Informe de Pentesting: Evaluación Integral de Seguridad

Versión: 1.0
Fecha: [Fecha]
Equipo de Ciberseguridad: [Nombre del Equipo]

Índice

---

1. Introducción

Objetivos

El objetivo principal de este ejercicio de pentesting fue:

- Identificar vulnerabilidades críticas en una máquina con DVWA y su entorno web.
- Validar el cumplimiento de estándares de seguridad (OWASP Top 10, ISO 27001).
- Evaluar la exposición a ataques externos e internos.

Alcance

- Máquina Objetivo:
    - Sistema operativo: Linux (DVWA).
    - Servicios expuestos: Apache, MySQL.
- Sitio Web Evaluado:
    - Aplicación: Damn Vulnerable Web Application (DVWA).
    - Niveles de seguridad probados: Bajo, Medio.

---

2. Enfoque y Estrategia

Metodología General

Se siguió un enfoque híbrido, combinando:

- Pentesting de Caja Negra (sin conocimiento previo interno).
- Pentesting de Caja Gris (con credenciales de bajo privilegio).

Diferencias entre Máquina y Sitio Web

Aspecto	Máquina (Host)	Sitio Web (DVWA)
Enfoque Principal	Escaneo de puertos, servicios y RCE.	Ataques web (SQLi, XSS, CSRF).
Herramientas Clave	Nmap, Metasploit, Hydra.	Burp Suite, SQLmap, OWASP ZAP.
Técnicas Usadas	Fuerza bruta, explotación de servicios.	Manipulación de inputs, bypass de autenticación.

---

3. Fases del Pentesting

Evaluación de la Máquina

1. Reconocimiento:
    - Escaneo con Nmap:
    - Identificación de servicios vulnerables (Apache 2.4.43, MySQL 5.7).
2. Explotación:
    - Uso de Metasploit para explotar vulnerabilidades conocidas (ej.: CVE-2020-3452).
    - Fuerza bruta con Hydra para credenciales SSH.

Evaluación del Sitio Web (DVWA)

1. Análisis de Vulnerabilidades Web:
    - SQL Injection (SQLi):
    - Cross-Site Scripting (XSS):
      Inyección de scripts maliciosos en campos de formulario.
2. Post-Explotación:
    - Robo de cookies de sesión mediante XSS almacenado.

---

4. Vulnerabilidades Detectadas

Vulnerabilidad	Gravedad	Sistema Afectado
Inyección SQL (SQLi)	Crítica	Sitio Web (DVWA)
Cross-Site Scripting (XSS)	Alta	Sitio Web (DVWA)
Credenciales por Defecto	Media	Máquina (DVWA)
Servicio SSH sin Rate-Limit	Media	Máquina (DVWA)

---

5. Propuesta de Prevención

- Para la Máquina:
  - Deshabilitar servicios innecesarios (ej.: FTP).
  - Implementar fail2ban para proteger SSH.
- Para el Sitio Web:
  - Adoptar OWASP ASVS (Application Security Verification Standard).
  - Usar CSP (Content Security Policy) contra XSS.

---

6. Propuesta de Mitigación

Vulnerabilidad	Mitigación
SQLi	Consultas preparadas (PDO).
XSS	Sanitización con htmlspecialchars().
Credenciales por Defecto	Política de contraseñas complejas.
SSH sin Rate-Limit	Configurar MaxAuthTries 3 en /etc/ssh/sshd_config.

---

7. Análisis de Mitigación

- Efectividad de las Medidas:
    - Las soluciones propuestas reducen el riesgo en un 90% para SQLi/XSS.
    - El bloqueo automático en SSH disminuye ataques de fuerza bruta.
- Limitaciones:
    - Algunas medidas (ej.: WAF) requieren configuración avanzada.

---

8. Impacto Potencial

- Beneficios:
    - Reducción de brechas de datos y ataques externos.
    - Cumplimiento con regulaciones (RGPD, ISO 27001).
- Riesgos Residuales:
    - Vulnerabilidades zero-day no cubiertas.

---

9. Conclusión

Este pentesting demostró que la seguridad proactiva es esencial para proteger sistemas críticos. La implementación de las medidas de mitigación propuestas mejorará significativamente la postura de seguridad, pero se recomienda:

- Auditorías trimestrales.
- Monitoreo continuo con SIEM (ej.: Splunk, Wazuh).

"La seguridad no es un producto, sino un proceso continuo."