UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Nombre:

Felipe Reyes

Profesor:

Mtro. Servando

Tema:

Cartografía del pentesting: análisis de metodologías de S.I

lunes, 16 de febrero de 2026

Introducción

Se analizarán los distintos tipos de metodologías en Seguridad e informática, para poder tener una idea de las posibles brechas de ataques a los sistemas informáticos.
Con lo cuál se busca tener una amplia vista de los pasos a seguir, tanto en los objetivos de los ciberdelincuentes hasta las posibles soluciones como un profesional, hacker ético, etc.
Dicho análisis está basado en pruebas controladas para poder dar una mejor defensa de los datos y evitar una filtración masiva con datos sensibles.

	MITRE ATT&CK	OWASP WSTG	NIST SP 800-115	OSSTMM	PTES	ISSAF
Descripción	Es una base de conocimientos universalmente accesible y actualizada para modelar, detectar, prevenir y combatir las amenazas de ciberseguridad	Es una organización de código abierto dedicada a la seguridad de aplicaciones web.	Proporciona un marco estructurado para realizar pruebas y evaluaciones de seguridad en sistemas de información.	Es un estándar abierto y una metodología integral desarrollada por el ISECOM para realizar auditorías de seguridad técnicas y operativas, pruebas de penetración y evaluaciones de vulnerabilidades	Método integral de pruebas de penetración	Es un marco de pruebas de penetración respaldado por el Information Systems Security Group (OISSG)
Fases De Implementación	Mapeo de Controles Identificación de Brechas Priorización Desarrollo de Detecciones Validación y Emulación	Recopilación de Información Pruebas de Configuración Gestión de Despliegue Pruebas de Gestión de Identidad	Planificación Ejecución Post-ejecución (Análisis) Reporting	Postura Evaluación Pruebas Análisis Informes	Interacciones Previas al Compromiso Recolección de Información Modelado de Amenazas Análisis de Vulnerabilidades	Planificación y Preparación Evaluación (Assessment) Informes y Seguimiento
Objetivo Principal	Las tácticas de ATT&CK corresponden estrechamente a las etapas o fases de un ciberataque	Establecer un marco de referencia universal que permita realizar pruebas de seguridad repetibles, consistentes y de	Servir como marco de referencia para la selección, implementación y técnicas de evaluación de seguridad	Proporcionar una métrica estandarizada y científica de la **seguridad operativa**	Ser la línea de base para pruebas de penetración y proporcionar una metodología estandarizada para los	Proporcionar una metodología estandarizada y repetible para que los

		alta calidad, asegurando que se cubran todos los vectores de ataque posibles en el entorno web moderno			profesionales y organizaciones de seguridad.	profesionales de seguridad
Escenarios	Ciberinteligencia de Amenazas (CTI) Operaciones de Red Team Centros de Operaciones de Seguridad (SOC)	Marco de pruebas OWASP Pruebas de penetración de API Pruebas de penetración de IoT	Auditorías de cumplimiento Pruebas de Penetración (Pen Testing) Gestión de Vulnerabilidades	Seguridad Humana Seguridad Física Seguridad Inalámbrica	Infraestructuras de red corporativas. Aplicaciones web y móviles.	External - Internal Assessment Pruebas de Aplicaciones Web Auditoría de Dispositivos
Orientación	Proactiva, basada en el comportamiento y centrada en el adversario	**Ofensivo:** Para profesionales de Red Team y Pentesters.	Técnicas de revisión Técnicas de prueba	Está dirigido a auditores de seguridad, pentesters, analistas de riesgo y CISO	Proporcionar un marco integral, sistemático y estandarizado para llevar a cabo auditorías técnicas de seguridad (pruebas de penetración)	Técnica y operativa
Responsible (s)	The MITRE Corporation	Fundación OWASP (Open Web Application Security Project)	Administradores de Seguridad/Analistas Directores de IT (CIO/CISO)	ISECOM	**Chris Nickerson** **Dave Kennedy**	Systems Security Group (OISSG)

			Auditores Externos		**HD Moore**	
URL	https://attack.mitre.org/	https://owasp.org/www-project-web-security-testing-guide/	https://www.nist.gov/privacy-framework/nist-sp-800-115	https://www.isecom.org/research.html	http://www.pentest-standard.org/	No Aplica
Existencia De Cetificaciones	Detection of Digital Certificates, Detection Strategy DET08xx	no emite certificaciones propias como entidad	Sin Certificaciones	OPST (OSSTMM Professional Security Tester) OPSA (OSSTMM Professional Security Analyst) OPSE (OSSTMM Professional Security Expert)	Sin Certificaciones	No aplica
Actualizaciones Vigentes	28 de October, 2025 (MITRE actualiza la base dos veces al año)	versión 4.2 (Se está trabajando en la V5)	April 23, 2021	se mantiene actualmente bajo la versión 3.02 (desde diciembre de 2010)	Sin Actualizaciones	No hay actualizaciones

Fuentes consultadas:

MITRE ATT&CK®. (s. f.). https://attack.mitre.org/

Ibm. (2025, November 26). Mitre Attack. IBM. https://www.ibm.com/mx-es/think/topics/mitre-attack?mhsrc=ibmsearch_a&mhq=MITRE%20ATT%26amp%3BCK

Finn, T. (2025, November 27). Metodología de pruebas de penetración. IBM. https://www.ibm.com/mx-es/think/insights/pen-testing-methodology

OWASP Web Security Testing Guide | OWASP Foundation. (s. f.). https://owasp.org/www-project-web-security-testing-guide/

Admin. (2024, 5 octubre). *Guía OSSTMM*. Tu Consultor TI. https://www.tuconsultorti.com/ciberseguridad/guia-osstmm/?srsltid=AfmBOorQCoBr08pSkfMRJeFHJZGe_wAqEumJRSxR-FjTuwB4RzS0iR87

DragoN. (2025, 17 mayo). OSSTMM, Manual de la Metodología Abierta de Testeo de Seguridad - DragonJAR. *DragonJAR - Servicios de Seguridad Informática*. https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml