Informe de Inteligencia

Reconocimiento para Prueba de Penetración

Organización: Cooperativa Eléctrica de Monte LTDA

Categoría: Reconocimiento para prueba de penetración

Fecha Inicio: 05-11-2025

Fecha finalización: 02-12-25

Investigador: David Padron

Contacto: pap@pentestingalpalo.pw

Indice

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 Cooperativa Eléctrica de Monte LTDA. 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, descubrmiento 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
- Modelos 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 ,anses.gob.ar, afip.gob.ar, registrocivil.ar, buenosaires.gob.ar, 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

- Spoofcheck
- 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 Cooperativa Eléctrica de Monte LTDA 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	

La Cooperativa presenta un riesgo crítico para algunos de los servicios de su infraestructura web lo que aumenta las probabilidades de acontecerse ...

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 la Cooperativa Eléctrica de Monte LTDA.

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.