181760 - Josué Emiliano Rosales Ramírez

	MTRE ATT& CK	OWASP WSTG	NIST SP 800 115	OSSTMM	PTES	ISSAF
Descripción breve de la metodología.	Se refiere a un grupo de tácticas organizadas en una matriz, que describen varias técnicas que utilizan los cazadores de amenazas, defensores y miembros del equipo rojo para evaluar el riesgo para una organización y clasificar los ataques.	Describe un marco de pruebas de aplicaciones web sugerido y también proporciona información general sobre cómo probar aplicaciones web con buenas prácticas de prueba.	Es una guía, por lo tanto ofrece metodologías, técnicas y procedimientos: →Planificación de la Evaluación de Seguridad →Ejecución de la Evaluación de Seguridad →Actividades Post-Pruebas →Escaneo de Vulnerabilidades →Técnicas de Pruebas de Seguridad (incluyendo revisiones y análisis, evaluaciones y valoraciones) →Pruebas de Penetración	Este manual proporciona un marco de trabajo que describe las fases a seguir en la ejecución de una auditoría de seguridad o Pentesting	Es un estandar que sirve como guía para la ejecución de pruebas de pentesting. Que ofrece un marco estructurado y sistematico con el fin de proporcionar claridad y uniformidad.	Es una extensa metodología donde detalla 3 fases para realizar una prueba de penetración. En esta hay un acuerdo de evaluacion que sirve como acuerdo legal entre ambas partes y distribuye sus pruebas de penetración en varias capas.
Fases de implementación.	Mas que fases, son técnicas que representan las etapas del ciclo de vida de un ataque de un adversario 1-Reconocimiento. 2-Desarrollo de recursos. 3-Acceso inicial. 4-Ejecución. 5-Persistencia. 6-Escalada de privilegios. 7-Evasión de defensa. 8-Acceso a credenciales. 9-Descubrimiento. 10-Movimiento lateral (amplia el alcance). 11-Colección. 12-Mando y control. 13-Exfiltración. 14-Impacto	1-Planificación y alcance 2-Configuración y Reconocimiento 3-Ejecución de pruebas 4-Informes y remedación	1-Planeación y preparación 2-Recolección de información 3-Analisis de vulnerabilidades y explotación 4-Actividades Post-testeo (Resumen ejecutivo y Apendice técnico)	Seguridad de la Información Procesos de Seguridad Tecnologías de Internet y su Seguridad Comunicaciones y Seguridad Seguridad Inalámbrica Evaluación de la Seguridad Física	1-Definición de alcance 2-Recopilación de información sobre el objetivo. 3-Explotación (Vulnerabilidades identificadas). 4-Post-explotación	**Fase 1**:Planificación y preparación (reunión legal para confirmar alncance, enfoque y metodología) **Fase 2**: Evaluación 1-Recopilación 2-Mapeo de Redes 3-Identificación de vulnerabilidades 4-Penetración 5-Obtener Acceso y escalar privilegios 6-Enumerando más 7-Comprometer usuarios/sitios remotos 8-Mantenimiento del acceso 9-Ocultar pistas **Fase 3**:Tratamiento que proporciona una plataforma para tomar una decisión sobre los riesgos residuales.
Objetivo principal (ejemplo: detección de técnicas de ataque, pruebas técnicas, evaluación de controles, etc	Es fortalecer los pasos que se toman después de que una organización se ha visto comprometida. De esta manera, el equipo de ciberseguridad puede responder preguntas importantes sobre cómo el atacante pudo penetrar en el sistema y qué hizo una vez que ingresó.	Proporcionar un marco de mejores prácticas comúnmente utilizadas por testeadores de penetración externos y organizaciones que realizan pruebas internas.	Proporciona a las organizaciones una visión general comprensiva y orientación sobre cómo realizar pruebas y evaluaciones de seguridad. El documento está destinado a dar a las organizaciones un enfoque estructurado para identificar vulnerabilidades y debilidades en sus sistemas de información, validar la efectividad de las medidas de seguridad y asegurar el cumplimiento de las políticas y regulaciones de seguridad.	Realización de pruebas de seguridad informática, proporcionando una metodología detallada para evaluar la seguridad en diversos sistemas, desde redes y aplicaciones web hasta dispositivos móviles y sistemas de control industrial.	Que la realización del pentesting cubra y reporte todos los hallazgos, pues cumple estandares de calidad. Además da gran aportación pues mitiga riesgos por su eficiencia operativa y sistematica.	Realización de pruebas de penetración con base y acuerdos legales entre ambas partes.
Escenarios en los que se utiliza.	⋆Compartir información entre organizaciones sobre cómo se comportan las amenazas ⋆Emulando el comportamiento y las tácticas de diferentes tipos de hackers con fines de capacitación interna ⋆Averiguar qué tácticas se utilizan con más frecuencia para que los equipos de ciberdefensa puedan estar atentos a ellas	Gestión de Configuración y Despliegue Gestión de Identidad Autenticación Autorización Gestión de Sesiones Validación de Entrada Manejo de Errores Criptografía Débil Lógica de Negocio Del lado del Cliente API	Se aplica en términos generales a cualquier organización o entidad que desee realizar pruebas y evaluaciones de seguridad de sus sistemas de información. Esto incluye agencias gubernamentales, empresas del sector privado y organizaciones sin fines de lucro	Al momento de realizar un lanzamiento de una página web o aplicación y que se desee realizar una evaluación de seguridad correcta	Se aplica en momentos donde se requiere de una buena documentación detallada sobre los riesgos hallados y se desee mas pruebas exhaustivas respecto a la seguridad de un sistema.	Cuando se requieren realizar pruebas de evaluación con el fin de tomar decisiones sobre los riegos que salieron, al ser muy extenso abarca todas las fases de una evaluación de seguridad, desde la planificación hasta la mitigación de riegos.
Orientación (ataque, defensa o evaluación).	Evaluación	Defensa	Evaluación	Pruebas	Evaluación de ataques.	Evaluación
Autores u organismos responsables.	MIT	The OWASP® Foundation	NIST (National Institute of Standards and Technology)	ISECOM	No organismo oficial	OISSG (Open Information Systems Security Group)
URL del material oficial.	https://attack.mitre.org	OWASP Web Security Testing Guide	NIST SP 800-115	https://www.isecom.org/OSSTMM.3.pdf .	The Penetration Testing Execution Standard	ISSAF - PYMESEC
Existencia de certificaciones asociadas.	No cuenta con certificaciones asociadas	No cuenta con certificaciones asociadas	No cuenta con certificaciones asociadas	OPSA (OSSTMM Professional Security Analyst) OPST (OSSTMM Professional Security Tester)	No cuenta con certificaciones asociadas	No cuenta con certificaciones asociadas
Versiones o actualizaciones vigentes.	ATT&CK v18.1 - 28 de Octubre del 2025	[Version 4.2] - 2020-12-03	La actualización más reciente fue lanzada en abril de 2021.	Ultima version 14 de Diciembre del 2010.	Última edición 30 de abril del 2012	2006
Fuentes	https://www.ibm.com/mx-es/think/topics/mitre-attack https://www.fortinet.com/lat/resources/cyberglossary/mitre-attck	https://devguide.owasp.org/es/06-verification/01-guides/01-wstg/	NIST 800-115 | Secureframe	https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml#Fundamentos_y_relevancia_de_OSSTMM_en_la_proteccion_digital	▶ Penetration Testing Execution Standard (PTES)	metodología issaf - Emilio Peinado https://pymesec.org/issaf/