# 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: https://www.sitwifi.com/

Fecha de análisis: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1.1 Subdominios encontrados:

|  |  |  |  |
| --- | --- | --- | --- |
| Subdominio  alice.sitwifi.com  cloud.sitwifi.com | IP  34.205.249.28  35.243.154.192 | TTL  ---  --- | Ubicación geográfica  AMAZON-AES United States  GOOGLE-CLOUD-PLATFORM United States |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1.2 Name Servers (NS):

ns-347.awsdns-43.com 205.251.193.91 AMAZON-02  
United States

ns-799.awsdns-35.net 205.251.195.31 AMAZON-02  
United States

1.3 Registros MX (servidores de correo):

-----

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

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

"b0nai9jihb5oh1enq6bt704kdq"

"dr4srbcvj2imjhhne0o0ka7pka"

"enmc5s1u53po6mibnf99tjbcd"

## 2. WHOIS y Datos de Registro

2.1 Registrar: Amazon Registrar, Inc.

2.2 Fecha de creación: 8/29/2008

2.3 Fecha de expiración: 8/29/2025

2.4 Estado del WHOIS (público/privado): PUBLICO

2.5 Contacto Técnico: +44.1483307527

2.6 Contacto Administrativo: +44.1483307527

## 3. Metadatos de Documentos (FOCA)

3.1 Lista de documentos recuperados (nombre y URL):

|  |  |  |
| --- | --- | --- |
| Nombre de documento | URL | Metadatos clave (Autor, Software, Fechas) |
| CODIDGO DE PRACTICA  CVenglish-SITWIFI2021 |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

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):

- \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4.2 Detalle de servicios expuestos:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP | Puerto | Servicio/Versión | CVE asociadas | Ubicación geográfica |
| 35.243.154.192 | 22  80  443  9000 |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

4.3 Observaciones adicionales:

- Puertos críticos expuestos: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Versiones vulnerables detectadas: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 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. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

5. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 7. Conclusión

Resumen de los hallazgos más relevantes y lecciones aprendidas:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_