



UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Ingeniería en Tecnologías de la Información

## Actividad 05

### Cartografiando el Pentesting

Análisis comparativo de metodologías de seguridad informática

**Materia:** Fundamentos del Hacking Ético

**Alumno:** Erik De La Rosa Rodriguez

**Docente:** Mtro. Servando López Contreras

**Fecha:** 12 de febrero de 2026

## **Objetivo General**

---

Analizar y comparar de manera estructurada las principales metodologías y marcos de referencia utilizados en pruebas de penetración y evaluación de la seguridad informática. La finalidad es comprender sus enfoques, objetivos, contextos de aplicación y alcances técnicos, fortaleciendo el criterio para seleccionar y aplicar la metodología más adecuada según los distintos escenarios de seguridad.

## **Objetivos Específicos**

---

- **Identificar y describir** las características fundamentales de las metodologías (propósito, fases, orientación).
- **Relacionar** cada metodología con escenarios de aplicación (web, infraestructura, organizacional, etc.).
- **Comparar** criterios como autores/organismos, documentación oficial, certificaciones y vigencia/actualizaciones.

## **Metodologías a Comparar**

---

MITRE ATT&CK, OWASP WSTG, NIST SP 800-115, OSSTMM, PTES, ISSAF.

Tabla 1: Comparativa Parte 1: Enfoque, fases, objetivos y uso

Metodología	Descripción	Fases	Objetivo	Uso	Orientación
MITRE ATT&CK	Base de conocimiento de tácticas y técnicas (TTPs) de adversarios basada en inteligencia real. Modela ataques y evalúa defensas.	1. Recolección 2. Mapeo técnicas 3. Simulación 4. Eval. detección 5. Mejora continua	Comprender y simular comportamiento real del adversario.	SOC, Blue Team, Threat Hunting, Red Teaming.	Defensa / Evaluación
OWASP WSTG	Guía estándar para pruebas de seguridad en aplicaciones web. Valida controles técnicos por categorías.	1. Recolección 2. Configuración 3. Autenticación 4. Autorización 5. Entradas/Lógica	Identificar fallos y validar controles en apps web.	Aplicaciones Web, APIs, Portales expuestos.	Ataque controlado
NIST SP 800-115	Guía formal para planeación y ejecución de evaluaciones técnicas, con énfasis en evidencia y reporte.	1. Planeación 2. Descubrimiento 3. Ataque 4. Reporte	Estandarizar procesos de auditoría técnica.	Auditorías, Cumplimiento, Gobierno, Banca.	Evaluación / Defensora
OSSTMM	Metodología científica centrada en métricas operacionales para minimizar la subjetividad y medir seguridad (RAV).	1. Alcance 2. Recolección 3. Análisis canales 4. Pruebas 5. Medición	Medir la seguridad de forma cuantificable.	Redes, Telecom, Seguridad Física y Humana.	Evaluación Técnica

<b>Metodología</b>	<b>Descripción</b>	<b>Fases</b>	<b>Objetivo</b>	<b>Uso</b>	<b>Orientación</b>
<b>PTES</b>	Estándar práctico "de facto" para la ejecución profesional de pentesting. Define desde el acuerdo hasta el reporte técnico.	1. Pre-engagement 2. Inteligencia 3. Amenazas 4. Vulns/Explotación 5. Reporte	Estandarizar la ejecución técnica del pentest.	Consultoría, Pentesting ofensivo em- presarial.	Ataque controlado
<b>ISSAF</b>	Marco integral que une pruebas técnicas con gestión de riesgos y procesos organizacionales.	1. Planeación 2. Evaluación 3. Pruebas técnicas 4. Análisis/Reporte	Evaluuar seguridad técnica alineada al riesgo.	Auditorías complejas, Evaluaciones	Evaluación / Defensa

Tabla 2: Comparativa Parte 2: Fuentes, certificaciones y vigencia

<b>Metodología</b>	<b>Autor</b>	<b>URL Oficial</b>	<b>Certificaciones</b>	<b>Versiones / Estado</b>
<b>MITRE</b>	MITRE Corp.	<a href="http://attack.mitre.org">attack.mitre.org</a>	Entrenamientos MITRE Engenuity; usado en GIAC.	Actualización continua (Matrix Enterprise/Mobile/ICS).
<b>ATT&amp;CK</b>				
<b>OWASP</b>	OWASP Foundation	<a href="http://owasp.org">owasp.org</a>	Base para OSCP, OSWE, GPEN, CEH.	WSTG v4.2 (Vigente y estable).
<b>WSTG</b>				
<b>NIST SP 800-115</b>	NIST (EE.UU.)	<a href="http://nist.gov">nist.gov</a>	Referencia en CI-SA, CISSP, CISM.	Documento SP 800-115 (Estándar vigente).
<b>OSSTMM</b>	ISECOM	<a href="http://isecom.org">isecom.org</a>	Oficiales: OPST, OPSA, OPSE.	OSSTMM 3.0 (Versión estable).
<b>PTES</b>	Comunidad	<a href="http://pentest-standard.org">pentest-standard.org</a>	Base práctica para la mayoría de certs ofensivas.	Estándar comunitario (Wiki), actualización continua.
<b>ISSAF</b>	OISSG	<a href="http://oissg.org">oissg.org</a>	Indirectamente en auditoría de sistemas.	Framework ISSAF (Proyecto inactivo, usado como referencia).

## Análisis Comparativo (Síntesis Técnica)

---

- **MITRE ATT&CK** no es un tutorial de hacking, sino una base de conocimiento. Es fundamental para equipos de defensa (Blue Teams) para mapear si sus controles detectan técnicas específicas.
- **OWASP WSTG** es perfecto si el objetivo es auditar una página o API, esta es la metodología obligatoria por su profundidad en capas (Lógica, Sesión, Datos).
- **NIST SP 800-115** e **ISSAF** son burocráticos y formales. Son ideales para bancos o gobierno donde el papel y la alineación con normativas son más importantes que el exploit en sí.
- **OSSTMM** intenta convertir la seguridad en ciencia exacta. Si el cliente pide métricas duras (ej. estamos 85 % seguros), OSSTMM provee las fórmulas.
- **PTES** es lo que realmente hacen los pentesters en la calle. Es directo, agresivo y cubre todo el ciclo de vida del ataque real.

## Conclusión

---

No existe una mejor metodología universal; la elección depende estrictamente del objetivo del negocio. Para un pentest técnico puro y duro, **PTES** y **OWASP** son los mas adecuados. Para cumplimiento normativo y auditoría, **NIST**. Para maduración de defensas internas, **MITRE ATT&CK**. Un profesional integral debe conocer las fortalezas de cada una para combinarlas híbridamente según el proyecto.

## Referencias

---

- ISECOM. (2010). *Open Source Security Testing Methodology Manual (OSSTMM 3.0)*. <https://www.isecom.org/OSSTMM.3.pdf>
- MITRE. (2024). *MITRE ATT&CK® framework*. <https://attack.mitre.org>
- National Institute of Standards and Technology. (2008). *Technical Guide to Information Security Testing and Assessment (SP 800-115)*. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>
- OISSG. (2022). *Information Systems Security Assessment Framework (ISSAF)*. <https://www.oissg.org/issaf>
- OWASP Foundation. (2023). *OWASP Web Security Testing Guide (WSTG) v4.2*. <https://owasp.org/www-project-web-security-testing-guide/>
- Penetration Testing Execution Standard. (2023). *PTES Technical Guidelines*. <http://www.pentest-standard.org>