📘 Glosario: Pruebas de Penetración, Metodologías y Herramientas

---

1. Prueba de Penetración (Pentesting)

Evaluación controlada de seguridad que simula ataques reales con el fin de identificar vulnerabilidades explotables en sistemas, redes o aplicaciones.

---

2. OWASP Testing Guide

Marco metodológico propuesto por OWASP para evaluar la seguridad de aplicaciones web. Se estructura en fases: planificación, recopilación de información, pruebas activas y reporte.

---

3. PTES (Penetration Testing Execution Standard)

Estándar profesional que define un proceso de siete fases para pruebas de penetración, aplicable a redes, aplicaciones e infraestructuras.

---

4. Reconocimiento

Primera fase del pentesting, donde se recopila información sobre el objetivo, de forma pasiva o activa, sin interactuar directamente o con interacciones mínimas.

---

5. Enumeración de Vulnerabilidades

Proceso que consiste en detectar debilidades técnicas, configuraciones incorrectas o versiones obsoletas de software susceptibles a explotación.

---

6. Explotación

Fase en la que se aprovechan vulnerabilidades previamente identificadas para simular accesos o ataques reales al sistema objetivo.

7. Post-explotación

Acciones realizadas tras comprometer un sistema, como elevar privilegios, mantener persistencia o acceder a información confidencial.

---

8. SQL Injection (SQLi)

Tipo de ataque en el que se inyectan comandos SQL a través de entradas no validadas para manipular bases de datos.

---

9. Cross-Site Scripting (XSS)

Vulnerabilidad que permite insertar y ejecutar scripts maliciosos en el navegador de un usuario legítimo a través de entradas no sanitizadas.

---

10. Cross-Site Request Forgery (CSRF)

Ataque que engaña a un navegador autenticado para ejecutar acciones no autorizadas en nombre del usuario sin su consentimiento.

---

11. Consultas Parametrizadas

Técnica de programación segura que evita inyecciones SQL al separar claramente los datos de las instrucciones del código.

---

12. CSP (Content Security Policy)

Política de seguridad que ayuda a mitigar ataques como XSS restringiendo los recursos que un navegador puede cargar y ejecutar.

---

13. SameSite (Cookie Attribute)

Atributo de seguridad para cookies que previene su envío automático en solicitudes entre sitios, mitigando ataques CSRF.

---

14. Metasploit Framework

Plataforma modular de pruebas de penetración que permite ejecutar exploits, payloads y tareas de post-explotación sobre sistemas vulnerables.

---

15. Burp Suite

Suite profesional de herramientas para auditoría de aplicaciones web. Permite interceptar tráfico, automatizar escaneos y realizar pruebas manuales.

---

16. Proxy Interceptante

Herramienta que actúa como intermediario entre el navegador y el servidor web, permitiendo inspeccionar y modificar solicitudes y respuestas.

---

17. Intruder (Burp Suite)

Herramienta de Burp Suite para realizar ataques automáticos como fuzzing o fuerza bruta sobre formularios y parámetros.

---

18. Spider (Burp Suite)

Módulo que rastrea y mapea automáticamente la estructura de una aplicación web, recopilando enlaces y formularios disponibles.

---

19. Exploit

Código o técnica que aprovecha una vulnerabilidad para comprometer un sistema, obtener acceso o ejecutar comandos no autorizados.

---

20. Ética Profesional en Pentesting

Conjunto de principios que rigen el comportamiento responsable del especialista en seguridad. Toda prueba debe realizarse con autorización formal y respetar la legislación vigente.
