Reporte de Pentesting: Evaluación de Vulnerabilidades en DVWA

---

1. Introducción

Objetivo

Realizar una prueba de penetración (pentesting) contra una máquina vulnerable configurada con Damn Vulnerable Web Application (DVWA) para identificar y explotar vulnerabilidades comunes en entornos web.

Alcance

- Target: Máquina con DVWA (IP: [IP Objetivo]).
- Máquina Atacante: Kali Linux (IP: [IP Atacante]).
- Técnicas Aplicadas: Reconocimiento, explotación de vulnerabilidades web (ej.: inyección SQL, XSS, CSRF) y escalación de privilegios.

---

2. Metodología

Herramientas Utilizadas

Herramienta	Uso
Nmap	Escaneo de puertos y servicios.
Burp Suite	Interceptación y manipulación de peticiones HTTP.
SQLmap	Automatización de ataques de inyección SQL.
Metasploit Framework	Explotación de vulnerabilidades conocidas.
John the Ripper	Fuerza bruta a contraseñas.

Técnicas Aplicadas

1. Reconocimiento:
    - Escaneo de puertos y enumeración de servicios.
    - Identificación de versiones de software vulnerables.
2. Explotación:
    - Ataques a formularios web (SQLi, XSS).
    - Bypass de autenticación.
3. Post-Explotación:
    - Escalación de privilegios dentro de DVWA.

---

3. Resultados

Vulnerabilidades Explotadas

1. Inyección SQL (SQLi) en DVWA

- Nivel de Gravedad: Crítico.
- Descripción: Se explotó un campo de login vulnerable a inyección SQL para extraer credenciales de la base de datos.

2. Cross-Site Scripting (XSS) Almacenado

- Nivel de Gravedad: Alto.
- Descripción: Inyección de código JavaScript malicioso en un campo de comentarios.

3. Fuerza Bruta a Credenciales

- Nivel de Gravedad: Medio.
- Descripción: Uso de Hydra para crackear la contraseña del usuario "admin".

---

4. Escalación de Privilegios

Técnicas Utilizadas

1. Abuso de Sesiones de Administrador:
    - Uso de cookies robadas vía XSS para suplantar al administrador.
2. Explotación de Configuraciones Inseguras:
    - Acceso al panel de control de DVWA con credenciales por defecto (admin:password).

Resultados Obtenidos

- Acceso como administrador a la base de datos y configuración del servidor.
- Ejecución remota de comandos (RCE) en la máquina DVWA (en niveles de seguridad "low").

---

5. Mitigación

Recomendaciones para Cada Vulnerabilidad

Vulnerabilidad	Solución
Inyección SQL	Usar consultas preparadas (PDO/MySQLi) y sanitizar inputs.
XSS	Implementar filtros (htmlspecialchars()) y CSP (Content Security Policy).
Fuerza Bruta	Habilitar CAPTCHA, límite de intentos y MFA.
Credenciales por Defecto	Cambiar contraseñas predeterminadas y aplicar políticas de complejidad.

Hardening Adicional

- Actualizar DVWA a la última versión.
- Restringir permisos de archivos (ej.: chmod 750 /var/www/html/).

---

6. Conclusión

El pentesting realizado demostró que DVWA es altamente vulnerable en configuraciones de seguridad baja/medio, permitiendo:

- Robo de información sensible vía SQLi.
- Ejecución de scripts maliciosos (XSS).
- Escalación a privilegios de administrador.

Recomendación Final:
Implementar un WAF (Web Application Firewall) y realizar auditorías periódicas de seguridad.