Lynis Auditoría de Seguridad

¿QUÉ ES LYNIS?

Lynis es una herramienta de **auditoría de seguridad** ampliamente utilizada en entornos **Unix** y **Linux**, diseñada para evaluar el **estado de seguridad de un sistema de manera automatizada.** A diferencia de otros escáneres de vulnerabilidades que se enfocan principalmente en redes o aplicaciones web, **Lynis** se centra en el **análisis interno del sistema operativo**, permitiendo identificar: **configuraciones incorrectas, malas prácticas, servicios inseguros y otros aspectos que pueden representar un riesgo.**

Esta herramienta es especialmente útil para **administradores de sistemas**, **auditores de seguridad** y **profesionales de ciberseguridad** que buscan una manera **rápida y detallada de evaluar el nivel de protección de un servidor o equipo local.** Además, es de código abierto, lo que facilita su revisión, modificación y adaptación a distintos entornos y políticas de seguridad.

Al ejecutar **Lynis**, se realiza un **análisis profundo de múltiples áreas del sistema**, incluyendo **autenticación de usuarios, permisos de archivos, servicios en ejecución, configuración del kernel, registros del sistema, políticas de contraseñas, y más.** Al finalizar, genera un informe con **recomendaciones específicas** para endurecer la seguridad del sistema, acompañado de un índice de seguridad que permite medir su estado de forma cuantitativa.

Gracias a su enfoque modular, **Lynis** permite ejecutar **auditorías completas** o centrarse en **categorías específicas**, como: **autenticación, redes o detección de malware.** Esto lo convierte en una herramienta flexible y eficiente tanto para auditorías rutinarias como para investigaciones más detalladas tras un incidente de seguridad.

En resumen, **Lynis** es una **solución robusta, práctica y altamente recomendable para mantener y fortalecer la seguridad en sistemas basados en Unix/Linux.**

Objetivo de la auditoría con Lynis

El objetivo principal de utilizar **Lynis** es identificar **posibles debilidades en la configuración de un sistema Linux y proporcionar recomendaciones que permitan mejorar su nivel de seguridad**. Esto incluye: la detección de servicios innecesarios, permisos mal configurados, ausencia de mecanismos de protección y otras vulnerabilidades que podrían ser aprovechadas por atacantes.

Áreas evaluadas por Lynis

Lynis realiza un análisis exhaustivo de diversas áreas clave del sistema operativo, entre las que se incluyen:

1. Configuraciones del sistema (*kernel*, archivos de configuración, *logs*).
2. Gestión de usuarios y autenticación.
3. Servicios de red y protocolos inseguros.
4. Aplicación de actualizaciones y parches.
5. Políticas de contraseñas y permisos.
6. Herramientas de detección de intrusos (IDS/IPS).
7. Sistemas de archivos y auditoría de *logs*.
8. *Software* instalado y posibles *backdoors*.

Resultados del análisis

Al finalizar la auditoría, **Lynis** entrega un informe que incluye:

1. Advertencias (*Warnings*): problemas detectados que requieren atención inmediata.

2. Sugerencias (*Suggestions*): recomendaciones para fortalecer la seguridad.
3. Índice de endurecimiento (*Hardening Index*): una puntuación que refleja el nivel de seguridad del sistema, sobre un máximo de 100.
4. Estos resultados permiten priorizar acciones y establecer un plan de mejora continua en la seguridad del sistema auditado.

Beneficios de usar Lynis

1. **Automatización**: permite realizar auditorías sin intervención manual.
2. **Rapidez y eficiencia**: el análisis completo se realiza en pocos minutos.
3. **No utiliza agentes externos**: no requiere instalación de componentes adicionales en el sistema.
4. **Personalizable**: se puede enfocar en áreas específicas según los intereses del auditor.
5. **Compatibilidad:** funciona en la mayoría de las distribuciones *Linux* y sistemas *Unix*.

Limitaciones de Lynis

Aunque **Lynis** es una herramienta muy útil, también tiene ciertas limitaciones:

- No detecta vulnerabilidades en aplicaciones *web* (como SQLi o XSS).
- No sustituye un escáner de red externo, ya que se centra únicamente en el sistema local.
- Las recomendaciones son genéricas, y es el auditor quien debe interpretarlas y aplicarlas según el contexto.

Buenas prácticas tras el análisis

Después de una auditoría con **Lynis**, se recomienda:

1. Revisar detalladamente el informe generado.
2. Priorizar la corrección de advertencias antes que las sugerencias.
3. Aplicar actualizaciones de seguridad pendientes.
4. Establecer una política de auditorías periódicas con seguimiento de mejoras.
5. Integrar los hallazgos en una estrategia de *hardening* y monitoreo continuo.

Comandos útiles de Lynis

Lynis se ejecuta desde la terminal y cuenta con una serie de comandos y opciones que permiten personalizar la auditoría según las necesidades del usuario. A continuación, se presentan los comandos más relevantes:

Pasos para Instalar y Ejecutar Lynis

1. Instalar Lynis

Asegúrate de que tu lista de paquetes esté actualizada y luego instala Lynis:

```
# Actualizar la lista de paquetes
sudo apt update

# Instalar el paquete Lynis
sudo apt install lynis -y
```

2. Ejecutar la Auditoría del Sistema

Una vez que la instalación finalice, el comando lynis estará disponible, y podrás ejecutar la auditoría:

```
sudo lynis audit system
```

El proceso de auditoría tardará un momento, ya que Lynis revisará cientos de configuraciones de seguridad en tu Ubuntu 24.04 y, al finalizar, te dará una puntuación de seguridad, junto con sugerencias para mejorar el endurecimiento (*hardening*) de tu sistema.

1. Auditoría completa del sistema

```
sudo lynis audit system
```

Este es el **comando principal**. Ejecuta una **auditoría integral del sistema**, evaluando todas las áreas disponibles, como: autenticación, servicios de red, *logs*, *kernel*, permisos, entre otros.

2. Auditoría rápida (modo no interactivo)

```
sudo lynis audit system --quick
```

Realiza una **auditoría automática y silenciosa**, sin solicitar confirmaciones. Es útil para integrarlo en scripts o tareas programadas.

3. Mostrar todas las pruebas disponibles

```
sudo lynis show tests
```

Muestra una lista completa de pruebas que **Lynis** puede ejecutar. Sirve para identificar áreas específicas del sistema que se pueden auditar.

4. Ejecutar pruebas por grupo de seguridad

```
sudo lynis audit system --tests-from-group "authentication"
```

Permite ejecutar solo un grupo específico de pruebas, como "authentication", "filesystems", "malware", "networking", entre otros. Es útil para auditorías focalizadas.

5. Ver grupos de pruebas disponibles

```
sudo lynis show groups
```

Muestra todos los grupos temáticos de pruebas que **Lynis** soporta, para facilitar auditorías parciales.

6. Guardar los resultados en un archivo
Los resultados se almacenan automáticamente en:

```
/var/log/lynis.log  /var/log/lynis-report.dat
```

7. Actualizar Lynis

```
sudo lynis update info
```

Mantener **Lynis** actualizado es importante para asegurar que las auditorías consideren las amenazas más recientes.

Resumen de los hallazgos más importantes, divididos por Advertencias (Warnings), Peligros (Dangers), y algunas Sugerencias (Suggestions) clave:

Advertencias (Warnings) y Peligros (Dangers) Críticos

Estos son los hallazgos que requieren tu atención inmediata para mejorar la seguridad.

Tipo	Módulo	Descripción (ES)	Acción Recomendada
PELIGRO	Usuarios	Permisos para el directorio: /etc/sudoers.d	Verifica los permisos de este directorio. Los permisos incorrectos podrían permitir a usuarios no autorizados modificar las reglas de sudo, escalando privilegios. Debería ser propiedad de root y tener permisos restrictivos como 0755 (o más restrictivos como 0750).
PELIGRO	Paquetes	Paquetes vulnerables encontrados (PKGS-7392).	Ejecuta sudo apt update && sudo apt upgrade para aplicar todas las actualizaciones de seguridad disponibles y corregir las vulnerabilidades en los paquetes.
PELIGRO	Correo	Divulgación de información en el banner SMTP (MAIL-8818).	Configura Postfix para ocultar la versión y el nombre del sistema operativo en el banner SMTP (el saludo inicial del servidor de correo). Puedes modificar la configuración de Postfix (smtpd_banner).
PELIGRO	Firewall	Módulos iptables cargados, pero sin reglas activas (FIRE-4512).	Tenemos el módulo del firewall cargado, pero no hay reglas para filtrar el tráfico. Debemos configurar un firewall (como ufw o iptables) y asegurarnos de que esté activo y con reglas para restringir las conexiones entrantes (y salientes si es necesario).
PELIGRO	Impresoras	Permisos de archivo de configuración	Revisar y corregir los permisos para el archivo de configuración de CUPS

Tipo	Módulo	Descripción (ES)	Acción Recomendada
		CUPS son un peligro.	**(probablemente /etc/cups/cupsd.conf u otros archivos relacionados). Deben ser restrictivos para evitar modificaciones no autorizadas.**
PELIGRO	**Logging**	**Archivos eliminados en uso (ARCHIVOS ENCONTRADOS).**	**Esto es común después de las actualizaciones de paquetes, pero indica que los procesos están usando archivos que han sido eliminados del disco, lo que podría impedir que se apliquen las correcciones de seguridad. Por lo general, requiere un reinicio de los servicios afectados o del sistema completo.**

Sugerencias de Seguridad Importantes (Suggestions)

Estas son áreas clave para mejorar el endurecimiento (hardening) del sistema:

1. Sistema Base y Kernel

- Kernel Hardening (Bastionado del kernel): Hay muchas configuraciones de sysctl que difieren de los valores recomendados por Lynis (DIFERENTE). Debes revisar y aplicar los valores sugeridos por Lynis para parámetros como:
    - kernel.kptr_restrict (para restringir la visibilidad de las direcciones del kernel).
    - net.ipv4.conf.all.accept_redirects y net.ipv4.conf.all.send_redirects (para prevenir ataques Man-in-the-Middle).
    - fs.suid_dumpable (para controlar la creación de core dumps para binarios SUID).
- GRUB2: Se encontró GRUB2 pero no tiene protección de contraseña (NINGUNO). Asegura GRUB con una contraseña para

prevenir que usuarios no autorizados modifiquen los parámetros de arranque.

2. Usuarios y Autenticación

- Cuentas sin fecha de caducidad: Se encontraron cuentas que no tienen una fecha de caducidad (Accounts without expire date [SUGERENCIA]). Establecer la caducidad puede ser una buena práctica de seguridad, especialmente para cuentas temporales.
- Métodos de hash de contraseñas (Password hashing methods [SUGERENCIA]): Asegúrate de que estás utilizando un algoritmo de hash de contraseñas fuerte (como yescrypt, argon2 o sha512) y que se han configurado suficientes rondas de hash (que está deshabilitado: Checking password hashing rounds [DESHABILITADO]).
- UMASK: Revisa y establece un valor umask por defecto más restrictivo en /etc/login.defs para los nuevos archivos y directorios creados.

3. Sistema de Ficheros

- Puntos de montaje separados (/home, /tmp, /var): Lynis sugiere tener puntos de montaje separados para /home, /tmp y /var ([SUGERENCIA]). Esto permite aplicar opciones de montaje restrictivas como nodev, noexec, y nosuid para limitar los vectores de ataque.
- Montaje /proc (hidepid): Se sugiere montar /proc con la opción hidepid para ocultar los procesos de otros usuarios, lo cual es una mejora de seguridad importante.

4. Software y Entorno

- Plugins de Debian (Recomendados): Instala las herramientas sugeridas para la gestión de paquetes:
  - libpam-tmpdir
  - apt-listbugs
  - apt-listchanges
  - needrestart (para saber qué servicios reiniciar después de una actualización).
- Firewall avanzado: Considera instalar y configurar fail2ban para proteger los servicios expuestos, como Apache o SSH (aunque SSH no está corriendo, es una buena práctica).

Resumen de Pasos Inmediatos

1. Actualiza el sistema: Ejecuta sudo apt update && sudo apt upgrade para abordar la vulnerabilidad de paquetes.
2. Corrige los permisos de sudoers: Revisa y corrige los permisos de /etc/sudoers.d (debe ser root:root con permisos 0755 o 0750).
3. Configura el Firewall: Instala y activa ufw o configura reglas de iptables de manera apropiada (por ejemplo, permitir solo el puerto 80/443 para Apache y bloquear el resto por defecto).
4. Asegura GRUB: Establece una contraseña para GRUB.
5. Reinicia si es necesario: Si el sistema ha estado corriendo mucho tiempo después de actualizaciones grandes, un reinicio podría eliminar los "Archivos eliminados en uso".
6. Oculta el Banner de Postfix: Modifica main.cf de Postfix para cambiar el smtpd_banner.

[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

- TIP (Consejo): Lynis te está ofreciendo una recomendación proactiva.
- Enhance Lynis audits (Mejora las auditorías de Lynis): Te sugiere cómo hacer que las auditorías sean más relevantes y personalizadas para tu entorno.
- By adding your settings to custom.prf (Añadiendo tu configuración a custom.prf): Te anima a crear un archivo de configuración personalizado. Esto es clave.
- See /etc/lynis/default.prf for all settings (Consulta /etc/lynis/default.prf para toda la configuración): Te indica dónde puedes ver todas las opciones que puedes anular o añadir.

¿Por qué es útil el custom.prf?

En lugar de modificar el archivo de configuración principal de Lynis (default.prf), que podría ser sobrescrito por una

actualización, el archivo custom.prf es el lugar recomendado para:

1. Ignorar pruebas: Si hay una prueba que es irrelevante para tu caso (por ejemplo, una configuración de seguridad que no aplica a tu máquina virtual), puedes desactivarla para que no aparezca como sugerencia o advertencia en cada auditoría.
2. Añadir pruebas personalizadas: Puedes incluir tus propios scripts o controles de seguridad específicos para tu organización o servidor.
3. Mantener la limpieza: Te permite mantener tus personalizaciones separadas de la configuración por defecto.

Pasos para Implementar el TIP

Si quieres empezar a usar esta función:

1. Crear el Archivo de Configuración Personalizado

Simplemente crea el archivo si no existe:

```
sudo touch /etc/lynis/custom.prf
```

2. Mover las Sugerencias a custom.prf

Busca las pruebas que te parezcan irrelevantes o que ya sabes que no vas a solucionar, y añádelas al archivo custom.prf usando la directiva skip-test.

Ejemplo Práctico:

Lynis nos sugirió que la versión es antigua: * This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]

Si decidimos ignorar esta comprobación hasta que tengamos tiempo de actualizar, añadiríamos esta línea a /etc/lynis/custom.prf:

Ignorar el aviso de que la versión de Lynis es antigua (se actualizará más tarde)

skip-test = LYNIS

La próxima vez que ejecutes sudo lynis audit system, ya no veremos ese mensaje.