



13 DE FEBRERO DE 2026

**ACTIVIDAD 05 -
CARTOGRAFIANDO EL PENTESTING:
ANÁLISIS
COMPARATIVO DE METODOLOGÍAS DE
SEGURIDAD
INFORMÁTICA**

CNOV SEGURIDAD INFORMATICA

AGUILAR ESPINOZA JUAN DIEGO
UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

En la ciberseguridad las metodologías de pruebas de penetración y evaluación son marcos de trabajo estructurados que guían a los profesionales para identificar, analizar y mitigar vulnerabilidades, aunque no todas las metodologías sirven para lo mismo ya que algunas se enfocan en aplicaciones web, otras en ataques reales y algunas en procesos técnicos a su vez utilizarlas garantiza que las evaluaciones sean profesionales.

Aspecto	MITRE ATT&CK	OWASP WSTG	NIST SP 800-115	OSSTMM	PTES	ISSAF
A. Descripción	Base de conocimiento global de tácticas y técnicas de adversarios basada en observaciones reales.	Guía exhaustiva para probar la seguridad de aplicaciones y servicios web.	Guía técnica para planificar y realizar evaluaciones de seguridad informática.	Metodología científica para el testeo de seguridad operacional y métricas.	Estándar diseñado para definir un lenguaje común y fases para pruebas de penetración.	Marco detallado para evaluaciones técnicas de sistemas de información.
B. Fases	Tácticas (Reconocimiento, Acceso Inicial, Ejecución, Persistencia, etc.).	Recopilación de info, Configuración, Identidad, Autenticación, Autorización, etc.	Planificación, Ejecución, Post-ejecución.	Seguridad Operacional, Confianza, Humana, Física, Inalámbrica, Telecomm, Datos.	Pre-acuerdo, Recolección de inteligencia, Modelado de amenazas, Análisis de vuln, Explotación, Post-explotación, Reporte.	Planificación, Evaluación (Reconocimiento, Escaneo, Enumeración, Explotación), Post-evaluación.
C. Objetivo Principal	Modelado de comportamiento de atacantes y detección de técnicas.	Pruebas técnicas específicas para aplicaciones web.	Evaluación técnica de controles y procesos de seguridad.	Medición de la seguridad operativa mediante métricas (RAV).	Estandarización de la calidad y profundización de un Pentest.	Evaluación técnica profunda de infraestructuras y sistemas.
D. Escenarios	Centros de Operaciones de Seguridad (SOC), Threat Hunting, Red Teaming.	Auditorías de aplicaciones web, desarrollo de software seguro (DevSecOps).	Auditorías gubernamentales y corporativas generales.	Auditorías de cumplimiento, seguridad física y de redes complejas.	Pruebas de penetración comerciales de alta calidad.	Evaluaciones técnicas detalladas de red y sistemas críticos.

E. Orientación	Defensa (Detección y respuesta).	Evaluación / Ataque (Web).	Evaluación (Procesos).	Evaluación (Operativa/Científica).	Ataque (Pentesting).	Ataque / Evaluación (Técnica).
F. Autores	MITRE Corporation.	OWASP Foundation.	NIST (EE. UU.).	ISECOM (Pete Herzog).	PTES Team (Expertos de la industria).	OISSG.
G. URL Oficial	attack.mitre.org	owasp.org	csrc.nist.gov	isecom.org	pentest-standard.org	oissg.org
H. Certificaciones	Certificaciones de vendor (ej. ATT&CK Defender).	No tiene una propia, pero influye en el OSWA de OffSec.	Ninguna específica (usada en certificaciones federales).	OPST, OPSA, OPSE.	No tiene certificación propia (es un estándar abierto).	No tiene certificación vigente activa.
I. Versión / Actualización	v14 (Actualización constante anual).	v4.2 (Actualizada periódicamente).	Versión Final (2008) - Sigue siendo referencia base.	v3.0 (v4 en desarrollo/borrador).	v1.0 (Actualización comunitaria).	v0.2.1 (Actualmente en desuso pero referencial).

Conclusiones

Como podemos observar en la tabla elegir una metodología depende del objetivo del proyecto, por ejemplo MITRE ATT&CK es indispensable para la defensa y entender al atacante, OWASP WSTG es el estándar por defecto para aplicaciones web, pero también PTES es la mejor opción para un consultor que busca entregar un reporte de pruebas de penetración completo, aunque en general se suelen combinar varias de estas para cubrir los requerimientos por completo.

Bibliografías

(No date) *MITRE ATT&CK®*. Available at: <https://attack.mitre.org/> (Accessed: 13 February 2026).

OWASP Web Security Testing Guide (no date) *OWASP Foundation*. Available at: <https://owasp.org/www-project-web-security-testing-guide/> (Accessed: 13 February 2026).

Scarfone, K., Souppaya, M., Cody, A. and Orebaugh, A. (2008) *Technical Guide to Information Security Testing and Assessment*, CSRC. Available at: <https://csrc.nist.gov/pubs/sp/800/115/final> (Accessed: 13 February 2026).

RESEARCH (no date) *ISECOM*. Available at: <https://www.isecom.org/research.html> (Accessed: 13 February 2026).

Main Page (no date) *The Penetration Testing Execution Standard*. Available at: http://www.pentest-standard.org/index.php/Main_Page (Accessed: 13 February 2026).