



Universidad
Francisco de
Vitoria
*Centro de
Documentación
Europea*
UFV Madrid

Informe de Enumeración Activa y Descubrimiento de Servicios.

Héctor Ramírez Lopez

Índice

1. alcance y metodología	3
1.2. Descripción del Objetivo	3
1.2. Alcance del Proyecto	3
1.3. Herramientas utilizadas	4
1.4. Metodología	5
2. Reconocimiento de Infraestructura (DNS y Red)	6
2.1 Resolución de Nombres y Registros DNS	6
3. Escaneo de puertos y análisis de banners.....	7
3.1 Descubrimiento de servicios (tcp/udp).....	7
3.2 Análisis de Banners	8
4. Fingerprinting Web y Tecnologías	9
4.1 Análisis de Cabeceras HTTP	9
4.2 identificación DE CMS Y FRAMEWORKS.....	9
5. Seguridad en la Capa de Transporte (TLS/SSL)	10
5.1 Análisis del Certificado	10
6. Enumeración de Contenido (Fuzzing).....	10
6.1 Descubrimiento de Directorios y Archivos	10
7. Análisis de Vulnerabilidades y Vectores de Ataque	11
7.1 Matriz de Versiones y CVEs Potenciales.....	11

1. alcance y metodología

1.2. Descripción del Objetivo

El objetivo de este ejercicio es realizar una Enumeración Activa sobre el dominio objetivo **aytocabanillas.org**. A diferencia de la fase OSINT, que se basa en la recolección pasiva de información pública, este procedimiento implica una comunicación directa con los servidores del objetivo para identificar su infraestructura, servicios expuestos y posibles vectores de ataque.

El análisis se centra en la identificación de tecnologías, versiones de software y configuraciones inseguras que podrían comprometer la confidencialidad, integridad o disponibilidad del sistema.

1.2. Alcance del Proyecto

El alcance de esta auditoría se limita estrictamente a los activos digitales autorizados para el ejercicio.

- **Objetivo Principal:** aytocabanillas.org.
- **Tipo de Prueba: Black Box (Caja Negra).** No tenemos ninguna información sobre la infraestructura, credenciales ni código fuente, toda la información la descubrimos desde cero.

1.3. Herramientas utilizadas

Para las pruebas se ha seleccionado un conjunto de herramientas de línea de comandos estándar en la industria de la ciberseguridad. Estas herramientas se clasifican según su función en las distintas capas del modelo OSI y la fase del ataque:

Herramienta	Categoría/Función	Utilidad
nslookup / dig	Infraestructura / DNS	Resolución de nombres, identificación de direcciones IP y registros de servidores de correo (MX) y nombres (NS).
nmap	Red / Escaneo de Puertos	Descubrimiento de hosts, detección de puertos abiertos (TCP/UDP) y detección básica de versiones de servicios.
nc (netcat)	Transporte / Conexión	Interacción manual con puertos abiertos (Banner Grabbing) para verificar servicios y respuestas crudas.
openssl	Cifrado / SSL/TLS	Ánalisis de la configuración de seguridad de los certificados SSL/TLS y verificación de protocolos criptográficos.
curl	Web / Cliente HTTP	Peticiones web manuales para analizar cabeceras HTTP, códigos de estado y redirections.
httpx	Web / Probing	Comprobación rápida de servidores web activos y detección de tecnologías en las respuestas.
whatweb	Web / Fingerprinting	Identificación automática del CMS, servidor web, frameworks y librerías utilizadas (Fingerprinting web).
ffuf	Web / Fuzzing	Enumeración de fuerza bruta para descubrir directorios ocultos, archivos de configuración y rutas no indexadas.

1.4. Metodología

El proceso de enumeración seguirá un orden para maximizar la detección de vectores:

1. **Reconocimiento de Infraestructura:** Identificación de la IP y resolución DNS (dig, nslookup).
2. **Descubrimiento de Servicios:** Escaneo de puertos y captura de banners para entender qué "puertas" están abiertas (nmap, nc).
3. **Análisis de Capa de Aplicación (Web):** Identificación del software que se ejecuta en los puertos web (whatweb, httpx, curl).
4. **Análisis de Seguridad en Transporte:** Verificación de la robustez del cifrado (openssl).
5. **Descubrimiento de Contenido:** Búsqueda de recursos ocultos mediante fuzzing (ffuf).
6. **Correlación de Vulnerabilidades:** Cruce manual de las versiones detectadas con bases de datos de vulnerabilidades conocidas (CVEs) para identificar vectores de riesgo.

2. Reconocimiento de Infraestructura (DNS y Red)

2.1 Resolución de Nombres y Registros DNS

- **Herramientas:** nslookup, dig.
- IP: 217.160.0.211.
- Registros MX: dig aytocabanillas.org mx

```
1 aspmx.l.google.com.  
10 aspmx2.googlemail.com.  
5 alt2.aspmx.l.google.com.  
5 alt1.aspmx.l.google.com.
```

- Registros NS (Nameservers): dig aytocabnillas.org ns

```
ns1075.ui-dns.org.  
ns1075.ui-dns.biz.  
ns1075.ui-dns.de.  
ns1075.ui-dns.com.
```

- Aparte se ha intentado una transferencia de zona para ver si fallaba o exponía subdominios en este caso ha fallado.

```
(kali㉿kali)-[~]  
$ dig @ns1075.ui-dns.de. aytocabanillas.org axfr  
  
; <>> DiG 9.20.15-1-Debian <>> @ns1075.ui-dns.de. aytocabanillas.org axfr  
; (2 servers found)  
;; global options: +cmd  
; Transfer failed
```

- Análisis: se ha identificado la dirección ip 217.160.0.211 y el correo es gestionado por Google.

3. Escaneo de puertos y análisis de banners

3.1 Descubrimiento de servicios (tcp/udp)

- **Herramientas:** nmap, nc (netcat).
- Ejecutamos el comando de nmap para ver que puertos están abiertos en este caso están abiertos el puerto 80 y el 443

```
(kali㉿kali)-[~]
└─$ nmap -sS 217.160.0.211
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-04 11:10 GMT
Nmap scan report for 217-160-0-211.elastic-ssl.ui-r.com (217.160.0.211)
Host is up (0.0069s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

- Usamos netcat para conectar manualmente a un puerto y vemos que los puertos aceptan la conexión.

```
(kali㉿kali)-[~]
└─$ nc -v 217.160.0.211 80
217-160-0-211.elastic-ssl.ui-r.com [217.160.0.211] 80 (http) open
he

(kali㉿kali)-[~]
└─$ nc -v 217.160.0.211 443
217-160-0-211.elastic-ssl.ui-r.com [217.160.0.211] 443 (https) open
```

- **Análisis:** Vemos dos puertos expuestos el 80 y el 443 los dos son puertos web.

3.2 Análisis de Banners

- **Herramientas:** curl,nmap
- **Respuesta del servidor:**

```
(kali㉿kali)-[~]
$ curl -I http://217.160.0.211
HTTP/1.1 404 Not Found
Server: nginx
Date: Thu, 04 Dec 2025 11:34:40 GMT
Content-Type: text/html
Content-Length: 146
Connection: keep-alive

(kali㉿kali)-[~]
$ nmap -sV -p 443 217.160.0.211
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-04 11:42 GMT
Nmap scan report for 217-160-0-211.elastic-ssl.ui-r.com (217.160.0.211)
Host is up (0.0056s latency).

PORT      STATE SERVICE      VERSION
443/tcp    open  ssl/https  nginx
```

Análisis: El banner del servicio en el puerto 80 revela que es un servidor Nginx y el del 443 también vemos lo mismo.

4. Fingerprinting Web y Tecnologías

4.1 Análisis de Cabeceras HTTP

- **Herramientas:** curl, httpx.
- **Qué incluir:**
 - Comando curl -I -L para ver las cabeceras de respuesta completa.

```
(kali㉿kali)-[~]
└─$ curl -I -L https://aytocabanillas.org
HTTP/2 200
content-type: text/html; charset=UTF-8
x-ws-rateLimit-limit: 1000
x-ws-rateLimit-remaining: 999
date: Thu, 04 Dec 2025 11:51:34 GMT
server: Apache
x-pingback: https://aytocabanillas.org/xmlrpc.php
link: <https://aytocabanillas.org/wp-json/>; rel="https://api.w.org/", <https://aytocabanillas.org/wp-json/wp/v2/page/>; type="application/json", <https://aytocabanillas.org/>; rel=shortlink
```

- Comando httpx -status-code -tech-detect para un escaneo rápido.

```
(kali㉿kali)-[~]
└─$ /go/bin/httpx -u https://aytocabanillas.org -status-code -tech-detect
[projectdiscovery.io]
[INF] Current httpx version v1.7.2 (latest)
[WRN] UI Dashboard is disabled, Use dashboard option to enable
https://aytocabanillas.org [200] Apache HTTP Server,CookieYes:3.3.8,MySQL,PHP,WordPress:6.8.3,YouTube,jQuery,jQuery Migrate:3.4.1

(kali㉿kali)-[~]
└─$
```

- **Análisis:** Podemos observar cabeceras como x-pingback o link y vemos que también encontramos varios servicios como: apache, MySQL, php, WordPress, YouTube, jQuery y migrate 3.4.1.

4.2 identificación DE CMS Y FRAMEWORKS

- **Herramientas:** whatweb.
- COMANDO whatweb -v [dominio].

```
(kali㉿kali)-[~]
└─$ whatweb -v aytocabanillas.org
WhatWeb report for http://aytocabanillas.org

WhatWeb report for https://aytocabanillas.org
Status : 200 OK
Title  : Ayto. Cabanillas #8211; Consulta aquí toda la información relativa a Cabanillas
IP     : 217.160.0.211
Country : GERMANY, DE

Summary : Apache, Email[ayuntamiento@aytocabanillas.org], Frame, Google-Analytics[Universal][UA-46118419-1], HTML5, HTTPServer[Apache], JQuery[3.7.1], MetaGenerator[WordPress 6.8.3], Script[speculationrules;text/javascript], UncommonHeaders[x-ws-rateLimit-limit,x-ws-rateLimit-remaining,link], WordPress[6.8.3], x-pingback[https://aytocabanillas.org/xmlrpc.php], X-UA-Compatible[ie=edge], YouTube
```

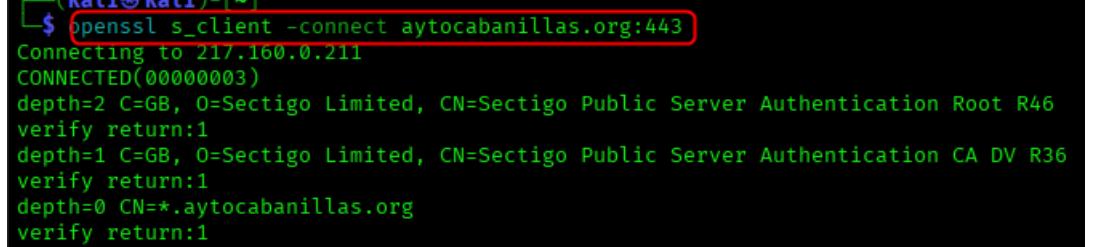
- **Análisis:** Se puede ver que nos lista el frame de google analitics, la version de jquery 3.7.1, la version de wordpress 6.8.3

5. Seguridad en la Capa de Transporte (TLS/SSL)

5.1 Análisis del Certificado

- **Herramientas:** openssl.

 - Comando: openssl s_client -connect dominio:443.



```
(Kali㉿Kali)-[~]
$ openssl s_client -connect aytocabanillas.org:443
Connecting to 217.160.0.211
CONNECTED(00000003)
depth=2 C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication Root R46
verify return:1
depth=1 C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV R36
verify return:1
depth=0 CN=*.aytocabanillas.org
verify return:1
```
 - Análisis:
 - Podemos ver que el certificado es valido
 - NotBefore: Nov 22 00:00:00 2025 GMT, NotAfter: Dec 6 23:59:59 2026
 - También vemos la entidad emisora que es Sectigo Public Server Authentication CA DV R36
 - CN=Sectigo Public Server Authentication CA DV R36
 - Vemos que caduca el 6 de diciembre de 2026 a las 23:59:59 GMT.
 - Tambien podemos que usa TLS version 1.2. Protocol : TLSv1.2

6. Enumeración de Contenido (Fuzzing)

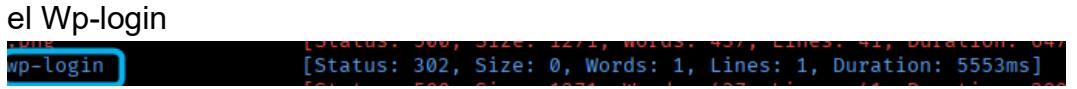
6.1 Descubrimiento de Directorios y Archivos

- **Herramientas:** ffuf.

 - Comando utilizado con el diccionario he elegido para el diccionario la ruta que se ve en la imagen hay kali guarda diccionarios.



```
(kali㉿kali)-[~]
$ ffuf -u https://aytocabanillas.org/FUZZ -w /usr/share/wordlists/dirb/common.txt
[Status: 300, Size: 1271, Words: 457, Lines: 41, Duration: 047ms]
wp-login [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 5553ms]
WP-cron
[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 5558ms]
```
 - Resultados encontrados (códigos 200, 301 -e, 403) tambien encontre el Wp-login



```
[Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 5553ms]
wp-login
[Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 5558ms]
WP-cron
```

7. Análisis de Vulnerabilidades y Vectores de Ataque

En este punto detectaremos versiones vulnerables y posibles vectores de ataque

7.1 Matriz de Versiones y CVEs Potenciales

Tecnología detectada	Versión	¿Antigua?	Vulnerabilidades
wordpress	6.8.3	si	XSS (Cross-Site Scripting)
jquery	3.7.1	si	XSS en selectores
Migrate	3.4.1	no	ninguna



Universidad
Francisco de
Vitoria
*Centro de
Documentación
Europea*
UFV Madrid