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

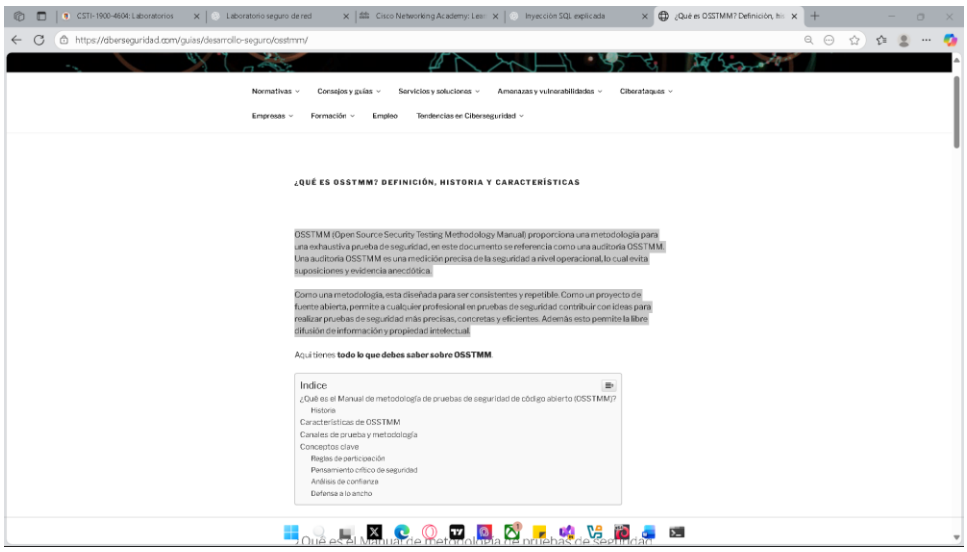
- Computadora personal o dispositivo móvil con acceso a internet

Instrucciones

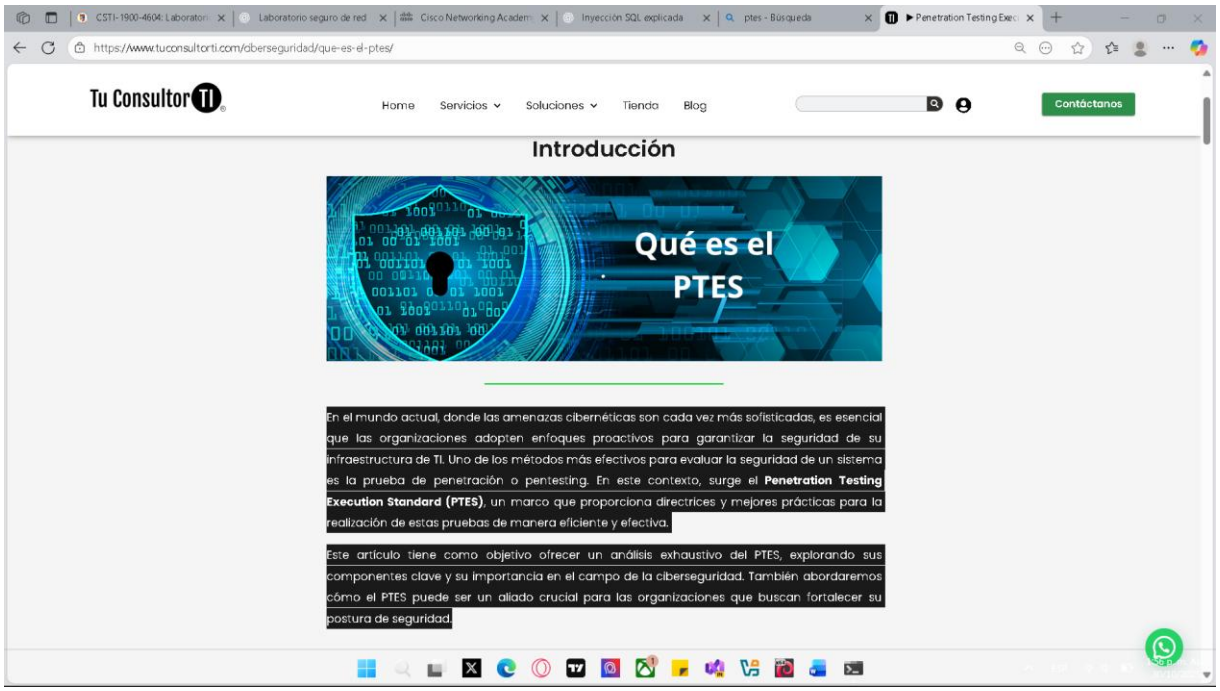
Parte 1: Realizar investigación de metodologías populares de pruebas de penetración

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

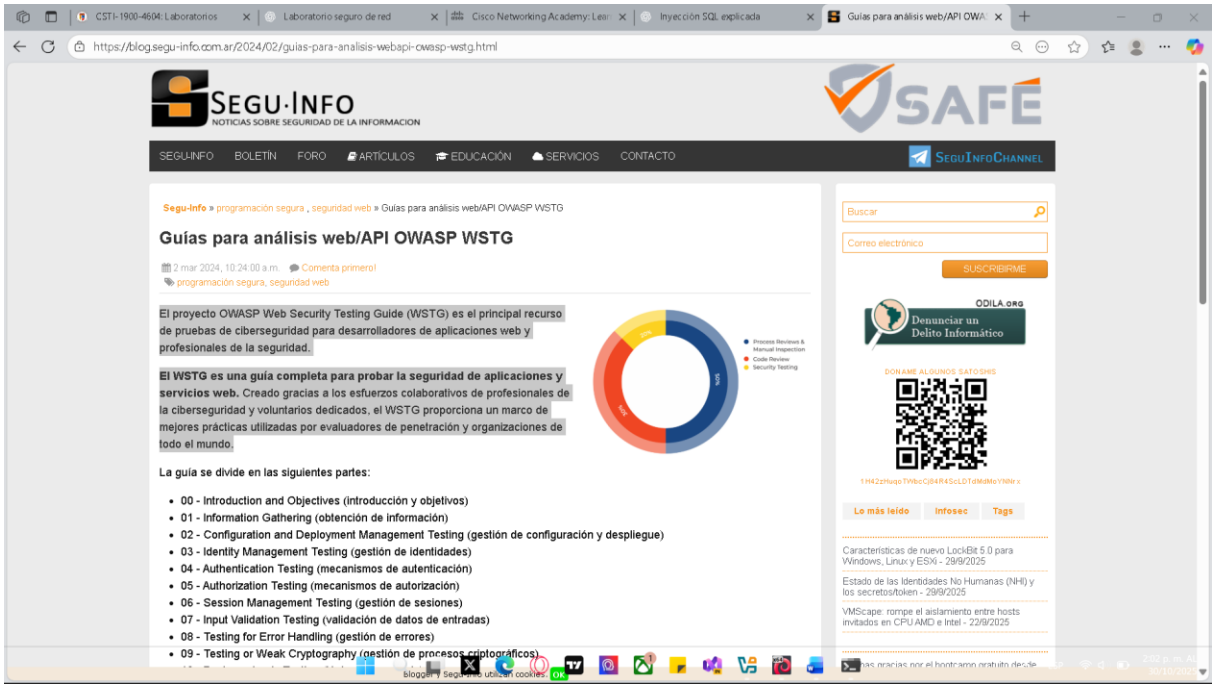
- OSSTMM



- PTES



- OWASP WSTG



- MITRE ATT Y CK

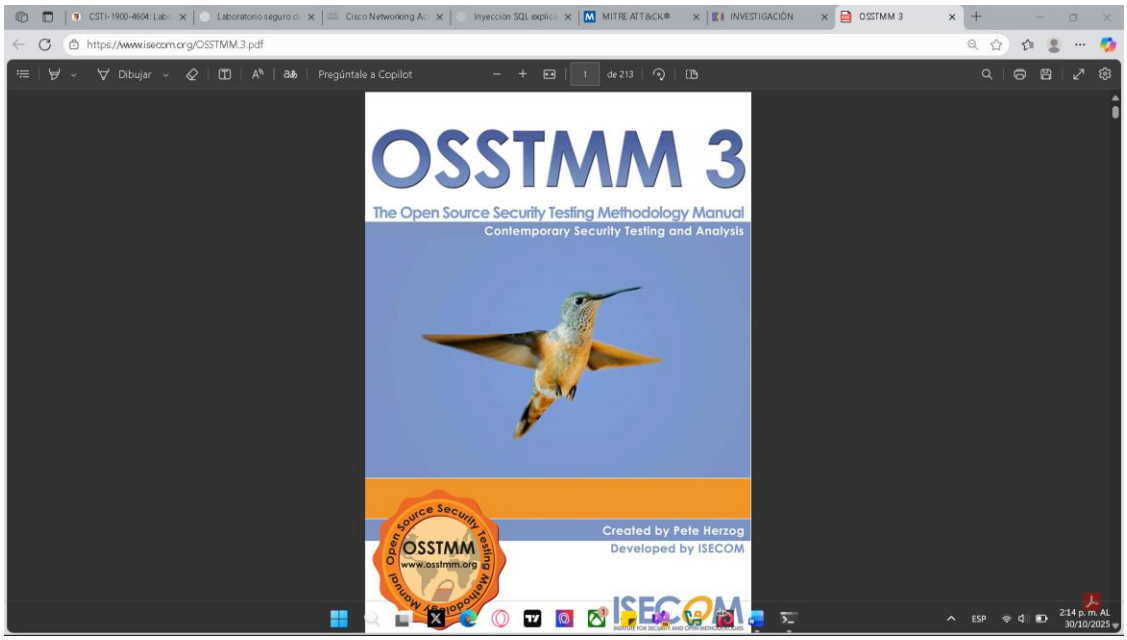
Paso 1: Recopile información sobre OSSTMM.

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.

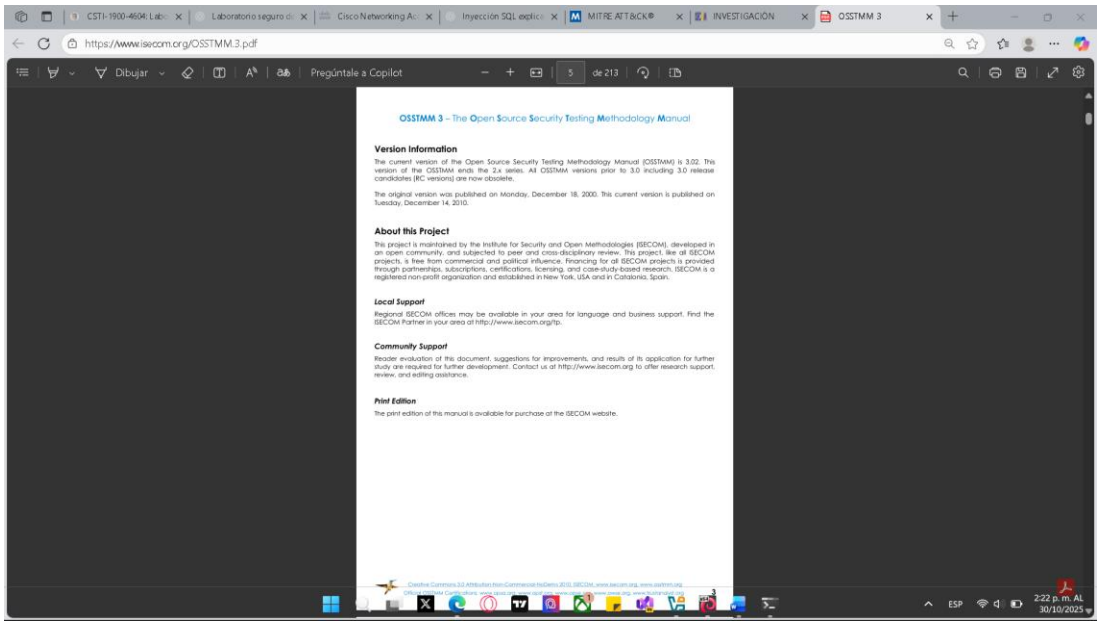
a. Navegue a https://www.isecom.org, haga clic en **RESEARCH** > **OSSTMM**.

b. 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?

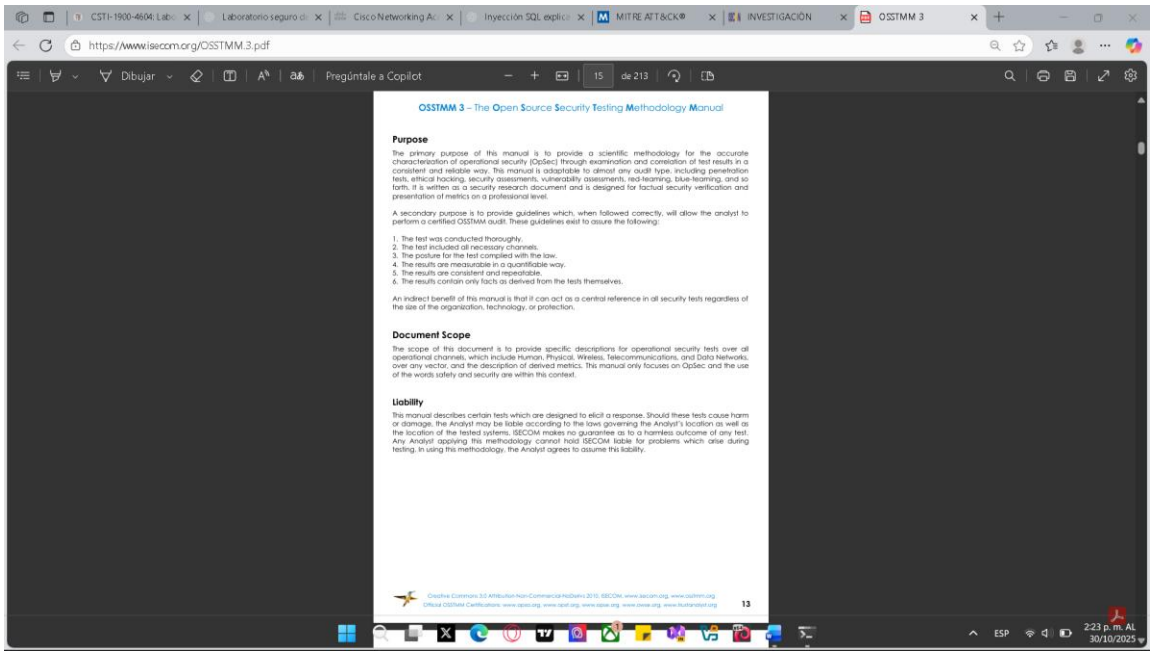


¿Qué organización desarrolla el OSSTMM? ¿Cómo se desempeñan?

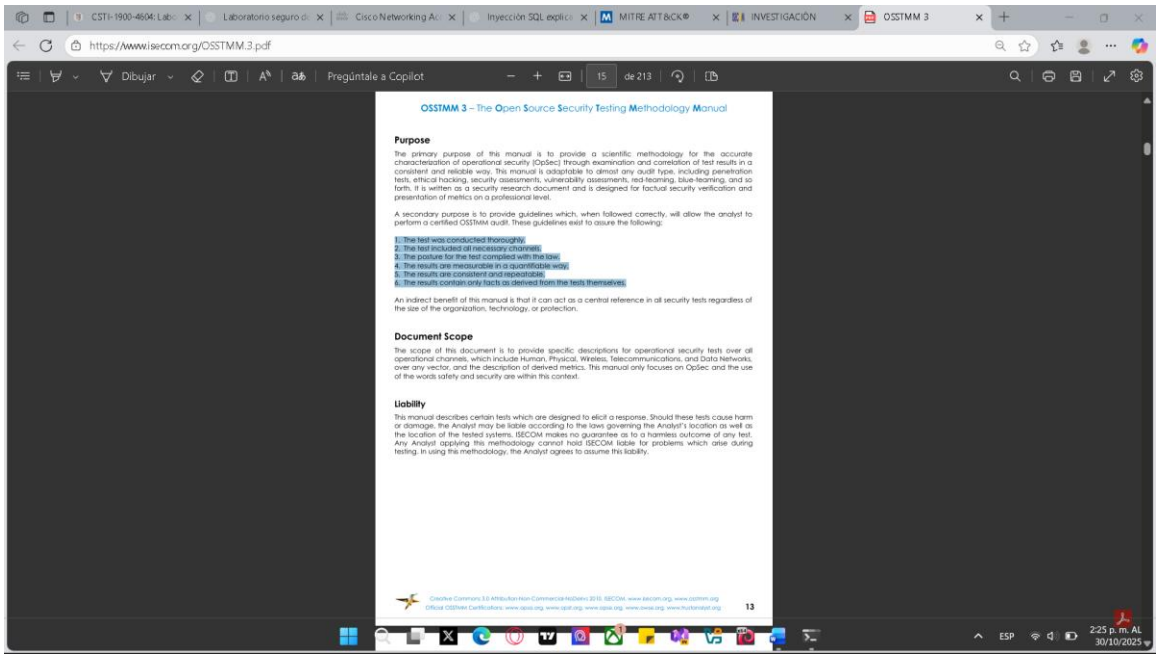


Instituto de Seguridad y Metodologías Abiertas. Las respuestas pueden variar. Publican certificaciones de seguridad, publican libros y realizan investigaciones. Publican un currículo de concientización sobre la seguridad para adolescentes y realizan otras actividades.

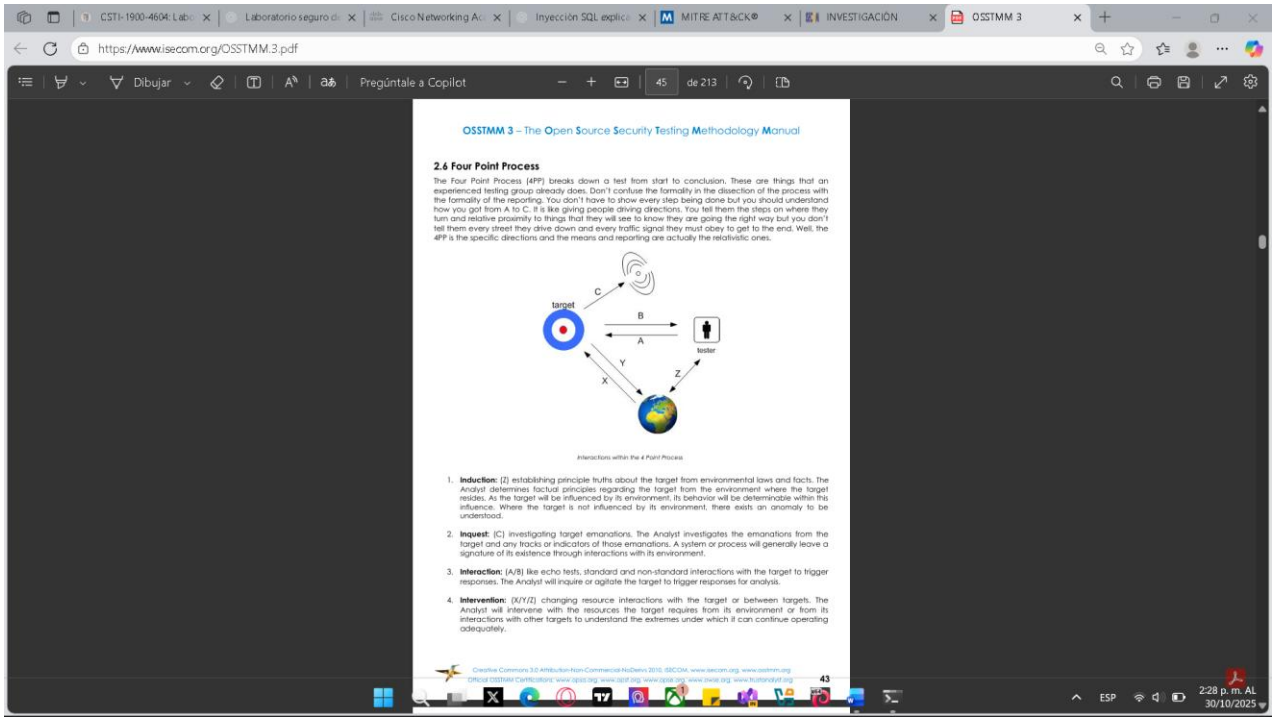
¿Cuáles son los propósitos primarios y secundarios declarados del OSSTMM, como se indica en la publicación de OSSTMM?

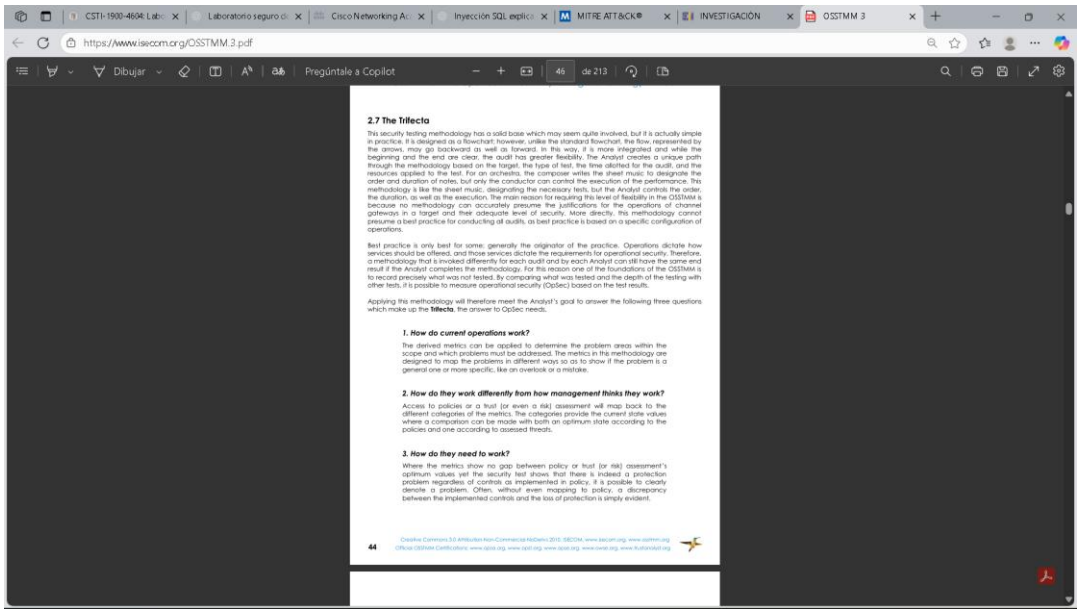


¿Qué seis resultados se garantizan, entonces, se siguen correctamente las pautas de OSSTM?



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





2.7 The Trifecta

This security testing methodology has a solid base which may seem quite involved, but it is actually simple in practice. It is designed as a flowchart; however, unlike the standard flowchart, the flow, represented by the arrows, may go backward as well as forward. In this way, it is more integrated and while the beginning and the end are clear, the audit has greater flexibility. The Analyst creates a unique path through the methodology based on the target, the type of test, the time allotted for the audit, and the resources applied to the test. For an orchestra, the composer writes the sheet music to designate the order and duration of notes, but only the conductor can control the execution of the performance. This methodology is like the sheet music, designating the necessary tests, but the Analyst controls the order, the duration, as well as the execution. The main reason for requiring this level of flexibility in the OSSTMM is because no methodology can accurately presume the justifications for the operations of channel gateways in a target and their adequate level of security. More directly, this methodology cannot presume a best practice for conducting all audits, as best practice is based on a specific configuration of operations.

Best practice is only best for some; generally the originator of the practice. Operations dictate how services should be offered, and those services dictate the requirements for operational security. Therefore, a methodology that is invoked differently for each audit and by each Analyst can still have the same end result if the Analyst completes the methodology. For this reason one of the foundations of the OSSTMM is to record precisely what was not tested. By comparing what was tested and the depth of the testing with other tests, it is possible to measure operational security (OpSec) based on the test results.

Applying this methodology will therefore meet the Analyst's goal to answer the following three questions which make up the **trifecta**, the answer to OpSec needs.

1. How do current operations work?

The derived metrics can be applied to determine the problem areas within the scope and which problems must be addressed. The metrics in this methodology are designed to map the problems in different ways so as to show if the problem is a general one or more specific, like an overlook or a mistake.

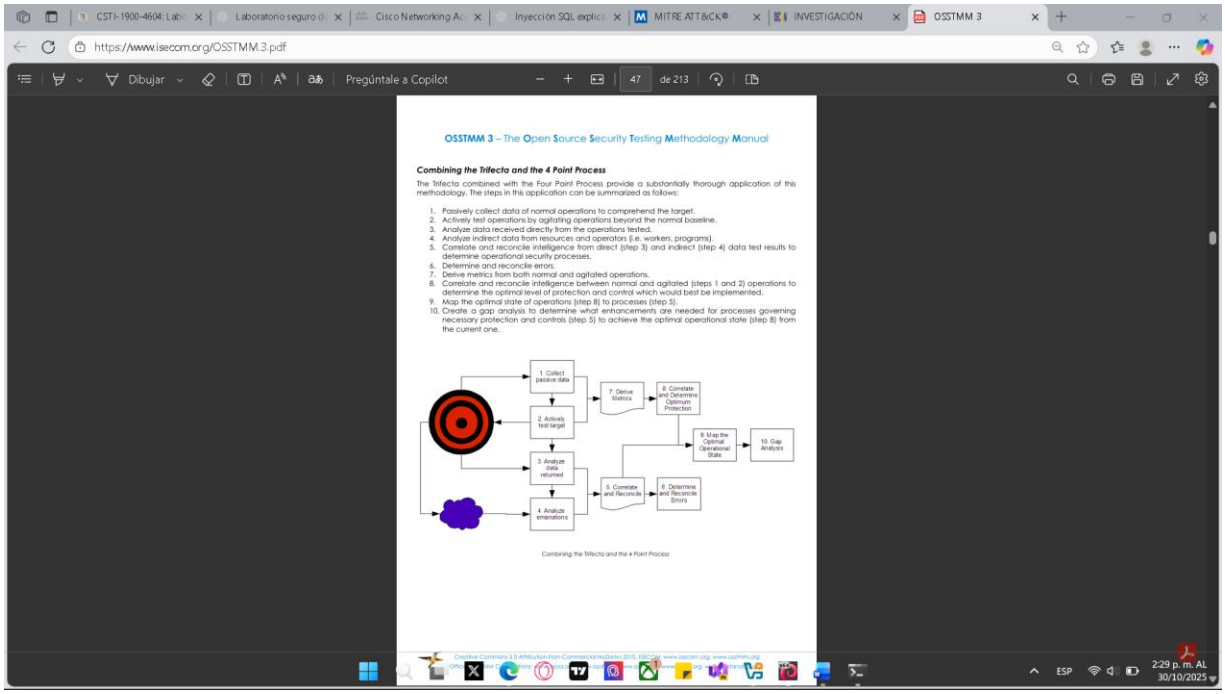
2. How do they work differently from how management thinks they work?

Access to policies or a trust (or even a risk) assessment will map back to the different categories of the metrics. The categories provide the current state values where a comparison can be made with both an optimum state according to the policies and one according to assessed threats.

3. How do they need to work?

Where the metrics show no gap between policy or trust (or risk) assessment's optimum values yet the security test shows that there is indeed a protection problem regardless of controls as implemented in policy, it is possible to clearly denote a problem. Often, without even mapping to policy, a discrepancy between the implemented controls and the loss of protection is simply evident.

44



OSSTMM 3 – The Open Source Security Testing Methodology Manual

Combining the Trifecta and the 4 Point Process

The Trifecta combined with the Four Point Process provide a substantially thorough application of this methodology. The steps in this application can be summarized as follows:

1. Passively collect data of normal operations to comprehend the target.
2. Actively test operations by agitating operations beyond the normal baseline.
3. Analyze data received directly from the operations tested.
4. Analyze indirect data from resources and operators (i.e. workers, programs).
5. Correlate and reconcile intelligence from direct (step 3) and indirect (step 4) data test results to determine operational security processes.
6. Determine and reconcile errors.
7. Derive metrics from both normal and agitated operations.
8. Correlate and reconcile intelligence between normal and agitated (steps 1 and 2) operations to determine the optimal level of protection and control which would best be implemented.
9. Map the optimal state of operations (step 8) to processes (step 5).
10. Create a gap analysis to determine what enhancements are needed for processes governing necessary protection and controls (step 5) to achieve the optimal operational state (step 8) from the current one.

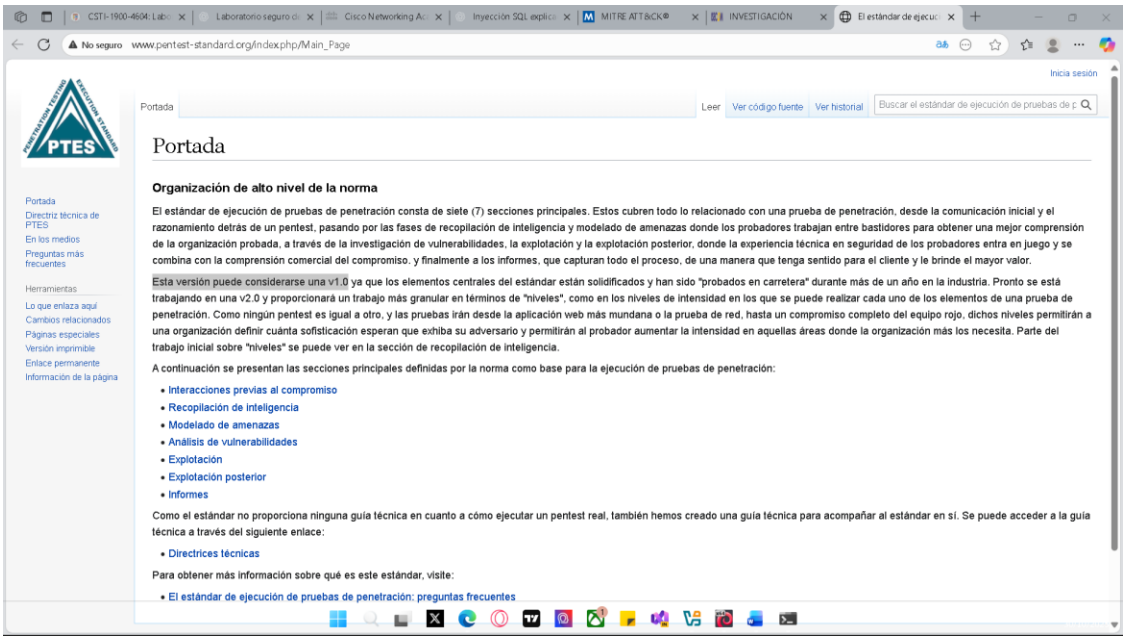
Combining the Trifecta and the 4 Point Process

Paso 2: Recopile información sobre PTES.

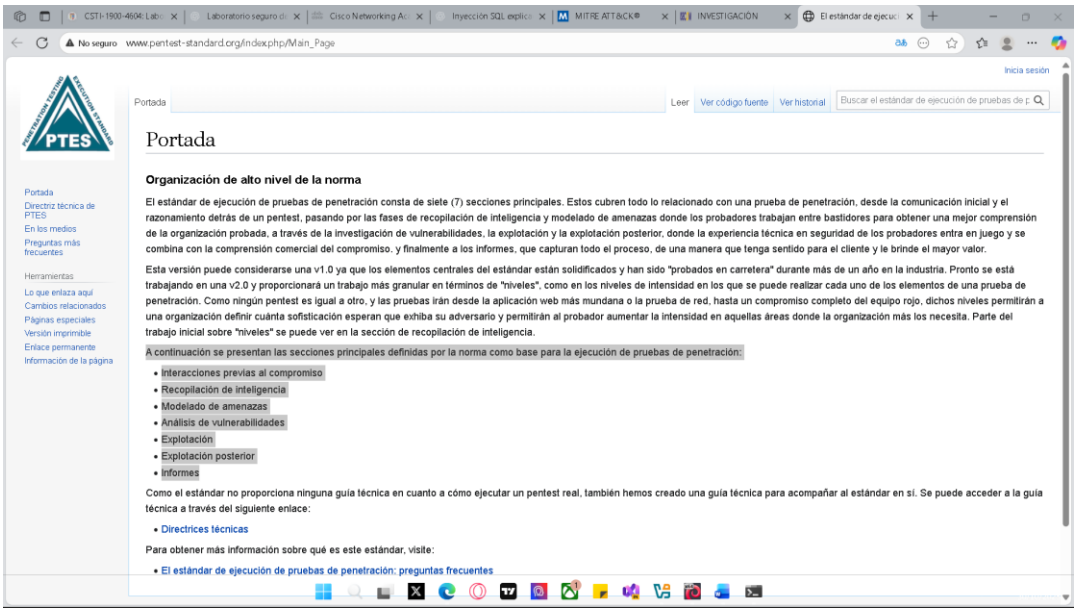
El Estándar de ejecución de pruebas de penetración es una guía completa para el proceso de realización de pruebas de penetración.

Vaya a www.pentest-standard.org.

¿Cuál es la última versión del estándar?

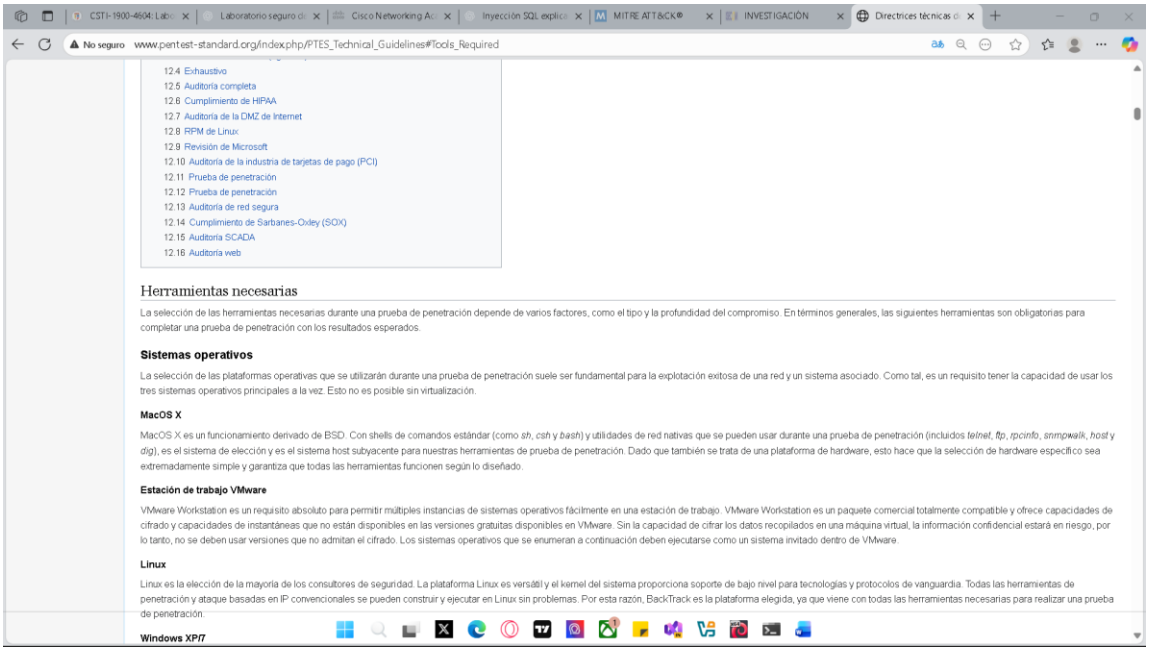


¿Cuáles son las siete secciones principales del PTES?



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

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

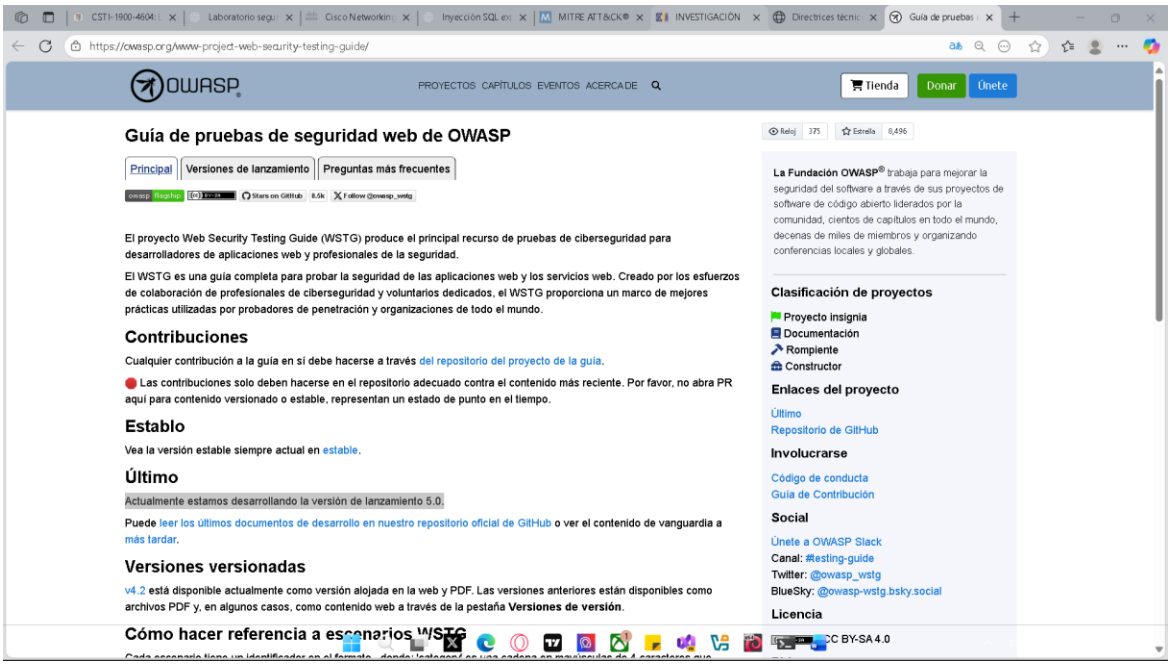


Paso 3: Recopile información sobre OWASP WSTG.

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?



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

1 frontispicio

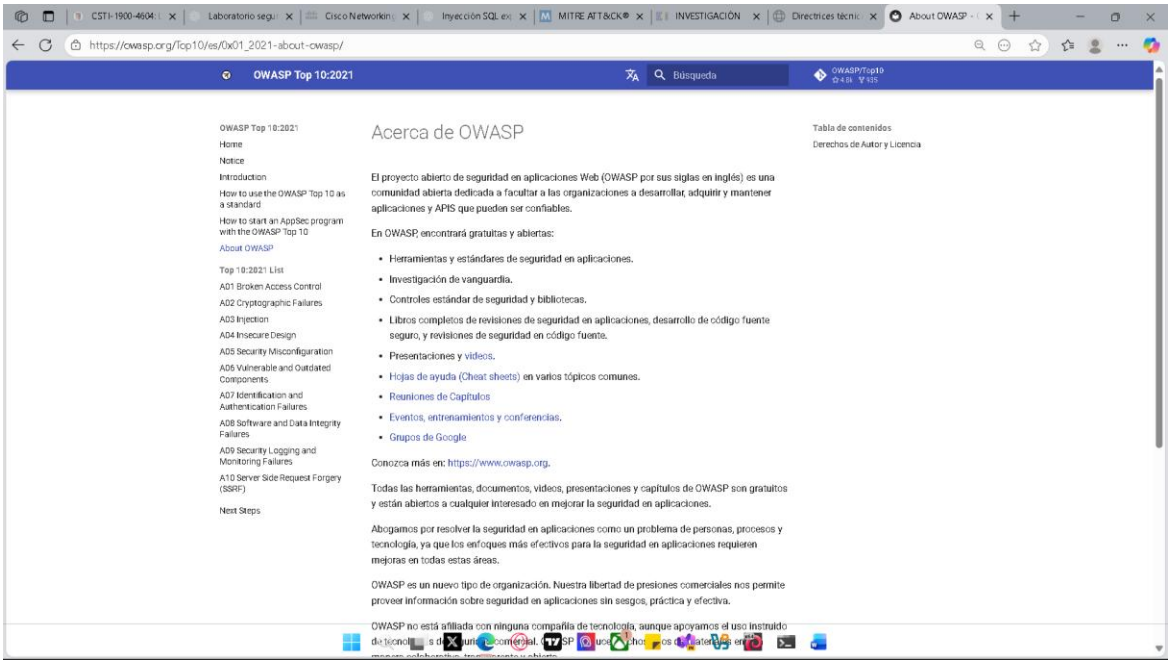
2 introducción

3 marco de prueba de owasp

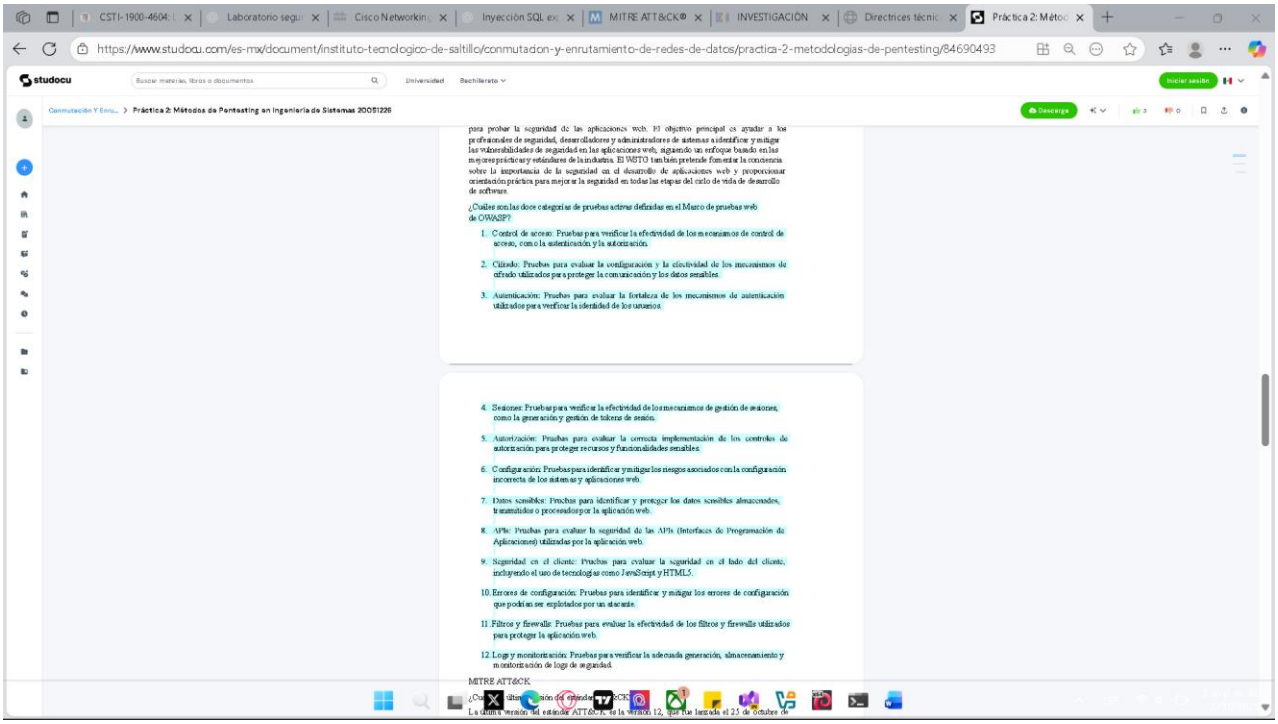
4 prueba de penetración de aplicaciones wed

5 informe

¿Cuál es el propósito declarado del OWASP WSTG?



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

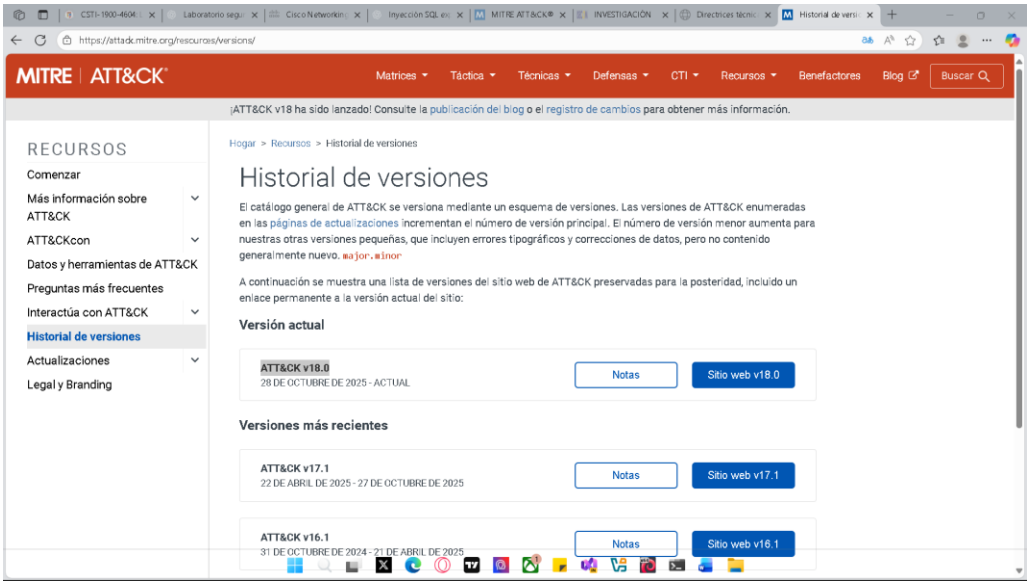


Paso 4: Recopile información sobre MITRE ATT & CK.

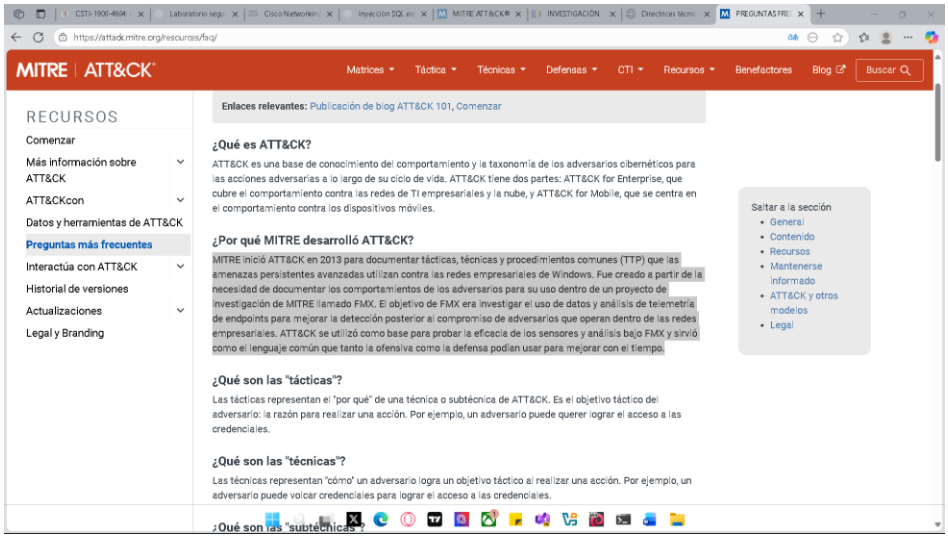
MITRE ATT & CK es una base de conocimiento detallada de tácticas, técnicas y procedimientos de atacantes (TTP) que se han recopilado de ataques reales. No es un manual o estándar sobre cómo realizar pruebas de penetración. Sin embargo, los probadores de penetración pueden usarlo para obtener ideas y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

a. Vaya al sitio web https://attack.mitre.org.

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



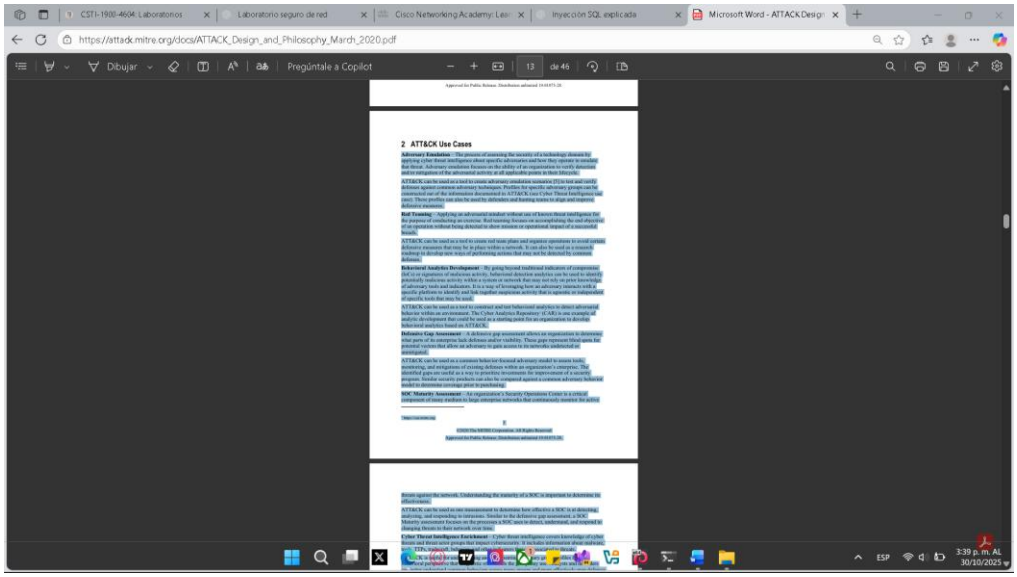
¿Por qué MITRE desarrolló ATT & CK? (**Pista**: consulte las preguntas frecuentes)



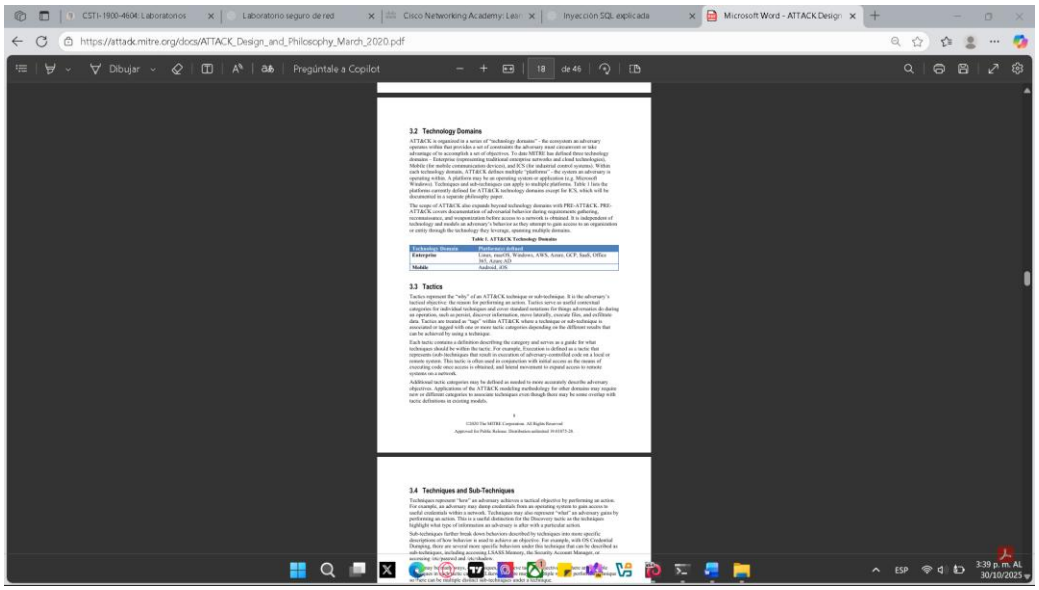
b. En el menú de la página, haga clic en **Recursos** > **Información general** > **Diseño y filosofía de ATT & CK**.

c. Abra y revise el pdf de Diseño y filosofía de ATT & CK.

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



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



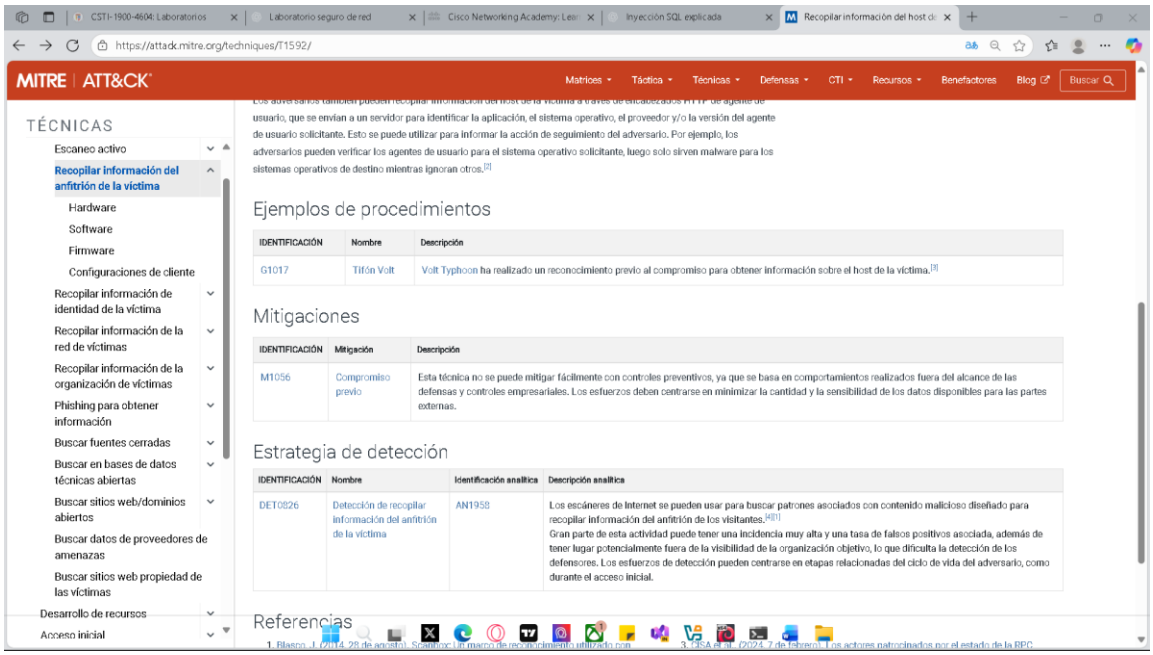
d. Vaya a la matriz empresarial de MITRE ATT & CK abriendo el menú **Matrices** y seleccionando **Enterprise**.

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.



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?

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.