Informe Final de Pentesting

Índice

---

1. Introducción

El objetivo principal de este informe es documentar el proceso completo de pruebas de penetración realizadas sobre los entornos vulnerables Metasploitable y DVWA (Damn Vulnerable Web Application). Durante las pruebas, se identificaron vulnerabilidades, se explotaron debilidades en los servicios y se implementaron estrategias para proponer medidas de mitigación y prevención. Este ejercicio busca reflejar la importancia de mantener los sistemas actualizados y seguros, cumpliendo con las mejores prácticas de ciberseguridad.

2. Enfoque y Estrategia

Se adoptó un enfoque estructurado para llevar a cabo el pentesting, destacando los siguientes puntos clave:

- **Reconocimiento:** Identificación de servicios y puertos abiertos mediante herramientas como Nessus y Nmap.
- **Explotación:** Uso de Metasploit y navegadores para atacar servicios y vulnerabilidades identificadas.
- **Documentación:** Registro detallado de todas las actividades realizadas, incluyendo comandos, resultados y capturas de pantalla.
- **Diferenciación:** Las pruebas incluyeron metodologías específicas tanto para la máquina vulnerable (Metasploitable) como para el sitio web vulnerable (DVWA).

3. Fases del Pentesting

3.1. Reconocimiento

Se utilizó Nmap para realizar un escaneo de puertos y detectar servicios vulnerables:

- **Puertos detectados:** 21 (FTP), 53 (DNS), 80 (HTTP), 8180 (Tomcat).
- **Herramientas adicionales:** Nessus para el escaneo inicial y Metasploit para confirmar vulnerabilidades específicas.

3.2. Explotación de Vulnerabilidades

Se ejecutaron los siguientes ataques:

1. **Servicio FTP (vsftpd 2.3.4):** Uso del módulo `vsftpd_234_backdoor` para acceder como superusuario.
2. **Aplicación web DVWA:** Inyección de comandos en niveles de seguridad Bajo, Medio y Alto.
   - Nivel Bajo: Ejecución de `ls -la /root`.
   - Nivel Medio: Lectura de `/etc/passwd`.
   - Nivel Alto: Obtención del directorio actual con `pwd`.
3. **Apache Tomcat:** Subida de archivos maliciosos mediante `tomcat_mgr_upload` para ganar acceso al servidor.

---

4. Vulnerabilidades Detectadas

1. **FTP (vsftpd 2.3.4):**
   - Esta vulnerabilidad se debe a una puerta trasera presente en la versión 2.3.4 del servicio vsFTPd. Permite a un atacante remoto obtener acceso no autenticado al sistema con privilegios elevados. Este problema está registrado bajo el CVE-2011-2523 y es considerado crítico debido al control total que se puede obtener sobre la máquina objetivo.
2. **DNS (ISC BIND 9.4.2):**
   - El servicio de DNS expone información sobre su versión en sus respuestas, lo que podría ser aprovechado por atacantes para identificar y explotar vulnerabilidades específicas asociadas a esta versión. Aunque no permite directamente la explotación del sistema, proporciona un punto de partida para posibles ataques dirigidos.
3. **HTTP (Apache 2.2.8):**
   - La versión expuesta del servidor Apache HTTP permite a los atacantes obtener detalles sobre el tipo y la configuración del servidor. Estas informaciones podrían ser utilizadas para lanzar ataques de denegación de servicio (DoS) o explotar vulnerabilidades conocidas de esa versión.
4. **Tomcat (Coyote JSP 1.1):**
   - El servidor de aplicaciones Apache Tomcat en su versión expuesta permite el acceso a su consola de administración sin medidas de autenticación fuertes. Esto facilita que un atacante suba archivos maliciosos para ejecutar código arbitrario, comprometiendo completamente el servidor.
5. **DVWA:**
   - La aplicación web Damn Vulnerable Web Application presenta vulnerabilidades en tres niveles de seguridad:
     - **Bajo:** Permite inyección de comandos sin ninguna validación.
     - **Medio:** Las validaciones implementadas son insuficientes y pueden ser evadidas mediante caracteres especiales.
     - **Alto:** Aunque hay controles más estrictos, todavía se permite la ejecución limitada de comandos con entradas manipuladas.

---

5. Propuesta de Prevención

1. **Desarrollo Seguro:** Establecer prácticas de codificación seguras para evitar vulnerabilidades conocidas.
2. **Validación de Entradas:** Implementar validaciones estrictas en las aplicaciones web para evitar inyecciones de comandos.
3. **Actualizaciones:** Mantener todos los servicios actualizados a sus versiones más recientes.
4. **Políticas de Seguridad:** Crear reglas claras para el acceso a servicios y la gestión de configuraciones.

---

6. Propuesta de Mitigación

1. **FTP:**
   - Actualizar el servicio vsftpd a una versión más reciente y segura que no contenga vulnerabilidades conocidas, como la puerta trasera identificada en la versión 2.3.4.
   - Implementar restricciones en el acceso al servicio FTP, limitando conexiones a direcciones IP autorizadas y restringiendo usuarios anónimos.
   - Realizar auditorías periódicas de configuración para verificar que no existan permisos innecesarios en directorios sensibles.
2. **DNS:**
   - Configurar el servicio ISC BIND para ocultar su versión en las respuestas a las consultas, evitando la exposición de información innecesaria.
   - Aplicar parches de seguridad y mantener la configuración actualizada para mitigar vulnerabilidades conocidas.
   - Implementar firewalls para controlar el acceso a los servicios DNS y evitar que puedan ser explotados por atacantes externos.
3. **HTTP:**
   - Deshabilitar la visualización de información del servidor web, como el tipo de servidor y su versión, configurando adecuadamente los encabezados HTTP.
   - Actualizar el servidor Apache HTTP a una versión que no tenga vulnerabilidades conocidas y que incluya medidas de seguridad adicionales.
   - Implementar reglas de firewall para filtrar el tráfico entrante y prevenir accesos no autorizados a directorios sensibles o servicios internos.
4. **DVWA:**
   - Mejorar las validaciones de entrada en todos los niveles de seguridad, asegurándose de que los datos ingresados sean sanitizados correctamente antes de ser procesados.
   - Habilitar el cifrado de datos en tránsito mediante HTTPS para proteger las credenciales y otros datos sensibles.
   - Configurar autenticación multifactor para los usuarios que acceden a la aplicación, reforzando la seguridad del sistema frente a intentos de acceso no autorizados.

---

7. Análisis de Mitigación

Las medidas implementadas mostraron una reducción significativa en la superficie de ataque:

- Servicios como FTP y DNS ahora tienen accesos restringidos.
- La aplicación web DVWA tiene validaciones que evitan inyecciones comunes.
- Las actualizaciones eliminaron vulnerabilidades críticas.

---

8. Impacto Potencial

Las vulnerabilidades explotadas tenían el potencial de comprometer sistemas enteros, exfiltrar información y escalar privilegios. Las medidas adoptadas fortalecieron la seguridad general y protegieron contra ataques similares en el futuro.

---

9. Conclusión

Este informe destaca la importancia de realizar auditorías de seguridad regularmente y mantener los sistemas actualizados. Las prácticas seguras implementadas reducen significativamente el riesgo de ataques exitosos, promoviendo un entorno de seguridad más robusto y confiable. La reflexión final es que un enfoque proactivo es esencial para proteger los activos digitales contra amenazas modernas.