12-2-2026

Comparación de metodologías de pruebas de penetración y evaluación de seguridad informática

Ivan Ros Padilla
UNIVERSIDAD POLITECNICA DE SAN LUIS POTOSI

Metodología	Descripción breve	Fases principales	Objetivo principal	Escenarios de uso	Orientacion	Organismo	URL	Certificaciones	Version vigente
MITRE ATT&CK	Base de conocimiento que documenta tácticas y técnicas reales utilizadas por atacantes.	Reconocimiento de tácticas, identificación de técnicas, mapeo de controles, detección y mitigación.	Identificar técnicas de ataque y mejorar capacidades defensivas.	SOC, análisis de amenazas, red teaming, detección avanzada.	Defensa / Inteligencia de amenazas	MITRE Corporation	https://attack.mitre.org	No certificación oficial directa (usada en certificaciones de ciberseguridad).	Actualización continua (Enterprise v14+)
OWASP WSTG	Guía de pruebas de seguridad para aplicaciones web desarrollada por OWASP.	Recolección de información, pruebas de configuración, autenticación, autorización, lógica de negocio, etc.	Evaluar vulnerabilidades en aplicaciones web.	Auditorías web, pruebas de seguridad en desarrollo seguro.	Ataque / Evaluación técnica	OWASP Foundation	https://owasp.org/www-project-web-security-testing-guide/	OWASP ofrece certificaciones como OWASP Web Security Expert.	WSTG v4.2
NIST SP 800-115	Guía técnica para pruebas de seguridad y evaluación de controles en sistemas de información.	Planeación, descubrimiento, ataque, reporte.	Evaluar controles de seguridad en entornos gubernamentales y empresariales.	Auditorías formales, cumplimiento normativo, sector público.	Evaluación / Defensa	National Institute of Standards and Technology (NIST)	https://csrc.nist.gov/publications/detail/sp/800-115/final	Relacionada con certificaciones gubernamentales y cumplimiento.	Publicación vigente (2008, aún referenciada oficialmente)
OSSTMM	Metodología abierta para pruebas de seguridad operacional basada en métricas cuantificables.	Planeación, pruebas técnicas, análisis de resultados, métricas RAV.	Medir seguridad operativa mediante métricas objetivas.	Evaluaciones formales, auditorías técnicas completas.	Evaluación técnica	ISECOM	https://www.isecom.org/OSSTMM.3.pdf	OSSTMM Professional Security Tester (OPST).	OSSTMM 3
PTES	Estándar técnico para ejecución de pruebas de penetración estructuradas.	Pre-engagement, inteligencia, modelado de amenazas, explotación, post-explotación, reporte.	Estandarizar el proceso de pentesting profesional.	Pentesting empresarial, pruebas internas y externas.	Ataque estructurado	Comunidad PTES	http://www.pentest-standard.org	No certificación oficial propia, pero base para CEH, OSCP.	Documento estable desde 2014

ISSAF	Marco detallado para evaluación de seguridad estructurada en múltiples dominios.	Planeación, evaluación técnica, análisis, reporte.	Evaluar infraestructura, redes y sistemas.	Auditorías empresariales completas.	Evaluación técnica	OISSG (Open Information Systems Security Group)	https://www.oissg.org/issaf	No certificación oficial directa.	Marco estable

Conclusión

Las metodologías analizadas presentan diferencias claras en su enfoque, alcance y orientación estratégica. Mientras que MITRE ATT&CK se centra en la inteligencia de amenazas y defensa basada en tácticas reales, marcos como PTES y OWASP WSTG se orientan a pruebas técnicas ofensivas estructuradas. Por su parte, NIST SP 800-115 y OSSTMM priorizan la evaluación formal y la medición objetiva de controles de seguridad.

La selección de una metodología adecuada depende del contexto organizacional, el objetivo de la evaluación y el nivel de madurez en ciberseguridad. En entornos empresariales modernos, la combinación de varios marcos suele ofrecer mejores resultados que la aplicación aislada de uno solo.

Referencias

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

MITRE Corporation. (2024). MITRE ATT&CK® framework. https://attack.mitre.org

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

Open Information Systems Security Group (OISSG). (n.d.). Information Systems Security Assessment Framework (ISSAF). https://www.oissg.org/issaf

OWASP Foundation. (2023). OWASP web security testing guide (WSTG) v4.2. https://owasp.org/www-project-web-security-testing-guide/

Penetration Testing Execution Standard (PTES). (2014). Penetration testing execution standard technical guidelines. http://www.pentest-standard.org