UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Actividad 05

Beltrán Reyna David – 183636

Universidad Politécnica de San Luis Potosí | Ingeniería en Tecnologías de la Información

Curso del Núcleo Optativo V: Seguridad Informática

Mtro. Servando López Contreras

6to. Semestre

Grupo: T46A

a 15 de febrero de 2026

Contenido

Actividad 05: Cartografiando el pentesting

Introducción

En la ciberseguridad profesional, la efectividad del *pentesting* reside en el rigor metodológico y no solo en la habilidad técnica aislada. Ante infraestructuras cada vez más complejas, es fundamental seleccionar el marco de trabajo adecuado para garantizar resultados precisos y útiles para el negocio.

Este análisis evalúa los enfoques y alcances de **MITRE ATT&CK, OWASP, NIST, OSSTMM, PTES e ISSAF**, proporcionando el criterio necesario para optimizar la planificación de auditorías de seguridad en contextos reales.

Tabla comparativa

Metodología	Descripción	Fases de implementación	Objetivo principal	Escenarios de uso	Orientación	Autores / Org. & URL Oficial	Certificaciones	Versión / Vigencia
MITRE ATT&CK	Base de conocimientos global de tácticas y técnicas de adversarios basada en observaciones reales.	14 ***Tácticas*** (Reconocimiento, Acceso Inicial, Ejecución, Persistencia, etc.).	Identificar brechas defensivas y emular comportamientos de atacantes.	Red Teaming, Cloud, Mobile, ICS, Caza de amenazas (Threat Hunting).	Ataque y Defensa: Emulación de adversarios y validación de detecciones.	MITRE Corporation. attack.mitre.org.	MAD (MITRE ATT&CK Defender).	v18.1 (Oct 2025) / Actualizada 2026.
OWASP WSTG	Guía exhaustiva para probar la seguridad de aplicaciones y servicios web durante todo el ciclo de vida.	Preparación, Definición/Diseño, Desarrollo, Despliegue, Mantenimiento y Operación.	Evaluación sistemática de vulnerabilidades en aplicaciones web y APIs.	Auditoría de aplicaciones web, servicios en la nube y aplicaciones móviles.	Evaluación: Pruebas técnicas enfocadas en el software y su infraestructura.	OWASP Foundation. owasp.org.	Conocimiento base para OSCP, OSWA, eWPTX.	v4.2 Estable / v5.0 en desarrollo (2026).
NIST SP 800-115	Guía técnica que establece las bases para realizar pruebas y evaluaciones de seguridad informática.	Planeación, Ejecución, Post-ejecución (Análisis y Reporte).	Asistir en la planificación y ejecución de pruebas técnicas de seguridad y mitigación de riesgos.	Organizaciones gubernamentales y grandes empresas que requieren cumplimiento normativo.	Evaluación: Enfoque metodológico en el control de riesgos y auditoría técnica.	NIST (EE. UU.). csrc.nist.gov.	NCSP 800-115 Foundation.	Estándar estable (2008) integrado a NIST CSF 2.0.
OSSTMM	Manual científico para auditorías técnicas que mide la seguridad operativa real mediante métricas.	Fase de Lanzamiento, Fase Inductiva, Ejecución (Pruebas), Documentación y Revisión.	Medir la seguridad operativa a través de la visibilidad, acceso y confianza.	Auditorías de red, seguridad física, inalámbrica y telecomunicaciones.	Evaluación: Cuantificación de la superficie de ataque y controles operativos.	ISECOM (Pete Herzog). isecom.org.	OPST, OPSA, OPSE.	v3.0 (Estable) / v4.0 en desarrollo (2026).
PTES	Estándar diseñado para	Pre-acuerdo, Recolección de	Proporcionar una estructura	Redes corporativas,	Ataque: Ejecución de	Comunidad de expertos	No tiene una propia, pero es el	Versión estable

	definir una base común de calidad en la ejecución de pruebas de penetración.	información, Modelado de amenazas, Análisis de vulnerabilidades, Explotación, Post-explotación, Reporte.	de alta calidad y lenguaje común para el Pentest profesional.	infraestructuras críticas y pruebas de penetración de caja negra/blanca.	pruebas ofensivas de extremo a extremo.	(Liderada por Nick Percoco). pentest-standard.org	estándar de facto en la industria.	ampliamente adoptada.
ISSAF	Marco de trabajo detallado que vincula la evaluación técnica con los objetivos de negocio de la empresa.	Planeación y Preparación, Evaluación (Assessment), Reporte y Limpieza.	Evaluar controles de seguridad en múltiples capas (Host, Aplicación, Red).	Evaluaciones profundas de sistemas operativos, bases de datos y aplicaciones empresariales.	Evaluación y Auditoría: Enfoque en controles técnicos y gobernanza.	OISSG (Open Information Systems Security Group). Archivado / Scribd.	No asociada.	v0.2.1 (Draft Histórico).

Conclusiones

La comparativa revela que la resiliencia organizacional depende de la integración táctica de estándares: mientras **PTES** y **OWASP** estructuran la ejecución ofensiva, **MITRE ATT&CK** permite emular comportamientos reales y **OSSTMM** aporta métricas científicas para medir la seguridad operativa.

En conclusión, transitar de un enfoque empírico a uno metodológico es vital para profesionalizar la práctica del *pentesting*. La correcta selección de estos marcos transforma la evaluación técnica en una capacidad estratégica que protege los activos críticos con rigor, ética y precisión.

Referencias

ISECOM. (2010). The Open Source Security Testing Methodology Manual (Version 3). https://www.isecom.org/

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/pubs/sp/800/115/final

Open Information Systems Security Group. (2006). Information Systems Security Assessment Framework (ISSAF). https://www.scribd.com/document/88158831/issaf0-2-1A

OWASP Foundation. (2025). Web Security Testing Guide (WSTG). https://owasp.org/www-project-web-security-testing-guide/

Penetration Testing Execution Standard. (s.f.). The Penetration Testing Execution Standard. http://www.pentest-standard.org/

The MITRE Corporation. (2025). MITRE ATT&CK. https://attack.mitre.org/