



Auditoria en Servidores Linux

PARTE II

HERRAMIENTA GRATUITA



x



HENRIQUE ALVES

Contenido

Introducción - Parte 2	3
Auditoría Seguridad Fase 2 - Auditoría servidores Linux con “Lynis”	4
1. Instalación de Lynis en Entornos Ubuntu.....	4
2. Métodos de Instalación de Lynis.....	5
2.1 Instalación desde el repositorio GitHub.....	5
2.2 Instalación a través del gestor de paquetes APT	5
3. Ejecución de la Auditoría de Seguridad con Lynis.....	5
3.2 Ejemplo de Salida de Lynis	6
4. Interpretación de los Resultados	7
5. Análisis de Logs tras la Auditoría con Lynis.....	8
6. Detalle sobre qué ámbitos reportan información relativa a la seguridad los dos ficheros que genera “Lynis”.	9
Documentación “lynis-report.dat”	9
Documentación “lynis.log”	11
12. Conclusión	14

Introducción - Parte 2

La auditoría de seguridad es un proceso continuo y esencial para garantizar la protección de los sistemas dentro de una infraestructura tecnológica. En la **primera parte** (de este informe, se abordó la evaluación de **Active Directory (AD)** mediante el uso de **Nessus**, identificando vulnerabilidades y aplicando medidas para mejorar la seguridad en entornos Windows.

En esta **segunda parte**, se amplía el alcance de la auditoría hacia **servidores Linux**, utilizando **Lynis**, una herramienta especializada en la evaluación de seguridad en sistemas Unix/Linux. A través de este análisis, se busca identificar configuraciones inadecuadas, detectar vulnerabilidades y proporcionar recomendaciones que permitan fortalecer la seguridad de estos entornos críticos.

Antes de proceder con esta fase, **se recomienda revisar la primera parte del informe**, ya que proporciona una base fundamental sobre la importancia de la auditoría en infraestructuras híbridas y la metodología utilizada en entornos Windows. Esta continuidad permitirá comprender mejor el enfoque integral de la auditoría y la importancia de evaluar distintos sistemas operativos dentro de una misma red.

En los siguientes apartados, se explicará el proceso de instalación y ejecución de Lynis, la interpretación de los resultados obtenidos y las estrategias de mejora para fortalecer la seguridad de los servidores Linux auditados.

Guía practica de auditoria primera parte:

https://www.linkedin.com/posts/henriquealvesc_gu%C3%ADa-pr%C3%A1ctica-de-auditor%C3%ADa-con-herramientas-activity-7298740760152084481-75WC?utm_source=share&utm_medium=member_desktop&rcm=ACoAADXMmLoB-77EMT0BQok0VZCXEEExF6pl8oS0

Auditoría Seguridad Fase 2 - Auditoría servidores Linux con “Lynis”

1. Instalación de Lynis en Entornos Ubuntu

En esta fase de la auditoría de seguridad, procederemos con la instalación y ejecución de **Lynis**, una herramienta especializada en la evaluación de seguridad en sistemas Linux. Para este proceso, se empleará **Ubuntu-dmz** y **Ubuntu-trust** como entornos de prueba.

Lynis es un software de auditoría y análisis de seguridad ampliamente utilizado en servidores Unix/Linux, con el propósito de identificar vulnerabilidades, verificar configuraciones del sistema y proporcionar recomendaciones de mejora. Su código fuente y documentación están disponibles en el siguiente repositorio oficial:

➡ Repositorio GitHub: <https://github.com/CISOfy/Lynis>

A través de este enlace, se puede acceder al procedimiento detallado de instalación. Adicionalmente, existen diversos tutoriales en plataformas como YouTube que explican su uso de manera práctica.

2. Métodos de Instalación de Lynis

Existen dos métodos principales para instalar Lynis en sistemas basados en Debian/Ubuntu:

2.1 Instalación desde el repositorio GitHub

Este método permite obtener la versión más reciente de Lynis directamente desde su repositorio oficial.

Los siguientes comandos ejecutan la descarga y ejecución del análisis de seguridad:

1. git clone <https://github.com/CISOfy/lynis>
2. cd lynis && ./lynis audit system

2.2 Instalación a través del gestor de paquetes APT

Alternativamente, Lynis se puede instalar directamente desde los repositorios oficiales de Ubuntu mediante **APT**:

```
sudo apt-get update && sudo apt-get install lynis -y
```

3. Ejecución de la Auditoría de Seguridad con Lynis

Una vez instalado Lynis, el proceso de auditoría del sistema puede iniciarse **con el siguiente comando**:

```
lynis audit system
```

Este análisis revisará diversas configuraciones del sistema, identificará vulnerabilidades y generará un informe detallado con recomendaciones de seguridad.

Como resultado, se generará un informe detallado que identificará áreas de mejora y recomendaciones para fortalecer la seguridad del servidor.

3.2 Ejemplo de Salida de Lynis

A continuación, se presenta un ejemplo del tipo de información que se obtiene tras la ejecución de la auditoría:

```

- Checking core dumps configuration
- configuration in systemd conf files
- configuration in etc/profile
- 'hard' configuration in security/limits.conf
- 'soft' configuration in security/limits.conf
- Checking setuid core dumps configuration
- Check if reboot is needed
[ NO ]

[+] Memoria y Procesos
.....
- Checking /proc/meminfo
- Searching for dead/zombie processes
- Searching for IO waiting processes
- Search prelink tooling
[ ENCONTRADO ]
[ NO ENCONTRADO ]
[ ENCONTRADO ]
[ NO ENCONTRADO ]

[+] Users, Groups and Authentication
.....
- Administrator accounts
- Unique UIDs
- Consistency of group files (grpck)
- Unique group IDs
- Unique group names
- Password file consistency
- Password hashing methods
- Checking password hashing rounds
- Query system users (non daemons)
- NIS+ authentication support
- NIS authentication support
- Sudoers file(s)
- Permissions for directory: /etc/sudoers.d
- Permissions for: /etc/sudoers
- Permissions for: /etc/sudoers.d/README
- PAM password strength tools
- PAM configuration files (pam.conf)
- PAM configuration files (pam.d)
- PAM modules
- LDAP module in PAM
- Accounts without expire date
- Accounts without password
- Locked accounts
- Checking user password aging (minimum)
- User password aging (maximum)
- Checking expired passwords
- Checking Linux single user mode authentication
- Determining default umask
- umask (/etc/profile)
- umask (/etc/login.defs)
- LDAP authentication support
- Logging failed login attempts
[ OK ]
[ OK ]
[ OK ]
[ OK ]
[ OK ]
[ OK ]
[ SUGERENCIA ]
[ DESACTIVADO ]
[ HECHO ]
[ ]
[ ]
[ ENCONTRADO ]
[ PELIGRO ]
[ PELIGRO ]
[ OK ]
[ OK ]
[ ENCONTRADO ]
[ ENCONTRADO ]
[ ENCONTRADO ]
[ ]
[ SUGERENCIA ]
[ OK ]
[ OK ]
[ DESACTIVADO ]
[ DESACTIVADO ]
[ OK ]
[ OK ]
[ NO ENCONTRADO ]
[ SUGERENCIA ]
[ ]
[ ENABLED ]

[+] Shells
.....
- Checking shells from /etc/shells

```

4. Interpretación de los Resultados

Los resultados de Lynis se clasifican en tres categorías principales:

- **[OK]** → Configuración correcta, no requiere cambios.
- **[WARNING]** → Riesgo potencial que debe ser evaluado y corregido si es necesario.
- **[SUGGESTION]** → Recomendación de mejora para fortalecer la seguridad.

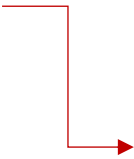
En este ejemplo, algunas de las principales áreas de mejora incluyen:

- Deshabilitar el acceso SSH directo para el usuario root.
- Activar un firewall (UFW o iptables) para mejorar la seguridad de la red.
- Configurar reglas de complejidad para contraseñas.
- Habilitar actualizaciones automáticas de seguridad.
- Revisar archivos con permisos inseguros en /tmp.

El **Security Score** y el **Hardening Index** proporcionan una evaluación general de la seguridad del sistema. Un puntaje más alto indica un mejor nivel de seguridad.

Suggestions (61):

- This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
- Install libpam-tmpdir to set \$TMP and \$TMPDIR for PAM sessions [DEB-0280]
- Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]

- 
- Configure password hashing rounds in /etc/login.defs [AUTH-9230]
 - When possible set expire dates for all password protected accounts [AUTH-9282]
 - Configure minimum password age in /etc/login.defs [AUTH-9286]
 - Configure maximum password age in /etc/login.defs [AUTH-9286]

5. Análisis de Logs tras la Auditoría con Lynis

Se generan registros detallados sobre el estado del sistema y las vulnerabilidades encontradas. Analizar estos **logs** es fundamental para comprender en profundidad los hallazgos y tomar decisiones informadas sobre la seguridad del servidor.

```
drwxr-xr-x  2 landscape landscape    4096 nov 11 10:32 landscape
-rw-rw-r--  1 root      utmp         292288 nov 29 16:52 lastlog
-rw-r----- 1 [REDACTED]  [REDACTED] 476152 nov 29 17:07 lynis.log
-rw-r----- 1 [REDACTED]  [REDACTED] 66272  nov 29 17:07 lynis-report.dat
drwx----- 2 root      root         4096 ago 24 2021 private
-rw-r----- 1 syslog    adm         625022 nov 29 17:07 syslog
```

6. Detalle sobre qué ámbitos reportan información relativa a la seguridad los dos ficheros que genera “Lynis”.

Documentación “lynis-report.dat” Ámbitos y Parámetros Importantes Detectados

1. Sistema Operativo y Kernel

Distribución: Ubuntu 20.04.3 LTS.

Versión del Kernel: 5.4.0-200-generic.

Virtualización: El sistema corre bajo un entorno de máquina virtual KVM.

Componentes del Kernel: Incluye soporte para PAM, SELinux, AppArmor, y otros sistemas de seguridad integrados.

2. Binarios y Permisos Especiales

Total de binarios detectados: 1385.

Binarios con permisos SUID: Se identificaron múltiples binarios con permisos especiales, lo que puede representar riesgos de escalación de privilegios si están mal configurados.

Ejemplos:

/usr/bin/sudo

/usr/bin/passwd

Binarios con permisos SGID: También se encontraron binarios con permisos SGID que requieren revisión para evitar accesos no autorizados.

3. Configuración de Servicios del Sistema

- **Servicios habilitados:** Varias unidades de systemd se encuentran activas, como: snap-core18-2128.mount y otras relacionadas con la funcionalidad del sistema.
- **Configuraciones críticas:** Se evaluaron configuraciones de puntos de montaje y servicios que pueden afectar la exposición del sistema a ataques.

4. Gestión de Actualizaciones y Vulnerabilidades

- **Actualización de binarios:** Lynis evaluó las versiones instaladas de binarios críticos, indicando posibles desactualizaciones.
- **Configuración de paquetes:** Se comprobó la ausencia de paquetes con vulnerabilidades conocidas.

5. Autenticación y Autorización

- **Autenticación de dos factores:** No está habilitada, ni requerida, lo que es una oportunidad de mejora para incrementar la seguridad.
- **Gestión de usuarios:** Se evaluaron los métodos de autenticación y los mecanismos PAM implementados.

6. Seguridad de Contenedores y Virtualización

- **Soporte para contenedores:** No se detectaron configuraciones específicas para contenerización activa.
- **Virtualización:** Identificación de que el entorno es un huésped KVM.

7. Políticas de Seguridad General

- **Uso de herramientas de seguridad integradas:** Lynis reporta la presencia de herramientas de seguridad como AppArmor y SELinux en el sistema.
- **Estado de configuraciones relacionadas con la seguridad:** Validación de parámetros que afectan la política de endurecimiento del sistema.

Oportunidades de mejora:

- **Implementar autenticación de dos factores (2FA):** Actualmente no está habilitada, lo cual podría fortalecer significativamente la protección del sistema.
- **Revisar y reducir binarios con permisos SUID y SGID:** Limitar estos permisos a lo estrictamente necesario.
- **Actualizar binarios desactualizados:** Asegurar que todas las aplicaciones y dependencias críticas estén en sus últimas versiones.

Esta tabla refleja los puntos clave del reporte relacionado con la seguridad, resumidos para su fácil comprensión:

Categoría	Parámetro	Detalle
Información General	Versión de Lynis	3.1.3
	Fecha del Análisis	29 de noviembre de 2024
	Auditor	No especificado
Sistema Operativo y Kernel	Sistema Operativo	Ubuntu 20.04.3 LTS
	Versión del Kernel	5.4.0-200-generic
	Virtualización	KVM
	Componentes de Seguridad del Kernel	SELinux, AppArmor, PAM
Seguridad en Binarios	Total de Binarios Analizados	1385
	Binarios con Permisos SUID	/usr/bin/sudo, /usr/bin/passwd, otros
	Binarios con Permisos SGID	/usr/bin/at, otros
Configuración del Sistema	Autenticación de Dos Factores (2FA)	No habilitada
	Unidades Systemd Activas	snap-core18, sys-kernel-config.mount
	Soporte para Contenedores	No configuraciones detectadas
Políticas de Seguridad	Gestión de Actualizaciones	Sin parches críticos pendientes

Documentación “lynis.log”

1. Información General del Análisis

- Fecha y Hora del Análisis: 29 de noviembre de 2024, 17:35:30.
- Versión de Lynis: 3.1.3.
- Auditor: No especificado.
- Inicio del Proceso: Verificación inicial de permisos en directorios críticos como `/home`, confirmando que estaban configurados adecuadamente.

2. Estado del Sistema

- Sistema Operativo: Ubuntu 20.04.3 LTS.
- Versión del Kernel: 5.4.0-200-generic.
- Entorno de Ejecución: Sistema operativo corriendo en una máquina virtual basada en KVM.

3. Configuración de Seguridad del Sistema

- Permisos de Archivos y Directorios:
 - Los permisos en directorios críticos como `/home` y configuraciones esenciales pasaron las verificaciones de seguridad iniciales.
 - Lynis no detectó configuraciones incorrectas o desviaciones en permisos básicos.
- Unidades de Systemd:
 - Evaluación exhaustiva de servicios habilitados. No se encontraron configuraciones inválidas que pudieran representar riesgos para el sistema.

4. Evaluación de Binarios y Servicios

- Binarios con Permisos SUID/SGID:
 - Se analizaron binarios críticos como `/usr/bin/sudo` y `/usr/bin/passwd` para detectar posibles riesgos asociados a permisos elevados.
 - Aunque los binarios configurados son funcionales, se recomienda revisar su necesidad para evitar posibles vectores de escalación de privilegios.
- Servicios Habilitados:
 - Varias unidades de systemd se encontraron activas, como `snap-core18`. Aunque funcionales, algunos servicios pueden optimizarse para mejorar la seguridad.

5. Revisión de Vulnerabilidades

- Gestión de Actualizaciones de Software:
 - Aunque no se encontraron paquetes críticamente desactualizados, algunos binarios pueden requerir actualizaciones para parches de seguridad más recientes.
- Configuraciones de Protección:
 - El sistema incluye configuraciones básicas de protección mediante AppArmor y SELinux, pero faltan implementaciones avanzadas.
 -

6. Recomendaciones y Oportunidades de Mejora

- Autenticación de Dos Factores (2FA):
 - Lynis destacó que no se encuentra habilitada en el sistema, lo que representa una mejora potencial significativa para reforzar la seguridad.
- Optimización de Binarios con Permisos Especiales:
 - Reducir los binarios con permisos SUID y SGID al mínimo necesario.
- Configuración de Servicios:
 - Deshabilitar servicios no utilizados o prescindibles para reducir la superficie de ataque.

Esta tabla refleja los puntos clave del reporte relacionado con la seguridad, resumidos para su fácil comprensión.

Categoría	Parámetro	Detalle
Inicio del Análisis	Fecha y Hora	29 de noviembre de 2024, 17:35:30
	Versión de Lynis	3.1.3
	Permisos Iniciales	Correctos según las verificaciones
Estado del Sistema	Sistema Operativo	Ubuntu 20.04.3 LTS
	Kernel	5.4.0-200-generic
Configuraciones de Seguridad	Análisis de Permisos de Archivos	Correctos en /home y directorios críticos
	Evaluación de Unidades de System	Sin configuraciones inválidas
Revisión de Vulnerabilidades	Binarios Analizados	1385 binarios, permisos especiales evaluados
	Estado de Binarios con SUID/SGID	Correcto, pero requiere ajustes específicos
Recomendaciones y Advertencias	Configuración de Autenticación	Falta habilitar 2FA
	Actualización de Paquetes	Algunos paquetes necesitan revisión

12. Conclusión

- ✓ El análisis de **logs** con **Lynis** permite identificar riesgos con mayor detalle.
- ✓ Se pueden extraer advertencias y sugerencias para tomar decisiones basadas en datos.
- ✓ Implementar las correcciones indicadas mejorará la seguridad del sistema.
- ✓ Se recomienda **automatizar la auditoría** periódica y mantener un monitoreo activo de los logs.

Además, este procedimiento se ha llevado a cabo en un único servidor Linux dentro de la red. Es fundamental continuar con la auditoría en los demás equipos para garantizar la seguridad de toda la infraestructura y mantener una red protegida.