(DB) Address Book Appliance System Hardening and Compliance Report

Pelumi Akande | Ross Barber | Carina Martinez-Lopez | Zoe Medina | Randall Seymore

October 6th - 9th, 2023

CYBR-510-02B

For issues with embedded content, please use the Google Doc
https://docs.google.com/document/d/1xPa492jQNgznei2aQ7mI5P7ob-KqznhJcaHgV5yYhYE/edit?usp=sharing

Table of Contents

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

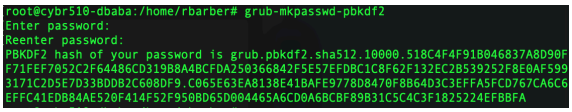
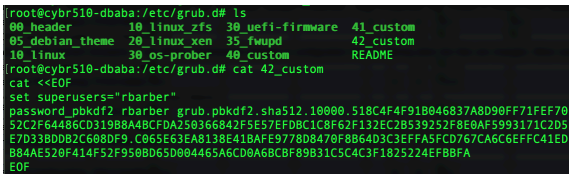
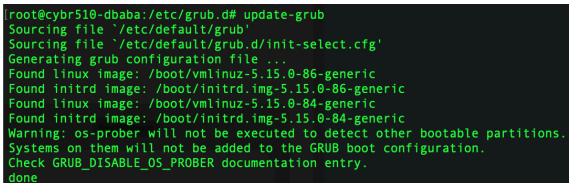
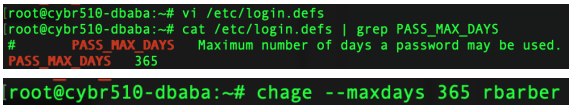
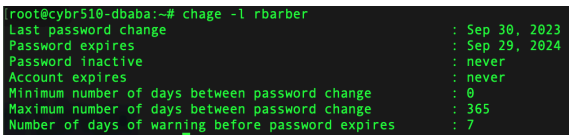
After downloading the Ubuntu Server 22.04.03 LTS image from https://ubuntu.com/download/server, a virtual machine with specifications described in the section above was deployed in a lab environment. The installation steps were followed to create a non root user and include a default ssh server configuration.

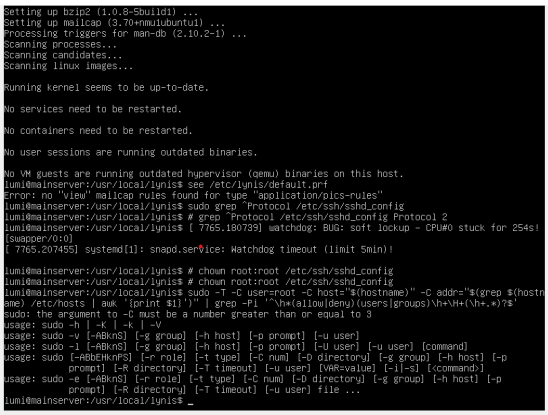
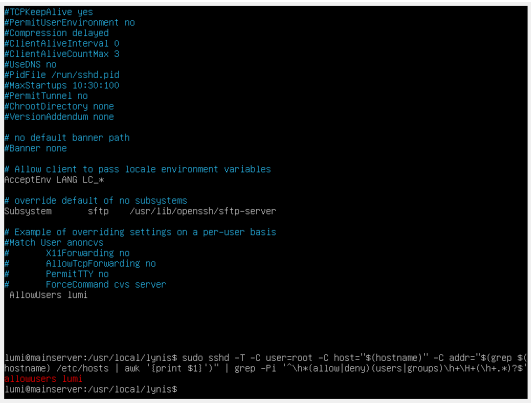
Following deployment, administrators connected to the VM remotely and performed apt package update and upgrade steps. The Lynis scanner was downloaded directly to the VM from https://github.com/CISOfy/Lynis and run as root to generate the Initial Lynis Vulnerability Scan Results.

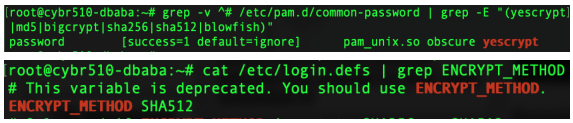
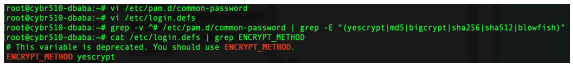
Recommendations from the initial scan were taken and identified on the Ubuntu 22.04 CIS Benchmark. Each set of guidance was combined to identify an appropriate configuration to harden the system accordingly. Testers performed each assigned test first on a replicated VM to validate feasibility and make 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>*-custom` configuration file:** cat <<EOF set superusers="*<username>*" password_pbkdf2 *<username>* *<encrypted-password>* EOF **3. Update the grub2 configuration:** cybr510-dbaba# update-grub	**Audit:**  **Remediation:**    **Results:** 
2	**Lynis Scan Recommendation** Configure maximum password age in /etc/login.defs [AUTH-9286] **CIS Benchmark Recommendation** 5.5.1.2 - Ensure password expiration is 365 days or less	**1. Set the PASS_MAX_DAYS parameter to conform to site policy in /etc/login.defs:** PASS_MAX_DAYS 365 **2. Modify user parameters for all users with a password set to match:** cybr510-dbaba# chage --maxdays 365 *<user>*	**Audit:**  **Remediation:**  **Result:** 

3	**Lynis Scan Recommendation** Consider hardening SSH configuration [SSH-7408]	**1. Firstly run sudo sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" \| grep -Pi '^\h*(allow\|deny)(users\|groups)\ h+\H+(\h+.*)?$'** **2. Then sudo nano /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:** 
	CIS Benchmark Recommendation 5.2.4 Configure SSH Server		

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

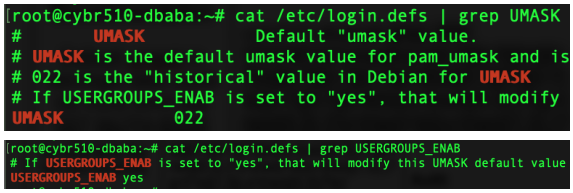
<table>
<tr>
<td rowspan="2">5</td>
<td>Lynis Scan Recommendation

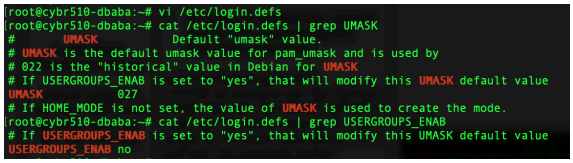
Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]</td>
<td rowspan="2">1. Remove or modify the `umask` of any files returned by the following command:

cybr510-dbaba# grep -RPi '(^|^[^#]*)\s*umask\s+([0-7][0-7][01][0-7]\b|[0-7][0-7][0-7][0-6]\b|[0-7][01][0-7]\b|[0-7][0-7][0-6]\b|(u=[rwx]{0,3},)?(g=[rwx]{0,3},)?o=[rwx]+\b|(u=[rwx]{1,3},)?g=[^rx]{1,3}(,o=[rwx]{0,3})?\b)' /etc/login.defs /etc/profile* /etc/bash.bashrc*

2. Edit `/etc/login.defs` and edit the `UMASK` and `USERGROUPS_ENAB` lines as follows:

UMASK 027

USERGROUPS_ENAB no</td>
<td rowspan="2">Audit:
 

Remediation/Results:
  </td>
</tr>
<tr>
<td>CIS Benchmark Recommendation

5.5.4 Ensure default user umask is 027 or more restrictive.</td>
</tr>
<tr>
<td rowspan="2">6</td>
<td>Lynis Scan Recommendation

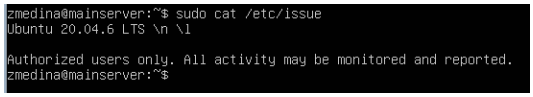
Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft</td>
<td rowspan="2">1. Run bash script provided by the benchmark to disable usb-storage</td>
<td rowspan="2">Audit:
 
Remediation:
 
Results:
  </td>
</tr>
<tr>
<td>CIS Benchmark Recommendation

1.1.10 Disable USB Storage</td>
</tr>
</table>

<table>
<tr>
<td>7</td>
<td>Lynis Scan Recommendation

Add a legal banner to /etc/issue, to warn unauthorized users

CIS Benchmark Recommendation

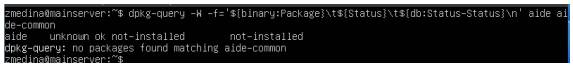
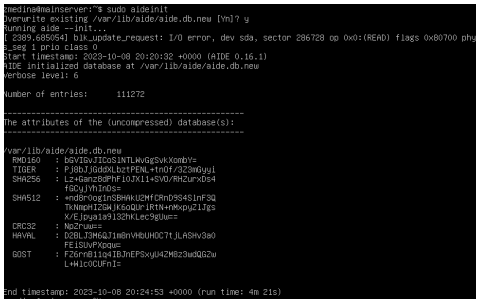
1.7.2 Ensure local login warning banner is configured properly</td>
<td>1. Enter command: sudo bash -c “echo ‘Authorized users only. All activity may be monitored and reported.’ >> /etc/issue”</td>
<td>Audit:
 
Remediation:
 
Result:
  </td>
</tr>
<tr>
<td>8</td>
<td>Lynis Scan Recommendation

Install a file integrity tool to monitor changes to critical and sensitive files

CIS Benchmark Recommendation

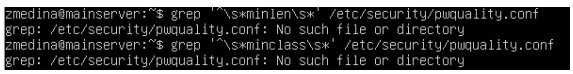
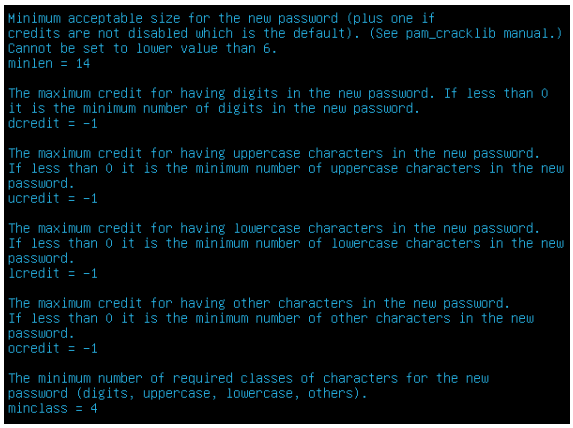
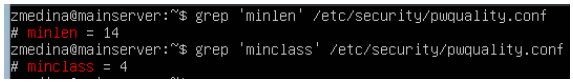
1.3.1 Ensure AIDE is installed</td>
<td>1. Enter command: sudo apt install aide aide-common

2. Enter command: sudo aideinit

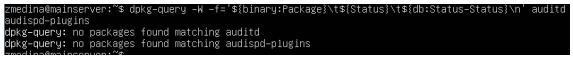
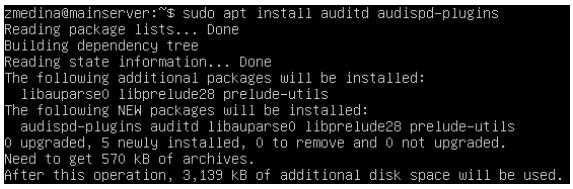
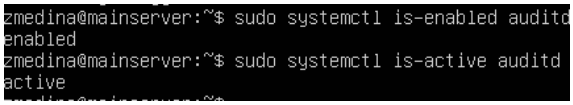
3. Configure mail server for sending logs</td>
<td>Audit:
 
Remediation:
 
Results:
  </td>
</tr>
</table>

<table>
<tr>
<td rowspan="2">9</td>
<td>Lynis Scan Recommendation

Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc</td>
<td rowspan="2">1. Enter command: sudo apt install libpam-pwquality

2. 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.</td>
<td rowspan="2">Audit:
 
Remediation:
 
Results:
  </td>
</tr>
<tr>
<td>CIS Benchmark Recommendation

5.4.1 Ensure password creation requirements are configured</td>
</tr>
<tr>
<td rowspan="2">10</td>
<td>Lynis Scan Recommendation

Enable auditd to collect audit information</td>
<td rowspan="2">1. Enter command: sudo apt install auditd audispd-plugins</td>
<td rowspan="2">Audit:
 
Remediation:
 
Results:
 
  </td>
</tr>
<tr>
<td>CIS Benchmark Recommendation

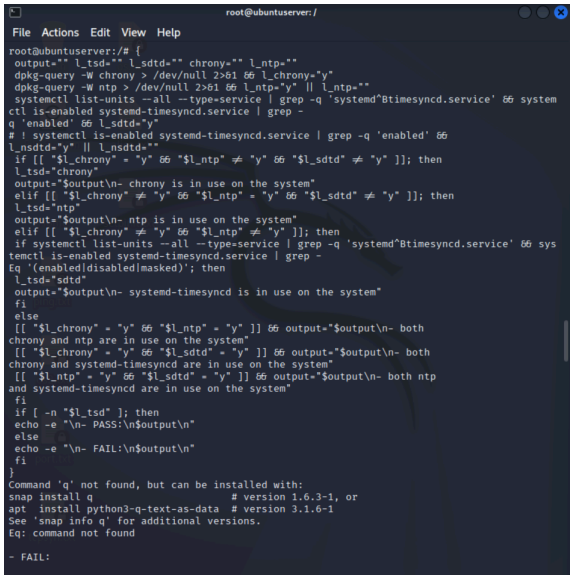
4.1.1.2 Ensure auditd is enabled</td>
</tr>
</table>

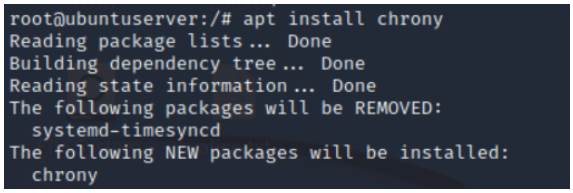
<table>
<tr>
<td rowspan="2">11</td>
<td>Lynis Scan Recommendation

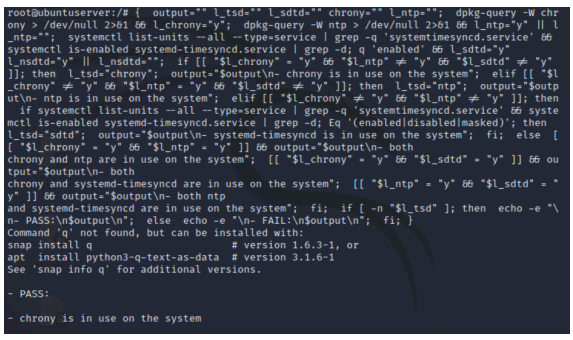
! systemd-timesyncd did not synchronize the time recently. [TIME-3185]</td>
<td rowspan="2">1. Enter command: apt install chrony

2. Enter command: systemctl stop systemd-timesyncd.service

3. Enter command: systemctl --now mask systemd-timesyncd.service

4. Enter command: apt purge ntp</td>
<td rowspan="2">Audit:
 

Remediation:
 

Results:
 
</td>
</tr>
<tr>
<td>CIS Benchmark Recommendation

2.1.1 Ensure time synchronization is in use.</td>
</tr>
</table>

<table>
<tr>
<td>12</td>
<td>Lynis Scan Recommendation

Configure minimum password age in /etc/login.defs [AUTH-9286]

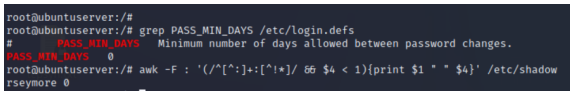
CIS Benchmark Recommendation

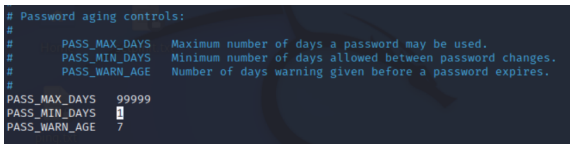
5.5.1.1 Ensure minimum days between password changes is configured.</td>
<td>1. Enter command: sudo nano /etc/login.defs

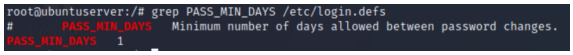
2. Change PASS_MIN_DAYS value from 0 to 1.

3. Press: Ctrl + x

4. Enter value: Y

5. Press enter to save changes.</td>
<td>Audit:
 

Remediation:
 

Results:
 
</td>
</tr>
<tr>
<td>13</td>
<td>Lynis Scan Recommendation

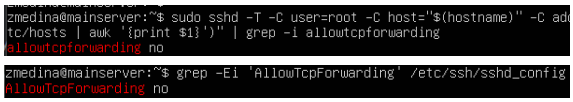
Consider hardening SSH configuration [SSH-7408] Details: AllowTcpForwarding (set YES to NO)

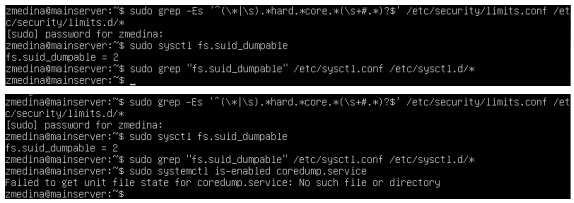
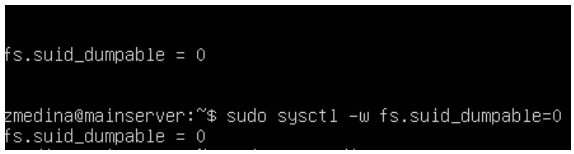
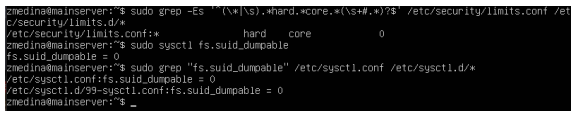
CIS Benchmark Recommendation

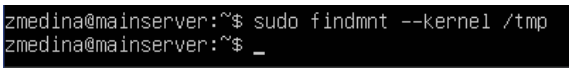
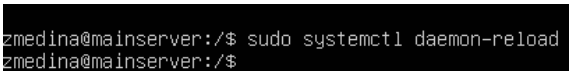
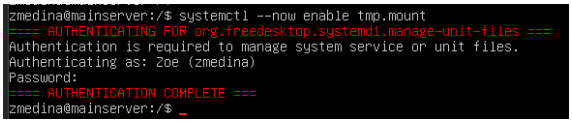
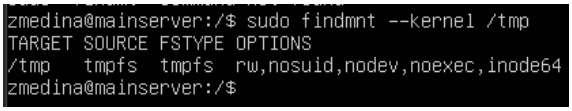
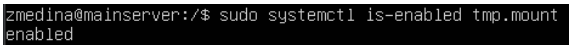
5.2.16 Ensure SSH AllowTcpForwarding is disabled</td>
<td>1. Enter the command: sudo nano /etc/ssh/sshd_config

2. Modify or add the line: “AllowTcpForwarding no”</td>
<td>Audit:
 

Remediation:
 

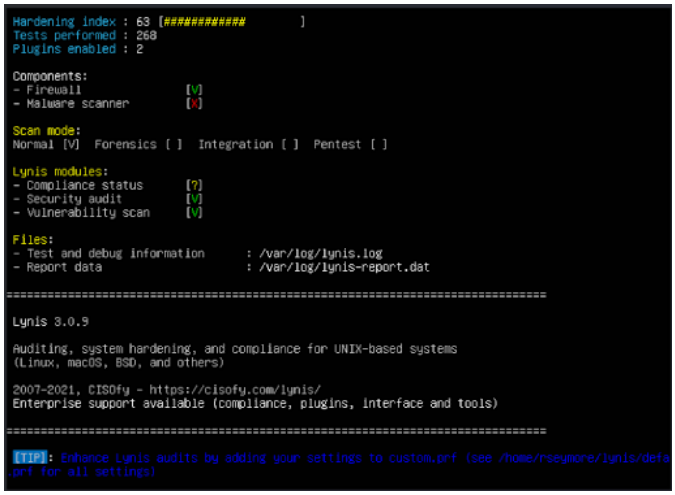
Results:
 
</td>
</tr>
</table>

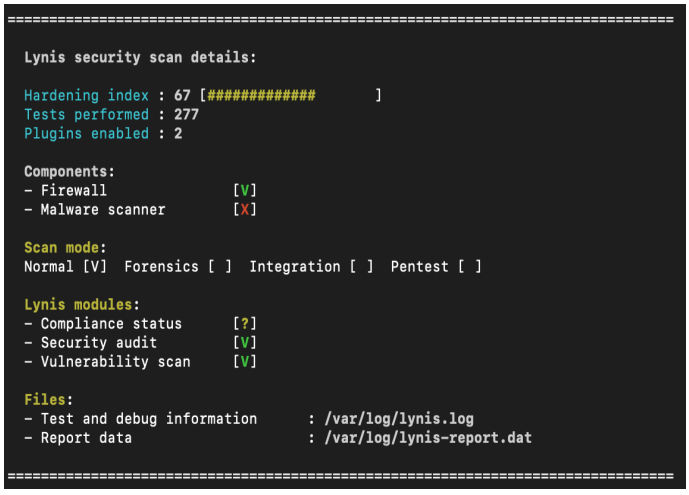
14	**Lynis Scan Recommendation** If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820] **CIS Benchmark Recommendation** 1.5.4 Ensure core dumps are restricted	1. **Enter command: sudo nano /etc/security/limits.conf** 2. **Modify or add the line: “ hard core 0”** 3. **Enter command: sudo nano /etc/sysctl.conf** 4. **Modify or add the line: “fs.suid_dumpable = 0”** 5. **Enter command: sudo sysctl -w fs.suid_dumpable=0** 6. **Enter command: sudo nano /etc/systemd/coredump.conf** 7. **Modify or add the line: “Storage=none”** 8. **Modify or add the line: “ProcessSizeMax=0”**	**Audit:**  **Remediation:**    **Results:** 

15	**Lynis Scan Recommendation** To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310] **CIS Benchmark Recommendation** 1.1.2.1 Ensure /tmp is a separate partition.	1. **Copy tmp.mount file to the /etc directory with command: sudo cp -v /usr/share/systemd/tmp.mount /etc/systemd/system/** 2. **Modify the tmp.mount file using command: sudo nano /etc/systemd/system/tmp.mount** 3. **Edit the options at the bottom to equal: 1777,strictatime,nosuid,nodev,noexec** 4. **Reload the service using command: sudo systemctl daemon-reload**	**Audit:**  **Remediation:**     **Results:**  

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 Data 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 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
  Hostname:                  cybr510-dbaba
  ---------------------------------------------------
  Profiles:                  /home/rbarber/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          ./plugins
  ---------------------------------------------------
  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 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                [ 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 ]
         - cron.service:                             [ UNSAFE ]
         - dbus.service:                             [ UNSAFE ]
         - dm-event.service:                         [ UNSAFE ]
         - dmesg.service:                            [ UNSAFE ]
         - emergency.service:                        [ UNSAFE ]
         - getty@tty1.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 ]
         - plymouth-start.service:                   [ UNSAFE ]
         - polkit.service:                           [ UNSAFE ]
         - rc-local.service:                         [ UNSAFE ]
         - rescue.service:                           [ UNSAFE ]
         - rsyslog.service:                          [ UNSAFE ]
         - snap.lxd.daemon.service:                  [ UNSAFE ]
         - snap.lxd.user-daemon.service:             [ UNSAFE ]
         - snapd.aa-prompt-listener.service:         [ UNSAFE ]
         - snapd.service:                            [ UNSAFE ]
         - ssh.service:                              [ UNSAFE ]
         - 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 ]
         - 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:                         [ UNSAFE ]
         - ubuntu-advantage.service:                 [ UNSAFE ]
         - udisks2.service:                          [ UNSAFE ]
         - unattended-upgrades.service:              [ UNSAFE ]
         - upower.service:                           [ PROTECTED ]
         - 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 ]
 - Checking default I/O kernel scheduler                     [ NOT FOUND ]
 - Checking for available kernel update              [ OK ]
 - Checking core dumps configuration
```

```
        - configuration in systemd conf files                   [ DEFAULT ]
        - configuration in /etc/profile                         [ DEFAULT ]
        - 'hard' configuration in /etc/security/limits.conf     [ DEFAULT ]
        - 'soft' configuration in /etc/security/limits.conf     [ DEFAULT ]
        - Checking setuid core dumps configuration              [ PROTECTED ]
  - Check if reboot is needed                                   [ YES ]

[+] Memory and Processes
------------------------------------
  - Checking /proc/meminfo                                      [ FOUND ]
  - 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 ]
  - Unique UIDs                                                 [ OK ]
  - Consistency of group files (grpck)                          [ OK ]
  - Unique group IDs                                            [ OK ]
  - Unique group names                                          [ OK ]
  - Password file consistency                                   [ OK ]
  - Password hashing methods                                    [ SUGGESTION ]
  - 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 ]
        - Permissions for: /etc/sudoers.d/README                [ OK ]
  - PAM password strength tools                                 [ SUGGESTION ]
  - PAM configuration files (pam.conf)                          [ FOUND ]
  - PAM configuration files (pam.d)                             [ FOUND ]
  - PAM modules                                                 [ FOUND ]
  - LDAP module in PAM                                          [ NOT FOUND ]
  - Accounts without expire date                                [ SUGGESTION ]
  - Accounts without password                                   [ OK ]
  - 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
        - umask (/etc/profile)                                  [ NOT FOUND ]
        - 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
        - Checking /home mount point                            [ SUGGESTION ]
        - Checking /tmp mount point                             [ SUGGESTION ]
        - Checking /var mount point                             [ SUGGESTION ]
  - Checking LVM volume groups                                  [ FOUND ]
        - Checking LVM volumes                                  [ FOUND ]
  - Query swap partitions (fstab)                               [ OK ]
```

```
  - Testing swap partitions                                [ OK ]
  - Testing /proc mount (hidepid)                          [ SUGGESTION ]
  - 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                                  [ PARTIALLY HARDENED ]
  - 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 ]
  - Checking USBGuard                                      [ NOT FOUND ]

[+] Storage
------------------------------------
  - Checking firewire ohci driver (modprobe config)        [ DISABLED ]

[+] 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
      - Searching dpkg package manager                     [ FOUND ]
      - Querying package manager
      - Query unpurged packages                            [ NONE ]
  - Checking security repository in sources.list file      [ OK ]
  - Checking APT package database                          [ OK ]
  - Checking vulnerable packages                           [ OK ]
  - Checking upgradeable packages                          [ SKIPPED ]
  - Checking package audit tool                            [ INSTALLED ]
      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
------------------------------------
  - Checking cups daemon                        [ NOT FOUND ]
  - Checking lp daemon                          [ NOT RUNNING ]

[+] Software: e-mail and messaging
------------------------------------

[+] Software: firewalls
------------------------------------
  - Checking iptables kernel module             [ FOUND ]
        - Checking iptables policies of chains  [ FOUND ]
        - Checking for empty ruleset            [ WARNING ]
        - Checking for unused rules             [ OK ]
  - Checking host based firewall                [ ACTIVE ]

[+] Software: webserver
------------------------------------
  - Checking Apache                             [ NOT FOUND ]
  - Checking nginx                              [ NOT FOUND ]

[+] SSH Support
------------------------------------
  - Checking running SSH daemon                 [ FOUND ]
        - Searching SSH configuration           [ FOUND ]
        - OpenSSH option: AllowTcpForwarding    [ SUGGESTION ]
        - OpenSSH option: ClientAliveCountMax   [ SUGGESTION ]
        - OpenSSH option: ClientAliveInterval   [ OK ]
        - OpenSSH option: FingerprintHash       [ OK ]
        - OpenSSH option: GatewayPorts          [ OK ]
        - OpenSSH option: IgnoreRhosts          [ OK ]
        - OpenSSH option: LoginGraceTime        [ OK ]
        - OpenSSH option: LogLevel              [ SUGGESTION ]
        - 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 ]
        - OpenSSH option: TCPKeepAlive          [ SUGGESTION ]
        - OpenSSH option: UseDNS                [ OK ]
        - OpenSSH option: X11Forwarding         [ SUGGESTION ]
        - OpenSSH option: AllowAgentForwarding  [ SUGGESTION ]
        - OpenSSH option: AllowUsers            [ NOT FOUND ]
        - OpenSSH option: AllowGroups           [ NOT FOUND ]

[+] SNMP Support
------------------------------------
  - Checking running SNMP daemon                [ NOT FOUND ]

[+] 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                [ OK ]
        - Checking Syslog-NG status                  [ NOT FOUND ]
        - Checking systemd journal status            [ FOUND ]
        - Checking Metalog status                    [ NOT FOUND ]
        - Checking RSyslog status                    [ FOUND ]
        - Checking RFC 3195 daemon status            [ NOT FOUND ]
        - Checking minilogd instances                [ NOT FOUND ]
  - Checking logrotate presence                      [ OK ]
  - Checking remote logging                          [ NOT ENABLED ]
  - Checking log directories (static list)           [ DONE ]
  - Checking open log files                          [ DONE ]
  - Checking deleted files in use                    [ DONE ]

[+] Insecure services
------------------------------------
  - Installed inetd package                          [ NOT FOUND ]
  - Installed xinetd package                         [ OK ]
        - xinetd status                              [ NOT ACTIVE ]
  - Installed rsh client package                     [ OK ]
  - Installed rsh server package                     [ OK ]
  - Installed telnet client package                  [ OK ]
  - Installed telnet server package                  [ NOT FOUND ]
  - Checking NIS client installation                 [ OK ]
  - Checking NIS server installation                 [ OK ]
  - Checking TFTP client installation                [ OK ]
  - Checking TFTP server installation                [ OK ]

[+] Banners and identification
------------------------------------
  - /etc/issue                                 [ FOUND ]
        - /etc/issue contents                  [ WEAK ]
  - /etc/issue.net                             [ FOUND ]
        - /etc/issue.net contents              [ WEAK ]

[+] Scheduled tasks
------------------------------------
  - Checking crontab and cronjob files         [ DONE ]

[+] Accounting
------------------------------------
  - Checking accounting information            [ NOT FOUND ]
  - Checking sysstat accounting data           [ NOT FOUND ]
  - Checking auditd                            [ NOT FOUND ]

[+] Time and Synchronization
------------------------------------
  - NTP daemon found: systemd (timesyncd)                [ FOUND ]
  - Checking for a running NTP daemon or client          [ OK ]
  - Last time synchronization                  [ 2819s ]

[+] Cryptography
------------------------------------
  - Checking for expired SSL certificates [0/141]        [ NONE ]

  [WARNING]: Test CRYP-7902 had a long execution: 11.979649 seconds

  - Found 0 encrypted and 1 unencrypted swap devices in use.  [ OK ]
  - Kernel entropy is sufficient               [ YES ]
  - HW RNG & rngd                              [ NO ]
  - SW prng                                    [ NO ]
  - MOR variable not found                     [ WEAK ]

[+] Virtualization
```

```
---------------------------------------

[+] Containers
---------------------------------------

[+] Security frameworks
---------------------------------------
  - Checking presence AppArmor                [ FOUND ]
        - Checking AppArmor status            [ ENABLED ]
        Found 39 unconfined processes
  - Checking presence SELinux                 [ NOT FOUND ]
  - Checking presence TOMOYO Linux            [ NOT FOUND ]
  - Checking presence grsecurity              [ NOT FOUND ]
  - Checking for implemented MAC framework    [ OK ]

[+] Software: file integrity
---------------------------------------
  - Checking file integrity tools
  - dm-integrity (status)                     [ DISABLED ]
  - dm-verity (status)                        [ DISABLED ]
  - Checking presence integrity tool          [ NOT FOUND ]

[+] 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
        - dev.tty.ldisc_autoload (exp: 0)             [ DIFFERENT ]
        - fs.protected_fifos (exp: 2)                 [ DIFFERENT ]
        - fs.protected_hardlinks (exp: 1)             [ OK ]
        - fs.protected_regular (exp: 2)               [ OK ]
        - fs.protected_symlinks (exp: 1)              [ OK ]
```

```
        - fs.suid_dumpable (exp: 0)                             [ DIFFERENT ]
        - kernel.core_uses_pid (exp: 1)                         [ OK ]
        - kernel.ctrl-alt-del (exp: 0)                          [ OK ]
        - kernel.dmesg_restrict (exp: 1)                        [ OK ]
        - kernel.kptr_restrict (exp: 2)                         [ 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 ]
        - kernel.yama.ptrace_scope (exp: 1 2 3)                 [ OK ]
        - 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 ]
        - 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 ]
        - net.ipv4.tcp_syncookies (exp: 1)                      [ OK ]
        - net.ipv4.tcp_timestamps (exp: 0 1)                    [ OK ]
        - net.ipv6.conf.all.accept_redirects (exp: 0)           [ DIFFERENT ]
        - net.ipv6.conf.all.accept_source_route (exp: 0)        [ OK ]
        - net.ipv6.conf.default.accept_redirects (exp: 0)       [ DIFFERENT ]
        - net.ipv6.conf.default.accept_source_route (exp: 0)            [ OK ]

[+] Hardening
------------------------------------
        - Installed compiler(s)                                 [ FOUND ]
        - 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)
- Use --upload 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
  Hostname:                  cybr510-dbaba
  ---------------------------------------------------
  Profiles:                  /home/rbarber/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          ./plugins
  ---------------------------------------------------
  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 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 ]
         - apport.service:                       [ UNSAFE ]
         - auditd.service:                       [ EXPOSED ]
         - chrony.service:                       [ PROTECTED ]
         - cloud-init-hotplugd.service:                  [ UNSAFE ]
         - cron.service:                         [ UNSAFE ]
         - dbus.service:                         [ UNSAFE ]
         - dm-event.service:                     [ UNSAFE ]
         - dmesg.service:                        [ UNSAFE ]
         - emergency.service:                    [ UNSAFE ]
         - getty@tty1.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 ]
         - plymouth-start.service:               [ UNSAFE ]
         - polkit.service:                       [ UNSAFE ]
         - postfix@-.service:                    [ UNSAFE ]
         - rc-local.service:                     [ UNSAFE ]
         - rescue.service:                       [ UNSAFE ]
         - rsyslog.service:                      [ UNSAFE ]
         - snap.lxd.daemon.service:                      [ UNSAFE ]
         - snap.lxd.user-daemon.service:                 [ UNSAFE ]
         - snapd.aa-prompt-listener.service:             [ UNSAFE ]
         - snapd.service:                        [ UNSAFE ]
         - ssh.service:                          [ UNSAFE ]
         - 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 ]
         - systemd-logind.service:               [ PROTECTED ]
         - systemd-networkd.service:                     [ PROTECTED ]
         - systemd-resolved.service:                     [ PROTECTED ]
         - systemd-rfkill.service:               [ UNSAFE ]
         - systemd-udevd.service:                        [ MEDIUM ]
         - thermald.service:                     [ UNSAFE ]
         - ubuntu-advantage.service:                     [ UNSAFE ]
         - udisks2.service:                      [ UNSAFE ]
         - unattended-upgrades.service:                  [ UNSAFE ]
         - 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 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
         - configuration in systemd conf files           [ DISABLED ]
         - configuration in /etc/profile                 [ DEFAULT ]
         - 'hard' configuration in /etc/security/limits.conf     [ DISABLED ]
         - 'soft' config in /etc/security/limits.conf (implicit)  [ DISABLED ]
         - Checking setuid core dumps configuration              [ PROTECTED ]
 - Check if reboot is needed                     [ NO ]
```

```
[+] Memory and Processes
------------------------------------
  - Checking /proc/meminfo                            [ FOUND ]
  - 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 ]
  - Unique UIDs                                       [ OK ]
  - Consistency of group files (grpck)                [ OK ]
  - Unique group IDs                                  [ OK ]
  - Unique group names                                [ OK ]
  - Password file consistency                         [ OK ]
  - Password hashing methods                          [ SUGGESTION ]
  - 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 ]
        - Permissions for: /etc/sudoers.d/README                      [ OK ]
  - PAM password strength tools                       [ OK ]
  - PAM configuration files (pam.conf)                [ FOUND ]
  - PAM configuration files (pam.d)                   [ FOUND ]
  - PAM modules                                       [ FOUND ]
  - LDAP module in PAM                                [ NOT FOUND ]
  - Accounts without expire date                      [ SUGGESTION ]
  - Accounts without password                         [ OK ]
  - Locked accounts                                   [ OK ]
  - User password aging (minimum)                     [ CONFIGURED ]
  - 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 ]
  - 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
        - 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 ]
  - Testing swap partitions                           [ OK ]
  - Testing /proc mount (hidepid)                     [ SUGGESTION ]
  - 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                             [ PARTIALLY HARDENED ]
```

```
  - Mount options of /dev/shm                    [ PARTIALLY HARDENED ]
  - Mount options of /run                        [ HARDENED ]
  - Mount options of /tmp                        [ HARDENED ]
  - 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
------------------------------------
  - 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
        - 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 ]
  - Checking upgradeable packages                [ SKIPPED ]
  - Checking package audit tool                  [ INSTALLED ]
        Found: apt-get
  - 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
------------------------------------
  - Checking cups daemon                         [ NOT FOUND ]
  - Checking lp daemon                           [ NOT RUNNING ]

[+] Software: e-mail and messaging
------------------------------------
  - Postfix status                               [ RUNNING ]
        - Postfix configuration                  [ FOUND ]
```

```
        - Postfix banner                        [ WARNING ]

[+] Software: firewalls
------------------------------------
  - Checking iptables kernel module             [ FOUND ]
        - Checking iptables policies of chains          [ FOUND ]
        - Checking for empty ruleset                    [ WARNING ]
        - Checking for unused rules                     [ OK ]
  - Checking host based firewall                [ ACTIVE ]

[+] Software: webserver
------------------------------------
  - Checking Apache                             [ NOT FOUND ]
  - Checking nginx                              [ NOT FOUND ]

[+] SSH Support
------------------------------------
  - Checking running SSH daemon                         [ FOUND ]
        - Searching SSH configuration                   [ FOUND ]
        - OpenSSH option: AllowTcpForwarding                    [ OK ]
        - OpenSSH option: ClientAliveCountMax                   [ SUGGESTION ]
        - OpenSSH option: ClientAliveInterval           [ OK ]
        - OpenSSH option: FingerprintHash               [ OK ]
        - OpenSSH option: GatewayPorts                  [ OK ]
        - OpenSSH option: IgnoreRhosts                  [ OK ]
        - OpenSSH option: LoginGraceTime                [ OK ]
        - OpenSSH option: LogLevel                      [ SUGGESTION ]
        - 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 ]
        - OpenSSH option: TCPKeepAlive                  [ SUGGESTION ]
        - OpenSSH option: UseDNS                        [ OK ]
        - OpenSSH option: X11Forwarding                 [ SUGGESTION ]
        - OpenSSH option: AllowAgentForwarding                  [ SUGGESTION ]
        - OpenSSH option: AllowUsers                    [ NOT FOUND ]
        - OpenSSH option: AllowGroups                   [ NOT FOUND ]

[+] SNMP Support
------------------------------------
  - Checking running SNMP daemon                        [ NOT FOUND ]

[+] 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                   [ OK ]
        - Checking Syslog-NG status                     [ NOT FOUND ]
        - Checking systemd journal status               [ FOUND ]
        - Checking Metalog status                       [ NOT FOUND ]
        - Checking RSyslog status                       [ FOUND ]
```

```
        - Checking RFC 3195 daemon status               [ NOT FOUND ]
        - Checking minilogd instances                   [ NOT FOUND ]
  - Checking logrotate presence                         [ OK ]
  - Checking remote logging                             [ NOT ENABLED ]
  - Checking log directories (static list)              [ DONE ]
  - Checking open log files                             [ DONE ]
  - Checking deleted files in use                       [ DONE ]

[+] Insecure services
---------------------------------------
  - Installed inetd package                             [ NOT FOUND ]
  - Installed xinetd package                            [ OK ]
        - xinetd status                                 [ NOT ACTIVE ]
  - Installed rsh client package                        [ OK ]
  - Installed rsh server package                        [ OK ]
  - Installed telnet client package                     [ OK ]
  - Installed telnet server package                     [ NOT FOUND ]
  - Checking NIS client installation                    [ OK ]
  - Checking NIS server installation                    [ OK ]
  - Checking TFTP client installation                   [ OK ]
  - Checking TFTP server installation                   [ OK ]

[+] Banners and identification
---------------------------------------
  - /etc/issue                                  [ FOUND ]
        - /etc/issue contents                           [ WEAK ]
  - /etc/issue.net                                      [ FOUND ]
        - /etc/issue.net contents                       [ WEAK ]

[+] Scheduled tasks
---------------------------------------
  - Checking crontab and cronjob files                  [ DONE ]

[+] Accounting
---------------------------------------
  - Checking accounting information                     [ NOT FOUND ]
  - Checking sysstat accounting data                    [ NOT FOUND ]
  - Checking auditd                                     [ ENABLED ]
        - Checking audit rules                          [ SUGGESTION ]
        - Checking audit configuration file             [ OK ]
        - Checking auditd log file                      [ FOUND ]

[+] Time and Synchronization
---------------------------------------
  - NTP daemon found: chronyd                           [ FOUND ]
  - Checking for a running NTP daemon or client         [ OK ]

[+] Cryptography
---------------------------------------
  - Checking for expired SSL certificates [0/142]       [ NONE ]

  [WARNING]: Test CRYP-7902 had a long execution: 12.073512 seconds

  - Found 0 encrypted and 1 unencrypted swap devices in use.  [ OK ]
  - Kernel entropy is sufficient                        [ YES ]
  - HW RNG & rngd                                       [ NO ]
  - SW prng                                             [ NO ]
  - MOR variable not found                              [ WEAK ]

[+] Virtualization
---------------------------------------

[+] Containers
---------------------------------------

[+] Security frameworks
---------------------------------------
  - Checking presence AppArmor                          [ FOUND ]
        - Checking AppArmor status                      [ ENABLED ]
```

```
        Found 39 unconfined processes
  - Checking presence SELinux                   [ NOT FOUND ]
  - Checking presence TOMOYO Linux                      [ NOT FOUND ]
  - Checking presence grsecurity                [ NOT FOUND ]
  - Checking for implemented MAC framework              [ OK ]

[+] Software: file integrity
------------------------------------
  - Checking file integrity tools
        - AIDE                                  [ FOUND ]
        - AIDE config file                      [ FOUND ]
        - AIDE database                         [ FOUND ]
  - dm-integrity (status)                       [ DISABLED ]
  - dm-verity (status)                          [ DISABLED ]
        - AIDE config (Checksum)                        [ OK ]
  - Checking presence integrity tool            [ FOUND ]

[+] 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
        - dev.tty.ldisc_autoload (exp: 0)               [ DIFFERENT ]
        - fs.protected_fifos (exp: 2)                   [ DIFFERENT ]
        - fs.protected_hardlinks (exp: 1)               [ OK ]
        - fs.protected_regular (exp: 2)                 [ OK ]
        - fs.protected_symlinks (exp: 1)                [ OK ]
        - fs.suid_dumpable (exp: 0)                     [ DIFFERENT ]
        - kernel.core_uses_pid (exp: 1)                 [ OK ]
        - kernel.ctrl-alt-del (exp: 0)                  [ OK ]
        - kernel.dmesg_restrict (exp: 1)                [ OK ]
        - kernel.kptr_restrict (exp: 2)                 [ 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 ]
            - kernel.yama.ptrace_scope (exp: 1 2 3)             [ OK ]
            - 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 ]
            - 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 ]
            - net.ipv4.tcp_syncookies (exp: 1)                  [ OK ]
            - net.ipv4.tcp_timestamps (exp: 0 1)                [ OK ]
            - net.ipv6.conf.all.accept_redirects (exp: 0)       [ DIFFERENT ]
            - net.ipv6.conf.all.accept_source_route (exp: 0)    [ OK ]
            - net.ipv6.conf.default.accept_redirects (exp: 0)   [ DIFFERENT ]
            - net.ipv6.conf.default.accept_source_route (exp: 0)        [ OK ]

[+] Hardening
------------------------------------
            - Installed compiler(s)                             [ FOUND ]
            - 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):
  ----------------------------
  ! 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>)
            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:

  Hardening index : 67 [##############            ]
  Tests performed : 277
  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)

================================================================================
```