🧠 Glosario – Roles y Responsabilidades del Hacker Ético

🔐 Analista de Seguridad Informática

Profesional encargado de monitorear, detectar e investigar amenazas a los sistemas informáticos en tiempo real. Utiliza herramientas como SIEM, IDS y IPS para prevenir y responder ante incidentes de seguridad.

🕵️ Auditor de Seguridad Informática

Especialista en evaluar el cumplimiento de normas, políticas y controles de seguridad de una organización. Realiza auditorías técnicas y administrativas conforme a estándares internacionales como ISO/IEC 27001 o NIST.

👩‍💻 Hacker Ético

Profesional autorizado para simular ataques informáticos con el fin de descubrir vulnerabilidades en los sistemas antes de que sean explotadas por ciberdelincuentes. Su trabajo se rige por principios éticos y marcos normativos.

💻 Pentester (Penetration Tester)

Especialista que realiza pruebas de penetración controladas para evaluar la seguridad de redes, aplicaciones o sistemas. Su objetivo es identificar y reportar debilidades técnicas que puedan ser explotadas.

✅ Consentimiento y Autorización

Principio fundamental del hacking ético que exige obtener un permiso formal, explícito y documentado por parte de la organización antes de realizar cualquier prueba o análisis de seguridad.

🔒 Confidencialidad

Compromiso ético y legal de proteger toda la información sensible accedida durante las pruebas de seguridad, evitando su divulgación o mal uso, en cumplimiento con normativas como el GDPR o leyes locales.

📣 Transparencia

Obligación de comunicar los hallazgos de seguridad de forma clara, completa y oportuna, sin ocultar ni minimizar vulnerabilidades. Garantiza una toma de decisiones informada por parte de la organización.

⚖️ Conflicto de Interés

Situación en la que un profesional podría verse influenciado por intereses personales, económicos o externos, comprometiendo su objetividad. El hacker ético debe evitar estos escenarios para mantener la integridad de su trabajo.

📚 ISO/IEC 27001

Norma internacional que establece los requisitos para implementar y gestionar un sistema de gestión de seguridad de la información (SGSI). Es uno de los marcos más utilizados en auditoría y cumplimiento en ciberseguridad.

🔍 OWASP (Open Web Application Security Project)

Organización sin fines de lucro que publica estándares abiertos para mejorar la seguridad del software, como el OWASP Top 10, utilizado comúnmente en pruebas de seguridad de aplicaciones web.

🧪 NIST SP 800-115

Guía técnica del Instituto Nacional de Estándares y Tecnología (NIST) para realizar pruebas de seguridad de sistemas de información. Establece métodos para evaluaciones controladas y efectivas.

🔎 SIEM (Security Information and Event Management)

Plataforma que centraliza la recopilación, análisis y correlación de eventos de seguridad en una red. Es utilizada por analistas para detectar incidentes de forma eficiente.

🚨 IDS/IPS (Intrusion Detection/Prevention Systems)

Sistemas que detectan (IDS) o bloquean (IPS) actividades maliciosas dentro de una red o sistema. Son herramientas clave para el monitoreo activo en ciberseguridad.

🌐 GDPR (General Data Protection Regulation)

Reglamento General de Protección de Datos de la Unión Europea. Establece lineamientos sobre la recopilación, procesamiento y protección de datos personales. Su incumplimiento puede generar sanciones graves.
