ACTIVIDAD 05

Cartografiando el pentesting: análisis comparativo de metodologías de seguridad informática

Zarate Domínguez David – 175842

16 DE FEBRERO DE 2026

UPSLP
CNO V Seguridad Informática

Introducción

El Pentesting o pruebas de penetración no es un proceso arbitrario; requiere de marcos de trabajo (frameworks) que estandaricen las fases de ejecución y aseguren la calidad de los resultados. En esta actividad se realiza un análisis comparativo entre las metodologías más influyentes de la industria, como MITRE ATT&CK, OWASP y NIST, con el objetivo de comprender sus enfoques particulares, desde la seguridad en aplicaciones web hasta la medición científica de la seguridad operativa.

Aspecto	MITRE ATT&CK	OWASP WSTG	NIST SP 800-115	OSSTMM	TES	ISSAF
Descripción	Base de conocimiento global de tácticas y técnicas de adversarios basada en ataques reales.	Guía líder para pruebas de seguridad en aplicaciones web y servicios relacionados.	Guía técnica para realizar pruebas y evaluaciones de seguridad en sistemas federales y privados.	Estándar científico para la medición de la seguridad operativa mediante canales de comunicación.	Estándar centrado en la calidad técnica y la gestión de negocios de un Pentest.	Marco exhaustivo que vincula la evaluación técnica con la gobernanza y procesos de negocio.
Fases	14 Tácticas (Reconocimiento, Acceso Inicial, Persistencia, Exfiltración, etc.).	11 categorías de prueba: Recopilación, Gestión de ID, Autenticación, Sesión, Validación de datos, etc. con +90 casos de prueba	1. Planificación 2. Ejecución 3. Post-ejecución (Análisis de hallazgos).	Canales 1. Canal Humano 2. Canal Físico 3. Canal Inalámbrico 4. Telecomunicaciones 5. Redes de Datos.	1. Pre-acuerdo 2. Inteligencia 3. Modelado 4. Vulnerabilidad 5. Explotación 6. Post-explotación 7. Reporte.	1. Planificación 2. Evaluación (Red, Host, App) 3. Reporte 4. Limpieza.
Objetivo	Detección de técnicas de ataque y simulación de adversarios (Red/Blue Team).	Asegurar el ciclo de vida de aplicaciones web y detectar vulnerabilidades críticas.	Evaluación de controles de seguridad y cumplimiento normativo.	Medir la seguridad operativa y el cumplimiento mediante métricas (RAV).	Estandarizar la ejecución técnica y los resultados comerciales de un Pentest.	Evaluación integral de infraestructura, políticas y seguridad de la información.

Escenarios	Operaciones de *Threat Hunting*, SOC y diseño de defensas activas.	Auditoría de aplicaciones web, portales corporativos y APIs.	Auditorías en agencias gubernamentales y sectores altamente regulados.	Pruebas de seguridad física y lógica donde se requiere medición científica.	Pentests profesionales externos o internos de gran escala.	Auditorías integrales de TI y gestión de riesgos corporativos.
Orientación	**Ataque y Defensa (Híbrido).**	**Evaluación y Ataque.**	**Evaluación Técnica.**	**Evaluación y Verificación.**	**Ataque y Negocio.**	**Evaluación y Gestión.**
Responsable	MITRE Corporation.	OWASP Foundation.	NIST (Gobierno EE. UU.).	ISECOM.	Comunidad liderada por expertos (PTES Board).	OISSG (Open Information Systems Security Group).
URL Oficial	attack.mitre.org	owasp.org/wstg	csrc.nist.gov	isecom.org	pentest-standard.org	https://sourceforge.net/ (si no funciona copiar el link directamente en el navegador)
Certificados	MAD (MITRE ATT&CK Defender).	No tiene una directa (influye en OSWE, CEH).	Alineado con CISA y CISSP.	OPST, OPSA, OPSE.	No tiene propia (base de la mayoría de certificaciones).	No vigente.
Versión	v16.x (Actualización continua).	v5.0 (Estable en 2026).	Referencia técnica base (revisada vía CSF 2.0).	v3.0 (v4.0 en desarrollo prolongado).	v1.1.(Estandar)	v0.2.1 (Considerado histórico).

Conclusión

El análisis comparativo permite concluir que no existe una metodología "superior" de forma absoluta, sino que su eficacia depende del contexto del proyecto. Mientras que OWASP WSTG es el estándar indiscutible para entornos web, PTES ofrece una estructura de negocio mucho más robusta para consultorías comerciales. Para nosotros como estudiantes de Tecnologías de la Información, el dominio de estos marcos proporciona una ventaja competitiva: permite transformar una simple búsqueda de fallos en un proceso de auditoría formal. La tendencia actual apunta hacia la adopción de MITRE ATT&CK para complementar el pentesting tradicional, permitiendo que las organizaciones no solo sepan qué tan vulnerables son, sino cómo se comportaría un adversario real dentro de su infraestructura.

Bibliografía

- MITRE Corporation. (2024). *MITRE ATT&CK v16*. https://attack.mitre.org/
- OWASP Foundation. (2024). *Web Security Testing Guide (WSTG)* (v. 4.2/5.0). https://owasp.org/www-project-web-security-testing-guide/
- National Institute of Standards and Technology. (2008). *Technical Guide to Information Security Testing and Assessment* (NIST Special Publication 800-115). U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-115/final
- Herzog, P. (2010). *Open Source Security Testing Methodology Manual (OSSTMM)* (v. 3). Institute for Security and Open Methodologies (ISECOM). https://www.isecom.org/research.html
- PTES Board. (s. f.). *The Penetration Testing Execution Standard*. http://www.pentest-standard.org/index.php/Main_Page
- Open Information Systems Security Group (OISSG). (2005). *Information Systems Security Assessment Framework (ISSAF)*. SourceForge. https://sourceforge.net/projects/issaf/