Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Una Mirada a Metodologías Para Pruebas de Penetración en Ciberseguridad

VIEM
Vicerrectoría de Innovación y Emprendimiento

ECBTI
Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación
Ceros y Unos

Boletín de Ciberseguridad

Medio de Divulgación del Centro de Respuestas a Incidentes Informáticos: CSIRT Académico UNAD

E-boletín Informativo CSIRT Académico UNAD

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número Veintiocho
Octubre de 2024

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CSIRT Académico UNAD

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas - Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo – Decano

Especialización en Seguridad Informática (ECBTI)
Ing. Sonia Ximena Moreno Molano – Líder Programa de Especialización en Seguridad Informática

Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign

Centro de Respuestas a Incidentes Informáticos CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Líder CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernandez

Revisó
Ing. Néstor Raúl Cárdenas Corral
Analista CSIRT Académico UNAD

Estado legal:
Periodicidad: Mensual
ISSN: 2806-0164

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Tabla de Contenido

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín de Ciberseguridad

Boletín informativo Número 28

Octubre 2024

Una Mirada a Metodologías Para Pruebas de Penetración en Ciberseguridad

Autores:

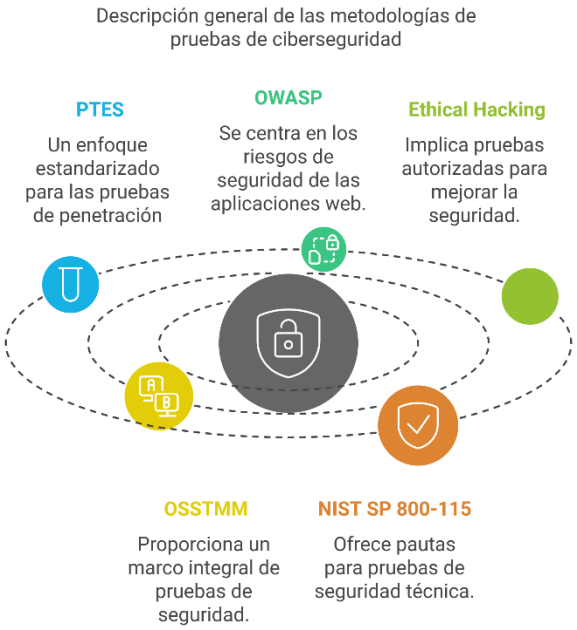
Daniel Felipe Palomo Luna
Docente Esp. Seguridad Informática
https://orcid.org/0009-0004-9507-4295

Luis Fernando Zambrano Hernández
CSIRT Académico UNAD
https://orcid.org/0000-0002-4690-3526

Sonia Ximena Moreno Molano
Líder Maestría en Ciberseguridad
https://orcid.org/0009-0002-6133-5157

Hernando José Peña Hidalgo
CSIRT Académico UNAD
https://orcid.org/0000-0002-3477-2645

Introducción



El En el ámbito de la ciberseguridad, las pruebas de penetración se han convertido en una herramienta esencial para identificar vulnerabilidades y evaluar la seguridad de sistemas y aplicaciones. Este documento ofrece una revisión exhaustiva de diversas metodologías reconocidas para la ejecución de pruebas de penetración, incluyendo el Penetration Testing Execution Standard (PTES), el Open Web Application Security Project (OWASP), las prácticas de hacking ético, el Open Source Security Testing Methodology Manual (OSSTMM) y la NIST Special Publication 800-115.

Cada una de estas metodologías es analizada en detalle, abordando sus fases, áreas de aplicación, ventajas y desventajas, con el propósito de proporcionar una visión integral para los profesionales de la ciberseguridad interesados en optimizar sus estrategias de evaluación y fortalecimiento de la seguridad.

Desarrollo

Una Mirada a las Fases

(PTES, 2022)Penetration Testing Execution Standard (PTES)

Metodología ampliamente utilizada para la realización de pruebas de penetración, proporcionando un marco integral que abarca todas las etapas necesarias para una evaluación de seguridad efectiva. La metodología se estructura en las siguientes fases(PTES, 2022):

Fase Interacción Inicial: Esta fase se enfoca en definir claramente el alcance del proyecto, las actividades a realizar y otros aspectos clave para garantizar el éxito de la prueba de penetración.

Fase Recolección de Datos: Se procede a analizar el objetivo mediante el uso de fuentes de inteligencia de código abierto (OSINT), recopilando datos y caracterizando el entorno objetivo.

Fase Evaluación de Amenazas: Se realiza un análisis del entorno interno y externo para identificar posibles elementos que podrían ser utilizados en ataques contra la organización.

Fase Identificación de Vulnerabilidades: Se llevan a cabo procesos de detección de errores en los sistemas de información que podrían ser explotados por un atacante.

Fase Ejecución de Explotación: En esta etapa, se ponen en práctica técnicas para obtener acceso a los sistemas o recursos, superando las barreras de seguridad.

Fase 6: Persistencia y Movimientos Laterales Esta fase se centra en implementar mecanismos para mantener el acceso conseguido y realizar movimientos laterales dentro del entorno, con el fin de controlar más activos y maximizar el valor del acceso obtenido.

Fase Elaboración del Informe: La fase final consiste en la creación del informe de auditoría, que incluye un análisis detallado de los resultados técnicos y metodológicos obtenidos, así como un resumen ejecutivo.

Áreas de Aplicación

- Aplicaciones web
- Infraestructura de red
- Aplicaciones móviles

Ventajas

- Marco integral que abarca todos los aspectos de las pruebas de penetración.
- Énfasis en la comunicación continua con las partes interesadas durante todo el proceso.

Desventajas

- Puede ser un proceso largo debido a su nivel de detalle.
- Requiere profesionales capacitados para llevarlo a cabo de manera efectiva.

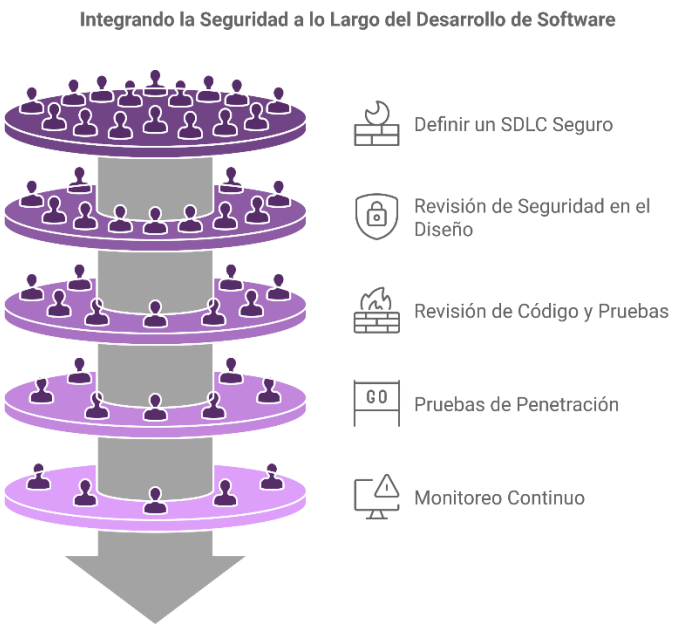
Open Web Application Security Project (OWASP)

Metodología abierta y estandarizada para la evaluación de la seguridad de aplicaciones web. Esta metodología se centra en la identificación, análisis y mitigación de vulnerabilidades en aplicaciones, siguiendo un enfoque estructurado y basado en las mejores prácticas de seguridad. La metodología OWASP se compone de las siguientes fases (OWASP, 2020):

Antes de iniciar el desarrollo: Definir un ciclo de vida de desarrollo de software (SDLC) que incorpore prácticas de seguridad desde el inicio.
Durante la definición y diseño: Revisar los requisitos de seguridad, el diseño y la arquitectura para identificar posibles vulnerabilidades antes de la implementación.
Durante el desarrollo: Realizar revisiones de código y pruebas unitarias para detectar y corregir fallos de seguridad en etapas tempranas.

Durante el despliegue: Llevar a cabo pruebas de penetración y verificar la configuración para asegurar que la aplicación esté protegida en el entorno de producción.

Mantenimiento y operaciones: Implementar revisiones periódicas y monitoreo continuo para identificar y mitigar nuevas amenazas o vulnerabilidades emergentes.



Áreas de Aplicación:

- Pruebas de seguridad para aplicaciones web
- Pruebas de seguridad para APIs

Ventajas:

- Enfocada específicamente en aplicaciones web, lo que la hace muy relevante para los desarrolladores web.
- Ofrece una amplia variedad de recursos y herramientas para los profesionales

Desventajas:

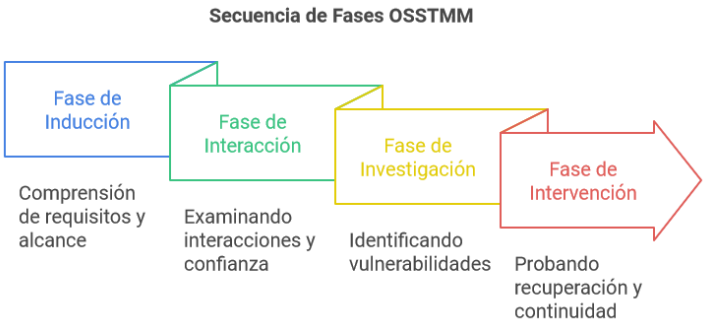
- Principalmente centrada en aplicaciones web, lo que limita su aplicabilidad a otras áreas.
- Puede no cubrir de manera exhaustiva todos los tipos de vulnerabilidades

Open Source Security Testing Methodology Manual (OSSTMM)

Metodología científica y estandarizada para la evaluación de la seguridad operativa en múltiples canales, incluyendo humanos, físicos, inalámbricos, telecomunicaciones y redes de datos. Diseñada por ISECOM, esta metodología proporciona un enfoque sistemático y basado en hechos para la realización de pruebas de seguridad, eliminando suposiciones y sesgos comunes en evaluaciones de riesgo tradicionales. El OSSTMM se centra en medir la efectividad de los controles de seguridad implementados y en cuantificar la exposición a posibles amenazas mediante el uso de métricas como el RAV (Risk Assessment Value) (Herzog, 2010)

Fase de Inducción: Inicia con la comprensión de los requisitos de la auditoría, el alcance y las restricciones aplicables. Se establece la dirección y se determinan los tipos de pruebas que serán más adecuadas.

Fase de Interacción: Se enfoca en las interacciones entre los objetivos y los activos definidos en el alcance. Incluye auditorías de visibilidad, verificación de acceso, y análisis de relaciones de confianza.



Fase de Investigación: Explora en profundidad el entorno para identificar información sensible y analizar procesos, configuraciones y otros elementos que puedan revelar vulnerabilidades.

Fase de Intervención: Realiza pruebas más agresivas para evaluar la capacidad de recuperación y la continuidad del servicio, y verifica el uso adecuado de medidas de contención y revisión de alertas

Áreas de Aplicación

- Seguridad física
- Seguridad de redes

Seguridad inalámbrica

Ventajas

- Ofrece un enfoque integral y estructurado para las pruebas de seguridad.
- Se enfoca en resultados medibles y métricas.

Desventajas

- Puede ser complejo y difícil de implementar para organizaciones más pequeñas.

Requiere un conocimiento profundo de los principios de seguridad.

A diferencia de otras metodologías, el OSSTMM aboga por una separación clara entre seguridad y riesgo, enfocándose en la creación de métricas objetivas y verificables que permitan una evaluación precisa de la superficie de ataque. Esta metodología es utilizada por auditores de seguridad y profesionales de ciberseguridad para realizar auditorías exhaustivas y obtener resultados consistentes y repetibles, lo que la convierte en una herramienta clave para la toma de decisiones estratégicas y operativas en entornos complejos

NIST SP 800-115: Technical Guide to Information Security Testing and Assessment

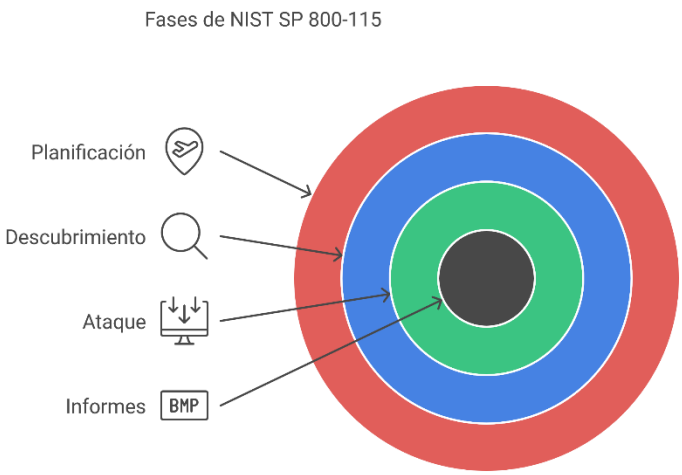
Proporciona un enfoque estructurado para realizar pruebas de penetración con el objetivo de identificar vulnerabilidades en sistemas de información y evaluar la efectividad de las medidas de seguridad implementadas. El proceso está compuesto por cuatro etapas principales («NIST SP 800-115», 2020):

Planificación: Esta etapa inicial implica la preparación y planificación de la prueba de penetración. Se definen los objetivos, el alcance, las reglas de involucramiento, y los métodos a utilizar. Se establece la coordinación con el personal afectado para minimizar los riesgos durante la prueba.

Descubrimiento: La fase de descubrimiento se centra en la recopilación de información acerca del sistema objetivo. Esto puede incluir el uso de herramientas de escaneo para identificar servicios, puertos abiertos, vulnerabilidades y configuraciones. Si se encuentra información adicional relevante, puede iniciarse un ciclo de "Additional Discovery" (Descubrimiento Adicional) para profundizar la exploración.

Ataque: Esta etapa implica la ejecución de los ataques planificados basados en la información recopilada. Los ataques pueden incluir intentos de explotación de vulnerabilidades, pruebas de acceso no autorizado y otras técnicas para evaluar la seguridad del sistema. El objetivo es validar las vulnerabilidades identificadas

Informe: La última fase consiste en la documentación de los hallazgos. Se elabora un informe que incluye el análisis de los datos obtenidos, las vulnerabilidades encontradas, el impacto potencial de estas, y las recomendaciones para mitigarlas. Este informe se comparte con los responsables para que puedan tomar medidas correctivas.



Áreas de aplicación

- Entornos gubernamentales y empresariales
- Evaluaciones de cumplimiento normativo

Ventajas

- Proporciona un enfoque estandarizado reconocido por agencias gubernamentales.
- Guías completas para diversos tipos de evaluaciones

Desventajas

- Puede ser demasiado complejo para organizaciones más pequeñas.
- Requiere adherirse a directrices estrictas, lo que puede limitar la flexibilidad.

Certified Ethical Hacker (CEH)

Marco estructurado que guía a los profesionales en la realización de pruebas de penetración de manera ética y sistemática. Esta metodología consta de seis fases clave (*CEH v11 Certified Ethical Hacker Study Guide | Wiley eBooks | IEEE Xplore*, s. f.):

Reconocimiento: Esta fase inicial implica la recopilación de la mayor cantidad de información posible sobre el objetivo, incluyendo sistemas, redes y dispositivos conectados. Se utilizan técnicas de reconocimiento pasivo y activo para identificar posibles puntos de entrada.

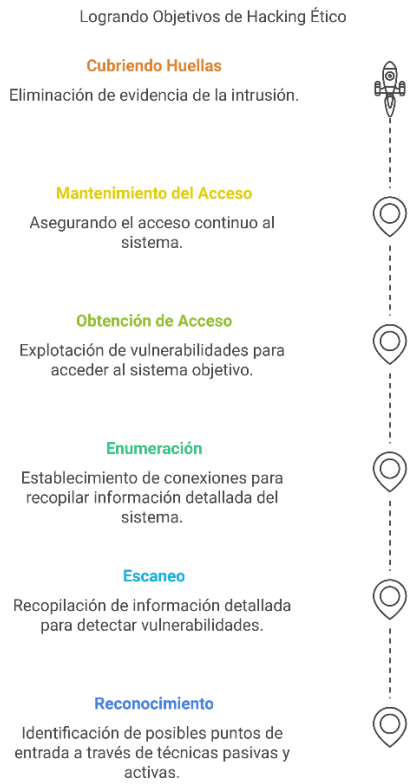
Escaneo: En esta etapa, se profundiza en la información obtenida para identificar detalles específicos como sistemas operativos, puertos abiertos y versiones de software. El objetivo es detectar vulnerabilidades que puedan ser explotadas

Enumeración: Aquí se establecen conexiones activas con los sistemas objetivo para obtener información detallada, como nombres de usuario, nombres de máquinas, recursos compartidos y servicios en ejecución.

Obtención de Acceso: En esta fase, se utilizan las vulnerabilidades identificadas para acceder al sistema objetivo. Se emplean diversas técnicas y herramientas para comprometer la seguridad del sistema.

Mantenimiento del Acceso: Una vez obtenido el acceso, el objetivo es mantenerlo el tiempo necesario para cumplir con los objetivos de la prueba. Esto puede implicar la instalación de puertas traseras o la escalada de privilegios.

Cubrir Huellas: La fase final consiste en eliminar cualquier evidencia de la intrusión para evitar la detección. Esto incluye la eliminación de registros y la restauración de configuraciones originales



Áreas de Aplicación:

- Seguridad de Redes , Aplicaciones Web y Nube, Ingeniería Social, Seguridad de Sistemas Móviles

Ventajas: Ofrece una perspectiva realista al replicar tácticas y técnicas utilizadas por atacantes reales, proporcionando una evaluación exhaustiva de la seguridad.

Desventajas: La implementación efectiva de la metodología CEH demanda un alto nivel de conocimientos técnicos y experiencia en ciberseguridad, lo que puede limitar su aplicación para profesionales con menor formación.

Tabla 1.

Usabilidad de metodología de acuerdo al ejercicio de auditoria a realizar

Metodología	Aplicaciones Web	Infraestructura de Red	Seguridad Física	Seguridad de Redes Inalámbricas	Seguridad de Sistemas Móviles	Cumplimiento Normativo	Seguridad Operativa	Ingeniería Social
PTES	✓	✓		✓	✓	✓	✓	
OWASP	✓				✓			
OSSTMM	✓	✓	✓	✓			✓	
NIST SP 800-115	✓	✓				✓	✓	
CEH	✓	✓		✓	✓	✓		✓

Nota. La tabla presenta una comparación de las cinco metodologías analizadas y ampliamente utilizadas en pruebas de penetración, destacando sus áreas de aplicabilidad en distintos tipos de evaluación e infraestructura. Este análisis permite identificar el enfoque de cada metodología y su adaptabilidad a diferentes escenarios de seguridad, lo cual es fundamental para seleccionar la herramienta adecuada según las necesidades específicas de la organización.

Software Open Source Aplicable en Metodologías de Pruebas de Penetración

Tabla 2.

Herramientas que se pueden usar por fases en un proceso de pentesting

Fase	Nombre de la Herramienta	Descripción	Enlace de Información
Planificación / Interacción Inicial	Recon-ng	Framework para la recopilación de información y mapeo de objetivos.	Recon-ng
	Maltego CE	Herramienta de análisis visual para explorar relaciones y datos relacionados con objetivos.	Maltego CE
	SpiderFoot	Automatización de la inteligencia OSINT para la recolección de datos.	SpiderFoot
Recolección de Datos / Descubrimiento	Nmap	Escaneo de puertos, identificación de servicios y sistemas operativos.	Nmap
	Fierce	Escaneo DNS para identificar redes y subdominios.	Fierce
	Wireshark	Captura y análisis de paquetes para evaluar tráfico de red.	Wireshark

	TheHarvester	Recolección de información OSINT sobre correos, hosts y más.	TheHarvester
Evaluación de Amenazas / Identificación de Vulnerabilidades	OpenVAS	Escáner de vulnerabilidades para redes y sistemas.	OpenVAS
	Nikto	Escáner de servidores web para configuraciones inseguras y vulnerabilidades.	Nikto
	Wfuzz	Fuerza bruta para detectar puntos vulnerables en aplicaciones web.	Wfuzz
	SQLMap	Automatización de pruebas de inyección SQL.	SQLMap
	OWASP ZAP	Escáner de vulnerabilidades en aplicaciones web.	OWASP ZAP
Ejecución de Explotación / Obtención de Acceso	Metasploit	Framework para explotación de vulnerabilidades.	Metasploit
	Hydra	Ataques de fuerza bruta a servicios de autenticación.	Hydra
	Aircrack-ng	Análisis y crackeo de redes inalámbricas.	Aircrack-ng
	John the Ripper	Herramienta para descifrar contraseñas y evaluar su fortaleza.	John the Ripper
Persistencia y Movimientos Laterales / Mantenimiento del Acceso	Empire	Framework para post-explotación y persistencia.	Empire
	Cobalt Strike (Community)	Herramienta para movimientos laterales y control avanzado.	Cobalt Strike
	Mimikatz	Extracción de credenciales en sistemas comprometidos.	Mimikatz
	PowerSploit	Conjunto de herramientas para post-explotación en Windows.	PowerSploit
Elaboración del Informe / Documentación de Resultados	Faraday IDE	Entorno para gestión de pruebas de penetración y reportes.	Faraday IDE
	Dradis Framework	Plataforma para consolidar y presentar hallazgos de seguridad.	Dradis Framework
	KeePass	Gestor seguro para credenciales obtenidas en pruebas de penetración.	KeePass

Conclusiones

En el ámbito de la ciberseguridad, la correcta implementación de pruebas de penetración es esencial para evaluar y fortalecer la protección de sistemas y aplicaciones frente a posibles amenazas. A partir del análisis del boletín del CSIRT Académico UNAD, se han revisado diversas metodologías reconocidas para llevar a cabo estas pruebas, identificando sus principales características, ventajas y limitaciones. A continuación, se presentan las conclusiones clave extraídas de este estudio, que proporcionan una visión integral de las prácticas actuales y su aplicabilidad en diferentes contextos de seguridad.

El uso de metodologías estandarizadas para pruebas de penetración, como PTES, OWASP, OSSTMM, NIST SP 800-115 y CEH, permite una evaluación más integral y estructurada de la seguridad, facilitando la identificación y mitigación efectiva de vulnerabilidades en diferentes entornos. Cada metodología ofrece un enfoque específico que se adapta mejor a ciertos escenarios, ya sea para aplicaciones web, infraestructura de red o sistemas de información.

Cada metodología tiene sus ventajas y limitaciones según el contexto de implementación. Por ejemplo, OWASP se enfoca principalmente en aplicaciones web, lo que puede limitar su aplicabilidad en otros tipos de entornos, mientras que OSSTMM ofrece un enfoque científico y basado en métricas para evaluar la seguridad operativa. Sin embargo, su complejidad puede ser un desafío para organizaciones más pequeñas o con menor madurez en ciberseguridad.

La implementación efectiva de estas metodologías requiere profesionales capacitados con conocimientos especializados en ciberseguridad, debido a la complejidad de las fases y técnicas empleadas. Además, la adopción de una metodología estandarizada como NIST SP 800-115 o CEH proporciona un marco reconocido por agencias gubernamentales y entidades reguladoras, lo que es crucial para cumplir con normativas de seguridad y mejorar la confianza en los sistemas evaluados.

Canales de comunicación

El CSIRT Académico UNAD, actualmente cuenta con los siguientes canales de comunicación:

- Correo: csirt@unad.edu.co
- Página web: https://csirt.unad.edu.co

Referentes Bibliograficos

CEH v11 Certified Ethical Hacker Study Guide | Wiley eBooks | IEEE Xplore. (s. f.). Recuperado 15 de noviembre de 2024, de https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/book/9946651

Herzog. (2010). *OSSTMM*. https://www.isecom.org/OSSTMM.3.pdf. https://www.isecom.org/books.html

NIST SP 800-115. (2020). *NIST*. https://www.nist.gov/privacy-framework/nist-sp-800-115

OWASP. (s. f.). *WSTG - v4.2 | OWASP Foundation*. Recuperado 15 de noviembre de 2024, de https://owasp.org/www-project-web-security-testing-guide/v42/

PTES. (2022). *The Penetration Testing Execution Standard Documentation*.