# 📘 Glosario: Fundamentos de Python en Ciberseguridad y Hacking Ético

---

## 1. Python

Lenguaje de programación interpretado, de alto nivel, multiplataforma y con una sintaxis clara. Es ampliamente utilizado en ciberseguridad por su flexibilidad, facilidad de aprendizaje y disponibilidad de librerías especializadas.

---

## 2. Lenguaje Interpretado

Tipo de lenguaje en el que el código fuente se ejecuta línea por línea mediante un intérprete, sin necesidad de compilación previa.

---

## 3. Multiplataforma

Capacidad de un software o lenguaje de programación para ejecutarse en diversos sistemas operativos como Linux, Windows y macOS sin modificar su código fuente.

---

## 4. Sintaxis Clara

Característica de los lenguajes de programación que permite escribir código fácil de leer, comprender y mantener. Python es reconocido por su sintaxis sencilla y cercana al lenguaje natural.

---

## 5. Paradigmas de Programación

Modelos de diseño de software. Python admite paradigmas estructurado, orientado a objetos y funcional, lo que le otorga gran flexibilidad.

---

## 6. Script

Archivo de código que automatiza tareas específicas. En seguridad, se usan scripts Python para escaneo, análisis, explotación y monitoreo.

---

## 7. Bibliotecas (Librerías)

Colección de módulos y funciones predefinidas que extienden las capacidades de Python, por ejemplo: `requests`, `socket`, `scapy`.

---

## 8. Exploit

Fragmento de código que aprovecha una vulnerabilidad en un sistema para ejecutar acciones no autorizadas.

---

## 9. Payload

Parte del exploit que realiza una acción específica dentro del sistema vulnerable, como abrir una shell o extraer información.

---

## 10. PoC (Proof of Concept)

Demostración técnica que valida la existencia y explotación de una vulnerabilidad en condiciones controladas.

---

## 11. Análisis Forense Digital

Proceso de recuperación y análisis de evidencia digital desde dispositivos comprometidos, usando herramientas como `Volatility`.

---

## 12. Volatility

Framework en Python especializado en análisis de memoria RAM para investigaciones forenses.

---

## 13. OWASP ZAP

Herramienta de análisis de vulnerabilidades en aplicaciones web, escrita en Java pero frecuentemente utilizada desde scripts Python.

---

## 14. SQLmap

Herramienta escrita en Python para detectar y explotar vulnerabilidades de inyección SQL en bases de datos web.

---

## 15. SET (Social Engineering Toolkit)

Framework en Python para realizar simulaciones de ataques de ingeniería social, como campañas de phishing controladas.

---

## 16. Scapy

Librería Python para manipular paquetes de red a bajo nivel, útil en análisis de tráfico, escaneo y spoofing.

---

## 17. Nmap

Herramienta de escaneo de red que puede ser integrada y automatizada mediante scripts Python.

---

## 18. Snort

Sistema de detección de intrusos (IDS) que puede ser complementado con soluciones personalizadas en Python para alertas y monitoreo.

---

## 19. IDS (Intrusion Detection System)

Sistema que supervisa redes o sistemas en busca de actividades maliciosas o violaciones de políticas de seguridad.

---

## 20. Cracking

Técnica para romper contraseñas o cifrados mediante ataques por diccionario, fuerza bruta u otros métodos.

---

## 21. John the Ripper

Herramienta para análisis de contraseñas y cracking, la cual integra scripts Python para automatización.

---

## 22. Requests

Librería Python para realizar peticiones HTTP de forma sencilla, muy útil en scripts de auditoría o scraping.

---

## 23. Socket

Módulo en Python que permite establecer conexiones de red en bajo nivel, clave para desarrollar herramientas de red.

---

## 24. Anaconda

Distribución de Python que permite gestionar entornos virtuales, dependencias y librerías de forma sencilla.

---

## 25. Spyder

IDE (Entorno de Desarrollo Integrado) para Python, orientado a científicos de datos y analistas de seguridad.

---

## 26. Jupyter Notebook

Entorno interactivo en navegador que permite crear y documentar código Python de forma reproducible y visual.

---

## 27. PTES (Penetration Testing Execution Standard)

Marco internacional de buenas prácticas para realizar pruebas de penetración estructuradas.

---

## 28. Curva de Aprendizaje

Medida de la facilidad o dificultad para aprender una tecnología. Python destaca por tener una curva de aprendizaje baja.

---

## 29. SIEM

Security Information and Event Management. Plataforma que centraliza registros de seguridad y genera alertas sobre eventos sospechosos.

---

## 30. Entorno de Desarrollo

Conjunto de herramientas y configuraciones utilizadas para escribir, probar y depurar código. En Python destacan Anaconda, Spyder y Jupyter.

---