CARTOGRAFIANDO EL PENTESTING: ANÁLISIS COMPARATIVO DE METODOLOGÍAS DE SEGURIDAD INFORMÁTICA

ACTIVIDAD 5

BRUNO AXEL PUENTE LUNA 177876
UNIVERSIDAD POLITECNICA DE SAN LUIS POTOSI

Contenidos

Introducción

Dentro de este documento se relata la investigación hecha acerca de las principales metodologías y marcos de referencia utilizados en pruebas de penetración y evaluación de seguridad informática, identificando y describiendo las características de cada una, tales como: propósito, fases de implementación y orientación estratégica; estas metodologías se relacionaran con escenarios donde la aplicación sea la mas adecuada; se compararan en criterio a los autores, documentación oficial, certificaciones y vigencia.

Las metodologías descritas serán las siguientes:

1. MTRE ATT&CK
2. OWASP WSTG
3. NIST SP 800-115
4. OSSTMM
5. PTES
6. ISSAF

Completa cada columna de la tabla de manera clara, precisa y sintetizada, considerando los siguientes aspectos:

A. Descripción breve de la metodología.
B. Fases de implementación.
C. Objetivo principal (ejemplo: detección de técnicas de
D. ataque, pruebas técnicas, evaluación de controles, etc).
E. Escenarios en los que se utiliza.
F. Orientación (ataque, defensa o evaluación).
G. Autores u organismos responsables.
H. URL del material oficial.
I. Existencia de certificaciones asociadas.

J. Versiones o actualizaciones vigentes.

Con toda esta información recolectada, se realizará una tabla de comparación de las 6 metodologías para que sea más comprensible su estudio.

Desarrollo

MITRE ATT&CK

"MITRE ATT&CK es una base de conocimientos accesible a nivel mundial sobre tácticas y técnicas adversarias basada en observaciones del mundo real. La base de conocimientos ATT&CK se utiliza como fundamento para el desarrollo de modelos y metodologías de amenazas específicos en el sector privado, en el gobierno y en la comunidad de productos y servicios de ciberseguridad.

Con la creación de ATT&CK, MITRE cumple su misión de resolver problemas para lograr un mundo más seguro, reuniendo a las comunidades para desarrollar una ciberseguridad más eficaz. ATT&CK es abierta y está disponible para cualquier persona u organización que desee utilizarla sin costo alguno." MITRE ATT&CK. https://attack.mitre.org/

A diferencia de las otras, ATT&CK no es una metodología de pentesting tradicional sino una base de conocimiento de tácticas, técnicas y procedimientos (TTP) usados por adversarios reales. Su enfoque es modelar comportamiento adversario para emular ataques y mejorar la defensa y detección.

OWASP Web Security Testing Guide (WSTG)

"El proyecto Web Security Testing Guide (WSTG) elabora el principal recurso de pruebas de ciberseguridad para desarrolladores de aplicaciones web y profesionales de la seguridad.

El WSTG es una guía completa para evaluar la seguridad de las aplicaciones y los servicios web. Creado gracias al esfuerzo conjunto de profesionales de la ciberseguridad y voluntarios dedicados, el WSTG proporciona un marco de buenas prácticas utilizado por evaluadores de penetración y organizaciones de todo el mundo." OWASP Web Security Testing Guide.
https://owasp.org/www-project-web-security-testing-guide/

WSTG es un estándar de pruebas especializado en aplicaciones web que funciona como checklist exhaustivo de controles y pruebas, más que un proceso cíclico tradición.

NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment)

"El Instituto Nacional de Estándares y Tecnología (NIST) elaboró este documento en cumplimiento de sus responsabilidades legales en virtud de la Ley Federal de Gestión de la Seguridad de la Información (FISMA) de 2002, Ley Pública 107-347. El NIST es responsable de desarrollar normas y directrices, incluidos los requisitos mínimos, para proporcionar una seguridad de la información adecuada para todas las operaciones y activos de la agencia; pero dichas normas y directrices no se aplicarán a los sistemas de seguridad nacional. Esta directriz es coherente con los requisitos de la Circular A-130 de la Oficina de Gestión y Presupuesto (OMB), sección 8b (3), «Protección de los sistemas de información de las agencias», tal y como se analiza en A-130, apéndice IV: Análisis de secciones clave. Se proporciona información complementaria en A-130, apéndice III." Scarfone, K. A., Souppaya, M. P., Cody, A., & Orebaugh, A. D. (2008). Technical guide to information security testing and assessment. National Institute of Standards and Technology.

NIST 800-115 es un estándar formal del gobierno de EE. UU. para pruebas de seguridad.

OSSTMM (Open Source Security Testing Methodology Manual)

"El objetivo principal de este manual es proporcionar una metodología científica para la caracterización precisa de la seguridad operativa (OpSec) mediante el examen y la correlación de los resultados de las pruebas de una manera coherente y confiable. Este manual se adapta a casi cualquier tipo de auditoría, incluyendo pruebas de penetración, hacking ético, evaluaciones de seguridad, evaluaciones de vulnerabilidad, equipos rojos, equipos azules, etc. Está redactado como un documento de investigación de seguridad y está diseñado para la verificación de seguridad objetiva y la presentación de métricas a nivel profesional." https://www.isecom.org/OSSTMM.3.pdf

OSSTMM es un marco amplio para evaluar la seguridad de sistemas y operaciones en varios dominios.

PTES (Penetration Testing Execution Standard)

“La norma de ejecución de pruebas de penetración consta de siete (7) secciones principales. Estas abarcan todo lo relacionado con una prueba de penetración, desde la comunicación inicial y el razonamiento que hay detrás de una prueba de penetración, pasando por las fases de recopilación de información y modelización de amenazas, en las que los evaluadores trabajan entre bastidores para comprender mejor la organización evaluada, hasta la investigación de vulnerabilidades, la explotación y la post explotación, en las que entran en juego los conocimientos técnicos de seguridad de los evaluadores, que se combinan con la comprensión del negocio del proyecto, y, por último, la elaboración de informes, que recogen todo el proceso de una manera que tenga sentido para el cliente y le aporte el máximo valor.”

https://web.archive.org/web/20260210040216/https://www.pentest-standard.org/index.php/Main_Page

PTES define un proceso detallado que abarca todo el ciclo de prueba de penetración.

ISSAF (Information Systems Security Assessment Framework)

“El Marco de Evaluación de la Seguridad de los Sistemas de Información (ISSAF) es un marco estructurado y revisado por pares que clasifica la evaluación de la seguridad de los sistemas de información en varios dominios y detalla criterios específicos de evaluación o prueba para cada uno de estos dominios. Su objetivo es proporcionar aportaciones sobre el terreno en materia de evaluación de la seguridad que reflejen situaciones de la vida real. El ISSAF debe utilizarse principalmente para cumplir los requisitos de evaluación de la seguridad de una organización y, además, puede utilizarse como referencia para satisfacer otras necesidades de seguridad de la información. El ISSAF incluye el aspecto crucial de los procesos de seguridad, su evaluación y refuerzo para obtener una visión completa de las vulnerabilidades que puedan existir.” https://untrustednetwork.net/files/issaf0.2.1.pdf

ISSAF es un marco completo, algo histórico, con guía paso a paso para pruebas de seguridad.

Metodología / Marco	A. Descripción breve	B. Fases de implementación	C. Objetivo principal	D. Escenarios de uso	E. Orientación	F. Autores / Organismos responsables	G. URL material oficial	H. Certificaciones asociadas	I. Versiones / Actualizaciones vigentes

MITRE ATT&CK	Base de conocimiento con tácticas, técnicas y procedimientos (TTPs) usados por adversarios reales, para entender y modelar ataques.	No tiene fases en orden secuencial como una metodología de pentesting tradicional; organiza tácticas por matrices (Enterprise, Mobile, etc.) que describen comportamiento adversario.	Entender técnicas reales de ataque y apoyar simulación, detección y defensa.	Red team avanzado, threat hunting, simulación de adversarios en infraestructuras y detección.	Ataque (red team) y evaluación/defensa (detección y respuesta).	MITRE Corporation (organización sin fines de lucro que mantiene ATT&CK).	https://attack.mitre.org/	No tiene certificación propia, pero se usa como base en certificaciones de Red Team/Threat Intelligence.	https://omegasec.eu/methodologies-in-use

OWASP WSTG	Guía técnica de pruebas de seguridad para aplicaciones web (checklist de pruebas según categorías de vulnerabilidades).	No es un proceso completo de fases como PTES, pero sí tiene secciones organizadas por tipos de pruebas (reconocimiento, autenticación, control de sesiones, lógica, etc.).	Evaluar vulnerabilidades de aplicaciones web con pruebas específicas (csrf, xss, sql injection).	Pentesting de aplicaciones web y APIs modernas.	Evaluación técnica de pruebas web (ataque técnico).	OWASP (Open Web Application Security Project).	https://owasp.org/www-project-web-security-testing-guide/	No aplica certificación propia, pero sirve como estándar para certificaciones como GWAPT/CSSLP.	https://owasp.org/www-project-web-security-testing-guide/v42/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies

NIST SP 800-115	Guía técnica de pruebas y evaluaciones de seguridad de sistemas informáticos, con énfasis en diseño, ejecución y reporte de pruebas.	Planificación → Descubrimiento/identificación (reconocimiento) → Análisis de vulnerabilidades y explotación → Post-Testing y reporte.	Proporcionar guías para planificación y ejecución de pruebas que identifiquen vulnerabilidades, analizar resultados y apoyar mitigación.	Evaluaciones formales de seguridad de TI, cumplimiento regulatorio, infraestructura, sistemas empresariales.	Evaluación estructurada de seguridad (auditoría técnica).	NIST (Instituto Nacional de Estándares y Tecnología, EE. UU.).	https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-115.pdf	Referenciado en certificaciones como CISSP/CISM/CISA (no certificación propia).	https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-115.pdf

OSSTMM	Manual de metodología abierta para pruebas de seguridad operativas (network, físico, humano, telecom, etc.) con enfoque en métricas de seguridad objetivas.	Incluye módulos de análisis operativo y métricas (no fases tradicionales como PTES, pero estructura por áreas de testeo detalladas).	Medir y evaluar seguridad operacional y controles con resultados cuantificados.	Auditorías de seguridad amplias (procesos, humanos, redes, telecomunicaciones, físico).	Evaluación amplia y defensiva (análisis objetivo de seguridad).	ISECOM (Institute for Security and Open Methodologies).	https://www.isecom.org/OSSTMM.3.pdf	Certificaciones ofrecidas por ISECOM (OSSA/OPSA/OWSE/OPSE/Trust Analyst).	https://www.isecom.org/OSSTMM.3.pdf

PTES	Estándar de ejecución de pruebas de penetración que abarca todo el ciclo de un pentest desde contacto hasta reporte.	Pre-engagement → Inteligencia → Modelado de amenazas → Análisis de vulnerabilidades → Explotación → Post-explotación → Reporting.	Proveer un proceso claro y técnico para ejecutar pentests completos.	Pentesting general (infraestructura, red, aplicaciones).	Ataque y evaluación técnica.	Comunidad PTES (PTES.org).	https://www.pentest-standard.org/index.php/Main_Page	Referenciado en certificaciones como OSCP, eCPPT (no certificación oficial propia).	https://web.archive.org/web/20260210040216/https://www.pentest-standard.org/index.php/Main_Page

ISSAF	Marco de evaluación de seguridad de sistemas que combina análisis técnico con control organizacional y herramientas.	Planificación y preparación → Assessment (análisis técnico y de controles) → Reporte y limpieza. *(estructura general y pasos internos según marco)*.	Evaluar y medir controles de seguridad y técnicas en sistemas y redes.	Evaluación de seguridad integral (organización, red, app).	Ataque y evaluación técnica/ organizacional.	Open Information Systems Security Group (OISSG).	Documento disponible en repositorios (ej. https://untrustednetwork.net/files/issaf0.2.1.pdf).	No tiene certificación oficial propia; se usa como referencia conceptual.	https://untrustednetwork.net/files/issaf0.2.1.pdf

Referencias

MITRE ATT&CK®. (s/f). Mitre.org. Recuperado el 14 de febrero de 2026, de https://attack.mitre.org/

OWASP Web Security Testing Guide. (s/f). Owasp.org. Recuperado el 14 de febrero de 2026, de https://owasp.org/www-project-web-security-testing-guide/

Scarfone, K. A., Souppaya, M. P., Cody, A., & Orebaugh, A. D. (2008). *Technical guide to information security testing and assessment*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-115.pdf

(S/f-a). Isecom.org. Recuperado el 14 de febrero de 2026, de https://www.isecom.org/OSSTMM.3.pdf

(S/f-b). Archive.org. Recuperado el 14 de febrero de 2026, de https://web.archive.org/web/20260210040216/https://www.pentest-standard.org/index.php/Main_Page

(S/f-c). Untrustednetwork.net. Recuperado el 14 de febrero de 2026, de https://untrustednetwork.net/files/issaf0.2.1.pdf