COMPARATIVA DE METODOLOGÍAS DE PENTESTING

JOSE ARMANDO PALOMO CERDA - 175932

CNO V - SEGURIDAD INFORMÁTICA | UPSLP

Fecha de Análisis: 13 de Febrero 2026

1. Objetivo del Análisis

El propósito de este artículo técnico es analizar de manera estructurada las principales metodologías y marcos de referencia utilizados en pruebas de penetración (pentesting). Al comparar sus enfoques, fases y orientaciones estratégicas, se busca fortalecer el criterio profesional para seleccionar la metodología adecuada según el entorno crítico a evaluar.

2. Tabla Comparativa de Metodologías Profesionales

METODOLOGÍA	DESCRIPCIÓN BREVE	FASES DE IMPLEMENTACIÓN	OBJETIVO PRINCIPAL	ORIENTACIÓN	ESCENARIOS DE USO	AUTORES / ENTIDAD
MITRE ATT&CK	Base de conocimientos global de tácticas y técnicas de adversarios basada en observaciones reales.	No lineal; se divide en Tácticas (ej. Acceso Inicial, Persistencia, Exfiltración).	Detección y clasificación de comportamientos de ataque.	Ataque / Defensa	Simulación de adversarios y auditorías de SOC.	MITRE Corporation (v14.1)
OWASP WSTG	Guía exhaustiva para pruebas de seguridad en aplicaciones web y servicios.	Recolección de info, Gestión de Identidad, Autenticación, Sesión, Validación de Datos.	Identificación de fallos lógicos y vulnerabilidades web.	Ataque / Evaluación	Aplicaciones Web, APIs, Portales Institucionales.	OWASP Foundation (v4.2)
NIST SP 800-115	Guía técnica fundamental para la realización de pruebas y exámenes de seguridad.	Planeación, Descubrimiento, Ejecución (Ataque), Reporte.	Estandarización de auditorías técnicas en organizaciones.	Evaluación	Sistemas federales, corporativos y cumplimiento normativo.	NIST (U.S. Dept. of Commerce)
OSSTMM	Estándar para la medición científica de la seguridad operativa.	Seguridad Humana, Física, Inalámbrica, Telecomunicaciones, Redes de Datos.	Medición del nivel de seguridad mediante métricas (RAV).	Evaluación / Operativa	Seguridad operativa integral y auditorías de confianza.	ISECOM (Pete Herzog) v3
PTES	Estándar diseñado para definir los requisitos mínimos de una prueba de penetración profesional.	Pre-engagement, Intelligence Gathering, Threat Modeling, Exploit, Post-Exploit.	Garantizar que el cliente reciba un pentesting de alta calidad técnica.	Ataque (Pentest)	Pentesting externo e interno de alto impacto.	Comité de Expertos (HD Moore et al.)
ISSAF	Marco de evaluación estructurado por dominios técnicos específicos.	Planeación, Evaluación, Reporte, Destrucción de Artefactos.	Evaluación granular de la arquitectura de seguridad.	Evaluación Técnica	Evaluación detallada de firewalls, VPNs e IDSs.	OISSG (v0.2.1)

Conclusión Metodológica

"La selección de una metodología no debe ser arbitraria. Mientras que MITRE ATT&CK es indispensable para la detección de ataques en curso, OWASP es la norma de facto para aplicaciones web. Por su parte, OSSTMM aporta la rigurosidad científica necesaria para medir la seguridad real, más allá del simple cumplimiento de listas de verificación. Un experto en ciberseguridad debe ser capaz de orquestar estos marcos para ofrecer una visión 360° del riesgo institucional."

Bibliografías

1. MITRE ATT&CK

MITRE Corporation. (2023). *MITRE ATT&CK® v14.1*. Recuperado de https://attack.mitre.org/

2. OWASP WSTG

OWASP Foundation. (2024). *Web Security Testing Guide (WSTG) version 4.2*. Recuperado de https://owasp.org/www-project-web-security-testing-guide/

3. NIST SP 800-115

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *Technical Guide to Information Security Testing and Assessment (NIST Special Publication 800-115)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-115

4. OSSTMM

Herzog, P. (2010). *Open Source Security Testing Methodology Manual (OSSTMM) version 3*. Institute for Security and Open Methodologies (ISECOM). Recuperado de https://www.isecom.org/OSSTMM.3.pdf

5. PTES (Penetration Testing Execution Standard)

PTES Technical Committee. (2014). *Penetration Testing Execution Standard (PTES)*. Recuperado de http://www.pentest-standard.org/index.php/Main_Page

6. ISSAF

OISSG Core Team. (2006). *Information Systems Security Assessment Framework (ISSAF) version 0.2.1*. Open Information Systems Security Group. Recuperado de https://www.google.com/search?q=https://web.archive.org/web/20120119150150/http://www.oissg.org/issaf/issaf0.2.1.pdf