UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Actividad 05

Cartografiando el pentesting: análisis comparativo de metodologías de seguridad informática

Alan Gilberto Sánchez Zavala

177263

Universidad Politécnica de
San Luis Potosi

Ciberseguridad

Contents

Introducción

Las pruebas de penetración requieren un enfoque estructurado y metodológico para ser efectivas. En este análisis se presenta una comparación de las principales metodologías y frameworks utilizados en la industria de la ciberseguridad, evaluando sus características distintivas, aplicaciones prácticas y nivel de adopción en entornos profesionales.

Tabla comparativa de metodologías de pruebas de penetración y evaluación de la seguridad informática.

Metodología	Descripción	Fases	Objetivo	Escenarios	Orientación	Autores	URL oficial	Certificados	Versiones /Actualizaciones vigentes
MTRE ATT&CK	Base de conocimientos de tácticas y técnicas de adversarios basada en observaciones del mundo real.	Tácticas, Técnicas y Procedimientos (TTPs).	Detección y descripción de comportamientos de ataque.	Red Teaming, Threat Hunting, SOC y emulación de adversarios.	**Defensa / Ataque** (Híbrida)	MITRE Corporation	https://attack.mitre.org/	MITRE ATT&CK Defender (MAD)	v16 (2024-2025)
OWASP WSTG	Guía exhaustiva para probar la seguridad de aplicaciones web y servicios web.	1. Recolección de información, 2. Configuración., 3. Identidad, 4.Autenticación, 5. Autorización, etc.	Evaluación técnica de vulnerabilidades en aplicaciones web.	Auditorías de aplicaciones web, APIs y servicios en la nube.	Evaluación (Técnica)	OWASP Foundation	https://owasp.org/www-project-web-security-testing-guide/	Referenciada en OSCP, EWPT, CASE.	v4.2 (v5 en desarrollo)
NIST SP 800-115	Guía técnica para realizar pruebas y evaluaciones de seguridad en	1. Planificación, 2.Descubrimiento, 3. Ejecución, 4. Post-ejecución.	Proporcionar una guía metodológica para pruebas técnicas de seguridad.	Entornos gubernamentales y corporativos que	Evaluación / Proceso	NIST (Gobierno EE.UU.)	https://csrc.nist.gov/publications/detail/sp/800-115/final	Ninguna directa (base para	Final (2008) - Sigue siendo

	sistemas federales.			requieren cumplimiento normativo.				CISA/CISSP).	estándar base.
OSSTMM	Metodología científica para la auditoría de seguridad y la medición de la operatividad.	1. Inducción, 2. Interacción, 3. Interrogación, 4. Evaluación.	Medición de la seguridad operativa (análisis de canales).	Auditorías integrales de infraestructura, redes y seguridad física.	Evaluación (Métrica)	Pete Herzog / ISECOM	https://www.google.com/search?q=https://www.isecom.org/OSSTMM.html	OPST, OPSA, OPSE.	v3.0 (v4 en draft)
PTES	Estándar que define los pasos mínimos necesarios para una prueba de penetración de calidad.	1. Pre engagement, 2. Intel, 3. Modelado, 4. Análisis, 5. Explotación, 6. Post-Exp, 7. Reporte.	Estandarizar el lenguaje y las expectativas de un Pentest profesional.	Pruebas de penetración comerciales y de alta complejidad técnica.	Ataque / Ejecución	Comunidad de expertos (Liderado por Dave Kennedy et al.)	http://www.pentest-standard.org/	Muy valorada en el sector (referencia para OSCP/LPT).	v1.1
ISSAF	Marco detallado que vincula la evaluación técnica con la gobernanza y los procesos.	1. Planificación, 2. Evaluación, 3. Informes, 4. Limpieza, 5. Destrucción.	Evaluación técnica profunda alineada con el cumplimiento y políticas.	Organizaciones grandes que buscan auditorías técnicas muy granulares.	Evaluación / Auditoría	OISSG (Open Information Systems Security Group)	N/A	Ninguna activa de forma masiva hoy día.	v0.2.1

Conclusión

Cada metodología presenta un enfoque único que responde a necesidades específicas del contexto operativo. MITRE ATT&CK destaca por su orientación hacia la comprensión del comportamiento adversario, siendo fundamental para equipos defensivos (Blue Team) y Red Team. OWASP WSTG se ha consolidado como el estándar de facto para auditorías de aplicaciones web, mientras que PTES ofrece una estructura completa para pruebas de penetración comerciales.

NIST SP 800-115, a pesar de su antigüedad (2008), continúa siendo relevante en entornos gubernamentales y corporativos que requieren cumplimiento normativo estricto. OSSTMM aporta un enfoque científico orientado a métricas cuantificables, útil para organizaciones que necesitan justificar inversiones en seguridad con datos objetivos.

Bibliografía

- MITRE Corporation. (2024). MITRE ATT&CK Framework. https://attack.mitre.org/
- OWASP Foundation. (2024). Web Security Testing Guide v4.2. https://owasp.org/www-project-web-security-testing-guide/
- NIST. (2008). SP 800-115: Technical Guide to Information Security Testing and Assessment. https://csrc.nist.gov/publications/detail/sp/800-115/final
- Herzog, P. / ISECOM. (2024). Open-Source Security Testing Methodology Manual (OSSTMM). https://www.isecom.org/OSSTMM.html
- Kennedy, D. et al. (2024). Penetration Testing Execution Standard (PTES). http://www.pentest-standard.org/
- OISSG. (2006). Information Systems Security Assessment Framework (ISSAF) v0.2.1.