Fase 1 - Corrección de un hackeo

1. Análisis Forense: Identificación de la Brecha

El análisis de los registros y del sistema de archivos revela que la seguridad de la máquina fue comprometida a través de múltiples vectores:

Acceso No Autorizado vía SSH: Se detectó un inicio de sesión exitoso para el usuario `root` desde la IP desconocida `192.168.0.134` el 8 de octubre a las 17:40:59. El atacante utilizó un puerto arbitrario para evadir detecciones simples.

Exposición Total del Directorio Web: La auditoría del directorio `/var/www/html` muestra que los archivos críticos de WordPress (incluyendo `wp-config.php`) tenían permisos `777` (lectura, escritura y ejecución para cualquier usuario).

Impacto: Esta configuración permitió que un atacante pudiera subir y ejecutar malware directamente en el servidor sin necesidad de contraseñas adicionales.

2. Vulnerabilidades Identificadas y Hallazgos

Vulnerabilidad	Evidencia Técnica	Riesgo
Configuración de FTP	Puerto 21 activo con el servicio `vsftpd`.	Protocolo inseguro e innecesario que expone archivos.
Configuración de SSH	Acceso permitido con contraseñas débiles y puerto 22 expuesto.	Alta probabilidad de compromiso por fuerza bruta.
Puertos Innecesarios	Puertos 21 (FTP) y 631 (CUPS) abiertos.	Aumento innecesario de la superficie de ataque.

Permisos en `wp-config.php`	El archivo tenía permisos de escritura/lectura universales.	Exposición de credenciales críticas de la base de datos MySQL.
Directorio Listable	Directorios de WordPress expuestos y con permisos inseguros.	Permite a atacantes explorar la estructura de archivos y encontrar archivos sensibles

3. Fase de Corrección y Bloqueo (Containment)

Para contener la amenaza y asegurar la infraestructura, se han ejecutado las siguientes acciones correctivas:

A. Cierre de Servicios e Interfases Innecesarias

Se procedió a deshabilitar los servicios que no son esenciales para la operación del servidor web:

- **Puerto 631 (Servicio de Impresión):**
  `sudo systemctl stop cups && sudo systemctl disable cups`
- **Puerto 21 (FTP):**
  `sudo systemctl stop vsftpd && sudo systemctl disable vsftpd`

B. Endurecimiento (Hardening) de Permisos de Archivos

Se aplicó el principio de "menor privilegio" para corregir la vulnerabilidad en el directorio web:

Directorios: Cambiados a `755` (el dueño puede escribir, otros solo leer/ejecutar).

Archivos generales: Cambiados a `644` (el dueño puede escribir, otros solo leer).

Archivo Crítico (`wp-config.php`): Se restringió al máximo con permisos `600` (solo el dueño puede leer/escribir) para proteger las credenciales de MySQL.

C. Restricción de Privilegios de Usuario

Se identificó que el usuario `debian` tenía permisos excesivos en el archivo `sudoers`.

Acción: Se debe eliminar o restringir la línea del usuario `debian` en el archivo de configuración de sudo para evitar que pueda escalar privilegios a `root` de manera descontrolada.

Esta intervención de la **Fase 1** neutraliza los vectores de ataque inmediatos y asegura la integridad de los datos críticos del sitio.