# 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: www2.aguakan.com

Fecha de análisis: 09/06/2025

1.1 Subdominios encontrados:

|  |  |  |  |
| --- | --- | --- | --- |
| Subdominio | IP | TTL | Ubicación geográfica |
| www2.aguakan.com | 18.215.10.229 | No especifica | El Colorado, Mexico |
| 159.54.136.137 | 159.54.136.137 | No especifica | El Colorado, Mexico |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1.2 Name Servers (NS):

- www2.aguakan.com

- amazonaws.com

1.3 Registros MX (servidores de correo):

- N/A

- N/A

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

- N/A

## 2. WHOIS y Datos de Registro

2.1 Registrar: 83356181\_DOMAIN\_COM-VRSN

2.2 Fecha de creación: 2024-01-23T22:09:03Z

2.3 Fecha de expiración: 2002-02-05T16:21:54Z

2.4 Estado del WHOIS (público/privado): clientTransferProhibited http://icann.org/epp#clientTransferProhibited

2.5 Contacto Técnico: +52.99889147004805, informatica@agukan.com

2.6 Contacto Administrativo: +52.9988914700, informatica@agukan.com

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

## 3. Metadatos de Documentos (FOCA)

3.1 Lista de documentos recuperados (nombre y URL):

|  |  |  |
| --- | --- | --- |
| Nombre de documento | URL | Metadatos clave (Autor, Software, Fechas) |
| IA23-24\_Aguakan\_digital.pdf | <https://www2.aguakan.com/docs/IA23-24_Aguakan_digital.pdf> |  |
| informeanual.pdf | <https://www2.aguakan.com/portal/wp-content/uploads/archivos/informeanual.pdf> |  |
|  |  |  |
|  |  |  |
|  |  |  |

3.2 Hallazgos relevantes de metadatos:

- Rutas internas encontradas: https://www2.aguakan.com/portal/wp-content/uploads

- Autores de documentos: No especifica

- Software y versiones: Documentos PDF

## 4. Servicios Expuestos (Shodan)

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

- 159.54.136.137

4.2 Detalle de servicios expuestos:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP | Puerto | Servicio/Versión | CVE asociadas | Ubicación geográfica |
| 159.54.136.137 | 22, 80, 443 | OpenSSH, Apache | Capturas debajo | El Colorado, Mexico |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

4.3 Observaciones adicionales:

- Puertos críticos expuestos: 22, 80, 443

- Versiones vulnerables detectadas:

Texto

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Sitio web

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

## 5. Hallazgos con Google Dorks

5.1 Consultas utilizadas y resultados encontrados:

|  |  |
| --- | --- |
| Consulta Dork | URL/Resultado encontrado |
| site:www2.aguakan.com filetype:pdf | <https://www2.aguakan.com/docs/IA23-24_Aguakan_digital.pdf> |
| site:www2.aguakan.com "Warning" | "Error" | "Notice" | <https://www2.aguakan.com/crees-que-hubo-un-error-en-tu-factura-del-agua-modulos-y-horarios-para-hacer-una-aclaracion/> |
|  |  |
|  |  |
|  |  |

5.2 Descripción de riesgos de cada hallazgo:

- Hallazgo 1: PDF con un informe de sostenibilidad

- Hallazgo 2: Ayuda con la factura de tu recibo de agua

- Hallazgo 3: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 6. Recomendaciones de Hardening Inicial

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

1. Restringir el acceso a archivos públicos no intencionados

2. Ocultar mensajes de error del servidor

3. Auditoría de indexación de Google

4. Configurar permisos adecuados a nivel de archivos y directorios

5. Establecer políticas de publicación de contenido

## 7. Conclusión

Resumen de los hallazgos más relevantes y lecciones aprendidas:

Se encontraron archivos accesibles desde Google y errores visibles en el sitio. Esto puede dar información útil a atacantes, ya que shodan muestra los CVE. Es importante controlar qué se muestra públicamente y mejorar la configuración del servidor para estar más protegidos.

## 8. Exploits por CVE

CVE‑2017‑3167

Tipo: Bypass de autenticación en Apache HTTPd (módulo ap\_get\_basic\_auth\_pw fuera de contexto).

Exploit público: No disponible.

Impacto: Acceso no autorizado si se da la combinación de versiones vulnerables y módulos específicos.

Mitigación: Actualizar a Apache ≥ 2.4.26 / 2.2.33.

2. CVE‑2017‑7679

Tipo: Lectura fuera de límites en módulo mod\_mime de Apache.

Exploit público: Sí, hay PoC en Perl (CVE\_2017\_7679.pl en GitHub).

Impacto: Posible divulgación de memoria o DoS.

Mitigación: Actualizar a Apache ≥ 2.4.26 / 2.2.33.

3. CVE‑2017‑8923

Tipo: Integer overflow en PHP (zend\_string\_extend) al concatenar cadenas.

Exploit público: Hay exploit disponible; se usan cadenas largas para provocar buffer overflow/DoS.

Impacto: DoS o posible corrupción de memoria.

Mitigación: Actualizar PHP ≥ 7.1.6 (o 7.1.5 corregido).

4. CVE‑2018‑1312

Tipo: Autenticación débil en Apache HTTPd (nonce predecible en Digest auth).

Exploit público: No hay PoC, pero se documenta técnica de replay.

Impacto: Posible reenvío permitido entre servidores del mismo cluster.

Mitigación: Actualizar a Apache ≥ 2.4.30.

5. CVE‑2019‑9641

Tipo: Lectura no inicializada en exif\_process\_IFD\_in\_TIFF (PHP EXIF).

Exploit público: Sin PoC público, aunque explotantes privados existen.

Impacto: RCE teórico o DoS mediante imagen EXIF maliciosa.

Mitigación: Actualizar PHP ≥ 7.1.27, 7.2.16 o 7.3.3.

6. CVE‑2021‑26691

Tipo: Heap overflow en mod\_session de Apache.

Exploit público: No disponible.

Impacto: DoS o posible RCE en escenarios específicos.

Mitigación: Apache ≥ 2.4.47 (parches en distribuciones modernas).