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	Enciclopedia de técnicas que usan los hackers en la vida real, ideal para aprender cómo atacar y defenderse.	Guía paso a paso para encontrar fallos en páginas web, creada por una comunidad experta en seguridad web.	Documento oficial del gobierno de EE.UU. con recomendaciones para hacer pruebas de seguridad formales.	Metodología que mide la seguridad con números y datos, como si fuera un "examen" de seguridad.	Estándar creado por expertos en hackeo ético para hacer pruebas de penetración de principio a fin.	Marco de trabajo que mezcla lo técnico con lo organizacional, pensado para empresas y auditorías.
02. Fases de implementación	*1. Recolección* *2. Mapeo* *3. Evaluación* *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	*Entender cómo piensan y actúan los atacantes para mejorar la defensa.*	*Encontrar vulnerabilidades en aplicaciones web antes de que lo hagan los malos.*	*Evaluar si los controles de seguridad de una organización realmente funcionan.*	*Medir la seguridad de forma objetiva, como si fuera un puntaje.*	*Estandarizar cómo se hacen las pruebas de penetración para que sean profesionales y completas.*	*Evaluar la seguridad de una empresa desde lo técnico hasta lo administrativo.*
04. Escenarios de uso	*Equipos de defensa (Blue Team), búsqueda de amenazas, análisis forense.*	*Pruebas de seguridad en sitios web, apps y servicios online.*	*Auditorías de cumplimiento, gestión de riesgos, empresas grandes.*	*Redes, telecomunicaciones, infraestructura crítica.*	*Empresas privadas, equipos de Red Team, consultorías.*	*Empresas con infraestructura compleja y políticas de seguridad.*
05. Orientación	Defensa y ataque (muy útil para ambos).	Ataque técnico (enfocado en web).	Evaluación y defensa (enfoque formal).	Evaluación técnica neutral.	Ataque estructurado y profesional	Evaluación y ataque técnico..
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	CEH, CISSP, Security+.	OSWE, eWPT, OSCP.	CISSP, CISA, CISM.	OPST (OSSTMM Professional Security Tester).	OSCP, GPEN, CEH.	No tiene certificación oficial propia.

09. Version vigente	Actualización continua (incluye móvil, nube, ICS).	Versión estable 4.2.	Publicación vigente desde 2008.	Versión 3.0.	Estándar comunitario vigente.	Marco de referencia académico.

Conclusión:

Tras el análisis comparativo de las metodologías de pruebas de seguridad, se concluye que no existe una metodología intrínsecamente superior a otra; cada una responde a objetivos, contextos y alcances específicos dentro del proceso de evaluación de la seguridad de la información. Su aplicabilidad depende del tipo de activo evaluado, del marco regulatorio aplicable, del nivel de madurez organizacional y de los objetivos estratégicos definidos para la prueba.

El marco **MITRE ATT&CK** resulta especialmente valioso para la comprensión estructurada de las tácticas, técnicas y procedimientos (TTPs) utilizados por actores maliciosos, permitiendo modelar escenarios realistas de amenaza y fortalecer capacidades de detección y respuesta. Por su parte, **OWASP Web Security Testing Guide (WSTG)**proporciona una guía técnica exhaustiva para la identificación y explotación controlada de vulnerabilidades en aplicaciones web, convirtiéndose en un estándar de referencia en pruebas específicas de este tipo de sistemas.

En entornos corporativos donde se requiere alineación con normativas, auditorías y estándares internacionales, los marcos del **NIST** ofrecen una estructura sólida para la gestión del riesgo, la implementación de controles y la evaluación sistemática de la seguridad. Finalmente, **OSSTMM** destaca por su enfoque cuantitativo y metodológico, orientado a la medición objetiva de la superficie de ataque y el nivel de exposición mediante métricas verificables.

Desde una perspectiva profesional, la selección adecuada de la metodología debe basarse en un análisis previo que considere el alcance del proyecto, el tipo de infraestructura evaluada, los requerimientos regulatorios y las expectativas del cliente. La correcta integración de estos marcos no solo mejora la efectividad técnica de las pruebas, sino que también garantiza un enfoque estructurado, ético y alineado con buenas prácticas internacionales.

En conclusión, la ciberseguridad no se limita a la ejecución técnica de pruebas de penetración, sino que implica una capacidad estratégica para seleccionar, adaptar y aplicar metodologías de manera coherente con el contexto organizacional. Esta visión integral fortalece el perfil profesional del especialista, promoviendo intervenciones más rigurosas, responsables y orientadas a la gestión integral del riesgo.

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].

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

https://www.netacad.com/launch?id=3b07bfc3-9b21-4dbd-909b-a235416df136&tab=curriculum&view=8557e701-847e-535e-b070-db96237065c2