UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

ACTIVIDAD 05 – Cartografiando el pentesting: análisis comparativo de metodologías de seguridad informática

MATERIA: CNO Seguridad informática
MAESTRO: Servando Lóez Contreras
ALUMNA: Karina Mendoza Aguado
MATRÍCULA: 179859
FECHA: 16/02/26

INTRODUCCIÓN

Las pruebas de penetración son fundamentales para identificar vulnerabilidades y mejorar la protección de los sistemas de información. Para realizarlas de manera ordenada, existen metodologías y marcos de referencia que orientan las actividades, definen fases de trabajo y ayudan a obtener resultados confiables.

En esta actividad se comparan seis propuestas reconocidas en el ámbito profesional: MITRE ATT&CK, OWASP WSTG, NIST SP 800-115, OSSTMM, PTES e ISSAF, con el fin de entender sus diferencias, alcances y los contextos en los que pueden aplicarse.

TABLA

Metodología	Descripción breve	Fases de implementación	Objetivo principal	Escenarios de uso	Orientación	Organización responsable	URL oficial	Certificaciones	Versiones / vigencia
MITRE ATT&CK	Base de conocimiento de tácticas y técnicas usadas por adversarios	Preparación → Mapeo de técnicas → Detección → Mitigación → Mejora	Entender, simular y defenderse de comportamientos de	SOC, threat hunting, evaluación de defensas.	Defensa / evaluación	MITRE	https://attack.mitre.org	No propias, pero usadas en varias (ej. defensivas).	Actualizaciones continuas.
OWASP WSTG	Guía para pruebas de seguridad en aplicaciones web.	Información → Configuración → Autenticación →	Detectar vulnerabilidades en apps web.	Pentesting web, auditorías de desarrollo.	Ataque / evaluación	OWASP	https://owasp.org/www-project-web-security-testing-guide/	Relacionadas con OWASP (ej. OSCP no, pero sí certs OWASP).	WSTG v4.x vigente.
NIST SP 800-115	Guía técnica para pruebas y evaluación de seguridad en organizacione	Planeación → Descubrimiento → Ataque → Reporte	Evaluar controles de seguridad de manera formal.	Gobierno, empresas reguladas.	Evaluación	NIST	https://csrc.nist.gov	Asociado a marcos NIST.	Publicación vigente, revisiones periódicas.
OSSTMM	Metodología científica para pruebas operativas de seguridad.	Inducción → Investigación → Interacción → Análisis	Medir seguridad de forma cuantificable.	Redes, físico, humano, wireless.	Evaluación	ISECOM	https://www.isecom.org	Algunas basadas en ISECOM.	Última versión 3.
PTES	Estándar que define proceso completo de un pentest.	Pre-engagement → Inteligencia → Modelado de amenazas →	Estandarizar pruebas de penetración.	Servicios profesionales de pentesting.	Ataque / evaluación	Comunidad PTES	http://www.pentest-standard.org	Referencia para varias.	Mantención comunitaria.
ISSAF	Marco detallado para evaluar seguridad técnica.	Planeación → Evaluación → Explotación → Reporte	Auditoría profunda de infraestructura.	Consultorías, auditorías empresariales.	Ataque / evaluación	OISSG	http://www.oissg.org	Base para formación profesional.	Versiones estables, pocas actualizaciones.

CONCLUSIÓN

La comparación demuestra que cada metodología posee fortalezas particulares y está diseñada para distintos contextos de aplicación. Mientras algunas priorizan la simulación de ataques, otras se centran en la evaluación de controles o en el análisis del comportamiento de los adversarios.
Por ello, más que elegir una como superior, resulta fundamental seleccionar la que mejor se adapte a los objetivos de la organización, permitiendo evaluaciones más precisas, estandarizadas y alineadas con las necesidades reales de seguridad.

BIBLIOGRAFÍA

- MITRE ATT&CK. (s. f.). ATT&CK knowledge base. https://attack.mitre.org/
- OWASP WSTG. (s. f.). Web security testing guide. https://owasp.org/www-project-web-security-testing-guide/
- National Institute of Standards and Technology. (2008). Technical guide to information security testing and assessment (SP 800-115). https://csrc.nist.gov/