telecom

ENERGIA ARGENTINA SA

Pentest (Pruebas de Intrusión) Comparativo

Informe Ejecutivo

02/10/2025

Tabla de Contenidos

Objetivos

El objetivo del proyecto es determinar el estado actual de seguridad sobre el alcance definido en el apartado correspondiente. Al mismo tiempo se ofrece una visión comparativa con la última evaluación realizada, identificando y documentando las vulnerabilidades que persisten en el tiempo, asi como las que han sido mitigadas o han surgido desde el análisis anterior. De esta forma se pueden evaluar las mejoras en la seguridad implementadas, y proporcionar recomendaciones específicas para abordar las nuevas amenazas y vulnerabilidades vigentes.

Las actividades del presente análisis fueron llevadas a cabo entre el **15/09/2025** y el **22/09/2025**. El análisis anterior utilizado para la comparación evolutiva fue ejecutado entre el **14/07/2025** y el **30/07/2025**.

Alcance

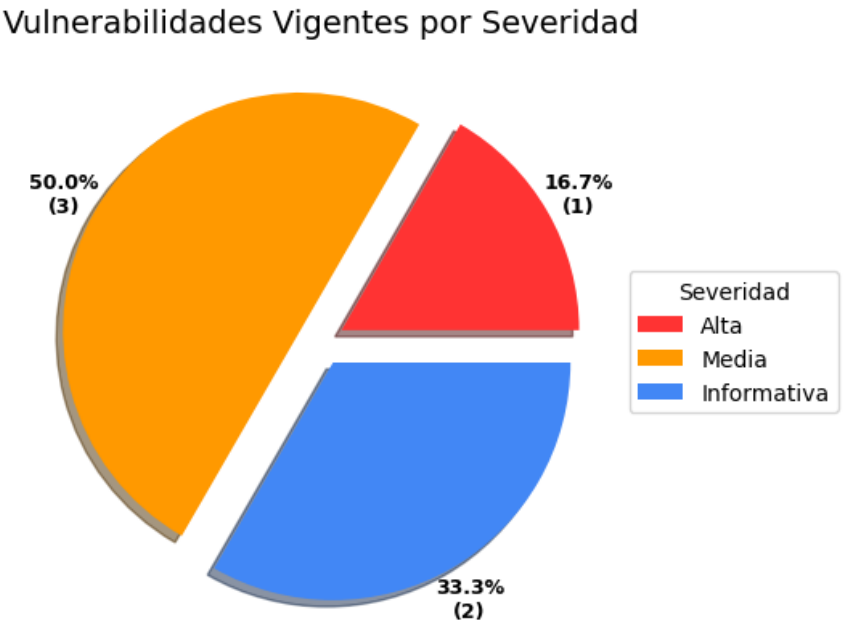
Las siguientes direcciones IP y/o URLs fueron suministradas para realizar una evaluación del tipo Pentest (Pruebas de Intrusión) Comparativo.

190.220.133.1
190.220.133.10
190.220.133.20
190.220.133.22
190.220.133.24
190.220.133.25
190.220.133.3
190.220.133.4
190.220.133.8
200.61.169.65
200.61.169.67
200.61.169.70
200.61.169.71
200.61.169.75
200.61.169.79
200.61.169.81
200.61.169.87
200.61.169.89
200.61.169.90
200.61.169.94

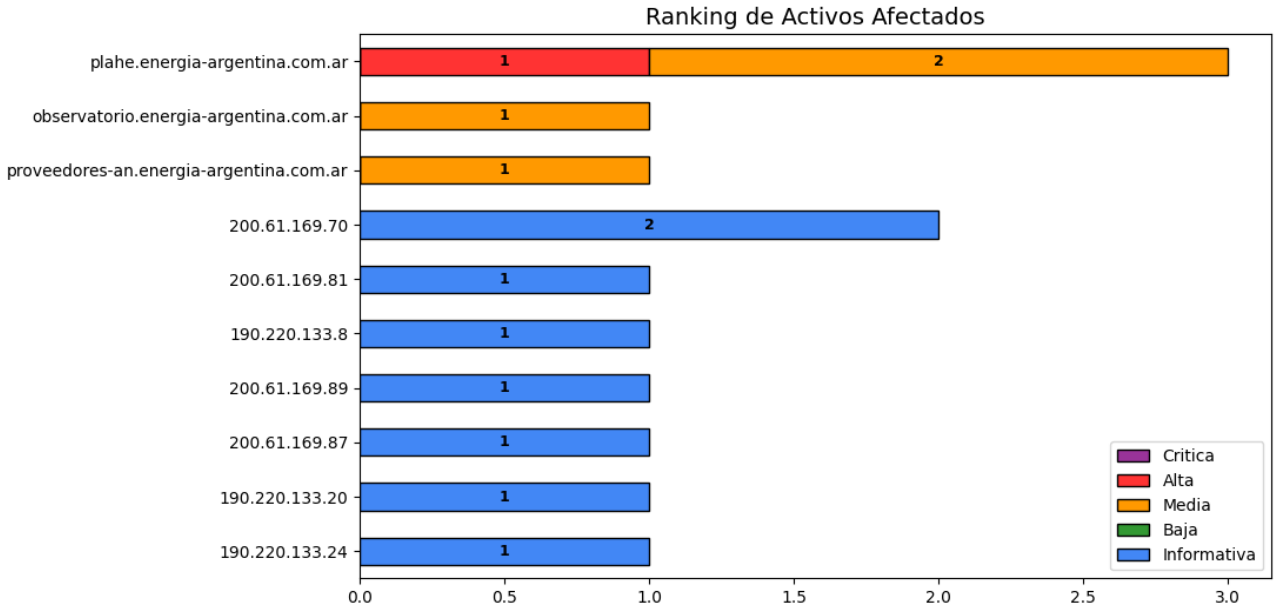
ems.energia-argentina.com.ar
geobservatorio.energia-argentina.com.ar
gpnk.energia-argentina.com.ar
hidroelectricas-argentinas.com.ar
http://observatorio.energia-argentina.com.ar
http://plahe.energia-argentina.com.ar
http://proveedores-an.energia-argentina.com.ar
https://observatorio.energia-argentina.com.ar
https://plahe.energia-argentina.com.ar
https://proveedores-an.energia-argentina.com.ar
intranet.energia-argentina.com.ar
observatorio.energia-argentina.com.ar
plahe.energia-argentina.com.ar
portal.energia-argentina.com.ar
portalproveedores.energia-argentina.com.ar
proveedores-an.energia-argentina.com.ar
vpn.energia-argentina.com.ar
www.energia-argentina.com.ar

Resumen de Hallazgos

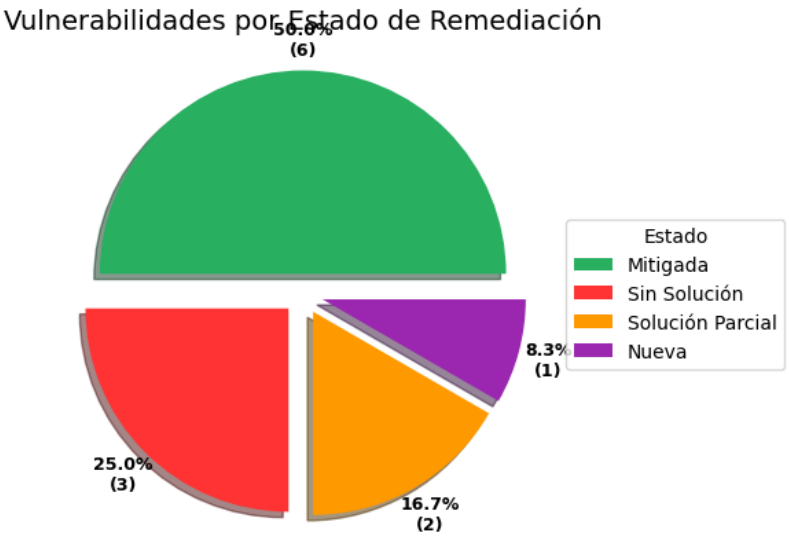
Como resultado del análisis actual se han identificado **6** vulnerabilidades, las cuales presentan la siguiente distribución en cuanto a su severidad: **1** de severidad alta, **3** de severidad media y **2** de carácter informativo.



En el siguiente gráfico se pueden observar los activos afectados que cuentan con mayor cantidad de vulnerabilidades vigentes al momento del último análisis.



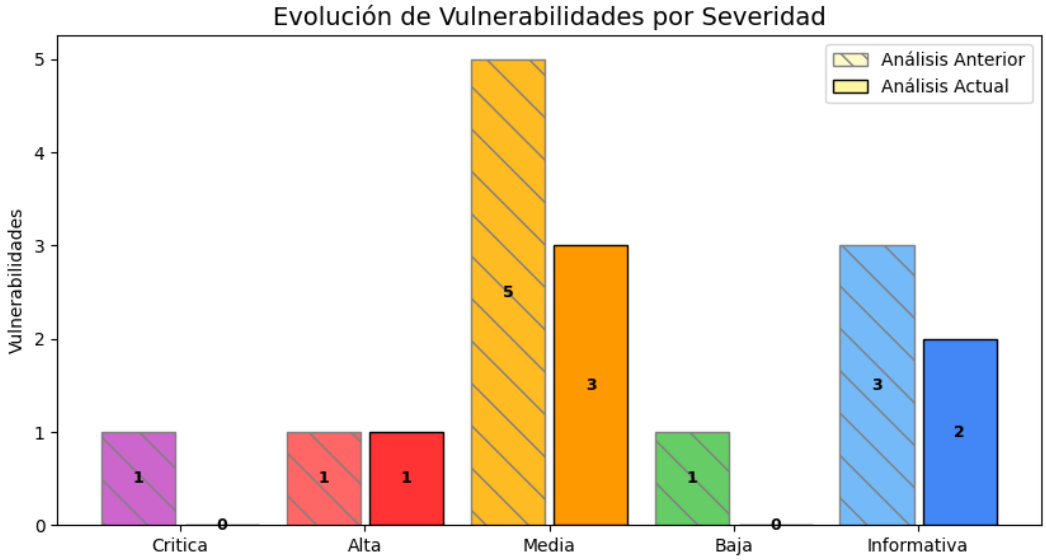
En base a la existencia de las vulnerabilidades detectadas en ambos análisis, y a las medidas de mitigación tomadas entre el informe previo y el actual, se presenta la siguiente clasificación por estado de remediación:



Se utlilizaron las siguientes definiciones para la clasificación:

- Mitigada: La vulnerabilidad fue detectada en el análisis anterior y no fue detectada en el análisis actual.
- Sin Solución: La vulnerabilidad fue detectada en ambas etapas, y sigue existiendo en los hosts y puertos detectados en el análisis anterior.
- Solución Parcial: La vulnerabilidad fue detectada en ambas etapas, pero dejó de detectarse (posible mitigación) en algunos hosts o puertos.
- Nueva: La vulnerabilidad no había sido detectada en el análisis anterior, y se presenta en el análisis actual.

El siguiente gráfico expone la evolución comparativa de las vulnerabilidades detectadas en el análisis anterior y el actual, segregadas por severidad:



Hallazgos

En el siguiente listado se puede visualizar el total de las vulnerabilidades detectadas en ambos análisis clasificadas por #ID.

#ID	Nombre	Severidad	Hosts Afectados Fase Anterior	Hosts Afectados Fase Actual	Hosts Afectados Nuevos	% Mitigación	Estado
1	Hypertext Preprocessor (PHP) Multiple Vulnerabilities	Critica	2	-	-	100%	Mitigada
2	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	Alta	7	-	-	100%	Mitigada
3	Insecure Direct Object Reference (IDOR)	Media	1	1	-	0%	Sin Solución
4	TLS/SSL Weak Cipher Suites	Media	7	-	-	100%	Mitigada
5	Insufficient File Type Validation in File Uploads	Media	1	1	-	0%	Sin Solución
6	GIT Detected	Media	1	2	1	0%	Sin Solución
7	User enumeration	Media	1	-	-	100%	Mitigada
8	Development configuration files	Baja	1	-	-	100%	Mitigada
9	Open TCP Services List	Informativa	6	9	4	17%	Solución Parcial
10	Firewall Detected	Informativa	12	-	-	100%	Mitigada
11	Open UDP Services List	Informativa	2	2	1	50%	Solución Parcial
12	Inyección SQL (SQLi)	Alta	-	1	1	-	Nueva

En el siguiente listado se puede visualizar el total de las vulnerabilidades detectadas en ambos análisis clasificadas por Severidad.

#ID	Nombre	Severidad	Hosts Afectados Fase Anterior	Hosts Afectados Fase Actual	Hosts Afectados Nuevos	% Mitigación	Estado
1	Hypertext Preprocessor (PHP) Multiple Vulnerabilities	**Critica**	2	-	-	100%	**Mitigada**
2	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	**Alta**	7	-	-	100%	**Mitigada**
12	Inyección SQL (SQLi)	**Alta**	-	1	1	-	**Nueva**
4	TLS/SSL Weak Cipher Suites	**Media**	7	-	-	100%	**Mitigada**
6	GIT Detected	**Media**	1	2	1	0%	**Sin Solución**
3	Insecure Direct Object Reference (IDOR)	**Media**	1	1	-	0%	**Sin Solución**
7	User enumeration	**Media**	1	-	-	100%	**Mitigada**
5	Insufficient File Type Validation in File Uploads	**Media**	1	1	-	0%	**Sin Solución**
8	Development configuration files	**Baja**	1	-	-	100%	**Mitigada**
9	Open TCP Services List	**Informativa**	6	9	4	17%	**Solución Parcial**
11	Open UDP Services List	**Informativa**	2	2	1	50%	**Solución Parcial**
10	Firewall Detected	**Informativa**	12	-	-	100%	**Mitigada**

Conclusiones

En base a las vulnerabilidades detectadas en la etapa anterior, se determinó el siguiente nivel de severidad general, dada la existencia de **1** vulnerabilidad con dicha severidad.

Nivel de Severidad Inicial	Critica

Luego de las mitigaciones aplicadas, el nivel de severidad actual se determina en base a la existencia de **1** vulnerabilidad con dicha severidad.

Nivel de Severidad Actual	Alta

A continuación se ofrece un listado de acciones recomendadas para mejorar la postura de seguridad del sistema y reducir el riesgo de explotación:

Acciones Recomendadas
Priorizar la remediación según la clasificación de riesgo.
Desarrollar un plan de acción para implementar la recomendación o remediación.
Realizar un análisis de la causa raíz.
Realizar entrenamiento de concientización.
Realizar el manejo de excepciones y la aceptación de riesgos para las vulnerabilidades que no se pueden remediar.
Volver a realizar el análisis de vulnerabilidades para identificar si las soluciones aplicadas son eficaces para remediar las vulnerabilidades expuestas.
Tener en cuenta las soluciones y referencias recomendadas en cada vulnerabilidad expuesta en este informe.

En base a los resultados obtenidos durante el análisis, se ofrecen las siguientes sugerencias de remediación para abordar y mitigar las vulnerabilidades identificadas:

Sugerencia de Remediación	Vulnerabilidad Abordada
Validar todas las entradas controladas por el usuario, verificando y sanitizando caracteres no permitidos. Establecer los mecanismos de seguridad suficientes para evitar ataques de SQL Injection y de Cross Site Scripting.	**#1 Inyección SQL (SQLi)**
Eliminar o restringir el acceso al directorio .git en entornos productivos.	**#3 GIT Detected**
Validar estrictamente qué campos puede solicitar el usuario, utilizar listas blancas de campos permitidos, y limitar los resultados al modelo autorizado por el rol del usuario.	**#4 Insecure Direct Object Reference (IDOR)**

Sugerencia de Remediación	Vulnerabilidad Abordada
Cuando se disponibiliza un formulario al usuario para subir archivos, realizar validaciones en el backend sobre el tipo de archivo subido, y no permitir tipos de archivos potencialmente inseguros. Además asegurar que los archivos subidos estén libres de malware y código malicioso en general.	**#5 Insufficient File Type Validation in File Uploads**
Restringir la exposición de puertos a los estrictamente necesarios, asegurando que los servicios asociados estén actualizados, correctamente configurados y monitoreados frente a accesos no autorizados.	**#6 Open TCP Services List**
	#7 Open UDP Services List

Recomendaciones Generales

Más allá de los hallazgos obtenidos a través del análisis realizado, resulta crucial establecer un enfoque holístico y multicapa en ciberseguridad. Las recomendaciones que proponemos buscan reforzar su infraestructura de TI y promover una cultura de seguridad resiliente, alineada con las tendencias y prácticas avanzadas del sector, adaptándose así a las dinámicas de un panorama digital que no cesa de cambiar. Recomendamos:

- **Visibilidad, detección y respuesta :** La habilidad para detectar y responder con celeridad a los incidentes de seguridad es fundamental. Contar con un servicio de SOC asegura que esté siempre un paso adelante de los riesgos potenciales.
- **Fortalecimiento de la Infraestructura de Red :** Los puntos débiles identificados en su red pueden fortalecerse de manera significativa a través de Firewalls de última generación y soluciones de seguridad para endpoints. Estas tecnologías son cruciales para una defensa perimetral robusta y ofrecen una protección proactiva contra una variedad de amenazas.
- **Capacitación y Conciencia de Seguridad :** Fomentar la conciencia sobre seguridad entre el personal es esencial, ya que los usuarios informados son la primera línea de defensa. Los programas de formación pueden disminuir de manera significativa el riesgo de brechas de seguridad al educar a los usuarios sobre las mejores prácticas y políticas de seguridad.
- **Análisis Continuo de Vulnerabilidades :** Es vital realizar análisis de vulnerabilidades y pruebas de penetración de forma regular para identificar y mitigar proactivamente las nuevas vulnerabilidades. Esta práctica garantiza la solidez y la adaptabilidad de su infraestructura frente a las amenazas emergentes.
- **Evaluaciones regulares :** Es vital realizar evaluaciones regulares, mantener la seguridad operativa de las plataformas y hardening de los firewalls para protección contra intrusiones. El cumplimiento de los estándares de seguridad es esencial, al igual que revisar los controles de seguridad IT y practicar una gobernanza y gestión de riesgos efectivas. Además, planes de crisis preparados son clave para una respuesta ágil y minimizar impactos en el negocio. Finalmente, tener planes de gestión de crisis bien desarrollados y probados asegura una respuesta rápida y eficaz ante incidentes imprevistos, mitigando los daños y preservando la continuidad del negocio.

Estas recomendaciones están pensadas para ser integradas dentro de un enfoque estratégico de seguridad, garantizando que no solo se atiendan los puntos débiles actuales, sino que también se establezca una base sólida para la seguridad futura. Nuestro equipo de expertos en ciberseguridad está listo para asesorar y apoyar la implementación de estas soluciones, asegurando que su empresa se mantenga a la vanguardia en protección y cumplimiento.

En Telecom, entendemos los desafíos intrincados de la ciberseguridad y estamos equipados para apoyar su empresa en cada paso del camino. Con nuestro portafolio integral y un equipo de profesionales experimentados, nos dedicamos a ayudarlo a alcanzar y mantener una postura de seguridad que no solo responda a las amenazas actuales, sino que también se anticipe y adapte a los riesgos del mañana.

Actividades Realizadas

Las actividades que se realizaron para el presente análisis se separaron en las etapas descriptas a continuación:

Etapa 1: Reconocimiento y Enumeración

En esta etapa se recopiló información sobre los activos informados en el alcance, incluyendo la identificación de rangos de IP, dominios, servidores, y cualquier información pública disponible. La enumeración implica descubrir y mapear activos, servicios y aplicaciones en la red para conformar la superficie de ataque. También se utilizó inteligencia de fuentes abiertas (OSINT) para complementar y ampliar la información obtenida.

Etapa 2: Análisis de Vulnerabilidades

Se utilizaron diferentes herramientas automatizadas para identificar y evaluar los servicios brindados y el tráfico de red en el sistema objetivo. Este proceso puede incluir análisis de código, escaneo de vulnerabilidades, y evaluación de configuraciones de seguridad. El objetivo es identificar debilidades que podrían ser explotadas por un atacante.

A continuación se listan algunas de las debilidades buscadas, sin ser el presente un listado exhaustivo:

- Detección de vulnerabilidades conocidas asociadas a la versión de software de los servicios instalados.
- Verificación de vulnerabilidades conocidas sobre el sistema operativo de base instalado.
- Detección de falta de actualizaciones (parches).
- Detección de errores de configuración o configuraciones predeterminadas.
- Utilización de algoritmos de cifrado inseguros, o ausencia de cifrado.
- Exposición de información.
- Tratamiento incorrecto de entradas manipuladas por el usuario (XSS, Inyección de comandos o código, etc)
- Detección de falencias en el proceso de autenticación.
- Errores en manejo de sesiones de usuario.
- Posibilidad de generar ataques de fuerza bruta.
- Credenciales predeterminadas o conocidas.
- Control de acceso inadecuado o inexistente.

Etapa 3: Modelado de Amenazas

Se utilizaron todos los datos recopilados en las fases anteriores para determinar la posibilidad de explotación. Se determinó el riesgo de las vulnerabilidades descubiertas durante esta fase utilizando principalmente la National Vulnerability Database (NVD), creada y mantenida por el gobierno de EE.UU. que analiza las vulnerabilidades de software publicadas en la base de datos Common Vulnerabilities and Exposures (CVE). La NVD clasifica la gravedad de las vulnerabilidades utilizando el Sistema de Puntuación de Vulnerabilidades Comunes (CVSS). Esta etapa se complementó con verificaciones manuales sobre estos equipos a fin de eliminar los “falsos positivos” y corroborar las detecciones.

Etapa 4: Explotación

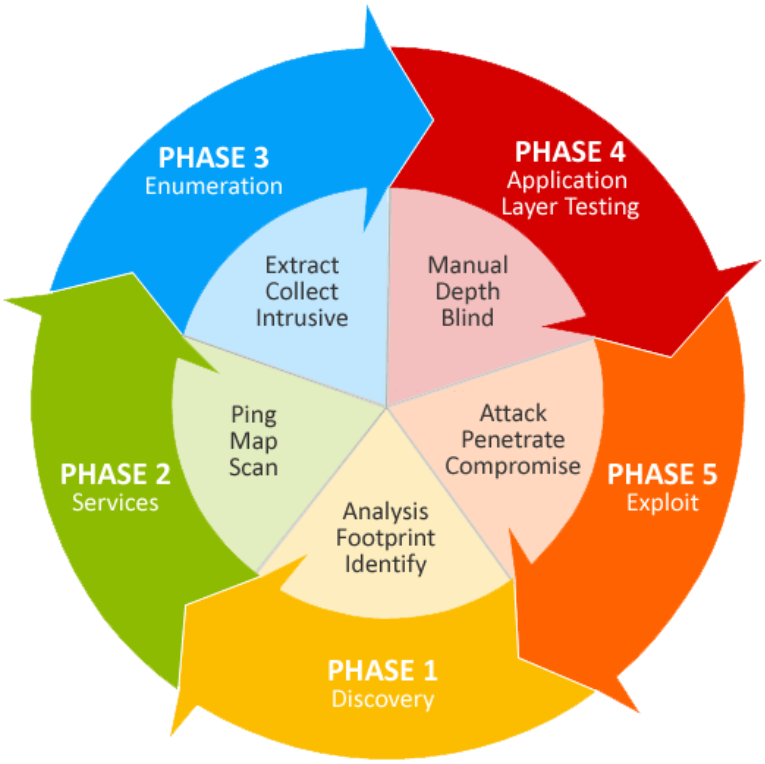
En esta etapa se intentaron explotar las vulnerabilidades identificadas para evaluar la resistencia del sistema a ataques reales. Se buscó determinar si las contramedidas de seguridad eran efectivas y si las vulnerabilidades podían ser explotadas con éxito para validar la profundidad y el alcance de las mismas.

Etapa 5: Informes

Una vez finalizadas las etapas de análisis, se generó un informe ejecutivo con un resumen gerencial de los hallazgos y equipos detectados, junto a un informe técnico donde se describen las vulnerabilidades, detallando el nivel de riesgo asociado, el impacto que estas pudieran tener en la seguridad, las recomendaciones de solución correspondientes, evidencia de las mismas y toda información adicional que fuera considerada útil para su identificación y corrección.

Anexo 1: Metodología

El enfoque utilizado se basa en el Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM), e incluye una combinación de pruebas automatizadas (cuando es posible) y de inspección manual (cuando sea necesario) de los servicios expuestos. El OSSTMM es un estándar ampliamente reconocido y utilizado en la industria de la seguridad informática. Fue desarrollado y publicado inicialmente por el ISECOM (Institute for Security and Open Methodologies) en el año 2001. Proporciona un marco completo y estructurado para llevar a cabo pruebas de penetración y evaluación de la seguridad en sistemas, redes y aplicaciones.



OSSTMM proporciona una serie de escenarios de prueba, técnicas y herramientas para realizar evaluaciones exhaustivas de seguridad. Está diseñado para ser utilizado por profesionales de la seguridad, equipos de pruebas de penetración y auditores de seguridad para identificar vulnerabilidades, evaluar la efectividad de las políticas de seguridad y proporcionar recomendaciones para fortalecer la infraestructura de una organización. Gracias a su enfoque cuantitativo y en detalle, el OSSTMM ha sido adoptado por muchas empresas y organizaciones como una metodología confiable para mejorar la seguridad informática y proteger los activos críticos.

Si bien se trata de un proceso mayoritariamente manual, durante el análisis se utilizaron una serie de herramientas automatizadas que permitieron disminuir los tiempos necesarios para la finalización de las tareas, como así también permitieron la manipulación del tráfico enviado a los servicios analizados.