Formato de Auditoría OSINT: Reconocimiento Pasivo de Dominio

Introducción

Objetivo: Realizar un reconocimiento pasivo completo de un dominio utilizando dnsdumpster.com, centrolops.net, FOCA, Shodan, Google Dorks y otras herramientas de OSINT.
Llena cada sección con la información obtenida durante la actividad.

1. Mapeo DNS y Subdominios

Dominio objetivo: lomastravel.com.mx

Fecha de análisis: 14/06/2025

1.1 Subdominios encontrados:

Subdominio	IP	TTL	Ubicación geográfica
admin.lomastravel.com.mx	34.36.139.91	300	Kansas City, US
lomastravel.com.mx.	104.196.208.44	300	North Charleston, US
blog.lomastravel.com.mx	34.74.137.175	300	North Charleston, US

1.2 Name Servers (NS):

ns-cloud-d2.googledomains.com

ns-cloud-d3.googledomains.com

1.3 Registros MX (servidores de correo):

-104.196.208.44

1.4 Registros TXT (SPF, DMARC, etc.):

"v=spf1include:_spf.google.com" "~all."

"google-site-verification=Sq1oXuQ-QNGpYaqDXQlu09ZOjMYCBjjMSIVbhRFvWwE"

"google-site-verification=entUML3CFrKt7IUeW77YV22bWjJptWdechoYOJVy2SM"

2. WHOIS y Datos de Registro

2.1 Registrar: NEUBOX Internet SA de CV

2.2 Fecha de creación: 2009-05-07

2.3 Fecha de expiración: 2026-05-06

2.4 Estado del WHOIS (público/privado): _____

2.5 Contacto Técnico: Viajes Turquesa del Caribe Mexicano SA de CV

2.6 Contacto Administrativo: Viajes Turquesa del Caribe Mexicano SA de CV

3. Metadatos de Documentos (FOCA)

3.1 Lista de documentos recuperados (nombre y URL):

Nombre de documento	URL	Metadatos clave (Autor, Software, Fechas)
Brochure GL Web	https://www.lomastravel.com.mx/pdf/Brochure_GL_Web.pdf	Adobe InDesign CC
RENTA_BURRITOS_SC.pdf	https://admin.lomastravel.com.mx/pdf/productos/RENTA_BURRITOS_SC.pdf	Samantha Fachey, Office XP
REPERTORIO_SAXOFON.pdf	https://admin.lomastravel.com.mx/pdf/productos/REPERTORIO_SAXOFON.pdf	Usuario, MS Office XP, Adobe InDesign
Telefonos_AssistCard_Esp.pdf	https://www.lomastravel.com.mx/pdf/Telefonos_AssistCard_Esp.pdf	

3.2 Hallazgos relevantes de metadatos:

- Rutas internas encontradas: Se detectó una ruta en el dominio admin.lomastravel.com.mx con el nombre de /pdf/

- Autores de documentos: Solamente dos, Samantha Fachey y Usuario

- Software y versiones: versiones de Adobe InDesign y MS Office XP

4. Servicios Expuestos (Shodan)

4.1 Lista de IPs a verificar (extraídas en Sección 1):

- _____

- _____

4.2 Detalle de servicios expuestos:

IP	Puerto	Servicio/Versión	CVE asociadas	Ubicación geográfica
104.196.208.44	22, 80, 443	OpenSSH, Apache HTTPD	CVE-2024-25117, CVE-2022-37454, CVE-2022-31629, CVE-2021-21703	North Charleston, US
34.23.56.146	22, 443	Apache httpd	CVE-2024-25117, CVE-2022-31629, CVE-2022-31628, CVE-2019-9641, CVE-2019-9638	North Charleston, US

4.3 Observaciones adicionales:

- Puertos críticos expuestos: La “devextranet” presenta múltiples fallas criticas principalmente por la versión de PHP, así como el dominio principal. Se encuentra vulnerabilidad del 2016 que puede permitir a atacantes remotos realizar un DoS.

- Versiones vulnerables detectadas:PHP 7.3.x

5. Hallazgos con Google Dorks

5.1 Consultas utilizadas y resultados encontrados:

Consulta Dork	URL/Resultado encontrado

5.2 Descripción de riesgos de cada hallazgo:

- Hallazgo 1: _____

- Hallazgo 2: _____

- Hallazgo 3: _____

6. Recomendaciones de Hardening Inicial

Basado en los hallazgos anteriores, sugerir medidas para mejorar la seguridad:

1. Actualizar versiones de PHP para deshacerse de errores de años pasados.

2. Verificar vulnerabilidades posibles en dev.extranet y en el sistema de ventas.

3. Aplicar reglas firewall para aplicación web

4. Habilitar MFA si no lo tuviera.

7. Conclusión

Resumen de los hallazgos más relevantes y lecciones aprendidas:

Esta práctica me pareció muy interesante porque muchas veces no pensamos en la cantidad de cosas que se pueden hacer con páginas que incluso pueden ser de uso diario y que alguien con el conocimiento suficiente podría aprovechar con fines maliciosos. Me parece interesante el saber que los metadatos pueden arrojar información como nombres completos, correos electrónicos y hasta los softwares que se utilizaron, incluyendo la fecha de creación/modificación de un archivo.