



Activando el pensamiento,  
generamos conocimiento.

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 organizaciones	G. URL Oficial	H. Certificaciones	I. Versión Vigente
1. MITRE ATT&CK	Base de conocimiento global de tácticas y técnicas de adversarios	Matriz de tácticas (Recon, Initial Access, Execución basada en observación, etc.). No es lineal.	Detección y descripción de SOC, Emulación de comportamiento adversario. Persistencia, / Threat técnicas	SOC, Emulación Defensa /	MITRE ATT&CK v16	MITRE Defender (Octubre 2024)	<a href="https://attack.mitre.org/">https://attack.mitre.org/</a>		
2. OWASP WSTG	Guías integrales (Recopila para probar la seguridad de aplicaciones web, y servicios web).	Evaluación de la seguridad de la aplicación web, configuración de servicios web, etc.).	Evaluación de la seguridad de las APIs, servicios web, y aplicaciones web.	Aplicación de controles de seguridad, identidad de usuarios, y autenticación.	Ataque / OWASP OWASP Foundation	Relacionadas: OSWA, OSWE (OffSec)	<a href="https://owasp.org/www-project-web-security-testing-guide/">https://owasp.org/www-project-web-security-testing-guide/</a>	v4.2 (v5)	(v5)
3. NIST SP 800-115	Guía técnica 1. para realizar evaluaciones y pruebas de ejecución.	ción, 2. Ejecución y 3. de pruebas de ejecución.	Estandarización mentales de , cumplimiento	Estandarización mentales de , cumplimiento	Evaluación / (EE. UU.)	NIST Alineada con CISA, como referencia	<a href="https://csrc.nist.gov/publications/sp-800-115/final">https://csrc.nist.gov/publications/sp-800-115/final</a>	Final (Vigente)	
4. OSSTMM	Estándar 1. para la evaluación científica de la seguridad física.	Medición Alcance, de la seguridad física.	Infraestructura crítica, (Científico Herzog)	Evaluación técnica de la seguridad física.	Evaluación técnica de la seguridad física.	ISECOM (Pete Herzog)	<a href="https://www.isecom.org/resource-search.html">https://www.isecom.org/resource-search.html</a>	OPST, OPSA	v3.0

	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. Pre- engagem ent, Intelligen	<a href="#">ml</a>
	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 un on, Post- vas para infraestruc Comunid <a href="http://ww">http://ww</a> para pentesti exploitati empresa ctura y Ataque ad de <a href="#">w.pentes</a> certificaci ng de on, s y redes (Proceso expertos <a href="#">t-</a> ones alta Reportin pentester compleja s de (Nick <a href="#">standard.</a> como 5. PTES calidad. g. s. s. negocio) Percoco) <a href="#">org/</a> OSCP v1.1 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 d en Explotaci segurida vas Evaluaci dominios ón), 3. d por tradicion ón /	Base <a href="https://so">https://so</a> Ninguna <a href="urceforge">urceforge</a> activa <a href=".net/proje">.net/proje</a> actualme <a href="cts/issaf/">cts/issaf/</a> nte v0.2.1
6. ISSAF	técnicos. Informe. capas. ales. Ataque OISSG	