

9. SEÑALES DE VIDA (O ALGO PEOR) EN LA RED

Practica [OSINT]- SEÑALES DE VIDA (O ALGO PEOR) EN LA RED

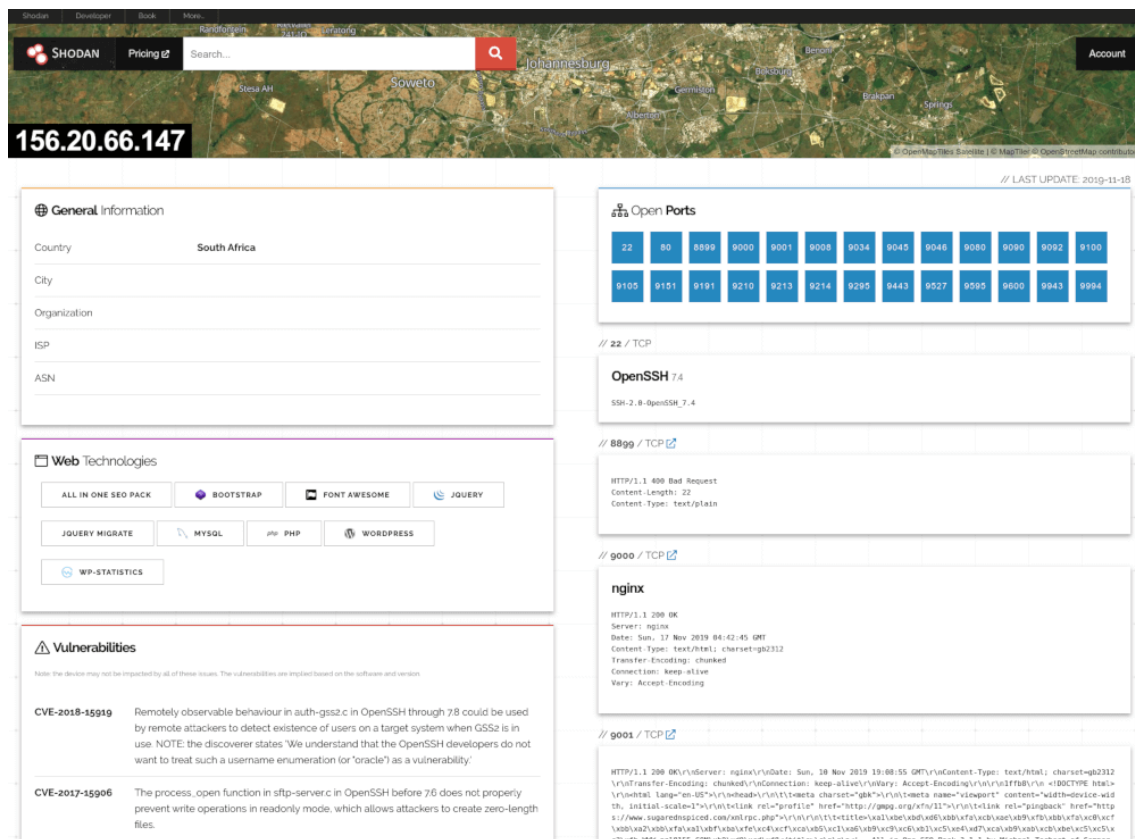
La nave **USCSS Nostromo** ha recibido una transmisión automática desde un sistema remoto. No se sabe si es una llamada de socorro... o una advertencia.

La compañía ha encomendado al **Equipo de Investigación (tus alumnos)** usar *Shodan* para rastrear:

- 1. Señales de dispositivos expuestos**
- 2. Orígenes de la transmisión**
- 3. Infraestructura del sistema remoto**
- 4. Posibles vectores de intrusión**

La misión: **analizar patrones, encontrar conexiones y trazar el mapa de un “nido” digital escondido.**

La actividad se divide en **3 fases**, cada una con un objetivo claro y un filtro de Shodan.



FASE 1 — Localizar señales: “Ping de movimiento”

Objetivo: practicar filtros por tipo de dispositivo + país/ciudad.


El sensor de movimiento de la Nostromo detecta *actividad anómala* en una zona del sistema. Necesitamos saber qué dispositivos expuestos hay allí.


Tareas:




1. **Buscar un tipo concreto de dispositivo** (puerta automatizada, cámara IP, sistema industrial, etc.)

Ejemplos:




- a. Cámaras IP:
product:GoAhead
product:"Hikvision"
port:554 has_screenshot:true
 - b. Paneles web expuestos:
http.title:"login"
2. **Añadir filtro de ubicación** (país o ciudad).
Por ejemplo, España: country:ES product:GoAhead O
por ciudad: city:Madrid http.title:login
3. Apuntar **IP, puerto, captura y versión** como si fueran
“señales biológicas”.

[Pricing](#) 

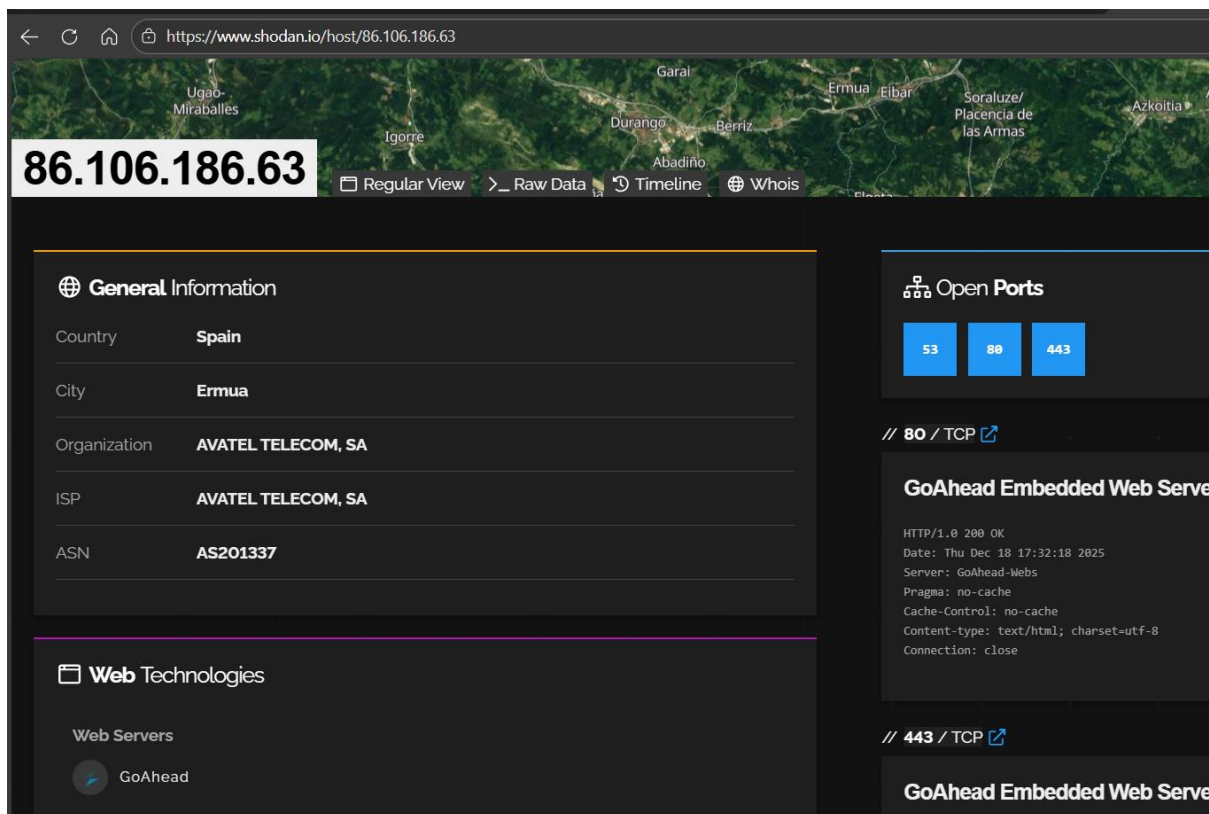
product:GoAhead country:es org:"DIRECCION GENERAL DE LA POLICIA" 

 View Report  View on Map  Advanced Search

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

195.53.174.94 
[DIRECCION GENERAL DE LA POLICIA](#)
 Spain, Madrid 

HTTP/1.1 200 OK
Server: GoAhead-Webs
Content-Type: text/html
Expires: Thu, 26 Oct 1995 00:00:00 GMT
Pragma: no-cache
Cache-control: no-cache
Connection: close



The screenshot shows the Shodan.io interface for the IP address 86.106.186.63. The top section features a map of the Basque region in Spain, with labels for locations like Ugao-Miraballes, Igerre, Durango, Berriz, Ermua, Eibar, Soralue/Placencia de las Armas, and Azkoitia. Below the map, the IP address 86.106.186.63 is prominently displayed. The main content area is divided into several sections:

- General Information:** A table listing details about the host:

Field	Value
Country	Spain
City	Ermua
Organization	AVATEL TELECOM, SA
ISP	AVATEL TELECOM, SA
ASN	AS201337
- Open Ports:** A section showing open ports 53, 80, and 443.
- Web Technologies:** A section showing the web server technology used, which is GoAhead.
- HTTP Headers:** A section showing the HTTP response headers for port 80 and 443, both using the GoAhead Embedded Web Server.

FASE 2 — Identificar el origen de la transmisión

Objetivo: buscar por **organización o dominio**.

La señal parece provenir de una colonia (una empresa, universidad o dominio). Deben “explorar todas las instalaciones” de ese lugar.

Ejercicios:

1. Elegir una organización pública o conocida:
Ejemplos: org:"Universidad Complutense"
org:"Telefonica"

Colmenar
del Arroyo

Gujula

Brunete

Boadilla
del Monte

Campamento

147.96.0.0

Regular View

> Raw Data

Timeline

Whois

General Information

Hostnames	ucm.es
	www.coie.ucm.es
	www.ope.ucm.es
Domains	ucm.es
Country	Spain
City	Madrid
Organization	Universidad Complutense de Madrid
ISP	Entidad Publica Empresarial Red.es
ASN	AS766

88.9.118.145

Regular View Raw Data Timeline Whois

General Information

Hostnames	145.red-88-9-118.dynamicip.rima-tde.net
Domains	rima-tde.net
Country	Spain
City	Sevilla
Organization	Telefonica de Espana SAU
ISP	TELEFONICA DE ESPANA S.A.U.
ASN	AS3352

2. Buscar todos los dispositivos de la misma entidad:
 hostname:"uic.es" hostname:"unizar.es"

Pricing [hostname:"uic.es"](#)

View Report View on Map Advanced Search

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to.](#)

403 - Forbidden: Access is denied.

161.71.96.118
 click.info.uic.es
 click.mail.ducatifscmunica.com.br
 Salesforce, Inc.
 Germany, Frankfurt am Main

SSL Certificate

Issued By:
 Common Name: DigiCert Global G2 TLS RSA SHA256 2020 CA1
 Organization: DigiCert Inc

Issued To:
 Common Name: click.info.uic.es
 Organization: Salesforce, Inc.

Supported SSL Versions:
 TLSv1.2, TLSv1.3

HTTP/1.1 403 Forbidden
 Cache-Control: no-cache, must-revalidate, max-age=0, no-store, private
 Content-Type: text/html
 Content-Security-Policy: default-src 'self'; frame-ancestors 'self'
 X-Frame-Options: SAMEORIGIN
 X-Content-Type-Options: nosniff
 Referrer-Policy: origin-when-cross-origin
 St...

FASE 3 — Conexión entre señales: seguir el rastro del xenomorfo

Objetivo: enlazar un dispositivo concreto → el resto del ecosistema.

Han encontrado una máquina sospechosa que transmite paquetes extraños. La misión es identificar **todo el entorno que la rodea**.

Cómo hacerlo:

1. Selecciona un dispositivo que hayas encontrado en Fase 1.
2. Observan:
 - a. dominio
 - b. ASN
 - c. organización
 - d. versión del servicio
3. Construyen una nueva búsqueda:

IP: 82.X.X.X

org: "Ayuntamiento de ____"

port 443 running nginx 1.18.0

Entonces buscar:

org:"Ayuntamiento de ____"
product:"nginx"

O incluso por **ASN**:

asn:3352 (o el ASN que toque)

SHODAN

Explore

Downloads

Pricing

Search

Basauri

Galdakao

Ugao-Miraballes

Igorre

Garai

Durango

Berriz

Abadiño

Ermua

Elbar

Soraluze/Placencia de las Armas

Azkoitia

91.126.146.69

Regular View

Raw Data

Timeline

Whois

General Information

Hostnames

h-91-126-146-69.wholesale.adamo.es

Domains

adamo.es

Country

Spain

City

Ermua

Organization

Adamo Telecom Iberia S.A.U

ISP

Adamo Telecom Iberia S.A.

ASN

AS35699

Open Ports

53

80

443

// 80 / TCP

GoAhead Embedded Web Server

HTTP/1.0 200 OK
Date: Thu Dec 18 09:42:55 2025
Server: GoAhead-Webs
Pragma: no-cache
Cache-Control: no-cache
Content-type: text/html; charset=utf-8
Connection: close

g

org:"Adamo Telecom Iberia S.A.U" product:"nginx"

Q

View Report

View on Map

Advanced Search

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

Servidor central de lecturas

91.126.39.138
comptadors.alanait.com
cli-5b7e278a.wholesale.adamo.es
comptadors.ofigrafic.es
Adamo Telecom Iberia S.A.U
Spain, Polinyà
eol-product

SSL Certificate

Issued By:
Common Name: R12
Organization: Let's Encrypt

Issued To:
Common Name: comptadors.ofigrafic.es

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 200 OK

Server: nginx/1.10.3

Date: Thu, 18 Dec 2025 07:33:34 GMT

Content-Type: text/html; charset=utf-8

Transfer-Encoding: chunked

Connection: keep-alive

X-UA-Compatible: IE=Edge,chrome=1

ETag: "6852a28b5ef78b1b568c0626f4100653"

Cache-Control: max-age=0, private, must-revalidate

...

Adv Dashboard

91.126.39.141
cli-5b7e278d.wholesale.adamo.es
agenda.alanait.com
agenda.ofigrafic.es
Adamo Telecom Iberia S.A.U
Spain, Polinyà
eol-product

SSL Certificate

Issued By:
Common Name: R13
Organization: Let's Encrypt

Issued To:
Common Name: agenda.ofigrafic.es

HTTP/1.1 200 OK

Server: nginx/1.22.1

Date: Thu, 18 Dec 2025 07:33:26 GMT

Content-Type: text/html

Content-Length: 89278

Connection: keep-alive

Last-Modified: Wed, 02 Nov 2022 16:31:11 GMT

Accept-Ranges: bytes

