

# 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 específica	El Colorado, Mexico
159.54.136.137	159.54.136.137	No específica	El Colorado, Mexico

A Records (subdomains from dataset)				
Host	IP	ASN	ASN Name	Open
www2.aguakan.com	18.215.10.229	ASN: 14618	AMAZON-AES	https://www2.aguakan.com
	ec2-18-215-10-229.compute-1.amazonaws.com	18.208.0.0/13	United States	https://www2.aguakan.com

### 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

Central Ops.net

Advanced online Internet utilities

Utilities

▼

Domain Dossier

Domain Check

Email Dossier

Browser Mirror

Ping

Traceroute

Nslookup / Dig

Domain Whois record

Queried **whois.internic.net** with "**dom aguakan.com**"...

Domain Name: AGUAKAN.COM

Registry Domain ID: 83356181\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.register.com

Registrar URL: http://www.register.com

Updated Date: 2024-01-23T22:09:03Z

Creation Date: 2002-02-05T16:21:54Z

Registry Expiry Date: 2029-02-05T16:21:54Z

Registrar: Register.com - Network Solutions, LLC

Registrar IANA ID: 9

Registrar Abuse Contact Email: domain.operations@web.com

Registrar Abuse Contact Phone: +1.8777228662

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Name Server: NS-CLOUD-E1.GOOGLEDOMAINS.COM

Name Server: NS-CLOUD-E2.GOOGLEDOMAINS.COM

Name Server: NS-CLOUD-E3.GOOGLEDOMAINS.COM

Name Server: NS-CLOUD-E4.GOOGLEDOMAINS.COM

Name Server: ZAZIL.AGUAKAN.COM

DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>> Last update of whois database: 2025-07-25T19:01:04Z <<<

3. Metadatos de Documentos (FOCA)

3.1 Lista de documentos recuperados (nombre y URL):

Nombre de documento	URL	Meta datos clave (Auto r, Softw are, Fecha s)
IA23-24_Aguakan_digital.pdf	<a href="https://www2.aguakan.com/docs/IA23-24_Aguakan_digital.pdf">https://www2.aguakan.com/docs/IA23-24_Aguakan_digital.pdf</a>	
informeanual.pdf	<a href="https://www2.aguakan.com/portal/wp-content/uploads/archivos/informeanual.pdf">https://www2.aguakan.com/portal/wp-content/uploads/archivos/informeanual.pdf</a>	

Id	Type	URL	
0	pdf	https://www2.aguakan.com/docs/1A23-24_Aguakan_di...	>
1	pdf	https://www2.aguakan.com/portal/wp-content/uploads...	>
2	pdf	https://www2.aguakan.com/portal/wp-content/uploads...	>
3	pdf	https://www2.aguakan.com/portal/wp-content/uploads...	>
4	pdf	https://www2.aguakan.com/portal/wp-content/uploads...	>
5	pdf	https://www2.aguakan.com/portal/wp-content/uploads...	>
6	pdf	https://www2.aguakan.com/portal/wp-content/uploads...	>
7	pdf	https://www2.aguakan.com/portal/wp-content/uploads...	>
8	pdf	https://www2.aguakan.com/portal/wp-content/uploads...	>
9	pdf	https://www2.aguakan.com/portal/wp-content/uploads...	>
10	pdf	https://www2.aguakan.com/portal/wp-content/uploads...	>

### 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:

 **Vulnerabilities**

Port 22 ▾ Latest ▾

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.


 **2025** (2)

**CVE-2025-32728**

**4.3** In sshd in OpenSSH before 10.0, the DisableForwarding directive does not adhere to the documentation stating that it disables X11 and agent forwarding.

**CVE-2025-26465**

**6.8** A vulnerability was found in OpenSSH when the VerifyHostKeyDNS option is enabled. A machine-in-the-middle attack can be performed by a malicious machine impersonating a legit server. This issue occurs due to how OpenSSH mishandles error codes in specific conditions when verifying the host key. For an attack to be considered successful, the attacker needs to manage to exhaust the client's memory resource first, turning the attack complexity high.

 **2023** (4)

**CVE-2023-51767**

**7.0** OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm\_answer\_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user

## Vulnerabilities

Port 80



Latest



Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

### 2024 (6)

**CVE-2024-40898**

**7.5**

SSRF in Apache HTTP Server on Windows with mod\_rewrite in server/vhost context, allows to potentially leak NTLM hashes to a malicious server via SSRF and malicious requests. Users are recommended to upgrade to version 2.4.62 which fixes this issue.

**CVE-2024-38477**


**7.5**

null pointer dereference in mod\_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request. Users are recommended to upgrade to version 2.4.60, which fixes this issue.

**CVE-2024-38476**


**9.8**

Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable. Users are recommended to upgrade to version 2.4.60, which fixes this issue.

 Vulnerabilities

Port 443 ▾Latest ▾

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

 2024 (7)

CVE-2024-40898

7.5

SSRF in Apache HTTP Server on Windows with mod\_rewrite in server/vhost context, allows to potentially leak NTLM hashes to a malicious server via SSRF and malicious requests. Users are recommended to upgrade to version 2.4.62 which fixes this issue.

CVE-2024-38477

7.5

null pointer dereference in mod\_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request. Users are recommended to upgrade to version 2.4.60, which fixes this issue.

CVE-2024-38476

9.8

Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable. Users are recommended to upgrade to version 2.4.60, which fixes this issue.

## 5. Hallazgos con Google Dorks

### 5.1 Consultas utilizadas y resultados encontrados:

Consulta Dork	URL/Resultado encontrado
site:www2.aguakan.com filetype:pdf	<a href="https://www2.aguakan.com/docs/1A23-24_Aguakan_digital.pdf">https://www2.aguakan.com/docs/1A23-24_Aguakan_digital.pdf</a>
site:www2.aguakan.com "Warning"   "Error"   "Notice"	<a href="https://www2.aguakan.com/crees-que-hubo-un-error-en-tu-factura-del-agua-modulos-y-horarios-para-hacer-una-aclaracion/">https://www2.aguakan.com/crees-que-hubo-un-error-en-tu-factura-del-agua-modulos-y-horarios-para-hacer-una-aclaracion/</a>

## 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 muestran 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  $\geq 2.4.26$  / 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  $\geq$  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  $\geq$  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  $\geq$  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  $\geq$  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  $\geq$  2.4.47 (parches en distribuciones modernas).