CARTOGRAFIANDO EL PENTESTING : ANÁLISIS COMPARATIVO DE METODOLOGÍAS DE SEGURIDAD INFORMÁTICA

CNO V – SEGURIDAD INFORMATICA

Juan Alejandro Pérez Ventura
180370@upslp.edu.mx

Metodología	Descripción breve	Fases de implementación	Objetivo principal	Escenarios de uso	Orientación
MITRE ATT&CK	Marco que documenta técnicas reales usadas por atacantes.	Basado en tácticas y técnicas (TTPs), no fases formales.	Mejorar detección y respuesta ante ataques.	SOC, Blue Team, Red Team, monitoreo de amenazas.	Defensa / Evaluación
OWASP WSTG	Guía para evaluar vulnerabilidades en aplicaciones web.	Revisión, análisis, pruebas manuales, explotación y reporte.	Detectar fallas en aplicaciones web.	Bancos, fintech, e-commerce.	Evaluación / Ataque ético
NIST SP 800-115	Norma formal para auditorías de seguridad.	Planeación, descubrimiento, pruebas, reporte.	Cumplimiento y control de riesgos.	Gobierno, corporativos, compliance.	Evaluación / Defensa
OSSTMM	Metodología integral para redes, procesos y seguridad física.	Análisis de vectores, métricas, validación y reporte.	Medir nivel real de seguridad operativa.	Auditorías completas empresariales.	Evaluación / Auditoría
PTES	Estándar práctico para pruebas de intrusión profesionales.	Acuerdos, reconocimiento, explotación, post-explotación, informe.	Ejecutar pentesting profesional.	Consultoras, ethical hacking.	Ataque / Evaluación
ISSAF	Marco antiguo para evaluaciones técnicas y organizacionales.	Recopilación, mapeo, explotación, análisis.	Evaluar infraestructura y procesos.	Auditorías tradicionales.	Evaluación

Metodología	Autor / Organismo responsable	URL de material	Certificaciones	Versiones vigentes
MITRE ATT&CK	MITRE Corporation	https://attack.mitre.org	No directa	Actualizaciones frecuentes
OWASP WSTG	OWASP Foundation	https://owasp.org/www-project-web-security-testing-guide/	Base para eWPT, OSCP	Versión 4.x activa
NIST SP 800-115	National Institute of Standards and Technology	https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-115.pdf	Base para CISSP, CISA	Vigente como referencia
OSSTMM	Institute for Security and Open Methodologies	https://www.isecom.org/OSSTMM.3.pdf	N/A (oficialmente)	Versión 3.x
PTES	Comunidad PTES	http://www.pentest-standard.org/	Base para OSCP, CEH	Estándar activo
ISSAF	Open Information Systems Security Group	https://bibdigital.epn.edu.ec/bitstream/15000/16740/1/CD-7336.pdf	N/A	Poca actualización

Referencias

¿Qué es el marco MITRE ATT&CK? (2024). Obtenido de https://www.ibm.com/mx-es/think/topics/mitre-attack

Guía de Pruebas de Seguridad Web (WSTG). (2024). Obtenido de https://devguide.owasp.org/es/06-verification/01-guides/01-wstg/

ISSAF – Marco de evaluación de seguridad de sistemas de información. (2017). Obtenido de https://bibdigital.epn.edu.ec/bitstream/15000/16740/1/CD-7336.pdf

NIST SP 800-115 – Marco de pruebas técnicas de seguridad. (2024). Obtenido de https://secureframe.com/es-es/frameworks-glossary/nist-800-115

OSSTMM – Manual Abierto de Metodología de Pruebas de Seguridad. (2023). Obtenido de https://www.isecom.org/OSSTMM.3.pdf

PTES – Estándar de ejecución de pruebas de penetración. (2023). Obtenido de http://www.pentest-standard.org/