Improved_harden_linux

El script **improved_harden_linux.sh** es una herramienta semi-automatizada para el endurecimiento de la seguridad de sistemas Linux (especialmente Debian/Ubuntu), buscando la conformidad con estándares como DISA STIG y CIS.

1. Pasos Guiados para la Instalación y Ejecución

Sigue estos pasos para obtener, preparar y ejecutar el script en tu sistema.

A. Preparación del Script

1. **Descargar el Script:** Utiliza el comando wget para obtener la última versión del script desde el repositorio de GitHub:

```
wget https://raw.githubusercontent.com/captainzero93/security_harden_linux/main/improved_harden_linux.sh
```

2. **Otorgar Permisos de Ejecución:** Haz que el archivo descargado sea ejecutable usando chmod:

```
chmod +x improved_harden_linux.sh
```

B. Ejecución y Aplicación (Modo Recomendado)

3. **Realizar una Prueba (Dry Run) - Recomendado:** Antes de aplicar cualquier cambio, es crucial previsualizar lo que hará el script. Esto muestra un informe detallado (**verbose**) sin modificar el sistema:

```
sudo ./improved_harden_linux.sh --dry-run -v
```

El registro de la salida del *script* de endurecimiento de seguridad (improved_harden_linux.sh) muestra que la **simulación** (o **dry-run**) se ejecutó **completamente** y **exitosamente** sin realizar cambios reales en el sistema.

El *script* se ejecutó en **modo de simulación** (--dry-run) con **verbosidad** (-v) y nivel de seguridad **moderado.**

Parámetros Clave

Parámetro	**Valor**	**Descripción**
Security Level	moderate	Nivel de endurecimiento aplicado (en una ejecución real).
Desktop Mode	true	Indica que se tuvo en cuenta el entorno gráfico (GNOME).
Dry Run	true	**Importante:** Solo simulación; no se aplicaron cambios reales.
Interactive	true	Indica que el *script* solicitaría interacción (en una ejecución real).
Executed modules	21	Todos los módulos de endurecimiento se simularon.

Módulos Ejecutados (Simulados)

Se simularon **21 módulos** de seguridad. Para cada módulo, el registro muestra: [INFO] [DRY RUN] Would X... y luego [SUCCESS] Module Y completed. Esto confirma que el *script* recorrió todas las etapas planeadas sin encontrar errores de sintaxis o lógica, y que **simularía** las siguientes acciones:

- **Actualizaciones:** Actualizar el sistema y configurar actualizaciones de seguridad automáticas.
- **Auditoría y Escaneo:** Configurar auditd, ejecutar Lynis, instalar *scanners* de *rootkits* y AIDE (integridad de archivos).
- **Red y Conexión:** Endurecer **SSH**, configurar ajustes de **IPv6**, configurar el *firewall* **UFW** y Fail2Ban.
- **Sistema y Kernel:** Asegurar la memoria compartida, configurar parámetros de *kernel* (sysctl), asegurar la configuración de *boot*.
- **Control de Acceso:** Configurar políticas de **contraseñas** fuertes, asegurar el acceso de **root**, configurar políticas de dispositivos **USB** y deshabilitar sistemas de archivos sin usar.

- **Software de Seguridad:** Instalar **ClamAV** y configurar **AppArmor**.
- **Utilidades:** Configurar sincronización de tiempo (**NTP**) y remover paquetes innecesarios.

Resultado Final

El *script* finalizó con:

- [SUCCESS] Security hardening completed!
- [INFO] Report: /root/security_hardening_report_20251110_084835.html

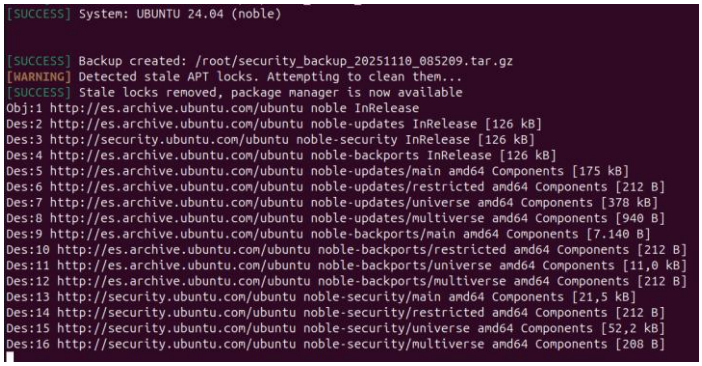
El resultado general es que la **prueba en seco fue exitosa** para todos los módulos, y se generó un **informe de seguridad** simulado en /root/security_hardening_report_20251110_084835.html.

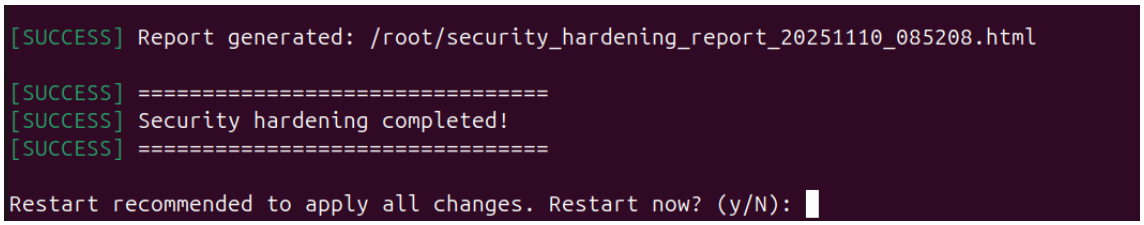
Siguiente Paso

Si está satisfecho con el resultado de la simulación, el siguiente paso sería ejecutar el *script* **sin** la opción --dry-run para aplicar realmente los cambios de endurecimiento.

4. **Ejecutar e Instalar:** Ejecuta el script con permisos de superusuario (sudo). Por defecto, utiliza el nivel de seguridad **Moderado** y se ejecuta en modo **interactivo**:

```
sudo ./improved_harden_linux.sh
```





5. **Interacción:** Durante la ejecución, el script te **pedirá confirmación** para ciertas funcionalidades de escritorio (como IPv6, mDNS, KDE Connect o Samba) que podría deshabilitar por seguridad. Responde según tus necesidades.
6. **Reiniciar:** Una vez que el script finalice, deberás **reiniciar el sistema** para que las nuevas configuraciones del kernel y otros servicios surtan efecto completo:

```
sudo reboot
```

NOTA IMPORTANTE (Servidores Remotos): Si estás endureciendo un servidor remoto, **debes** configurar y probar las claves SSH antes de ejecutar el script. Un alto nivel de seguridad podría bloquear la autenticación por contraseña, impidiendo tu acceso si no tienes una clave configurada. Para servidores, se sugiere un nivel de seguridad alto y no interactivo:

```
sudo ./improved_harden_linux.sh -l high -n
```

2. Opciones de Uso (Flags) y Niveles de Seguridad

El script ofrece varias opciones de línea de comando para personalizar la ejecución, incluyendo niveles de seguridad y selección de módulos.

A. Opciones de Línea de Comando Principales

Puedes combinar estas opciones para afinar el proceso de endurecimiento:

- **Seleccionar Nivel de Seguridad (-l o --level):**
    - Establece el nivel de protección deseado. Los niveles disponibles son: low (baja), moderate (moderada, por defecto), high (alta) y paranoid (paranoico).
    - *Ejemplo:* sudo ./improved_harden_linux.sh -l high
- **Modo No Interactivo (-n o --non-interactive):**
    - Ejecuta el script sin detenerse a hacer preguntas, útil para la automatización.
    - *Ejemplo:* sudo ./improved_harden_linux.sh -n
- **Habilitar Módulos Específicos (-e o --enable):**
    - Permite ejecutar **solo** los módulos de seguridad indicados (separados por comas).
    - *Ejemplo:* sudo ./improved_harden_linux.sh -e firewall,ssh_hardening
- **Deshabilitar Módulos Específicos (-x o --disable):**
    - Permite omitir ciertos módulos que no deseas aplicar.
    - *Ejemplo:* sudo ./improved_harden_linux.sh -x clamav,aide
- **Restaurar el Sistema (-r o --restore):**
    - Utiliza la copia de seguridad creada automáticamente por el script para revertir los cambios.
    - *Ejemplo:* sudo ./improved_harden_linux.sh --restore
- **Generar Informe (-R o --report):**
    - Realiza una auditoría del estado actual de seguridad del sistema sin aplicar ningún cambio.
    - *Ejemplo:* sudo ./improved_harden_linux.sh --report

B. Niveles de Seguridad del Script

Elige el nivel de seguridad en función del uso de tu sistema:

1. **Low (Baja):**
    - Proporciona una protección básica, ideal para entornos de aprendizaje o desarrollo.

- *Incluye:* Reglas de firewall sencillas, endurecimiento de SSH (mantiene la autenticación por contraseña).

2. **Moderate (Moderado - Por Defecto):**
    - Nivel de seguridad equilibrado, recomendado para **usuarios de escritorio** y la mayoría de los casos de uso general.
    - *Incluye:* Firewall completo, **Fail2Ban**, auditd (registro de auditoría) y endurecimiento básico del kernel.
3. **High (Alta):**
    - Seguridad fuerte, ideal para **servidores de producción** y usuarios con altas exigencias de seguridad.
    - *Incluye:* Todo lo de Moderado, más endurecimiento del kernel más estricto y restricciones en el acceso a dispositivos USB.
4. **Paranoid (Paranoico):**
    - Máxima seguridad. **No recomendado para sistemas de escritorio** debido a las severas restricciones.
    - *Incluye:* El endurecimiento más agresivo del kernel, tiempo de espera de Zero GRUB y las restricciones USB más estrictas.