📘 Glosario Técnico Profesional: Reconocimiento de Superficies de Ataque en Python

---

1. Superficie de Ataque

Conjunto de todos los puntos de entrada, exposición o interacción que pueden ser aprovechados por un atacante para comprometer la seguridad de un sistema. Incluye rutas web, formularios, cabeceras, API endpoints, subdominios, entre otros. Su análisis permite anticiparse a vectores de explotación comunes.

---

2. Requests (Python)

Biblioteca HTTP para Python que facilita la realización de peticiones GET, POST, PUT, DELETE, entre otras. Es ampliamente utilizada en el reconocimiento automático de servicios web para verificar disponibilidad, interpretar códigos de respuesta y analizar encabezados de red. Su simplicidad la convierte en estándar de facto para scripts de reconocimiento.

---

3. BeautifulSoup

Librería de Python que permite analizar documentos HTML y XML, facilitando la extracción estructurada de elementos como etiquetas, formularios, enlaces y parámetros. Se utiliza en ciberseguridad para el descubrimiento automatizado de puntos de entrada dentro del DOM de aplicaciones web.

---

4. Enumeración de Directorios (Directory Bruteforcing)

Técnica de reconocimiento que consiste en intentar acceder a rutas y archivos comunes o sensibles de una aplicación web (`/admin`, `/backup.zip`, `/config`). Se realiza con diccionarios predefinidos y puede automatizarse con scripts en Python. Es fundamental en la etapa de mapeo de superficie expuesta.

---

5. Fingerprinting Web

Proceso de identificación de tecnologías, frameworks y configuraciones utilizadas por una aplicación a partir de información como cabeceras HTTP, cookies, comportamiento del servidor o estructura del código HTML. Es clave para personalizar ataques posteriores y seleccionar vectores de intrusión eficaces.

---

6. Reconocimiento Pasivo

Método de recopilación de información sin interactuar directamente con el objetivo. Incluye búsquedas en motores de indexación (Google Dorking), exploración de metadatos en documentos públicos, o análisis de registros DNS y WHOIS. Aunque Python no se usa directamente en todas estas tareas, puede automatizar gran parte de ellas.

---

7. Enumeración Activa

Contraparte del reconocimiento pasivo, donde el analista interactúa directamente con la aplicación objetivo para descubrir rutas, formularios, servicios o configuraciones expuestas. Incluye el uso de peticiones HTTP controladas, escaneo de puertos o pruebas sobre parámetros. Python permite automatizar esta enumeración con alta precisión.

---

8. Subdominios Expuestos

Partes del dominio principal que pueden apuntar a servicios independientes y a menudo mal configurados o desactualizados (`admin.ejemplo.com`, `dev.ejemplo.com`). Son objetivos comunes durante el reconocimiento, ya que su exploración puede revelar entornos vulnerables no documentados.

---

9. Enumeración de Formularios

Análisis estructurado de los formularios de entrada en una aplicación web para identificar posibles puntos de inyección, parámetros manipulables o falta de validación del lado del servidor. Python, junto a librerías como BeautifulSoup, permite automatizar la detección y categorización de estos elementos.

---

10. Ética del Pentesting

Conjunto de principios que regulan la práctica responsable del reconocimiento y análisis de seguridad. Incluye obtener autorización explícita, limitar el impacto de las pruebas, proteger los datos recolectados y reportar hallazgos de manera profesional. En entornos educativos o laborales, su cumplimiento es obligatorio para evitar consecuencias legales.
