# 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: \_\_\_\_abix.mx

Fecha de análisis: \_\_\_\_07/06/2025\_\_\_\_\_\_\_\_\_\_\_

1.1 Subdominios encontrados:

|  |  |  |  |
| --- | --- | --- | --- |
| Subdominio | IP | TTL | Ubicación geográfica |
| acs.abix.mx | 63.245. 105.247 | 54 | TELECOMUNICACIONES S.A. DE C.V., MX México |
| dns1.bix.mx | 63.245.105.251 | 56 | TELECOMUNICACIONES S.A. DE C.V., MX México |
| dns2.bix.mx | 63.245.105.252 | 56 | TELECOMUNICACIONES S.A. DE C.V., MX México |
| ems.abix.mx | 63.245.105.249 | 54 | TELECOMUNICACIONES S.A. DE C.V., MX México |
| gráfico.abix.mx | 63.245.105.254 |  | TELECOMUNICACIONES S.A. DE C.V., MX México |

1.2 Name Servers (NS):

- \_\_\_\_\_en57.domaincontrol.com \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- \_\_\_\_\_\_\_\_\_\_\_\_\_ en58.domaincontrol.com \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.3 Registros MX (servidores de correo):

- 10 aspmx.l.google.com

- 50 aspmx3.googlemail.com

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

- "google-site-verification=PpJ7seWMMEO63L-TjDURmUy9nmX6IC7ZPPtxcVGL\_Gk"

- "\_globalsign-domain-verification=Qk1ilg6O7SYxcHxUZJP966oNVwaEqNSvoK61WuFdoB"

- "v=spf1 include:turbo-smtp.com include:\_spf.smtp.com include:\_spf.google.com ip4:63.245.105.248 +a +mx ~all"

## 2. WHOIS y Datos de Registro

2.1 Registrar: \_\_\_\_\_\_\_\_\_Verizon Business (MCICS)\_\_\_\_\_

2.2 Fecha de creación: \_\_\_\_\_\_\_1998-07-31\_\_\_\_\_\_\_\_

2.3 Fecha de expiración: \_\_\_\_\_\_\_\_N/D\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2.4 Estado del WHOIS (público/privado): \_\_\_\_\_\_\_publico\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2.5 Contacto Técnico: \_\_\_\_\_\_\_SWIPPER\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2.6 Contacto Administrativo: \_\_\_\_\_\_\_\_VZ-DNSADMIN\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 3. Metadatos de Documentos (FOCA)

3.1 Lista de documentos recuperados (nombre y URL):

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

3.2 Hallazgos relevantes de metadatos:

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

- Autores de documentos:

N/D

- Software y versiones:

N/D

## 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 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

4.3 Observaciones adicionales:

- Puertos críticos expuestos: \_\_\_\_\_\_\_\_N/D\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Versiones vulnerables detectadas: \_\_\_\_\_\_ Ciertos paquetes Red Hat Enterprise Linux (RHEL) 4 y 5 para OpenSSH, firmados en agosto de 2008 utilizando una clave legítima Red Hat GPG \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 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: \_\_\_\_\_N/D\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Hallazgo 2: \_\_\_\_\_\_\_\_\_\_N/D\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Hallazgo 3: \_\_\_\_\_\_\_\_\_N/D\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 6. Recomendaciones de Hardening Inicial

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

1. \_\_\_\_\_\_\_\_\_\_actualizaciones\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. \_\_\_\_\_\_\_\_\_\_n/d\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. \_\_\_\_\_\_\_\_\_\_n/d\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 7. Conclusión

Resumen de los hallazgos más relevantes y lecciones aprendidas:

\_\_\_\_\_\_\_TIENEN UNA PROECCION BUENA ALMENOS EN TEMA DE SU PAGINA LA CUAL NO SE PUDO SACAR INFORMACION IMPORTANTE DE LA METADATA\_\_\_\_\_\_\_