UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

ACTIVIDAD 05: Cartografiando el pentesting: análisis comparativo de metodologías de seguridad informática

Carrera: ITI

Asignatura: CNO V Seguridad informática

Pablo de Jesús Salazar Hernández - 171580

Mtro. Servando López Contreras

13/02/2026

Metodología	Descripción	Fases de implementación	Objetivo principal	Escenarios de utilidad	Orientación	Autores u organismos responsabilidades	URL del material oficial	Existencia de certificaciones asociadas	Versiones o actualizaciones vigentes
MTRE ATT&CK	Marco de conocimiento que documenta tácticas y técnicas usadas por atacantes reales	Reconocimiento, Ejecución, Persistencia, Escalada de privilegios, Defensa evasiva, etc. (basado en tácticas).	Analizar y mejorar la detección y respuesta ante amenazas.	Threat hunting, análisis de malware, red team/blue team, SOC.	Defensa y análisis ofensivo.	MITRE	https://attack.mitre.org/	No ofrece certificación oficial propia.	Actualización continua (versión Enterprise, Mobile e ICS activas).
OWASP WSTG	Guía metodológica para pruebas de seguridad en aplicaciones web.	Información y recopilación, pruebas de configuración, autenticación, autorización, lógica de negocio, etc.	Estandarizar pruebas de penetración en aplicaciones web.	Pentesting web, auditorías de seguridad en aplicaciones.	Ofensiva (pentesting web).	OWASP	https://owasp.org/www-project-web-security-testing-guide/	No hay certificación directa del WSTG, pero OWASP tiene programas educativos.	Versión 4.2 (WSTG v4.2 vigente).
NIST SP 800-115	Guía técnica para pruebas y evaluación de seguridad en sistemas de	Planificación, descubrimiento, ataque, reporte.	Proporcionar lineamientos formales para pruebas técnicas de seguridad.	Auditorías gubernamentales, evaluación de controles, cumplimiento	Evaluación formal y cumplimiento.	National Institute of Standards and Technology (NIST)	https://csrc.nist.gov/publications/detail/sp/800-115/final	No certificación específica del documento.	Publicación vigente (2008, aún referenciada oficialmente).

	información			normativo.					
OSSTMM	Metodología científica para pruebas de seguridad operacional	Inducción, Investigación, Interacción, Intervención.	Medir la seguridad operativa de forma cuantificable.	Auditorías físicas, humanas, telecomunicaciones y redes.	Ofensiva y auditoría integral.	ISECOM	https://www.isecom.org/OSSTMM.3.pdf	Sí, certificaciones profesionales de ISECOM.	OSSTMM 3.0 versión vigente.
PTES	Estándar técnico que define un proceso estructurado para pruebas de penetración	Pre-engagement, recopilación de información, modelado de amenazas, explotación, post-explotación, reporte.	Estandarizar el proceso completo de pentesting.	Pentesting empresarial y consultoría de seguridad.	Ofensiva.	Desarrollado por la comunidad de seguridad (Penetration Testing Execution Standard).	http://www.pentest-standard.org	No certificación oficial propia.	Documento base vigente sin versiones numeradas frecuentes.
ISSAF	Marco detallado para pruebas de seguridad estructuradas.	Planeación, evaluación, explotación, mantenimiento de acceso, reporte.	Proveer guía paso a paso para pruebas de penetración	Pentesting técnico profundo y formación.	Ofensiva.	Open Information Systems Security Group (OISSG)	http://www.oissg.org/issaf	No certificación oficial vigente.	Proyecto sin actualizaciones recientes formales.

Referencias

MITRE. (s. f.). MITRE ATT&CK® knowledge base. https://attack.mitre.org/

OWASP. (s. f.). OWASP Web Security Testing Guide (WSTG). https://owasp.org/www-project-web-security-testing-guide/

National Institute of Standards and Technology. (2008). Technical guide to information security testing and assessment (Special Publication 800-115). U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-115/final

ISECOM. (2010). Open Source Security Testing Methodology Manual (OSSTMM) 3.0. https://www.isecom.org/OSSTMM.3.pdf

Penetration Testing Execution Standard. (s. f.). PTES technical guidelines. http://www.pentest-standard.org

Open Information Systems Security Group. (s. f.). Information Systems Security Assessment Framework (ISSAF). http://www.oissg.org/issaf