Informe de Pentesting - Informe Profesional

Fecha: 9 de enero de 2026

Nombre del Autor: Javier Rubier

Proyecto: Evaluación de seguridad de servidores web, bases de datos y servicios

2. Metodología

Para realizar la evaluación de seguridad, se utilizaron las siguientes metodologías y herramientas:

- Escaneo de puertos: nmap, ss, netstat.
- Pruebas de configuración: Revisión manual de archivos de configuración como sshd_config, vsftpd.conf, wp-config.php.
- Exploración de vulnerabilidades web: Análisis de configuraciones en Apache y permisos de archivos.
- Pruebas de contraseñas débiles: Evaluación de contraseñas en MySQL y autenticación SSH.
- Exploits conocidos: Verificación de configuraciones inseguras, como directorios listables y accesos anónimos en FTP.

3. Hallazgos de Seguridad

3.1 Directorio Web Listable

- Descripción: Se encontró que los directorios web en el servidor estaban configurados para ser listados, lo que permitió la exposición no intencionada de archivos y directorios sensibles.
- Impacto: Los atacantes pueden obtener información sobre la estructura del servidor y, potencialmente, acceder a archivos no protegidos.

- Solución Propuesta: Deshabilitar la indexación de directorios en los archivos de configuración del servidor web (Apache/Nginx) añadiendo la línea Options -Indexes en los archivos .htaccess o la configuración de servidor principal.

3.2 Permisos Incorrectos en wp-config.php

- Descripción: Se identificó que los permisos del archivo wp-config.php eran demasiado permisivos, lo que podría permitir que usuarios no autorizados accedan a la configuración de la base de datos de WordPress.
- Impacto: Un atacante que obtenga acceso a este archivo puede ver credenciales sensibles y otros parámetros importantes.
- Solución Propuesta: Establecer los permisos de wp-config.php a chmod 600 para restringir el acceso a solo el propietario del archivo.

3.3 Puertos Innecesarios Abiertos

- Descripción: Durante el escaneo de puertos, se detectaron puertos innecesarios abiertos, algunos de los cuales no estaban siendo utilizados por servicios legítimos.
- Impacto: La exposición de puertos innecesarios aumenta la superficie de ataque, lo que facilita a los atacantes encontrar vectores de entrada.
- Solución Propuesta: Revisar todos los puertos abiertos mediante ss -tuln y nmap. Utilizar ufw o iptables para bloquear puertos innecesarios.

3.4 Configuración de SSH

- Descripción: Se encontró que el servidor SSH estaba configurado para permitir el acceso como usuario root, lo cual representa un riesgo de seguridad significativo, especialmente en ataques de fuerza bruta.
- Impacto: El acceso sin restricciones como root puede ser explotado fácilmente por un atacante con contraseñas débiles o mediante ataques de diccionario.
- Solución Propuesta: Editar el archivo de configuración de SSH (/etc/ssh/sshd_config) y establecer PermitRootLogin no. Asegurar que el acceso se haga únicamente mediante autenticación con claves SSH y deshabilitar la autenticación por contraseña. Reiniciar el servicio SSH con systemctl restart sshd.

3.5 Configuración de FTP

- Descripción: El servidor FTP estaba configurado para permitir accesos anónimos, lo que permite a cualquier usuario acceder a ciertos directorios y archivos sin autenticación.
- Impacto: La exposición de directorios sensibles a través de FTP puede resultar en la filtración de datos privados y puede ser aprovechada para cargar o descargar archivos maliciosos.
- Solución Propuesta: Deshabilitar el acceso anónimo configurando anonymous_enable=NO en el archivo de configuración de vsftpd.conf. Asegurar que todos los usuarios estén restringidos a sus directorios con chroot_local_user=YES. Verificar las configuraciones de los usuarios en /etc/ftpusers y /etc/vsftpd.user_list.

3.6 Configuración de MySQL

- Descripción: La configuración de MySQL no estaba completamente segura, ya que la base de datos aceptaba conexiones desde direcciones externas.

- Impacto: Las bases de datos accesibles desde fuera de la red local son un objetivo ideal para ataques de inyección SQL, ataques de denegación de servicio (DoS) o robo de datos.
- Solución Propuesta: Configurar MySQL para escuchar solo en la dirección local (127.0.0.1) mediante la modificación de bind-address en el archivo mysqld.cnf. Cambiar las contraseñas predeterminadas y asegurarse de que las cuentas de usuario tengan privilegios mínimos. Ejecutar SHOW GRANTS para verificar los privilegios de los usuarios y ajustar según sea necesario.

4. Recomendaciones Generales

1. Actualización de Software: Asegurarse de que todos los servicios, como Apache, MySQL, vsftpd y SSH, estén actualizados con los últimos parches de seguridad.
2. Monitoreo de Logs: Habilitar el monitoreo de logs de seguridad para detectar posibles intrusiones o accesos no autorizados.
3. Seguridad en la Red: Implementar un firewall a nivel de red para restringir el acceso a puertos solo desde direcciones IP confiables.
4. Auditoría Regular: Realizar auditorías de seguridad periódicas para evaluar la eficacia de las medidas correctivas y detectar nuevas vulnerabilidades.

5. Conclusiones

La infraestructura analizada presenta varias debilidades críticas en la configuración de servicios que podrían ser explotadas por un atacante. Al aplicar las soluciones recomendadas en este informe, se mejorará considerablemente la seguridad del sistema, reduciendo la superficie de ataque y protegiendo los datos sensibles de accesos no autorizados.

Recomendación Final: Implementar las medidas correctivas lo antes posible para mitigar los riesgos y proteger la infraestructura ante posibles ataques.

Firma:

Javi

Empresa: Javi