

Metodologías para la auditoria de la seguridad

¿Qué es un informe de pruebas de penetración?

Un informe de pruebas de penetración es un documento que detalla los resultados de una evaluación de seguridad realizada utilizando técnicas de prueba de penetración. El informe debe incluir información sobre el alcance del compromiso, los objetivos de la prueba y un resumen de los hallazgos. También debe tener recomendaciones para la remediación.

¿Cuándo se utiliza un informe de pruebas de penetración?

Los informes de pruebas de penetración se pueden utilizar para:

Identificar vulnerabilidades de seguridad: Un probador de penetración intentará explotar las vulnerabilidades en los sistemas de una organización para obtener acceso a datos confidenciales o interrumpir las operaciones. El evaluador documentará los pasos para explotar las vulnerabilidades, lo que puede ayudar a la organización a identificar y solucionar los problemas.

Evaluar la eficacia de los controles de seguridad: Al probar la capacidad de la organización para detectar y responder a los ataques, un informe de pruebas de penetración puede ayudar a evaluar la efectividad de sus controles de seguridad.

Comprenda dónde son vulnerables los sistemas: Las pruebas de penetración pueden ayudar a una organización a identificar qué sistemas y datos están en mayor riesgo de ataque. Esta información se puede utilizar para priorizar las mejoras de seguridad.

Determine qué pasos seguir para mejorar la seguridad: Basándose en los resultados de una prueba de penetración, una organización puede determinar qué pasos debe tomar para mejorar su postura de seguridad. Estos pasos pueden incluir la implementación de nuevos controles de seguridad, la mejora de la conciencia de los empleados sobre los riesgos de seguridad o el aumento de la inversión en infraestructura de seguridad.

¿Por qué es esencial un informe de pruebas de penetración?

Un informe de pruebas de penetración es esencial por una variedad de razones:

Debilidades del sistema: Un buen informe de pruebas de penetración es esencial porque puede ayudarlo a comprender las debilidades de su sistema y lo que se debe hacer para solucionarlas. Puede realizar los cambios necesarios en su sistema para mejorar su seguridad identificando estas debilidades.

Seguridad general: Puede proporcionar información valiosa a la administración sobre la seguridad general de los sistemas de la organización. Esta información se puede utilizar para decidir si invertir en medidas de seguridad adicionales. También se puede utilizar para evaluar la eficacia de las medidas de seguridad existentes.

Justificación del gasto: También puede ayudarlo a justificar el gasto de contratar a una empresa profesional de pruebas de penetración. En muchos casos, el costo de contratar a una empresa profesional es mucho menor que reparar el daño que podría haberse evitado si se hubieran realizado las pruebas adecuadas.

Componentes de un informe de pruebas de penetración empresarial

Un informe de pruebas de penetración empresarial es un documento que detalla los resultados de una evaluación de seguridad de un sistema informático, red o aplicación web. El informe debe incluir información sobre las vulnerabilidades descubiertas, los pasos tomados para explotarlas y las recomendaciones para su reparación.

Un informe bien escrito proporcionará recomendaciones claras y viables que se pueden utilizar para mejorar la postura de seguridad de la organización. También debe ser fácil de entender tanto para el personal técnico como para el no técnico.

Componentes de un informe de pruebas de penetración empresarial

Los siguientes son algunos de los componentes clave que deben incluirse en un informe de pruebas de penetración empresarial:

- **Resumen ejecutivo:** El resumen ejecutivo resume brevemente todos los detalles clave del informe. Hablará al lector de una manera que le permita saber qué pasos se tomaron, qué encontró finalmente el informe y una descripción general o lo más destacado de los próximos pasos, que podrían incluir recomendaciones.
- **Herramientas, métodos y vectores:** Esta sección cubre las herramientas que utilizó y los métodos que eligió para realizar la prueba de pluma. Además de proporcionar un esquema general o una narrativa de sus hacks éticos, también detalle los caminos que tomó con patrones de ataque detallados paso a paso y vectores seleccionados.
- **Resultados detallados:** Aquí es donde enumerará todos los riesgos de seguridad, vulnerabilidades, puntos de penetración, amenazas y preocupaciones. Incluya los aspectos técnicos de cada hallazgo en detalle.
- **Conclusión:** En esta sección del informe se reitera el resumen ejecutivo, pero con un enfoque en los próximos pasos.
- **Recomendaciones:** Aunque su trabajo es, en última instancia, hacer la prueba de pluma y evaluar el estado de la postura de seguridad general de la organización, también podría ser responsable de proporcionar orientación sobre formas de mejorar la seguridad. Si es así, póngalos en una sección separada y sea lo más detallado posible.
- **Apéndice:** Incluya esta sección para gráficos, registros y cualquier información que quede fuera del alcance del proyecto pero que crea que podría ser útil.

Metodologías y estándares populares de pruebas de penetración

OSSTMM

El [Open Source Security Testing Methodology Manual](#) (OSSTMM) es una metodología de prueba de PenTesting planteada por ISECOM y creado por Pete Herzog (Institute for Security and Open Methodologies, 2010). Proporciona un marco científico para las pruebas de PenTesting de red y la evaluación de vulnerabilidades y ofrece una guía completa que puede ser utilizada adecuadamente por un probador certificado. El OSSTMM cubre cinco categorías:

- Controles de datos e información
- Concienciación sobre la seguridad entre el personal
- Controles de fraude e ingeniería social
- Controles para dispositivos en red, incluidos ordenadores y dispositivos inalámbricos
- Controles de seguridad física

Uno de los principales beneficios del OSSTMM es su alto nivel de flexibilidad. Si los probadores de PenTesting aplican el OSSTMM correctamente, pueden usarlo para resolver vulnerabilidades encontradas en múltiples dispositivos, incluidos equipos, servidores, dispositivos inalámbricos y más.

OSSTMM

Desde una perspectiva técnica, esta técnica está dividida en 4 grupos clave: alcance, canal, índice y vector.

- El **alcance** define un proceso de recolecta de información en todos los bienes en el ambiente objetivo.
- El **canal** determina el tipo de comunicación e interacción que habrá con los bienes los cuales pueden ser físicos, espectros y comunicativos. Todos estos canales representan un único set de los componentes de seguridad y deben ser testeados y verificados durante el periodo de evaluación. En estos componentes estarían comprendidos la seguridad física, la psicología humana, la información de la red los medios de comunicación Wireless y las telecomunicaciones.
- El **índice** es un método para clasificar bienes objetivo que se corresponde con sus particulares identificaciones como la dirección MAC o la dirección IP.
- El **vector** concluye en qué dirección puede el auditor evaluar y analizar cada bien funcional.

OSSTMM

Estas pruebas generalmente examinan el objetivo evaluando sus:

- Controles de acceso.
- Procesos de seguridad.
- Controles de información.
- Localizaciones físicas.
- Protección de los perímetros.
- El nivel de conciencia de seguridad.
- Nivel de confianza.
- Control de protección de fraude.

OSSTMM

Todos los procedimientos de ensayo ponen el foco en lo que hay que testear, como ha de ser testado, que tácticas han de ser aplicadas antes, durante y después del test y como interpretar y correlacionar los resultados finales.

Capturar el estado actual de la protección del objetivo es muy útil e inestimable.

Para poner solución, la metodología OSSTMM ha introducido el termino **RAV (Risk Assessment Values)**, por sus siglas en ingles).

La función básica del RAV es analizar los resultados de las pruebas y computar el valor actual de la seguridad basado en tres factores, seguridad operacional, pérdida de control y limitaciones.

El resultado final es conocido como **RAV score**.

Desde el punto de vista empresarial, el RAV score, ayuda a optimizar y justificar las inversiones en medidas de seguridad.

OSSTMM

Ámbito

- Cuando, que y cuales eventos son testeados.
- ISECOM Exige que un test de seguridad puede considerarse

OSSTMM si:

- Es cuantificable.
- Consistente y que se puede repetir.
- Válido más allá del periodo de tiempo actual.
- Basado en el merito del testeador y analista, y no en marcas comerciales.
- Exhaustivo.
- Concordante con las leyes individuales y locales y el derecho humano a la privacidad

OSSTMM Convergencia entre dominios

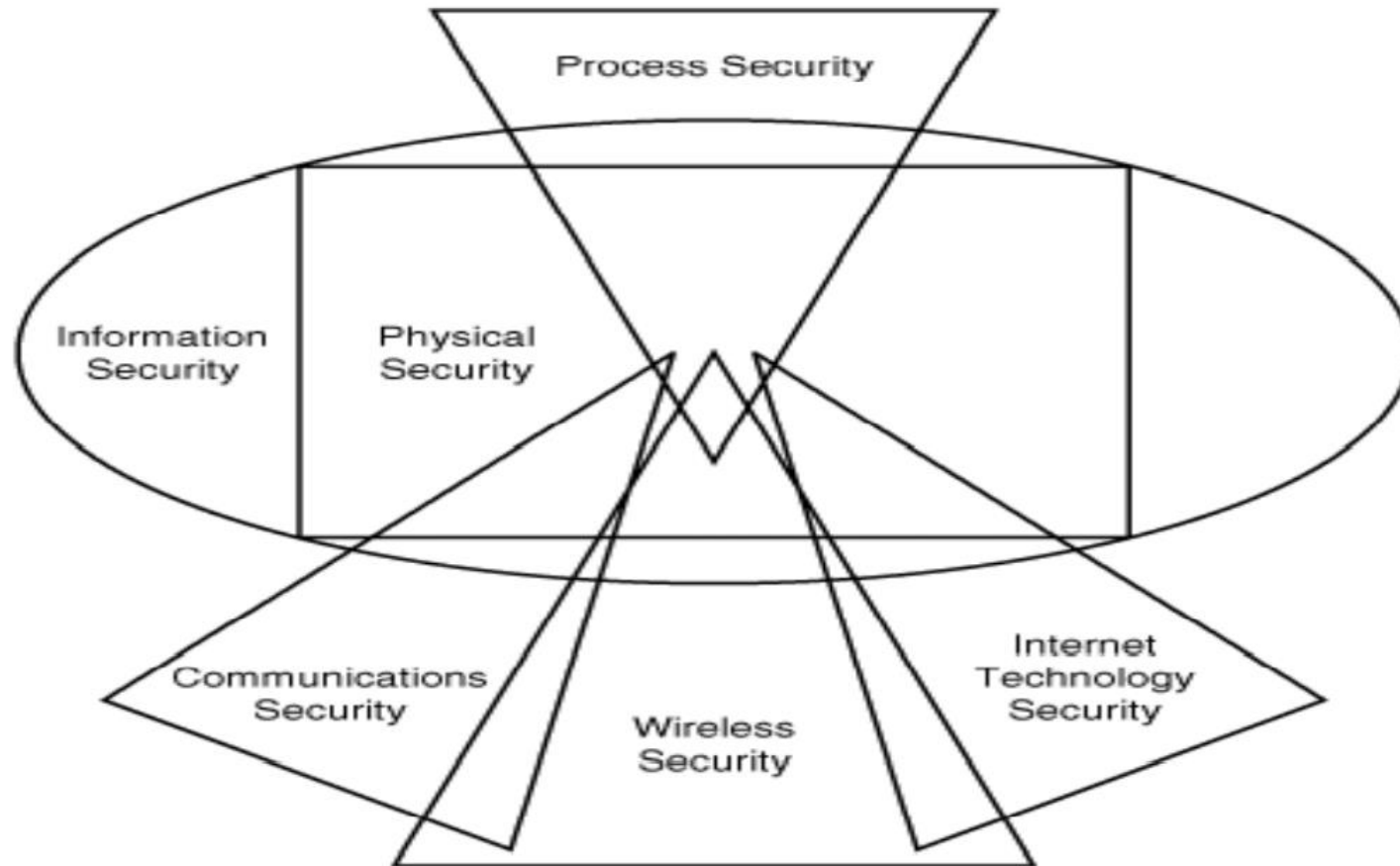
El OSSTMM se centra en los detalles técnicos de los elementos que deben ser probados.

¿Qué hacer antes, durante y después de una prueba de seguridad?, y ¿cómo medir los resultados?

Se divide en 6 grandes grupos:

- Seguridad de la Información
- Seguridad de los Procesos
- Seguridad en las tecnologías de Internet
- Seguridad en las Comunicaciones
- Seguridad Inalámbrica
- Seguridad física

OSSTMM Convergencia entre dominios



OSSTMM

Sección A

- Seguridad de la Información
 - Revisión de la Inteligencia Competitiva (Google)
 - Revisión de la Privacidad (LOPD, LSSI)
 - Recolección de Documentos (FOCA)

OSSTMM

Sección B

- Seguridad de los Procesos
 - Testeo de Solicitud (Ingeniería social)
 - Testeo de Sugerencia Dirigida (Ingeniería social Phising)
 - Testeo de las Personas Confiables (Ingeniería social)

OSSTMM

Sección C

- Seguridad en las tecnologías de Internet (1)
 - Exploración de Red (whois y DNS)
 - Escaneo de puertos (el gran Nmap)
 - Identificación de los Servicios del Sistema (Telnet, Netcat y Nmap)
 - Identificación del Sistema (Telnet, Netcat y Nmap para estudio de banners y fingerprint)
 - Búsqueda de vulnerabilidades y verificación (exploits)
 - Testeo de aplicaciones de Internet (Metasploit)
 - Testeo del router (Telnet, traceroute)
 - Testeo de sistemas de confianza (ACLs)

OSSTMM

Sección C

- Seguridad en las tecnologías de Internet (2)
 - Testeo del Firewall (Traceroute)
 - Testeo de los Sistemas de Detección de Intrusos (IDS)
 - Testeo de medidas de protección (virus, troyanos, código malicioso)
 - Testeo de contraseñas (John the ripper)
 - Testeo de Denegación de Servicio (herramientas de stress)
 - Revisión de las políticas de seguridad (Microsoft Word y Acrobat Reader)

OSSTMM

Sección D

- Seguridad en las Comunicaciones
 - Testeo de PBX (Centralitas telefónicas, números 900)
 - Testeo del Correo de Voz
 - Revisión del FAX (políticas de envío, ACLs, FTP)
 - Testeo del router (wardialing, WarVox sobre VoIP)

OSSTMM

Sección E

– Seguridad Inalámbrica

- Verificación de Radiación Electromagnética (EMR)
- Verificación de Redes Inalámbricas (aircrack, kismet)
- Verificación de Bluetooth (Super Bluetooth Hack)
- Verificación de Dispositivos de Entrada Inalámbricos
- Verificación de Dispositivos de biometría
- Verificación de Dispositivos de Vigilancia Inalámbricos
- Verificación de Dispositivos de Transacción Inalámbricos (lectores códigos de barras CheckPoint)
- Verificación de RFID (pasaporte británico)
- Verificación de Sistemas Infrarrojos (MIRT semáforos)
- Revisión de Privacidad (sniffers inalámbricos)

OSSTMM

Sección F

- Seguridad Física Revisión de Perímetro (Datacenter)
 - Revisión de la monitorización (dispositivos de entrada)
 - Evaluación de Controles de Acceso
 - Revisión de Respuesta de Alarmas
 - Revisión de Ubicación
 - Revisión de Entorno (alrededores de la empresa, posibles desastres naturales)

OSSTMM Acreditación

- Una planilla de datos de test de seguridad es necesaria (Star), firmada por los testeadores, acompañando todos los reportes finales para obtener un test certificado OSSTMM.
 - Incluyen cuales módulos y tareas han sido testeadas hasta su conclusión.
 - Cuales no han sido testeados hasta su conclusión y su justificación.
 - Y cuales son los test no aplicables y su justificación.

OSSTMM

Razones del uso de Planillas

- Las razones para el uso de planillas de datos son las siguientes:
 - Sirve como prueba de un testeo de OSSTMM minucioso.
 - Responsabiliza al testeador por el test.
 - Es una declaración precisa al cliente.
 - Brinda una apropiada visión general.
 - Suministra una lista de comprobación clara para el testeador.

OSSTMM Sellos de informe

Este test ha sido ejecutado con OSSTMM disponible en <http://www.osstmm.org> y mediante este sello se afirma que está dentro de las mejores prácticas de se testeo de seguridad.



OSSTMM

Lineamientos de Acción

- Ventas y Mercadeo
 - Miedo infundado.
 - Ofrecer servicios gratuitos a cambio de fallar en el test o entregar premios del objetivo están prohibidos.
 - Competencias de hacking, cracking y violación de sitios, están prohibidos.
 - Ejecutar test de seguridad sin permiso.
 - Usar nombre de clientes previos.
 - Asesoría acertada, aun cuando se deba desviar a otra compañía.

OSSTMM

Lineamientos de Acción

- Contratos y negociaciones:
 - No divulgación.
 - Explicar claramente los límites y peligros de un análisis de seguridad.
 - Especificar el origen de las pruebas (análisis remoto).
 - Incluir información de contacto en caso de emergencia.
 - Permisos claros y específicos para análisis que involucre fallas de supervivencia, negación de servicios, análisis de procesos o ingeniería social.
 - Contener los procesos para contratos futuros y cambios en las condiciones de trabajo.

OSSTMM

Lineamientos de Acción

- **Ámbito:**
 - Claramente definido.
 - Explicar claramente los límites del análisis de seguridad.
- **Plan de trabajo**
 - Incluir tiempo calendario como horas hombre.
 - Incluir horas de análisis.

OSSTMM

Lineamientos de Acción

- Entregar reglas del contrato al cliente
 - No se permiten cambios de red inusuales durante el análisis.
 - El cliente debe notificar sólo al personal clave, para evitar aumentos en la seguridad (trampa).
 - Para pruebas con privilegios, se debe proveer de mecanismos de acceso independientes. Con privilegios típicos.
 - Primero testear sin privilegios y luego con los permisos otorgados.

OSSTMM Test

- Para la realización de los test los analistas deben conocer sus herramientas.
- No realizar pruebas de denegación de servicios sin permiso explícito.
- Para la Ing. Social se deben realizar encuestas anónimas a personal no especializado.
- Las vulnerabilidades de alto riesgo se deben informar de inmediato con una solución práctica.
- Prohibida la denegación de servicios distribuida (DDOS).
- Prohibido todo tipo de ataques por inundación o saturación.

OSSTMM Informes

- Los informes debe incluir una solución práctica.
- Se deben incluir los hallazgos desconocidos e informarse como tales.
- Se deben especificar todos los estados de seguridad encontrados, no solo las medidas de seguridad fallidas.
- Usar indicadores cualitativos, basándose en formulas matemáticas y no en la intuición.
- Confirmar la recepción del informe.
- Los canales para la entrega de informes deben ser confidenciales

OSSTMM

Mapa de seguridad

- Las secciones del manual de OSSTMM son:
 1. Seguridad de la información
 2. Seguridad de los procesos.
 3. Seguridad de las tecnologías de Internet.
 4. Seguridad de las comunicaciones.
 5. Seguridad inalámbrica.
 6. Seguridad física

OSSTMM

Evaluación de Riesgo

- Es mantenida por el analista.
- Toda la información se considera válida, para proveer una evaluación de riesgo válida.
- El riesgo significa que todos los límites de la presencia de seguridad tendrán un efecto perjudicial en la gente.

OSSTMM

Seguridad perfecta

- En la seguridad perfecta los analistas calibran con el cliente que se puede considerar seguridad perfecta.
- Mejores prácticas.
- Regulaciones en la industria del cliente.
- La política de seguridad del cliente y los asuntos legales.
- Se puede comparar el estado actual de seguridad y la “seguridad perfecta”.

OSSTMM

Valores de evaluación de riesgo

- Los valores de evaluación de riesgo (RAV), se definen como la degradación de la seguridad sobre un ciclo de vida específico.
- Se debe basar en las mejores prácticas para test periódicos.
- Están definidos matemáticamente.
- Clasificaciones de tipo de riesgo:
 - a. Identificados
 - b. Verificado
 - c. No aplicable

OSSTMM

Valores de evaluación de riesgo

Valores de la Evaluación de Riesgo

Módulo	Ciclo (días)	Degradación (%)	Influencia (x)
Revisión de Postura			
Verificación de Radiación Electromagnética (EMR)	Debería ser realizada en nuevas instalaciones o cada vez que se añada un nuevo dispositivo a una configuración segura existente.		
Verificación de Redes Inalámbricas 802.11	28 días	1.3%	
Verificación de Redes Bluetooth	28 días	1.3%	
Verificación de Dispositivos de Entrada Inalámbricos	60 días	2.8%	
Verificación de Dispositivos de Mano Inalámbricos	60 días	2.8%	
Verificación de Comunicaciones sin Cables	60 días	2.8%	
Verificación de Dispositivos de Vigilancia Inalámbricos	Debería ser realizada en nuevas instalaciones o cada vez que se añada un nuevo dispositivo a una configuración segura existente.		
Verificación de Dispositivos de Transacción Inalámbricos	Debería ser realizada en nuevas instalaciones o cada vez que se añada un nuevo dispositivo a una configuración segura existente.		
Verificación de RFID	365 días		
Verificación de Infrarrojos	120 días	.6%	
Revisión de Privacidad	70 días	2.1%	

OSSTMM

Propósito del Manual OSSTMM

El propósito principal del manual es proporcionar una metodología científica para la estructura precisa de la seguridad operacional a través de la examinación y la correlación de los resultados de las pruebas de una manera consistente y confiable.

El segundo propósito es suministrar pautas que permitan al analista realizar una auditoría OSSTMM certificada. Estas pautas aseguran que la prueba se realizó a fondo e incluyó todos los canales necesarios; la postura de la prueba cumplió con la ley; los resultados se pueden medir de forma cuantificable, son consistentes y repetibles, y contienen solo hechos derivados de las pruebas mismas.

OSSTMM

Alcance del Manual OSSTMM

Proporcionar **descripciones específicas** para las pruebas de seguridad operacional en todos los canales operativos, como, la seguridad humana, física, inalámbrica, telecomunicación y de redes de datos. El manual se enfoca en la seguridad operacional.

OSSTMM Responsabilidad

El manual OSSTMM cuenta con pruebas diseñadas para obtener una respuesta.

Estas pruebas podrían ocasionar daños.

Al utilizar esta metodología, el analista acepta asumir esta responsabilidad, de acuerdo con las leyes que rigen en el país donde se ejecuta el manual, así también como la ubicación de los sistemas probados.

OSSTMM

Certificación y Acreditación

Para contar con una auditoría certificada por OSSTMM, se necesita que el Informe de Auditoría de Prueba de Seguridad, STAR6 por sus siglas en inglés, sea revisado lo que fue y no fue probado, para ser aplicable a la certificación.

Una auditoría certificada OSSTMM ofrece beneficios:

- Sirve como prueba de una prueba de hechos
- Responsabiliza al analista de la prueba
- Proporciona un resultado claro para el cliente
- Ofrece una visión general más completa que un resumen ejecutivo
- Proporciona métricas comprensibles.

OSSTMM

Qué se necesita saber acerca de OSSTMM

La seguridad operacional consiste en las diferentes políticas y procedimientos implementados por la administración de la instalación computacional.

La metodología OSSTMM mide el buen funcionamiento de la seguridad operacional.

En el contexto de seguridad operacional, **se llama seguridad** a la separación de un activo y una amenaza (security), y al control de una amenaza o sus efectos (safety).

OSSTMM Seguridad (security)

Es la separación entre un activo y cualquier amenaza que existe o que no existe. Hay tres formas de lograr esta separación:

- a) Mover el activo para crear una barrera física o lógica entre él y las amenazas.
- b) Cambiar la amenaza a un estado inofensivo.
- c) Destruir la amenaza.

OSSTMM Seguridad (security)

Al analizar el estado de la seguridad, se identifica **donde existe la posibilidad de interacción y dónde no.**

Se reconoce que interacciones son necesarias para las operaciones y cuáles no.

El analista de seguridad no cuenta con el conocimiento de la razón de ser de todos los puntos interactivos, estos puntos interactivos se conceptualizan como la **Porosidad.**

OSSTMM Seguridad (security)

La porosidad disminuye la separación entre una amenaza y un acceso.

Cuenta con tres elementos como ser:

1. La **visibilidad** que es un medio para calcular la oportunidad de llegar al activo
2. El **acceso** es la capacidad de interactuar y acceder al activo
3. La **confianza** es la aceptación de interacción libre entre dos activos u objetivos dentro del alcance.

Por lo tanto, **el aumento de la porosidad es la disminución de la seguridad.**

OSSTMM Seguridad (security), Controles

Ante las amenazas, los controles proveen seguridad en las operaciones. Cuando se requiere interacción, los controles influyen en el impacto de las amenazas y sus efectos.

Los controles se agrupan en interactivos y de proceso.

OSSTMM

Seguridad (security), Controles

a- **Controles Interactivos:** Influyen directamente en la visibilidad, el acceso y en las interacciones de confianza. Se compone de:

1- **Autenticación:** es cada instancia de autenticación requerida para obtener acceso. Ej., en una auditoría de seguridad física en donde se solicita una tarjeta de identificación y la huella dactilar, se suma 2 a los controles de autenticación.

2- **Indemnización:** son todas las instancias de métodos utilizados para la compensación por pérdidas referidas a los activos. Ej., un seguro que cubre el robo de 30 equipos de computación cuenta como 30.

OSSTMM

Seguridad (security), Controles

3- **Resistencia:** es cada instancia de acceso o confianza donde una falla en el sistema de seguridad no provea un nuevo acceso. Ej., existe un servicio web que solicita credenciales y las valida contra una base de datos, en el caso que este servicio pierda la conexión con la base, entonces no debe validar ninguna credencial hasta la restauración de la conexión. En caso de rechazar las credenciales, cuenta como 1 el valor de resistencia. Existe la posibilidad de que el servicio no esté correctamente diseñado y cuando pierde la conexión comience a validar todas las credenciales, inclusive las que no son correctas; en ese caso la resistencia es 0.

4- **Subyugación:** son todos los puntos de acceso o confianza donde la interacción deba cumplir condiciones preestablecidas. Ej., el uso de PKI8 para las comunicaciones entre un cliente y un servidor cuenta como 1 ya que la comunicación sólo puede establecerse si cumplen esa condición.

5- **Continuidad:** son todos los puntos de acceso o confianza donde una falla no cause una interrupción en la interacción. Dentro de los ejemplos para este punto se encuentran la redundancia y el balanceo de carga. En seguridad física, si una puerta se bloquea y no existe una entrada alternativa para los clientes entonces tiene continuidad 0 para ese vector.

OSSTMM

Seguridad (security), Controles

b- **Controles de Proceso:** Utilizados para crear procesos defensivos. Protegen los activos una vez que la amenaza esté presente. Se compone de:

6- **No repudio:** es cada acceso o confianza que provea algún mecanismo de no repudio, tal que exista alguna forma de determinar que la interacción se produjo en un tiempo determinado entre las partes identificadas. Dentro del canal de las redes de datos, los archivos de logs brindan mecanismos para el no repudio.

7- **Confidencialidad:** es cada instancia de acceso o confianza que provea mecanismos para evitar revelar información a terceros no autorizados. Un ejemplo claro de confidencialidad es el cifrado de la información.

OSSTMM Seguridad (security), Controles

8- **Privacidad:** es cada acceso o confianza donde el método de interacción sea ocultado. Esto no quiere decir que la información viaje codificada, sino que no se sepa que hay comunicación o que ésta sea ofuscada de alguna manera. En seguridad física, un cuarto cerrado donde se efectúe la comunicación entre personas provee privacidad.

9- **Integridad:** es cada acceso o confianza donde la interacción brinde algún mecanismo que permita conocer si la información fue modificada por terceros no autorizados. En el canal de las redes de datos, una función de hash9 puede usarse para proveer integridad.

10- **Alarma:** es cada acceso o confianza que genere un registro o notificación cuando exista algún evento no autorizado o erróneo. En las redes de datos, los archivos de logs cuentan como alarma, aunque estos no generen una notificación inmediata. También se debe sumar un punto por cada equipo monitoreado por un sistema de detección de intrusiones o antivirus.

OSSTMM

Objetivos de garantía de la información

Al agrupar los controles de operación en referencia a los objetivos de la seguridad de la información, es como sigue:

Objetivos de garantía de la información	Controles de operación
Confidencialidad	Confidencialidad Privacidad Autenticación Resistencia
Integridad	Integridad No repudio Subyugación
Disponibilidad	Continuidad Indemnización Alarma

OSSTMM Limitaciones

La limitación es el estado de la seguridad con respecto a las fallas y restricciones conocidas dentro del alcance de las operaciones.

Son las vulnerabilidades, debilidades y problemas para mantener la separación entre un activo y una amenaza o para asegurar que los controles continúan funcionando correctamente.

Dentro del OSSTMM, las clasificaciones de Limitación son:

a- **Vulnerabilidad:** es cada falla o error que pueda llevar a un acceso no autorizado o denegar un acceso legítimo. Un ejemplo referido al canal de las redes de datos puede ser un proceso que permite la sobreescritura de áreas de memoria que lleven a la ejecución de código malicioso.

b- **Debilidad:** son todas las fallas o errores en los controles de interacción: autenticación, indemnización, resistencia, subyugación y continuidad. Un ejemplo de debilidad en el canal de las redes de datos puede ser una pantalla que solicita credenciales de acceso que no posea límites en cuanto a la cantidad de intentos.

OSSTMM Limitaciones

- c- **Preocupación:** son todas las fallas en los controles de proceso: no repudio, confidencialidad, privacidad, integridad y alarma. Un ejemplo de preocupación es un proceso que genere archivos de log con los datos de los participantes involucrados, pero no almacene correctamente la fecha y hora de la transacción.
- d- **Exposición:** es cada acción no justificada, falla o error que provean visibilidad de los objetivos o activos, ya sea de forma directa o indirecta. Un claro ejemplo de exposición son los banners que brindan información de la aplicación que está corriendo detrás de un puerto específico.
- e- **Anomalía:** es cada elemento desconocido que no puede clasificarse dentro de las operaciones normales, ya que esto puede ser un síntoma para problemas de seguridad futuros. Un ejemplo de anomalías dentro del canal de las redes de datos es una respuesta ICMP proveniente de una dirección IP inexistente.

OSSTMM Limitaciones

Categoría		Seguridad Operacional	Limitaciones
Operaciones		Visibilidad	Exposición
		Acceso	Vulnerabilidad
		Confianza	
Controles	Clase A – Interactivo	Autenticación	Debilidad
		Indemnización	
		Resistencia	
		Subyugación	
		Continuidad	
	Clase B – Proceso	No repudio	Preocupación
		Confidencialidad	
		Privacidad	
		Integridad	
		Alarma	
			Anomalías

OSSTMM

La seguridad real

El rol de los controles es reducir y manejar la porosidad.

Las limitaciones entonces reducen la efectividad de la seguridad operacional y de los controles.

El resultado de una auditoría que demuestra la seguridad, los controles y las limitaciones está exponiendo efectivamente la seguridad real.

El término seguridad real hace referencia a una instantánea de la superficie de ataque en un ambiente operacional.

OSSTMM

Definición de alcance de una prueba de seguridad

La metodología cuenta con pasos y puede ser utilizada y adaptarla a cualquier organización en la que se requiera obtener información importante de una auditoria de seguridad de la información.

Los 7 pasos que se propone seguir para llevar a cabo una prueba de seguridad exitosa se describen a continuación:

OSSTMM

Definición de alcance de una prueba de seguridad

- a- **Definir los activos que se desea proteger.** Los mecanismos de protección de dichos activos son los Controles, mismos que se probaran para identificar las Limitaciones.
- b- **Identificar el área alrededor de los activos,** en donde se deben incluir los mecanismos de protección y los procesos o servicios contruidos en torno a los activos. Esto se conoce como la Zona de enfrentamiento.
- c- **Definir todo fuera de la zona de enfrentamiento que es necesario para mantener a los activos operativos,** tales como: electricidad, alimentos, agua, aire, suelo estable, información, legislación y reglamentos; y los ambientes y cosas con las que puede trabajar. Eso se conoce como el alcance de la prueba.

OSSTMM

Definición de alcance de una prueba de seguridad

d- **Definir como el alcance interactúa dentro de sí y con el exterior**, para ello es necesario fraccionar los activos dentro del alcance conforme la dirección de las interacciones tales como: del interior al exterior, del exterior al interior, en el interior para el interior. Esto se conoce como los vectores, idealmente, cada vector debería considerar una prueba separada con una duración corta, antes de que el ambiente de la prueba presente cambios notables.

e- **Identificar los equipos que serán necesarios para cada prueba**. Dentro de cada vector, las interacciones pueden ocurrir en varios niveles, estos mismos se clasifican según su función en cinco canales.

OSSTMM

Definición de alcance de una prueba de seguridad

f- **Determinar la información que se desea obtener de la prueba.** El tipo de prueba debe ser definido de forma individual, la metodología OSSTMM identifica seis tipos de pruebas; de los cuales, dependiendo de la cantidad de información que el auditor conoce acerca de los objetivos y lo que el objetivo espera de la prueba, se deberá definir de forma individual la que más se adapte a las necesidades del proceso a desarrollarse en la evaluación de cada uno de los canales.

g- **Hay que asegurar que la prueba de seguridad cumpla con las normas judiciales,** esto con el fin de asegurar que el proceso que se lleve a cabo no genere malentendidos, confusiones o falsas expectativas.

El resultado final será una medida de su Superficie de Ataque. La superficie de ataque es la parte no protegida del Alcance de un Vector definido.

OSSTMM Alcance de los canales

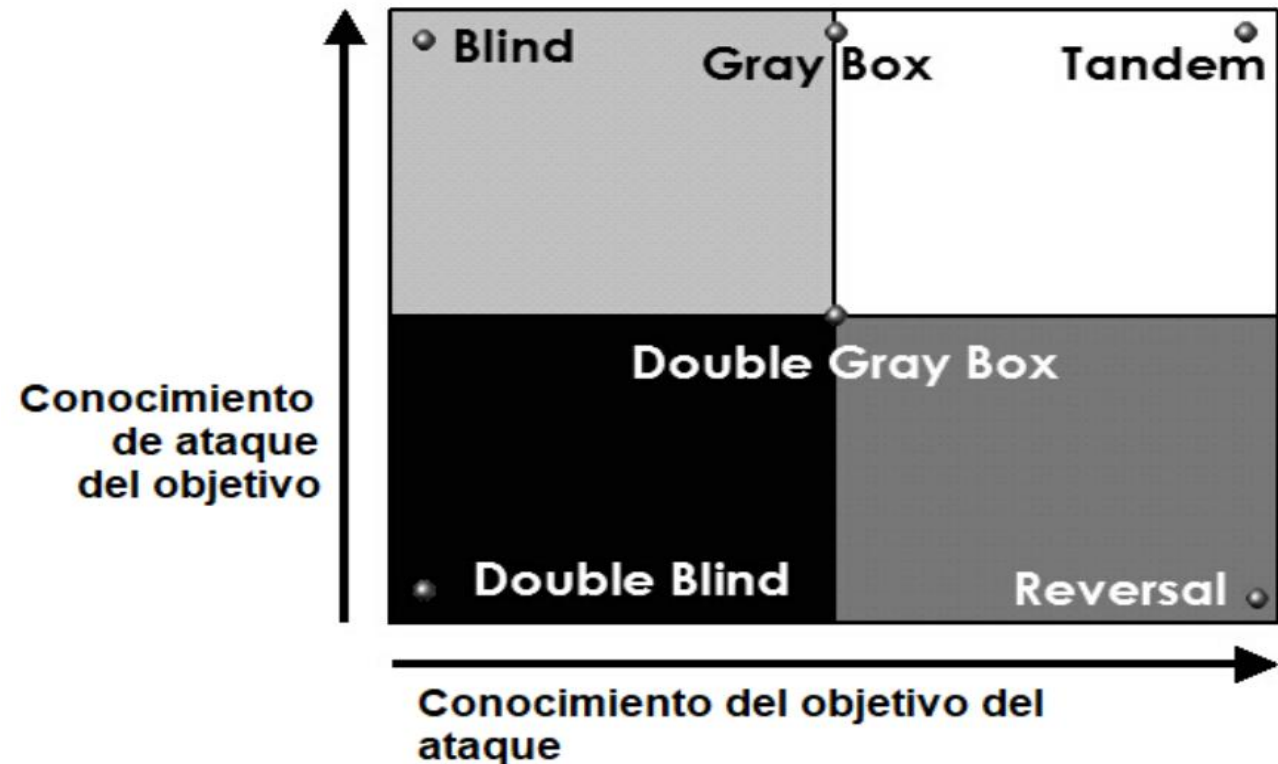
Es el entorno de seguridad operativo total posible para cualquier interacción con el activo. El alcance se compone de tres clases, divididos en cinco canales:

Clase	Canal	Descripción
Seguridad Física PHYSSEC ¹¹	Humano	Comprende el elemento humano cuando la interacción es física o psicológica.
	Físico	Comprende el elemento tangible tales como el hardware, maquinaria, puertas, ventanas, pizarras, escritos.
Seguridad del espectro SPECSEC ¹²	Medios Inalámbricos	Comprende todas las comunicaciones electrónicas, señales y emanaciones en el espectro electromagnético.
Seguridad de las Comunicaciones COMSEC ¹³	Telecomunicaciones	Comprende todas las redes de telecomunicaciones, donde la interacción es a través de líneas telefónicas.
	Redes de datos	Comprende todos los sistemas electrónicos y redes de datos donde la interacción es a través de líneas de red cableadas.

OSSTMM Tipos de prueba

Hay diferentes formas de testear la seguridad que han sido clasificadas bajo la metodología OSSTMM y sus organizaciones la presentan bajo seis tipos de estándares de testeo de seguridad:

- Ciego
- Doble Ciego
- Caja gris
- Doble Caja Gris
- Tándem
- Reversal



Ciego

La prueba ciega no requiere ningún conocimiento previo acerca del objetivo. Sin embargo, el objetivo es informado antes de la ejecución de una auditoria de alcance.

El Hacking Ético y los juegos de guerra son ejemplos de este tipo de prueba.

Doble Ciego

En el Doble Ciego, ningún auditor requiere información previa sobre el objetivo, pero el objetivo tampoco es informado con anterioridad a la prueba.

Las auditorias de Caja Negra y las pruebas de penetración son ejemplos de Doble Ciego.

Al ser la auditoria que más se acerca a los casos reales, esta es la más usada a día de hoy porque obliga a usar la mejor variedad de herramientas y técnicas para alcanzar el objetivo requerido.

Caja Gris

Aquí el auditor tiene información limitada acerca del objetivo y el objetivo además es informado con anterioridad a la ejecución de la prueba.

La evaluación de vulnerabilidades es uno de los ejemplos básicos de Caja Gris.

Doble Caja Gris

La Doble Caja Gris es similar a la anterior (Caja Gris) solo que hay un periodo de tiempo limitado para la auditoria y no hay canales o vectores probados.

Las pruebas de Caja Blanca son un ejemplo de Doble Caja Gris.

Tándem

En este estándar, el auditor tiene la mínima información del objetivo y además, el objetivo es informado con anterior a la ejecución de la prueba.

Reversal

Para finalizar, en Reversal, el auditor, tiene toda la información sobre el objetivo, pero el objetivo no será nunca informado sobre cómo y cuándo se realizará el test.

OSSTMM

Reglas de compromiso

Estas reglas definen las pautas operativas de las prácticas aceptables en las pruebas de marketing y venta, la realización de trabajos de prueba y el manejo de los resultados de los compromisos de prueba:

- a- Ventas y marketing
- b- Evaluación / Entrega estimada
- c- Contratos y negociaciones
- d- Definición del alcance
- e- Plan de prueba
- f- Proceso de prueba
- g- Informes

OSSTMM

Métricas de la seguridad operacional

Una métrica operativa es una medida constante que nos informa la comprobación de hechos en relación con el mundo físico en el que vivimos.

Son operativas porque son números con los que podemos trabajar de manera constante, día a día, y de persona a persona.

OSSTMM

Conociendo el RAV

La función básica del RAV es analizar los resultados de las pruebas y computar el valor actual de la seguridad basado en tres factores, seguridad operacional, controles y limitaciones.

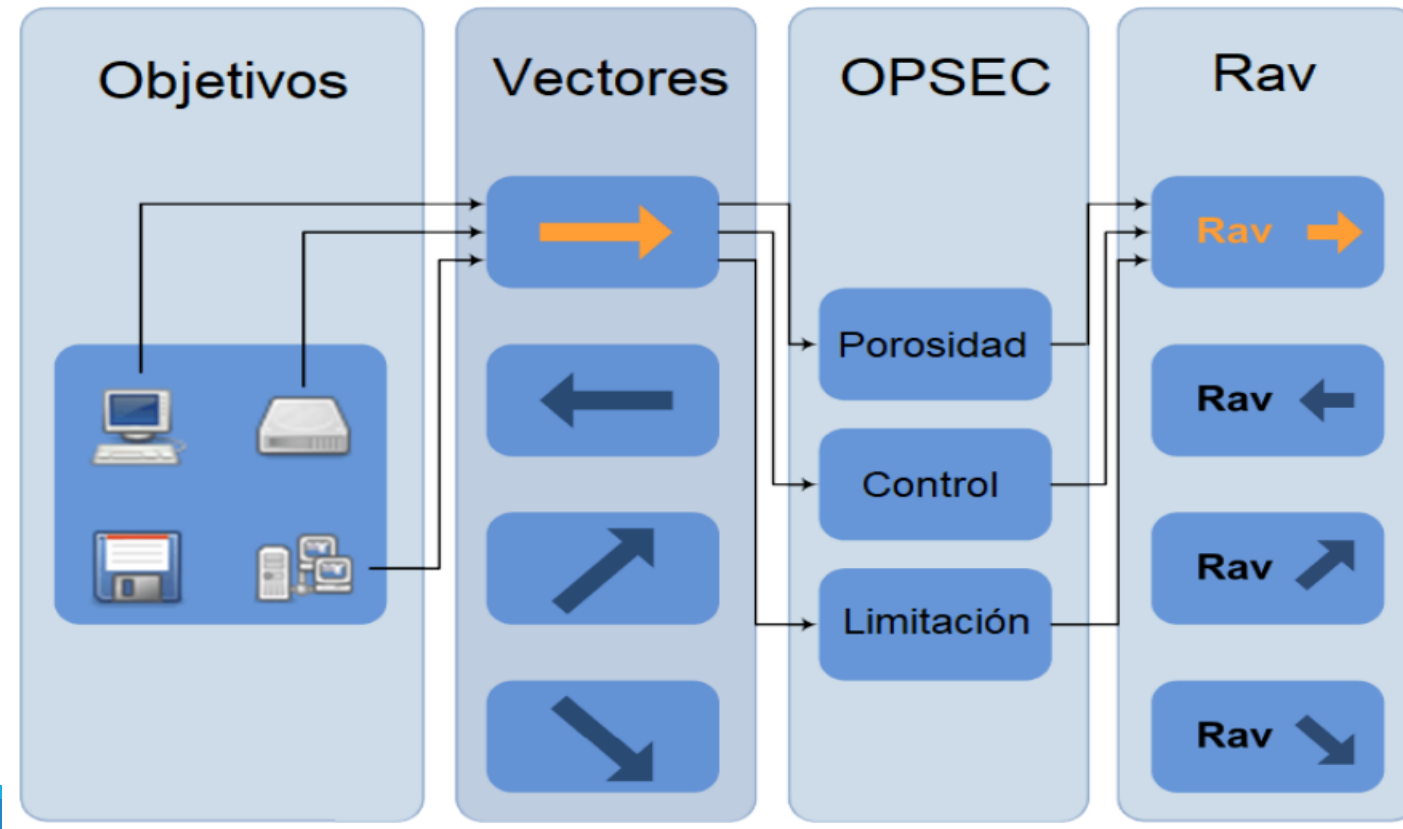
El resultado final es conocido como la puntuación RAV.

Desde el punto de vista organizacional, el RAV, ayuda a optimizar y justificar las inversiones en medidas de seguridad.

OSSTMM

Cómo hacer un RAV

El RAV fue diseñado originalmente para pruebas de operaciones, donde el auditor se enfoca en el comportamiento del objetivo en lugar de la configuración



OSSTMM

Cómo hacer un RAV



Calculadora RAV: Una forma sencilla y directa de hacer RAVs es usar las hojas de cálculo creadas específicamente para calcular la superficie de ataque y varias métricas requeridas populares a partir de los datos de prueba.

Esta hoja de cálculo está disponible en el sitio web de ISECOM.

La hoja de cálculo de RAV es para determinar el equilibrio entre porosidad, controles y limitaciones.

OSSTMM

Cómo hacer un RAV

Attack Surface Security Metrics				
OSSTMM version 3.0				
Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.				
OPSEC				
Visibility	1			
Access	3			
Trust	0			
Total (Porosity)	4			OPSEC 6.776361
CONTROLS			True Controls 3.837843	
Class A		Missing		
Authentication	7	0		
Indemnification	0	4		Full Controls 4.986272
Resilience	0	4		
Subjugation	0	4		
Continuity	0	4		True Coverage A 20.00%
Total Class A	7	16		
Class B		Missing		True Coverage B 25.00%
Non-Repudiation	0	4		
Confidentiality	0	4		
Privacy	1	3		Total True Coverage 22.50%
Integrity	0	4		
Alarm	9	0		
Total Class B	10	15		
		True Missing		
All Controls Total	17	31		
Whole Coverage	42.50%	77.50%		
LIMITATIONS				
		Item Value	Total Value	Limitations 15.730239
Vulnerabilities	4	8.750000	35.000000	
Weaknesses	5	5.000000	25.000000	
Concerns	8	4.750000	38.000000	Security Δ -17.72
Exposures	0	5.025000	0.000000	
Anomalies	0	4.250000	0.000000	
Total # Limitations	17		98.0000	True Protection 81.13
Actual Security: 82,2269 ravs				

OSSTMM

Las fases de prueba de la OSSTMM

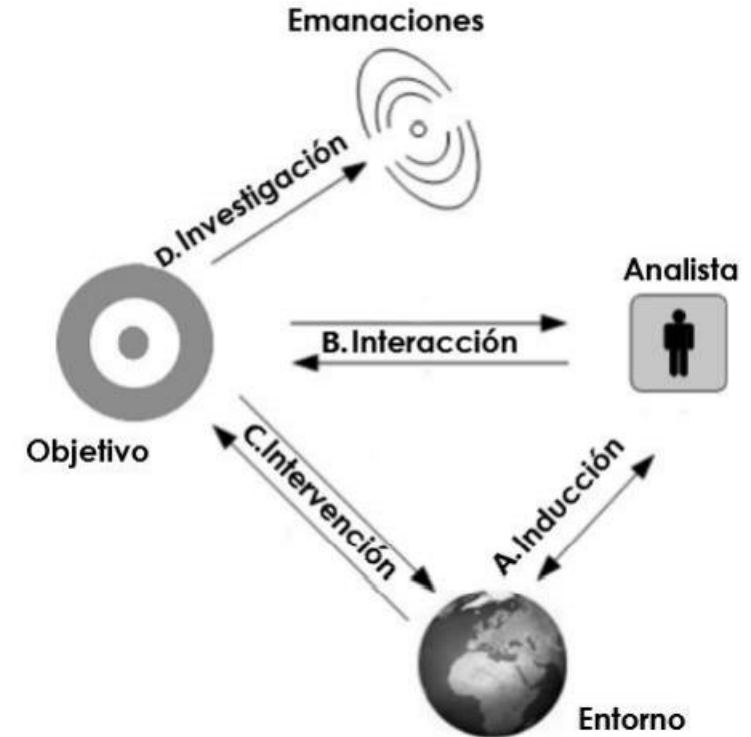
El proceso de cuatro puntos considera el **análisis del entorno**, la **interacción directa**, las **emanaciones del objetivo** y la **modificación del ambiente**, asegurando una revisión integral.

a- Fase de inducción

El Analista estudia el entorno donde reside el objetivo, debido a que de una manera y otra condiciona su comportamiento y muchas veces dicho comportamiento deriva directamente de la influencia que recibe del ambiente. El entorno puede ser un sitio web, se debe identificar cual es el sitio web que se va a evaluar.

b- Fase de interacción

Interactuar directamente con el objetivo y observar las respuestas obtenidas. La interacción puede ser haciendo consultas, aplicando pruebas en el módulo de control de acceso, ver cómo responde, realizando conexiones de distintas formas, a través de distintos protocolos. Esta fase define el alcance.



OSSTMM

Las fases de prueba de la OSSTMM

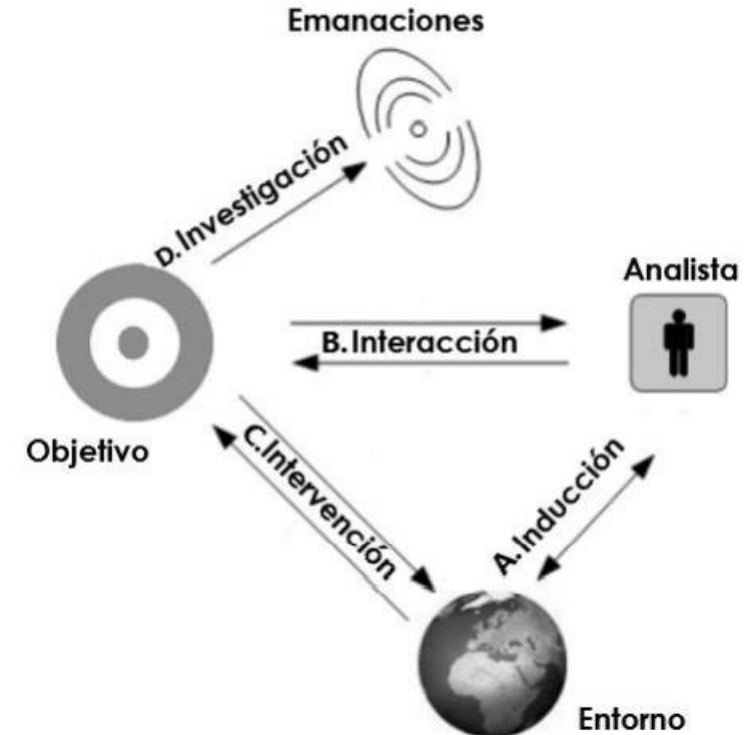
El proceso de cuatro puntos considera el **análisis del entorno**, la **interacción directa**, las **emanaciones del objetivo** y la **modificación del ambiente**, asegurando una revisión integral.

c- Fase de investigación

Analizar las emanaciones que provengan del objetivo, así también como cualquier pista o indicador de las emanaciones mencionadas.

d- Fase de intervención

Estas pruebas se centran en los recursos que los objetivos requieren en el alcance. Modificar los recursos del entorno que necesita el objetivo y observar cómo responde.



OSSTMM CANALES

Un análisis completo de seguridad requiere una evaluación de los canales humano, físico, medios inalámbricos, telecomunicaciones y redes de datos.

En la práctica el analista de seguridad puede abarcar sólo algunos canales.

Un objetivo de cumplimiento en las pruebas de seguridad en los distintos canales es la medición de brechas con el estándar de seguridad requerido descrito en la política de la empresa, las regulaciones del sector o la legislación regional.

OSSTMM Cumplimiento

El cumplimiento es la alineación con un conjunto de políticas generales, donde el tipo de cumplimiento requerido depende de la región y el gobierno actual, la industria y los tipos de negocios y la legislación de respaldo.

El OSSTMM reconoce tres tipos de cumplimiento:



OSSTMM Informe con el reporte STAR

STAR es el informe de auditoría de pruebas de seguridad.

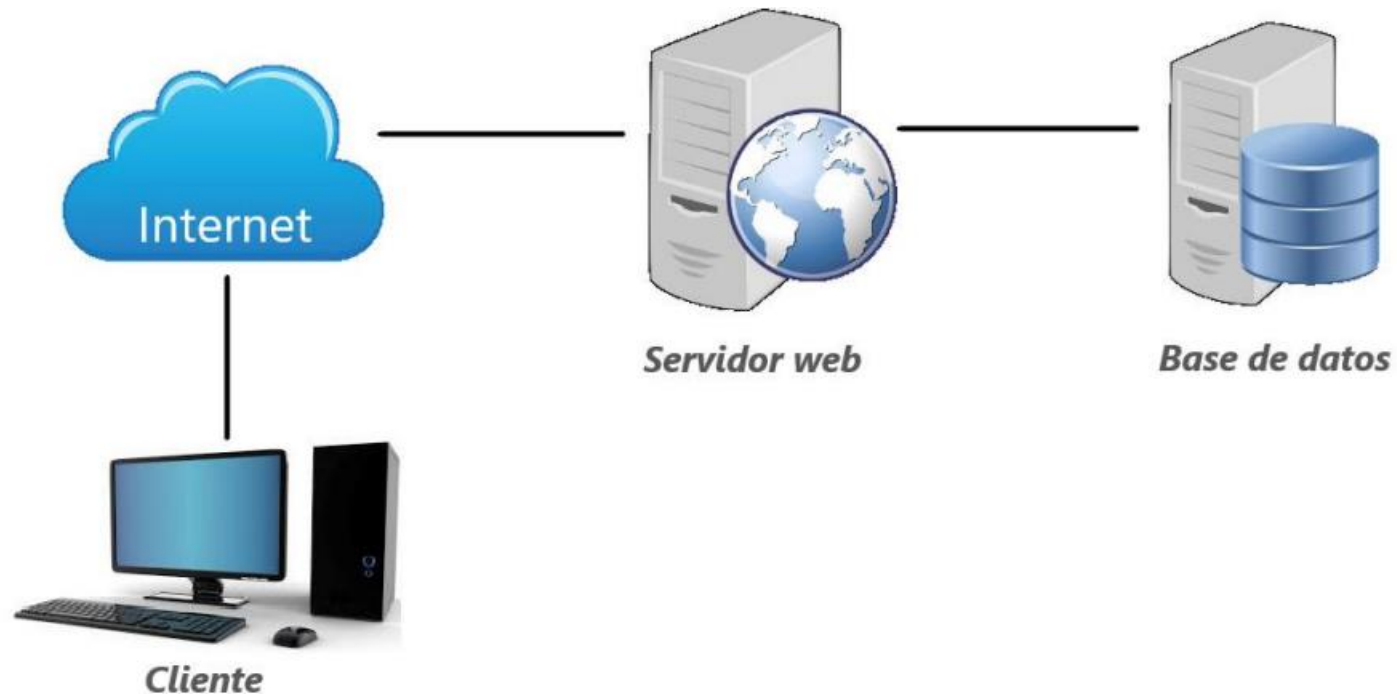
Hace referencia a las palabras en inglés Security Test Audit Report.

Su propósito es presentarse como un resumen ejecutivo el cálculo preciso que indique la superficie de ataque de los objetivos probados dentro de un alcance particular.

OSSTMM

Caso de estudio: prueba de seguridad en la infraestructura

A continuación, se mostrará un ejemplo simple donde se analizará la seguridad desde el punto de vista de la infraestructura. El esquema del ejemplo es como sigue:



OSSTMM

Caso de estudio: prueba de seguridad en la infraestructura

La estructura consta de las siguientes partes:

- Un servidor web corriendo una aplicación que puede ser accedida a través de Internet.
 - Servidor Apache
 - Soporte para PHP
 - Sólo permite conexiones HTTPS
- El servidor responde mensajes ICMP echo request/reply (ping)
 - Una base de datos que contiene la información de la aplicación.
 - Servidor MySQL
 - Sólo tiene en escucha al puerto 3306
 - No responde pings.

OSSTMM

Seguridad operacional

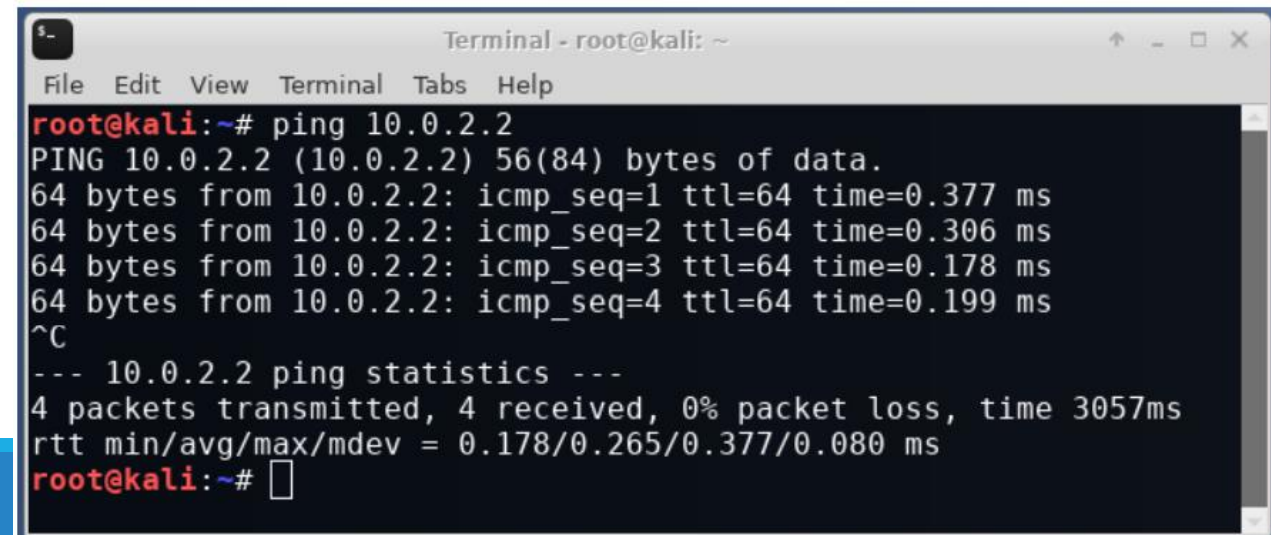
El análisis será sobre la infraestructura y no sobre las posibles interacciones de la aplicación web que pueda estar corriendo sobre el servidor.

a- Acceso

Contar todos los puntos de acceso por cada lugar de interacción. Con las herramientas NMAP y Ping es posible determinar los puertos abiertos del servidor expuesto a internet y la respuesta a ICMP echo request/reply.

Comando 1: ping servidorweb

Resultado: Host activo



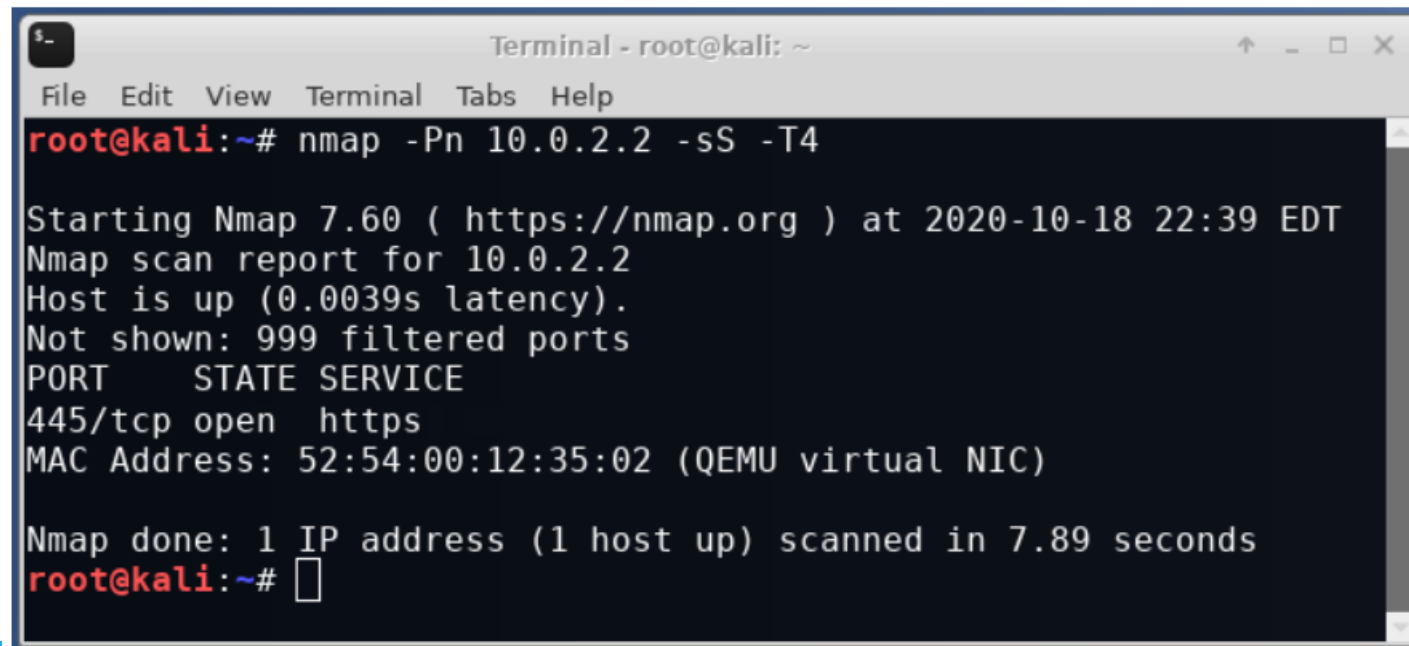
```
Terminal - root@kali: ~
File Edit View Terminal Tabs Help
root@kali:~# ping 10.0.2.2
PING 10.0.2.2 (10.0.2.2) 56(84) bytes of data.
64 bytes from 10.0.2.2: icmp_seq=1 ttl=64 time=0.377 ms
64 bytes from 10.0.2.2: icmp_seq=2 ttl=64 time=0.306 ms
64 bytes from 10.0.2.2: icmp_seq=3 ttl=64 time=0.178 ms
64 bytes from 10.0.2.2: icmp_seq=4 ttl=64 time=0.199 ms
^C
--- 10.0.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3057ms
rtt min/avg/max/mdev = 0.178/0.265/0.377/0.080 ms
root@kali:~#
```

OSSTMM Seguridad operacional

Comando 2: `nmap -Pp servidorweb -sS -T4`

Resultado: Puerto abierto 443, el resto de los puertos están cerrados.

Accesos: 2 → puerto 443 y respuesta a ping

A terminal window titled "Terminal - root@kali: ~" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows the command `root@kali:~# nmap -Pn 10.0.2.2 -sS -T4` and its output. The output indicates that the host is up, 999 filtered ports were not shown, and port 443/tcp is open with the service https. The scan was completed in 7.89 seconds.

```
root@kali:~# nmap -Pn 10.0.2.2 -sS -T4

Starting Nmap 7.60 ( https://nmap.org ) at 2020-10-18 22:39 EDT
Nmap scan report for 10.0.2.2
Host is up (0.0039s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
443/tcp   open  https
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 7.89 seconds
root@kali:~#
```


OSSTMM Seguridad operacional

b- Visibilidad

Contar todos los puntos visibles dentro del objetivo. Existe un solo host visible desde internet y es el que está directamente expuesto a la web.

Pero como existe la posibilidad de interactuar con la base de datos a través del servidor web se puede determinar claramente que existe un servidor de base de datos, por lo tanto, la visibilidad cuenta como 2.

Visibilidad: 2 → servidor web y servidor de base de datos

c- Confianza

Contar cada punto de confianza por cada lugar de interacción. El único punto de confianza que existe es la comunicación entre el servidor de base de datos y el servidor web.

Confianza: 1 → comunicación entre el servidor de base de datos y el servidor web

OSSTMM Controles

Controles en el servidor HTTPS

a- **Confidencialidad:** El protocolo https provee confidencialidad debido a que la información que es transmitida entre el cliente y el servidor se encuentra encriptada. El control de privacidad no se aplica, debido a que no se protege el método de comunicación; es decir, un atacante puede saber que el protocolo usado es https, aunque no pueda determinar el contenido.

- Suma 1 a los controles.

b- **Integridad:** El protocolo https provee integridad ya que una modificación no autorizada en los datos sería detectada por el mismo.

- Suma 1 a los controles.

c- **Subyugación:** El hecho que la comunicación sea únicamente bajo el protocolo https indica que el control de subyugación es aplicado correctamente. No se permite al cliente elegir la forma de comunicación, el servidor determina que el intercambio de datos se hace bajo https.

- Suma 1 a los controles.

d- **No repudio:** El sistema de logs provisto por Apache provee el control de no repudio.

- Suma 1 a los controles.

OSSTMM Controles

Controles en el servidor de base de datos

e- **Autenticación:** El acceso a la base de datos requiere credenciales válidas, por lo tanto, el control de autenticación está siendo aplicado.

- Suma 1 a los controles.

f- **Subyugación:** El acceso está únicamente permitido entre el servidor web y la base de datos, cualquier otro intento de conexión que no sea por ese medio será denegado.

- Suma 1 a los controles.

OSSTMM Limitaciones

a- **Preocupación:** El servidor web acepta cifrado de 56 bit, que son considerados como débiles.

Suma 1 a las limitaciones.

Conexiones de uso compartido de archivos

Windows usa el cifrado de 128 bits para ayudar a proteger las conexiones de uso compartido de archivos. Algunos dispositivos no admiten el cifrado de 128 bits y deben usar el cifrado de 40 o 56 bits.

- ☐ Usar el cifrado de 128 bits para ayudar a proteger las conexiones de uso compartido de archivos (recomendado)
- ☒ Habilitar el uso compartido de archivos para dispositivos que usan el cifrado de 40 o 56 bits

OSSTMM Limitaciones

b- **Exposición:** El banner obtenido a través de una conexión al servidor https brinda información.

Suma 1 a las limitaciones.

```
misspatricia:~ # telnet 192.168.2.129 80
Trying 192.168.2.129...
Connected to 192.168.2.129.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Sat, 17 Nov 2012 15:46:32 GMT
Server: Apache/2.2.20 (Ubuntu)
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=UTF-8
```

**Servidor Apache 2.2.20
corriendo en un Linux
Ubuntu**

OSSTMM

Calculadora de RAVs de OSSTMM

Posterior a la obtención de los valores, se procede a cargar estos valores de entrada en la planilla que provee ISECOM para el cálculo de RAVs.

Los resultados son calculados automáticamente.

Attack Surface Security Metrics

OSSTMM version 3.0

OPSEC

Visibility	2
Access	2
Trust	1
Total (Porosity)	5

CONTROLS

Class A

Authentication	1	Missing	4
Indemnification	0		5
Resilience	0		5
Subjugation	2		3
Continuity	0		5
Total Class A	3		22


Class B

Non-Repudiation	1	Missing	4
Confidentiality	1		4
Privacy	0		5
Integrity	1		4
Alarm	0		5
Total Class B	3		22

		True Missing	
All Controls Total	6		44
Whole Coverage	12,00%		88,00%

LIMITATIONS

Vulnerabilities	0	Item Value	Total Value
Weaknesses	0	9,800000	0,000000
Concerns	1	5,400000	5,400000
Exposures	1	0,904000	0,904000
Anomalies	0	0,376000	0,000000
Total # Limitations	2		6,3040



True Controls
3,187403

Full Controls
3,187403

True Coverage A
12,00%

True Coverage B
12,00%

Total True Coverage
12,00%



Security Δ
-11,94

True Protection
88,06

Actual Security: 88,15 ravs

OSSTMM Resultados

Existen dos expresiones que permiten realizar una interpretación de los valores obtenidos en la seguridad actual del canal auditado, la primera es Seguridad Δ como se muestra en la ilustración marcada de color rojo, la cual muestra el equilibrio que existe entre los valores numéricos de la porosidad, los controles y las limitaciones, por lo tanto, un delta positivo (+) muestra lo mucho que se gasta en controles o incluso si el exceso de gasto es demasiado en un tipo de control; un delta negativo (-) muestra una falta de controles o que se controlan a sí mismos con limitaciones que no pueden proteger adecuadamente al objetivo.

La otra expresión permite analizar el riesgo de la superficie de ataque es la Seguridad Actual, en donde para el canal auditado posee un valor numérico de 88,15 RAVs, lo que se traduce en una deficiencia del alcance de aproximadamente un 12%; y por tanto se puede asegurar que existe un porcentaje de vulnerabilidades dentro del sistema de seguridad que se maneja dentro de la organización.

OWASP

La Fundación Open Web Application Security Project (OWASP) (2020, 2021, 2022) mantiene metodologías de prueba de PenTesting y guías completas para probar dispositivos web, móviles y de firmware. Cuando se ejecutan correctamente, las metodologías OWASP pueden ayudar a los probadores a identificar una serie de vulnerabilidades en el firmware de una red y en las aplicaciones móviles o web.

NIST

El [Instituto Nacional de Estándares y Tecnología](#) (NIST; 2022) es una agencia dentro del Departamento de Comercio de los Estados Unidos. El objetivo del NIST con respecto a los estándares de seguridad de la información no es establecer una metodología específica, sino crear una serie de estándares de prueba. Si bien se requiere que el gobierno federal cumpla con los estándares del NIST, otras redes a menudo también se adhieren a ellos.

Los estándares NIST deben considerarse el mínimo absoluto, no los únicos estándares que una empresa u otra organización debe cumplir. Cualquier PenTesting certificado debe estar familiarizado con las metodologías de prueba de red y aplicación creadas por NIST.

PTES

El marco del [Estándar de Ejecución de Pruebas de Penetración](#) (PTES; 2014) es una metodología de prueba de PenTesting que abarca siete secciones:

- Interacciones previas al compromiso
- Recopilación de inteligencia
- Modelado de amenazas
- Análisis de vulnerabilidades
- Explotación
- Post-explotación
- Informes

PTES (2012) también proporciona una extensa guía técnica que permite a los Pentester ejecutar la metodología.

PTES Fases de una prueba de penetración

Interacciones previas

Se refiere a la negociación o acuerdo durante la cual se definirán los puntos y la profundidad a evaluar, las fechas de la evaluación, la Carta Blanca, entre otros.

PTES Fases de una prueba de penetración

Recolección de información

Es aquella en la que el ataque se dedicará a obtener y recopilar toda la información posible sobre el objetivo. En esta fase se encuentran la subfase de FootPrinting. Aquí nos encargaremos, por ejemplo, de encontrar información DNS, Whois, RSS, etc. También será el lugar donde llevaremos a cabo los ataques de Ingeniería Social.

PTES Fases de una prueba de penetración

Modelado de amenaza

Se analizan los planes de contingencia, así como el equipo técnico, las instalaciones (redes, hardware y software), así como las herramientas, exploits y payloads disponibles para analizar la efectividad de las diversas vías de ataque disponibles.

PTES Fases de una prueba de penetración

Análisis de Vulnerabilidades

En esta fase, con los datos recogidos en la fase anterior, se buscan las posibles vías y métodos de ataque, conocidos como FingerPrinting (Scanning y Enumeración) así como información sobre usuarios, nombres de equipos, etc.

PTES Fases de una prueba de penetración

Explotación

Ponemos las herramientas a atacar a las vulnerabilidades detectadas para comprometer el sistema y obtener acceso.

PTES Fases de una prueba de penetración

Post-explotación

Es aquella donde se persigue obtener acceso al sistema de manera perdurable en el tiempo de manera que podamos realizar en un tiempo indeterminado el ataque a las vulnerabilidades detectadas. También es el momento en el que se inyecta código malicioso (troyanos, Keyloggers, Virus, worms, etc.) en la/s maquina/s objetivo.

PTES Fases de una prueba de penetración

Informe

Tras la evaluación, con las pruebas recogidas y los test realizados, se procede a analizar los resultados para dar un veredicto final sobre el estado de la seguridad, en los ámbitos analizados.

PTES Características claves y beneficios

- Es un marco de auditoria **muy completo** que cubre la técnica así como otros aspectos importantes de una prueba de penetración, como la influencia del alcance, informando y protegiéndote al auditor de seguridad
- Tiene **instrucciones detalladas** sobre cómo realizar muchas de las tareas que son requeridas para probar con precisión la seguridad de un entorno
- Se forma para auditores de seguridad mediante pruebas de penetración experimentadas por expertos que realizan estas tareas a diario
- Incluye las **tecnologías más comunes**, así **como las que no son tan comunes**
- Es **fácil de entender** y puede adaptarlo a sus propias necesidades de prueba

ISSAF

El [Marco de Evaluación de la Seguridad de los Sistemas de Información \(ISSAF\)](#) es un enfoque especializado para las pruebas PenTesting (Open Information Systems Security Group, 2006). Su extensa guía, que tiene más de 1.200 páginas, establece el marco detrás de esta metodología de prueba. El enfoque comprensible de ISSAF es fácil de personalizar para las organizaciones individuales y los probadores, lo que permite la creación de planes de prueba personalizados. Cualquier probador de penetración que utilice múltiples herramientas debe adherirse a la metodología ISSAF.

Es importante señalar que el ISSAF va mucho más allá de las simples pruebas de PenTesting: también abarca la creación de herramientas que se pueden utilizar para educar a otras personas que tienen acceso a una red. También garantiza que las personas que utilizan una red determinada se adhieran a los estándares legales apropiados.