UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Universidad Politécnica de San Luis Potosí

Materia:

Seguridad Informática

Octavo Semestre

Profesor:

Servando López Contreras

Alumna:

América Fabiola Guerra Ramírez - 179884

Tarea: Cartografiando el pentesting

Fecha de entrega: 13 de febrero de 2026

Introducción

El pentesting (penetration testing) es un proceso fundamental dentro de la Seguridad Informática, ya que permite evaluar la resistencia de un sistema, red o aplicación ante ataques reales. Existen diversas metodologías y estándares que guían estas pruebas, cada una con enfoques distintos dependiendo del tipo de organización que se buscan proteger.

En esta actividad se realiza una comparación estructurada de metodologías y marcos reconocidos internacionalmente, como MITRE ATT&CK, OWASP WSTG, NIST SP 800-115, OSSTMM, PTES e ISSAF, con el objetivo de identificar sus características principales, fases, objetivos, escenarios de aplicación y relevancia en el pentesting moderno.

Desarrollo

Metodología	*Descripción*	*Fases de implementación*	*Objetivo principal*	*Escenarios de uso*	*Orientación*	*Autores/ organismos*	*URL*	*Certificaciones asociadas*	*Versiones / vigencia*
MTRE ATT&CK	Es una base de conocimientos que recopila y organiza tácticas, técnicas y procedimientos (TTP) usados por atacantes reales, con el fin de modelar, detectar, prevenir y combatir amenazas cibernéticas basadas en comportamientos adversarios.	Reconocimiento Desarrollo de recursos Acceso inicial Ejecución Persistencia Escalamiento de privilegios Evasión de defensa Acceso a credenciales Descubrimiento Movimiento lateral Recopilación Comando y control Exfiltración Impacto	Crear un estándar de referencia para: detectar técnicas de ataque simular ataques reales mejorar defensas mediante mitigaciones fortalecer planes de respuesta a incidentes	Threat Hunting (caza de amenazas) clasificación de alertas y respuesta a incidentes evaluación de madurez de un SOC red teaming / emulación de adversarios diseño y mejora de controles de seguridad integración en SIEM, SOAR, EDR,	Defensiva / análisis de amenazas (Blue Team), con apoyo ofensivo. Porque permite clasificar técnicas reales usadas por atacantes, ayudando a detectar y mejorar controles de seguridad.	Desarrollado y mantenido por MITRE Corporation, organización sin fines de lucro, con apoyo de una comunidad global de ciberseguridad.	https://attack.mitre.org/	No tiene una certificación oficial propia directa, pero está muy ligado a certificaciones y entrenamientos de ciberseguridad como: Blue Team / SOC Analyst Red Team Threat Hunter certificaciones como OSCP, CEH, CISSP	Se actualiza continuamente. Matrices activas (Enterprise, Mobile, ICS).

				XDR y UEBA				(lo usan como referencia)	
OWASP WSTG	Es una comunidad abierta que desarrolla metodologías, guías y herramientas para mejorar la seguridad de aplicaciones web, móviles y APIs.	Requisitos Diseño Desarrollo Implementación Mantenimiento	Detectar y prevenir vulnerabilidades en aplicaciones web y APIs, especialmente las más comunes.	Desarrollo de software seguro Auditorías de aplicaciones web Pentesting de APIs Revisión de código	Ofensiva y preventiva Porque se usa para realizar pruebas de penetración web (ataque controlado), pero también sirve para prevenir vulnerabilidades durante el desarrollo seguro.	Comunidad global de OWASP Foundation.	https://owasp.org/	no tiene certificaciones oficiales propias, pero está muy ligada a certificaciones como: OSCP CEH eWPT	se actualiza periódicamente (la versión más reciente es OWASP Top 10: 2021 y próximas actualizaciones en desarrollo).
NIST SP 800-115	Es una guía técnica del NIST que describe procesos y recomendaciones para realizar pruebas de penetración y evaluaciones de seguridad en sistemas de	Revisión de documentación Escaneo y rastreo de red Evaluación de vulnerabilidades Ingeniería social Pentesting técnico	Proporcionar un marco técnico para la evaluación de controles de seguridad y reducción de riesgos de ciberataques.	Empresas financieras Organizaciones gubernamentales Auditorías profesionales Evaluación de infraestructura TI	Evaluación y auditoría defensiva. Porque está enfocada en evaluar controles de seguridad y riesgos de manera formal, para corregir	Creado por el NIST (National Institute of Standards and Technology).	https://csrc.nist.gov/publications/detail/sp/800-115/final	No tiene una certificación directa, pero se relaciona con certificaciones como: CISSP CISA CEH	La guía se mantiene vigente como referencia técnica. Es una publicación formal oficial del NIST.ç-

	información. Análisis de resultados Reporte y recomendaciones Corrección de vulnerabilidades				fallas antes de que sean explotadas			Security +	
OSSTMM	Realizar pruebas de seguridad operativa mediante métricas medibles y basadas en hechos	Seguridad humana Seguridad física Comunicaciones inalámbricas Telecomunicaciones Redes de datos	Evaluar de manera medible y estructurada la seguridad operativa de una organización.	Auditorías de seguridad empresarial Evaluación integral de infraestructura tecnológica Pruebas de seguridad física y humana (no solo digital)	Auditoría y medición (evaluación cuantitativa). Porque se centra en medir la seguridad usando métricas, considerando infraestructura tecnológica, humana y física.	Desarrollado por ISECOM (Institute for Security and Open Methodologies).	https://www.isecom.org/OSSTMM.3.pdf	OPST (OSSTMM Professional Security Tester)	La versión más conocida es OSSTMM 3.
PTES	Es un estándar que define un proceso claro para ejecutar pruebas de penetración, desde la	Recopilación de inteligencia Modelado de amenazas Análisis de vulnerabilidades	Guiar la ejecución de pruebas técnicas de penetración con resultados	Pentesting empresarial estándar Evaluación de redes corporativas	Ofensiva (pentesting técnico) con enfoque profesional. Porque describe el	Comunidad y equipo de expertos del estándar PTES.	http://www.pentest-standard.org/	No tiene certificación oficial propia, pero se usa como referencia en	El estándar se mantiene vigente en su sitio oficial y es

	recolección de información hasta el reporte final.	Explotación Reporte Post-explotación (seguimiento)	claros y documentados.	Auditorías técnicas de ciberseguridad	proceso típico de un pentest real: reconocimiento, explotación, post-explotación y reporte.			certificaciones como: OSCP CEH GPEN	ampliamente utilizado como guía práctica.
ISSAF	Es un marco completo para pruebas de seguridad que detalla herramientas, procedimientos y resultados esperados.	Recopilación de información Mapeo de red Identificación de vulnerabilidades Penetración Obtención y elevación de privilegios Mantenimiento del acceso Compromiso de usuarios/sitios remotos Eliminación de huellas del evaluador	Realizar pruebas de penetración exhaustivas simulando ataques reales.	Evaluación de seguridad empresarial completa Pentesting avanzado Auditorías profundas de redes y sistemas	Ofensiva avanzada / auditoría profunda. Porque incluye técnicas más detalladas y etapas avanzadas como escalamiento de privilegios, persistencia y eliminación de huellas.	Creado por OISSG (Open Information Systems Security Group).	http://www.oissg.org/issaf	No es común que tenga certificaciones oficiales directas ampliamente reconocidas.	Se considera una metodología estable, pero no se actualizan tan frecuentemente como OWASP o NIST.

Conclusión

Las metodologías de pentesting y evaluación de seguridad son esenciales para identificar riesgos y vulnerabilidades en organizaciones modernas. Cada estándar analizado cumple una función específica: MITRE ATT&CK se enfoca en el comportamiento del atacante, OWASP WSTG en aplicaciones web, NIST SP 800-115 en auditorías formales, OSSTMM en medición cuantitativa de seguridad, PTES en pruebas de penetración estructuradas e ISSAF en evaluaciones avanzadas.

En conclusión, la elección de una metodología depende del tipo de sistema evaluado y del objetivo de la organización. Sin embargo, combinar varios enfoques permite obtener resultados más completos, confiables y alineados a escenarios reales de ciberseguridad.

Referencias

ITGLOBAL.COM. (2024, 3 MARZO). [:EN-N;]PENETRETION TESTING: 5 METODOLOGIES OF PENTESTPENETRETION TESTING: 5 METODOLOGIES OF PENTEST. ITG MX. https://mx.itglobal.com/blog/5-metodologias-de-pruebas-de-penetracion/

FINN, T. (2025, 27 NOVIEMBRE). METODOLOGÍA DE PRUEBAS DE PENETRACIÓN. IBM. https://www.ibm.com/mx-es/think/insights/pen-testing-methodology

IBM. (2025, 26 NOVIEMBRE). MITRE ATTACK. IBM. https://www.ibm.com/mx-es/think/topics/mitre-attack