ACTIVIDAD 05

CNO V: Seguridad Informática

16 DE FEBRERO DE 2026

CASTILLO OLVERA CARLOS RENÉ

182033

Mtro. Servando López Contreras

Metodología	Descripción breve	Fases de implementación	Objetivo principal	Escenarios de uso	Orientación	Autores / Organismo	URL oficial	Certificaciones asociadas	Versiones vigentes
MITRE ATT&CK	Marco de conocimiento que documenta tácticas y técnicas reales usadas por adversarios basadas en casos reales. No es una metodología de pentesting tradicional, sino un modelo de referencia para simulación y defensa.	1. Selección de matriz (Enterprise, Mobile, ICS) 2. Identificación de tácticas 3. Mapeo de técnicas 4. Simulación o evaluación de controles 5. Análisis de cobertura defensiva	Detectar, analizar y simular técnicas reales de ataque para fortalecer la defensa.	Red Team, Blue Team, Purple Team, threat hunting, SOC, evaluación de madurez defensiva.	Defensa y evaluación ofensiva controlada	MITRE Corporation	https://attack.mitre.org	No oficial propia; usada en certificaciones como Security+, CEH, CySA+, etc.	Actualizaciones continuas (Enterprise ATT&CK v14+ en adelante)
OWASP WSTG	Guía metodológica para pruebas de seguridad en aplicaciones web. Forma parte del proyecto OWASP.	1. Información y configuración 2. Pruebas de autenticación 3. Gestión de sesiones 4. Validación de entradas 5. Lógica de negocio 6. Criptografía 7. Cliente	Evaluar vulnerabilidades en aplicaciones web.	Auditorías de aplicaciones web, APIs, comercio electrónico, desarrollo seguro (SDLC).	Ataque técnico estructurado	OWASP Foundation	https://owasp.org/www-project-web-security-testing-guide/	No certificación directa; relacionada con OSCP, eWPT, GWAPT, etc.	WSTG v4.2 (estable)
NIST SP 800-115	Guía técnica del gobierno de EE.UU. para pruebas y evaluación de seguridad. Enfocada en controles y cumplimiento normativo.	1. Planificación 2. Descubrimiento 3. Ataque 4. Reporte	Evaluar la efectividad de controles de seguridad.	Entornos gubernamentales, auditorías regulatorias, evaluación de cumplimiento.	Evaluación y defensa	NIST (National Institute of Standards and Technology)	https://csrc.nist.gov/publications/detail/sp/800-115/final	Asociada a certificaciones como CISSP, CISA, CAP	Publicación original 2008 (vigente como referencia técnica)
ISECOM OSSTMM	Manual metodológico abierto para pruebas de seguridad operativa. Basado en métricas cuantificables (RAV).	1. Alcance 2. Recolección de información 3. Análisis de canales (humano, físico, inalámbrico, telecom, datos) 4. Verificación 5. Métricas y reporte	Medir la seguridad operativa mediante pruebas verificables.	Infraestructura crítica, auditorías integrales, seguridad física y lógica.	Evaluación técnica estructurada	ISECOM	https://www.isecom.org/OSSTMM.3.pdf	OSSTMM Professional Security Tester (OPST)	OSSTMM 3.0
Penetration Testing Execution Standard (PTES)	Estándar técnico que define un proceso completo de pentesting desde pre-engagement hasta reporte.	1. Pre-engagement 2. Recolección de inteligencia 3. Modelado de amenazas 4. Análisis de vulnerabilidades 5. Explotación 6. Post-explotación 7. Reporte	Estandarizar la ejecución profesional de pruebas de penetración.	Pentesting corporativo, pruebas internas/externas, Red Team.	Ataque controlado	Comunidad PTES	http://www.pentest-standard.org	No certificación oficial propia	Versión técnica estable (no actualizaciones frecuentes recientes)
Open Information Systems Security Group ISSAF	Marco detallado para evaluación de seguridad técnica con enfoque práctico en pruebas de penetración.	1. Planeación 2. Evaluación 3. Explotación 4. Post-explotación 5. Reporte	Proporcionar guía técnica detallada para pruebas de seguridad.	Auditorías técnicas profundas, pruebas en infraestructura y redes.	Ataque técnico	OISSG (Open Information Systems Security Group)	http://www.oissg.org/issaf	No certificación oficial activa	Última versión pública 0.2 (proyecto con poca actualización reciente)

Fuentes:

Cisco Networking Academy. (s. f.). Hacker Ético [Curso en línea]. https://www.netacad.com/launch?id=3b07bfc3-9b21-4dbd-909ba235416df136&tab=curriculum&view=8557e701-847e-535e-b070-db96237065c2

Finn, T. (2025, noviembre 27). Principales metodologías de las pruebas de penetración. Ibm.com. https://www.ibm.com/mx-es/think/insights/pen-testing-methodology

¿Qué es Mitre Att&CK Framework y cómo es útil? (s/f). Fortinet. Recuperado el 16 de febrero de 2026, de https://www.fortinet.com/lat/resources/cyberglossary/mitre-attck

RSI Security. (2024, diciembre 9). NIST's penetration testing recommendations explained. RSI Security. https://blog.rsisecurity.com/nists-penetration-testing-recommendations-explained/

WSTG. (s/f). Owasp.org. Recuperado el 16 de febrero de 2026, de https://devguide.owasp.org/es/06-verification/01-guides/01-wstg/