

Práctica de laboratorio: Comparación de metodologías de pruebas de penetración

Objetivos

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Comparar varias metodologías de pruebas de penetración
- Realizar una investigación de las metodologías populares de pruebas de penetración

Aspectos básicos/Situación

Está realizando una prueba de penetración para un cliente. Para demostrar que los métodos planificados son válidos, utilizará metodologías de pruebas de penetración conocidas y aceptadas. Debido a que hay más de una metodología para elegir, decide investigar y comparar cuatro de las metodologías más utilizadas para familiarizarse con las fortalezas de cada una.

Recursos necesarios

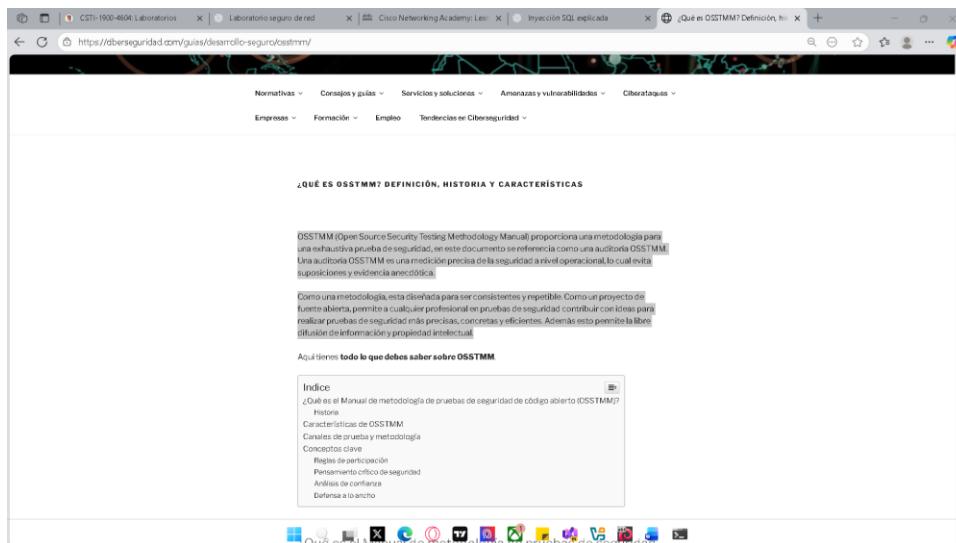
- Computadora personal o dispositivo móvil con acceso a internet

Instrucciones

Parte 1: Realizar investigación de metodologías populares de pruebas de penetración

Con su motor de búsqueda favorito, investigue cuatro de las metodologías de pruebas de penetración más populares:

- OSSTMM



- PTES

Práctica de laboratorio: Comparación de metodologías de pruebas de penetración

The screenshot shows a web browser with multiple tabs open at the top. The main content area features a large banner with the text "Qué es el PTES" over a background of binary code and a keyhole. Below the banner, there is a text block explaining the importance of PTES in modern cybersecurity. A sidebar on the right contains social media icons and a QR code.

Introducción

En el mundo actual, donde las amenazas ciberneticas son cada vez más sofisticadas, es esencial que las organizaciones adopten enfoques proactivos para garantizar la seguridad de su infraestructura de TI. Uno de los métodos más efectivos para evaluar la seguridad de un sistema es la prueba de penetración o pentesting. En este contexto, surge el **Penetration Testing Execution Standard (PTES)**, un marco que proporciona directrices y mejores prácticas para la realización de estas pruebas de manera eficiente y efectiva.

Este artículo tiene como objetivo ofrecer un análisis exhaustivo del PTES, explorando sus componentes clave y su importancia en el campo de la ciberseguridad. También abordaremos cómo el PTES puede ser un aliado crucial para las organizaciones que buscan fortalecer su postura de seguridad.

- OWASP WSTG

The screenshot shows a web browser displaying the OWASP Web Security Testing Guide (WSTG) on the Segu-Info channel. The page includes a navigation bar with links like SEGUINFO, BOLETIN, FORO, ARTICULOS, EDUCACION, SERVICIOS, and CONTACTO. The main content area features a circular diagram illustrating the different phases of the WSTG process. On the right side, there is a sidebar with a search bar, a "Correo electrónico" input field, a "SUSCRÍBEME" button, and a QR code for reporting cybercrimes to ODILA.org.

Guías para análisis web/API OWASP WSTG

El proyecto OWASP Web Security Testing Guide (WSTG) es el principal recurso de pruebas de ciberseguridad para desarrolladores de aplicaciones web y profesionales de la seguridad.

El WSTG es una guía completa para probar la seguridad de aplicaciones y servicios web. Creado gracias a los esfuerzos colaborativos de profesionales de la ciberseguridad y voluntarios dedicados, el WSTG proporciona un marco de mejores prácticas utilizadas por evaluadores de penetración y organizaciones de todo el mundo.

La guía se divide en las siguientes partes:

- 00 - Introduction and Objectives (Introducción y objetivos)
- 01 - Information Gathering (obtención de información)
- 02 - Configuration and Deployment Management Testing (gestión de configuración y despliegue)
- 03 - Identity Management Testing (gestión de identidades)
- 04 - Authentication Testing (mecanismos de autenticación)
- 05 - Authorization Testing (mecanismos de autorización)
- 06 - Session Management Testing (gestión de sesiones)
- 07 - Input Validation Testing (validación de datos de entradas)
- 08 - Testing for Error Handling (gestión de errores)
- 09 - Testing or Weak Cryptography (gestión de procesos criptográficos)

- MITRE ATT Y CK

The screenshot shows the MITRE ATT&CK website. At the top, there are tabs for 'Matrices', 'Táctica', 'Técnicas', 'Defensas', 'CTI', 'Recursos', 'Benefactores', and 'Blog'. A search bar is also present. Below the header, a message says: '¡ATT&CK v18 ha sido lanzado! Consulte la publicación del blog o el registro de cambios para obtener más información.' The main content area features the ATT&CK logo and navigation links like 'Comenzar', 'Hacer un recorrido', 'Contribuir', 'Blog', 'Preguntas más frecuentes', and 'Página aleatoria'. To the right, there is a text box about ATT&CK being a global knowledge base of tactics and techniques used by adversaries based on real-world observations, and another box about its mission to create a safer world through collaboration between government, industry, and the cybersecurity community.

Matriz de ATT&CK para empresas

Diseño: Lateral | Mostrar subtécnicas | Ocultar subtécnicas

Reconocimiento	Desarrollo de recursos	Acceso inicial	Ejecución	Persistencia	Escalada de privilegios	Evasión de defensa	Acceso a credenciales	Descubrimiento	Movimiento lateral	Colección	Comando y control
11 técnicas	8 técnicas	17 técnicas	17 técnicas	23 técnicas	14 técnicas	47 técnicas	17 técnicas	34 técnicas	9 técnicas	17 técnicas	18 técnicas
Escaneo activo (8) Recopilar información del entorno de la víctima (4) Reconocer	Adquirir acceso (9) Adquirir infraestructura (9) Cuentas comprometidas (8)	Inyección de contenido Comando de administración de la red Intérprete de comandos y secuencias de comandos (8)	Manipulación de cuentas (7) Trabajo de BITS Ejecución de scripts y automatización (8)	Mecanismo de control de elevación de usuario (6) Manipulación de tokens de acceso (8)	Mecanismo de control de elevación de abuso (6) Manipulación de aplicaciones (8)	Adversario en el medio (4) Fuerza bruta (4)	Adversario en el medio (4) Detección de ventanas de aplicaciones (4) Desplazamiento de información (4)	Exploitación de servicios remotos Detección de ventanas de aplicaciones (4)	Explotación de cuentas (4) Fuerza bruta (4)	Adversario en el medio (4) Anular los datos recibidos (8)	Protocolo de capa de aplicación (8) Comunicación a través de medios extensos

Paso 1: Recopile información sobre OSSTMM.

En este paso, aprenderá sobre el Manual de metodología de pruebas de seguridad de código abierto (OSSTMM), que incluye una metodología completa para la evaluación de la seguridad.

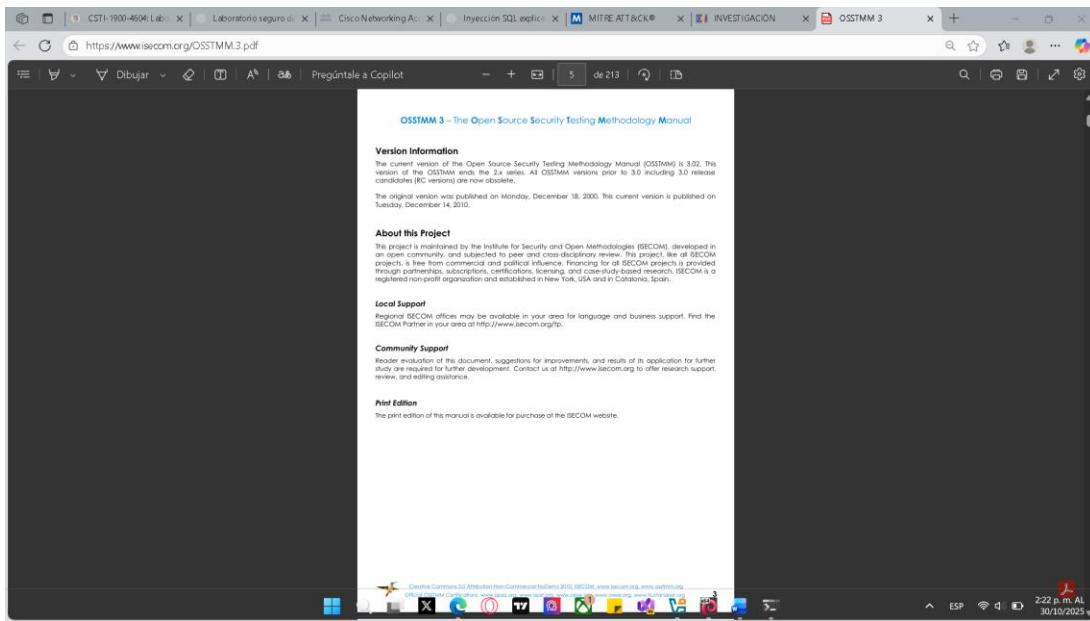
- Navegue a <https://www.isecom.org>, haga clic en RESEARCH > OSSTMM.
- En la página principal de OSSTMM, vea el documento de OSSTMM.

¿Cuál es la última versión del manual y su fecha de derechos de autor?

The screenshot shows a PDF document titled 'OSSTMM 3: The Open Source Security Testing Methodology Manual - Contemporary Security Testing and Analysis'. The cover features a hummingbird in flight. Below the title, it says 'Created by Pete Herzog' and 'Developed by ISECOM'. The ISECOM logo is at the bottom. The document has 213 pages.

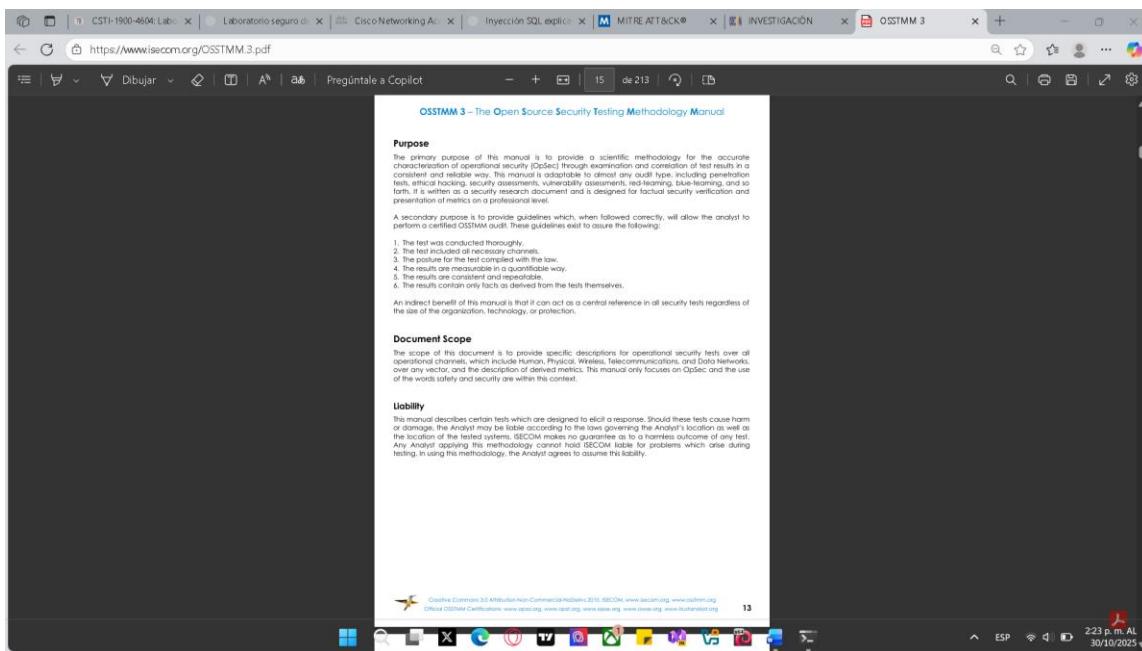
¿Qué organización desarrolla el OSSTMM? ¿Cómo se desempeñan?

Práctica de laboratorio: Comparación de metodologías de pruebas de penetración



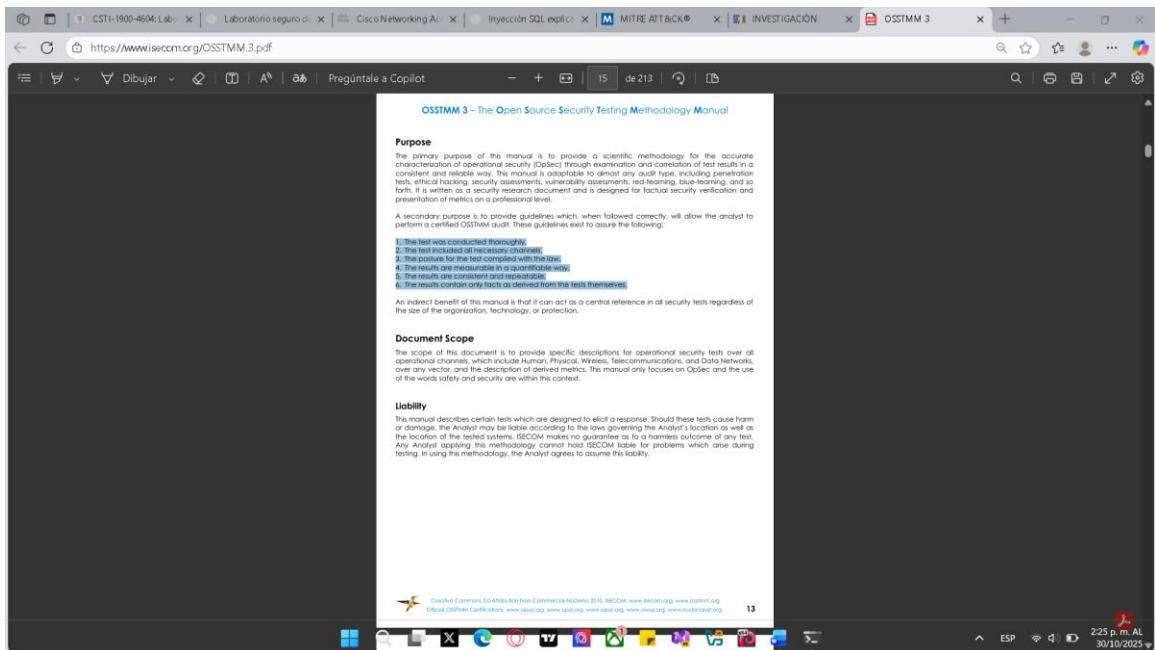
Instituto de Seguridad y Metodologías Abiertas. Las respuestas pueden variar. Publican certificaciones de seguridad, publican libros y realizan investigaciones. Publican un currículum de concientización sobre la seguridad para adolescentes y realizan otras actividades.

¿Cuáles son los propósitos primarios y secundarios declarados del OSSTMM, como se indica en la publicación de OSSTMM?



¿Qué seis resultados se garantizan, entonces, se siguen correctamente las pautas de OSSTM?

Práctica de laboratorio: Comparación de metodologías de pruebas de penetración



Purpose
The primary purpose of this manual is to provide a scientific methodology for the accurate characterization of operational security (OpSec) through examination and correlation of test results in a consistent and reliable way. This manual is adaptable to almost any audit type, including penetration tests, security reviews, and compliance assessments. The manual is intended to be a living document, so it is not set in stone. It is written as a research document and is designed for focused security verification and presentation of metrics on a professional level.

A secondary purpose is to provide guidelines which, when followed correctly, will allow the analyst to perform a successful OpSec audit. These guidelines exist to ensure the following:

1. The test was conducted **legally**.
2. The test included all necessary controls.
3. The posture for the test complied with the test.
4. The results are accurate.
5. The results are consistent and repeatable.
6. The results contain only facts as derived from the tests themselves.

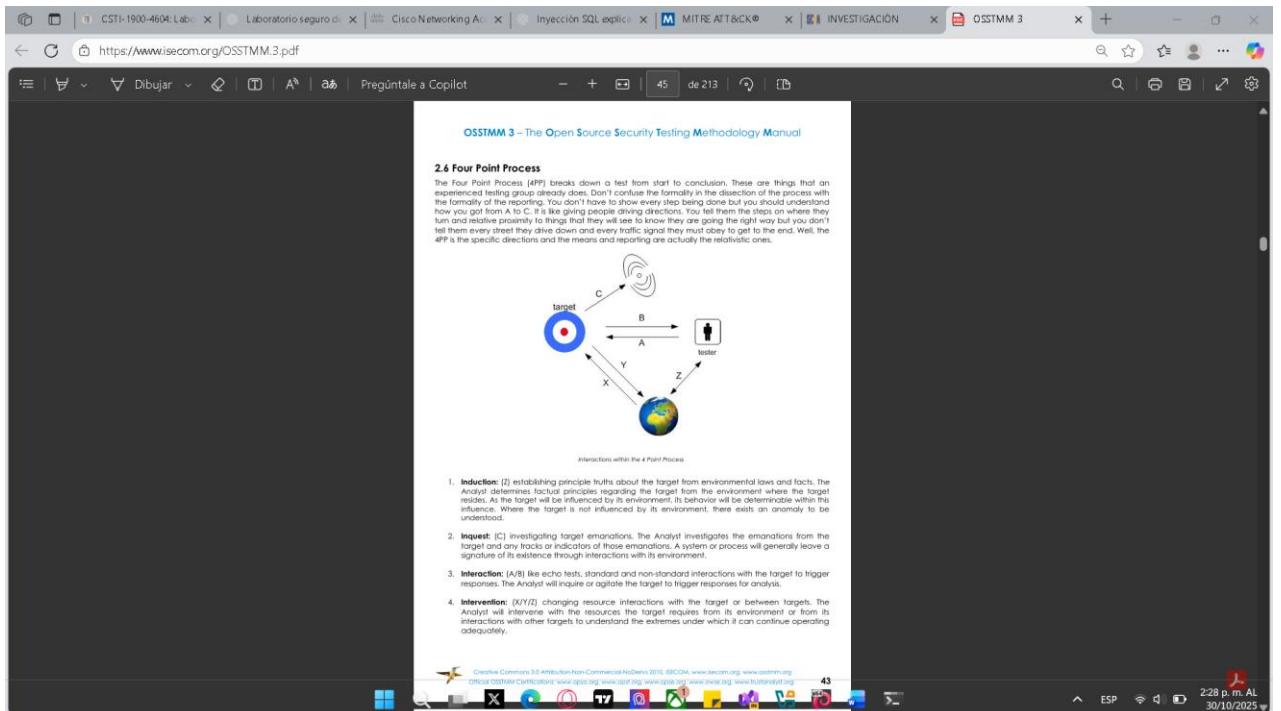
An indirect benefit of this manual is that it can act as a central reference in all security tests regardless of the size of the organization, technology, or protection.

Document Scope
The scope of this document is to provide specific descriptions for operational security tests over all operational channels, which include Human, Physical, Wireless, Telecommunications, and Data Networks, over any vector, and the description of derived metrics. This manual only focuses on OpSec and the use of the world's safety and security are within this context.

Liability
This manual describes certain tests which are designed to elicit a response. Should these tests cause harm or damage, the Analyst may be held responsible according to the laws governing that Analyst's location, as well as the laws of the target organization. ISCOM makes no claims as to the outcomes of any test. Any Analyst applying this methodology cannot hold ISCOM liable for problems which arise during testing. In using the methodology, the Analyst agrees to assume this liability.

Creative Commons 3.0 Attribution Non-Commercial NoDerivs 2018. ISCOM. www.iscom.org. www.osstmm.org
Creative Commons Certifications: www.opsec.org. www.osstmm.org. www.oewa.org. www.hackersafe.org

¿Cuáles son los diez pasos para aplicar OSSTM cuando se combinan el proceso de 4 puntos y Trifecta?



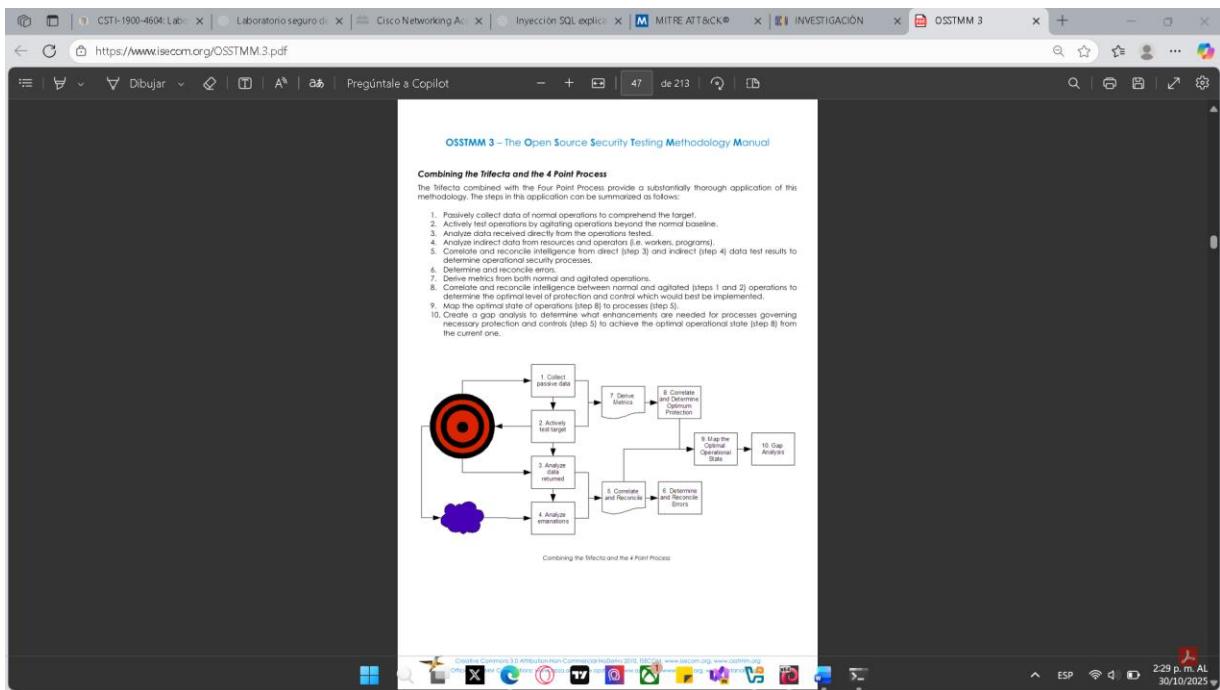
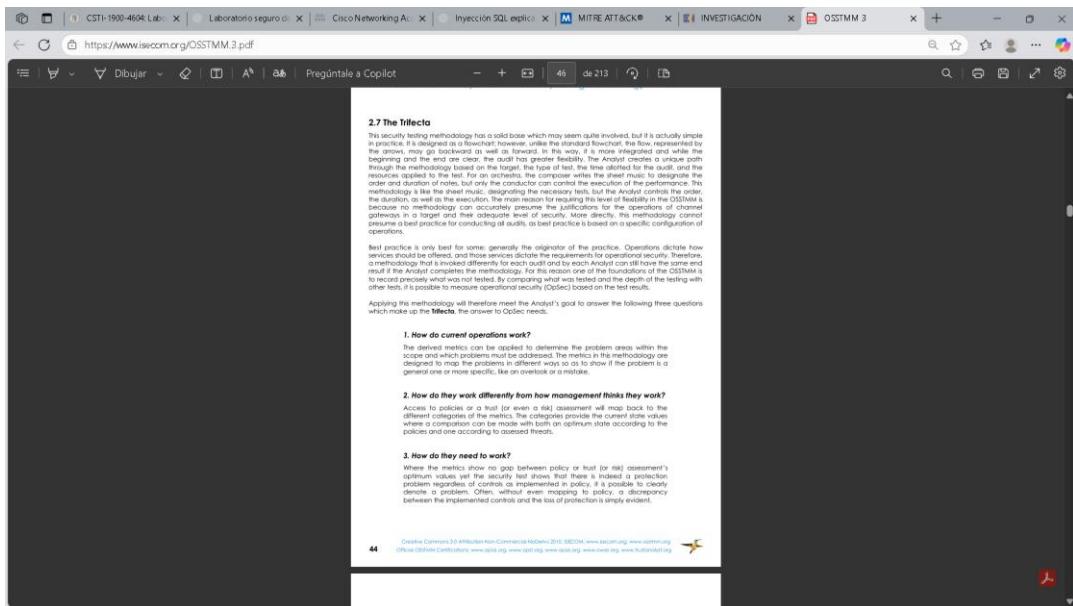
2.6 Four Point Process
The Four Point Process (4PP) breaks down a test from start to conclusion. These are things that an experienced tester grows to know very quickly. Don't include the terminology in the discussion of the process with the formula for the reporting. You don't have to show every step being done but you should understand how you got from A to C. It is like giving people driving directions. You tell them the steps on where they should go and probably tell them that there are going to be some stops along the way but you don't tell them every street they drive down and every traffic signal they must obey to get to the end. Well, the 4PP is the specific directions and the means and reporting are actually the non-specific ones.

Interactions within the 4 Point Process:

1. **Induction:** [I] establishing principle truths about the target from environmental laws and facts. The Analyst determines factual principles regarding the target from the environment where the target resides. The target will be influenced by its environment; its behavior will be determinable within this influence. Where the target is not influenced by its environment, there exists an anomaly to be understood.
2. **Inquest:** [C] investigating target behavior, the Analyst investigates the emanations from the target and any track or signature of those emanations. A system or process will generally leave a signature or evidence through interactions with its environment.
3. **Interaction:** [A/B] echo tests, standard and non-standard interactions with the target to trigger responses. The Analyst will induce or agitate the target to observe responses for analysis.
4. **Intervention:** [X/Y/Z] changing resource interactions with the target or between targets. The Analyst will intervene with the resources the target requires from its environment or from its interactions with other targets to understand the extremes under which it can continue operating adequately.

Creative Commons 3.0 Attribution Non-Commercial NoDerivs 2018. ISCOM. www.iscom.org. www.osstmm.org
Creative Commons Certifications: www.opsec.org. www.osstmm.org. www.oewa.org. www.hackersafe.org

Práctica de laboratorio: Comparación de metodologías de pruebas de penetración



Paso 2: Recopile información sobre PTES.

El Estándar de ejecución de pruebas de penetración es una guía completa para el proceso de realización de pruebas de penetración.

Vaya a www.pentest-standard.org.

¿Cuál es la última versión del estándar?

Práctica de laboratorio: Comparación de metodologías de pruebas de penetración

The screenshot shows a web browser window with the URL www.pentest-standard.org/index.php/Main_Page. The page title is "Portada". The main content area discusses the "Organización de alto nivel de la norma" (High-level organization of the standard), stating that the standard consists of seven sections. It highlights the transition from a penetration test to intelligence gathering and threat modeling. A sidebar on the left contains links for "Portada", "Directriz técnica de PTES", "En los medios", "Preguntas más frecuentes", "Herramientas", "Lo que enlaza aquí", "Cambios relacionados", "Páginas especiales", "Versión imprimible", "Enlace permanente", and "Información de la página". The right sidebar includes links for "Leer", "Ver código fuente", "Ver historia", and "Buscar el estándar de ejecución de pruebas de p". The bottom of the page features a toolbar with various icons.

¿Cuáles son las siete secciones principales del PTES?

This screenshot is identical to the one above, showing the "Portada" page of the PTES website. It reiterates the seven sections of the standard and the transition from penetration testing to intelligence gathering and threat modeling. The sidebar and footer are also identical, providing links for various sections and search functionality.

¿Cuál es el propósito declarado del PTES? (Pista: consulte las preguntas frecuentes)

Práctica de laboratorio: Comparación de metodologías de pruebas de penetración

The screenshot shows a web browser with multiple tabs open. The active tab displays the 'Preguntas más frecuentes' (FAQ) section of the PTES website. The page title is 'Preguntas más frecuentes'. A sidebar on the left contains links to various sections like 'Portada', 'Documentos técnicos de PTES', 'En los medios', 'Preguntas más frecuentes', 'Herramientas', 'Lo que enlaza aquí', 'Cambios relacionados', 'Páginas especiales', 'Versión imprimible', 'Enlace permanente', and 'Información de la página'. The main content area is titled 'Contenido [ocultar]' and lists '1 Estándar de ejecución de pruebas de penetración: las preguntas frecuentes' with 18 numbered questions. Below this, another section is titled 'Estándar de ejecución de pruebas de penetración: las preguntas frecuentes' with a question about what the standard is.

¿Qué documento especifica las herramientas y técnicas que se utilizarán en las siete secciones de la prueba?

The screenshot shows a web browser with multiple tabs open. The active tab displays the 'Tools_Required' section of the PTES website. The page title is 'Directrices técnicas'. The main content area lists '12.4 E-hausivo', '12.5 Auditoría completa', '12.6 Cumplimiento de HIPAA', '12.7 Auditoría de la DMZ de Internet', '12.8 RFP de Linux', '12.9 Revisión de Microsoft', '12.10 Auditoría de la industria de tarjetas de pago (PCI)', '12.11 Prueba de penetración', '12.12 Prueba de penetración', '12.13 Auditoría de red segura', '12.14 Cumplimiento de Sarbanes-Oxley (SOX)', '12.15 Auditoría SCADA', and '12.16 Auditoría web'. Below this, there are sections for 'Herramientas necesarias' and 'Sistemas operativos'.

Paso 3: Recopile información sobre OWASP WSTG.

OWASP WSTG es una guía para probar la seguridad de las aplicaciones y los servicios web. No es una guía general para las pruebas de penetración. En cambio, se centra en desarrollar, implementar y mantener aplicaciones web seguras.

Vaya a <https://owasp.org/www-project-web-security-testing-guide/>.

¿Cuál es la última versión del estándar WSTG?

Práctica de laboratorio: Comparación de metodologías de pruebas de penetración

The screenshot shows the homepage of the OWASP Web Security Testing Guide (WSTG). The top navigation bar includes links for PROYECTOS, CAPÍTULOS, EVENTOS, ACERCA DE, and a search bar. A sidebar on the right provides information about the OWASP Foundation, its projects (Insignia, Documentation, Complete, Constructor), links to the GitHub repository, and social media links. The main content area discusses the WSTG project, its purpose (to produce a principal resource for web security testing), and its development status (version 5.0). It also covers contributions, stable versions, and how to reference scenarios.

Acceda a la versión estable actual de WSTG. ¿Cuáles son las cinco fases del marco de pruebas de seguridad web?

1 frontispicio

2 introducción

3 marco de prueba de owasp

4 prueba de penetración de aplicaciones wed

5 informe

¿Cuál es el propósito declarado del OWASP WSTG?

The screenshot shows the About OWASP page of the OWASP Top 10:2021 website. The left sidebar lists various sections such as Introduction, How to use the OWASP Top 10 as a standard, How to start an AppSec program with the OWASP Top 10, About OWASP, Top 10:2021 List, A01 Broken Access Control, A02 Cryptographic Failures, A03 Injection, A04 Insecure Design, A05 Security Misconfiguration, A06 Vulnerable and Outdated Components, A07 Identification and Authentication Failures, A08 Software and Data Integrity Failures, A09 Security Logging and Monitoring Failures, A10 Server Side Request Forgery (SSRF), and Next Steps. The main content area discusses the project's mission to provide free resources for application security, its history, and its impact. It also mentions the OWASP community and its various initiatives.

Práctica de laboratorio: Comparación de metodologías de pruebas de penetración

¿Cuáles son las doce categorías de pruebas activas definidas en el marco de pruebas web de OWASP?

The screenshot shows a web browser with multiple tabs open. The active tab displays a document titled 'Práctica 2: Métodos de Pentesting en Ingeniería de Sistemas 2023I226'. The document lists the twelve active testing categories defined in the OWASP Web Testing Framework:

- Control de acceso: Pruebas para verificar la efectividad de los mecanismos de control de acceso, como la autenticación y la autorización.
- Código: Pruebas para evaluar la configuración y la efectividad de los mecanismos de código utilizado para proteger la comunicación y los datos sensibles.
- Autenticación: Pruebas para evaluar la fortaleza de los mecanismos de autenticación utilizados para verificar la identidad de los usuarios.
- Sesiones: Pruebas para verificar la efectividad de los mecanismos de gestión de sesiones, como la generación y gestión de tokens de sesión.
- Autorización: Pruebas para evaluar la correcta implementación de los controles de autorización para proteger recursos y funcionalidades sensibles.
- Configuración: Pruebas para identificar y mitigar los riesgos asociados con la configuración incorrecta de los sistemas y aplicaciones web.
- Datos sensibles: Pruebas para identificar y proteger los datos sensibles almacenados, transmitidos o procesados por la aplicación web.
- APIs: Pruebas para evaluar la seguridad de las APIs (Interfaces de Programación de Aplicaciones) utilizadas por la aplicación web.
- Seguridad en el cliente: Pruebas para evaluar la seguridad en el lado del cliente, incluyendo el uso de tecnologías como JavaScript y HTML5.
- Errores de configuración: Pruebas para identificar y mitigar los errores de configuración que podrían ser explotados por un atacante.
- Filtros y Firewall: Pruebas para evaluar la efectividad de los filtros y firewalls utilizados para proteger la aplicación web.
- Log y monitoreo: Pruebas para verificar la adecuada generación, almacenamiento y monitorización de logs de seguridad.

Paso 4: Recopile información sobre MITRE ATT & CK.

MITRE ATT & CK es una base de conocimiento detallada de tácticas, técnicas y procedimientos de atacantes (TTP) que se han recopilado de ataques reales. No es un manual o estándar sobre cómo realizar pruebas de penetración. Sin embargo, los probadores de penetración pueden usarlo para obtener ideas y orientación sobre cómo aprovechar las vulnerabilidades como parte de una prueba.

- Vaya al sitio web <https://attack.mitre.org>.

¿Cuál es la última versión del estándar ATT & CK?

The screenshot shows the MITRE ATT&CK website. The main navigation bar includes links for Matrices, Tácticas, Técnicas, Defensas, CTI, Recursos, Benefactores, and Blog. The current page is 'Historial de versiones'. A sidebar on the left provides links to 'RECURSOS', 'Comenzar', 'Más información sobre ATT&CK', 'ATT&CKcon', 'Datos y herramientas de ATT&CK', 'Preguntas más frecuentes', 'Interactúa con ATT&CK', 'Historial de versiones' (which is highlighted), 'Actualizaciones', and 'Legal y Branding'. The main content area displays the 'Historial de versiones' section, which states: '¡ATT&CK v18 ha sido lanzado! Consulte la publicación del blog o el registro de cambios para obtener más información.' Below this, the 'Versión actual' section shows 'ATT&CK v18.0' (28 DE OCTUBRE DE 2025 - ACTUAL) with 'Notas' and 'Sitio web v18.0' buttons. The 'Versiones más recientes' section shows 'ATT&CK v17.1' (22 DE ABRIL DE 2025 - 27 DE OCTUBRE DE 2025) and 'ATT&CK v16.1' (31 DE OCTUBRE DE 2024 - 21 DE ABRIL DE 2025), each with 'Notas' and 'Sitio web' buttons.

Práctica de laboratorio: Comparación de metodologías de pruebas de penetración

¿Por qué MITRE desarrolló ATT & CK? (**Pista:** consulte las preguntas frecuentes)

The screenshot shows the MITRE ATT&CK website. In the top navigation bar, there is a link labeled 'PREGUNTAS FRE'. On the left sidebar, under the 'RECURSOS' section, there is a 'Preguntas más frecuentes' (FAQ) link. The main content area displays several frequently asked questions, such as '¿Qué es ATT&CK?' and '¿Por qué MITRE desarrolló ATT&CK?'. A sidebar on the right provides links to other sections like 'General', 'Contenido', and 'Recursos'.

- En el menú de la página, haga clic en **Recursos > Información general > Diseño y filosofía de ATT & CK**.
- Abra y revise el pdf de Diseño y filosofía de ATT & CK.

¿Qué seis casos de uso comunes para ATT & CK se describen?

The screenshot shows a Microsoft Word document titled 'Microsoft Word - ATTACKDesign_and_Philosophy_March_2020.pdf'. The document is a scanned version of a PDF, specifically the '2 ATTACK Use Cases' section. It contains several paragraphs of text describing different use cases, such as 'Attacker's Objective', 'Red Team', 'Defender's Objective', 'Blue Team', and 'Defender's Countermeasures'. The text is in Spanish.

¿Cuáles son los tres dominios tecnológicos de ATT y CK?

Práctica de laboratorio: Comparación de metodologías de pruebas de penetración

The screenshot shows a Microsoft Edge browser window with several tabs open. The active tab displays the MITRE ATT&CK matrix for the Enterprise environment. The page is divided into sections: 3.2 Technology Domains, 3.3 Tactics, and 3.4 Techniques and Sub-Techniques. The Tactics section includes a table mapping tactics to technologies like Linux, macOS, Windows, AWS, Azure, GCP, Intel, Office 365, and Solaris. The Techniques section provides detailed descriptions of various tactics such as Reconnaissance, Persistence, and Lateral Movement.

- d. Vaya a la matriz empresarial de MITRE ATT & CK abriendo el menú **Matrices** y seleccionando **Enterprise**.
- e. La matriz representa las tácticas como encabezados de columna con las técnicas organizadas como entradas en cada columna. Para obtener información sobre una técnica determinada, haga clic en su entrada. Se muestra información adicional en la página de información. La página de información puede incluir sub-técnicas, procedimientos, mitigaciones, métodos de detección y referencias. No todas las técnicas incluyen procedimientos.

En la columna de la táctica de **reconocimiento**, haga clic en la entrada **Recopilar información de identidad de la víctima**.

Revise la información

¿Cuáles son las tres sub-técnicas que se proporcionan para esta técnica?aquí.

The screenshot shows the MITRE ATT&CK website with the 'Recolectar información del anfitrión de la víctima' technique selected. The page is organized into sections: Ejemplos de procedimientos, Mitigaciones, Estrategia de detección, and Referencias. The 'Ejemplos de procedimientos' section lists 'G1017' (Tifón Volt) as an example. The 'Mitigaciones' section lists 'M1056' (Compromiso previo). The 'Estrategia de detección' section lists 'DET0826' (Detección de recolectar información del anfitrión de la víctima). Each section contains a detailed description of the technique and its impact.

- f. Seleccione la sub-técnica de Direcciones de correo electrónico. Revise la información

Mire las entradas en Procedimientos.

¿Quién es el grupo Lazarus? Realizaron una campaña para recopilar direcciones de correo electrónico para ataques posteriores. ¿Cómo recopilaron y utilizaron las direcciones de correo electrónico?

The screenshot shows the MITRE ATT&CK website with the URL <https://attack.mitre.org/techniques/T1589/002/>. The main content is titled "Reúna información sobre la identidad de la víctima: Direcciones de correo electrónico". It includes a sidebar with a tree view of techniques under "EMPRESA" and "RECONOCIMIENTO". The main content area provides a detailed description of the technique, mentioning how adversaries can gather email addresses from various sources like company websites, social networks, and Office 365. It also lists examples such as "AADInternales" and "APT32". The right sidebar contains metadata: IDENTIFICACIÓN: T1589.002, Subtécnica de: T1589, Tácticas: Reconocimiento, Plataformas: PRE, Colaboradores: Jannie Li, Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Versión: 1.3, Creado: 02 Octubre 2020, Última modificación: 24 de octubre de 2025, and a link to "Versión Permalink".

Quién es Lazarus Group: aparece como un actor/grupo (G0032) listado en ATT&CK; es un grupo de amenazas conocido por campañas de ciberespionaje y operaciones avanzadas (véase la referencia incluida en la entrada de MITRE).

Cómo recopilaron y usaron direcciones de correo: MITRE documenta que **Lazarus Group recopiló direcciones de correo pertenecientes a varios departamentos de la organización objetivo y las empleó en campañas de spear-phishing y phishing de seguimiento (follow-on phishing)** para conseguir acceso inicial o compromiso posterior. (ATT&CK incluye como ejemplo la referencia a un informe sobre la campaña ThreatNeedle / actividades de Lazarus).

Preguntas de reflexión

1. ¿Por qué es importante seguir una metodología de pruebas de penetración reconocida?

Seguir una metodología reconocida (por ejemplo, basada en ATT&CK, OSSTMM, PTES o similares) es importante porque:

Consistencia y cobertura: asegura que las pruebas sean sistemáticas y que no se pasen por alto fases clave del ataque (reconocimiento, acceso inicial, movimiento lateral, exfiltración, etc.).

Reproducibilidad y trazabilidad: un proceso estandarizado facilita repetir pruebas, comparar resultados en el tiempo y documentar evidencia.

Legalidad y ética: reduce riesgos legales/operativos al aplicar límites, autorizaciones y procedimientos definidos.

Medición y priorización: permite mapear hallazgos contra un marco (por ejemplo, ATT&CK) para priorizar mitigaciones según riesgo/impacto y comunicar resultados con lenguaje comprensible para defensores y gerencia.

Mejor comunicación: un lenguaje común (TTPs mapeadas) facilita que equipos de SOC, CTI, ingeniería y gestión entiendan y actúen sobre los hallazgos.