Universidad
Francisco de Vitoria
UFV Madrid

Explorando la Superficie de Internet con Shodan.io

Héctor Ramírez López

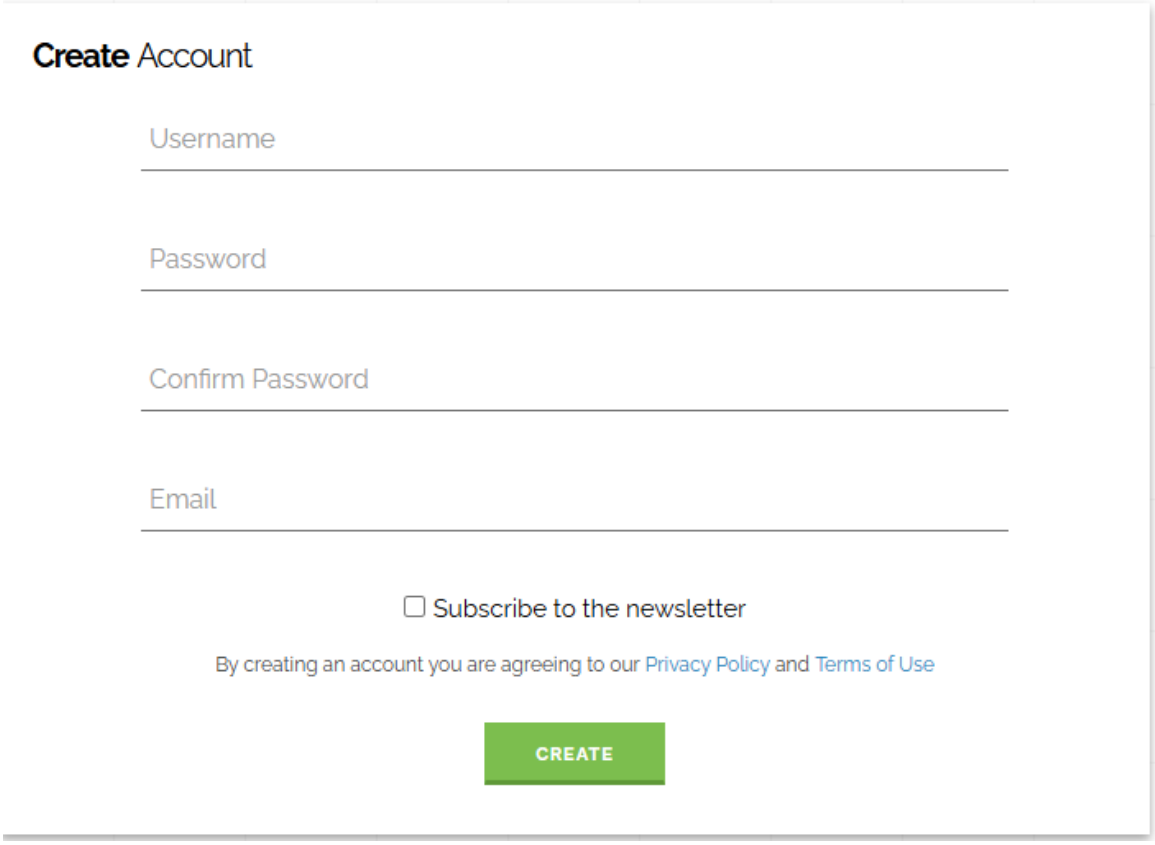
Índice

Ejercicio 1-Exploración básica

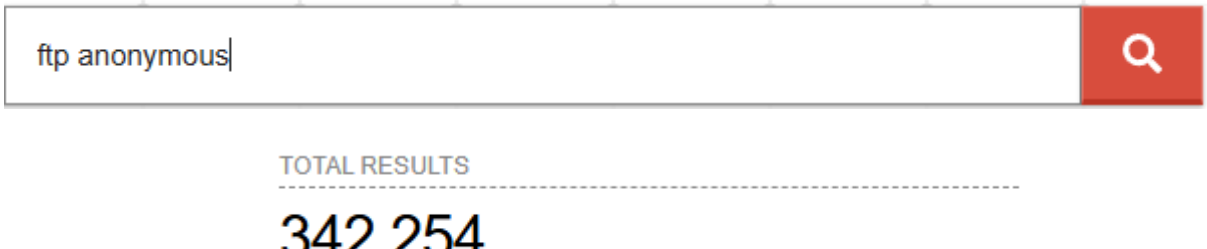
Objetivo: Familiarizarse con la interfaz de Shodan.

Procedimiento

1. Entré a https://www.shodan.io y creé una cuenta.



2. Realicé las búsquedas solicitadas: apache, ftp anonymous, default password



3. Para cada resultado abrí el detalle del host y copié: IP, país, puerto, banner, hostnames.

Apache

124.255.234.201

- **IP**: 124.255.234.201.
- **País**: Japón.
- **Puertos**: 80, 81, 82, 83, 400, 427, 785, 789 etc.
- **Banner**: Apache/2.4.62 (Unix).
- **Versión**: 2.4.62.
- **Hostnames**: 201.234.255.124.ap.mvno.net.
- **Observaciones**: En el banner aparece el software y la versión exacta lo que permite buscar CVEs, aparece nombres de dominios como cmstreamer.com, axis.com y youtube.com lo que indica que podría ser una Axis CamStreamer

```
Server: Apache/2.4.62 (Unix) OpenSSL/3.0.15
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'self' camstreamer.com https://*.googleapis.com https://*.gstatic.com cdn3.iconfinder.com camstreamer.c
om www.youtube.com; frame-ancestors 'self' camstreamer.com https://*.googleapis.com https://*.gstatic.com cdn3.iconfinder.com camstreamer.co
m www.youtube.com; connect-src 'self' https://*.google-analytics.com https://*.analytics.google.com https://*.googletagmanager.com https://
*.axis.com mediastream: blob: camstreamer.com https://*.googleapis.com https://*.gstatic.com cdn3.iconfinder.com camstreamer.com www.youtub
e.com; script-src 'self' https://*.googletagmanager.com https://www.google-analytics.com https://ssl.google-analytics.com https://*.axis.com
camstreamer.com https://*.googleapis.com https://*.gstatic.com cdn3.iconfinder.com camstreamer.com www.youtube.com; style-src 'self' 'unsafe
-inline' camstreamer.com https://*.googleapis.com https://*.gstatic.com cdn3.iconfinder.com camstreamer.com www.youtube.com; img-src 'self'
https://*.google-analytics.com https://*.googletagmanager.com https://*.axis.com data: blob: camstreamer.com https://*.googleapis.com http
s://*.gstatic.com cdn3.iconfinder.com camstreamer.com www.youtube.com; media-src 'self' mediastream: blob: camstreamer.com https://*.googlea
pis.com https://*.gstatic.com cdn3.iconfinder.com camstreamer.com www.youtube.com; object-src 'none'
```

Vulnerabilities

1	11	11	2	0

FTP anonymous

115.85.49.194

- **IP**:115.85.49.194.
- **País**: Filipinas.
- **Puertos**: 21, 22, 23, 80, 443.
- **Banner**: Pure-FTPd [privsep].
- **Hostnames**: 194.49.85.115.dsl.service.static.**eastern-tele.com.**
- **Observaciones**: En el banner se puede observar que el puerto 21 está sin cifrar por lo que es vulnerable a ataques de sniffing y robo de credenciales y también podemos observar que el acceso anónimo esta activo o mal configurado, puede ser un sistema nas

Pure-FTPd

```
220---------- Welcome to Pure-FTPd [privsep] ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 07:25. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
421 Unable to set up secure anonymous FTP
211-Extensions supported:
 EPRT
 IDLE
 MDTM
 SIZE
 REST STREAM
 MLST type*;size*;sizd*;modify*;UNIX.mode*;UNIX.uid*;UNIX.gid*;unique*;
 MLSD
 ESTA
 PASV
 EPSV
 SPSV
 ESTP
211 End.
```

Default password

5.78.122.162

- **IP**: 5.78.122.162.
- **País**: Estados Unidos.
- **Puertos**: 22, 137, 443, 445, 3000, 3001, 8079, 8080, 8081.
- **Banner**: HTTP/1.1.
- **Versión**: 1.1.
- **Hostnames**: static.162.122.78.5.clients.**your-server.de**
- **Observaciones:** podemos ver que puede ser un servidor Linux y que la autenticación de smb esta deshabilitada esto indica que cualquier persona que se conecta al servicio puede acceder a los recursos compartidos sin usuario ni contraseña.

```
SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.13
Key type: ecdsa-sha2-nistp256
Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBK8I6DGjeWzM7SYj+9aI5jBy
/6mUl3yVQsKNixdL2GeonjL+jHEAyrLPp83S6744mKwXcbHx6zVFglGAx5t0so0=
Fingerprint: 66:79:4f:84:56:a1:f9:8d:fd:d3:33:91:84:ad:11:e3
```

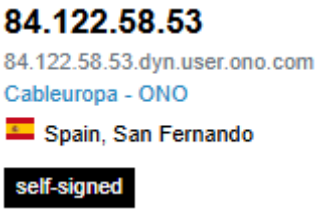
```
SMB Status:
  Authentication: disabled
  SMB Version: 2
  Capabilities: raw-mode
```

Ejercicio 2-Uso de filtros avanzados

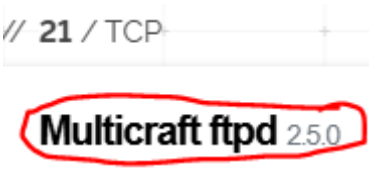
Procedimiento

Objetivo: Aprender a refinar búsquedas con operadores.

1. **Port:3389 Country:ES**-RDP en España



Observaciones: podemos ver en el banner del FTP la versión exacta del software (multicraft 2.5.0) en el del RDP nos da información del sistema operativo exacto y el nombre del host por último vemos que hay varios CVEs .



Vulnerabilities

All ports | Latest

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

2024 (2)

CVE-2024-5458 — 5.3 In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, due to a code logic error, filtering functions such as filter_var when validating URLs (FILTER_VALIDATE_URL) for certain types of URLs the function will result in invalid user information (username + password part of URLs) being treated as valid user information. This may lead to the downstream code accepting invalid URLs as valid and parsing them incorrectly.

CVE-2024-3566 — 9.8 A command inject vulnerability allows an attacker to perform command injection on Windows applications that indirectly depend on the CreateProcess function when the specific conditions are satisfied.

2023 (6)

CVE-2023-3824 — 9.4 In PHP version 8.0.* before 8.0.30, 8.1.* before 8.1.22, and 8.2.* before 8.2.8, when loading phar file, while reading PHAR directory entries, insufficient length checking may lead to a stack buffer overflow, leading potentially to memory corruption or RCE.

2. **product:mikrotik country:ES**

product:mikrotik country:ES

83.53.133.191

191.red-83-53-133.dynamicip.rima-tde.net

Telefonica de Espana SAU

Spain, Barcelona

Observaciones: Los datos útiles que podemos obtener de los banners son el tipo de dispositivo es un router Mikrotik (RB2011UiAs-2HnD), nombre del equipo CECOGA-LERMA y la antigüedad del dispositivo que la indica en segundos (146.800.500)

3. **ssl.cert.subject.cn: *. telefonica.es**-filtrar certificado SSL

Observaciones: Los datos que podemos ver en el banner del certificado SSL nos indican que es de un entorno de desarrollo y normalmente esta información no deberia de ser accesible (apiseg.dev.telefonica.es) también nos da el nombre de la organización en este caso telefónica, la ubicación, quien ha emitido el certificado y la fecha de validez.

SSL Certificate

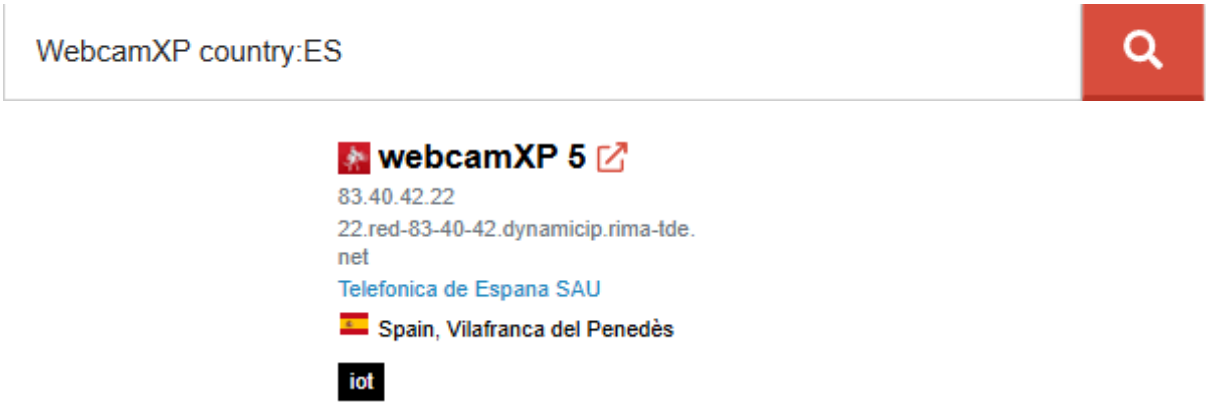
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:5e:b6:8a:8c:9f:6d:6f:80:3a:5d:74:b7:68:bd:e4
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
        Validity
            Not Before: Jul 21 00:00:00 2025 GMT
            Not After : Apr 14 23:59:59 2026 GMT
        Subject: C=ES, L=Madrid, O=TELEFONICA DE ESPA\xC3\x91A SA, CN=apiseg.dev.telefonica.es
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b1:39:a5:4a:cb:3b:79:36:b1:5f:6c:26:7e:dd:
                    b4:f1:57:a0:5b:94:60:9b:aa:f0:02:fc:a3:16:e7:
                    42:a1:15:0e:73:b9:57:cd:87:96:87:23:6e:f9:be:
                    94:bf:75:bc:76:c5:e6:fd:9a:41:68:5c:ff:48:90:
                    4f:32:77:73:7c:73:e9:fe:39:57:cb:30:4c:28:0a:
                    a2:28:f8:59:ce:14:79:59:c0:c7:55:5b:c5:60:c9:
                    e8:c8:43:b1:5f:d3:b6:ca:0b:19:ae:03:3b:7d:1f:
                    ba:ee:cf:74:b1:5d:b5:29:02:bc:e2:b0:43:54:32:
                    48:25:4b:9a:a9:c0:12:ac:00:b5:37:ea:8f:e2:f8:
                    59:25:8e:c5:c4:bd:30:ea:60:7f:7a:45:4e:35:ed:
                    a6:32:d9:f1:57:0c:68:b1:bf:3e:55:ea:45:23:10:
                    d4:7a:5d:24:f8:ea:59:15:c3:21:c4:81:11:fa:10:
                    b6:94:9f:f7:bf:f5:b0:26:d6:87:d3:b0:41:9e:db:
                    9e:98:9f:04:6b:ff:c8:83:85:0a:51:d3:16:19:80:
                    7c:eb:a9:86:ed:df:6c:fd:11:09:06:69:f0:22:33:
                    2c:3e:f1:02:57:42:a6:bd:19:6f:1d:71:fd:60:53:
                    74:da:ad:c8:18:3e:a1:34:9e:84:c6:39:ea:3e:fc:
                    8f:f1
```

Ejercicio 3-Identificación de IOT

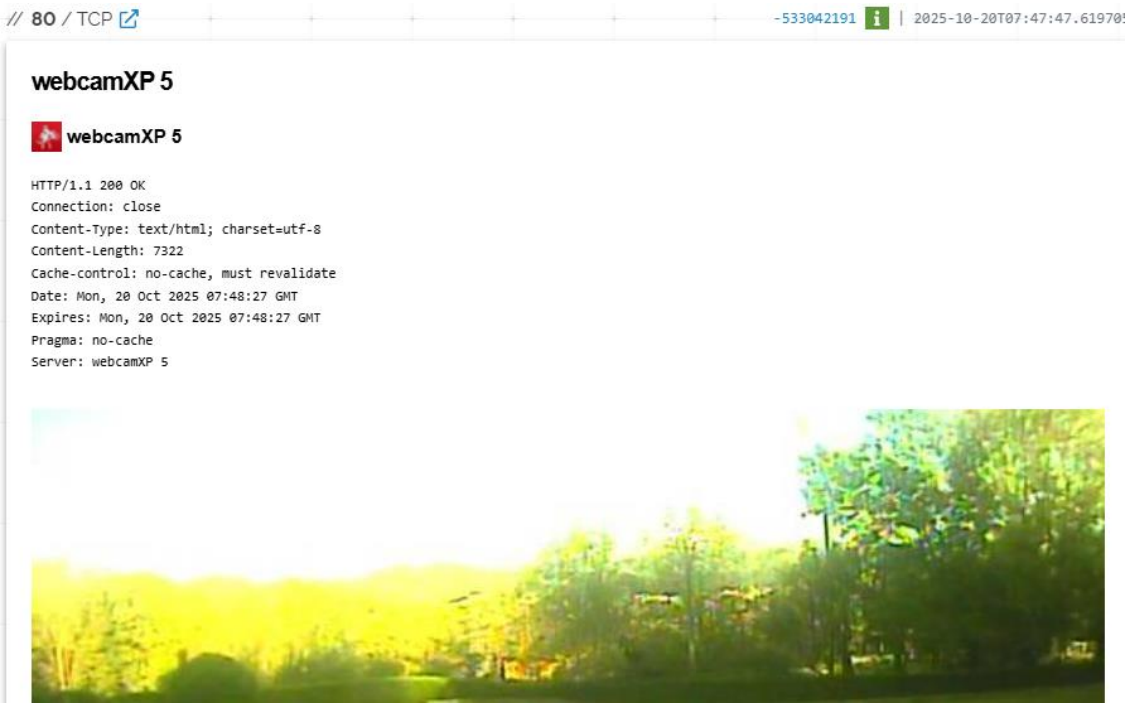
Procedimiento

Objetivo: Detectar dispositivos de domótica.

1. WebcamXP country:ES



- **IP**: 83.40.42.22.
- **País**: España.
- **Puerto**: 80.
- **Banner**: HTTP/1.1.
- **Producto**:webcamXP.



2. Port:554 has_screenshot:true

Port:554 has_screenshot:true

46.2.247.129

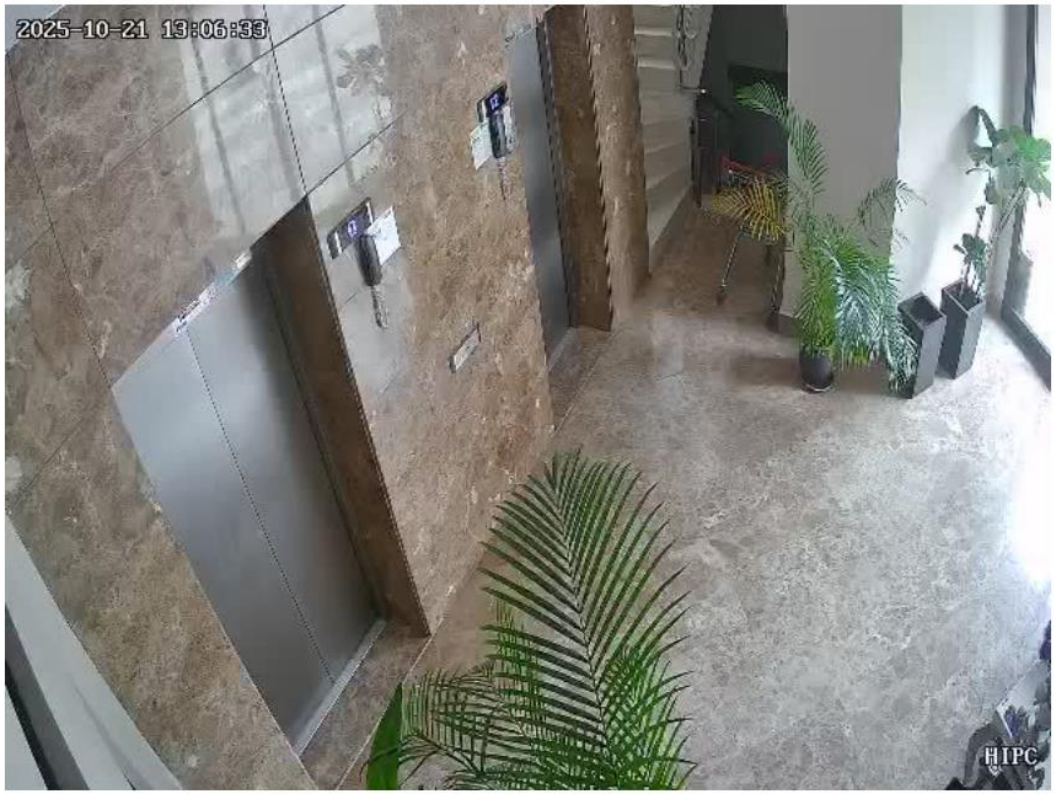
Koc.Net DSL Izmir

Turkey, Istanbul

- IP: 46.2.247.129.
- País: Turquía.
- Puertos:80, 554, 555, 556, 1723, 2000, 8291.
- Banner: RTSP/1.0
- Producto: Servidor de medios.

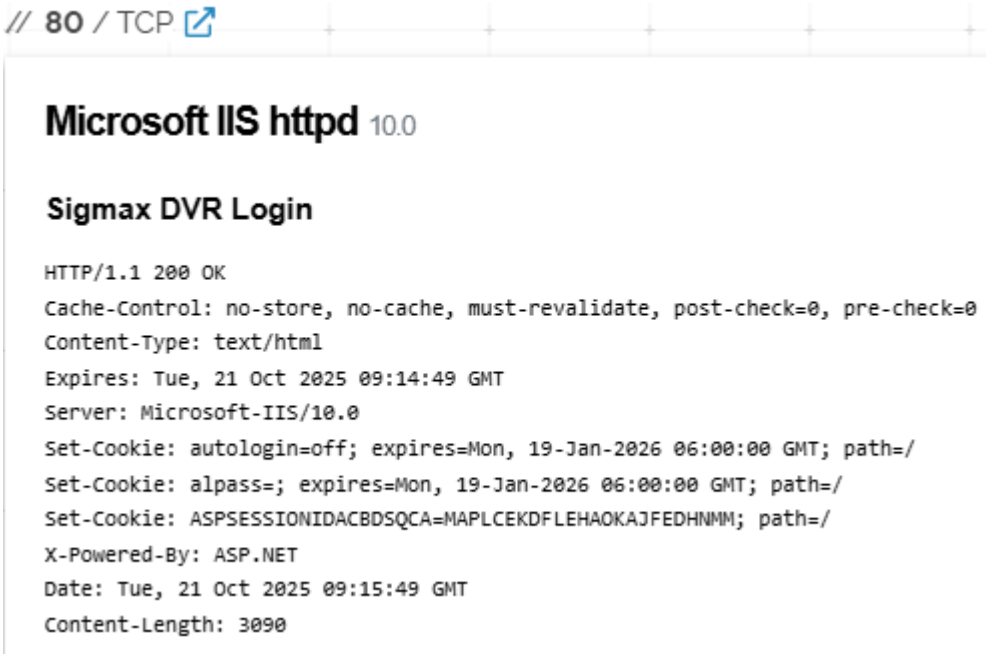
// 554 / TCP -1300977169 | 2025-10-21T09:59:56.791

```
RTSP/1.0 200 OK
CSeq: 1
Content-Length: 0
Date: Tue, Oct 21 2025 11:06:32 GMT
Public: OPTIONS, DESCRIBE, SETUP, PLAY, PAUSE, TEARDOWN, GET_PARAMETER, SET_PARAMETER, HEARTBEAT
```



3. title:"DVR Login"

- **IP**: 104.11.118.89.
- **País**: Estados unidos.
- **Puertos**:80, 1081, 5938, 8000.
- **Banner**: HTTP/1.1.
- **Producto**: Grabador de video digital.



4. port:23 country:ES-telnet abierto

- **IP**: 88.31.70.68.
- **País**: España.
- **Puerto:** 23.
- **Banner**: Alwon E20 Telnet.
- **Producto**: Modulo de comunicación ip.

Riesgos:

1. Exposición de cámaras (WebcamXP)
   - Accesos no autorizados.
   - Exposición de imágenes privadas.
   - Filtración de información.

2. Servidores de medios
   - RCE (ejecución de código remota).
   - Exposición de archivos internos (archivos de video o imágenes).

3. Módulo de comunicación ip
   - Intercepción de comunicación.
   - Control remoto.
   - Exposición de la red interna.

4. Riesgos generales de estos dispositivos

Riesgo	Explicación
Credenciales por defecto	Permite acceso a cualquier atacante
Vulnerabilidades conocidas	Muchos modelos no reciben actualizaciones (exploits públicos)
Reconocimiento corporativo	Revelan ubicación e infraestructura interna.
Legal	Filtración de imágenes puede infringir leyes de privacidad y GDPR.
Ataques de denegación de servicios	Algunos dispositivos no manejan bien peticiones externas y pueden caerse
Pivot hacia red interna	Dispositivos comprometidos pueden ser la puerta de entrada a servidores o bases de datos

Universidad
Francisco de Vitoria
UFV Madrid

RAMIREZ LOPEZ HECTOR - 53858461M

Firmado digitalmente por RAMIREZ LOPEZ HECTOR - 53858461M
Fecha: 2025.10.22 11:03:39 +02'00'