Actividad 05

Cartografiando el pentesting

Mauricio Josafat Salinas Carrillo
Maestro: Servando Lopez Contreras
13 de febrero de 2026

Descripción de la metodología

Metodología	A. Descripción Breve
1. MITRE ATT&CK	Base de conocimiento global estructurada en matrices que mapea las tácticas, técnicas y procedimientos (TTPs) reales de los adversarios. Su propósito principal es cambiar el enfoque defensivo de la simple búsqueda de vulnerabilidades hacia la comprensión profunda del comportamiento del atacante, mejorando así la detección y la emulación de amenazas.
2. OWASP WSTG	Guía técnica exhaustiva y estándar de facto para la evaluación de la seguridad en aplicaciones web. Su enfoque central es el aseguramiento de la calidad (QA), integrando pruebas de seguridad rigurosas en todas las fases del Ciclo de Vida de Desarrollo de Software (SDLC) mediante la estrategia *Shift-Left*, garantizando aplicaciones resilientes desde su diseño.
3. NIST SP 800-115	Marco metodológico oficial del gobierno de EE. UU. diseñado para estandarizar la planificación, ejecución y reporte de pruebas de penetración. Su propósito fundamental es garantizar la consistencia y repetibilidad de las evaluaciones técnicas, sirviendo como pilar fundamental para el cumplimiento riguroso de normativas y la gestión de riesgos institucionales.
4. OSSTMM	Metodología analítica basada en principios científicos que busca eliminar la subjetividad y las suposiciones en las auditorías de seguridad operacional (OpSec). Su enfoque diferencial radica en basarse en "hechos verificados" para cuantificar de manera exacta y medible la superficie de ataque real mediante el cálculo de métricas de riesgo (RAV).
5. PTES	Estándar pragmático desarrollado por la comunidad de seguridad para estructurar el ciclo de vida completo de un pentesting comercial. Su propósito es tender un puente entre la técnica y el negocio, alineando la ejecución avanzada (modelado de amenazas, explotación) con el valor estratégico, asegurando calidad desde el pre-compromiso hasta el reporte.

6. ISSAF	Marco de evaluación estructurado en capas, históricamente reconocido por su extrema granularidad técnica. Aunque actualmente es considerado un marco *Legacy* (obsoleto), **su enfoque original era proporcionar listas de verificación paso a paso**, vinculando cada fase de la auditoría con herramientas específicas para cada tecnología o infraestructura evaluada.

Fases de Implementación

Metodología	B. Fases de Implementación
1. MITRE ATT&CK	**14 Tácticas:** Reconocimiento, Desarrollo de Recursos, Acceso Inicial, Ejecución, Persistencia, Escalada Privilegios, Evasión, Acceso Credenciales, Descubrimiento, Movimiento Lateral, Colección, C2, Exfiltración, Impacto.
2. OWASP WSTG	**Ciclo SDLC:** 1. Antes del Desarrollo, 2. Definición/Diseño, 3. Desarrollo, 4. Despliegue (Pentesting), 5. Mantenimiento.
3. NIST SP 800-115	**Proceso:** 1. Planificación, 2. Descubrimiento, 3. Ataque/ Ejecución, 4. Reporte.
4. OSSTMM	**Fases:** 1. Inducción, 2. Interacción, 3. Investigación, 4. Intervención. (Analiza canales: Humano, Físico, Inalámbrico, Telecom, Redes).
5. PTES	**7 Fases:** 1. Pre-compromiso, 2. Inteligencia, 3. Modelado Amenazas, 4. Vuln Analysis, 5. Explotación, 6. Post-Explotación, 7. Reporte.
6. ISSAF	**Capas:** 1. Planificación, 2. Evaluación (Info Gathering -> Network Mapping -> Vuln ID -> Penetration -> Tracks), 3. Reporte.

Objetivo Principal

Metodología	C. Objetivo Principal
1. MITRE ATT&CK	Clasificar comportamientos para mejorar detección, inteligencia (CTI) y emulación.
2. OWASP WSTG	Aseguramiento de calidad (QA) en software web y detección temprana de fallos.
3. NIST SP 800-115	Estandarizar procedimientos de evaluación técnica y cumplimiento en agencias federales.
4. OSSTMM	Medición científica de la superficie de ataque y verificación de hechos (*Facts*).
5. PTES	Estructurar la ejecución del pentesting para garantizar valor y calidad al cliente.
6. ISSAF	Ofrecer guías paso a paso y checklists detallados para tecnologías específicas.

Escenarios en los que se usa

Metodología	D. Escenarios de Uso
1. MITRE ATT&CK	Threat Intelligence, Purple Teaming, mejora de SIEM/ EDR.
2. OWASP WSTG	Auditoría web/APIs, DevSecOps, Code Reviews.
3. NIST SP 800-115	Cumplimiento (FISMA/FedRAMP), auditorías formales.
4. OSSTMM	Auditorías físicas/lógicas, métricas exactas de riesgo.
5. PTES	Pentesting comercial (Blackbox), Red Teaming.
6. ISSAF	Académico, referencia para metodologías internas.

Orientación de la metodología de pruebas de penetración

Metodología	E. Orientación y Explicación Técnica
1. MITRE ATT&CK	**Orientación Híbrida (Purple Teaming).** No ejecuta ataques *per se*, sino que cataloga las tácticas y técnicas (TTPs) ofensivas para que los equipos defensivos (Blue Teams) puedan modelar amenazas, crear reglas de detección en soluciones SIEM/EDR y evaluar empíricamente su postura de seguridad basándose en inteligencia de amenazas (Defensa informada por el adversario).
2. OWASP WSTG	**Orientación Defensiva y de Evaluación (Aseguramiento de Calidad).** Su enfoque preventivo busca integrar controles de seguridad directamente en el pipeline de desarrollo (CI/CD) mediante la estrategia *Shift-Left*. Promueve la ejecución de revisiones de código estático y dinámico (SAST/DAST) para mitigar vulnerabilidades lógicas y técnicas antes del paso a producción.
3. NIST SP 800-115	**Orientación de Evaluación Técnica y Auditoría.** Se enfoca en la validación estructurada de controles de seguridad para garantizar el cumplimiento normativo. Su metodología es conservadora: prioriza la identificación y el análisis de vulnerabilidades minimizando el riesgo operativo, recomendando la explotación activa solo cuando es estrictamente necesario para validar un riesgo de cumplimiento.
4. OSSTMM	**Orientación de Evaluación Analítica y Métrica.** Utiliza un enfoque empírico para calcular la "superficie de ataque" mediante el Valor de Evaluación de Riesgos (RAV). Se diferencia por medir la "porosidad" de las defensas operacionales (físicas, humanas, de red e inalámbricas) basándose exclusivamente en hechos verificables, reduciendo a cero las suposiciones o falsos positivos.

5. PTES	**Orientación Ofensiva (Red Teaming / Pentesting comercial).** Diseñada para simular amenazas avanzadas de manera controlada. Pone un fuerte énfasis técnico en las fases de explotación y post-explotación (ej. pivoteo de red, exfiltración de datos, escalada de privilegios) para demostrar de forma tangible el impacto real que un atacante tendría sobre los activos críticos del negocio.
6. ISSAF	**Orientación de Evaluación Técnica y Explotación Procedimental.** Proveía un enfoque *bottom-up* altamente estructurado, guiando al auditor técnico mediante listas de verificación granulares. Vinculaba directamente cada vector de ataque con herramientas específicas de software (comandos, scripts) para evaluar de forma procedimental las distintas capas de la infraestructura (red, sistema operativo, base de datos).

Autores u Organismos responsables, URL del material oficial, certificaciones asociadas y versiones vigentes

Metodología	F. Autores	G. URL / H. Certs / I. Versión
1. MITRE ATT&CK	MITRE Corp.	**Web oficial:** attack.mitre.org **Certificación:** MITRE Defender (MAD) **Versión vigente:** v18 (2025)
2. OWASP WSTG	OWASP Fdn.	**Web oficial:** owasp.org **Certificación:** No directa (vinculada a AppSec) **Versión vigente:** v4.2 / v5.0 (Dev)
3. NIST SP 800-115	NIST (EE.UU.)	**Web oficial:** csrc.nist.gov **Certificación:** CISA, CISM, CAP **Versión vigente:** Rev 1 (Vigente)
4. OSSTMM	ISECOM	**Web oficial:** isecom.org **Certificación:** OPST, OPSA, OPSE **Versión vigente:** v3.02
5. PTES	Comunidad PTES	**Web oficial:** pentest-standard.org **Certificación:** CompTIA PenTest+, CEH **Versión vigente:** v1.0

6. ISSAF	OISSG (Disuelto)	**Web oficial:** Inactivo **Certificación:** Inexistentes **Version vigente:** Legacy/ Deprecated

Bibliografia:

MITRE Corporation. (2025). MITRE ATT&CK®: Adversarial Tactics, Techniques, and Common Knowledge. Recuperado de https://attack.mitre.org

OWASP Foundation. (2020/2025). *Web Security Testing Guide (WSTG) v4.2 & v5.0*. Recuperado de 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). Recuperado de https://csrc.nist.gov

Herzog, P. / ISECOM. (2010). The Open Source Security Testing Methodology Manual (OSSTMM) 3.0. Recuperado de https://www.isecom.org/

PTES Team. (2014). *The Penetration Testing Execution Standard*. Recuperado de http://www.pentest-standard.org/

OISSG. (Legacy). *Information Systems Security Assessment Framework (ISSAF)*. Referenciado en literatura académica y repositorios de archivo.