TOP 10 VULNERABILIDADES EN OWASP

1. Introducción

El propósito de este informe es documentar el proceso de pentesting realizado en el entorno designado, detallando las vulnerabilidades identificadas y proporcionando recomendaciones para fortalecer la seguridad. Este ejercicio se llevó a cabo con el objetivo de identificar posibles riesgos y mejorar la protección de los sistemas evaluados, tanto en cumplimiento de normativas como en la mitigación de amenazas reales. El alcance del pentesting incluyó la evaluación de la infraestructura de la máquina y el sitio web asociados al entorno en cuestión.

2. Enfoque y Estrategia

La metodología aplicada en este pentesting se centró en una combinación de reconocimiento, explotación de vulnerabilidades y análisis posterior de la seguridad. El enfoque varió según el objetivo; en el caso de la máquina, se priorizó la identificación de vulnerabilidades en los servicios expuestos, mientras que para el sitio web se hizo hincapié en probar la seguridad de la interfaz de usuario y los mecanismos de autenticación. Ambos enfoques aseguran una revisión exhaustiva de posibles vectores de ataque.

3. Fases del Pentesting

El proceso de pentesting se dividió en varias fases:

- **Reconocimiento**: Se utilizaron herramientas como Nmap para mapear los puertos abiertos y los servicios activos.
- **Enumeración**: Identificación detallada de versiones y configuraciones de servicios.
- **Explotación**: Se emplearon herramientas como Metasploit para probar la explotación de vulnerabilidades conocidas y evaluar la resistencia de los sistemas.
- **Post-Explotación**: En esta fase, se analizaron los privilegios obtenidos y el alcance del acceso a los recursos del sistema.

Cada fase se realizó meticulosamente para garantizar una evaluación precisa de la seguridad.

4. Vulnerabilidades Detectadas

Durante el proceso de pentesting, se identificaron varias vulnerabilidades, entre las que destacan:

- **Inyección SQL** en el sitio web, permitiendo acceso no autorizado a la base de datos.
- **Configuración de seguridad incorrecta** en servicios de red, lo cual facilitó el reconocimiento de servicios sensibles.
- **Autenticación débil** en el sistema de login, lo cual aumenta el riesgo de ataques de fuerza bruta.

Cada vulnerabilidad fue documentada y verificada para asegurar la validez de los resultados obtenidos.

5. Propuesta de Prevención

Para prevenir la introducción de futuras vulnerabilidades, se sugieren las siguientes estrategias:

- Implementar políticas de actualización y parcheo continuo de software.
- Establecer reglas de control de acceso y autenticación multi-factor para reducir los riesgos de acceso no autorizado.
- Realizar revisiones de configuración de seguridad de manera periódica para ajustar cualquier parámetro de riesgo.

Estas medidas ayudarán a mantener la seguridad del sistema frente a nuevas amenazas.

6. Propuesta de Mitigación

Para mitigar las vulnerabilidades actuales, se recomienda:

- **Revisión de consultas SQL** y uso de consultas preparadas para evitar ataques de inyección.
- Configuración adecuada de los servicios de red, asegurando que sólo los servicios necesarios estén expuestos y con los permisos correctos.
- Implementación de complejidad en contraseñas y autenticación multi-factor en los módulos de login del sitio web.

Estas recomendaciones son esenciales para minimizar los riesgos identificados durante el pentesting.

7. Análisis de Mitigación

La efectividad de estas medidas fue evaluada y se concluye que su implementación reduciría significativamente el impacto y probabilidad de explotación de las vulnerabilidades. Es crucial asegurar que los sistemas se mantengan alineados con las recomendaciones de seguridad para preservar la integridad del entorno.

8. Impacto Potencial

La implementación de las medidas propuestas fortalecerá considerablemente la seguridad general del sistema. Las vulnerabilidades descubiertas, de ser explotadas, podrían llevar a una fuga de datos, interrupción de servicios críticos o acceso no autorizado a información

sensible. Por lo tanto, abordar estas vulnerabilidades es fundamental para proteger la infraestructura y la privacidad de los datos manejados.

9. Conclusión

La prevención y la mitigación de vulnerabilidades son componentes esenciales de una estrategia de seguridad efectiva. Este informe demuestra la importancia de realizar evaluaciones de seguridad periódicas y aplicar medidas preventivas y correctivas de manera proactiva. Mantener un enfoque en la mejora continua de la seguridad garantizará que el sistema esté preparado para enfrentar posibles amenazas en el futuro.