telecom

SEABOARD ENERGIAS RENOVABLES Y ALIMENTOS SRL

Pentest (Pruebas de Intrusión)

Informe Ejecutivo

25/11/2025

Tabla de Contenidos

Objetivos

El objetivo del proyecto consiste en el descubrimiento y posterior ejecución de un **Pentest (Pruebas de Intrusión)** sobre la infraestructura de **SEABOARD ENERGIAS RENOVABLES Y ALIMENTOS SRL** especificada en el alcance, con la finalidad de identificar debilidades y proponer las recomendaciones de remediación

Las actividades fueron realizadas entre el **08/10/2025** y el **25/11/2025**.

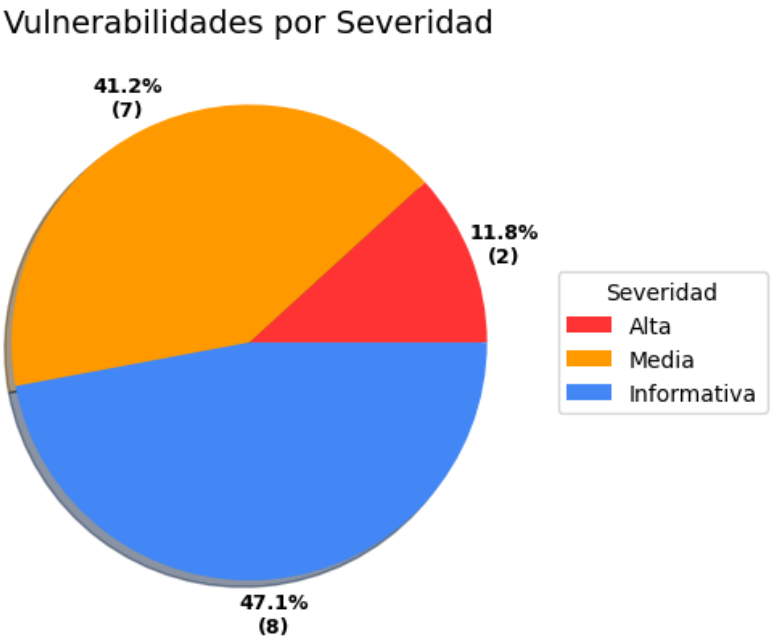
Alcance

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

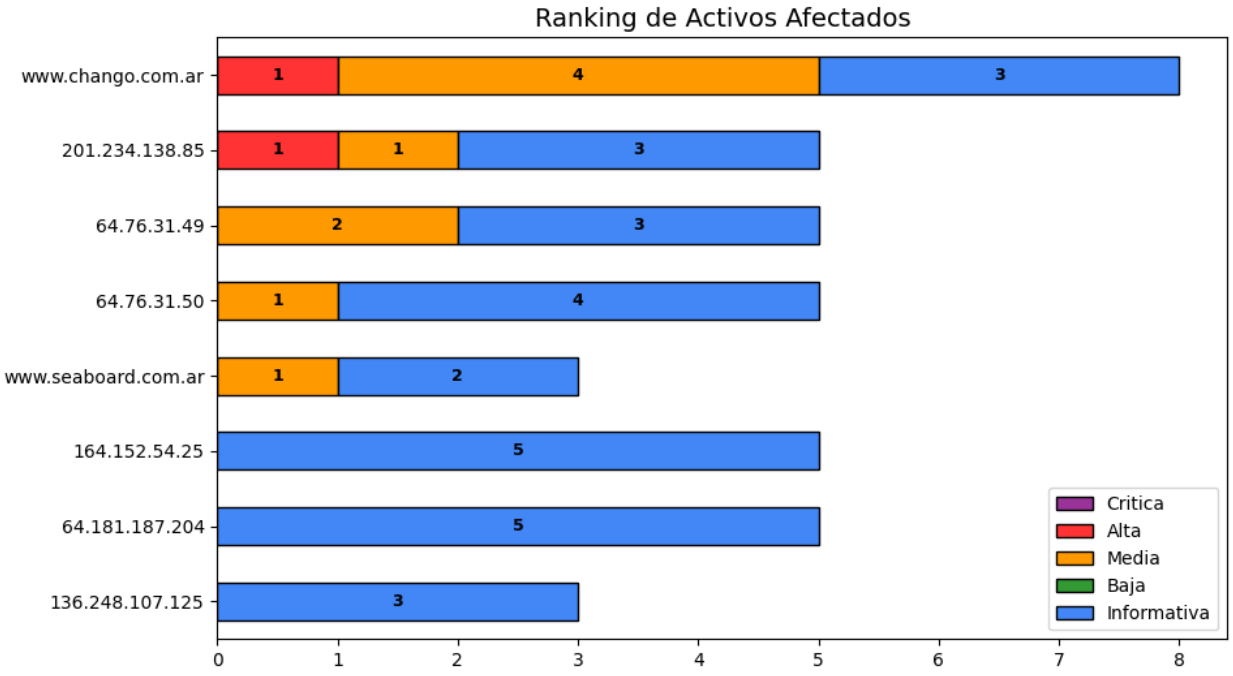
136.248.107.125
164.152.54.25
181.80.16.67
181.80.16.68
200.55.57.197
201.234.138.85
64.181.187.204
64.76.31.49
64.76.31.50
64.76.31.51
64.76.31.52
www.apigdesa.seaboard.com.ar
www.chango.com.ar
www.jdepedidos.seaboard.com.ar
www.seaboard.com.ar

Resumen de Hallazgos

Como resultado del análisis realizado se han identificado **17** vulnerabilidades, las cuales presentan la siguiente distribución en cuanto a su severidad: **2** de severidad alta, **7** de severidad media y **8** de carácter informativo.



En el siguiente gráfico se pueden observar los activos afectados que cuentan con mayor cantidad de vulnerabilidades detectadas.



Hallazgos

En el siguiente listado se pueden visualizar las vulnerabilidades detectadas en el presente análisis clasificadas por Severidad.

#ID	Nombre	Severidad	Hosts Afectados
#1	Information disclosure via api misconfigurations	**Alta**	1
#2	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	**Alta**	1
#3	SSL Certificate - Expired	**Media**	1
#4	SSL Certificate - Signature Verification Failed Vulnerability	**Media**	1
#5	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)	**Media**	2
#6	User enumeration	**Media**	1
#7	Directory Listing	**Media**	1
#8	Host Header Injection	**Media**	1
#9	Frameable response (potential Clickjacking)	**Media**	2
#10	Robots.txt file	**Informativa**	2
#11	List of Web Directories Requiring Authentication	**Informativa**	1
#12	Firewall Detected	**Informativa**	6
#13	Target Network Information	**Informativa**	3
#14	Open TCP Services List	**Informativa**	6
#15	Default Web Page	**Informativa**	6
#16	HTTP TRACE method is enabled	**Informativa**	1
#17	WordPress Plugins Detected	**Informativa**	1

Conclusiones

En base a las vulnerabilidades detectadas y el análisis de las mismas, se puede determinar el siguiente nivel de severidad general, dada la existencia de **2** vulnerabilidades con dicha severidad.

Nivel de Severidad	Alta

A continuación se ofrece un listado de acciones recomendadas para mejorar la postura de seguridad del sistema y reducir los riesgos 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
Es necesario revisar la configuración de la API para garantizar que únicamente se exponga la información estrictamente necesaria para su funcionamiento. Se debe implementar un control adecuado de autenticación y autorización en cada endpoint, evitando respuestas que incluyan datos sensibles o internos del sistema.	**#1 Information disclosure via api misconfigurations**
Deshabilitar el uso de protocolos (SSLv3, TLS1.0, TLS1.1) y algoritmos de cifrado considerados débiles o vulnerables (DES, 3DES, IDEA, CBC, RC2, RC4, MD5, SHA1), en favor de protocolos criptográficamente más fuertes.	**#2 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)**
	#5 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)
Instalar un certificado de servidor con fechas de inicio y final válidas.	**#3 SSL Certificate - Expired**
Instalar un certificado de servidor firmado por una autoridad de certificado de terceros de confianza.	**#4 SSL Certificate - Signature Verification Failed Vulnerability**
Asegurar que los mensajes de errores de acceso, o al intentar recuperar la contraseña, no permitan diferenciar si el usuario existe o no en la aplicación	**#6 User enumeration**
Revisar la configuración de los servidores web y deshabilitar la funcionalidad de listado de directorios en los mismos.	**#7 Directory Listing**

Sugerencia de Remediación	Vulnerabilidad Abordada
Es fundamental validar el encabezado Host recibido en cada solicitud, asegurando que coincida únicamente con el dominio legítimo de la aplicación. Para ello, se recomienda implementar una lista blanca de dominios permitidos en el servidor o en la lógica de la aplicación, evitando confiar en valores proporcionados por el cliente.	**#8 Host Header Injection**
Verificar la correcta implementación de los atributos de seguridad en los Headers HTTP.	**#9 Frameable response (potential Clickjacking)**
Revisar la configuración del firewall aplicando el principio de mínimo privilegio, unificando respuestas a puertos no autorizados y complementando con monitoreo y registros de intentos de escaneo.	**#12 Firewall Detected**
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.	**#14 Open TCP Services List**
Deshabilitar las páginas por defecto que pueden otorgar más información a un atacante, incluyendo aquellas características útiles en entornos de desarrollo que divulgan información.	**#15 Default Web Page**

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.

Durante el proceso, se detectó que algunos hosts no respondieron a las pruebas iniciales, por lo que no fue posible realizar un análisis detallado sobre ellos.

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.

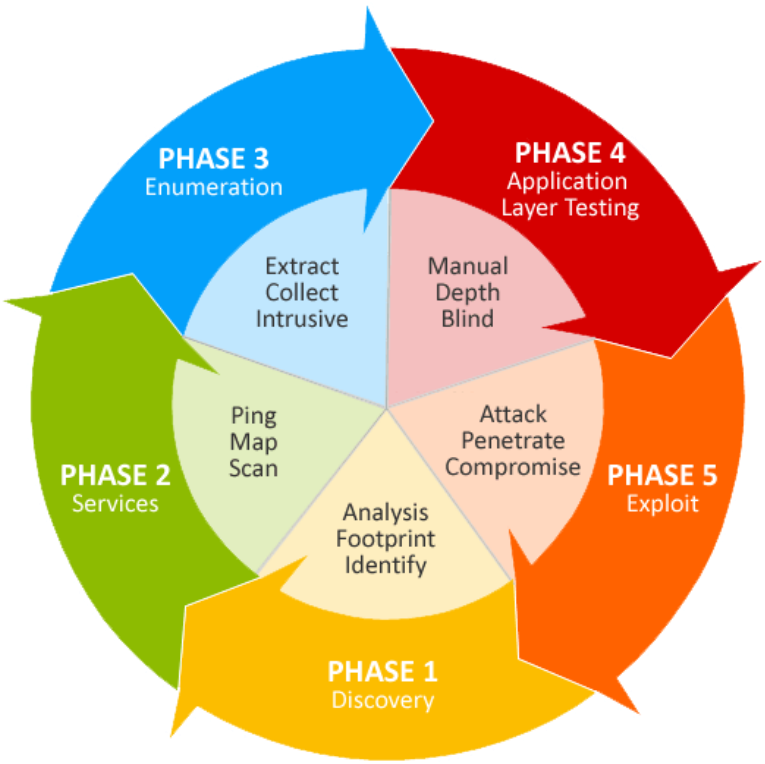
Etapa 5: Informes

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.