UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Actividad 5 - Cartografiando el pentesting: análisis comparativo de metodologías de seguridad informática

Pedro Damian Jasso Dávila - 176658

CNO V: Seguridad Informática

13/02/2026

Mtro. Servando López Contreras

Cartografiando el pentesting

Introducción

En este trabajo se va a analizar seis de las metodologías más importantes y utilizadas a nivel global: MITRE ATT&CK, OWASP WSTG, NIST SP 800-115, OSSTMM, PTES e ISSAF. A través de esta tabla comparativa, se busca entender cómo cada una de ellas ayuda a identificar vulnerabilidades, evaluar riesgos y fortalecer las defensas de una organización dependiendo de sus necesidades específicas.

Actividad

MITRE ATT&CK	
Descripción	El marco **MITRE ATT&CK** funciona como una base de conocimientos global y dinámica que cataloga las tácticas y técnicas observadas en ataques reales. Su enfoque principal es la defensa basada en el conocimiento profundo del atacante. Universalmente accesible y actualizada para modelar, detectar, prevenir y combatir las amenazas de ciberseguridad.
Fases de implementación	• **Emulación de adversario:** Diseñar ataques basados en grupos específicos. • **Red Teaming:** Ejecución de ejercicios de ataque avanzado. • **Desarrollo de análisis de comportamiento:** Identificar patrones de ataque en lugar de solo firmas. • **Evaluación de brechas defensivas:** Detectar puntos ciegos en la infraestructura.

	• **Evaluación de madurez de SOC:** Medir la capacidad de respuesta del centro de operaciones. • **Enriquecimiento de inteligencia de amenazas cibernéticas:** Integrar datos externos sobre nuevos vectores de ataque.
Objetivo principal	Proporcionar información sobre tácticas y técnicas, utilizadas por ciberdelincuentes.
Escenarios en los que se utiliza	• Clasificación de alertas, detección de amenazas y respuesta. • Caza amenazas. • Equipo rojo/emulación de adversario. • Análisis de brechas de seguridad y evaluaciones de madurez del centro de operaciones de seguridad
Orientación	Defensa
Autores u organismos responsables	MITRE Corporation, una organización sin fines de lucro, y es mantenido por MITRE con aportes de una comunidad global de profesionales de la ciberseguridad.
Material original	https://www.ibm.com/mx-es/think/topics/mitre-attack
Certificaciones asociadas	• SANS Institute (GIAC) • CREST (Organización internacional de seguridad) • Certificaciones de Offensive Security • Certificaciones de Blue Team / SOC • Certificaciones específicas de Threat Intelligence
Versiones o actualizaciones vigentes	Versión 16 lanzada en octubre de 2024

OWASP WSTG	
Descripción	La **Web Security Testing Guide (WSTG)** es la referencia definitiva para la evaluación de seguridad en servicios y aplicaciones web, ofreciendo un marco de mejores prácticas para evaluadores internos y externos.
Fases de implementación	• **Planificación y Preparación:** Definir el alcance de la prueba web. • **Reconocimiento Pasivo/Activo:** Recolección de información sobre el objetivo. • **Pruebas de Configuración y Gestión:** Revisión de la infraestructura del servidor. • **Pruebas de Autenticación y Gestión de Sesiones:** Verificar la seguridad de los inicios de sesión. • **Pruebas de Autorización y Control de Acceso:** Validar que los usuarios solo accedan a lo permitido. • **Pruebas de Validación de Entrada (Inyecciones):** Búsqueda de fallos como SQLi o XSS. • **Pruebas de Lógica de Negocio:** Evaluar el flujo operativo de la aplicación. • **Pruebas de APIs y Servicios Web:** Análisis de comunicaciones entre sistemas. • **Pruebas del Lado del Cliente:** Evaluación de seguridad en el navegador del usuario. • **Revisión y Reporte:** Documentación final de vulnerabilidades.
Objetivo principal	Identificar y corregir vulnerabilidades específicas del entorno web.

Escenarios en los que se utiliza	• Pentesting Ético Formal • Bug Bounty Programs • Desarrollo Seguro (DevSecOps) • Auditorías de Cumplimiento • Respuesta a Incidentes
Orientación	Evaluación
Autores u organismos responsables	OWASP WSTG fue creado por y para la comunidad de seguridad.
Material original	https://owasp-org.translate.goog/www-project-web-security-testing-guide/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc
Certificaciones asociadas	• OSWE (Offensive Security Web Expert) • GWAPT (GIAC Web Application Penetration Tester) • Burp Suite Certified Practitioner de PortSwigger • Certificaciones de eLearnSecurity
Versiones o actualizaciones vigentes	WSTG v4.2 (2021)
NIST SP 800-115	
Descripción	Marco metodológico formal para la evaluación técnica de seguridad, base fundamental para programas de evaluación en sectores altamente regulados.
Fases de implementación	• **Planificación:** Establecer objetivos y reglas de compromiso. • **Descubrimiento:** Identificar activos y servicios en la red.

	• **Ataque:** Ejecutar pruebas de penetración para confirmar vulnerabilidades. • **Reporte:** Entrega de resultados y recomendaciones técnicas.
Objetivo principal	Asistir a las organizaciones en la planificación y ejecución de exámenes de seguridad de la información de manera estructurada.
Escenarios en los que se utiliza	• Sector Público Federal de EE.UU. • Sectores Regulados. • Organizaciones de Alta Madurez. • Base para Programas de Evaluación Interna
Orientación	Evaluación
Autores u organismos responsables	Gobierno de Estados Unidos
Material original	https://www.nist.gov/privacy-framework/nist-sp-800-115
Certificaciones asociadas	No hay certificaciones oficiales emitidas por NIST
Versiones o actualizaciones vigentes	Única versión lanzada en 2008
OSSTMM	
Descripción	La **Metodología de Manual de Pruebas de Seguridad de Código Abierto (OSSTMM)** se distingue por su enfoque científico y holístico.

	No se limita a buscar fallos, sino que busca medir la seguridad operacional con precisión matemática.
Fases de implementación	• **Seguridad Humana:** Evaluación de protocolos y concienciación del personal. • **Seguridad Física:** Pruebas de acceso a instalaciones y hardware. • **Seguridad Inalámbrica (Wireless):** Análisis de redes Wi-Fi, Bluetooth y radiofrecuencia. • **Telecomunicaciones:** Evaluación de sistemas de voz y datos digitales. • **Redes de Datos:** Pruebas exhaustivas sobre la infraestructura de red.
Objetivo principal	Evaluación cuantitativa de la seguridad a través de diversos canales (humano, físico, inalámbrico, telecomunicaciones y redes).
Escenarios en los que se utiliza	• Grandes corporaciones. • Equipos de aseguramiento. • Telecomunicaciones. • Logística.
Orientación	Evaluación
Autores u organismos responsables	ISECOM
Material original	https://www.isecom.org/OSSTMM.3.pdf
Certificaciones asociadas	• OPST (OSSTMM Professional Security Tester) • OPSA (OSSTMM Professional Security Analyst) • OPSE (OSSTMM Professional Security Expert)

Versiones o actualizaciones vigentes	OSSTMM 3 (2016)
PTES	
Descripción	El **Penetration Testing Execution Standard (PTES)** nació para eliminar la ambigüedad en la industria, estableciendo qué debe esperar un cliente de una prueba de penetración de alta calidad.
Fases de implementación	• **Pre-engagement:** Acuerdos contractuales y definición de límites. • **Intelligence Gathering:** Recolección minuciosa de información sobre el objetivo. • **Threat Modeling:** Identificación y diseño de posibles vectores de ataque. • **Vulnerability Analysis:** Análisis sistemático de debilidades detectadas. • **Exploitation:** Ejecución de ataques para ganar acceso a los sistemas. • **Post-Exploitation:** Evaluación del impacto real tras el compromiso del sistema. • **Reporting:** Presentación profesional de hallazgos y mitigaciones.
Objetivo principal	Estandarizar las fases de un pentest para asegurar que se cubran todos los aspectos técnicos y operativos, desde el acuerdo inicial hasta la explotación.
Escenarios en los que se utiliza	• Pentesting externo (Red team / Seguridad perimetral). • Pentesting interno (Red interna y Active Directory). • Pentesting de aplicaciones web. • Pentesting de infraestructura cloud (AWS, Azure, GCP). • Pentesting de ingeniería social y físico.

Orientación	Ataque
Autores u organismos responsables	Comunidad de ciberseguridad.
Material original	https://www-pentest--standard-org.translate.goog/index.php/PTES_Technical_Guidelines?_x_tr_sch=http&_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc
Certificaciones asociadas	• Certified Lead Ethical Hacker (PECB). • GPEN (GIAC Penetration Tester). • OSCP.
Versiones o actualizaciones vigentes	No hay un sistema de versiones, pero se divide por componentes: El Estándar (The Standard) La Guía Técnica (Technical Guidelines)
ISSAF	
Descripción	El **Information Systems Security Assessment Framework (ISSAF)** es una metodología extremadamente exhaustiva diseñada para evaluaciones de "Caja Blanca" (White Box) y auditorías profesionales de principio a fin.

Fases de implementación	• **Planificación y Preparación:** Intercambio inicial de información y definición del entorno. • **Evaluación (Assessment):** Ejecución técnica detallada de las pruebas de seguridad. • **Reporte y Limpieza:** Entrega de informe final y eliminación de cualquier herramienta de ataque utilizada.
Objetivo principal	Proporcionar un marco técnico estandarizado para evaluar la seguridad de los sistemas de información de manera profesional y organizada.
Escenarios en los que se utiliza	• Auditorías de Cumplimiento (Compliance). • Pentesting de "Caja Blanca" (White Box). • Evaluación de Infraestructuras Críticas. • Formación de Nuevos Auditores.
Orientación	Evaluación y ataque
Autores u organismos responsables	OISSG (Open Information Systems Security Group).
Material original	https://pymesec.org/issaf/
Certificaciones asociadas	• CISA (Certified Information Systems Auditor) de ISACA. • CISSP (Certified Information Systems Security Professional). • CEH (Certified Ethical Hacker). • OSCP (Offensive Security Certified Professional).
Versiones o actualizaciones vigentes	v0.2 (2000)

Conclusión

Tras el análisis comparativo de cada metodología, queda claro que no existe una metodología única o mejor que las demás, sino que cada una cumple un propósito específico dentro del ecosistema de la ciberseguridad. Mientras que MITRE ATT&CK es indispensable para entender el comportamiento de los adversarios y mejorar la detección defensiva, marcos como PTES y OWASP WSTG ofrecen estructuras robustas para la ejecución de pruebas ofensivas en infraestructuras y aplicaciones web, respectivamente, NIST SP 800-115 e ISSAF proporcionan el rigor necesario para auditorías formales y evaluaciones técnicas, mientras que OSSTMM destaca por su enfoque científico y matemático para medir la seguridad operacional. Por último, es importante saber que seleccionar y combinar con estos marcos según el contexto organizacional que es lo que garantiza una identificación de riesgos efectiva y una protección real de los activos digitales.