📘 Glosario: Técnicas de Reconocimiento y Escaneo en Seguridad Informática

---

1. Reconocimiento

Fase inicial en una prueba de penetración que consiste en recolectar información sobre el objetivo para identificar posibles vectores de ataque.

---

2. Reconocimiento Pasivo

Técnica que permite recopilar información sin interactuar directamente con el sistema objetivo, minimizando el riesgo de detección.

---

3. Reconocimiento Activo

Proceso de recolección de información que implica consultas directas al sistema objetivo, como DNS o servicios de red, con mayor probabilidad de ser detectado.

---

4. WHOIS

Protocolo y herramienta utilizada para obtener información pública sobre registros de dominios, incluyendo contactos administrativos, fechas y servidores DNS.

---

5. TheHarvester

Herramienta de recolección de información que permite obtener correos electrónicos, subdominios y nombres de usuario desde motores de búsqueda y redes sociales.

---

6. Shodan

Buscador especializado en dispositivos conectados a internet (IoT), que permite descubrir servidores, cámaras, routers, y otros sistemas expuestos públicamente.

---

7. NSLookup

Comando que permite consultar registros DNS específicos (como A, MX, CNAME) de un dominio, útil para el reconocimiento activo.

---

8. DIG (Domain Information Groper)

Herramienta avanzada de consulta DNS que permite obtener detalles técnicos extensos sobre dominios y servidores asociados.

---

9. Escaneo de Puertos

Técnica utilizada para identificar qué puertos están abiertos en un sistema y qué servicios están escuchando en ellos.

---

10. Nmap

Herramienta de escaneo de red ampliamente utilizada que permite descubrir hosts, puertos abiertos, versiones de servicios y vulnerabilidades mediante scripts NSE.

---

11. NSE (Nmap Scripting Engine)

Motor de scripting de Nmap que permite ejecutar scripts predefinidos para realizar tareas avanzadas como detección de vulnerabilidades, autenticación y fuzzing.

---

12. Nessus

Escáner de vulnerabilidades comercial desarrollado por Tenable. Realiza análisis de seguridad profundos en sistemas, redes y servicios.

---

13. OpenVAS

(Open Vulnerability Assessment System) Escáner de código abierto que permite realizar auditorías de seguridad completas en redes y servidores.

---

14. Vulnerabilidad

Debilidad en un sistema o aplicación que puede ser explotada para comprometer su confidencialidad, integridad o disponibilidad.

---

15. Simulación de Ataques

Proceso controlado de explotación de vulnerabilidades con el fin de validar su impacto real y evidenciar la necesidad de correcciones.

---

16. Metasploit Framework

Entorno modular para la explotación de vulnerabilidades, pruebas de post-explotación, generación de payloads y automatización de ataques controlados.

---

17. SQLMap

Herramienta automatizada para detectar y explotar inyecciones SQL en aplicaciones web. Facilita la extracción de bases de datos en entornos vulnerables.

---

18. Auditoría de Seguridad

Evaluación técnica sistemática que permite identificar debilidades en redes, sistemas o aplicaciones, con el fin de mitigarlas antes de ser explotadas.

---

19. Ética Profesional

Conjunto de principios y normas que regulan el comportamiento responsable de los profesionales de la ciberseguridad, asegurando que sus acciones sean legales y autorizadas.

---

20. Autorización Explícita

Permiso formal y documentado que debe ser obtenido antes de realizar cualquier tipo de prueba de seguridad sobre un sistema ajeno.
