UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

UNIVERSIDAD POLITÉCNICA DE SAN LUIS

POTOSÍ

CARRERA: Ingeniería en Tecnologías de la Información

MATERIA: CNO V: Seguridad Informática

TRABAJO: Actividad 05 Cartografiando el

pentesting

Grupo: T46A

PARCIAL 1

Donaldo Demián Gómez Arreguín 179822

Profesor: Servando Lopez

Contreras

Fecha de entrega: 16/02/202

Introducción

En el ámbito de la seguridad informática, la evaluación de sistemas y la identificación de vulnerabilidades requieren metodologías estructuradas que permitan analizar riesgos de manera sistemática y reproducible. A lo largo del tiempo, distintas organizaciones y comunidades de ciberseguridad han desarrollado marcos de referencia y estándares para guiar las pruebas de penetración, la evaluación de controles y el análisis de amenazas desde diferentes enfoques, ya sea ofensivo, defensivo o de evaluación integral.

La presente actividad tiene como objetivo analizar comparativamente seis de las metodologías y frameworks más relevantes en el campo del pentesting y la evaluación de seguridad: MITRE ATT&CK, OWASP WSTG, NIST SP 800-115, OSSTMM, PTES e ISSAF. Cada uno de estos enfoques aporta una perspectiva particular sobre cómo comprender, ejecutar o medir la seguridad en sistemas de información, permitiendo seleccionar la metodología más adecuada según el contexto, el tipo de sistema y el objetivo de la evaluación.

Este análisis comparativo facilita la comprensión de sus características, fases, aplicaciones y orientación metodológica, fortaleciendo el criterio técnico para su uso en escenarios reales de seguridad informática.

Tabla comparativa:

La tabla siguiente presenta un análisis sintético de las principales metodologías y marcos de referencia utilizados en pruebas de penetración y evaluación de seguridad informática. Para cada metodología se describen aspectos clave como su propósito, estructura o fases, escenarios de aplicación, orientación (ofensiva, defensiva o de evaluación), organismo responsable, vigencia y disponibilidad de certificaciones asociadas.

La comparación permite identificar similitudes y diferencias entre los enfoques, destacando que algunas metodologías se orientan a la ejecución práctica de pruebas de penetración (por ejemplo, PTES y OWASP WSTG), mientras que otras proporcionan marcos conceptuales o de medición de seguridad (como MITRE ATT&CK y OSSTMM). Asimismo, se observa que ciertos estándares, como NIST SP 800-115, se enfocan en evaluaciones formales dentro de organizaciones, mientras que ISSAF propone un enfoque detallado de assessment técnico.

De esta manera, la tabla facilita la selección informada de la metodología más adecuada según el contexto de aplicación, el alcance de la evaluación y los objetivos de seguridad establecidos.

179822@upslp.edu.mx

Metodología	Descripción	Fases de Implementación	Objetivo principal	Escenarios de uso	Orientación	Autores	URL	Certificación	Vigencia
MITRE ATT&CK	Base de conocimiento de tácticas y técnicas de adversarios.	1. Matriz 2. Tácticas 3. Técnicas	Modelar y detectar ataques reales.	SOC, Red/Purple Team, detección.	Defensa / Evaluación	MITRE	attack.mitre.org	MAD (ATT&CK Defender)	v18.1 (2025)
OWASP WSTG	Guía de pruebas de seguridad en aplicaciones web.	Áreas de testing web	Identificar vulnerabilidades web.	Pentest web, auditorías app.	Ataque / Evaluación	OWASP	owasp.org/WSTG	No directa	v4.2
NIST SP 800-115	Guía formal de pruebas y evaluación de seguridad.	1. Planning 2. Discovery 3. Attack 4. Report.	Estandarizar testing organizacional.	Auditorías, gobierno, empresa.	Evaluación	NIST	csrc.nist.gov/800-115	N/A	2008 (vigente)
OSSTMM	Metodología medible de seguridad operacional.	Canales: físico, humano, red, etc.	Medir seguridad integral.	Auditoría infraestructura/global.	Evaluación	ISECOM	isecom.org	OPSA/OPST	3.02
PTES	Estándar práctico de ejecución de pentest.	7 fases (pre→post→reporte).	Estandarizar pentesting real.	Pentest red/interno/externo.	Ataque	PTES	pentest-standard.org	N/A	Estable
ISSAF	Framework detallado de assessment técnico.	Fases + checklists técnicos.	Evaluación profunda de sistemas.	Auditoría técnica completa.	Evaluación / Ataque	OISSG	issaf.org	Limitada	0.2.1

179822@upslp.edu.mx

Conclusión

El análisis comparativo de las metodologías MITRE ATT&CK, OWASP WSTG, NIST SP 800-115, OSSTMM, PTES e ISSAF permite comprender que no existe un único enfoque universal para la evaluación de la seguridad informática, sino que cada marco responde a necesidades y contextos específicos. Mientras algunas metodologías se orientan a la ejecución práctica de pruebas ofensivas, otras se centran en la medición de la postura de seguridad o en la comprensión de las técnicas empleadas por los adversarios.

Esta diversidad metodológica resulta fundamental en el ámbito profesional, ya que permite seleccionar el enfoque más adecuado según el tipo de sistema, el objetivo de la evaluación y el nivel de profundidad requerido. Por ejemplo, OWASP WSTG y PTES son particularmente útiles en pruebas técnicas de penetración, MITRE ATT&CK contribuye al análisis y detección de amenazas reales, y NIST SP 800-115 u OSSTMM aportan estructuras formales para evaluaciones organizacionales.

En conclusión, el conocimiento y la correcta aplicación de estas metodologías fortalecen la capacidad de análisis, evaluación y gestión de la seguridad en entornos reales, constituyendo herramientas esenciales para el ejercicio profesional en ciberseguridad.

Referencias

- MITRE Corporation. (2025). MITRE ATT&CK® framework. https://attack.mitre.org
- OWASP Foundation. (2023). OWASP Web Security Testing Guide (WSTG). https://owasp.org/www-project-web-security-testing-guide/
- National Institute of Standards and Technology (NIST). (2008). Technical guide to information security testing and assessment (SP 800-115). https://csrc.nist.gov/publications/detail/sp/800-115/final
- ISECOM. (2010). OSSTMM 3: Open Source Security Testing Methodology Manual. https://www.isecom.org
- Penetration Testing Execution Standard (PTES). (2014). PTES technical guidelines. http://www.pentest-standard.org
- Open Information Systems Security Group (OISSG). (2005). Information Systems Security Assessment Framework (ISSAF).