📘 Glosario – Hacking Ético y Ciberseguridad

🔐 Activo Digital

Cualquier recurso informático con valor para una organización, como datos, sistemas, aplicaciones o infraestructura.

💥 Ataque Informático

Acción maliciosa que intenta dañar, interrumpir o acceder sin autorización a sistemas o datos digitales.

🧠 Auditoría de Seguridad

Evaluación técnica y/o procedimental de los sistemas de una organización para verificar su nivel de protección frente a amenazas.

👩‍💻 Certified Ethical Hacker (CEH)

Certificación internacional otorgada por EC-Council que valida las habilidades técnicas y éticas necesarias para realizar hacking ético de forma profesional.

🔎 Confidencialidad

Principio que garantiza que la información solo será accesible por personas autorizadas y se mantendrá protegida de divulgaciones indebidas.

📜 Convenio de Budapest

Tratado internacional sobre ciberdelincuencia que promueve la cooperación legal entre países para combatir los delitos informáticos.

⚖️ CFAA (Computer Fraud and Abuse Act)

Ley estadounidense que regula y penaliza el acceso no autorizado a sistemas informáticos.

🔧 Evaluación de Vulnerabilidades

Proceso sistemático para identificar, clasificar y priorizar debilidades en un sistema que pueden ser explotadas por atacantes.

👥 GPEN (GIAC Penetration Tester)

Certificación emitida por el SANS Institute que valida habilidades avanzadas en pruebas de penetración.

🔍 Hacking Ético

Práctica autorizada y regulada de realizar pruebas de seguridad sobre sistemas informáticos con el fin de identificar y mitigar vulnerabilidades.

📊 ISO/IEC 27001

Norma internacional que define los requisitos para establecer, implementar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

🛠️ Metodología OSSTMM

(Open Source Security Testing Methodology Manual): Protocolo abierto para evaluar seguridad desde diversas dimensiones, como la humana, física, digital y wireless.

🌐 Metodología OWASP Testing Guide

Guía estándar desarrollada por OWASP para evaluar la seguridad de aplicaciones web mediante pruebas técnicas estructuradas.

📚 NIST SP 800-115 / 800-53

Publicaciones del Instituto Nacional de Estándares y Tecnología (EE.UU.) que proporcionan lineamientos y controles técnicos para auditorías y seguridad informática.

🤝 Permiso Previo / Autorización Formal

Consentimiento legal otorgado por el propietario de un sistema, indispensable para realizar cualquier actividad de hacking ético.

👩‍⚖️ Proporcionalidad

Principio que orienta a los profesionales del hacking ético a limitar la intrusión o daño potencial a lo estrictamente necesario durante una prueba.

📘 Reglamento General de Protección de Datos (RGPD)

Normativa de la Unión Europea que regula la recopilación, almacenamiento y procesamiento de datos personales, aplicable también al hacking ético.

🧾 Reporte Técnico

Documento formal generado por un hacker ético que detalla hallazgos, impactos potenciales y recomendaciones de seguridad tras una auditoría.

👩‍🎓 Responsabilidad Profesional

Compromiso ético y legal que asume el profesional para actuar con integridad, respetando leyes, normas y estándares del sector.

👩‍🔬 Tester de Penetración (Pentester)

Especialista en ciberseguridad que realiza pruebas controladas de intrusión para detectar y corregir vulnerabilidades.

🧱 Vulnerabilidad

Debilidad técnica o lógica en un sistema, red o aplicación que puede ser explotada por un atacante para comprometer su seguridad.
