Informe Detallado de la Fase 1 - Corrección del Hackeo

1. Introducción

Este informe detalla el proceso de análisis forense, detección y mitigación de las vulnerabilidades explotadas en el servidor comprometido. Se incluye un análisis profundo de cada vulnerabilidad encontrada, la criticidad de la misma y las medidas aplicadas para solventarlas.

2. Análisis Forense

Se utilizaron diversas técnicas y herramientas para identificar accesos no autorizados, modificaciones en archivos críticos, procesos sospechosos y configuraciones de seguridad incorrectas en el sistema.

3. Herramientas Utilizadas y Justificación

- **rkhunter**: Detecta rootkits y malware persistente.
- **chkrootkit**: Analiza archivos en busca de rootkits activos.
- **debsums**: Verifica la integridad de los paquetes instalados.
- **netstat**: Identifica conexiones y puertos abiertos.
- **journalctl**: Revisión de logs de sistema en tiempo real.
- **last, who, w**: Identificación de usuarios y accesos recientes.
- **grep y find**: Búsqueda de archivos sospechosos.
- **systemctl**: Comprobación del estado de servicios del sistema.
- **Apache logs**: Revisión de actividad en el servidor web.
- **awk y getent**: Verificación de usuarios en el sistema.
- **ps aux**: Identificación de procesos en ejecución.
- **Nmap**: Escaneo de puertos abiertos en el sistema.

4. Vulnerabilidades Detectadas

Vulnerabilidad	Crítica	Estado
Listado de directorios en Apache	Alta	Corregida
Puertos innecesarios abiertos	Media	Corregida

Permisos incorrectos en archivos críticos	Alta	Corregida
Accesos sospechosos en logs	Alta	Investigado
SSH con autenticación débil	Crítica	Corregida

5. Medidas Correctivas Aplicadas

- **Apache**: Se deshabilitó la opción de listado de directorios en la configuración de Apache.

- **Firewall**: Se cerraron puertos innecesarios para reducir la superficie de ataque.

- **Permisos**: Se restringieron los permisos en archivos críticos como wp-config.php.

- **Usuarios**: Se eliminaron accesos sospechosos y se reforzó la autenticación SSH.

- **Logs**: Se implementó una auditoría para detectar intentos de acceso no autorizados.

6. Evaluación de la Corrección

Se realizaron pruebas posteriores a la corrección para validar que cada vulnerabilidad fue mitigada exitosamente. El sistema se encuentra en un estado seguro, con mejoras en las configuraciones y monitoreo continuo.

7. Conclusión

Gracias a este proceso de análisis y mitigación, se han eliminado brechas de seguridad críticas en el servidor. Se recomienda continuar con auditorías periódicas para prevenir futuros ataques.