

**UNIVERSIDAD POLITÉCNICA DE  
SAN LUIS POTOSÍ**

**CARRERA: INGENIERIA EN TECNOLOGIAS DE LA INFORMACION**

**MATERIA: SEGURIDAD INFORMATICA**

**TRABAJO: RESUMEN DEL LIBRO**

**PARCIAL: 1**

**Alumno:** Rodriguez Moreno Cristian Alejandro/ Matrícula:181641

**Profesor:** Servando López Contreras

Metodología / Marco	A. Descripción breve	B. Fases de implementación	C. Objetivo principal	D. Escenarios en los que se utiliza	E. Orientación	F. Autores u organismos	G. URL Oficial	H. Certificaciones	I. Versión Vigente
1. MITRE ATT&CK	Base de conocimiento global de tácticas y técnicas de adversarios basada en observaciones reales.	Matriz de tácticas (Recon, Initial Access, Ejecución, Persistencia, etc.). No es lineal. 12 categorías	Detección y descripción de comportamientos y técnicas de ataque.	SOC, Emulación de adversarios, Threat Intelligence (CTI).	Defensa / Emulación de ataque	MITRE Corporation	<a href="https://attack.mitre.org">https://attack.mitre.org</a>	MITRE ATT&CK Defender (MAD)	v16 (Octubre 2024)
2. OWASP WSTG	Guía integral para probar la seguridad de aplicaciones web y servicios web. Guía técnica para realizar evaluaciones y pruebas de seguridad de la información.	Guías (Recopilación de información, Configuración, Autenticación, etc.). 1. Planificación, 2. Ejecución, 3. Post-ejecución (Análisis de resultados).	Evaluación de técnicas de control de identidad, seguridad en aplicaciones web.	Aplicaciones Web, APIs, Servicios en la nube.	Ataque / Evaluación Técnica	OWASP Foundation	<a href="https://owasp.org/www-project-web-security-testing-guide/">https://owasp.org/www-project-web-security-testing-guide/</a>	Relaciones: OSWA, OSWE (OffSec)	v4.2 (v5 en desarrollo)
3. NIST SP 800-115	Guía para realizar evaluaciones y pruebas de seguridad de la información.	1. Planificación, 2. Ejecución, 3. Post-ejecución (Análisis de resultados).	Estandarización de pruebas y revisión de seguridad.	Gubernamentales, Cumplimiento (Compliance) y Auditoría.	Evaluación / Auditoría	NIST (EE.UU.)	<a href="https://csrc.nist.gov/publications/details/sp800-115/final">https://csrc.nist.gov/publications/details/sp800-115/final</a>	Alineada con CISA, Security+	Final (Vigente como referencia)
4. OSSTMM	Estándar científico para la evaluación	1. Alcance, 2. Canal (Físico, Medición de la seguridad)	Infraestructura crítica, seguridad	Evaluación (Científica)	ISECOM (Pete Herzog)	<a href="https://www.isecom.org/research.htm">https://www.isecom.org/research.htm</a>	OPST, OPSA	v3.0	

	<p>ón de la segurida Espectral d , etc.), 3. d operativ Índice de operativa a y segurida a través métricas d de d física y . (RAVs). métricas. de redes. <a href="#">ml</a> Pre- engagem ent, Intelligen</p> <p>Estándar ce que Gatherin define g, Threat los Modeling proceso , Definir s Vulnerabi un Pentestin necesari lity lenguaje g os para Analysis, común y corporati realizar Exploitati expectati vo de Base un on, Post- vas para infraestru Comunid <a href="http://www.pentes">http://www.pentes</a> para pentesti exploitati empresa ctura y Ataque ad de <a href="http://www.pentes">w.pentes</a> certificaci ng de on, s y redes (Proceso expertos <a href="http://www.pentes">t-</a> ones alta Reportin pentester compleja s de (Nick <a href="http://www.pentes">standard.</a> como calidad. g. s. s. negocio) Percoco) <a href="http://www.pentes">org/</a> OSCP v1.1</p> <p>Marco 1. estructur Planifica ado que ción, 2. Evaluaci organiza Evaluaci ón las ón profunda Centros pruebas (Recon, de de datos, de Enumera controles redes segurida ción, de corporati <a href="https://sourceforge.net/projects/issaf/">https://so</a> Ninguna d en Explotaci segurida vas Evaluaci <a href="https://sourceforge.net/projects/issaf/">urceforge</a> activa dominios ón), 3. d por tradicion ón / <a href="https://sourceforge.net/projects/issaf/">.net/proje</a> actualme 6. ISSAF técnicos. Informe. capas. ales. Ataque OISSG <a href="https://sourceforge.net/projects/issaf/">cts/issaf/</a> nte v0.2.1</p>
5. PTES	
6. ISSAF	