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

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.	1. Reconnaissance 2. Resource Development 3. Initial Access 4. Execution 5. Persistence 6. Privilege Escalation 7. Defense Evasion 8. Credential Access 9. Discovery 10. Lateral Movement 11. Collection 12. Command and Control 13. Exfiltration 14. Impact	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. Information Gathering 2. Config. & Deployment Management Testing 3. Identity Management Testing	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)

		4. Authentication Testing 5. Authorization Testing 6. Session Management Testing 7. Input Validation Testing 8. Error Handling 9. Cryptography 10. Business Logic Testing 11. Client-side Testing 12. API Testing							
NIST SP 800-115	Guía técnica para realizar pruebas y evaluaciones de seguridad en sistemas federales.	1. Planning 2. Discovery 3. Attack 4. Reporting	Proporcionar una guía metodológica para pruebas técnicas de seguridad.	Entornos gubernamentales y corporativos que requieren cumplimiento normativo.	Evaluación / Proceso	NIST (Gobierno EE.UU.)	https://csrc.nist.gov/publications/detail/sp/800-115/final	Ninguna directa (base para CISA/CISSP).	Final (2008) - Sigue siendo estándar base.
OSSTMM	Metodología científica	1. Induction Phase	Medición de la seguridad	Auditorías integrales de infraestructu	Evaluación (Métrica)	Pete Herzog / ISECOM	https://www.google.com/search?q=https://w	OPST, OPSA, OPSE.	v3.0 (v4 en draft)

	para la auditoría de seguridad y la medición de la operatividad.	2. Interaction Phase 3. Investigation Phase 4. Intervention Phase	operativa (análisis de canales).	ra, redes y seguridad física.			ww.isecom.org/OSSTMM.html		
PTES	Estándar que define los pasos mínimos necesarios para una prueba de penetración de calidad.	1. Pre-engagement Interactions 2. Intelligence Gathering 3. Threat Modeling 4. Vulnerability Analysis 5. Exploitation 6. Post Exploitation 7. Reporting	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	1. Planning and Preparation 2. Assessment (Steps: Info Gathering, Network Mapping,	Evaluación técnica profunda alineada con el cumplimi	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

	con la gobernanza y los procesos.	Vuln ID, Penetration, Gaining Access, Priv Esc,	ento y políticas.						