📘 Glosario: Análisis de Seguridad y Pruebas de Penetración

---

1. Análisis de Seguridad

Proceso sistemático que evalúa la postura de seguridad de una infraestructura tecnológica con el fin de identificar vulnerabilidades, medir riesgos y proponer medidas correctivas alineadas con estándares como ISO/IEC 27001 o NIST.

---

2. Prueba de Penetración (Pentesting)

Evaluación controlada y autorizada que simula ataques reales a sistemas, redes o aplicaciones, para descubrir vulnerabilidades explotables y validar mecanismos de defensa existentes.

---

3. OWASP (Open Web Application Security Project)

Organización sin fines de lucro que promueve buenas prácticas de seguridad en aplicaciones web. Su marco es ampliamente adoptado en pruebas de seguridad.

---

4. Reconocimiento (Reconnaissance)

Primera fase del pentesting, enfocada en recopilar información pública (OSINT) de la organización objetivo sin interacción directa que alerte al sistema.

---

5. OSINT (Open Source Intelligence)

Conjunto de técnicas para recolectar información de fuentes abiertas, como redes sociales, buscadores, bases de datos públicas y registros DNS.

---

6. Escaneo (Scanning)

Fase en la que se ejecutan técnicas activas para identificar puertos abiertos, servicios disponibles y vulnerabilidades técnicas en los activos digitales.

---

7. Nmap

Herramienta de escaneo de redes utilizada para descubrir hosts y servicios activos mediante el envío de paquetes y análisis de respuestas.

---

8. Explotación (Exploitation)

Etapa en la que se aprovechan vulnerabilidades identificadas para obtener acceso a sistemas, demostrando el impacto real de los hallazgos.

---

9. Metasploit Framework

Plataforma de desarrollo de exploits y herramientas de post-explotación utilizada para validar vulnerabilidades durante pentests.

---

10. Mantenimiento del Acceso (Maintaining Access)

Técnicas empleadas para conservar acceso a un sistema comprometido, simulando el comportamiento de un atacante persistente (APT).

---

11. Rootkit

Conjunto de herramientas utilizadas por un atacante para ocultar su presencia en un sistema y mantener el acceso persistente.

---

12. Informe y Remediación

Última fase del pentest. Consiste en generar un documento técnico que detalla hallazgos, su severidad (por ejemplo usando CVSS) y acciones recomendadas.

---

13. CVSS (Common Vulnerability Scoring System)

Estándar para clasificar la severidad de vulnerabilidades de seguridad mediante una escala numérica que ayuda a priorizar remediaciones.

---

14. Entorno Controlado

Ambiente de pruebas aislado que replica la infraestructura de producción sin afectar la operación real, utilizado para pruebas seguras.

---

15. Ética del Pentesting

Conjunto de principios que rigen la conducta de los profesionales durante pruebas de seguridad: confidencialidad, consentimiento informado, respeto a la privacidad y cumplimiento legal.

---

16. PTES (Penetration Testing Execution Standard)

Estándar abierto que define las fases, requisitos y buenas prácticas para realizar pruebas de penetración profesionales y estructuradas.

---

17. NIST SP 800-115

Publicación especial del NIST que proporciona una guía técnica para realizar evaluaciones de seguridad y pruebas de penetración en entornos empresariales.

---

18. Backdoor

Mecanismo oculto que permite acceso remoto no autorizado a un sistema, empleado por atacantes o como técnica de persistencia durante el pentest.

---

19. Legalidad en Pentesting

El uso de técnicas ofensivas en ciberseguridad requiere autorización explícita. Las pruebas sin permiso pueden ser consideradas delitos informáticos.

---

20. Ciclo de Vida del Pentest

Secuencia estructurada de actividades que va desde la planificación y recolección de información hasta la elaboración del informe final y acciones correctivas.
