# Ejemplos de Actividad OSINT: Reconocimiento Pasivo de Dominio

## Introducción

A continuación se muestran ejemplos de los resultados que se deben obtener en cada sección de la actividad.  
Esta guía sirve como referencia para que los estudiantes comprendan el formato y la profundidad del análisis.

## 1. Mapeo DNS y Subdominios (Ejemplo)

Dominio objetivo: biodiversion

Fecha de análisis: 2025/06/05

1.1 Subdominios encontrados:

|  |  |  |  |
| --- | --- | --- | --- |
| Subdominio | IP | TTL | Ubicación geográfica |
| autodiscover.biodiversion.com.mx | 174.127.106.65 | 3600 | USA |
| cpanel.biodiversion.com.mx | 174.127.106.65 | 3600 | USA |
| cpcalendars.biodiversion.com.mx | 174.127.106.65 | 3600 | USA |
| webdisk.biodiversion.com.mx | 174.127.106.65 | 3600 | USA |
| webmail.biodiversion.com.mx | 174.127.106.65 | 3600 | USA |

1.2 Name Servers (NS):

ns3.hubyweb.com

ns4.hubyweb.com

ns1.hubyweb.com

ns2.hubyweb.com

1.3 Registros MX (servidores de correo):

0 biodiversion.com.mx 69.4.234.136 USA

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

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

## 2. WHOIS y Datos de Registro (Ejemplo)

2.1 Registrar: Webzi

2.2 Fecha de creación: 2011-06-23

2.3 Fecha de expiración: 2025-06-23

2.4 Estado del WHOIS (público/privado): Público

2.5 Contacto Técnico:

Nombre: Luis Adrián Solís Contreras

Ciudad: Cancún

Estado: Quintana Roo

País: México

2.6 Contacto Administrativo: Contacto administrativo:

Nombre: Luis Adrián Solís Contreras

Ciudad: Cancún

Estado: Quintana Roo

País: México

## 3. Metadatos de Documentos (FOCA) (Ejemplo)

3.1 Lista de documentos recuperados (nombre y URL):

No se encontraron archivos

## 4. Servicios Expuestos (Shodan) (Ejemplo)

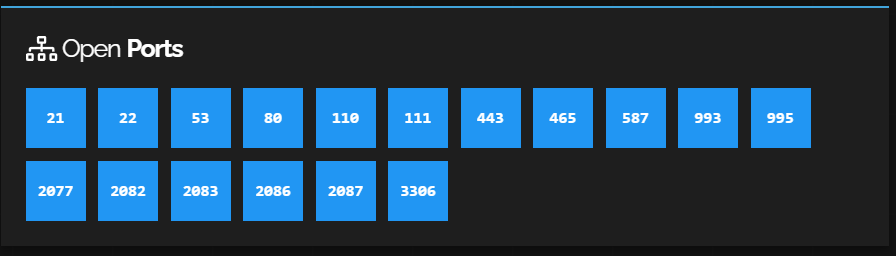
4.1 Lista de IPs a verificar (extraídas en Sección 1):

69.4.234.136

174.127.106.65

4.2 Detalle de servicios expuestos:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP | Puerto | Servicio/Versión | CVE asociadas | Ubicación geográfica |
| 69.4.234.136 | 21 | TCP | [**CVE-2007-2768**](https://www.shodan.io/search?query=vuln:CVE-2007-2768) | USA |



4.3 Observaciones adicionales:

Puertos críticos expuestos: 22 (SSH) en entorno de producción sin restricción de acceso.

Versiones vulnerables detectadas en Apache

## 5. Hallazgos con Google Dorks (Ejemplo)

5.1 Consultas utilizadas y resultados encontrados:

site:biodiversion.com.mx filetype:pdf http://www.biodiversion.com.mx/wp-content/uploads/2015/10/requisitos\_bio\_1.pdf

5.2 Descripción de riesgos de cada hallazgo:

Nada en riesgo

## 6. Recomendaciones de Hardening Inicial (Ejemplo)

1. Restringir puertos.

2. Actualizar Apache a versiones parcheadas que mitiguen las CVEs identificadas.

3. Agregar seguridad https

4. segmentación de red para evitar la centralización de los subdominios.

## 7. Conclusión (Ejemplo)

El dominio **biodiversion.com.mx** presenta varios servicios expuestos y configuraciones que pueden representar riesgos de seguridad, como versiones vulnerables de Apache, puertos abiertos (FTP y SSH) y falta de HTTPS. Además, todos los subdominios están centralizados en una misma IP, lo que representa un punto único de fallo. Se recomienda actualizar software, restringir accesos y aplicar medidas de seguridad (hardening) para reducir vulnerabilidades y proteger la infraestructura.