UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Actividad 05

CARTOGRAFIANDO EL PENTESTING

Análisis comparativo de metodologías de seguridad informática

173030 Sánchez Mayeli

Introducción

En la presente actividad se analizan y comparan diversas metodologías y marcos de referencia utilizados en pruebas de penetración y evaluación de la seguridad informática. El propósito es identificar sus fases de implementación, orientación estratégica, escenarios de aplicación y vigencia actual, con el fin de comprender sus diferencias y complementariedades. Este análisis permite determinar cuál metodología resulta más adecuada según el contexto organizacional, el tipo de sistema evaluado y los objetivos específicos de la evaluación de seguridad.

MITRE ATT&CK	
Descripción	Framework de conocimiento que documenta tácticas y técnicas utilizadas por adversarios reales. No es una metodología secuencial de pentesting, sino una matriz de comportamiento adversario basada en inteligencia de amenazas.
Fases de implementación	Organizado en tácticas como Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Exfiltration e Impact.
Objetivo	Mapear técnicas reales para fortalecer capacidades de detección, respuesta y emulación de ataques.
Escenarios	SOC, threat hunting, red team, purple team y validación de controles.
Orientación	Ataque y defensa (híbrido).
Autores u organismos responsables	MITRE Corporation.
URL	https://attack.mitre.org
Existencia de certificaciones asociadas	No certifica directamente; ampliamente usado en formación avanzada de ciberseguridad.
Versiones o actualizaciones vigentes	Actualizaciones periódicas (v18.x en 2025).

OWASP WSTG	
Descripción	Guía comunitaria para pruebas de seguridad en aplicaciones web.
Fases de implementación	Incluye Information Gathering, Authentication, Authorization, Session Management, Input Validation, Cryptography, Business Logic, entre otras áreas.
Objetivo	Identificar vulnerabilidades en aplicaciones web mediante pruebas estructuradas.
Escenarios	Pentesting web y auditorías de aplicaciones.
Orientación	Ofensiva (evaluación controlada).

Autores u organismos responsables	OWASP Foundation.
URL	https://owasp.org/www-project-web-security-testing-guide/
Existencia de certificaciones asociadas	Usada como referencia en certificaciones de seguridad web.
Versiones o actualizaciones vigentes	v4.2 estable; v5.0 en desarrollo.

NIST SP 800-115	
Descripción	Guía técnica para la planificación y ejecución de pruebas y evaluaciones de seguridad.
Fases de implementación	Planning, Discovery, Attack y Reporting.
Objetivo	Estandarizar evaluaciones técnicas formales en organizaciones.
Escenarios	Entornos gubernamentales y corporativos.
Orientación	Defensiva (evaluación y aseguramiento).
Autores u organismos responsables	NIST.
URL	https://csrc.nist.gov/pubs/sp/800/115/final
Existencia de certificaciones asociadas	Marco referenciado en auditorías y gestión de seguridad.
Versiones o actualizaciones vigentes	Publicación final 2008, aún vigente como referencia.

OSSTMM	
Descripción	Metodología científica para medir seguridad operacional con métricas cuantificables.
Fases de implementación	Evaluación por canales de comunicación y métricas como RAV y STAR.
Objetivo	Medir exposición real y efectividad de controles.
Escenarios	Infraestructura crítica y telecomunicaciones.
Orientación	Evaluación técnica estructurada.
Autores u organismos responsables	ISECOM.
URL	https://www.isecom.org/OSSTMM.3.pdf
Existencia de certificaciones asociadas	OPST, OPSA, OPSE.
Versiones o actualizaciones vigentes	OSSTMM 3.

PTES	
Descripción	Estándar comunitario que define el proceso completo de un pentest profesional.
Fases de implementación	Pre-engagement, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation,

	Post-Exploitation, Reporting.
Objetivo	Estandarizar pruebas de penetración end-to-end.
Escenarios	Consultoría y pentest empresarial formal.
Orientación	Ofensiva estructurada.
Autores u organismos responsables	Comunidad PTES.
URL	https://www.pentest-standard.org/
Existencia de certificaciones asociadas	Relacionado con formación práctica en pentesting.
Versiones o actualizaciones vigentes	Estándar comunitario estable.

ISSAF	
Descripción	Framework histórico para auditorías de seguridad con procedimientos detallados.
Fases de implementación	Planeación, evaluación técnica y reporte.
Objetivo	Guiar auditorías integrales.
Escenarios	Consultoría y revisiones técnicas detalladas.
Orientación	Evaluación con prácticas ofensivas.
Autores u organismos responsables	OISSG.
URL	
Existencia de certificaciones asociadas	No vigentes oficiales.
Versiones o actualizaciones vigentes	Marco histórico (draft 0.2).

Análisis comparativo y conclusión

Las metodologías no compiten entre sí, sino que se complementan. PTES estructura el proceso completo de pentesting; OWASP WSTG especializa pruebas en aplicaciones web; NIST SP 800-115 aporta formalidad institucional; OSSTMM introduce medición cuantitativa; MITRE ATT&CK conecta pruebas con técnicas reales observadas en amenazas; e ISSAF funciona como referencia histórica. En contextos latinoamericanos, una estrategia efectiva combina NIST (planeación), PTES (ejecución), OWASP (aplicaciones web) y MITRE (validación de detección y respuesta).

Referencias

MITRE ATT&CK – https://attack.mitre.org
OWASP WSTG – https://owasp.org/www-project-web-security-testing-guide/
NIST SP 800-115 – https://csrc.nist.gov/pubs/sp/800/115/final
OSSTMM – https://www.isecom.org/OSSTMM.3.pdf
PTES – https://www.pentest-standard.org/