Cartografiando el pentesting

Rodríguez Morin Estefano Alessandro

178584

CNO V: Seguridad Informática

16/02/2026

Introducción

La presente actividad consiste en un análisis técnico y comparativo de las metodologías y marcos de referencia más influyentes en el ámbito del *pentesting* y la evaluación de seguridad informática. A través de una investigación estructurada, se han catalogado seis estándares distintos:

- **MITRE ATT&CK**
- **OWASP WSTG**
- **NIST SP 800-115**
- **OSSTMM**
- **PTES**
- **ISSAF**

Desglosaremos sus fases operativas, objetivos estratégicos y contextos de aplicación. El propósito es establecer un criterio sólido que permita al profesional de ciberseguridad seleccionar la herramienta metodológica más adecuada según el activo a evaluar, garantizando procesos sistemáticos, repetibles y alineados con los estándares internacionales de la industria.

Metodología	A. Descripción	B. Fases de Implementación	C. Objetivo Principal	D. Escenarios de uso	E. Orientación	F. Autores /Organismo	G. URL Oficial	H. Certificaciones	I. Versiones Vigentes
1. MITRE ATT&CK	Base de conocimiento global sobre tácticas y técnicas de adversarios basadas en observaciones del mundo real.	No tiene fases lineales. Se organiza en Matrices (Enterprise, Mobile, ICS) que contienen Tácticas (el "qué") y Técnicas (el "cómo").	Entender y categorizar el comportamiento del adversario para mejorar la detección y defensa.	Threat Hunting, Red Teaming, Ingeniería de Detección, Emulación de adversarios.	Ofensiva / Defensiva (Purple Teaming)	MITRE Corporation	attack.mitre.org	MITRE ATT&CK Defender (MAD)	v16 (Actualizada frecuentemente)
2. OWASP WSTG	Guía principal para pruebas de seguridad en aplicaciones web, ofreciendo un marco integral para evaluar la seguridad	Marco de pruebas: Recopilación de info, Gestión de config, Identidad, Autenticación, Autorización, Sesión, Validación de datos, Criptografía, etc.	Asegurar que las aplicaciones web sean seguras mediante pruebas exhaustivas y estandarizadas.	Auditoría de aplicaciones Web, Desarrollo Seguro (SDLC), Bug Bounty.	Evaluación / Defensiva	OWASP (Open Worldwide Application Security Project)	owasp.org/www-project-web-security-testing-guide/	No específica de WSTG, pero base para certs web (ej. OSWE).	v4.2 (Estable) / v5.0 (En desarrollo)

	del software.								
3. NIST SP 800-115	Guía técnica para realizar evaluaciones de seguridad de la información, enfocada en agencias federales de EE. UU. pero estándar global.	1. Planificación 2. Descubrimiento 3. Ataque/Explotación 4. Reporte	Proporcionar pautas para planificar y conducir evaluaciones técnicas de seguridad.	Auditorías de cumplimiento (FISMA/FedRAMP), Evaluaciones corporativas formales.	Evaluación	NIST (National Institute of Standards and Technology)	csrc.nist.gov	No tiene certificación propia directa.	Rev 1 (Vigente desde 2008, complementada por nuevos SP).
4. OSSTMM	Metodología científica para pruebas de seguridad que cuantifica la seguridad basándose en hechos y	Se divide en canales: Humano, Físico, Inalámbrico, Telecomunicaciones y Redes de Datos.	Proporcionar una medición científica y métrica de la seguridad operativa (RAVs - Risk Assessment Values).	Auditorías integrales, cumplimiento normativo, pruebas donde se requiere métrica exacta.	Evaluación (Auditoría)	ISECOM (Institute for Security and Open Methodologies)	isecom.org	OPST, OPSA, OPSE	v3.0 (Oficial) / v4.0 (Borrador/Draft)

	métricas verificables.								
5. PTES	Estándar creado por la comunidad para definir qué es y cómo se debe ejecutar una prueba de penetración profesional.	1. Pre-acuerdo 2. Inteligencia 3. Modelado de amenazas 4. Análisis de vulnerabilidad. 5. Explotación 6. Post-explotación 7. Reporte	Estandarizar el proceso y la calidad de las pruebas de penetración (el "Pentest" puro).	Pentesting de red, Pentesting externo/interno, contratos comerciales de hacking ético.	Ofensiva (Ataque simulado)	Equipo PTES (Grupo de consultores expertos)	pentest-standard.org	eCPPT / PTP (Históricamente alineada, ahora INE Security).	v1.0 (Lanzamiento original, sigue siendo el estándar de facto).
6. ISSAF	Marco de trabajo muy detallado que vincula fases de evaluación con herramie	Fase I: Planificación y Prep. Fase II: Evaluación (muy granular por capas).	Ofrecer una guía detallada paso a paso para la evaluación	Entornos legacy, formación académica histórica, auditorías muy procedimentales.	**Evaluación**	OISSG (Open Information Systems Security Group)	Sitio oficial extinto (disponible en archivos/repositorios).	Existía una certificación, actualmente descontinuada.	v0.2.1 (Proyecto inactivo/Descontinuado).

	ntas específicas y controles.	Fase III: Reporte y Limpieza.	de sistemas.						

Análisis Comparativo

Al contrastar estas metodologías, se observa una clara segmentación entre marcos de **evaluación técnica** y marcos de **emulación de adversarios**. Mientras que **PTES** y **NIST SP 800-115** proporcionan una estructura procedimental para la ejecución de pruebas de penetración generales, **OWASP WSTG** se especializa exclusivamente en la capa de aplicación web, ofreciendo un nivel de granularidad que las metodologías generales no alcanzan. Por otro lado, **MITRE ATT&CK** rompe el esquema lineal de fases para enfocarse en una matriz de comportamientos, permitiendo una transición hacia el *Purple Teaming* donde la ofensiva sirve directamente para fortalecer las reglas de detección defensiva.

Un punto crítico revelado en el análisis es la vigencia y el rigor científico. Metodologías como **OSSTMM** destacan por su enfoque en la medición métrica del riesgo, diferenciándose de propuestas más descriptivas. Sin embargo, se evidencia una brecha generacional: mientras **MITRE** y **OWASP** mantienen actualizaciones constantes para hacer frente a amenazas emergentes, marcos como **ISSAF** han quedado relegados a un valor histórico, demostrando que en la ciberseguridad, la utilidad de una metodología está directamente ligada a su capacidad de evolución frente al panorama de amenazas actual.

Conclusión

La selección de una metodología de seguridad no debe ser arbitraria, sino que debe responder a los objetivos de negocio y la infraestructura técnica del cliente. Se concluye que una evaluación integral moderna a menudo requiere la **combinación de varios marcos**: utilizar **PTES** para la gestión del proyecto, **OWASP** para las pruebas de software y **MITRE ATT&CK** para validar la capacidad de respuesta ante incidentes. La estandarización de estos procesos no solo profesionaliza la labor del *pentester*, sino que asegura que los resultados sean medibles, comparables y, sobre todo, útiles para la mitigación real de riesgos en la organización.

Referencias Bibliográficas (APA)

- **ISECOM.** (2010). *OSSTMM 3 - The Open Source Cybersecurity Methodology Manual*. Recuperado de https://www.isecom.org/OSSTMM.3.pdf
- **MITRE Corporation.** (2024). *MITRE ATT&CK® Enterprise Matrix*. Recuperado de https://attack.mitre.org/
- **NIST.** (2008). *Technical Guide to Information Security Testing and Assessment (SP 800-115)*. National Institute of Standards and Technology. Recuperado de https://csrc.nist.gov/pubs/sp/800/115/final
- **OWASP Foundation.** (2024). *OWASP Web Security Testing Guide (WSTG) v4.2*. Recuperado de https://owasp.org/www-project-web-security-testing-guide/
- **PTES Team.** (2014). *The Penetration Testing Execution Standard*. Recuperado de http://www.pentest-standard.org/index.php/Main_Page