Hardening Linux

Jose Jimenez

Índice

Introducción ..... pag. 1

Auditoría Inicial ..... pag. 2
- Inicio de sesión
- Instalación de Lynis
- Cuestiones y Respuestas ..... pag. 3

Supervisión de puntos específicos ..... pag. 4
- 1.3.1 - Actualizaciones y Parches ..... pag. 5
- 2.2.14 - Nis ..... pag. 7
- 2.2.17 - Rsync ..... pag. 9
- 2.3.2 - Cliente Rsh ..... pag. 11
- 2.3.3 - Cliente Talk ..... pag. 13
- 2.3.6 - RPC ..... pag. 15
- 4.1.2 - /etc/crontab ..... pag. 17
- 4.5.1.1 - Días min. cambio de contraseña .. pag. 19
- 4.5.1.2 - Expiración de contraseña ..... pag. 21
- 4.5.1.4 - Bloqueo de contraseña ..... pag. 23
- 6.1.1 - Permisos /etc/passwd ..... pag. 25
- 6.1.3 - Permisos /etc/group ..... pag. 27

Auditoría final ..... pag. 29
- Cuestiones y Respuestas

Introducción

En el presente trabajo, se llevará a cabo una auditoría de seguridad en un sistema operativo Ubuntu, empleando la herramienta Lynis. Esta auditoría tiene como objetivo identificar fallos de seguridad o configuraciones deficientes que puedan comprometer la integridad y seguridad del sistema. Para ello, el proceso se desarrollará en tres etapas:

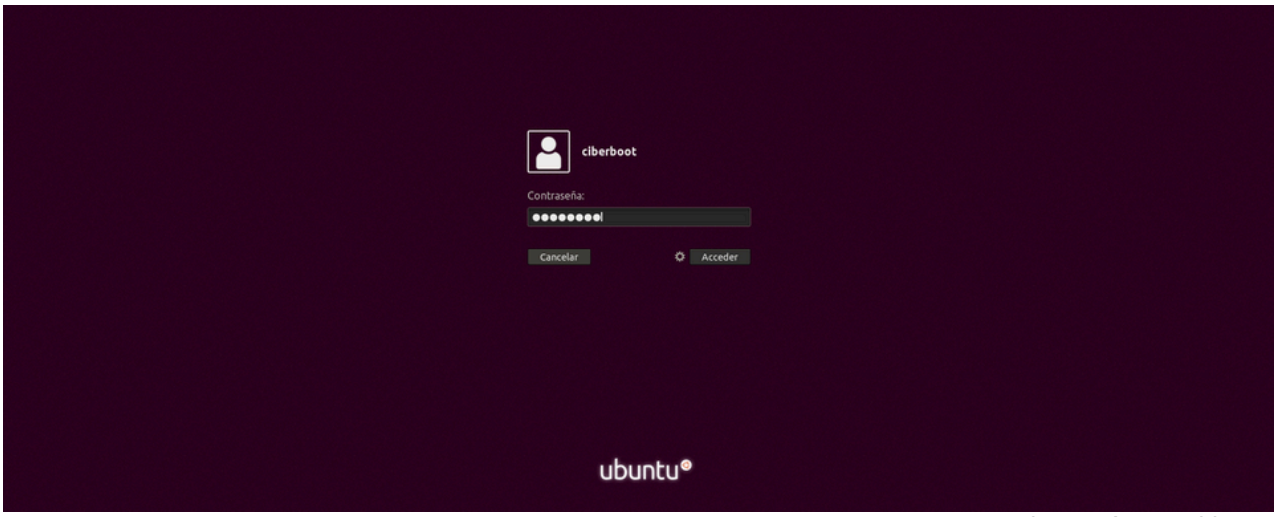
1. En primer lugar, se realizará una auditoría inicial con Lynis para detectar cualquier posible vulnerabilidad o configuración insegura en el sistema. Esta fase permite establecer una base de referencia respecto a las condiciones de seguridad del sistema en su estado actual.
2. A continuación, se abordarán ciertos puntos específicos que requieren revisión. Estos puntos son seleccionados en función de las recomendaciones de seguridad y configuraciones recomendadas para Ubuntu, de manera que, si se encuentra alguna desviación de las buenas prácticas, se proceda a realizar los ajustes necesarios en el sistema.
3. Finalmente, se ejecutará una segunda auditoría con Lynis para evaluar el impacto de las correcciones aplicadas. Este paso permite validar que las configuraciones actualizadas han mejorado la seguridad del sistema y han mitigado los problemas previamente identificados.

Con este enfoque, se busca realizar un análisis exhaustivo del sistema, documentando cada etapa del proceso y evaluando la efectividad de las medidas correctivas implementadas.

Lynis es una herramienta de seguridad probada en batalla para sistemas que ejecutan sistemas operativos basados en Linux, macOS o Unix. Realiza un análisis exhaustivo del estado de sus sistemas para respaldar el fortalecimiento del sistema y las pruebas de cumplimiento. El proyecto es un software de código abierto con licencia GPL y está disponible desde 2007”. Lynis: Auditoría, fortalecimiento del sistema, pruebas de cumplimiento.

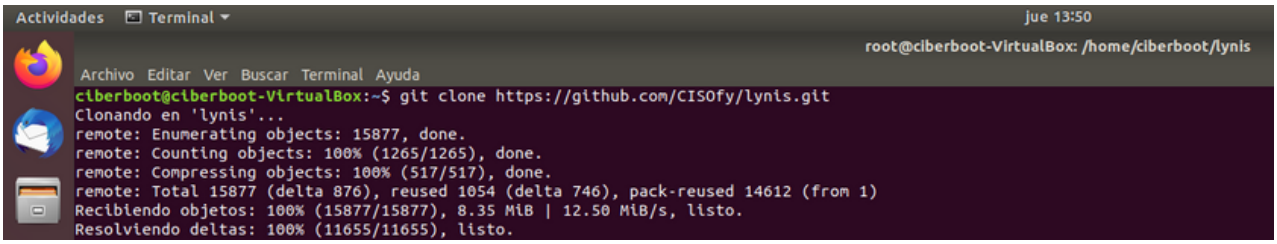
El objetivo principal de Lynis es probar las defensas de seguridad y brindar sugerencias para fortalecer aún más el sistema. Para ello, busca información general del sistema, paquetes de software vulnerables y posibles problemas de configuración. Lo que lo hace idoneo, para que administradores de sistemas y auditores TI, puedan evaluar las defensas de seguridad de sus sistemas y los equipos de una organización.

Para llevar a cabo el análisis de auditoría para esta máquina en primer lugar se ha realizado el inicio de sesión.



Inicio de sesión en el host.

Seguido de la clonación de su repositorio oficial en Github para su uso.



Instalación de Lynis.

Posteriormente al uso de la herramienta a continuación se responden a las preguntas del ejercicio y se adjuntan evidencias de los respuestas:

Responder a las siguientes cuestiones:

1- ¿En qué porcentaje de cumplimiento nos encontramos?

- Nos encontramos en el porcentaje 59 de cumplimiento.

2- ¿Cuántos "Warning" salieron?

- Salieron 3 Warning

3- ¿Cuántas sugerencias?

- Como resultado 52 Sugerencias

Evidencias de las respuestas:

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

  Lynis security scan details:

  Hardening index : 59 [###########         ]
  Tests performed : 283
  Plugins enabled : 2
```

Porcentaje de cumplimiento del host.

```
Archivo  Editar  Ver  Buscar  Terminal  Pestañas  Ayuda
root@ciberboot-VirtualBox: /home/ciberboot/lynis
root@ciberb
================================================================================

  -[ Lynis 3.1.3 Results ]-

  Warnings (3):
  ----------------------------
  ! This version 18.04 is marked end-of-life as of 2023-05-01 [GEN-0010]
      https://cisofy.com/lynis/controls/GEN-0010/

  ! Found one or more vulnerable packages. [PKGS-7392]
      https://cisofy.com/lynis/controls/PKGS-7392/

  ! iptables module(s) loaded, but no rules active [FIRE-4512]
      https://cisofy.com/lynis/controls/FIRE-4512/

  Suggestions (52):
  ----------------------------
  * Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/BOOT-5122/

  * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/KRNL-5820/

  * Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/AUTH-9229/
```

Número de Warnings y Suggestions.

Supervisión de puntos específicos

A continuación utilizando el manual "CIS Ubuntu Linux 18.04 LTS Benchmark v2.2.0 - 03-27-2024" se realizarán los siguientes controles y correcciones en sistema en caso de ser necesario.

1.3.1 - Asegúrese de que las actualizaciones, parches y software de seguridad adicional estén instalados.

2.2.14 - Asegúrese de que el servidor NIS no esté instalado. (De estarlo desinstálelo)

2.2.17 - Asegúrese de que el servicio rsync no esté instalado o esté enmascarado. (De estarlo desinstálelo)

2.3.2 - Asegúrese de que el cliente rsh no esté instalado. (De estarlo desinstálelo)

2.3.3 - Asegúrese de que el cliente talk no esté instalado. (De estarlo desinstálelo)

2.3.6 - Asegúrese de que RPC no esté instalado. (De estarlo desinstálelo)

4.1.2 - Asegúrese de que los permisos en /etc/crontab estén configurados.

4.5.1.1 - Asegúrese de que se haya configurado el número mínimo de días entre cambios de contraseña.

4.5.1.2 - Asegúrese de que la expiración de la contraseña sea de 365 días o menos.

4.5.1.4 - Asegúrese de que el bloqueo de contraseña inactiva sea de 30 días o menos.

6.1.1 - Asegúrese de que los permisos en /etc/passwd estén configurados.

6.1.3 - Asegúrese de que los permisos en /etc/group estén configurados.

- 1.3.1 - Asegúrese de que las actualizaciones, parches y software de seguridad adicional estén instalados.

1.3 Configure Software and Patch Management 130
1.3.1 Ensure updates, patches, and additional security software are installed (Manual) 131

1.3.1 Ensure updates, patches, and additional security software are installed (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Periodically patches are released for included software either due to security flaws or to include additional functionality.

Rationale:

Newer patches may contain security enhancements that would not be available through the latest full update. As a result, it is recommended that the latest software patches be used to take advantage of the latest functionality. As with any software installation, organizations need to determine if a given update meets their requirements and verify the compatibility and supportability of any additional software against the update revision that is selected.

Audit:

Verify there are no updates or patches to install:

```
# apt -s upgrade
```

Remediation:

Run the following command to update all packages following local site policy guidance on applying updates and patches:

```
# apt upgrade
```

OR

```
# apt dist-upgrade
```

References:

1. NIST SP 800-53 Rev. 5: SI-2

La documentación recomienda utilizar el siguiente comando para actualizar los paquetes y parches.

- **Comando**: apt -s upgrade // apt upgrade

```
root@ciberboot-VirtualBox:/home/ciberboot/lynis# apt -s upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  gir1.2-goa-1.0 gir1.2-snapd-1
Utilice «sudo apt autoremove» para eliminarlos.

Enable UA Infra: ESM to receive additional future security updates.
See https://ubuntu.com/18-04 or run: sudo ua status

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Se instalarán los siguientes paquetes NUEVOS:
  ubuntu-advantage-desktop-daemon ubuntu-pro-client ubuntu-pro-client-l10n
Se actualizarán los siguientes paquetes:
  apt apt-utils base-files command-not-found command-not-found-data deja-dup fwupd fwupd-signed gir1.2-notify-0.7 grub-commor
  libapt-pkg5.0 libc-bin libfwupd2 libip4tc0 libip6tc0 libiptc0 libkeyutils1 libklibc libnetplan0 libnotify-bin libnotify4 li
  linux-firmware locales multiarch-support netplan.io nplan python-apt-common python3-apt python3-commandnotfound python3-sof
  software-properties-common software-properties-gtk tcpdump ubuntu-advantage-tools ufw update-manager update-manager-core up
54 actualizados, 3 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
```

```
root@ciberboot-VirtualBox:/home/ciberboot/lynis# apt upgrade -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  gir1.2-goa-1.0 gir1.2-snapd-1
Utilice «sudo apt autoremove» para eliminarlos.

Enable UA Infra: ESM to receive additional future security updates.
See https://ubuntu.com/18-04 or run: sudo ua status

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

- 2.2.14 - Asegúrese de que el servidor NIS no esté instalado. (De estarlo desinstálelo)

2.2 Special Purpose Services **260**
2.2.1 Ensure X Window System is not installed (Automated) 261
2.2.2 Ensure Avahi Server is not installed (Automated) 263
2.2.3 Ensure CUPS is not installed (Automated) 265
2.2.4 Ensure DHCP Server is not installed (Automated) 267
2.2.5 Ensure LDAP server is not installed (Automated) 269
2.2.6 Ensure NFS is not installed (Automated) 271
2.2.7 Ensure DNS Server is not installed (Automated) 273
2.2.8 Ensure FTP Server is not installed (Automated) 275
2.2.9 Ensure HTTP server is not installed (Automated) 277
2.2.10 Ensure IMAP and POP3 server are not installed (Automated) 279
2.2.11 Ensure Samba is not installed (Automated) 281
2.2.12 Ensure HTTP Proxy Server is not installed (Automated) 283
2.2.13 Ensure SNMP Server is not installed (Automated) 285
2.2.14 Ensure NIS Server is not installed (Automated) 287

2.2.14 Ensure NIS Server is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The Network Information Service (NIS) (formally known as Yellow Pages) is a client-server directory service protocol for distributing system configuration files. The NIS server is a collection of programs that allow for the distribution of configuration files.

Rationale:

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed and other, more secure services be used

Audit:

Run the following command to verify `nis` is not installed:

```
# dpkg-query -s nis &>/dev/null && echo "nis is installed"
```

Nothing should be returned.

Remediation:

Run the following command to remove `nis`:

```
# apt purge nis
```

References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-7

Al comprobar si NIS está instalado el resultado es positivo y se procede a su eliminación según la documentación.

- **Comando**: dpkg-query -s nis &>/dev/null && echo "nis is installed"
- **Resultado**: nis is installed.
- **Comando**: apt purge nis
- **Resultado**: Eliminación de Nis.

```
root@ciberboot-VirtualBox:/home/ciberboot/lynis# dpkg-query -s nis &>/dev/null && echo "nis is installed"
nis is installed
root@ciberboot-VirtualBox:/home/ciberboot/lynis# apt purge nis
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  gir1.2-goa-1.0 gir1.2-snapd-1 libtirpc1 rpcbind
Utilice «sudo apt autoremove» para eliminarlos.
Los siguientes paquetes se ELIMINARÁN:
  nis*
0 actualizados, 0 nuevos se instalarán, 1 para eliminar y 0 no actualizados.
Se liberarán 613 kB después de esta operación.
¿Desea continuar? [S/n]
(Leyendo la base de datos ... 174778 ficheros o directorios instalados actualmente.)
Desinstalando nis (3.17.1-1build1) ...
Procesando disparadores para man-db (2.8.3-2ubuntu0.1) ...
(Leyendo la base de datos ... 174704 ficheros o directorios instalados actualmente.)
Purgando ficheros de configuración de nis (3.17.1-1build1) ...
Procesando disparadores para systemd (237-3ubuntu10.57) ...
Procesando disparadores para ureadahead (0.100.0-21) ...
root@ciberboot-VirtualBox:/home/ciberboot/lynis#
```

- 2.2.17 - Asegúrese de que el servicio rsync no esté instalado o esté enmascarado. (De estarlo desinstálelo)

2.2 Special Purpose Services **260**
2.2.1 Ensure X Window System is not installed (Automated) 261
2.2.2 Ensure Avahi Server is not installed (Automated) 263
2.2.17 Ensure rsync service is either not installed or is masked (Automated) 294

2.2.17 Ensure rsync service is either not installed or is masked (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `rsync` service can be used to synchronize files between systems over network links.

Rationale:

The `rsync` service presents a security risk as the `rsync protocol` is unencrypted. The `rsync` package should be removed or if required for dependencies, the `rsync` service should be stopped and masked to reduce the attack area of the system.

Audit:

Run the following command to verify `rsync` is not installed:

```
# dpkg-query -s rsync &>/dev/null && echo "rsync is installed"
```

Nothing should be returned.
-- OR --
Run the following commands to verify that `rsync` is inactive and masked:

```
# systemctl is-active rsync

inactive

# systemctl is-enabled rsync

masked
```

Remediation:

Run the following command to remove `rsync`:

```
# apt purge rsync
```

-- OR --
Run the following commands to stop and mask `rsync`:

```
# systemctl stop rsync

# systemctl mask rsync
```

References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-7

Comprobando que Rsync está instalado y no está enmascarado se procede a su eliminación según el protocolo de la documentación.

- **Comando:** dpkg-query -s rsync &>/dev/null && echo "rsync is installed"
- **Resultado:** rsync is installed
- **Comando:** systemctl is-active rsync
- **Resultado:** inactive
- **Comando:** apt purge rsync
- **Resultado:** Eliminación de Rsync.

```
root@ciberboot-VirtualBox:/home/ciberboot/lynis# dpkg-query -s rsync &>/dev/null && echo "rsync is installed"
rsync is installed
root@ciberboot-VirtualBox:/home/ciberboot/lynis# systemctl is-active rsync
inactive
root@ciberboot-VirtualBox:/home/ciberboot/lynis# systemctl is-enabled rsync
enabled
root@ciberboot-VirtualBox:/home/ciberboot/lynis# apt purge rsync
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  gir1.2-goa-1.0 gir1.2-snapd-1 libtirpc1 rpcbind
Utilice «sudo apt autoremove» para eliminarlos.
Los siguientes paquetes se ELIMINARÁN:
  rsync* ubuntu-standard*
0 actualizados, 0 nuevos se instalarán, 2 para eliminar y 0 no actualizados.
Se liberarán 778 kB después de esta operación.
¿Desea continuar? [S/n]
(Leyendo la base de datos ... 174696 ficheros o directorios instalados actualmente.)
Desinstalando ubuntu-standard (1.417.5) ...
Desinstalando rsync (3.1.2-2.1ubuntu1.6) ...
Procesando disparadores para man-db (2.8.3-2ubuntu0.1) ...
(Leyendo la base de datos ... 174665 ficheros o directorios instalados actualmente.)
Purgando ficheros de configuración de rsync (3.1.2-2.1ubuntu1.6) ...
Procesando disparadores para systemd (237-3ubuntu10.57) ...
Procesando disparadores para ureadahead (0.100.0-21) ...
root@ciberboot-VirtualBox:/home/ciberboot/lynis#
```

- 2.3.2 - Asegúrese de que el cliente rsh no esté instalado. (De estarlo desinstálelo)

2.3 Service Clients **296**
2.3.1 Ensure NIS Client is not installed (Automated) 297
2.3.2 Ensure rsh client is not installed (Automated) 299

2.3.2 Ensure rsh client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `rsh-client` package contains the client commands for the rsh services.

Rationale:

These legacy clients contain numerous security exposures and have been replaced with the more secure SSH package. Even if the server is removed, it is best to ensure the clients are also removed to prevent users from inadvertently attempting to use these commands and therefore exposing their credentials. Note that removing the `rsh-client` package removes the clients for `rsh` , `rcp` and `rlogin` .

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Audit:

Verify `rsh-client` is not installed. Use the following command to provide the needed information:

```
# dpkg-query -s rsh-client &>/dev/null && echo "rsh-client is installed"
```

Nothing should be returned.

Remediation:

Uninstall `rsh`:

```
# apt purge rsh-client
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

Comprobación de la instalación y eliminación de Rsh-Client según la documentación oficial.

- **Comando**: dpkg-query -s rsh-client &>/dev/null && echo "rsh-client is installed"
- **Resultado**: rsh-client is installed
- **Comando**: apt purge rsh-client
- **Resultado**: Eliminación de rsh-client del sistema.

```
root@ciberboot-VirtualBox:/home/ciberboot/lynis# dpkg-query -s rsh-client &>/dev/null && echo "rsh-client is installed"
rsh-client is installed
root@ciberboot-VirtualBox:/home/ciberboot/lynis#  apt purge rsh-client
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  gir1.2-goa-1.0 gir1.2-snapd-1 libtirpc1 rpcbind
Utilice «sudo apt autoremove» para eliminarlos.
Los siguientes paquetes se ELIMINARÁN:
  rsh-client*
0 actualizados, 0 nuevos se instalarán, 1 para eliminar y 0 no actualizados.
Se liberarán 92,2 kB después de esta operación.
¿Desea continuar? [S/n]
(Leyendo la base de datos ... 174663 ficheros o directorios instalados actualmente.)
Desinstalando rsh-client (0.17-17ubuntu0.1) ...
update-alternatives: utilizando /usr/bin/scp para proveer /usr/bin/rcp (rcp) en modo automático
update-alternatives: utilizando /usr/bin/ssh para proveer /usr/bin/rsh (rsh) en modo automático
update-alternatives: utilizando /usr/bin/slogin para proveer /usr/bin/rlogin (rlogin) en modo automático
Procesando disparadores para man-db (2.8.3-2ubuntu0.1) ...
root@ciberboot-VirtualBox:/home/ciberboot/lynis#
```

- 2.3.3 - Asegúrese de que el cliente talk no esté instalado. (De estarlo desinstálelo)

2.3 Service Clients **296**
2.3.1 Ensure NIS Client is not installed (Automated) 297
2.3.2 Ensure rsh client is not installed (Automated) 299
2.3.3 Ensure talk client is not installed (Automated) 301

2.3.3 Ensure talk client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `talk` software makes it possible for users to send and receive messages across systems through a terminal session. The `talk` client, which allows initialization of talk sessions, is installed by default.

Rationale:

The software presents a security risk as it uses unencrypted protocols for communication.

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Audit:

Verify `talk` is not installed. The following command may provide the needed information:

```
# dpkg-query -s talk &>/dev/null && echo "talk is installed"
```

Nothing should be returned.

Remediation:

Uninstall `talk`:

```
# apt purge talk
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

El resultado de la búsqueda del Cliente Talk ha sido positiva y se procede a su eliminación.

- **Comando**: dpkg-query -s talk &>/dev/null && echo "talk is installed"
- **Resultado**: talk is installed
- **Comando**: apt purge talk
- **Resultado**: Eliminación del Cliente Talk

```
root@ciberboot-VirtualBox:/home/ciberboot/lynis# dpkg-query -s talk &>/dev/null && echo "talk is installed"
talk is installed
root@ciberboot-VirtualBox:/home/ciberboot/lynis# apt purge talk
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  gir1.2-goa-1.0 gir1.2-snapd-1 libtirpc1 rpcbind
Utilice «sudo apt autoremove» para eliminarlos.
Los siguientes paquetes se ELIMINARÁN:
  talk*
0 actualizados, 0 nuevos se instalarán, 1 para eliminar y 0 no actualizados.
Se liberarán 55,3 kB después de esta operación.
¿Desea continuar? [S/n]
(Leyendo la base de datos ... 174652 ficheros o directorios instalados actualmente.)
Desinstalando talk (0.17-15build2) ...
Procesando disparadores para man-db (2.8.3-2ubuntu0.1) ...
root@ciberboot-VirtualBox:/home/ciberboot/lynis#
```

- 2.3.6 - Asegúrese de que RPC no esté instalado. (De estarlo desinstálelo)

2.3 Service Clients **296**
2.3.1 Ensure NIS Client is not installed (Automated) 297
2.3.2 Ensure rsh client is not installed (Automated) 299
2.3.3 Ensure talk client is not installed (Automated) 301
2.3.4 Ensure telnet client is not installed (Automated) 303
2.3.5 Ensure LDAP client is not installed (Automated) 305
2.3.6 Ensure RPC is not installed (Automated) 307

2.3.6 Ensure RPC is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Remote Procedure Call (RPC) is a method for creating low level client server applications across different system architectures. It requires an RPC compliant client listening on a network port. The supporting package is rpcbind."

Rationale:

If RPC is not required, it is recommended that this services be removed to reduce the remote attack surface.

Audit:

Run the following command to verify `rpcbind` is not installed:

```
# dpkg-query -s rpcbind &>/dev/null && echo "rpcbind is installed"
```

Nothing should be returned.

Remediation:

Run the following command to remove `rpcbind`:

```
# apt purge rpcbind
```

References:

1. NIST SP 800-53 Rev. 5: CM-7

La comprobación de la instalación de Rpcbind ha dado como resultado positivo y se procede a su eliminación del sistema.

- **Comando**: dpkg-query -s rpcbind &>/dev/null && echo "rpcbind is installed"
- **Resultado**: rpcbind is installed
- **Comando**: apt purge rpcbind
- **Resultado**: Eliminación de Rpcbind.

```
root@ciberboot-VirtualBox:/home/ciberboot/lynis# dpkg-query -s rpcbind &>/dev/null && echo "rpcbind is installed"
rpcbind is installed
root@ciberboot-VirtualBox:/home/ciberboot/lynis# apt purge rpcbind
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  gir1.2-goa-1.0 gir1.2-snapd-1 libtirpc1
Utilice «sudo apt autoremove» para eliminarlos.
Los siguientes paquetes se ELIMINARÁN:
  rpcbind*
0 actualizados, 0 nuevos se instalarán, 1 para eliminar y 0 no actualizados.
Se liberarán 152 kB después de esta operación.
¿Desea continuar? [S/n]
(Leyendo la base de datos ... 174645 ficheros o directorios instalados actualmente.)
Desinstalando rpcbind (0.2.3-0.6ubuntu0.18.04.4) ...
Warning: Stopping rpcbind.service, but it can still be activated by:
  rpcbind.socket
Procesando disparadores para man-db (2.8.3-2ubuntu0.1) ...
(Leyendo la base de datos ... 174632 ficheros o directorios instalados actualmente.)
Purgando ficheros de configuración de rpcbind (0.2.3-0.6ubuntu0.18.04.4) ...
Procesando disparadores para systemd (237-3ubuntu10.57) ...
Procesando disparadores para ureadahead (0.100.0-21) ...
root@ciberboot-VirtualBox:/home/ciberboot/lynis#
```

- 4.1.2 - Asegúrese de que los permisos en /etc/crontab estén configurados.

4 Access, Authentication and Authorization **468**
4.1 Configure time-based job schedulers **469**
4.1.1 Ensure cron daemon is enabled and active (Automated) 470
4.1.2 Ensure permissions on /etc/crontab are configured (Automated) 471

4.1.2 Ensure permissions on /etc/crontab are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/crontab` file is used by `cron` to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file.

Note: Other methods, such as `systemd timers`, exist for scheduling jobs. If another method is used, `cron` should be removed, and the alternate method should be secured in accordance with local site policy

Rationale:

This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` :

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/crontab

Access: (600/-rw-------) Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/crontab` :

```
# chown root:root /etc/crontab
# chmod og-rwx /etc/crontab
```

Default Value:

Access: (644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

Revisando los permisos de configuración de /etc/crontab se ha encontrado que tenía permisos de escritura para grupos y otros. Estos permisos han sido eliminados por seguridad.

- **Comando**: stat -Lc 'Access: (%a/%A) Uid: (%u/ %U) Gid: (%g/ %G)' /etc/crontab
- **Resultado**: Access: (644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)
- **Comando**: chown root:root /etc/crontab // chmod og-rwx /etc/crontab
- **Resultado**: Access: (600/-rw-------) Uid: (0/ root) Gid: (0/ root)

```
root@ciberboot-VirtualBox:/home/ciberboot/lynis# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/crontab
Access: (644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)
root@ciberboot-VirtualBox:/home/ciberboot/lynis# chown root:root /etc/crontab
root@ciberboot-VirtualBox:/home/ciberboot/lynis# chmod og-rwx /etc/crontab
root@ciberboot-VirtualBox:/home/ciberboot/lynis# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/crontab
Access: (600/-rw-------) Uid: ( 0/ root) Gid: ( 0/ root)
root@ciberboot-VirtualBox:/home/ciberboot/lynis#
```

- 4.5.1.1 - Asegúrese de que se haya configurado el número mínimo de días entre cambios de contraseña.

4.5 User Accounts and Environment **577**
4.5.1 Set Shadow Password Suite Parameters **578**
4.5.1.1 Ensure minimum days between password changes is configured (Automated) 579

4.5.1.1 Ensure minimum days between password changes is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PASS_MIN_DAYS` parameter in `/etc/login.defs` allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that `PASS_MIN_DAYS` parameter be set to 1 or more days.

Rationale:

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Audit:

Run the following command and verify `PASS_MIN_DAYS` conforms to site policy (no less than 1 day):

```
# grep PASS_MIN_DAYS /etc/login.defs

PASS_MIN_DAYS 1
```

Run the following command and Review list of users and PAS_MIN_DAYS to Verify that all users' PAS_MIN_DAYS conforms to site policy (no less than 1 day):

```
# awk -F : '(/^[^:]+:[^!*]/ && $4 < 1){print $1 " " $4}' /etc/shadow

No <user>:<PASS_MIN_DAYS> should be returned
```

Remediation:

Set the `PASS_MIN_DAYS` parameter to 1 in `/etc/login.defs`:

```
PASS_MIN_DAYS 1
```

Modify user parameters for all users with a password set to match:

```
# chage --mindays 1 <user>
```

Default Value:

PASS_MIN_DAYS 0

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Comprobando el número mínimo de días para cambiar la contraseña se obtiene el resultado de que el usuario “ciberboot” tiene el valor 0 días. Se ha cambiado la configuración a 15 días desapareciendo éste de los resultados al hacer la consulta.

- **Comando**: awk -F : '(/^[^:]+:[^!*]/ && $4 < 1){print $1 " " $4}' /etc/shadow
- **Resultado**: ciberboot 0
- **Comando**: chage --mindays 15 ciberboot
- **Resultado**: El usuario deberá cambiar la contraseña cada 15 días.

```
root@ciberboot-VirtualBox:/home/ciberboot/lynis# grep PASS_MIN_DAYS /etc/login.defs
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
PASS_MIN_DAYS   0
root@ciberboot-VirtualBox:/home/ciberboot/lynis# awk -F : '(/^[^:]+:[^!*]/ && $4 < 1){print $1 " " $4}' /etc/shadow
ciberboot 0
```

```
root@ciberboot-VirtualBox:/home/ciberboot/lynis# chage --mindays 15 ciberboot
root@ciberboot-VirtualBox:/home/ciberboot/lynis# awk -F : '(/^[^:]+:[^!*]/ && $4 < 1){print $1 " " $4}' /etc/shadow
root@ciberboot-VirtualBox:/home/ciberboot/lynis#
```

- 4.5.1.2 - Asegúrese de que la expiración de la contraseña sea de 365 días o menos.

4.5 User Accounts and Environment **577**
4.5.1 Set Shadow Password Suite Parameters **578**
4.5.1.1 Ensure minimum days between password changes is configured (Automated) 579
4.5.1.2 Ensure password expiration is 365 days or less (Automated) 581

4.5.1.2 Ensure password expiration is 365 days or less (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PASS_MAX_DAYS` parameter in `/etc/login.defs` allows an administrator to force passwords to expire once they reach a defined age.

Rationale:

The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity. It is recommended that the `PASS_MAX_DAYS` parameter does not exceed `365` days and is greater than the value of `PASS_MIN_DAYS`.

Audit:

Run the following command and verify `PASS_MAX_DAYS` conforms to site policy, does not exceed 365 days, and is greater than `PASS_MIN_DAYS`:

```
# grep PASS_MAX_DAYS /etc/login.defs

PASS_MAX_DAYS 365
```

Run the following command and Review list of users and `PASS_MAX_DAYS` to verify that all users' `PASS_MAX_DAYS` conforms to site policy, does not exceed 365 days, and is no less than `PASS_MIN_DAYS`

```
# awk -F: '(/^[^:]+:[^!*]/ && ($5>365 || $5~/([0-1]|-1|\s*)/)){print $1 " " $5}' /etc/shadow

No <user>:<PASS_MAX_DAYS> should be returned
```

Remediation:

Set the `PASS_MAX_DAYS` parameter to conform to site policy in `/etc/login.defs` :

```
PASS_MAX_DAYS 365
```

Modify user parameters for all users with a password set to match:

```
# chage --maxdays 365 <user>
```

Default Value:

PASS_MAX_DAYS 99999

Al realizar si el usuario “ciberboot” tenía la expiración del cambio de contraseña definida en 365 días o menos, se ha encontrado que estaba configurada en 99999 días. La cual se ha procedido al cambio de configuración para cada 180 días.

- **Comando**: awk -F: '(/^[^:]+:[^!*]/ && ($5>365 || $5~/([0-1]|-1|\s*)/)){print $1 " " $5}' /etc/shadow
- **Resultado**: ciberboot 99999
- **Comando**: chage --maxdays 180 ciberboot
- **Resultado**: ciberboot 180

```
root@ciberboot-VirtualBox:/home/ciberboot/lynis# grep PASS_MAX_DAYS /etc/login.defs
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
PASS_MAX_DAYS   99999
root@ciberboot-VirtualBox:/home/ciberboot/lynis# awk -F: '(/^[^:]+:[^!*]/ && ($5>365 || $5~/([0-1]|-1|\s*)/)){print $1 " " $5}' /etc/shadow
ciberboot 99999
root@ciberboot-VirtualBox:/home/ciberboot/lynis# chage --maxdays 180 ciberboot
root@ciberboot-VirtualBox:/home/ciberboot/lynis# awk -F: '(/^[^:]+:[^!*]/ && ($5>365 || $5~/([0-1]|-1|\s*)/)){print $1 " " $5}' /etc/shadow
ciberboot 180
root@ciberboot-VirtualBox:/home/ciberboot/lynis#
```

- 4.5.1.4 - Asegúrese de que el bloqueo de contraseña inactiva sea de 30 días o menos.

4.5 User Accounts and Environment **577**
4.5.1 Set Shadow Password Suite Parameters **578**
4.5.1.1 Ensure minimum days between password changes is configured (Automated) 579
4.5.1.2 Ensure password expiration is 365 days or less (Automated) 581
4.5.1.3 Ensure password expiration warning days is 7 or more (Automated) 583
4.5.1.4 Ensure inactive password lock is 30 days or less (Automated) 585

4.5.1.4 Ensure inactive password lock is 30 days or less (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 30 days after password expiration be disabled.

Rationale:

Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Audit:

Run the following command and verify `INACTIVE` conforms to site policy (no more than 30 days):

```
# useradd -D | grep INACTIVE

INACTIVE=30
```

Verify all users with a password have Password inactive no more than 30 days after password expires:
Run the following command and Review list of users and INACTIVE to verify that all users' INACTIVE conforms to site policy (no more than 30 days):

```
# awk -F: '(/^[^:]+:[^!*]/ && ($7~/(\s*|-1)/ || $7>30)){print $1 " " $7}' /etc/shadow

No <user>:<INACTIVE> should be returned
```

Remediation:

Run the following command to set the default password inactivity period to 30 days:

```
# useradd -D -f 30
```

Modify user parameters for all users with a password set to match:

```
# chage --inactive 30 <user>
```

Default Value:

INACTIVE=-1

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

Al comprobar si el bloqueo de contraseña inactiva estaba definido en 30 días o menos hemos comprobado que el usuario “ciberboot” tenía el valor establecido en -1. Se ha realizado la modificación con el valor de 30 días.

- **Comando**: useradd -D | grep INACTIVE
- **Resultado**: INACTIVE=-1
- **Comando**: awk -F: '(/^[^:]+:[^!*]/ && ($7~/(\s*|-1)/ || $7>30)){print $1 " " $7}' /etc/shadow
- **Resultado:** ciberboot
- **Comando**: useradd -D -f 30
- **Comando**: chage --inactive 30 ciberboot
- **Comando**: awk -F: '(/^[^:]+:[^!*]/ && ($7~/(\s*|-1)/ || $7>30)){print $1 " " $7}' /etc/shadow
- **Resultado:** ciberboot 30

```
root@ciberboot-VirtualBox:/home/ciberboot/lynis# useradd -D | grep INACTIVE
INACTIVE=-1
root@ciberboot-VirtualBox:/home/ciberboot/lynis# awk -F: '(/^[^:]+:[^!*]/ && ($7~/(\s*|-1)/ || $7>30)){print $1 " " $7}' /etc/shadow
ciberboot
root@ciberboot-VirtualBox:/home/ciberboot/lynis# useradd -D -f 30
root@ciberboot-VirtualBox:/home/ciberboot/lynis# chage --inactive 30 ciberboot
root@ciberboot-VirtualBox:/home/ciberboot/lynis# awk -F: '(/^[^:]+:[^!*]/ && ($7~/(\s*|-1)/ || $7>30)){print $1 " " $7}' /etc/shadow
ciberboot 30
root@ciberboot-VirtualBox:/home/ciberboot/lynis# useradd -D | grep INACTIVE
INACTIVE=30
root@ciberboot-VirtualBox:/home/ciberboot/lynis#
```

- 6.1.1 - Asegúrese de que los permisos en /etc/passwd estén configurados.

6 System Maintenance **777**
6.1 System File Permissions **778**
6.1.1 Ensure permissions on /etc/passwd are configured (Automated) 779

6.1.1 Ensure permissions on /etc/passwd are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/passwd` file contains user account information that is used by many system utilities and therefore must be readable for these utilities to operate.

Rationale:

It is critical to ensure that the `/etc/passwd` file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command to verify `/etc/passwd` is mode 644 or more restrictive, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)'  /etc/passwd

Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/passwd`:

```
# chmod u-x,go-wx /etc/passwd
# chown root:root /etc/passwd
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

Realizando la comprobación de permisología del archivo /etc/passw se ha hallado que no estaba configurado correctamente y se ha procedido a solucionarlo mediante la documentación oficial.

- **Comando**: stat -Lc 'Access: (%#a/%A) Uid: (%u/ %U) Gid: (%g/ %G)' /etc/passwd
- **Resultado**: Access: (0777/-rwxrwxrwx) Uid: (0/ root) Gid: (0/ root)
- **Comando**: chmod u-x,go-wx /etc/passwd
- **Comando**: chown root:root /etc/passwd
- **Comando**: stat -Lc 'Access: (%#a/%A) Uid: (%u/ %U) Gid: (%g/ %G)' /etc/passwd
- **Resultado:** Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

```
root@ciberboot-VirtualBox:/home/ciberboot/lynis# stat -Lc 'Access: (%#a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/passwd
Access: (0777/-rwxrwxrwx) Uid: ( 0/ root) Gid: ( 0/ root)
root@ciberboot-VirtualBox:/home/ciberboot/lynis# chmod u-x,go-wx /etc/passwd
root@ciberboot-VirtualBox:/home/ciberboot/lynis#  chown root:root /etc/passwd
root@ciberboot-VirtualBox:/home/ciberboot/lynis# stat -Lc 'Access: (%#a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/passwd
Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)
root@ciberboot-VirtualBox:/home/ciberboot/lynis#
```

- 6.1.3 - Asegúrese de que los permisos en /etc/group estén configurados.

6 System Maintenance **777**
6.1 System File Permissions **778**
6.1.1 Ensure permissions on /etc/passwd are configured (Automated) 779
6.1.2 Ensure permissions on /etc/passwd- are configured (Automated) 781
6.1.3 Ensure permissions on /etc/group are configured (Automated) 783

6.1.3 Ensure permissions on /etc/group are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/group` file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.

Rationale:

The `/etc/group` file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

Audit:

Run the following command to verify `/etc/group` is mode 644 or more restrictive, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/group

Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ root)
```

Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/group`:

```
# chmod u-x,go-wx /etc/group
# chown root:root /etc/group
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

Realizando la comprobación de permisología del archivo /etc/group se ha hallado que no estaba configurado correctamente y se ha procedido a solucionarlo mediante la documentación oficial.

- **Comando**: stat -Lc 'Access: (%#a/%A) Uid: (%u/ %U) Gid: (%g/ %G)' /etc/group
- **Resultado**: Access: (0777/-rwxrwxrwx) Uid: (0/ root) Gid: (0/ root)
- **Comando**: chmod u-x,go-wx /etc/group
- **Comando**: chown root:root /etc/group
- **Comando**: stat -Lc 'Access: (%#a/%A) Uid: (%u/ %U) Gid: (%g/ %G)' /etc/group
- **Resultado:** Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

```
root@ciberboot-VirtualBox:/home/ciberboot/lynis# stat -Lc 'Access: (%#a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/group
Access: (0777/-rwxrwxrwx) Uid: ( 0/ root) Gid: ( 0/ root)
root@ciberboot-VirtualBox:/home/ciberboot/lynis# chmod u-x,go-wx /etc/group
root@ciberboot-VirtualBox:/home/ciberboot/lynis#  chown root:root /etc/group
root@ciberboot-VirtualBox:/home/ciberboot/lynis# stat -Lc 'Access: (%#a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/group
Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)
root@ciberboot-VirtualBox:/home/ciberboot/lynis#
```

Responder a las siguientes cuestiones:

1- ¿En qué rango de cumplimiento nos encontramos tras los cambios realizados?

- Tras los cambios el sistema está en el 63%.

2- ¿Cuántos "Warning" salieron esta vez?

- Salieron 2 Warning

3- ¿Cuántas sugerencias nos quedan por realizar?

- Como resultado 46 Sugerencias

Evidencias de las respuestas:

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

  Lynis security scan details:

  Hardening index : 63 [############        ]
  Tests performed : 279
  Plugins enabled : 2
```

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

  -[ Lynis 3.1.3 Results ]-

  Warnings (2):
  ----------------------------
  ! This version 18.04 is marked end-of-life as of 2023-05-01 [GEN-0010]
      https://cisofy.com/lynis/controls/GEN-0010/

  ! iptables module(s) loaded, but no rules active [FIRE-4512]
      https://cisofy.com/lynis/controls/FIRE-4512/

  Suggestions (46):
  ----------------------------
  * Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/BOOT-5122/

  * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
    - Related resources
      * Website: https://cisofy.com/lynis/controls/KRNL-5820/
```