📚 Glosario – Metodología del Hacking Ético

🔒 Burp Suite

Plataforma integrada de pruebas de seguridad para aplicaciones web. Permite interceptar, modificar y automatizar peticiones HTTP/S. Su versión profesional incluye herramientas avanzadas para la explotación de vulnerabilidades.

🧠 CVSS (Common Vulnerability Scoring System)

Sistema estandarizado para asignar puntuaciones a vulnerabilidades en función de su severidad, impacto y facilidad de explotación. Utilizado para priorizar correcciones en entornos empresariales.

🧱 Dirbuster / Gobuster

Herramientas para realizar ataques de fuerza bruta sobre directorios y archivos web ocultos. Permiten descubrir rutas no indexadas que pueden exponer información sensible.

🛠️ Enumeración

Fase del hacking ético que implica identificar servicios, usuarios, sistemas operativos y otras estructuras accesibles en la red del objetivo. Se apoya en técnicas activas que revelan información detallada del entorno.

💥 Explotación

Proceso mediante el cual un atacante ético aprovecha vulnerabilidades detectadas para comprometer sistemas, obtener acceso no autorizado o alterar el funcionamiento normal del sistema.

🔎 Google Dorks

Consultas avanzadas en motores de búsqueda que permiten localizar información sensible (como archivos, configuraciones o datos expuestos) utilizando operadores específicos.

🛡️ Hacking Ético

Práctica profesional de realizar pruebas controladas sobre sistemas informáticos con el propósito de detectar y corregir vulnerabilidades antes de que sean explotadas por actores maliciosos. Requiere autorización y adherencia a marcos legales y éticos.

📋 Informe Técnico de Pentesting

Documento final del proceso de hacking ético que detalla hallazgos, impacto potencial, evidencias técnicas y recomendaciones de remediación. Debe estar dirigido tanto a audiencias técnicas como a nivel gerencial.

🌐 Maltego

Herramienta de análisis de relaciones y visualización de inteligencia de fuentes abiertas (OSINT), que permite mapear entidades y conexiones entre dominios, correos, IPs y redes sociales.

💻 Metasploit Framework

Marco modular para desarrollar, probar y ejecutar exploits contra objetivos vulnerables. Incluye herramientas para post-explotación como Meterpreter, automatización de payloads y evasión de antivirus.

🧩 Meterpreter

Shell interactiva avanzada incluida en Metasploit que permite realizar tareas post-explotación como escalar privilegios, capturar contraseñas o pivotar hacia otras máquinas.

🧮 Nmap (Network Mapper)

Escáner de red que permite descubrir hosts y servicios en una red. Utiliza paquetes personalizados para detectar puertos abiertos, sistemas operativos, versiones de servicios, y posibles vulnerabilidades.

🌍 OSINT (Open Source Intelligence)

Conjunto de técnicas para recopilar información desde fuentes públicas o abiertas como motores de búsqueda, redes sociales, bases de datos públicas, entre otros. Fundamental en las primeras fases del reconocimiento.

🗒️ OWASP Testing Guide

Guía oficial de OWASP que ofrece una metodología estandarizada para evaluar la seguridad de aplicaciones web, incluyendo pruebas específicas para los 10 riesgos más comunes del OWASP Top 10.

🧠 Pentesting (Penetration Testing)

Evaluación controlada de seguridad donde se simulan ataques reales para identificar y corregir vulnerabilidades en aplicaciones, redes o sistemas. El pentesting es una práctica central del hacking ético.

🔗 Pivoting

Técnica avanzada de post-explotación que permite utilizar una máquina comprometida como punto de salto para acceder a otros sistemas internos no accesibles directamente desde el exterior.

📊 PTES (Penetration Testing Execution Standard)

Estándar internacional que define las fases del pentesting profesional: desde la planificación y modelado de amenazas hasta el análisis post-explotación y la documentación final.

🔁 Reconocimiento

Primera fase del hacking ético donde se recopila información sobre el objetivo, tanto pasivamente (sin interacción directa) como activamente (mediante escaneo). Esta fase es clave para diseñar una estrategia de ataque eficaz.

🔐 SQLMap

Herramienta de código abierto para automatizar la detección y explotación de vulnerabilidades de inyección SQL en aplicaciones web. Puede realizar extracción de bases de datos completas.

🔧 Shodan

Motor de búsqueda especializado en dispositivos conectados a Internet. Permite encontrar servidores, cámaras, routers y otros dispositivos accesibles públicamente con información detallada de su configuración y servicios.

⏱️ Schedule Plan / Gantt

Herramientas de planificación que permiten dividir el proceso de pentesting en fases controladas por tiempo. Usadas para gestionar recursos, tiempos de ejecución y validación de resultados.
