**Informe Técnico**

**Análisis de Seguridad y Validación de Vulnerabilidades – Lección 1**

**1. Escenario**

Formando parte del equipo de ciberseguridad de una empresa ficticia, se asignó la evaluación de un servidor de pruebas con IP **192.168.1.150**. El objetivo fue aplicar las fases iniciales de un **pentest ético**, incluyendo reconocimiento, escaneo de servicios, validación de vulnerabilidades y propuesta de mitigación, documentando todo el proceso de manera profesional.

**2. Metodología**

La práctica se llevó a cabo en las siguientes fases:

1. **Reconocimiento inicial** con herramientas como whois, nslookup, dig y simulación de búsquedas en Shodan.
2. **Escaneo activo de puertos y servicios** con nmap -sS -sV -T4 -p- 192.168.1.150.
3. **Búsqueda de vulnerabilidades conocidas (CVEs)** en los servicios detectados, apoyándose en **ExploitDB y MITRE CVE**.
4. **Simulación de explotación segura** utilizando herramientas como **Nikto, sqlmap o Metasploit**.
5. **Reporte técnico** con hallazgos, riesgo asociado y recomendaciones de mitigación.

**3. Resultados**

**3.1 Reconocimiento**

* Tecnologías visibles: servidor web Apache, posible CMS en /login.
* Rutas sensibles identificadas: /admin, /backup.

**3.2 Escaneo de Puertos**

Ejemplo de hallazgos con Nmap:

* **Puerto 22 (SSH):** OpenSSH 7.2
* **Puerto 80 (HTTP):** Apache httpd 2.4.29
* **Puerto 3306 (MySQL):** Servidor expuesto

Servicios candidatos a análisis: Apache y MySQL.

**3.3 Vulnerabilidades encontradas**

* **Apache httpd 2.4.29**: CVE-2019-0211 (escalamiento de privilegios).
* **MySQL**: Riesgo de acceso no autenticado en versiones antiguas.

**3.4 Simulación de explotación**

Se utilizó sqlmap para probar inyección en http://192.168.1.150/products.php?id=1, evidenciando respuesta del servidor con errores SQL, confirmando posible **SQL Injection**.

**4. Recomendaciones de Seguridad**

1. Actualizar Apache a una versión estable y corregida.
2. Restringir acceso a MySQL desde hosts externos.
3. Implementar **validación y parametrización** de consultas SQL.
4. Configurar políticas de firewall que cierren puertos innecesarios.
5. Reforzar autenticación en rutas sensibles con **MFA** y limitar accesos administrativos.

**5. Reflexión**

El ejercicio demostró que incluso servicios comunes como Apache o MySQL pueden ser vectores de ataque si no están configurados o actualizados correctamente. Además, resaltó la importancia de un enfoque estructurado en pruebas de penetración y la necesidad de documentar los hallazgos de forma clara y profesional.

**6. Conclusión**

El análisis del servidor **192.168.1.150** permitió identificar vulnerabilidades críticas y simular su explotación de manera controlada. Se comprobó la efectividad de herramientas de pentesting en entornos reales y se propusieron medidas para mitigar riesgos. Este laboratorio refuerza la relevancia de integrar procesos de **pentesting ético y gestión de vulnerabilidades** en la estrategia de ciberseguridad de cualquier organización.