net - /etc/issue.net contents	D] [WEAK] [FOUND] [WEAK]
[+] Scheduled tasks	
- Checking crontab and cronjob files	[DONE]
[+] Accounting	
- Checking accounting information - Checking sysstat accounting data - Checking auditd	[NOT FOUND] [NOT FOUND] [NOT FOUND]
[+] Time and Synchronization	
- NTP daemon found: systemd (timesyncd) - Checking for a running NTP daemon or client - Last time synchronization	[FOUND] [OK] [2819s]
[+] Cryptography	
- Checking for expired SSL certificates [0/141]	[NONE]
[WARNING]: Test CRYP-7902 had a long execu	tion: 11.979649 seconds
 Found 0 encrypted and 1 unencrypted swap do Kernel entropy is sufficient HW RNG & rngd SW prng MOR variable not found 	evices in use. [OK] [YES] [NO] [NO] [WEAK]
[+] Virtualization	

```
[+] Containers
[+] Security frameworks
 - Checking presence AppArmor
                                                [FOUND]
                                                [ENABLED]
          - Checking AppArmor status
          Found 39 unconfined processes
 - Checking presence SELinux
                                                 [NOT FOUND]
                                                 [ NOT FOUND ]
 - Checking presence TOMOYO Linux
 - Checking presence grsecurity
                                                 [NOT FOUND]
 - Checking for implemented MAC framework
                                                [OK]
[+] Software: file integrity
 - Checking file integrity tools
                                                 [DISABLED]
 - dm-integrity (status)
 - dm-verity (status)
                                                 [DISABLED]
                                                 [ NOT FOUND ]
 - Checking presence integrity tool
[+] Software: System tooling
 - Checking automation tooling
 - Automation tooling
                                                 [NOT FOUND]
 - Checking for IDS/IPS tooling
                                                 [ NONE ]
[+] Software: Malware
 - Malware software components
                                               [NOT FOUND]
[+] File Permissions
 - Starting file permissions check
          File: /boot/grub/grub.cfg
                                                 [SUGGESTION]
          File: /etc/crontab
                                                 [SUGGESTION]
          File: /etc/group
                                                 [OK]
          File: /etc/group-
                                                 [OK]
          File: /etc/hosts.allow
                                                [OK]
          File: /etc/hosts.deny
                                                [OK]
          File: /etc/issue
                                                 [ OK ]
          File: /etc/issue.net
                                                  [ OK ]
          File: /etc/passwd
                                                [OK]
          File: /etc/passwd-
                                                [OK]
          File: /etc/ssh/sshd config
                                                 SUGGESTION ]
          Directory: /root/.ssh
                                                 [ OK ]
          Directory: /etc/cron.d
                                                [ SUGGESTION ]
          Directory: /etc/cron.daily
                                                 SUGGESTION ]
          Directory: /etc/cron.hourly
                                                SUGGESTION
          Directory: /etc/cron.weekly
                                                [SUGGESTION]
          Directory: /etc/cron.monthly
                                                [SUGGESTION]
[+] Home directories
 - Permissions of home directories
                                                 [OK]
 - Ownership of home directories
                                                 [OK]
 - Checking shell history files
                                                 [ OK ]
[+] Kernel Hardening
 - Comparing sysctl key pairs with scan profile
                                                           [DIFFERENT]
          - dev.tty.ldisc_autoload (exp: 0)
          - fs.protected_fifos (exp: 2)
                                                           [ DIFFERENT ]
          - fs.protected_hardlinks (exp: 1)
                                                            OK]
         - fs.protected_regular (exp: 2)
- fs.protected_symlinks (exp: 1)
                                                           [ OK ]
                                                           [OK]
```

```
[DIFFERENT]
         - fs.suid_dumpable (exp: 0)
         - kernel.core_uses_pid (exp: 1)
                                                          [OK]
                                                          OK]
         - kernel.ctrl-alt-del (exp: 0)
         - kernel.dmesg_restrict (exp: 1)
                                                          OK]
         kernel.kptr restrict (exp: 2)
                                                          [ DIFFERENT 1
         - kernel.modules_disabled (exp: 1)
                                                          [ DIFFERENT ]
         - kernel.perf_event_paranoid (exp: 3)
                                                          DIFFERENT ]
         - kernel.randomize_va_space (exp: 2)
                                                          OK ]
                                                          DIFFERENT ]
         kernel.sysrg (exp: 0)
         - kernel.unprivileged_bpf_disabled (exp: 1)
                                                          DIFFERENT ]
         - kernel.yama.ptrace_scope (exp: 1 2 3)
                                                           OK 1
         - net.core.bpf_jit_harden (exp: 2)
                                                          DIFFERENT ]
         - net.ipv4.conf.all.accept redirects (exp: 0)
                                                         [DIFFERENT]
         - 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)
                                                          DIFFERENT ]
         - net.ipv4.conf.all.mc_forwarding (exp: 0)
                                                          OK]
         - net.ipv4.conf.all.proxy_arp (exp: 0)
                                                          OK ]
                                                          DIFFERENT ]
         net.ipv4.conf.all.rp_filter (exp: 1)
         - net.ipv4.conf.all.send redirects (exp: 0)
                                                          [DIFFERENT]
         - net.ipv4.conf.default.accept_redirects (exp: 0) [ DIFFERENT ]
         - net.ipv4.conf.default.accept_source_route (exp: 0)
                                                                   [OK]
         net.ipv4.conf.default.log_martians (exp: 1)
                                                         [DIFFERENT]
         - net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)
                                                                   [OK]
         - net.ipv4.icmp_ignore_bogus_error_responses (exp: 1)
                                                                   [OK]
         - net.ipv4.tcp syncookies (exp: 1)
         - net.ipv4.tcp_timestamps (exp: 0 1)
                                                         ίοκί
         net.ipv6.conf.all.accept_redirects (exp: 0)
                                                          [DIFFERENT]
         - net.ipv6.conf.all.accept_source_route (exp: 0)
                                                          OK 1
         - net.ipv6.conf.default.accept_redirects (exp: 0)
                                                         [DIFFERENT]
         - net.ipv6.conf.default.accept_source_route (exp: 0)
                                                                   [ OK ]
[+] Hardening
                                                         [FOUND]

    Installed compiler(s)

         - Installed malware scanner
                                                         [ NOT FOUND ]
         - Non-native binary formats
                                                         [FOUND]
[+] Custom tests
 - Running custom tests...
                                                [NONE]
[+] Plugins (phase 2)
 - Plugins (phase 2)
                                                [DONE]
______
 -[ Lynis 3.0.9 Results ]-
 Warnings (3):
 ! Reboot of system is most likely needed [KRNL-5830]
         - Solution : reboot
         https://cisofy.com/lynis/controls/KRNL-5830/
 ! iptables module(s) loaded, but no rules active [FIRE-4512]
         https://cisofy.com/lynis/controls/FIRE-4512/
 ! systemd-timesyncd did not synchronize the time recently. [TIME-3185]
         https://cisofy.com/lynis/controls/TIME-3185/
 Suggestions (42):
 * Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
         https://cisofy.com/lynis/controls/BOOT-5122/
```

- * Consider hardening system services [BOOT-5264]
 - Details: Run '/usr/bin/systemd-analyze security SERVICE' for each service https://cisofy.com/lynis/controls/BOOT-5264/
- * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820] https://cisofy.com/lynis/controls/KRNL-5820/
- * Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229] https://cisofy.com/lynis/controls/AUTH-9229/
- * Configure password hashing rounds in /etc/login.defs [AUTH-9230] https://cisofy.com/lynis/controls/AUTH-9230/
- * Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262] https://cisofy.com/lynis/controls/AUTH-9262/
- * When possible set expire dates for all password protected accounts [AUTH-9282] https://cisofy.com/lynis/controls/AUTH-9282/
- * Configure minimum password age in /etc/login.defs [AUTH-9286] https://cisofy.com/lynis/controls/AUTH-9286/
- * Configure maximum password age in /etc/login.defs [AUTH-9286] https://cisofy.com/lynis/controls/AUTH-9286/
- * Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328] https://cisofy.com/lynis/controls/AUTH-9328/
- * To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310] https://cisofy.com/lynis/controls/FILE-6310/
- * To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310] https://cisofy.com/lynis/controls/FILE-6310/
- * To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310] https://cisofy.com/lynis/controls/FILE-6310/
- * Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000] https://cisofy.com/lynis/controls/USB-1000/
- * Check DNS configuration for the dns domain name [NAME-4028] https://cisofy.com/lynis/controls/NAME-4028/
- * Install debsums utility for the verification of packages with known good database. [PKGS-7370] https://cisofy.com/lynis/controls/PKGS-7370/
- * Install package apt-show-versions for patch management purposes [PKGS-7394] https://cisofy.com/lynis/controls/PKGS-7394/
- * Determine if protocol 'dccp' is really needed on this system [NETW-3200] https://cisofy.com/lynis/controls/NETW-3200/
- * Determine if protocol 'sctp' is really needed on this system [NETW-3200] https://cisofy.com/lynis/controls/NETW-3200/
- * Determine if protocol 'rds' is really needed on this system [NETW-3200] https://cisofy.com/lynis/controls/NETW-3200/
- * Determine if protocol 'tipc' is really needed on this system [NETW-3200] https://cisofy.com/lynis/controls/NETW-3200/
- * Consider hardening SSH configuration [SSH-7408]
 Details: AllowTcpForwarding (set YES to NO)
 https://cisofy.com/lynis/controls/SSH-7408/
- * Consider hardening SSH configuration [SSH-7408]

- Details : ClientAliveCountMax (set 3 to 2) https://cisofy.com/lynis/controls/SSH-7408/

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

* Consider hardening SSH configuration [SSH-7408]
- Details: MaxAuthTries (set 6 to 3)
https://cisofy.com/lynis/controls/SSH-7408/

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

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

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

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

* Consider hardening SSH configuration [SSH-7408]
- Details: AllowAgentForwarding (set YES to NO)
https://cisofy.com/lynis/controls/SSH-7408/

- * Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154] https://cisofy.com/lynis/controls/LOGG-2154/
- * Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126] https://cisofy.com/lynis/controls/BANN-7126/
- * Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130] https://cisofy.com/lynis/controls/BANN-7130/
- * Enable process accounting [ACCT-9622] https://cisofy.com/lynis/controls/ACCT-9622/
- * Enable sysstat to collect accounting (no results) [ACCT-9626] https://cisofy.com/lynis/controls/ACCT-9626/
- * Enable auditd to collect audit information [ACCT-9628] https://cisofy.com/lynis/controls/ACCT-9628/
- * Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350] https://cisofy.com/lynis/controls/FINT-4350/
- * Determine if automation tools are present for system management [TOOL-5002] https://cisofy.com/lynis/controls/TOOL-5002/
- * Consider restricting file permissions [FILE-7524]
 Details : See screen output or log file
 - Solution: Use chmod to change file permissions https://cisofy.com/lynis/controls/FILE-7524/
- * 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/lynis/controls/KRNL-6000/
- * Harden compilers like restricting access to root user only [HRDN-7222] https://cisofy.com/lynis/controls/HRDN-7222/

* 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, Wazuh https://cisofy.com/lynis/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) - Useupload to upload data to central system (Lynis Enterprise users)					
Lynis security scan details:					
Hardening index: 63 [##########] Tests performed: 268 Plugins enabled: 2					
Components: - Firewall [V] - Malware scanner [X]					
Scan mode: Normal [V] Forensics [] Integration [] Pentest []					
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					
Lynis 3.0.9					
Auditing, system hardening, and compliance for UNIX-based systems (Linux, macOS, BSD, and others)					
2007-2021, CISOfy - https://cisofy.com/lynis/ Enterprise support available (compliance, plugins, interface and tools)					

Post-Hardening Lynis Vulnerability Scan Results

```
[Lynis 3.0.9]
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
 welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.
 2007-2021, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
[+] Initializing program
- Detecting OS...
                                           [DONE]
- Checking profiles...
                                           [DONE]
 Program version:
                          3.0.9
 Operating system:
                          Linux
 Operating system name:
                          Ubuntu
 Operating system version: 22.04
 Kernel version:
                          5.15.0
 Hardware platform:
                          x86 64
                          cybr510-dbaba
 Hostname:
 Profiles:
                 /home/rbarber/lynis/default.prf
                 /var/log/lynis.log
 Log file:
 Report file:
                 /var/log/lynis-report.dat
 Report version:
                          1.0
 Plugin directory:
                          ./plugins
 Auditor:
                 [Not Specified]
 Language:
                          en
 Test category:
                          all
 Test group:
 - Program update status...
                                           [ NO UPDATE ]
[+] System tools
- Scanning available tools...
- Checking system binaries...
[+] Plugins (phase 1)
Note: plugins have more extensive tests and may take several minutes to complete
 - Plugin: pam
        [..]
 - Plugin: systemd
        [.....]
[+] Boot and services
- Service Manager
                                           [systemd]
 - Checking UEFI boot
                                           [DISABLED]
 - Checking presence GRUB2
                                           [FOUND]
        - Checking for password protection
                                                    [OK]
 - Check running services (systemctl)
                                           [DONE]
        Result: found 24 running services
 - Check enabled services at boot (systemctl)
                                                    [DONE]
        Result: found 52 enabled services
 - Check startup files (permissions)
                                           [OK]
```

```
- Running 'systemd-analyze security'
         - ModemManager.service:
                                                        [ MEDIUM ]
                                               [UNSAFE]
         - apport.service:
         - auditd.service:
                                               [EXPOSED]
         - chrony.service:
                                               PROTECTÉD 1
                                                        [UNSAFE]
         - cloud-init-hotplugd.service:
                                               [UNSAFE]
         - cron.service:
                                               [UNSAFE]
         - dbus.service:
                                               Î UNSAFE Î
         - dm-event.service:
                                               [UNSAFE]
         - dmesg.service:
         - emergency.service:
                                                UNSAFE 1
         - getty@tty1.service:
                                                UNSAFE]
         - irgbalance.service:
                                               MEDIUM 1
         - iscsid.service:
                                               [UNSAFE]
         - lvm2-lvmpolld.service:
                                                UNSAFE 1
         - lxd-agent.service:
                                               [UNSAFE]
         - multipathd.service:
                                               [UNSAFE]
         - networkd-dispatcher.service:
                                                         [UNSAFE]
         - open-vm-tools.service:
                                               [UNSAFE]
                                               [UNSAFE]
         - plymouth-start.service:
         - polkit.service:
                                               [UNSAFE]
         - postfix@-.service:
                                                UNSAFE]
         - rc-local.service:
                                               [UNSAFE]
                                               [UNSAFE]
         - rescue.service:
         - rsyslog.service:
                                               [UNSAFE]
                                                         [UNSAFE]
         - snap.lxd.daemon.service:
         - snap.lxd.user-daemon.service:
                                                         [UNSAFE]
         - snapd.aa-prompt-listener.service:
                                                         [UNSAFE]
         - snapd.service:
                                               [UNSAFE]
                                               [UNSAFE]
         - ssh.service:
         - systemd-ask-password-console.service:
                                                         [UNSAFE]
         - systemd-ask-password-plymouth.service:
                                                         [ UNSAFE ]
         - systemd-ask-password-wall.service:
                                                        [UNSAFE]
         - systemd-fsckd.service:
                                               [UNSAFE]
         - systemd-initctl.service:
                                               [UNSAFE]
         - systemd-journald.service:
                                                         [PROTECTED]
                                               [PROTECTED]
         - systemd-logind.service:
                                                        [ PROTECTED 1
         - systemd-networkd.service:
         - systemd-resolved.service:
                                                         [PROTECTED]
         - systemd-rfkill.service:
                                               [UNSAFE]
         - systemd-udevd.service:
                                                        [MEDIUM]
         - thermald.service:
                                               [UNSAFE]
                                                        [UNSAFE]
         - ubuntu-advantage service:
         - udisks2.service:
                                               [UNSAFE]
                                                        [UNSAFE]
         - unattended-upgrades.service:
         - user@1000.service:
                                               [UNSAFE]
         - uuidd.service:
                                               [PROTECTED]
         - vgauth.service:
                                               [UNSAFE]
[+] Kernel
- Checking default run level
                                               [RUNLEVEL 5]
- Checking CPU support (NX/PAE)
         CPU support: PAE and/or NoeXecute supported
                                                                  [FOUND]
                                                        [DONE]
 - Checking kernel version and release
 - Checking kernel type
                                               [DONE]
- Checking loaded kernel modules
                                               [DONE]
         Found 67 active modules
 - Checking Linux kernel configuration file
                                               [FOUND]
 - Checking default I/O kernel scheduler
                                                        [ NOT FOUND ]
- Checking for available kernel update
                                               [OK]
 - Checking core dumps configuration
                                                        [DISABLED]
         - configuration in systemd conf files
         - configuration in /etc/profile
                                                         [ DEFAULT ]
         - 'hard' configuration in /etc/security/limits.conf
                                                         DISABLED 1
         - 'soft' config in /etc/security/limits.conf (implicit) [ DISABLED ]
         - Checking setuid core dumps configuration
                                                                  [PROTECTED]
 - Check if reboot is needed
```

```
[+] Memory and Processes
- Checking /proc/meminfo
                                               [FOUND]
                                                         NOT FOUND ]
- Searching for dead/zombie processes
- Searching for IO waiting processes
                                               I NOT FOUND 1
- Search prelink tooling
                                               [ NOT FOUND ]
[+] Users, Groups and Authentication
- Administrator accounts
                                               [OK]
- Unique UIDs
                                               [ OK ]
                                               [ OK ]
- Consistency of group files (grpck)
                                               įοκί
- Unique group IDs
- Unique group names
                                               [OK]
- Password file consistency
                                                OK 1
- Password hashing methods
                                               [SUGGESTION]
                                                         [DISABLED]
- Checking password hashing rounds
- Query system users (non daemons)
                                                         [DONE]
- NIS+ authentication support
                                               [ NOT ENABLED ]
                                               [ NOT ENABLED ]
- NIS authentication support
- Sudoers file(s)
                                               [FOUND]
                                                         [ WARNING ]
         - Permissions for directory: /etc/sudoers.d
         - Permissions for: /etc/sudoers
                                                         [OK]
         - Permissions for: /etc/sudoers.d/README
                                                                  [OK]
- PAM password strength tools
                                               [ OK ]
- PAM configuration files (pam.conf)
                                               [ FOUND ]
- PAM configuration files (pam.d)
                                               [FOUND]
                                               [FOUND]
- PAM modules
- LDAP module in PAM
                                               [ NOT FOUND ]
- Accounts without expire date
                                                SUGGESTION ]
- Accounts without password
                                               [OK]
- Locked accounts
                                               įοκί
                                               [CONFIGURED]
- User password aging (minimum)
- User password aging (maximum)
                                                         [CONFIGURED]
- Checking expired passwords
                                               [OK]
- Checking Linux single user mode authentication
                                                         [OK]
- Determining default umask
         - umask (/etc/profile)
                                               [ NOT FOUND ]

    umask (/etc/login.defs)

                                                         [OK]
                                               [ NOT ENABLED ]
- LDAP authentication support
- Logging failed login attempts
                                               [ENABLED]
[+] Shells
- Checking shells from /etc/shells
         Result: found 10 shells (valid shells: 10).
         - Session timeout settings/tools
                                                         [NONE]
- Checking default umask values
         - Checking default umask in /etc/bash.bashrc
                                                                  [NONE]
         - Checking default umask in /etc/profile
                                                         [NONE]
[+] File systems
- Checking mount points
         - Checking /home mount point
                                                         [ SUGGESTION ]
         - Checking /tmp mount point
                                                         [OK]
         - Checking /var mount point
                                                         [SUGGESTION]
 - Checking LVM volume groups
                                               [FOUND]
         - Checking LVM volumes
                                                         [FOUND]
 - Query swap partitions (fstab)
                                               [OK]
                                               iok]
- Testing swap partitions
                                               [SUGGESTION]
- Testing /proc mount (hidepid)
- Checking for old files in /tmp
                                               [OK]
- Checking /tmp sticky bit
                                               [ OK ]
- Checking /var/tmp sticky bit
                                                [OK]
- ACL support root file system
                                               [ENABLED]
- Mount options of /
                                               [ OK ]
 - Mount options of /boot
                                               [ DEFAULT ]
 - Mount options of /dev
                                               [ PARTIALLÝ HARDENED ]
```

```
[ PARTIALLY HARDENED ]
 - Mount options of /dev/shm
 - Mount options of /run
                                              [HARDENED]
                                              [HARDENED]

    Mount options of /tmp

 - Total without nodev:7 noexec:13 nosuid:10 ro or noexec (W^X): 8 of total 31
- Disable kernel support of some filesystems
[+] USB Devices
- Checking usb-storage driver (modprobe config)
                                                        [DISABLED]
 - Checking USB devices authorization
                                                        [DISABLED]
 - Checking USBGuard
                                              [NOT FOUND]
[+] Storage
- Checking firewire ohci driver (modprobe config)
                                                        [DISABLED]
[+] NFS
                                              [NOT FOUND]
- Check running NFS daemon
[+] Name services
                                              [FOUND]
- Checking search domains
                                              [FOUND]
 - Checking /etc/resolv.conf options
 - Searching DNS domain name
                                              [UNKNOWN]
 - Checking /etc/hosts
         - Duplicate entries in hosts file
                                                                 [FOUND]
         - Presence of configured hostname in /etc/hosts
                                                        [NOT FOUND]
         - Hostname mapped to localhost
                                                        [OK]
         - Localhost mapping to IP address
[+] Ports and packages
- Searching package managers
         - Searching dpkg package manager
                                                        [FOUND]
         - Querying package manager
         - Query unpurged packages
                                                        [FOUND]
 - Checking security repository in sources.list file
                                                        [OK]
- Checking APT package database
                                                        [OK]
 - Checking vulnerable packages
                                              [WARNING]
                                                        [SKIPPED]
 - Checking upgradeable packages
- Checking package audit tool
                                              [INSTALLED]
         Found: apt-get
 - Toolkit for automatic upgrades (unattended-upgrade)
                                                        [FOUND]
[+] Networking
- Checking IPv6 configuration
                                              [ENABLED]
                                                        [ AUTO ]
         Configuration method
         IPv6 only
                                              [ NO ]
 - Checking configured nameservers
         - Testing nameservers
         Nameserver: 127.0.0.53
                                                        [OK]
         - DNSSEC supported (systemd-resolved)
                                                                 [ NO ]
                                              [DONE]

    Getting listening ports (TCP/UDP)

 - Checking promiscuous interfaces
                                              [OK]
                                              [NOT ACTIVE]
 - Checking status DHCP client
                                                       [NOT FOUND]
 - Checking for ARP monitoring software
- Uncommon network protocols
                                              [0]
[+] Printers and Spools
                                               [ NOT FOUND ]
- Checking cups daemon
- Checking Ip daemon
                                              [ NOT RUNNING ]
[+] Software: e-mail and messaging
                                              [RUNNING]
 - Postfix status
         - Postfix configuration
                                                        [FOUND]
```

- Postfix banner	[WARNING]
[+] Software: firewalls	-
	[FOUND] [FOUND] [WARNING] [OK] [ACTIVE]
	[NOT FOUND]
- Checking nginx	[NOT FOUND]
[+] SSH Support	
- Checking running SSH daemon - Searching SSH configuration - OpenSSH option: AllowTcpForwardin - OpenSSH option: ClientAliveCountMatery openSSH option: ClientAliveInterval - OpenSSH option: ClientAliveInterval - OpenSSH option: FingerprintHash - OpenSSH option: IgnoreRhosts - OpenSSH option: LoginGraceTime - OpenSSH option: LoginGraceTime - OpenSSH option: MaxAuthTries - OpenSSH option: PermitRootLogin - OpenSSH option: PermitRootLogin - OpenSSH option: PermitTunnel - OpenSSH option: PermitTunnel - OpenSSH option: PrintLastLog - OpenSSH option: StrictModes - OpenSSH option: TCPKeepAlive - OpenSSH option: UseDNS - OpenSSH option: AllowAgentForward - OpenSSH option: AllowAgentForward - OpenSSH option: AllowUsers - OpenSSH option: AllowGroups	[SUĞGESTION] [OK] [OK] [OK] [OK] [OK] [SUGGESTION] [SUGGESTION] [SUGGESTION] [OK] ment [OK] [OK] [OK] [OK] [OK] [SUGGESTION] [OK] [OK] [SUGGESTION] [OK] [OK] [SUGGESTION] [OK] [SUGGESTION] [OK] [SUGGESTION] [OK] [SUGGESTION]
[+] SNMP Support	
- Checking running SNMP daemon	[NOT FOUND]
[+] Databases	
No database engines found	
[+] LDAP Services	
- Checking OpenLDAP instance [+] PHP	[NOT FOUND]
	[NOT FOUND]
[+] Squid Support	[HOLL GOND]
	[NOT FOUND]
[+] Logging and files	
- Checking for a running log daemon - Checking Syslog-NG status - Checking systemd journal status - Checking Metalog status - Checking RSyslog status	[OK] [NOT FOUND] [FOUND] [NOT FOUND] [FOUND]

- Checking RFC 3195 daemon status - Checking minilogd instances - Checking logrotate presence - Checking remote logging - Checking log directories (static list) - Checking open log files - Checking deleted files in use	[NOT FOUND] [NOT FOUND] [OK] [NOT ENABLED] [DONE] [DONE] [DONE]
[+] Insecure services	
- Installed inetd package - Installed xinetd package - xinetd status - Installed rsh client package - Installed rsh server package - Installed telnet client package - Installed telnet server package - Installed telnet server package - Checking NIS client installation - Checking TFTP client installation - Checking TFTP server installation	[NOT FOUND] [OK] [NOT ACTIVE] [OK] [OK] [OK] [OK] [OK] [NOT FOUND] [OK] [OK] [OK]
[+] Banners and identification	
- /etc/issue [FOUNE - /etc/issue contents	D] [WEAK]
- /etc/issue.net - /etc/issue.net contents	[FOUND] [WEAK]
[+] Scheduled tasks	
- Checking crontab and cronjob files	[DONE]
[+] Accounting	
	[NOT FOUND] [NOT FOUND] [ENABLED] [SUGGESTION] [OK] [FOUND]
[+] Time and Synchronization	
	[FOUND] [OK]
[+] Cryptography	
- Checking for expired SSL certificates [0/142]	[NONE]
[WARNING]: Test CRYP-7902 had a long execu	tion: 12.073512 seconds
 Found 0 encrypted and 1 unencrypted swap de Kernel entropy is sufficient HW RNG & rngd SW prng MOR variable not found 	evices in use. [OK] [YES] [NO] [NO] [WEAK]
[+] Virtualization	
[+] Containers	
[+] Security frameworks	
	[FOUND] [ENABLED]

```
Found 39 unconfined processes
 - Checking presence SELinux
                                                [NOT FOUND]
 - Checking presence TOMOYO Linux
                                                          [NOT FOUND]
                                                [NOT FOUND]
 - Checking presence grsecurity
 - Checking for implemented MAC framework
                                                          [OK]
[+] Software: file integrity
 - Checking file integrity tools
                                                [FOUND]
         - AIDE
         - AIDE config file
                                                 FOUND
                                                 [FOUND]

    AIDE database

 - dm-integrity (status)
                                                [DISABLÉD]
                                                [DISABLED]
 - dm-verity (status)
         - AIDE config (Checksum)
                                                          [OK]
                                                [FOUND]

    Checking presence integrity tool

[+] Software: System tooling
 - Checking automation tooling
 - Automation tooling
                                                [NOT FOUND]
 - Checking for IDS/IPS tooling
                                                [ NONE ]
[+] Software: Malware
                                                [NOT FOUND]
- Malware software components
[+] File Permissions
 - Starting file permissions check
         File: /boot/grub/grub.cfg
                                                          [SUGGESTION]
         File: /etc/crontab
                                                [SUGGESTION]
         File: /etc/group
                                                [ OK ]
         File: /etc/group-
                                                 [OK]
         File: /etc/hosts.allow
                                                 [OK]
         File: /etc/hosts.deny
                                                          [OK]
         File: /etc/issue
                                                [OK]
         File: /etc/issue.net
                                                 [OK]
         File: /etc/passwd
                                                 [OK]
         File: /etc/passwd-
                                                [OK]
         File: /etc/ssh/sshd_config
                                                          [SUGGESTION]
         Directory: /root/.ssh
                                                [OK]
                                                          [SUGGESTION]
         Directory: /etc/cron.d
         Directory: /etc/cron.daily
                                                          SUGGESTION ]
         Directory: /etc/cron.hourly
                                                          [SUGGESTION]
                                                           SUGGESTION
         Directory: /etc/cron.weekly
         Directory: /etc/cron.monthly
                                                          [ SUGGESTION ]
[+] Home directories
 - Permissions of home directories
                                                [OK]
 - Ownership of home directories
                                                 įοκί
 - Checking shell history files
                                                 [OK]
[+] Kernel Hardening
 - Comparing sysctl key pairs with scan profile
         - dev.tty.ldisc_autoload (exp: 0)
                                                          [DIFFERENT]
         - fs.protected_fifos (exp: 2)
                                                          [ DIFFERENT ]
         - fs.protected_hardlinks (exp: 1)
                                                          [OK]
                                                           į ok j
         - fs.protected_regular (exp: 2)
         - fs.protected_symlinks (exp: 1)
                                                           [ OK ]
                                                           [DIFFERENT]
         - fs.suid_dumpable (exp: 0)
         - kernel.core_uses_pid (exp: 1)
                                                           [OK]
                                                          [OK]
         - kernel.ctrl-alt-del (exp: 0)
         - kernel.dmesg_restrict (exp: 1)
                                                           [ OK ]
         - kernel.kptr_restrict (exp: 2)
                                                           [DIFFERENT]
         - kernel.modules_disabled (exp: 1)
                                                          [DIFFERENT]
         - kernel.perf_event_paranoid (exp: 3)
                                                          [ DIFFERENT ]
```

```
- kernel.randomize_va_space (exp: 2)
                                                         [OK]
         - kernel.sysrq (exp: 0)
                                                         [ DIFFERENT ]
         - kernel.unprivileged_bpf_disabled (exp: 1)
                                                          DIFFERENT I
         - kernel.yama.ptrace_scope (exp: 1 2 3)
                                                          [ OK ]
         - net.core.bpf_jit_harden (exp: 2)
                                                          Î DIFFERENT 1
         - net.ipv4.conf.all.accept_redirects (exp: 0)
                                                         [ DIFFERENT ]
         - 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)
                                                         l OK I
         - net.ipv4.conf.all.log_martians (exp: 1)
                                                         [DIFFERENT]
                                                         įοκ j
         - net.ipv4.conf.all.mc_forwarding (exp: 0)
         - net.ipv4.conf.all.proxy_arp (exp: 0)
                                                          [ OK ]
         - net.ipv4.conf.all.rp filter (exp: 1)
                                                         DIFFERENT ]
         - net.ipv4.conf.all.send_redirects (exp: 0)
                                                          [ DIFFERENT ]
         - net.ipv4.conf.default.accept redirects (exp: 0)
                                                         [ DIFFERENT ]
         - net.ipv4.conf.default.accept_source_route (exp: 0)
                                                                   [OK]
         - net.ipv4.conf.default.log_martians (exp: 1)
                                                         [DIFFERENT]
         - net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)
                                                                   [OK]
         - net.ipv4.icmp_ignore_bogus_error_responses (exp: 1)
                                                                   [OK]
                                                         į ok į
         - net.ipv4.tcp_syncookies (exp: 1)
         - net.ipv4.tcp_timestamps (exp: 0 1)
                                                          [ OK ]
                                                          [DIFFERENT]
         - net.ipv6.conf.all.accept_redirects (exp: 0)
         - net.ipv6.conf.all.accept_source_route (exp: 0)
                                                         [OK]
                                                         [DIFFERENT]
         net.ipv6.conf.default.accept_redirects (exp: 0)
         - net.ipv6.conf.default.accept_source_route (exp: 0)
                                                                  [OK]
[+] Hardening
         - Installed compiler(s)
                                                         [FOUND]
         - Installed malware scanner
                                                          NOT FOUND 1
         - Non-native binary formats
                                                         [FOUND]
[+] Custom tests
 - Running custom tests...
                                               [NONE]
[+] Plugins (phase 2)
                                                [DONE]
 - Plugins (phase 2)
______
 -[ Lynis 3.0.9 Results ]-
 Warnings (3):
 ! Found one or more vulnerable packages. [PKGS-7392]
         https://cisofy.com/lynis/controls/PKGS-7392/
 ! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]
         https://cisofy.com/lynis/controls/MAIL-8818/
 ! iptables module(s) loaded, but no rules active [FIRE-4512]
         https://cisofy.com/lynis/controls/FIRE-4512/
 Suggestions (35):
 * Consider hardening system services [BOOT-5264]
         - Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service
         https://cisofy.com/lynis/controls/BOOT-5264/
 * Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229]
         https://cisofy.com/lynis/controls/AUTH-9229/
 * Configure password hashing rounds in /etc/login.defs [AUTH-9230]
         https://cisofy.com/lynis/controls/AUTH-9230/
 * When possible set expire dates for all password protected accounts [AUTH-9282]
         https://cisofy.com/lynis/controls/AUTH-9282/
```

- * To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310] https://cisofy.com/lynis/controls/FILE-6310/
- * To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310] https://cisofy.com/lynis/controls/FILE-6310/
- * Check DNS configuration for the dns domain name [NAME-4028] https://cisofy.com/lynis/controls/NAME-4028/
- * Purge old/removed packages (1 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, cron jobs and startup scripts. [PKGS-7346]

https://cisofy.com/lynis/controls/PKGS-7346/

- * Install debsums utility for the verification of packages with known good database. [PKGS-7370] https://cisofy.com/lynis/controls/PKGS-7370/
- * Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or unattended-upgrades [PKGS-7392] https://cisofy.com/lynis/controls/PKGS-7392/
- * Install package apt-show-versions for patch management purposes [PKGS-7394] https://cisofy.com/lynis/controls/PKGS-7394/
- Determine if protocol 'dccp' is really needed on this system [NETW-3200] https://cisofy.com/lynis/controls/NETW-3200/
- Determine if protocol 'sctp' is really needed on this system [NETW-3200] https://cisofy.com/lynis/controls/NETW-3200/
- * Determine if protocol 'rds' is really needed on this system [NETW-3200] https://cisofy.com/lynis/controls/NETW-3200/
- Determine if protocol 'tipc' is really needed on this system [NETW-3200] https://cisofy.com/lynis/controls/NETW-3200/
- * You are advised to hide the mail_name (option: smtpd_banner) from your postfix configuration. Use postconf -e or change your main.cf file (/etc/postfix/main.cf) [MAIL-8818] https://cisofy.com/lynis/controls/MAIL-8818/
- * Consider hardening SSH configuration [SSH-7408]
 Details : ClientAliveCountMax (set 3 to 2)
 https://cisofy.com/lynis/controls/SSH-7408/
- * Consider hardening SSH configuration [SSH-7408]
 Details : LogLevel (set INFO to VERBOSE)
 https://cisofy.com/lynis/controls/SSH-7408/
- * Consider hardening SSH configuration [SSH-7408]
 Details: MaxAuthTries (set 6 to 3)
 https://cisofy.com/lynis/controls/SSH-7408/
- * Consider hardening SSH configuration [SSH-7408]
 Details: MaxSessions (set 10 to 2)
 https://cisofy.com/lynis/controls/SSH-7408/
- * Consider hardening SSH configuration [SSH-7408]
 Details : Port (set 22 to)
 https://cisofy.com/lynis/controls/SSH-7408/
- * Consider hardening SSH configuration [SSH-7408]
 Details : TCPKeepAlive (set YES to NO) https://cisofy.com/lynis/controls/SSH-7408/
- * Consider hardening SSH configuration [SSH-7408]
 Details: X11Forwarding (set YES to NO)
 https://cisofy.com/lynis/controls/SSH-7408/
- * Consider hardening SSH configuration [SSH-7408]
 Details: AllowAgentForwarding (set YES to NO)

https://cisofy.com/lynis/controls/SSH-7408/

- * Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154] https://cisofy.com/lynis/controls/LOGG-2154/
- * Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126] https://cisofy.com/lynis/controls/BANN-7126/
- * Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130] https://cisofy.com/lynis/controls/BANN-7130/
- * Enable process accounting [ACCT-9622] https://cisofy.com/lynis/controls/ACCT-9622/
- * Enable sysstat to collect accounting (no results) [ACCT-9626] https://cisofy.com/lynis/controls/ACCT-9626/
- * Audit daemon is enabled with an empty ruleset. Disable the daemon or define rules [ACCT-9630] https://cisofy.com/lynis/controls/ACCT-9630/
- * Determine if automation tools are present for system management [TOOL-5002] https://cisofy.com/lynis/controls/TOOL-5002/
- * Consider restricting file permissions [FILE-7524]
 - Details : See screen output or log file
 - Solution : Use chmod to change file permissions https://cisofy.com/lynis/controls/FILE-7524/
- * 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>)

Solution: Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>https://cisofy.com/lynis/controls/KRNL-6000/

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

* 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, Wazuh https://cisofy.com/lynis/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:

Tests performed : 277 Plugins enabled : 2

Components:

- Firewall [\

- Malware scanner [X]

Scan mode:

Normal [V] Forensics [] Integration [] Pentest []

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	
========		
Lynis 3.0.9		
Auditing, system han (Linux, macOS, BSD	dening, and compliance for UNIX-based systems , and others)	
	https://cisofy.com/lynis/ vailable (compliance, plugins, interface and tools)	