# 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: cancuntravelgroup.com

Fecha de análisis: 10-06-25

Realizado por: Diego Domínguez Ladrón de Guevara IRIYC91

1.1 Subdominios encontrados:

|  |  |  |  |
| --- | --- | --- | --- |
| Subdominio | IP | TTL | Ubicación geográfica |
| vps-909878.cancuntravelgroup.com | 162.240.33.10 | 14400 | Provo, USA |
| b2b.cancuntravelgroup.com | 107.178.221.178 | 14400 | Council Bluffs, USA |
| ns1.cancuntravelgroup.com | 162.240.33.10 | 8128 | Provo, USA |
| bineasy.cancuntravelgroup.com | 44.240.57.238 | 14400 | Boardman, USA |
| cotizador.cancuntravelgroup.com | 44.240.57.238 | 1 | Boardman, USA |

1.2 Name Servers (NS):

- ns1.cancuntravelgroup.com

- ns2.cancuntravelgroup.com

1.3 Registros MX (servidores de correo):

- cancuntravelgroup.com

- mail.cancuntravelgroup.com

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

- apple-domain-verification=eat7RWhvNCem0VQC

- google-site-verification=qBgHw10AFfpraV62JuNA6FWu1r\_Qx6-QpClXW1GEnnk

- v=spf1 include:\_spf.google.com ~all

- v=spf1 ip4:162.240.33.10 +a +mx +ip4:162.241.60.200 +include:websitewelcome.com include:\_spf.criaenvio.com ~all

- v=spf1 ip4:162.240.33.10 +a +mx +ip4:162.241.60.200 ~all

## 2. WHOIS y Datos de Registro

2.1 Registrar: GoDaddy.com, LLC

2.2 Fecha de creación: 14 de julio de 2011

2.3 Fecha de expiración: 14 de julio de 2027

2.4 Estado del WHOIS (público/privado): privado (Domains By Rpoxy, LLC)

2.5 Contacto Técnico: netops@unifiedlayer.com

2.6 Contacto Administrativo: netops@unifiedlayer.com

## 3. Metadatos de Documentos (FOCA)

3.1 Lista de documentos recuperados (nombre y URL):

|  |  |  |
| --- | --- | --- |
| Nombre de documento | URL | Metadatos clave (Autor, Software, Fechas) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

3.2 Hallazgos relevantes de metadatos:

- Rutas internas encontradas: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Autores de documentos: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Software y versiones: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 4. Servicios Expuestos (Shodan)

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

- 162.240.33.10

- 44.240.57.238

4.2 Detalle de servicios expuestos:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP | Puerto | Servicio/Versión | CVE asociadas | Ubicación geográfica |
| 162.240.33.10 | 22 | OpenSSH 7.4 | CVE-2023-38408 (9.8), CVE-2025-26465, CVE-2025-32728, CVE-2023-51767, CVE-2023-51385 | Provo, USA |
| 162.240.33.10 | 22022 | OpenSSH 7.4 | CVE-2023-38408 (9.8), CVE-2025-26465, CVE-2025-32728, CVE-2023-51767, CVE-2023-51385 | Provo, USA |
| 162.240.33.10 | 3306 | MySQL 5.7.41 | CVE-2023-21980 (7.1), CVE-2023-22084, CVE-2023-22028, CVE-2023-22026, CVE-2023-22015 | Provo, USA |
| 44.240.57.238 | 443 | Nginx 1.18.0 | CVE-2023-44487, CVE-2021-23017, CVE-2021-3618 | Boardman, USA |

4.3 Observaciones adicionales:

- Puertos críticos expuestos: 22, 22022, 443

- Versiones vulnerables detectadas: OpenSSH 7.4 y ngginx 1.18.0

## 5. Hallazgos con Google Dorks

5.1 Consultas utilizadas y resultados encontrados:

|  |  |
| --- | --- |
| Consulta Dork | URL/Resultado encontrado |
| site:cancuntravelgroup.com inurl:admin | Ninguno |
| site:cancuntravelgroup.com inurl:cpanel | Ninguno |
| site:cancuntravelgroup.com ext:pdf | Ninguno |
| site:cancuntravelgroup.com ext:docx | Ninguno |
| site:cancuntravelgroup.com ext:xlsx | Ninguno |

5.2 Descripción de riesgos de cada hallazgo:

- Hallazgo 1: Ninguno

## 6. Recomendaciones de Hardening Inicial

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

1. Consolidar registros SPF en uno solo válido y sintácticamente correcto, ya que tener múltiples puede provocar fallos.

2. Reducir TTL a un valor prudente, como 300 o 600 segundos para registros dinámicos. TTL 1 puede generar inestabilidad o sobrecarga en DNS.

3. Actualizar urgentemente OpenSSH a una versión soportada (la 7.4 tiene múltiples CVEs críticos como CVE-2023-38408).

4. Mover el puerto 3306 a una red interna o VPN si no es necesario público.

5. Actualizar a una versión estable más reciente (por lo menos 1.24) para mitigar vulnerabilidades como CVE-2023-44487 (HTTP/2 Rapid Reset).

6. Deshabilitar el acceso SSH si no es necesario públicamente (filtrar por IP o usar VPN).

7. Todos los subdominios con portales de login deben:

* Tener HTTPS forzado (no redirección débil).
* Tener límites de intentos y CAPTCHA.
* Incluir alertas de login y MFA si es posible.
* Validar si el portal está expuesto innecesariamente al público (por ejemplo, /flamingo, /cotizador, etc.).

8. El subdominio b2b.cancuntravelgroup.com redirige a un tercero (xpc.mx): esto debe ser validado contractual y legalmente, y verificar que no haya redirects abiertos (open redirect) o problemas de seguridad cruzada.

## 7. Conclusión

Resumen de los hallazgos más relevantes y lecciones aprendidas:

Esta práctica representó mi primer acercamiento formal a la recolección de información mediante técnicas OSINT en el contexto de una auditoría de ciberseguridad. A lo largo del ejercicio, pude experimentar de manera directa cómo se estructura un proceso de reconocimiento pasivo y activo sobre una infraestructura web, y la importancia de cada dato aparentemente trivial en la construcción de un panorama completo de amenazas.

Una de las principales lecciones fue comprender que la seguridad de un sistema no depende únicamente de sus herramientas o tecnologías, sino también de su configuración, mantenimiento y visibilidad pública. El hecho de utilizar métodos no intrusivos y aun así obtener información significativa me permitió dimensionar el alcance que puede tener un atacante sin necesidad de explotar vulnerabilidades directamente.

Finalmente, esta experiencia me ayudó a desarrollar una mentalidad más crítica respecto a la exposición de sistemas en línea, y reforzó mi interés por seguir profundizando en temas de ciberseguridad, especialmente en áreas como el hacking ético, el hardening de servidores y la evaluación de superficies de ataque.