📘 Glosario: Entornos Controlados, Herramientas de Pentesting y Ciberseguridad Ofensiva

---

1. Pentesting (Prueba de Penetración)

Simulación controlada y autorizada de un ataque cibernético contra sistemas, redes o aplicaciones con el fin de identificar y mitigar vulnerabilidades antes de que sean explotadas por actores maliciosos.

---

2. Entorno Controlado

Infraestructura tecnológica aislada diseñada para realizar pruebas de seguridad sin afectar los sistemas productivos. Permite practicar técnicas ofensivas de forma segura y legal.

---

3. Kali Linux

Distribución de Linux basada en Debian especializada en seguridad informática. Desarrollada por Offensive Security, incluye más de 600 herramientas para pruebas de penetración, auditorías y análisis forense.

---

4. Vulnhub

Plataforma comunitaria que proporciona máquinas virtuales con vulnerabilidades intencionales para prácticas de hacking ético. Utilizada en simulaciones realistas y desafíos de ciberseguridad.

---

5. Docker

Tecnología de contenedores que permite desplegar aplicaciones y entornos aislados de forma rápida, ligera y reproducible. Muy útil para simular servicios vulnerables y escenarios de ataque.

---

6. VirtualBox / VMware

Software de virtualización que permite ejecutar máquinas virtuales en sistemas anfitriones. Facilita la práctica en entornos controlados como los distribuidos por Vulnhub.

---

7. APT (Advanced Package Tool)

Sistema de gestión de paquetes en Debian y derivados como Kali Linux. Permite instalar, actualizar y eliminar programas desde la terminal.

---

8. Nmap

Herramienta de escaneo de redes que permite descubrir hosts activos, puertos abiertos, servicios y sistemas operativos en una red.

---

9. Metasploit Framework

Plataforma de pruebas de penetración que permite el desarrollo, prueba y ejecución de exploits. Incluye módulos de explotación, payloads y post-explotación.

---

10. SQLMap

Herramienta automatizada que detecta y explota vulnerabilidades de inyección SQL en aplicaciones web. Capaz de extraer bases de datos y comprometer sistemas vulnerables.

---

11. DVWA (Damn Vulnerable Web Application)

Aplicación web intencionalmente vulnerable utilizada para pruebas de seguridad ofensiva. Disponible como máquina virtual o contenedor Docker.

---

12. OWASP ZAP

(Zed Attack Proxy) Herramienta open-source para pruebas de seguridad en aplicaciones web. Permite interceptar, modificar y analizar el tráfico HTTP.

---

13. Burp Suite

Suite de herramientas profesionales para auditoría de aplicaciones web. Incluye proxy, escáner de vulnerabilidades, repeater, intruder, entre otros.

---

14. Live USB / Live CD

Modo de ejecución de sistemas operativos como Kali Linux directamente desde medios extraíbles sin necesidad de instalación en disco.

---

15. Red NAT / Solo-Anfitrión

Modos de configuración de red en máquinas virtuales que permiten el aislamiento o la conexión controlada entre el host y la VM para fines de pruebas.

---

16. Exploit

Código o técnica que aprovecha una vulnerabilidad para comprometer un sistema, obtener acceso o ejecutar comandos no autorizados.

---

17. Shell

Entorno interactivo donde el usuario puede ejecutar comandos. En pentesting, obtener una shell en el sistema objetivo indica que se ha comprometido.

---

18. Fuzzing

Técnica utilizada para descubrir errores o vulnerabilidades enviando datos aleatorios, inválidos o inesperados a una aplicación.

---

19. Escaneo de Puertos

Proceso de envío de paquetes a una IP para identificar qué servicios están activos en qué puertos. Técnica común en la fase de reconocimiento.

---

20. Autorización Explícita

Permiso documentado y formal requerido antes de realizar pruebas ofensivas sobre un sistema o red, de acuerdo con principios éticos y legales.
