

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

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

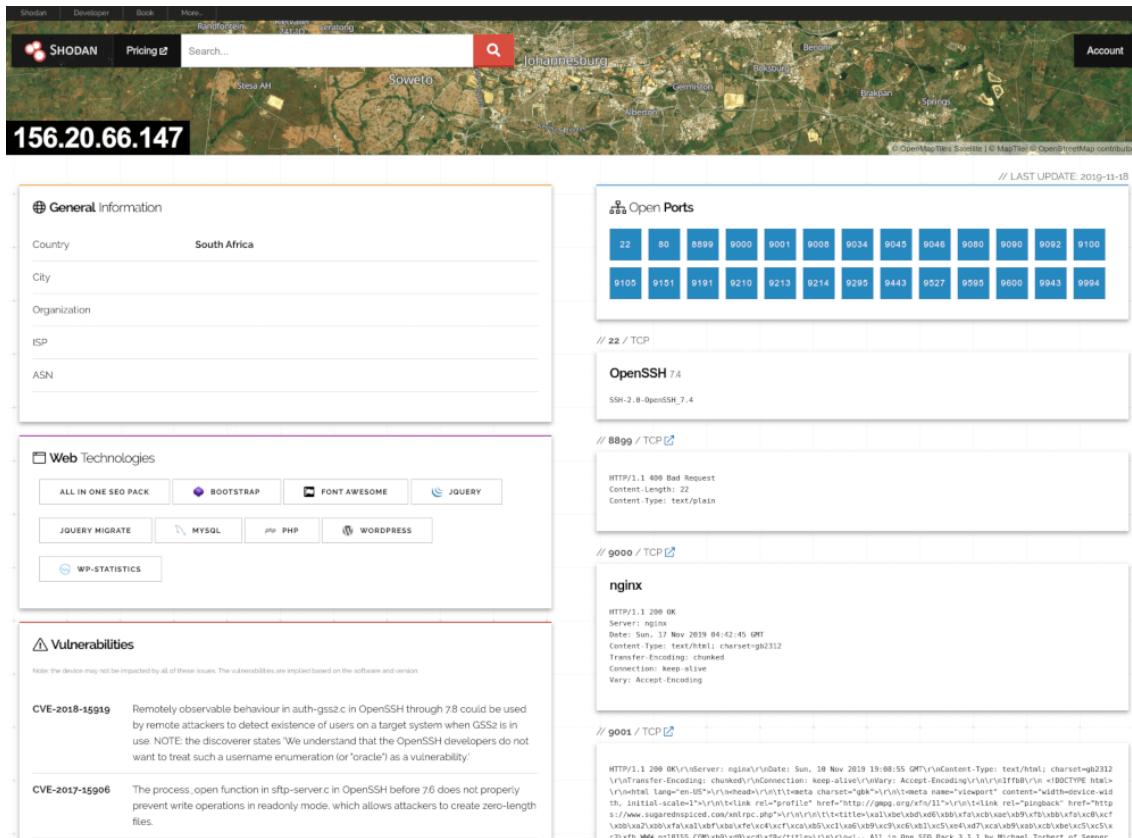
La nave **USCSS Nostromo** ha recibido una transmisión automática desde un sistema remoto. No se sabe si es una llamada de socorro... o una advertencia.

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”.

The screenshot shows a search interface with a dark theme. At the top, there is a search bar containing the query "product:GoAhead country:es org:"DIRECCION GENERAL DE LA POLICI". To the right of the search bar is a red search button with a white magnifying glass icon. Below the search bar, there are three navigation links: "View Report", "View on Map", and "Advanced Search". A "Product Spotlight" banner at the top of the main content area reads: "Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)". The main content area displays information for the IP address 195.53.174.94. It includes the IP address itself, a blue link to "DIRECCION GENERAL DE LA POLICIA", a small flag icon for Spain, and the location "Spain, Madrid". To the right of this information is a list of HTTP headers: "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", and "Connection: close".

86.106.186.63

General Information

Country	Spain
City	Ermua
Organization	AVATEL TELECOM, SA
ISP	AVATEL TELECOM, SA
ASN	AS201337

Web Technologies

Web Servers
GoAhead

Open Ports

53	80	443
----	----	-----

// 80 / TCP

GoAhead Embedded Web Server

```
HTTP/1.0 200 OK
Date: Thu Dec 18 17:32:18 2025
Server: GoAhead-Webs
Pragma: no-cache
Cache-Control: no-cache
Content-type: text/html; charset=utf-8
Connection: close
```

// 443 / TCP

GoAhead Embedded Web Server

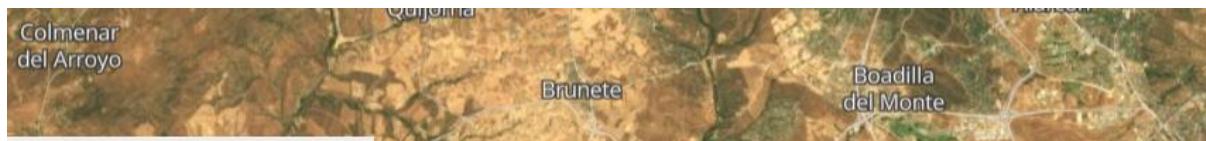
## FASE 2 — Identificar el origen de la transmisión

**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"



**147.96.0.0**

Regular View Raw Data Timeline Whois

---

## General Information

**ucm.es**

Hostnames	<a href="#">www.coie.ucm.es</a> <a href="#">www.ope.ucm.es</a>
Domains	<a href="#">ucm.es</a>
Country	<b>Spain</b>
City	<b>Madrid</b>
Organization	<b>Universidad Complutense de Madrid</b>
ISP	<b>Entidad Publica Empresarial Red.es</b>
ASN	<b>AS766</b>

**General Information**

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

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.ducatifscomunica.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)

**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**

```
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
```

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

**Servidor central de lecturas**

91.126.39.138  
comptadores.alanait.com  
cli-5b7e278a.wholesale.adamo.es  
comptadores.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:  
comptadores.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:

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

