

# Informe de Inteligencia

Reconocimiento para Prueba de Penetración



Organización: Grupo Mexx S.R.L

Categoría: Reconocimiento para prueba de penetración

Fecha Inicio: 05-05-2025

Fecha finalización: 03-06-25

Investigador: David Padron

Contacto: pap@pentestingalpalo.pw

# Índice

Declaración de Confidencialidad.....	6
Misión y objetivos de la fase recopilación de inteligencia.....	6
Misión.....	6
Objetivos.....	6
Introducción.....	7
Alcance y Objetivos.....	7
Objetivo de la investigación:.....	7
Alcance de la investigación:.....	7
Se contemplan los siguientes aspectos de investigación:.....	7
Limites de la investigación:.....	8
Metodología.....	8
Técnicas y procedimientos:.....	8
Herramientas para recopilar datos:.....	9
1. Reconocimiento organización:.....	9
2. Reconocimiento huella digital:.....	9
3. Reconocimiento dominios y subdominios:.....	9
4. Reconocimiento Infraestructura de red.....	9
5. Reconocimiento del aplicativo.....	10
6. Reconocimiento de metadatos en archivos.....	10
7. Reconocimiento servidor SMTP.....	10
8. Reconocimiento direcciones de correos electrónicos.....	10
9. Reconocimiento perfiles LinkedIn.....	10
10. Reconocimiento de usuarios.....	10
11. Esquemas y grafos.....	11
Resumen Ejecutivo.....	12
Hallazgos Claves:.....	12
Riesgo:.....	12
Hallazgos.....	14
1. Reconocimiento de la organización.....	14
1.1 Perfil corporativo.....	15
1.2 Ubicación Geoespacial.....	15
1.2.1 Vista física.....	16
1.3 Información impositiva.....	16
1.3.1 Datos de Identificación.....	16
1.3.2 Información de AFIP.....	16
1.5 Registro de Marca.....	17
1.5.1 [REDACTED].....	17
1.5.2 [REDACTED].....	18
1.5.3 [REDACTED].....	18
1.5.4 Análisis de Inteligencia.....	19
1.6 Directivos.....	19
2. Reconocimiento Infraestructura General.....	20
2.1 Dominio [REDACTED].....	20
2.2 Domain Whois Record.....	20
2.3 Network Whois Record.....	21
2.4 DNS Servers.....	21
2.4.1 Reconocimiento DNS.....	22
2.4.2 Análisis de Seguridad.....	23

1. Ausencia [REDACTED]	23
2. Exposición [REDACTED]	24
3. Política [REDACTED]	24
2.4.3 Interpretación en contexto de Seguridad	24
2.5 IP Lookup	24
2.5.1 Filtración [REDACTED]	25
2.5.2 TraceRoute	26
Dominio [REDACTED]	26
Dominio [REDACTED]	26
Dominio [REDACTED]	26
2.6 Certificado SSL	27
2.7 Geolocalización IP	27
2.8 Tecnologías Web	28
2.9 Firewall (WAF)	29
2.9.1 [REDACTED]	29
2.9.2 [REDACTED]	29
2.10 Enumeración de URLs [REDACTED]	30
2.10.1 Login Administrador	31
Análisis de Inteligencia	31
2.10.2 Rutas Administración	32
Rutas [REDACTED]	32
2.10.3 URLs [REDACTED]	35
2.10.4 Amazon [REDACTED]	36
2.11 Vulnerabilidades detectadas	37
2.11.1 [REDACTED]	37
2.11.2 [REDACTED]	38
2.11.3 [REDACTED]	39
2.12 Descubrimiento de directorios	39
2.12.1 F [REDACTED]	39
2.12.2 F [REDACTED]	41
2.12.3 F [REDACTED]	41
2.12.4 Análisis de Inteligencia	42
2.13 Enumeración de Subdominios	42
3. Reconocimiento Puertos de Red	44
3.1 Dirección IP [REDACTED]	44
1. Reconocimiento Subdominios	46
1.1 [REDACTED]	46
1.2 Domain Whois Record	46
1.3 Network Whois Record	48
1.4 DNS Servers	50
2.4.1 Reconocimiento DNS	50
2.5 IP Lookup	52
2.5.2 TraceRoute	52
Dominio [REDACTED]	52
2.6 Certificado SSL	52
2.7 Geolocalización IP	53
2.8 Tecnologías Web	53
2.9 Firewall (WAF)	53
2.10 Enumeración de URLs	54
3. Reconocimiento Puertos de Red	55

3.1 Dirección IP [REDACTED].....	55
3.2 Análisis de Riesgo.....	58
3.2.1 Resumen de Riesgo:.....	58
3.2.2 A [REDACTED].....	59
CVEs Relevantes.....	59
3.2.3 [REDACTED].....	59
CVEs Relevantes.....	59
3.2.4 [REDACTED].....	60
CVEs Relevantes.....	60
3.2.5 [REDACTED].....	60
3.2.6 [REDACTED].....	60
CVEs Relevantes.....	60
3.2.7 [REDACTED].....	60
3.2.8 [REDACTED].....	61
3.3 Conclusión de Riego.....	61
4. Filtraciones de Datos.....	62
4.1 [REDACTED].....	62
4.2 [REDACTED].....	62
4.2.1 J [REDACTED].....	62
5. Infraestructura de red.....	64
5.1 Topología de la empresa.....	64
5.1.1 Datos relevantes de infraestructura.....	64
5.1.2 Análisis de seguridad.....	65
5.2 Arquitectura de red.....	66
5.3 Análisis de riesgo.....	66
5.3.1 Enumeración de posibles riesgos.....	67
Aplicación web.....	67
Servidor e infraestructura de red.....	67
Datos.....	68
Continuidad del negocio.....	68
1. Reconocimiento Subdominios.....	68
1.1 [REDACTED].....	68
1.2 Domain Whois Record.....	68
1.3 Network Whois Record.....	69
1.4 DNS Servers.....	69
1.5 IP Lookup.....	69
1.6 Certificado SSL.....	69
1.7 Geolocalización IP.....	69
1.8 Tecnologías Web.....	69
1.9 Firewall (WAF).....	71
1.10 Enumeración de URLs.....	71
1.10.1 Landing Page.....	72
1.10.2 Login Administrador.....	72
1.10.3 Login Clientes.....	74
1.11 Vulnerabilidades detectadas.....	74
1.11.1 [REDACTED].....	74
POC:.....	75
Análisis URL (Threat Intelligence).....	75
1.11.2 [REDACTED].....	77
1.11.3 [REDACTED].....	79

[REDACTED]	79
[REDACTED]	79
[REDACTED]	79
1.11.4 URL [REDACTED]	80
1.11.5 [REDACTED]	80
Explotación [REDACTED]	80
Explotación y Pruebas de Concepto (POC)	82
A. [REDACTED]	83
1. Explotación	83
1.1 Payload de explotación	83
1.2 [REDACTED]	83
1.3 Explotación	86

## **Declaración de Confidencialidad**

Este documento contiene información recopilada y analizada durante la fase de reconocimiento para la posterior prueba de penetración. El contenido incluye información de carácter público relacionado con potenciales vulnerabilidades y brechas de seguridad detectadas en los sistemas de Grupo Mexx S.R.L. Se recomienda manejar este documento con medidas especiales de protección, garantizando su confidencialidad y restringiendo su acceso únicamente a personal autorizado.

## **Misión y objetivos de la fase recopilación de inteligencia**

### **Misión**

La misión de la fase de recopilación de inteligencia es obtener, validar y estructurar información pública y accesible sobre el objetivo que permita construir una base de conocimiento operativa y accionable para el equipo de pentesting. El propósito es maximizar el entendimiento de la superficie de ataque sin generar interacción detectable con los activos objetivo.

### **Objetivos**

Recopilar datos relevantes sobre la infraestructura, aplicaciones, servicios y personal asociados al objetivo.

Verificar y filtrar la información para eliminar ruido y falsos positivos.

Correlacionar hallazgos técnicos y humanos para identificar vectores de entrada prioritarios.

Generar productos de inteligencia operativa (TTPs, escenarios de ataque y playbooks) que orienten la fase de explotación.

Documentar evidencia y fuentes para facilitar la reproducibilidad y auditoría del proceso.

# Preámbulo

## Introducción

Este informe presenta los resultados de la fase de **Intelligence Gathering** realizada por el OSINT Pentester. Contiene la metodología aplicada, las fuentes y herramientas utilizadas, los datos recolectados, el análisis y la inteligencia producida —orientada a apoyar las decisiones operativas del Red Team durante la ejecución de la prueba de penetración. Se incluyen priorizaciones, escenarios de ataque plausibles, y recomendaciones tácticas para su reutilización por el equipo técnico.

## Alcance y Objetivos

### Objetivo de la investigación:

El objetivo de la investigación es llevar a cabo un reconocimiento de infraestructura informática que permita analizar la superficie de ataque del objetivo para detectar fallos y vulnerabilidades de seguridad que posteriormente serán utilizados por el equipo de pentesters para desarrollar las pruebas de concepto. Este caso se desempeñara tanto el reconocimiento como la prueba de penetración de tipo “Black Box”, sin ningún traspaso previo de información por parte de la empresa objetivo.

### Alcance de la investigación:

Para esta fase de reconocimiento se emplearan técnicas y procedimientos de recolección de datos pasivo y activos controlados, buscando minimizar el impacto de las operaciones sobre la infraestructura del objetivo.

### Se contemplan los siguientes aspectos de investigación:

- Datos generales de la organización
- Detección y enumeración de dominios, subdominios, direcciones ip
- Geolocalización de direcciones ip
- Identificación de tecnologías en servidores y aplicativos
- Consulta de registros DNS, MX, certificados SSL
- Descubrimiento de puertos de red
- Enumeración de URLs, Endpoints y APIs
- Análisis de metadatos en archivos
- Configuración de seguridad en servidor SMTP

- Reconocimiento de direcciones de correo electrónico, perfiles de linkedin
- Investigación de perfiles ejecutivos

## **Limites de la investigación:**

- Acceso a cuentas de Google, Gmail, logins CMS, redes sociales
- Técnicas y procedimientos de ingeniería social para obtener información
- Denegaciones de servicio
- Modificación de configuraciones de seguridad en servidores o aplicativos
- Defacement

## **Metodología**

El proceso de investigación que conlleva recopilar, analizar y generar inteligencia sobre la organización objetivo se lleva a cabo mediante una metodología estándar que consta de los siguientes pasos:

1. Planificación — Elección del objetivo.
2. Recolección pasiva — Fuentes y técnicas pasivas.
3. Recolección activa controlada — Sondeos ligeros, enumeración no intrusiva.
4. Normalización y almacenamiento — Estructura de los datos recolectados.
5. Análisis y correlación — Herramientas y criterios para unir evidencias.
6. Producción de inteligencia — Escenarios, vectores, oportunidades

## **Técnicas y procedimientos:**

Para el siguiente reconocimiento se pretende utilizar diferentes técnicas y procedimientos que incluyen herramientas online y de terminal (CLI) para la obtención de información general de la empresa, datos impositivos, registro de marca, cúpula ejecutiva, cantidad de empleados, entre otros. Por otro lado se pretende analizar la infraestructura de red de la organización, obtención de registros de dominios, registros dns, mx, direcciones ips, enumeración de subdominios, geolocalización de servidores, enumeración de tecnologías, investigación de filtraciones de datos, servidores mal configurados, descubrimiento de endpoints, APIs, URLs, entre otros. Por último se pretende hacer una búsqueda de direcciones de correos electrónicos corporativos y perfilamiento del personal de la empresa.

# Herramientas para recopilar datos:

## 1. Reconocimiento organización:

- Información general: <https://www.zoominfo.com>
- Agentes de IA: GPT, Copilot
- Información impositiva: <https://www.cuitonline.com>, <https://www.dateas.com/es/empresa/cooperativa-electrica-de-monte-ltda-30545697889>, [argentina.gob.ar](http://argentina.gob.ar), [anses.gob.ar](http://anses.gob.ar), [afip.gob.ar](http://afip.gob.ar), [registrocivil.ar](http://registrocivil.ar), [buenosaires.gob.ar](http://buenosaires.gob.ar), [jus.gob.ar](http://jus.gob.ar).
- Información de Marca: <https://portaltramites.inpi.gob.ar/marcasconsultas/busqueda>
- Directivos: dorks

## 2. Reconocimiento huella digital:

- Spiderfoot

## 3. Reconocimiento dominios y subdominios:

- whois (whois)
- dns (dnsx, dnsrecon)
- ip (nslookup, mtr)
- hosts (urlscan, alientvault, virustotal)
- ssl (openssl, ssl-checker)
- cdn/waf (httpx, wafw00f)
- geo (hackertarget, alienvault)
- technologies (whatweb, httpx, wappalyzer)
- urls (katana, gau + wayback + hakrawler)
- subdomains (osintTool, subfinder, dorks, alienvault)
- fuzz directory (wfuzz, pentest-tools)

## 4. Reconocimiento Infraestructura de red

- Shodan, Censys, Fofa
- Nmap

- <https://pentest-tools.com/network-vulnerability-scanning/port-scanner-online-nmap>

## **5. Reconocimiento del aplicativo**

- Burpsuit
- Consola del navegador (browser)
- Código frontend (browser)

## **6. Reconocimiento de metadatos en archivos**

- Exiftool
- Metagoofil

## **7. Reconocimiento servidor SMTP**

- Spoofer
- Espoofer
- Swaks

## **8. Reconocimiento direcciones de correos electrónicos**

- <https://github.com/FeathersMcgr4w/osintTool>
- <https://github.com/m8sec/CrossLinked>
- <https://snov.io/es/buscador-de-correo-electronico>
- <https://github.com/megadose/holehe>
- <https://github.com/mxrch/GHunt>

## **9. Reconocimiento perfiles LinkedIn**

- <https://github.com/FeathersMcgr4w/osintTool>
- <https://www.lusha.com/>
- <https://www.linkedin.com/>

## **10. Reconocimiento de usuarios**

- <https://github.com/sherlock-project/sherlock>

## **11. Esquemas y grafos**

- Maltego
- Gephi
- Drawio

## Resumen Ejecutivo

El siguiente informe de recopilación de inteligencia deriva de una investigación de carácter privado sobre la empresa Grupo Mexx S.R.L en el marco de un trabajo de reconocimiento sobre la infraestructura de red de la organización en busca de fallos y vulnerabilidades de seguridad para su posterior explotación (POC) y análisis de riesgo que derivara en un informe para su posterior reporte a la empresa afectada. El objetivo de este trabajo es alertar y concientizar a la organización afectada sobre los riesgos de seguridad que se acontecen en su infraestructura informática y ofrecer servicios de consultoría por parte de Pentesting Al Palo para remediarlos.

### Hallazgos Claves:

Dentro de la infraestructura de servicios web se identifican los siguientes fallos y vulnerabilidades más críticos:



### Riesgo:

Crítico

Grupo Mexx S.R.L posee un mal ...



# Versión limitada de informe



El presente documento corresponde a una versión resumida y parcialmente anonimizada del informe de investigación desarrollado en el marco de actividades de reconocimiento orientadas a pruebas de penetración sobre Grupo Mexx S.R.L.

El acceso a la versión completa del informe requiere la coordinación previa de una reunión virtual, instancia en la que será posible dialogar directamente con el investigador responsable del trabajo, analizar los hallazgos obtenidos y abordar aspectos técnicos específicos de la investigación.

La publicación de este material tiene como único propósito exponer las capacidades, metodologías y competencias técnicas aplicadas por el investigador en entornos reales. En ningún caso se busca comercializar, divulgar o comprometer información privada, sensible o confidencial de terceros.

Este contenido está dirigido exclusivamente a reclutadores, profesionales de recursos humanos, responsables de contratación y organizaciones interesadas en la contratación de servicios de investigación, ciberinteligencia, pruebas de penetración (pentesting) o propuestas laborales, tanto en modalidad de relación de dependencia como de servicios profesionales independientes.