ACTIVIDAD 05 Cartografiando el pentesting: análisis comparativo de metodologías de seguridad informática

Metodología / Criterio	MITRE ATT&CK	OWASP WSTG	NIST SP 800-115	OSSTMM	PTES	ISSAF
01. Descripción breve	*Base de conocimiento que documenta tácticas, técnicas y procedimientos (TTPs) usados por adversarios reales.*	*Guía técnica para pruebas de seguridad en aplicaciones web desarrollada por OWASP.*	*Guía técnica para pruebas y evaluación de controles de seguridad en sistemas de información.*	*Metodología científica basada en métricas cuantificables para medir seguridad operacional.*	*Marco estándar que define el proceso profesional de pruebas de penetración.*	*Marco integral para evaluación técnica y organizacional de la seguridad.*
02. Fases de implementación	*1. Recolección 2.Mapeo de técnicas 3.Evaluación de controles 4.Simulación 5.Mejora defensiva*	*1.Información 2.Configuración 3.Autenticación 4.Autorización 5.Validación 6.Lógica 7.Cliente*	*1.Planeación 2.Descubrimiento 3.Ataque 4.Reporte*	*1.Alcance 2.Recolección 3.Pruebas técnicas 4.Análisis cuantitativo 5.Reporte*	*1.Pre-engagement 2.Intelligence 3.Threat modeling 4.Vulnerability analysis 5.Exploitation 6.Post-exploitation 7.Reporting*	*1.Planeación 2.Evaluación 3.Explotación 4.Reporte 5.Mejora continua*
03. Objetivo principal	*Detección y análisis de técnicas de ataque basadas en inteligencia real.*	*Identificación de vulnerabilidades web.*	*Evaluación formal de controles de seguridad.*	*Medición objetiva del nivel de seguridad.*	*Estandarizar el proceso completo de pentesting.*	*Evaluación integral de seguridad organizacional.*
04. Escenarios de uso	*SOC, Threat Hunting, Red/Blue Team, análisis forense.*	*Pentesting web, auditorías de software.*	*Auditorías, cumplimiento normativo, gestión de riesgos.*	*Infraestructura, redes, telecomunicaciones.*	*Empresas privadas, Red Team corporativo.*	*Infraestructura empresarial y políticas de seguridad.*
05. Orientación	*Defensa y evaluación ofensiva.*	*Ataque (ofensiva técnica).*	*Evaluación y defensa.*	*Evaluación técnica neutral.*	*Ataque estructurado.*	*Evaluación y ofensiva técnica.*
06. Autor / Organismo	*MITRE Corporation*	*OWASP Foundation*	*NIST (EE.UU.)*	*ISECOM*	*Comunidad PTES*	*OISSG*
07. URL oficial	*https://attack.mitre.org*	*https://owasp.org/www-project-web-security-testing-guide/*	*https://csrc.nist.gov/publications/detail/sp/800-115/final*	*https://www.isecom.org/*	*http://www.pentest-standard.org*	*https://pymesec.org/issaf/*
08. Certificacion asociada	*Referencia en CEH, CISSP, Security+.*	*Relacionada con OSWE, eWPT, OSCP.*	*Referencia en CISSP, CISA, CISM.*	*OPST (OSSTMM Professional Security Tester).*	*Relacionada con OSCP, GPEN, CEH.*	*Sin certificación oficial propia.*
09. Version vigente	*Actualización continua (Enterprise, Mobile, ICS).*	*Versión estable 4.2.*	*Publicación vigente desde 2008.*	*Versión 3.0.*	*Estándar comunitario vigente.*	*Marco de referencia académico.*

Jorge Emmanuel López Monsiváis 179842

Conclusión:

En conclusión, el análisis comparativo de las metodologías MITRE ATT&CK, OWASP WSTG, NIST SP 800-115, OSSTMM, PTES e ISSAF permitió identificar que cada una cumple un propósito específico dentro del ámbito de la ciberseguridad. Aunque todas están orientadas a fortalecer la seguridad de la información, difieren en su enfoque, estructura y aplicación práctica. Algunas se centran en la identificación de técnicas de ataque reales, otras en pruebas especializadas como aplicaciones web, y otras funcionan como marcos formales para auditorías y evaluación de controles.

El estudio de estas metodologías demuestra la importancia de contar con estándares y guías estructuradas para realizar pruebas de penetración de manera ética, profesional y organizada. Asimismo, evidencia que la elección de una metodología depende del contexto, los objetivos de la evaluación y el tipo de infraestructura a analizar. Comprender sus diferencias y alcances contribuye al desarrollo de una visión más integral y estratégica en la gestión de la seguridad informática.

Referencias consultadas:

Open Information Systems Security Group. (s. f.). ISSAF – Information Systems Security Assessment Framework. https://pymesec.org/issaf/

ISECOM. (s. f.). *Open Source Security Testing Methodology Manual (OSSTMM)*. https://www.isecom.org/research.html#content5-9z

Cisco Networking Academy. (s. f.). *Hacker Ético* [Curso en línea]. https://www.netacad.com/launch?id=3b07bfc3-9b21-4dbd-909b-a235416df136&tab=curriculum&view=8557e701-847e-535e-b070-db96237065c2