📘 Glosario Técnico Profesional: Escaneo y Enumeración de Servicios con Python y Nmap

---

1. Escaneo de Puertos

Técnica utilizada para identificar qué puertos de red están abiertos o activos en un sistema objetivo. Los puertos abiertos indican servicios en ejecución, lo que permite al analista mapear la exposición real del dispositivo. Es la base del reconocimiento activo en auditorías de seguridad.

---

2. Enumeración de Servicios

Proceso de recopilación de información detallada sobre los servicios detectados tras un escaneo, incluyendo nombre del servicio, versión del software, sistema operativo, banners y posibles módulos o plugins. Esta etapa permite correlacionar vulnerabilidades conocidas y priorizar acciones correctivas.

---

3. Nmap (Network Mapper)

Herramienta de código abierto diseñada para escaneo de redes y detección de servicios. Nmap puede identificar hosts activos, servicios en ejecución, sistemas operativos, políticas de firewall y vulnerabilidades comunes. Es ampliamente utilizada tanto en pentesting como en administración de red.

---

4. python-nmap

Librería de Python que permite interactuar con Nmap de forma programática. Facilita la automatización de escaneos, el procesamiento de resultados y la integración en flujos personalizados de análisis de seguridad, monitoreo o respuesta a incidentes.

---

5. TCP SYN Scan (-sS)

Técnica de escaneo que envía paquetes SYN para identificar puertos abiertos sin completar el handshake TCP. Es rápido y discreto, y por ello, uno de los métodos preferidos en auditorías de seguridad no intrusivas.

---

6. Detección de Versión (-sV)

Modo de escaneo en Nmap que intenta identificar la versión exacta de los servicios que se ejecutan en puertos abiertos. Permite correlacionar automáticamente con vulnerabilidades conocidas (por ejemplo, CVEs).

---

7. Escaneo Avanzado (-A)

Opción en Nmap que habilita múltiples técnicas de análisis: detección de sistema operativo, traceroute, scripts NSE (Nmap Scripting Engine), y fingerprinting detallado de servicios. Se utiliza cuando se requiere un perfil completo del objetivo.

---

8. CVE (Common Vulnerabilities and Exposures)

Base de datos pública que cataloga vulnerabilidades conocidas de software. Cada vulnerabilidad tiene un identificador único (ej. CVE-2023-1234). Se utiliza para correlacionar resultados de escaneo con riesgos reales y priorizar mitigaciones.

---

9. Reconocimiento Activo

Fase del análisis de seguridad en la que se interactúa directamente con los sistemas objetivo, mediante solicitudes de red o pruebas controladas, con el fin de recolectar información técnica concreta. A diferencia del reconocimiento pasivo, implica riesgo y debe realizarse con autorización.

---

10. Seguridad Preventiva Automatizada

Enfoque que incorpora herramientas automáticas para detectar puntos débiles en infraestructura de forma continua y sin intervención humana directa. Combina escaneo programado, análisis de resultados, generación de alertas y retroalimentación para mitigar amenazas antes de que sean explotadas.
