UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Act. 5 Cartografiando el pentesting

CNO V – Seguridad Informática

Viernes 13 febrero, 2026

Elisa Alejandra Arellano Wratny

177339

Tabla de comparación

	MTRE ATT&CK	OWASP WSTG	NIST SP 800-115	OSSTMM	PTES	ISSAF
Descripción breve	Marco de conocimiento de tácticas, técnicas y procedimientos (TTPs) usados por adversarios para modelar ataques reales.	Guía de pruebas de seguridad para aplicaciones web (Web Security Testing Guide).	Guía técnica para pruebas de seguridad y evaluación de sistemas de información.	Manual abierto de pruebas de seguridad que cubre redes, sistemas, personas y procesos.	Estándar para ejecución de pruebas de penetración con fases claras y prácticas.	Marco de evaluación de seguridad de sistemas con guía amplia de pruebas.
Fases de	Es una matriz de tácticas y técnicas que cubre todo el ciclo de vida del ataque.	Suele organizarse en secciones de requisitos de pruebas, pero como guía técnica no sigue fases rígidas.	Planificación, recopilación de información, análisis de vulnerabilidades, explotación y reporte.	Identificación, análisis de vulnerabilidades, evaluación física/humana y reporte.	Pre-engagement, inteligencia, modelado de amenaza, snálisis de vulnerabilidades, explotación, post-explotación, reporte.	Incluye gestión de proyecto, pre-/post-assessment, técnica de pruebas, análisis, reportes y best practices.
Objetivo	Documentar y mapear técnicas de ataque para simulación, detección y respuesta.	Detectar vulnerabilidades en aplicaciones web.	Proveer un enfoque estructurado, repetible y documentado para pruebas técnicas.	Evaluación completa de seguridad operativa con métricas cuantificables.	Estandarizar el proceso de pentesting y guiar al tester en todas sus etapas.	Evaluar seguridad incluyendo procesos, controles y vulnerabilidades técnicas.

Escenarios uso	Red teaming, threat hunting, simulación de adversaries, pruebas de defensa y evaluación de controles.	Pentesting de aplicaciones web, APIs y servicios web.	Organizaciones que requieren cumplimiento normativo y evaluación formal (gobierno, empresas).	Seguridad organizacional amplia: redes, comunicaciones, físico y humano.	Pentesting general (redes, sistemas y aplicaciones integradas).	Empresas que buscan evaluación integral (técnica y organizacional).
Orientación	Defensa y evaluación.	Evaluación técnica enfocada al ataque de aplicaciones web.	Evaluación técnica con enfoque en cumplimiento y documentación.	Evaluación de seguridad, con fuerte rigor y medición (puede apoyar ataque y defensa).	Ataque y evaluación técnica estructurada.	Evaluación completa (técnica y organizativa).
Autores	MITRE Corporation	OWASP (Open Web Application Security Project).	NIST (Instituto Nacional de Estándares y Tecnología, EE. UU.).	ISECOM (The Institute for Security and Open Methodologies).	Comunidad de seguridad / Pentest Standard (grupo open).	InfoSec (historical / comunidad de evaluación).
URL oficial	https://attack.mitre.org/	https://owasp.org/www-project-web-security-testing-guide/	https://www.nist.gov/privacy-framework/nist-sp-800-115	https://www.isecom.org/OSSTMM.3.pdf	https://www.pentest standard.org/	No hay URL oficial simple, suele referenciarse en documentos académicos.
Certificaciones	No hay, pero hay cursos y prácticas alineadas.	No tiene certificación propia, pero se usa en certificaciones de pentesting (OSCP, CEH).	No hay certificación oficial, pero se usa como modelo en auditorías y pruebas certificadas (ISO/IEC, auditorías GRC).	Existen certificaciones OSSTMM relacionadas con ISECOM (por ejemplo, certificados de auditoría).	No existe certificación oficial PTES, pero es base de muchas prácticas profesionales.	No hay certificaciones específicas asociadas, es un marco de referencia clásico.
Versiones	Actualizado continuamente (Enterprise, Mobile, ICS)	WSTG v4.1 es la versión estable más reciente.	SP 800-115 (vigente como guía técnica)	OSSTMM v3 es la versión más usada (actualización menor con tiempo).	PTES ha evolucionado, pero mantiene 7 fases clave.	No hay actualizaciones frecuentes (histórico, usado como referencia).