

396 - LINUX Y UBUNTU

Revisa tu servidor SSH con ssh-audit en Ubuntu

Audita tu propio servidor SSH, detecta algoritmos antiguos y deja una configuración más robusta.



NIVEL
Avanzado

TIEMPO
30 min

CATEGORÍA
Linux y Ubuntu

WEB
soporteinformatico360.com

Muchos servidores SSH siguen aceptando cifrados antiguos o el acceso con contraseña. Con ssh-audit puedes revisar tu propio equipo y ver qué mejorar, igual que haría un auditor, pero solo en lo que es tuyo.

■ Qué necesitas

- ✓ Ubuntu con OpenSSH Server instalado
- ✓ Un usuario con permisos sudo
- ✓ Acceso físico o una segunda sesión abierta
- ✓ Permiso si el servidor no es tuyo

■ Paso a paso

01

Instala la herramienta

ssh-audit está en los repositorios de Ubuntu. Instálala con apt.

```
Terminal
$ sudo apt update
$ sudo apt install ssh-audit
$
```

02

Audita tu propio equipo

Lanza el análisis contra tu servidor. Verás en rojo y amarillo los algoritmos que conviene retirar.

```
Terminal
$ ssh-audit localhost
$
```

03

Revisa la configuración activa

Comprueba si se permite entrar con contraseña o como root. Lo ideal es usar claves y no permitir el acceso directo de root.

```
Terminal
$ sudo sshd -T | grep -Ei 'password auth|permitroot'
$
```

04

Aplica los cambios con cuidado

Crea un archivo propio en `/etc/ssh/sshd_config.d/` con tus ajustes, por ejemplo `PermitRootLogin no`. Así no tocas el archivo original.

`endurecer.conf`

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

05

Comprueba y reinicia

Valida la sintaxis antes de reiniciar el servicio. Si `sshd -t` no muestra errores, ya puedes aplicar.

`Terminal`

```
$ sudo sshd -t
$ sudo systemctl restart ssh
$ █
```

06

Vuelve a auditar

Ejecuta de nuevo `ssh-audit` y compara. Prueba a entrar desde otra sesión antes de cerrar la que tienes abierta.

■ Consejos

CONSEJO 1

Desactiva la contraseña solo cuando tu clave SSH ya funcione.

CONSEJO 2

Mantén siempre una sesión abierta mientras cambias la configuración.

CONSEJO 3

Repite la auditoría tras cada actualización importante.



Importante: Audita solo servidores propios o con permiso por escrito: analizar sistemas ajenos sin autorización es delito. Si te quedas fuera del servidor, necesitarás acceso físico o la consola del proveedor.

¿Prefieres que lo hagamos por ti?

Diagnóstico sin compromiso y presupuesto cerrado antes de empezar. soporte@soporteinformatico360.com
En taller, a domicilio en Madrid o por asistencia remota. soporteinformatico360.com

910 117 112