



SPRINT_22

RETO_HARDENING

1- ANÁLISIS DE LA MÁQUINA LINUX HARDENING

- Se procede a instalar la herramienta Lynis, herramienta usada en auditorías y evaluaciones de seguridad en sistemas Unix y Linux, diseñada para realizar análisis profundos del sistema y generar recomendaciones para mejorar su seguridad.

Del resultado final arrojado por la aplicación, se puede observar que, de las 229 pruebas que se han realizado durante el escaneo del sistema, la evaluación de seguridad del mismo se encuentra bajo, concretamente en un 52 % de cumplimiento (hardening index), recomendándose, en estos casos, la implementación de mejoras

```
Lynis security scan details:
Hardening index : 52 [#####
Tests performed : 229
Plugins enabled : 1
```

Se han detectado un total de 5 warnings o advertencias, siendo posibles vulnerabilidades en el sistema que Lynis detecta durante el escaneo, requiriendo acción inmediata de remediación para no comprometer el sistema

```
Warnings (5):
-----
! Version of Lynis is very old and should be updated [LYNIS]
  https://cisofy.com/controls/LYNIS/

! No password set for single mode [AUTH-9308]
  https://cisofy.com/controls/AUTH-9308/

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

! Couldn't find 2 responsive nameservers [NETW-2705]
  https://cisofy.com/controls/NETW-2705/

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

La herramienta de escaneo ha encontrado un total de 54 suggestions o sugerencias para mejorar la seguridad del sistema, no siendo necesariamente problemas críticos, pero implementarlas, ayudan a obtener una puntuación de hardening index superior, siendo algunas de ellas:

```
Suggestions (54):
-----
* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [CUST-0280]
  https://your-domain.example.org/controls/CUST-0280/

* Install libpam-usb to enable multi-factor authentication for PAM sessions [CUST-0285]
  https://your-domain.example.org/controls/CUST-0285/

* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [CUST-0810]
  https://your-domain.example.org/controls/CUST-0810/

* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [CUST-0811]
  https://your-domain.example.org/controls/CUST-0811/
```

2- APPLICACIÓN DE HARDENING AL SISTEMA - GUIA “CIS_Ubuntu_Linux_18.04 LTS_Benchmark_v2.2.0”

1) 1.3.1- actualizaciones y parches

El perfil aplicable es de nivel 1, por lo que se tratan de recomendaciones de bajo impacto para el sistema, ideales para la mayoría de los entornos, tanto para servidores privados como estaciones de trabajo, sin mermar demasiado el uso y rendimientos del equipo. Este nivel describe que es recomendable tener actualizado el sistema, teniendo en cuenta los requerimientos y verificar la compatibilidad con el resto del software del equipo

AUDITORIA

Se aplica el comando indicado para auditar (sudo apt -s upgrade), encontrando que solo 3 paquetes necesitaban actualizaciones y 2 paquetes que no eran necesarios y habría que eliminarlos con la función “autoremove”

```
ciberboot@ciberboot-VirtualBox:~$ sudo 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.
Se actualizarán los siguientes paquetes:
  python3-update-manager update-manager update-manager-core
3 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Inst python3-update-manager [1:18.04.11.13] (1:18.04.13.1 Ubuntu:18.04/bionic-up
dates [all]) [update-manager-core:amd64 ]
Inst update-manager-core [1:18.04.11.13] (1:18.04.13.1 Ubuntu:18.04/bionic-updat
es [all]) [update-manager:amd64 ]
Inst update-manager [1:18.04.11.13] (1:18.04.13.1 Ubuntu:18.04/bionic-updates [a
ll])
Conf python3-update-manager (1:18.04.13.1 Ubuntu:18.04/bionic-updates [all])
Conf update-manager-core (1:18.04.13.1 Ubuntu:18.04/bionic-updates [all])
Conf update-manager (1:18.04.13.1 Ubuntu:18.04/bionic-updates [all])
ciberboot@ciberboot-VirtualBox:~$
```

REMEDIACIÓN

Actualizar el sistema y eliminar los dos archivos no necesarios con el comando “sudo apt update && sudo apt autoremove”, quedando finalmente:

```
ciberboot@ciberboot-VirtualBox:~$ sudo apt -s upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
ciberboot@ciberboot-VirtualBox:~$
```

2) 2.2.14.- Asegurar que el servidor NIS no esta instalado.

El perfil aplicable es de nivel 1, por lo que se tratan de recomendaciones de bajo impacto para el sistema, ideales para la mayoría de los entornos, tanto para servidores privados como estaciones de trabajo, sin mermar demasiado el uso y rendimientos del equipo. Este nivel describe que es recomendable tener actualizado el sistema, teniendo en cuenta los requerimientos y verificar la compatibilidad con el resto del software del equipo

El protocolo cliente-servidor tiene una colección de programas que permiten la distribución de los archivos de configuración, pero presenta vulnerabilidades frente a ataques DoS, buffer overflow, además de tener una pobre autenticación, siendo generalmente remplazado por el protocolo LDAP, siendo mas seguro y recomendado.

AUDITORÍA

Se realiza la comprobación y se encuentra en el sistema instalado, iniciándose automáticamente en el inicio del equipo:

```
ciberboot@ciberboot-VirtualBox:~$ sudo find / -name nis 2>/dev/null
/etc/apparmor.d/abstractions/nis
/etc/default/nis
/etc/init.d/nis
/snap/core20/1081/etc/apparmor.d/abstractions/nis
/snap/core20/2434/etc/apparmor.d/abstractions/nis
/snap/core22/1663/etc/apparmor.d/abstractions/nis
/snap/core18/2128/etc/apparmor.d/abstractions/nis
/snap/core18/2846/etc/apparmor.d/abstractions/nis
/snap/snapd/21759/usr/lib/snapd/apparmor.d/abstractions/nis
/usr/share/nis
/usr/share/doc/nis
/usr/share/lintian/overrides/nis
```

REMEDIACION

Se elimina del servidor este protocolo de transferencia de configuraciones inseguras.

```
ciberboot@ciberboot-VirtualBox:~$ sudo 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.
  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]
```

```
ciberboot@ciberboot-VirtualBox:~$ sudo apt purge nis
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
El paquete «nis» no está instalado, no se eliminará
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
ciberboot@ciberboot-VirtualBox:~$ █
```

Se comprueba, posteriormente al eliminado, la búsqueda del comando NIS, no apareciendo nada:

```
ciberboot@ciberboot-VirtualBox:~$ sudo find / -name nis 2>/dev/null
ciberboot@ciberboot-VirtualBox:~$
```

3) 2.2.17.- Asegurar que el servicio rsync no esta instalado o este enmascarado. Si es así, debe ser desistalarlo.

El perfil aplicable es de nivel 1, por lo que se tratan de recomendaciones de bajo impacto para el sistema, ideales para la mayoría de los entornos, tanto para servidores privados como estaciones de trabajo, sin mermar demasiado el uso y rendimientos del equipo. Este nivel describe que es recomendable tener actualizado el sistema, teniendo en cuenta los requerimientos y verificar la compatibilidad con el resto del software del equipo.

El servicio “rsync” puede ser usado para sincronizar archivos entre los sistemas en la red, presentando un riesgo de seguridad, ya que el protocolo que utiliza esta desencriptado, por lo que es visible en texto plano. Este servicio debería ser desinstalado o si requiere ser usado, deber pararse y enmascarse para reducir la superficie de ataque del sistema.

AUDITORÍA

Se comprueba que el servicio se encuentra instalado , en funcionamiento pero inactivo y no enmascarado, por lo que se procederá a su desinstalación:

```
ciberboot@ciberboot-VirtualBox:~$ dpkg-query -s rsync &>/dev/null && echo "rsyn
c is installed"
rsync is installed
ciberboot@ciberboot-VirtualBox:~$ systemctl is-active rsync
inactive
ciberboot@ciberboot-VirtualBox:~$ systemctl is-enabled rsync
enabled
ciberboot@ciberboot-VirtualBox:~$ █
```

Además, se observa el archivo, en la ruta “/usr/share/bash-completion/completions/rsync”, el cual, está relacionado con las funciones de auto-completado de Bash para el comando rsync, no afectando directamente a la funcionalidad del sistema, y su presencia no implica que el cliente rsync esté instalado, por lo que no se eliminará del sistema, por si en un futuro se instalase nuevamente la herramienta “rsync”, que tenga disponible la opción de auto-completado activa.

```
ciberboot@ciberboot-VirtualBox:~$ sudo find / -name rsync 2>/dev/null
[sudo] contraseña para ciberboot:
/snap/core20/1081/usr/share/bash-completion/completions/rsync
/snap/core20/2434/usr/share/bash-completion/completions/rsync
/snap/core22/1663/usr/share/bash-completion/completions/rsync
/snap/core18/2128/usr/share/bash-completion/completions/rsync
/snap/core18/2846/usr/share/bash-completion/completions/rsync
/usr/share/bash-completion/completions/rsync
```

REMEDIACIÓN

Se procede a su desinstalación completa, con resultado positivo.

```
ciberboot@ciberboot-VirtualBox:~$ sudo apt purge rsync
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
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] s
(Leyendo la base de datos ... 174669 ficheros o directorios instalados actualmen-
te.)
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 ... 174638 ficheros o directorios instalados actualmen-
te.)
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) ...
ciberboot@ciberboot-VirtualBox:~$ # dpkg-query -s rsync &>/dev/null && echo "rsy-
nc is installed"
ciberboot@ciberboot-VirtualBox:~$ 
```

4) 2.3.2.- Asegurar que el cliente “rsh” no esta instalado y si es así, desistalarlo.

El perfil aplicable es de nivel 1, por lo que se tratan de recomendaciones de bajo impacto para el sistema, ideales para la mayoría de los entornos, tanto para servidores privados como estaciones de trabajo, sin mermar demasiado el uso y rendimientos del equipo. Este nivel describe que es recomendable tener actualizado el sistema, teniendo en cuenta los requerimientos y verificar la compatibilidad con el resto del software del equipo.

El paquete “rsh-client” contiene los comandos del cliente para poder utilizar el servicio “rsh”, los cuales, contienen numerosos riesgos de seguridad, habiendo sido reemplazados por el paquete “SSH”, mucho más seguro.

Deben asegurarse que, en caso de eliminar el servidor, también deben eliminar este paquete de los clientes, debido a que intenten usar estos comandos, sin darse cuenta, exponiendo sus credenciales.

El paquete elimina los clientes “rsh”, “rcp” y “rlogin”, por lo que si están en un entorno de pruebas o de resolución de problemas, hay que tener en cuenta estas premisas y eliminar todo tal cual se ha comentado con la finalidad de evitar accidentes o uso mal intencionado.

AUDITORÍA

Se comprueba que el servicio “rsh-client” se encuentra instalado en el sistema

```
ciberboot@ciberboot-VirtualBox:~$ sudo dpkg-query -s rsh-client &>/dev/null && echo "rsh-client is installed"
[sudo] contraseña para ciberboot:
rsh-client is installed
ciberboot@ciberboot-VirtualBox:~$
```

Se realiza una búsqueda en el sistema, de los posibles clientes que contienen el paquete analizado, encontrándose todos en las mismas rutas del equipo, las cuales, dependen del comando “update-alternatives” que puede haber colocado enlaces simbólicos para estos comandos apuntando a alternativas disponibles en el sistema.

Se comprueban posibles de las dependencias “snap” y “update-alternatives”, no encontrando ninguna que pueda causar problemas al equipo por su desinstalación, no obstante, la aplicación “snap” es un entorno de ejecución, que contiene bibliotecas y dependencias necesarias para ejecutar aplicaciones basadas en Gnome (snap 20), como la calculadora (snap 18), por lo que, teniendo en cuenta que estamos ante un nivel 1 de seguridad, no se desistalarán estos paquetes del sistema.

```
ciberboot@ciberboot-VirtualBox:~$ sudo find / -name rsh 2>/dev/null
/var/lib/dpkg/alternatives/rsh
/etc/alternatives/rsh
/snap/core20/1081/usr/bin/rsh
/snap/core20/2434/usr/bin/rsh
/snap/core22/1663/usr/bin/rsh
/snap/core18/2128/usr/bin/rsh
/snap/core18/2846/usr/bin/rsh
/usr/bin/rsh
/usr/lib/apt/methods/rsh
ciberboot@ciberboot-VirtualBox:~$ sudo find / -name rlogin 2>/dev/null
/var/lib/dpkg/alternatives/rlogin
/etc/alternatives/rlogin
/snap/core20/1081/usr/bin/rlogin
/snap/core20/2434/usr/bin/rlogin
/snap/core22/1663/usr/bin/rlogin
/snap/core18/2128/usr/bin/rlogin
/snap/core18/2846/usr/bin/rlogin
/usr/bin/rlogin
ciberboot@ciberboot-VirtualBox:~$ sudo find / -name rcp 2>/dev/null
/var/lib/dpkg/alternatives/rcp
/etc/alternatives/rcp
/snap/core20/1081/usr/bin/rcp
/snap/core20/2434/usr/bin/rcp
/snap/core22/1663/usr/bin/rcp
/snap/core18/2128/usr/bin/rcp
/snap/core18/2846/usr/bin/rcp
/usr/bin/rcp
ciberboot@ciberboot-VirtualBox:~$ apt-cache depends update-alternatives
E: No se encontró ningún paquete
ciberboot@ciberboot-VirtualBox:~$ apt-cache depends snap
snap
Depende: libc6
```

Por otro lado, encontramos la ruta “/usr/lib/apt/methods/rsh”, usada por el sistema de gestión de paquetes APT, para descargarlos de un servidor remoto a través del protocolo obsoleto RSH. Por ello, se comprueba en el sistema APT si en su listas de fuentes, hay alguna referencia a rsh con resultado negativo por lo que no se eliminará tampoco, por no haber riesgo alguno.

```
GNU nano 2.9.3                               /etc/apt/sources.list

deb cdrom:[Ubuntu 18.04.6 LTS _Bionic Beaver_ - Release amd64 (20210915)]/ bionic main restricted
## or updates from the Ubuntu security team.
deb http://es.archive.ubuntu.com/ubuntu/ bionic-backports main restricted universe multiverse
# deb-src http://es.archive.ubuntu.com/ubuntu/ bionic-backports main restricted universe multiver$


## Uncomment the following two lines to add software from Canonical's
## 'partner' repository.
## This software is not part of Ubuntu, but is offered by Canonical and the
## respective vendors as a service to Ubuntu users.
# deb http://archive.canonical.com/ubuntu bionic partner
# deb-src http://archive.canonical.com/ubuntu bionic partner

[ No se encontró «rsh» ]
^G Ver ayuda      ^O Guardar      ^W Buscar      ^K Cortar Texto  ^J Justificar  ^C Posición
^X Salir          ^R Leer fich.   ^A Reemplazar   ^U Pegar txt    ^I Ortografía ^L Ir a línea
```

REMEDIACIÓN

Se realiza una comprobación de dependencias de este paquete, únicamente encontrando como relevante la librería de uso común “libc6”, la cual no comporta ningún riesgo al sistema, ya que con la aplicación que podría causar algún conflicto es “suidmanager”, y esto no sucederá porque se procederá a desistalar el paquete.

```
ciberboot@ciberboot-VirtualBox:~$ apt-cache depends rsh-client
rsh-client
Depende: libc6
Entra en conflicto: <suidmanager>
Reemplaza: <netstd>
```

```
ciberboot@ciberboot-VirtualBox:~$ sudo apt purge rsh-client
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
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] s
(Leyendo la base de datos ... 174636 ficheros o directorios instalados actualmente.)
Desinstalando rsh-client (0.17-17ubuntu0.1) ...
update-alternatives: utilizando /usr/bin/scp para proveer /usr/bin/rpc (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) ...
```

```
ciberboot@ciberboot-VirtualBox:~$ sudo update-alternatives --remove rsh /usr/bin/ssh
[sudo] contraseña para ciberboot:
ciberboot@ciberboot-VirtualBox:~$ sudo update-alternatives --remove rcp /usr/bin/scp
ciberboot@ciberboot-VirtualBox:~$ sudo update-alternatives --remove rlogin /usr/bin/slogin
```

Como resultado si ahora se busca los nombres de los clientes del paquete rsh, vemos que sólo quedan los que hemos autorizado por no ser riesgo para el sistema.

```
ciberboot@ciberboot-VirtualBox:~$ sudo find / -name rsh -o -name rcp -o -name rlogin 2>/dev/null
/snap/core20/1081/usr/bin/rsh
/snap/core20/1081/usr/bin/rlogin
/snap/core20/1081/usr/bin/rsh
/snap/core20/2434/usr/bin/rcp
/snap/core20/2434/usr/bin/rlogin
/snap/core20/2434/usr/bin/rsh
/snap/core22/1663/usr/bin/rcp
/snap/core22/1663/usr/bin/rlogin
/snap/core22/1663/usr/bin/rsh
/snap/core18/2128/usr/bin/rcp
/snap/core18/2128/usr/bin/rlogin
/snap/core18/2128/usr/bin/rsh
/snap/core18/2846/usr/bin/rcp
/snap/core18/2846/usr/bin/rlogin
/snap/core18/2846/usr/bin/rsh
/usr/lib/apt/methods/rsh
```

5) 2.3.3.- Asegurar que el cliente talk no este instalado, y si lo estuviese, desistalar.

El perfil aplicable es de nivel 1, por lo que se tratan de recomendaciones de bajo impacto para el sistema, ideales para la mayoría de los entornos, tanto para servidores privados como estaciones de trabajo, sin mermar demasiado el uso y rendimientos del equipo. Este nivel describe que es recomendable tener actualizado el sistema, teniendo en cuenta los requerimientos y verificar la compatibilidad con el resto del software del equipo.

El software “talk”, es una aplicación obsoleta que hace posible que los usuarios envíen y reciban mensajes a través del sistema mediante una sesión de terminal, presentando un riesgo de seguridad ya que utiliza protocolos no cifrados en la comunicación, pudiendo ser interceptados por usuarios malintencionados teniendo acceso a información en texto plano.

En el caso que se use en entornos de testing o resolución concreta de problemas, es aconsejable retirar los clientes después de su uso para evitar accidentes o mal uso intencional.

En la actualidad esta aplicación ha sido sustituida por herramientas mas modernas y seguras como:SSH, mensajería instantánea, emails, etc

AUDITORÍA

Se comprueba que se encuentra instalado en el sistema, así como se realiza búsqueda de archivos con el nombre de la aplicación, existiendo varias rutas, casi coincidiendo con las de la misma instalación.

```
ciberboot@ciberboot-VirtualBox:~$ dpkg-query -s talk &>/dev/null && echo "talk is installed"
talk is installed
ciberboot@ciberboot-VirtualBox:~$ sudo find / -name talk 2>/dev/null
[sudo] contraseña para ciberboot:
/var/lib/dpkg/alternatives/talk
/etc/alternatives/talk
/usr/bin/talk
/usr/share/doc/talk
ciberboot@ciberboot-VirtualBox:~$ apt-cache depends talk
```

Se comprueban las dependencias que tiene esta aplicación con el resto del sistema, siendo librerías de uso común, por lo que su desinstalación no tendrá efecto perjudicial en el sistema.

```
ciberboot@ciberboot-VirtualBox:~$ apt-cache depends talk
talk
Depende: libc6
Depende: libncurses5
Depende: libtinfo5
Sugiere: talkd
  inetutils-talkd
Reemplaza: <netstd>
```

REMEDIACIÓN

Se realiza la desinstalación completa de la aplicación “talk”, comprobando, posteriormente, la búsqueda de archivos con el nombre “talk”, sin resultados positivos.

```
ciberboot@ciberboot-VirtualBox:~$ sudo apt autoclean && sudo apt autoremove
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
ciberboot@ciberboot-VirtualBox:~$ sudo find / -name talk 2>/dev/null
ciberboot@ciberboot-VirtualBox:~$
```

6) 2.3.6.- Asegurar que RPC no esté instalado, y en casi afirmativo, desistalarlo.

El perfil aplicable es de nivel 1, por lo que se tratan de recomendaciones de bajo impacto para el sistema, ideales para la mayoría de los entornos, tanto para servidores privados como estaciones de trabajo, sin mermar demasiado el uso y rendimientos del equipo. Este nivel describe que es recomendable tener actualizado el sistema, teniendo en cuenta los requerimientos y verificar la compatibilidad con el resto del software del equipo.

El RCP (llamada por el procedimiento remoto) es un protocolo que permite a los programas ejecutar funciones en sistemas remotos como si fueran locales a través de TCP o UDP, creando aplicaciones cliente-servidor de bajo nivel en diferentes arquitecturas del sistema.

Es un método muy transparente pero contempla una serie de riesgos como es la falta de cifrado, por lo que podrían ser interceptadas las comunicaciones, siendo un método muy antiguo que se sigue usando aun, aunque haya sido sustituido por otros mas modernos como REST o SOAP.

AUDITORÍA

Se comprueba si se encuentra instalado en el sistema, ejecutando “rpcbind” que no se encuentra instalado, pero al realizar una búsqueda por el sistema, encontramos varios archivos pertenecientes a su instalación, a lo mejor por un fallo en la desinstalación o por haberlo hecho solo con “apt remove”.

```
ciberboot@ciberboot-VirtualBox:~$ rpcbind
No se ha encontrado la orden «rpcbind», pero se puede instalar con:
sudo apt install rpcbind
ciberboot@ciberboot-VirtualBox:~$ sudo find / -name rpcbind 2>/dev/null
[sudo] contraseña para ciberboot:
/run/rpcbind
/etc/init.d/rpcbind
/etc/insserv.conf.d/rpcbind
```

Con la finalidad de corregir este fallo, y desistalar de manera completa la aplicación , primero vamos a volver a instalarla y después la eliminaremos con “apt purge”:

```
ciberboot@ciberboot-VirtualBox:~$ sudo apt install rpcbind
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
 libtirpc1
Se instalarán los siguientes paquetes NUEVOS:
 libtirpc1 rpcbind
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 118 kB de archivos.
Se utilizarán 364 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://es.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libtirpc1 amd64 0.2.5-1.2ubuntu0.1 [75,7 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu bionic-updates/main amd64 rpcbind amd64 0.2.3-0.6ubuntu0.18.04.4 [42,1 kB]
Descargados 118 kB en 1s (117 kB/s)
Seleccionando el paquete libtirpc1:amd64 previamente no seleccionado.
(Leyendo la base de datos ... 174619 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../libtirpc1_0.2.5-1.2ubuntu0.1_amd64.deb ...
Desempaquetando libtirpc1:amd64 (0.2.5-1.2ubuntu0.1) ...
Seleccionando el paquete rpcbind previamente no seleccionado.
Preparando para desempaquetar .../rpcbind_0.2.3-0.6ubuntu0.18.04.4_amd64.deb ...
Desempaquetando rpcbind (0.2.3-0.6ubuntu0.18.04.4) ...
Configurando libtirpc1:amd64 (0.2.5-1.2ubuntu0.1) ...
Configurando rpcbind (0.2.3-0.6ubuntu0.18.04.4) ...
Procesando disparadores para libc-bin (2.27-3ubuntu1.6) ...
Procesando disparadores para systemd (237-3ubuntu10.57) ...
Procesando disparadores para man-db (2.8.3-2ubuntu0.1) ...
Procesando disparadores para ureadahead (0.100.0-21) ...
ciberboot@ciberboot-VirtualBox:~$ rpcbind
rpcbind: another rpcbind is already running. Aborting
ciberboot@ciberboot-VirtualBox:~$ sudo systemctl status rpcbind
● rpcbind.service - RPC bind portmap service
   Loaded: loaded (/lib/systemd/system/rpcbind.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-11-18 23:01:47 CET; 18s ago
       Docs: man:rpcbind(8)
   Main PID: 2672 (rpcbind)
      Tasks: 1 (limit: 4656)
     CGroup: /system.slice/rpcbind.service
             └─2672 /sbin/rpcbind -f -w
ciberboot@ciberboot-VirtualBox:~$ sudo apt purge rpcbind
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
 libtirpc1
Utilice «sudo apt autoremove» para eliminarlo.
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] s
(Leyendo la base de datos ... 174637 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 ... 174624 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) ...
ciberboot@ciberboot-VirtualBox:~$ sudo apt autoclean && sudo apt autoremove
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los siguientes paquetes se ELIMINARÁN:
 libtirpc1
0 actualizados, 0 nuevos se instalarán, 1 para eliminar y 0 no actualizados.
Se liberarán 212 kB después de esta operación.
¿Desea continuar? [S/n] s
(Leyendo la base de datos ... 174619 ficheros o directorios instalados actualmente.)
Desinstalando libtirpc1:amd64 (0.2.5-1.2ubuntu0.1) ...
Procesando disparadores para man-db (2.8.3-2ubuntu0.1) ...
Procesando disparadores para libc-bin (2.27-3ubuntu1.6) ...
```

Una vez realizada la desinstalación completa, se procede a comprobar su veracidad, con resultado positivo.

```
ciberboot@ciberboot-VirtualBox:~$ rpcbind
bash: /sbin/rpcbind: No existe el archivo o el directorio
ciberboot@ciberboot-VirtualBox:~$ sudo find / -name rpcbind 2>/dev/null
ciberboot@ciberboot-VirtualBox:~$
```

7) 4.1.2.- Asegurar de que los permisos en /etc/crontab estén configurados.

El perfil aplicable es de nivel 1, por lo que se tratan de recomendaciones de bajo impacto para el sistema, ideales para la mayoría de los entornos, tanto para servidores privados como estaciones de trabajo, sin mermar demasiado el uso y rendimientos del equipo. Este nivel describe que es recomendable tener actualizado el sistema, teniendo en cuenta los requerimientos y verificar la compatibilidad con el resto del software del equipo.

EL servicio “cron”. es un servicio que se ejecuta en segundo plano y gestiona las tareas programadas del archivo /etc/crontab a nivel de sistema, y debe estar estrictamente protegido contra accesos no autorizados que pueda usar maliciosamente las tareas programadas mediante su modificación.

Existen otros métodos, como “systemd timers” para programar tareas y trabajos, por lo que si se usa este método se debe desactivar “cron” y dejar como alternativo al principal

En caso de una mala configuración, podrían brindar a usuarios no autorizados, la capacidad de elevar sus privilegios, obteniendo la capacidad de obtener información sobre el sistema, trabajos que se ejecutando.

AUDITORÍA

Se procede a ejecutar el comando “sudo stat -Lc 'Access: (%a/%A) Uid: (%u/ %U) Gid: (%g/ %G)' /etc/crontab”, para saber el estado en que se encuentra:

```
ciberboot@ciberboot-VirtualBox:~$ sudo stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/crontab
[sudo] contraseña para ciberboot:
Access: (644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)
ciberboot@ciberboot-VirtualBox:~$
```

Como se puede observar tiene la configuración por defecto el crontab, otorgándole al usuario root permisos de escritura y lectura y a otros usuarios le lectura de los archivos. Esta configuración podría permitir a usuarios malintencionados acceder a la lectura de los trabajos almacenados allí (scripts de mantenimiento, copias de seguridad,etc). Por ese motivo, la guía CIS-Benchmark recomienda quitar este privilegio de lectura a usuario no root.

REMEDIACIÓN

Se realiza un cambio de propietario y grupo del archivo “etc/crontab” y un cambio de permisos eliminando cualquier permiso a otros usuarios y su grupo asociado (rwx), quedando finalmente:

```
ciberboot@ciberboot-VirtualBox:~$ sudo chown root:root /etc/crontab
ciberboot@ciberboot-VirtualBox:~$ sudo chmod og-rwx /etc/crontab
ciberboot@ciberboot-VirtualBox:~$ sudo stat -Lc 'Access: (%a/%A) Uid: (%u/%U) Gid: (%g/%G)' /etc/crontab
Access: (600/-rw-----)Uid: (0/ root) Gid: (0/ root)
ciberboot@ciberboot-VirtualBox:~$ ls -l /etc/crontab
-rw----- 1 root root 722 nov 16 2017 /etc/crontab
ciberboot@ciberboot-VirtualBox:~$ stat /etc/crontab
  Fichero: /etc/crontab
  Tamaño: 722           Bloques: 8           Bloque E/S: 4096   fichero regular
Dispositivo: 801h/2049d Nodo-i: 262287      Enlaces: 1
Acceso: (0600/-rw-----) Uid: (0/ root) Gid: (0/ root)
Acceso: 2024-11-19 22:52:47.536000121 +0100
Modificación: 2017-11-16 06:29:19.000000000 +0100
    Cambio: 2024-11-19 23:11:31.801153075 +0100
  Creación: -
```

8) 4.5.1.1.- Asegurar de que se haya configurado el número mínimo de días entre cambios de contraseña.

El perfil aplicable es de nivel 1, por lo que se tratan de recomendaciones de bajo impacto para el sistema, ideales para la mayoría de los entornos, tanto para servidores privados como estaciones de trabajo, sin mermar demasiado el uso y rendimientos del equipo. Este nivel describe que es recomendable tener actualizado el sistema, teniendo en cuenta los requerimientos y verificar la compatibilidad con el resto del software del equipo.

La configuración del parámetro PASS_MIN_DAYS en el archivo “etc/login.defs” permite establecer un número mínimo de días que deben transcurrir antes de que un usuario pueda cambiar su contraseña nuevamente desde el último cambio, siendo una medida de seguridad diseñada para evitar abusos en el sistema de políticas de contraseñas, como evitar utilizar contraseñas prohibidas.

Este archivo regular los parámetros relacionados con las contraseñas y cuentas de usuarios en Linux, especificando el número de días mínimo que deben transcurrir antes que pueda proceder al cambio de contraseña el usuario, si llega al número 0, podrá cambiarla y si tiene un numero mayor, deberá esperar los días correspondientes a ese número.

AUDITORÍA

La configuración correcta de este archivo es importante, ya que, sin esta restricción, un usuario puede cambiar rápidamente su contraseña varias veces para reutilizar una contraseña anterior, lo que puede anular las políticas de reutilización de contraseñas, reduciendo el riesgo de ataques relacionados con cambios de contraseñas.

Además, muchas normativas y estándares de seguridad (como CIS, NIST, o ISO 27001) requieren que las contraseñas tengan un período mínimo antes de ser cambiadas nuevamente.

Por todo lo anterior, se procede a comprobar el numero de días establecidos en el sistema auditado, teniendo el establecido por defecto en el sistema que es “PASS_MIN_DAYS 0”, el cual incumple la normativa de seguridad que debe ser al menos 1, estando el usuario “ciberboot” con la posibilidad de cambiar y reutilizar la contraseña las veces que quiera, mermando la seguridad del sistema.

```
ciberboot@ciberboot-VirtualBox:~$ sudo grep PASS_MIN_DAYS /etc/login.defs
[sudo] contraseña para ciberboot:
#      PASS_MIN_DAYS  Minimum number of days allowed between password changes.
PASS_MIN_DAYS  0
ciberboot@ciberboot-VirtualBox:~$
```

REMEDIACIÓN

Se procede a su concreción , cambiando el PASS_MIN_DAY a 1 m junto con el del usuario “ciberboot”:

```
ciberboot@ciberboot-VirtualBox:~$ sudo PASS_MIN_DAYS 1
sudo: PASS_MIN_DAYS: orden no encontrada
ciberboot@ciberboot-VirtualBox:~$  PASS_MIN_DAYS 1
PASS_MIN_DAYS: orden no encontrada
ciberboot@ciberboot-VirtualBox:~$ sudo nano /etc/login.defs
ciberboot@ciberboot-VirtualBox:~$ sudo  chage --mindays 1 ciberboot
ciberboot@ciberboot-VirtualBox:~$ sudo grep PASS_MIN_DAYS /etc/login.defs
#      PASS_MIN_DAYS  Minimum number of days allowed between password changes.
PASS_MIN_DAYS  1
ciberboot@ciberboot-VirtualBox:~$ sudo awk -F ':|:' '$4 < 1{print
$1 " " $4}' /etc/shadow
ciberboot@ciberboot-VirtualBox:~$
```

9) 4.5.1.2.- Asegurar de que la expiración de la contraseña sea de 365 días o menos.

La configuración correcta de este archivo es importante, ya que, sin esta restricción, un usuario puede cambiar rápidamente su contraseña varias veces para reutilizar una contraseña anterior, lo que puede anular las políticas de reutilización de contraseñas, reduciendo el riesgo de ataques relacionados con cambios de contraseñas.

Continuamos con otro parámetro relacionado con el directorio “/etc/login.defs/”: PASS_MAX_DAYS, permitiendo a los administradores forzar que las contraseñas caduquen una vez llegado el tiempo establecido, permitiendo esta medida prevenir el uso de credenciales no autorizadas obtenidas mediante el empleo de fuerza bruta, ya que su uso estará limitado al tiempo establecido en este parámetro, siendo el vector de ataque mas reducido cuando menor sea la antigüedad de este parámetro.

AUDITORÍA

Se procede a comprobar el estado del sistema “hardening” para ver si este parámetro no supera los 365 días y es mayor que el valor del parámetro PASS_MIN_DAYS, comprobando que no cumple la normativa:

```
#  
# Password aging controls:  
#  
#      PASS_MAX_DAYS      Maximum number of days a password may be used.  
#      PASS_MIN_DAYS      Minimum number of days allowed between password changes.  
#      PASS_WARN_AGE      Number of days warning given before a password expires.  
  
PASS_MAX_DAYS    9999  
PASS_MIN_DAYS    1  
PASS_WARN_AGE    7  
  
ciberboot@ciberboot-VirtualBox:~$ sudo nano /etc/login.defs  
ciberboot@ciberboot-VirtualBox:~$ sudo awk -F: '('/^[:]+:[^!*]/ && ($5>365 || $5~  
/([0-1]-1|\s*/)){print $1 " " $5}' /etc/shadow  
ciberboot 99999  
ciberboot@ciberboot-VirtualBox:~$
```

REMEDIACIÓN

Se modifica el archivo /etc/login.defs, reduciendo el tiempo máximo a 365 días y el mínimo a 7 días, así como se le aplican los nuevos cambios a los usuarios del sistema, en este caso “ciberboot”

```
# Password aging controls:  
#  
#      PASS_MAX_DAYS      Maximum number of days a password may be used.  
#      PASS_MIN_DAYS      Minimum number of days allowed between password changes.  
#      PASS_WARN_AGE      Number of days warning given before a password expires.  
  
PASS_MAX_DAYS    365  
PASS_MIN_DAYS    7  
PASS_WARN_AGE    14  
  
ciberboot@ciberboot-VirtualBox:~$ sudo chage --maxdays 365 ciberboot  
ciberboot@ciberboot-VirtualBox:~$ grep PASS_MAX_DAYS /etc/login.defs  
#      PASS_MAX_DAYS      Maximum number of days a password may be used.  
PASS_MAX_DAYS    365  
ciberboot@ciberboot-VirtualBox:~$ sudo awk -F: '('/^[:]+:[^!*]/ && ($5>365 || $5~  
/([0-1]-1|\s*/)){print $1 " " $5}' /etc/shadow  
ciberboot 365  
ciberboot@ciberboot-VirtualBox:~$
```

10) 4.5.1.4.- Asegurar que el bloqueo de contraseña inactiva sea igual o menor a 30 días.

La configuración correcta de este archivo es importante, ya que, sin esta restricción, un usuario puede cambiar rápidamente su contraseña varias veces para reutilizar una contraseña anterior, lo que puede anular las políticas de reutilización de contraseñas, reduciendo el riesgo de ataques relacionados con cambios de contraseñas.

Las cuentas de usuario que han estado inactivas durante un período de tiempo determinado, deben ser desactivadas automáticamente, siendo recomendable, para cuentas que estén inactivas durante 30 días, después de haber expirado la contraseña.

AUDITORÍA

Las cuentas inactivas representan una amenaza para la seguridad del sistema, ya que evita que cuentas no utilizadas permanezcan activas indefinidamente, lo que podría ser explotado por atacantes.

Vamos a comprobar si el sistema hardening cumple con las políticas del CIS en esta materia, siendo su valor recomendado en establecer un máximo de 30 días de inactividad antes que la cuenta sea bloqueada:

```
ciberboot@ciberboot-VirtualBox:~$ sudo useradd -D | grep INACTIVE
[sudo] contraseña para ciberboot:
INACTIVE=-1
ciberboot@ciberboot-VirtualBox:~$ sudo awk -F: '(/^[:]+:[^!*]/ && ($7~/(\s*-1)
/ || $7>30)){print $1 " " $7}' /etc/shadow
ciberboot
```

Como se puede observar, el usuario ciberboot tiene la cuenta inactiva y no existe límite establecido como periodo de inactividad.

REMEDIACIÓN

Se procede a remediar este punto conforme a las políticas establecidas por el CIS, indicando 30 días como periodo de inactividad y se lo vamos a aplicar a todos los usuarios:

```
ciberboot@ciberboot-VirtualBox:~$ useradd -D -f 30
useradd: no se puede crear un nuevo archivo de preferencias predeterminadas
ciberboot@ciberboot-VirtualBox:~$ sudo useradd -D -f 30
ciberboot@ciberboot-VirtualBox:~$ sudo chage --inactive 30 ciberboot
ciberboot@ciberboot-VirtualBox:~$ sudo useradd -D | grep INACTIVE
INACTIVE=30
ciberboot@ciberboot-VirtualBox:~$ sudo awk -F: '(/^[:]+:[^!*]/ && ($7~/(\s*-1)
/ || $7>30)){print $1 " " $7}' /etc/shadow
ciberboot 30
ciberboot@ciberboot-VirtualBox:~$
```

11) 6.1.1.- Asegurar que permisos en el directorio /etc/passwd esten configurados.

La configuración correcta de este archivo es importante, ya que, sin esta restricción, un usuario puede cambiar rápidamente su contraseña varias veces para reutilizar una contraseña anterior, lo que puede anular las políticas de reutilización de contraseñas, reduciendo el riesgo de ataques relacionados con cambios de contraseñas.

El archivo “/etc/passwd” es un componente crítico de los sistemas operativos basados en UNIX y Linux, conteniendo información sobre las cuentas de usuario en el sistema, incluyendo nombres de usuario, identificadores de usuario (UID), identificadores de grupo (GID), información del usuario, directorios de inicio y shells predeterminados

Este archivo debe ser accesible a todas las cuentas del sistema porque es utilizado por muchas utilidades, pudiendo ser modificado únicamente por usuarios autorizados, ya que esto podría permitir la creación de cuentas maliciosas, manipulación de información de usuarios legítimos y escalamiento de privilegios en el sistema por usuarios maliciosos.

AUDITORÍA

Se procede a la verificación del estado del directorio “etc/passwd” para comprobar si cumple con los entandares establecidos en la guía CIS, encontrándose mal configurado con permisos totales para todos los usuarios:

```
ciberboot@ciberboot-VirtualBox:~$ sudo stat -Lc 'Access: (%#a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/passwd
[sudo] contraseña para ciberboot:
Access: (0777/-rwxrwxrwx) Uid: ( 0/ root) Gid: ( 0/ root)
```

REMEDIACIÓN

Se procede a modificar los permisos y adecuarlos para mejorar la seguridad del sistema:

```
ciberboot@ciberboot-VirtualBox:~$ sudo chmod 644 /etc/passwd
ciberboot@ciberboot-VirtualBox:~$ sudo chown root:root /etc/passwd
ciberboot@ciberboot-VirtualBox:~$ sudo stat -Lc 'Access: (%#a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/passwd
Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)
```

12) 6.1.3.- Asegurar que los permisos en “/etc/group” estén bien configurados.

La configuración correcta de este archivo es importante, ya que, sin esta restricción, un usuario puede cambiar rápidamente su contraseña varias veces para reutilizar una contraseña anterior, lo que puede anular las políticas de reutilización de contraseñas, reduciendo el riesgo de ataques relacionados con cambios de contraseñas.

El archivo “/etc/group” es otro archivo fundamental en los sistemas basados en Unix/Linux y define los grupos de usuarios del sistema, proporcionando una forma de gestionar permisos y accesos a recursos compartidos.

Cada grupo puede tener uno o más usuarios, y estos grupos se utilizan para asignar permisos de acceso a archivos, directorios u otros recursos.

AUDITORIA

Se comprueba si el directorio “/etc/group” si cumple con los permisos necesarios para mantener una postura de seguridad adecuada en el sistema, según los estándares del CIS, resultando tener permisos plenos para todos los usuarios, pudiendo ser usada esta mala configuración por usuarios maliciosos que accedan al sistema:

```
ciberboot@ciberboot-VirtualBox:~$ stat -Lc 'Access: (%#a/%A) U
id: ( %u/ %U) Gid: ( %g/ %G)' /etc/group
Access: (0777/-rwxrwxrwx)Uid: ( 0/ root) Gid: ( 0/ root)
```

REMEDIACION

Se procede a modificar los permisos establecidos para realizar una configuración segura del directorio analizado:

```
ciberboot@ciberboot-VirtualBox:~$ sudo chown root:root /etc/gr
oup
[sudo] contraseña para ciberboot:
ciberboot@ciberboot-VirtualBox:~$ sudo chmod 644 /etc/group
ciberboot@ciberboot-VirtualBox:~$ stat -Lc 'Access: (%#a/%A) U
id: ( %u/ %U) Gid: ( %g/ %G)' /etc/group
Access: (0644/-rw-r--r--)Uid: ( 0/ root) Gid: ( 0/ root)
```

3- RE-ANÁLISIS DEL SISTEMA LINUX-HARDENING - IMPLEMENTACIÓN DE RECOMENDACIONES DE LA GUÍA “CIS_Ubuntu_Linux_18.04_LTS_Benchmark_v2.2.0”

- Se procede nuevamente a utilizar la herramienta Lynis, diseñada para realizar análisis profundos del sistema y generar recomendaciones para mejorar su seguridad.

Del resultado final arrojado por la aplicación, se puede observar que, de las 225 pruebas que se han realizado durante el escaneo del sistema, la evaluación de seguridad del mismo se encuentra aun baja (0-60 -bajo), concretamente en un 57 % de cumplimiento (hardening index), recomendándose seguir en esta linea de implementación de mejoras del sistema, ya que aplicando 12 de las 282 mejoras de seguridad que recomienda el CIS Ubuntu Linux 18.04 LTS Benchmark (03/07/24) la implementación de mejoras, se ha conseguido aumentar un 5% del hardening index, por lo que, aplicando la lógica, podríamos llegar a cumplir el 100% del cumplimiento si implementaríamos todas las medidas.

```
Lynis security scan details:

Hardening index : 57 [#####
Tests performed : 225
Plugins enabled : 1
```

Se han detectado un total de 4 warnings o advertencias, una menos que al análisis anterior, por lo que la linea de implementación CIS esta haciendo su cometidos pero , sigue siendo necesario continuar con las acciones de remediación.

```
Warnings (4):
-----
! Version of Lynis is very old and should be updated [LYNIS]
  https://cisofy.com/controls/LYNIS/

! No password set for single mode [AUTH-9308]
  https://cisofy.com/controls/AUTH-9308/

! Couldn't find 2 responsive nameservers [NETW-2705]
  https://cisofy.com/controls/NETW-2705/

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

El warnings que ha sido remediado es:

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

La herramienta de escaneo ha encontrado un total de 51 suggestions o sugerencias para mejorar la seguridad del sistema, ayudando a obtener una puntuación de hardening index superior, obteniendo 3 sugerencias menos que en el primer análisis.

4- CONCLUSIONES

Las guías como CIS Ubuntu Linux Benchmark permiten realizar mejoras de seguridad de manera organizada y prioritaria, con un enfoque basado en niveles, los cuales, aseguran que las configuraciones de menor impacto se implementen primero, evitando interrupciones significativas en la operatividad del sistema.

Ademas, están diseñadas para ser aplicables tanto a servidores críticos como a estaciones de trabajo, permitiendo una mejora de la seguridad sin comprometer el rendimiento general, lo que es especialmente útil en ambientes mixtos.

La implementación basada en estándares reconocidos, ayuda a mitigar riesgos al identificar configuraciones inseguras, servicios obsoletos y vulnerabilidades comunes.

Las auditorías periódicas permiten detectar vulnerabilidades que podrían surgir tras actualizaciones, cambios de configuración o la instalación de nuevos servicios, siendo cruciales herramientas como Lynis, para evaluar el estado de seguridad inicial y los avances logrados tras aplicar remediaciones en el sistema, permitiendo con sus informes desarrollar planes de acción más efectivos, priorizando las áreas de mayor riesgo del sistema.

En definitiva, aunque se logró un avance significativo, del 52% al 57% en el hardening index, únicamente con la aplicación de 4,22% del total de las medidas paleteadas por la guía CIS, por lo que si implementáramos el 100% se alcanzaría el 100% de cumplimiento.

No obstante, hay que recordar que una postura de seguridad óptima requiere un esfuerzo constante, dado que la seguridad no es un estado estático, sino un objetivo dinámico, siendo esencial tratarlo desde un enfoque holístico y adaptarse rápidamente a la evolución de las técnicas de ataque, manteniendo actualizado con nuevas guías y herramientas el sistema.