

Seguridad en Linux:

Buenas prácticas de hardening

"Linux Hardening Básico" es una guía práctica para mejorar la seguridad en sistemas Linux (Ubuntu/Debian) mediante configuraciones esenciales como firewall, control de accesos y monitoreo.



Víctor Suárez Cruz

27/01/2025
Técnico de Sistemas

Índice

Introducción.....	2
Contexto Técnico.....	3
Justificación de Herramientas.....	3
1. Actualización y limpieza del sistema.....	4
Ejecuta estos comandos para asegurarte de que el sistema está actualizado y eliminar paquetes innecesarios:.....	4
2. Configuración del firewall (UFW).....	6
Configuramos el firewall para permitir solo tráfico esencial como SSH:.....	6
3. Configuración segura de SSH.....	8
Edita el archivo de configuración de SSH:.....	8
Modifica o asegúrate de tener estas configuraciones:.....	8
4. Control de usuarios y permisos.....	9
Revisamos usuarios y deshabilitamos cuentas innecesarias:.....	9
Cambiamos permisos críticos en archivos del sistema:.....	9
5. Monitoreo y auditoría de logs.....	10
Instalamos y configuramos herramientas de monitoreo:.....	10
Podemos automatizar reportes de seguridad con:.....	10

Introducción

En un mundo cada vez más conectado, los sistemas Linux son una pieza clave en infraestructuras críticas, servidores y aplicaciones. Sin embargo, su popularidad también los convierte en un objetivo atractivo para los atacantes. Este informe se centra en las buenas prácticas de hardening, un proceso esencial para reducir vulnerabilidades y fortalecer la seguridad del sistema operativo.

El propósito de este documento es proporcionar una guía paso a paso para principiantes y administradores de sistemas, ayudándoles a proteger sus servidores Linux contra posibles amenazas. Las configuraciones propuestas abarcan desde el endurecimiento del acceso SSH hasta la monitorización de eventos, con un enfoque práctico y adaptable.

Contexto Técnico

Este documento está dirigido a:

- Estudiantes de administración de sistemas y ciberseguridad que buscan aprender prácticas básicas de seguridad.
- Administradores de sistemas interesados en mejorar la protección de sus servidores.
- Entusiastas de Linux que deseen aplicar configuraciones seguras en sus entornos personales.

Justificación de Herramientas

En cada etapa del proceso de hardening se han utilizado herramientas y configuraciones ampliamente reconocidas por su eficacia y simplicidad:

- UFW (Uncomplicated Firewall): Ideal para configurar reglas básicas de firewall de manera rápida y sencilla, especialmente en sistemas Ubuntu/Debian.
- Logwatch: Permite generar reportes automáticos y detallados de eventos críticos registrados en los logs del sistema.
- SSH: Configurar un acceso seguro es esencial para evitar intentos de acceso no autorizado y fortalecer la autenticación.
- Gestión de permisos de archivos: Garantiza que los datos sensibles no sean accesibles por usuarios no autorizados

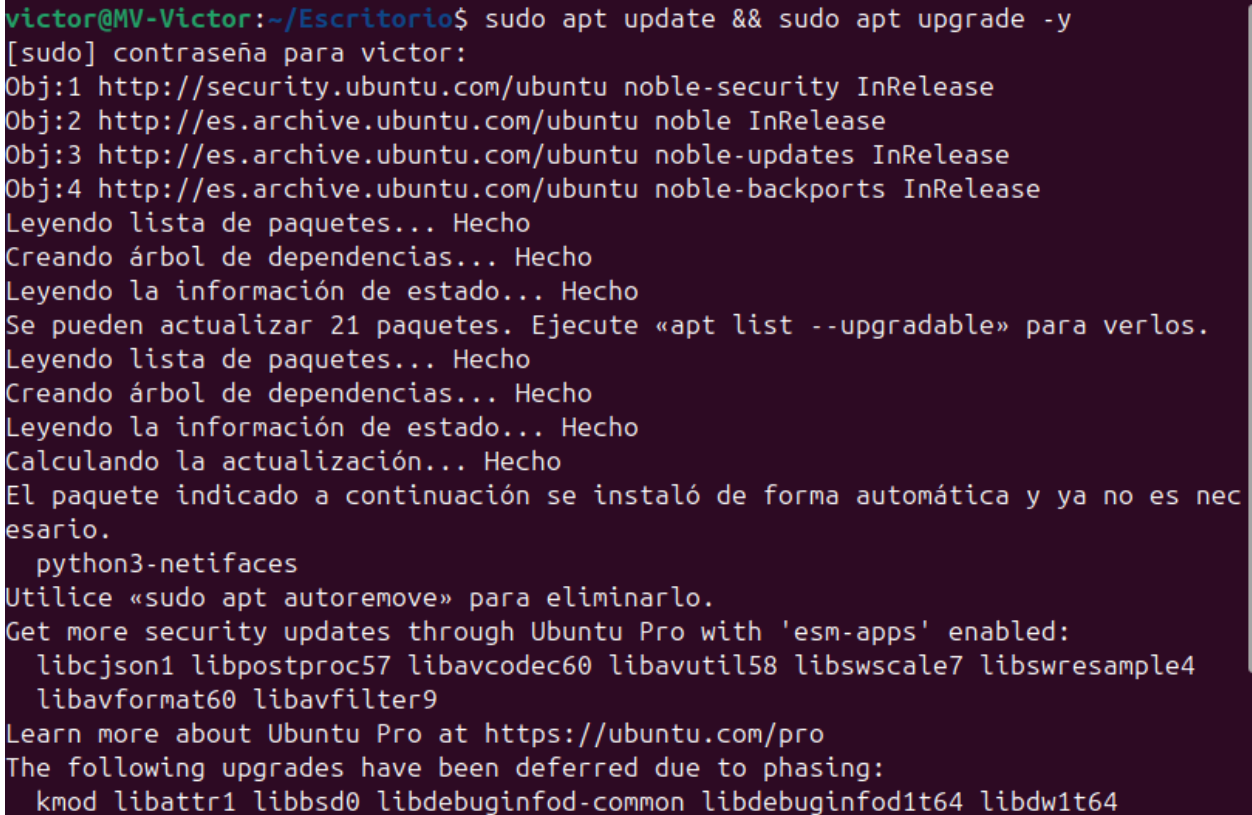
1. Actualización y limpieza del sistema

Ejecuta estos comandos para asegurarte de que el sistema está actualizado y eliminar paquetes innecesarios:

Actualizar el sistema



```
1 sudo apt update && sudo apt upgrade -y
```



```
victor@MV-Victor:~/Escritorio$ sudo apt update && sudo apt upgrade -y
[sudo] contraseña para victor:
Obj:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Obj:2 http://es.archive.ubuntu.com/ubuntu noble InRelease
Obj:3 http://es.archive.ubuntu.com/ubuntu noble-updates InRelease
Obj:4 http://es.archive.ubuntu.com/ubuntu noble-backports InRelease
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 21 paquetes. Ejecute «apt list --upgradable» para verlos.
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
  python3-netifaces
Utilice «sudo apt autoremove» para eliminarlo.
Get more security updates through Ubuntu Pro with 'esm-apps' enabled:
  libcjson1 libpostproc57 libavcodec60 libavutil58 libswscale7 libswresample4
  libavformat60 libavfilter9
Learn more about Ubuntu Pro at https://ubuntu.com/pro
The following upgrades have been deferred due to phasing:
  kmod libattr1 libbsd0 libdebuginfod-common libdebuginfod1t64 libdw1t64
```

Eliminar paquetes innecesarios



1 sudo apt autoremove -y

```
victor@MV-Victor:~/Escritorio$ sudo apt autoremove -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los siguientes paquetes se ELIMINARÁN:
  python3-netifaces
0 actualizados, 0 nuevos se instalarán, 1 para eliminar y 21 no actualizados.
Se liberarán 58,4 kB después de esta operación.
(Leyendo la base de datos ... 150747 ficheros o directorios instalados actualmen
te.)
Desinstalando python3-netifaces:amd64 (0.11.0-2build3) ...
```




1 sudo apt autoclean

```
victor@MV-Victor:~/Escritorio$ sudo apt autoclean
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
```

2. Configuración del firewall (UFW)

Configuramos el firewall para permitir solo tráfico esencial como SSH:


Denegar todas las conexiones entrantes



```
1 sudo ufw default deny incoming
```

```
victor@MV-Victor:~/Escritorio$ sudo ufw default deny incoming
La política incoming predeterminada cambió a «deny»
(asegúrese de actualizar sus reglas consecuentemente)
```

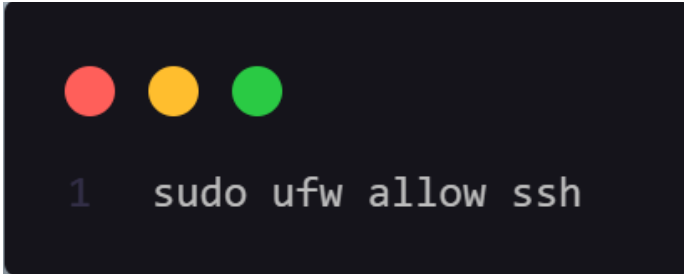
Permitir todas las conexiones salientes



```
1 sudo ufw default allow outgoing
```

```
victor@MV-Victor:~/Escritorio$ sudo ufw default allow outgoing
La política outgoing predeterminada cambió a «allow»
(asegúrese de actualizar sus reglas consecuentemente)
```

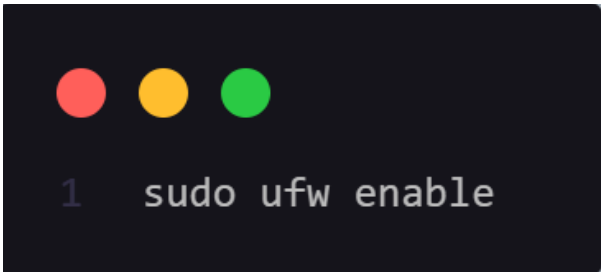
Permitir SSH



```
1 sudo ufw allow ssh
```

```
victor@MV-Victor:~/Escritorio$ sudo ufw allow ssh
Reglas actualizadas
Reglas actualizadas (v6)
```

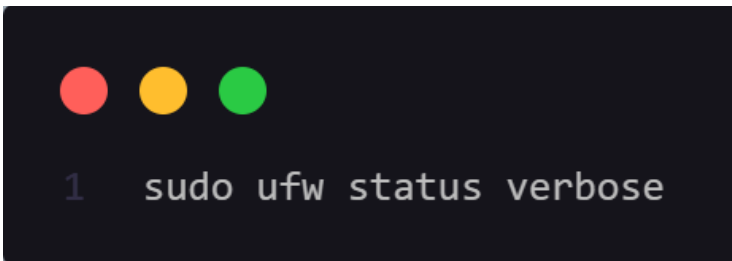
Habilitar el firewall



```
1 sudo ufw enable
```

```
victor@MV-Victor:~/Escritorio$ sudo ufw enable
El cortafuegos está activo y habilitado en el arranque del sistema
```

Verificación del estado



```
1 sudo ufw status verbose
```

```
victor@MV-Victor:~/Escritorio$ sudo ufw status verbose
Estado: activo
Acceso: on (low)
Predeterminado: deny (entrantes), allow (salientes), disabled (enrutados)
Perfiles nuevos: skip

Hasta          Acción      Desde
-----
22/tcp         ALLOW IN    Anywhere
22/tcp (v6)    ALLOW IN    Anywhere (v6)
```


3. Configuración segura de SSH

Edita el archivo de configuración de SSH:



```
1 sudo nano /etc/ssh/sshd_config
```

```
victor@MV-Victor:~/Escritorio$ sudo nano /etc/ssh/sshd_config
```

Modifica o asegúrate de tener estas configuraciones:

```
# Evita login directo con root
```

```
PermitRootLogin no
PasswordAuthentication no
PermitEmptyPasswords no
MaxAuthTries 3
```

```
# Usar solo llaves SSH, no
contraseñas
```


```
# No permitir contraseñas
vacías
```

```
# Máximo de intentos antes
de bloquear
```

4. Control de usuarios y permisos

Revisamos usuarios y deshabilitamos cuentas innecesarias:

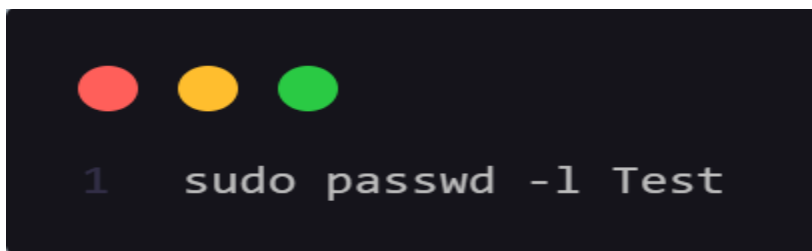
Ver lista de usuarios en el sistema



```
1 cut -d: -f1 /etc/passwd
```

```
victor@MV-Victor:~/Escritorio$ cut -d: -f1 /etc/passwd
```

Bloquear una cuenta innecesaria (ejemplo usuario 'test')

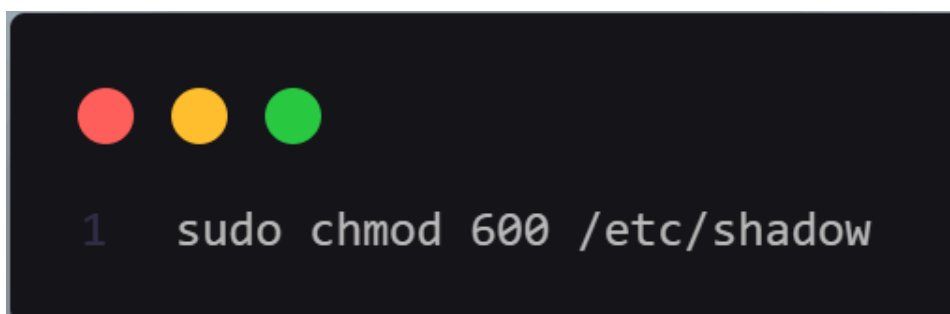


```
1 sudo passwd -l Test
```

```
victor@MV-Victor:~/Escritorio$ sudo passwd -l Test
passwd: contraseña cambiada.
```

Cambiamos permisos críticos en archivos del sistema:

Proteger contraseñas de usuarios



```
1 sudo chmod 600 /etc/shadow
```

```
victor@MV-Victor:~/Escritorio$ sudo chmod 600 /etc/shadow
```

Configuración de usuarios accesible solo para lectura




```
1 sudo chmod 644 /etc/shadow
```

```
victor@MV-Victor:~/Escritorio$ sudo chmod 644 /etc/passwd
```

5. Monitoreo y auditoría de logs

Instalamos y configuramos herramientas de monitoreo:


Instalar logwatch para revisar logs automáticamente



```
1 sudo apt install logwatch -y
```

```
victor@MV-Victor:~/Escritorio$ sudo apt install logwatch -y
```

Revisar los logs de inicio de sesión fallidos



```
1 sudo cat /var/log/auth.log | grep "Failed password"
```

```
victor@MV-Victor:~/Escritorio$ sudo cat /var/log/auth.log | grep "Failed password"
```

Podemos automatizar reportes de seguridad con:

```
victor@MV-Victor:~/Escritorio$ sudo logwatch --detail High --mailto email@dominio.com --range
```