# 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: utrivieramaya.edu.mx

Fecha de análisis: 2025-06-09

1.1 Subdominios encontrados:

|  |  |  |  |
| --- | --- | --- | --- |
| Subdominio | IP | ASN | Ubicación geográfica |
| cpcontacts.utrivieramaya.edu.mx | 108.179.232.57 | 19871 108.179.232.0/23 | AMAZON-02 United States |
| www.grupoanderson.com | 3.33.251.168 | AMAZON-02 United States | AMAZON-AES United States |
| servicios.utrivieramaya.edu.mx | 186.96.183.196 | 22884 186.96.183.0/24 | TOTAL PLAY TELECOMUNICACIONES SA DE CV, MX Mexico |
| utrmconectado.utrivieramaya.edu.mx | 108.179.232.57 | 19871 108.179.232.0/23 | NETWORK-SOLUTIONS-HOSTING United States |
| www.utrmconectado.utrivieramaya.edu.mx | 108.179.232.57 | 19871 108.179.232.0/23 | NETWORK-SOLUTIONS-HOSTING United States |
| webdisk.utrivieramaya.edu.mx | 108.179.232.57 | 19871 108.179.232.0/23 | NETWORK-SOLUTIONS-HOSTING United States |

1.2 Name Servers (NS):

- ns2.dns-parking.com

- ns1.dns-parking.com

1.3 Registros MX (servidores de correo):

5 utrivieramaya-edu-mx.mail.protection.outlook.com

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

"v=spf1 include:spf.protection.outlook.com -all"

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

2.1 Registrar: IANA -

2.2 Fecha de creación:  2006-04-26

2.3 Fecha de expiración:  2026-04-25

2.4 Estado del WHOIS (público/privado): Público

2.5 Contacto Técnico: UNIVERSIDAD TECNOLOGICA DE LA RIVIERA MAYA

2.6 Contacto Administrativo: UNIVERSIDAD TECNOLOGICA DE LA RIVIERA MAYA

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

3.1 Lista de documentos recuperados (nombre y URL):

|  |  |  |
| --- | --- | --- |
| Nombre de documento | URL | Metadatos clave (Autor, Software, Fechas) |
| Reforma integral | https://utrivieramaya.edu.mx/wp-content/uploads/2024/12/2-REGLAMENTO-DE-LA-LEY-DE-PLANEACION-PARA-EL-DESARROLLO-DEL-ESTADO-DE-QROO.pdf | Autor: OSCAR SANTIAGO SERAPIO; Software: Adobe Acrobat 10; Fecha: creación: 30-07-2008 |
| REGLAMENTO DE LA LEY DE PLANEACION PARA EL DESARROLLO DEL ESTADO DE QROO.PDF | https://utrivieramaya.edu.mx/wp-content/uploads/2024/12/2-REGLAMENTO-DE-LA-LEY-DE-PLANEACION-PARA-EL-DESARROLLO-DEL-ESTADO-DE-QROO.pdf | Autor: ; Software: LOVEPDF 2019; Fecha creación: 17-11-2023 |
| PROGRAMA INSTITUCIONA-UTRM.PDF | https://utrivieramaya.edu.mx/wp-content/uploads/2024/11/PROGRAMA-INSTITUCIONAL-UTRM-2023-2027.pdf | Autor: ; Software: Microsoft PDFIUM; Fecha creación: 27-08-2024 |
| PROGRAMAS DE EDUCACION CONTINUA.PDF | https://utrivieramaya.edu.mx/wp-content/uploads/2024/12/Reglamento\_de\_Programas\_de\_Educacion\_Continua\_SEQ.pdf | Autor: SEQ; Software: Microsoft Office 2007; Fecha creación: 10.1.2014 |

3.2 Hallazgos relevantes de metadatos:

- Rutas internas encontradas: /wp-content/uploads/2024/11/ART91FRXVII-3ER-TRIMESTRE.xlsx

- Autores de documentos:

LILIANA ELIZABETH DE LA CRUZ,OSCAR SANTIAGO SERAPIO

- Software y versiones:

Microsoft Office 2007,LOVEPDF,PEDFIUM

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

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

Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

- 93.184.216.34

- 93.184.216.50

- 192.0.2.10

4.2 Detalle de servicios expuestos:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP | Puerto | Servicio/Versión | CVE asociadas | Ubicación geográfica |
| 93.184.216.34 | 80 | Apache 2.4.46 | CVE-2021-41773 | Los Angeles, CA |
| 93.184.216.34 | 443 | nginx 1.18.0 | CVE-2020-11738 | Los Angeles, CA |
| 93.184.216.50 | 25 | Postfix 3.3.0 | N/A | Los Angeles, CA |
| 192.0.2.10 | 22 | OpenSSH 7.4 | CVE-2018-15473 | Ashburn, VA |
| 93.184.216.60 | 21 | vsftpd 3.0.3 | CVE-2019-12815 | Los Angeles, CA |

4.3 Observaciones adicionales:

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

- Versiones vulnerables detectadas en Apache y nginx.

## 5. Hallazgos con Google Dorks (Ejemplo)

5.1 Consultas utilizadas y resultados encontrados:

|  |  |
| --- | --- |
| Consulta Dork | URL/Resultado encontrado |
| site:utrivieramaya.edu.mx | https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiIuMWTiuWNAxX-38kDHRZ9OcUQFnoECCcQAQ&url=https%3A%2F%2Futrivieramaya.edu.mx%2Fdocumentotitulo%2F&usg=AOvVaw2OCS9DGmt1GN1iKnJPU9WL&opi=89978449 |
| filetype: "pdf"utrivieramaya.edu.mx | https://utrivieramaya.edu.mx/wp-content/uploads/2024/12/Carpeta-Definitiva-Primera-S.E.-2024.pdf |
| site:utrivieramaya.edu.mx intext:"usuario" | intext:"contraseña" | intext:"password" | https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjEwvL4juWNAxVK5ckDHZhPCMM4ChAWegQIExAB&url=https%3A%2F%2Fbuzon.utrivieramaya.edu.mx%2Fopen.php&usg=AOvVaw20O0fZTEAKRLLNFKbs4t00&opi=89978449 |

5.2 Descripción de riesgos de cada hallazgo:

- Hallazgo 1: Posible punto de inyeccion

## 6. Recomendaciones de Hardening Inicial (Ejemplo)

1. Restringir acceso a informacion confidencial.

2. Eliminar o proteger con autenticación el directorio /logs/.

3. Revisar y eliminar archivos con credenciales en texto plano.

## 7. Conclusión

Durante esta actividad se llevo acabo una investigacion de la ciberseguridad de el dominio de utrivieramaya.edu.mx y se encontraron posibles puntos criticos que pueden ser usados malintencionadamente.