Linux Security Hardening Script

Un script de endurecimiento de seguridad completo y listo para la producción para sistemas Debian/Ubuntu. Implementa automáticamente las mejores prácticas de seguridad, crea usuarios administradores seguros y configura herramientas de monitoreo de nivel empresarial.

Perfecto para servidores, estaciones de trabajo y máquinas virtuales. Trabaja de forma interactiva o totalmente automatizada.

Características

- **Totalmente automatizado** - Se ejecuta sin interacción del usuario (opcional)
- **Creación automática de usuarios:** crea un usuario administrador seguro con un nombre de usuario aleatorio
- **Endurecimiento integral** - 29 pasos de endurecimiento de seguridad
- **Escaneo** de **seguridad** - Lynis, RKHunter, integración de AIDE
- **Registro detallado** - Cada acción documentada
- **Seguro para volver a correr** - Se puede ejecutar varias veces de forma segura
- **VPS-Safe** - Prueba cuentas antes de deshabilitar root
- **Retroceso** automático - Revierte en errores de configuración de SSH
- **Zero Dependencies** - Solo utiliza herramientas integradas
- **Works** Offline - No se requiere Internet después de la instalación del paquete

¿Qué se endurece?

Seguridad del sistema

- Endurecimiento SSH (deshabilitar el inicio de sesión de root, autenticación de solo tecla, restricciones de puerto)

- Configuración de firewall (Fail2Ban para protección contra fuerza bruta SSH)
- Parámetros del núcleo (endurecimiento de sysctl)
- Permisos de archivo (archivos sensibles protegidos)
- Políticas de la cuenta de usuario (envejecimiento de contraseñas, requisitos de calidad)
- Deshabilitar servicios y protocolos de red innecesarios
- Restricciones de acceso del compilador
- Prevención de volcado de núcleo

Monitoreo y detección

- Monitorización de integridad de archivos (AIDE)
- Detección de rootkit (RKHunter)
- Auditoría del sistema (auditado con reglas integrales)
- Escaneo de seguridad (Lynis)
- Contabilidad de procesos
- Monitorización y rotación de registros

Control de acceso

- Configuración PAM (calidad de contraseña, historial)
- Restricciones de grupo de sudo
- Su restricciones de comando (grupo de ruedas)
- Tiempos de espera de sesión
- Banners legales

Seguridad de la red

- Cookies de TCP SYN
- Reenvío de IP desactivado
- ICMP redirección deshabilitada
- Enrutamiento de origen desactivado
- Filtrado de ruta inversa
- Endurecimiento IPv6

Requisitos previos

Requerido

- **OS:** Debian 10+ o Ubuntu 18.04+
- **Usuario** : Acceso a la raíz (sudo)
- **Disk**Disco: ~500MB espacio libre para troncos y paquetes

Para servidores remotos (VPS)

- **Claves de SSH**: Root debe tener las teclas SSH configuradas
    - Si no, usa --local-vmBandera para pruebas
- **Acceso:** Mantén abierta la sesión actual de SSH durante las pruebas

Para máquinas virtuales locales/estaciones de trabajo

- Sin requisitos especiales
- Uso --local-vmBandera para omitir las comprobaciones de teclas SSH

https://github.com/Z-A-P-P-I-T/Debian-Ubuntu-Security-Hardening-Script/blob/main/debian-ubuntu-hardening-script.sh

```
sudo apt install git -y
```

```
git clone https://github.com/Z-A-P-P-I-T/Debian-Ubuntu-Security-Hardening-Script.git
```

```
chmod +x debian-ubuntu-hardening-script.sh
```

```
sudo ./debian-ubuntu-hardening-script.sh
```

El script de *hardening* está diseñado para aumentar la seguridad, y uno de sus pasos iniciales (paso 1 de 29) es **deshabilitar la autenticación con contraseña para el usuario root a través de SSH** (o deshabilitar completamente el acceso de root por SSH).

Para que esto no te bloquee fuera del servidor, el script exige que primero configures la **autenticación basada en claves SSH (SSH keys).**

Dado que estamos trabajando en una **VirtualBox**, que es un entorno de prueba local (VM), el script te proporciona una bandera (flag) de línea de comandos para **saltarte esta verificación de seguridad** y continuar con el resto de los pasos de endurecimiento.

Acción Requerida: Vuelve a ejecutar el script, pero añadiendo el argumento --local-vm.

```
sudo ./debian-ubuntu-hardening-script.sh --local-vm
```

Al usar esta opción, el script asumirá que no necesitas las claves SSH configuradas para root y procederá con los 28 pasos de endurecimiento restantes.