UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

CARRERA: INGENIERIA EN TECNOLOGIAS DE LA INFORMACION

MATERIA: SEGURIDAD INFORMATICA

TRABAJO: CARTOGRAFIANDO EL PENTESTING: ANÁLISIS COMPARATIVO DE METODOLOGÍAS DE SEGURIDAD INFORMÁTICA

PARCIAL: 1

Alumno: Rodriguez Moreno Cristian Alejandro/ Matrícula:181641

Profesor: Servando López Contreras

Metodología	A. Descripción breve	B. Fases de implementación	C. Objetivo principal	D. Escenarios de uso
MITRE ATT&CK	Es una lista de tácticas y métodos que usan los ciberdelincuentes basándose en incidentes reales.	No es secuencial. Se basa en matrices de tácticas (por qué) y técnicas (cómo).	Establecer un vocabulario estándar para describir acciones de adversarios y fortalecer la detección.	Diseño de operaciones (ofensivo) e identificación de puntos débiles (defensivo).
OWASP WSTG	Guía de referencia completa para evaluar la seguridad de aplicaciones web mediante pruebas.	12 áreas de evaluación (autenticación, gestión de sesiones, lógica de negocio, etc.).	Ofrecer un estándar reconocido para realizar pruebas metódicas y exhaustivas en aplicaciones web.	Auditorías web, revisiones de código y ciclos de desarrollo seguro.
NIST SP 800-115	Documento del gobierno con recomendaciones para pruebas de seguridad en sistemas.	Tres etapas: Preparación, Desarrollo (ataque) y Cierre (informes).	Asistir en la planificación y ejecución de evaluaciones técnicas para detectar vulnerabilidades.	Entidades gubernamentales y corporaciones con requisitos normativos federales.
OSSTMM	Manual con enfoque riguroso y verificable para cuantificar la seguridad operacional (humana, física y digital).	Examen de canales: humano, entorno físico, redes inalámbricas y comunicaciones.	Brindar un procedimiento para obtener resultados cuantificables y contrastables (métricas RAVs).	Evaluaciones integrales que contemplan instalaciones, procedimientos e interacción humana.
PTES	Estándar desarrollado por expertos para unificar criterios y definir el proceso completo de un pentesting.	7 fases: Acuerdo, Inteligencia, Amenazas, Vulnerabilidades, Explotación, Post-explotación e Informes.	Crear un estándar universal para que contratantes y profesionales compartan el mismo entendimiento.	Consultores de seguridad y compañías que definen servicios de pentesting contratados.
ISSAF	Marco de evaluación exhaustivo sobre facetas técnicas, organizativas y legales (actualmente de uso residual).	Áreas de conocimiento (redes, sistemas, apps) con etapas desde preparación hasta reporte.	Ofrecer un marco integral con técnicas, metodologías y ejemplos de herramientas de intrusión.	Referencia histórica o extracción de ideas para dominios particulares.

Metodología	E. Orientación	F. Autores / Organismo	G. URL del material oficial	H. Certificaciones	I. Versión vigente
MITRE ATT&CK	Ataque y Defensa	MITRE Corporation	https://attack.mitre.org/	No cuenta con certificación	Renovación continua (consultar portal oficial).
OWASP WSTG	Evaluación	OWASP Foundation	https://owasp.org/www-project-web-security-testing-guide/	Base fundamental de acreditaciones en seguridad web (eWPT, OSWE).	Edición 4.2 (estable).
NIST SP 800-115	Evaluación	NIST	https://csrc.nist.gov/pubs/sp/800/115/final	No posee certificaciones	Publicado en el año 2008.
OSSTMM	Evaluación y Defensa	ISECOM	https://www.isecom.org/OSSTMM.3.pdf	Certificaciones oficiales OPST y OPSA.	Edición 3 (2010).
PTES	Ataque y Evaluación	Comunidad de especialistas	http://www.pentest-standard.org/	Reconocido en el sector como estándar de referencia	Versión completa de 2010.
ISSAF	Ataque y Evaluación	OISSG	https://pymesec.org/issaf/	No generó certificaciones	Borrador 0.2 (2006).