UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

SEGURIDAD INFORMATICA

CARTOGRAFIANDO EL PENTESTING: ANÁLISIS COMPARATIVO DE METODOLOGÍAS DE SEGURIDAD INFORMÁTICA

Moreno Solís Gisela Geraldine 176522

Criterio	1. MITRE ATT&CK	2. OWASP WSTG	3. NIST SP 800-115	4. OSSTMM	5. PTES	6. ISSAF
A. Descripción	Base de conocimientos global sobre tácticas y técnicas de adversarios basada en observaciones del mundo real.	Guía técnica principal para pruebas de seguridad en aplicaciones web, enfocada en vulnerabilidades comunes.	Guía técnica de seguridad de la información para realizar evaluaciones y pruebas de penetración en sistemas federales (EE. UU.).	Metodología científica y basada en métricas para evaluar la seguridad operativa a través de diferentes canales.	Estándar diseñado para ofrecer un lenguaje común y un marco de trabajo para la ejecución de pruebas de penetración comerciales.	Framework (ya descontinuado) que ofrecía una guía muy detallada y estructurada para la evaluación de seguridad de sistemas.
B. Fases de implementación	Matrices (Enterprise, Mobile, ICS) divididas en **14 Tácticas** (ej. Reconocimiento, Acceso Inicial, Persistencia, Exfiltración).	1. Recopilación de info. 2. Gestión de config. 3. Gestión de identidad. 4. Autenticación. 5. Autorización. 6. Gestión de sesiones. 7. Validación de datos.	1. Planificación. 2. Descubrimiento. 3. Ataque. 4. Reporte.	**Fases:** Inducción, Interacción, Inquisición, Intervención. **Canales:** Humano, Físico, Inalámbrico, Telecom, Redes de datos.	1. Pre-acuerdo. 2. Recolección de Inteligencia. 3. Modelado de Amenazas. 4. Análisis de Vulnerabilidades. 5. Explotación. 6. Post-Explotación. 7. Reporte.	1. Planificación y preparación. 2. Evaluación. 3. Tratamiento. 4. Acreditación.
C. Objetivo principal	Clasificar y describir ciberataques para mejorar la detección, la inteligencia de amenazas y la emulación de adversarios.	Proporcionar un marco exhaustivo para probar la seguridad de aplicaciones y servicios web.	Orientar a organizaciones (especialmente gubernamentales) sobre cómo planificar y ejecutar evaluaciones técnicas de seguridad.	Proporcionar una medición científica y cuantificable (RAVs) de la seguridad operativa.	Estandarizar la **ejecución** de un pentest para garantizar calidad y consistencia en el servicio.	Evaluar controles de seguridad con un nivel de detalle técnico muy granular y específico.
D. Escenarios de uso	Threat Hunting, Red Teaming, mejora de SOCs, emulación de adversarios.	Auditorías de aplicaciones web, desarrollo seguro (SDLC), pruebas de cumplimiento (PCI-DSS).	Auditorías de cumplimiento (FISMA), evaluaciones de seguridad en agencias federales o corporativos.	Auditorías que requieren métricas exactas de seguridad y cumplimiento normativo estricto.	Pentesting comercial (caja negra/blanca/gris), consultoría de seguridad ofensiva estándar.	Evaluaciones técnicas profundas y complejas (aunque su uso ha disminuido por falta de actualización).
E. Orientación	**Defensa / Ataque** (Emulación y Detección).	**Evaluación** (Enfoque en AppSec y Bugs).	**Evaluación** (Cumplimiento y Auditoría).	**Evaluación / Defensa** (Métricas de seguridad).	**Ataque** (Ofensiva / Pentesting puro).	**Evaluación** (Auditoría técnica).
F. Autores / Organismos	**MITRE Corporation**.	**OWASP Foundation** (Open Web Application Security Project).	**NIST** (National Institute of Standards and Technology).	**ISECOM** (Institute for Security and Open Methodologies) - Pete Herzog.	Grupo de expertos en seguridad (Nickerson, et al.).	**OISSG** (Open Information Systems Security Group).
G. URL Oficial	attack.mitre.org	owasp.org/www-project-web-security-testing-guide	csrc.nist.gov/publications/detail/sp/800-115/final	isecom.org/research.html	pentest-standard.org	(Sitio inactivo, archivos en sourceforge.net/projects/issaf)
H. Certificaciones	MITRE ATT&CK Defender (MAD).	No directa (usada en OSWE, GWAPT, etc.).	No directa (referencia clave en CISA, CISM, CEH).	**OPST** (OSSTMM Professional Security Tester), **OPSA**.	Referencia para **eCPPT** (eLearnSecurity) y **OSCP**.	Anteriormente CPT (Certified Penetration Tester) de IACRB (legado).
I. Versiones vigentes	v16 (se actualiza semestralmente).	v4.2 (Estable) / v5.0 (En desarrollo).	Rev 1 (2008) - Aún vigente como estándar base.	v3.0 (Vigente) / v4 (Borrador/Investigación).	v1.0 (Estándar continuo).	v0.2.1 (2006) - **Descontinuado / Legado**.