

Práctica 2: Análisis ético de la exposición IoT mediante Shodan

Seguridad de las comunicaciones Inalambricas

Autor: Cheuk Kelly Ng Pante (alu0101364544@ull.edu.es)

Fecha: 7 de diciembre de 2025

Índice general

1. Realizar la búsqueda referente al protocolo Modbus	1
2. Búsqueda de dispositivos en España que usen el puerto 47808	2
3. Selección de 3 dispositivos y análisis de sus vulnerabilidades	4

1. Realizar la búsqueda referente al protocolo Modbus

Para este caso se va a usar **port:502 modbus** en el motor de búsqueda de Shodan. A continuación, se muestran algunos de los resultados obtenidos:

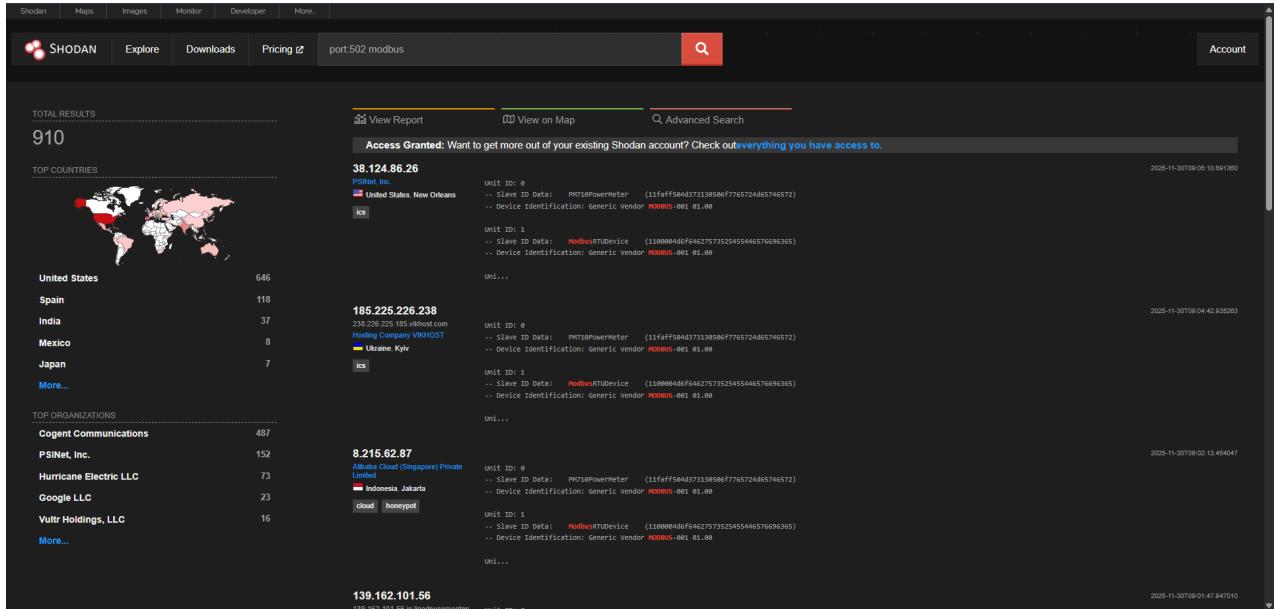


Figura 1.1: Resultado de la búsqueda Modbus en Shodan

Al seleccionar uno de los resultados, se puede observar la siguiente información:

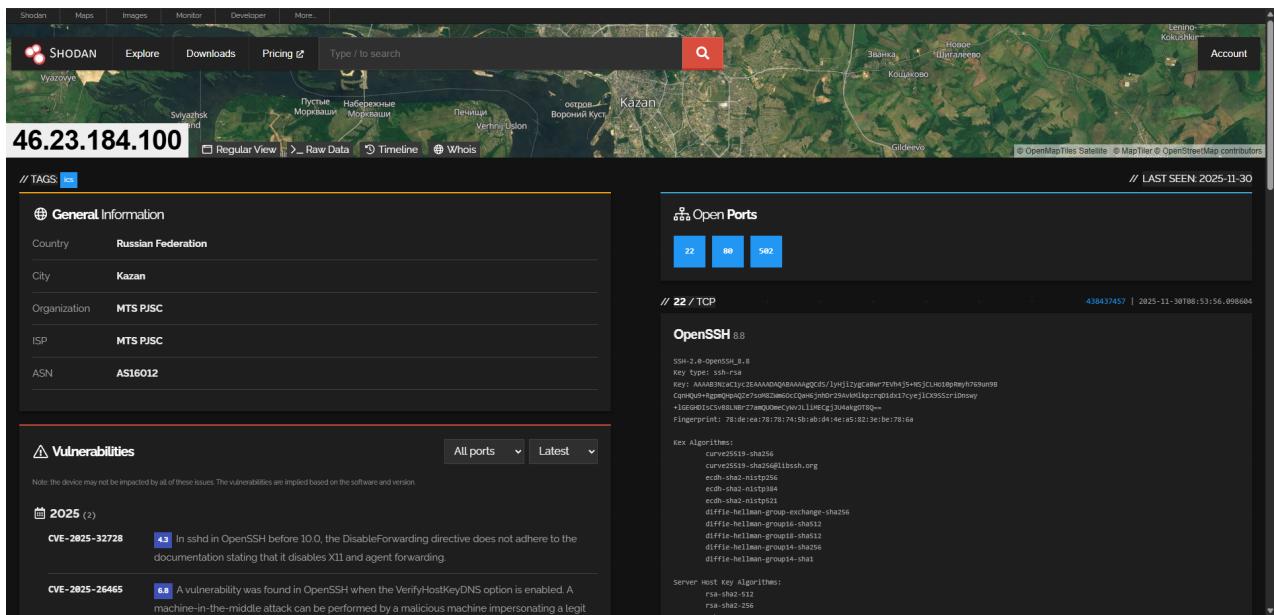


Figura 1.2: Información de un dispositivo Modbus

Y podemos ver que el puerto 80 está abierto, por lo que podemos intentar acceder a la interfaz web del dispositivo, viendo así una interfaz de login:



Figura 1.3: Interfaz web de un dispositivo Modbus

La interfaz parece corresponder al panel de administración de un router o CPE (dispositivo de cliente provisto por un ISP), es decir, probablemente la interfaz web de gestión de un router doméstico.

2. Búsqueda de dispositivos en España que usen el puerto 47808

Para este caso se va a usar **port:47808 country:ES** en el motor de búsqueda de Shodan. A continuación, se muestran algunos de los resultados obtenidos:

Figura 2.1: Resultado de la búsqueda en España en Shodan

Al seleccionar uno de los resultados, se puede observar la siguiente información:

Figura 2.2: Información de un dispositivo en España

Para este caso, el puerto 80 también está abierto, por lo que podemos intentar acceder a la interfaz web del dispositivo, viendo así una interfaz de login de un servidor Apache ubicado en Madrid, España:

Figura 2.3: Interfaz web de un dispositivo en España

3. Selección de 3 dispositivos y análisis de sus vulnerabilidades

Dispositivos webcamxp

Descripción	Cámaras IP de videovigilancia gestionadas mediante el software <code>webcamxp</code> , accesibles a través de una interfaz web HTTP/HTTPS.
Parámetros de búsqueda	<code>webcamxp country:es</code>
# de resultados	<i>5 resultados para webcamxp country:es</i>
Parámetros de acceso por defecto	Acceso a través de navegador web apuntando a la IP pública y puerto HTTP/HTTPS publicados; si el administrador no ha cambiado la configuración, el servicio puede estar expuesto con credenciales por defecto o incluso sin autenticación sólida.

IP:	81.22.234.236
Organización:	AVATEL TELECOM, SA
Localización:	Torrevieja, Spain
Puerto:	80/tcp (redirección a HTTPS en el mismo host)
URL:	<code>http://81.22.234.236/</code> → redirige a <code>https://81.22.234.236/</code>
Observación:	El servicio en el puerto 80 responde con un código HTTP 308 Permanent Redirect hacia HTTPS y usa el servidor web Caddy; el dispositivo está etiquetado como IoT y presenta múltiples puertos abiertos, lo que indica un sistema de videovigilancia o pasarela expuesta directamente a Internet.
Evidencias:	Captura de pantalla del panel de Shodan donde se observa la IP 81.22.234.236, la organización AVATEL TELECOM, SA, la localización en Torrevieja (Spain), la lista de puertos abiertos (80, 82, 83, 84, 85, 88, 89, 90, 91, 92, 94, 97, 98, 100, 106, 111, 554) y el banner HTTP del puerto 80 con respuesta 308 y servidor Caddy.
Observación	Desde el punto de vista de seguridad, la exposición de un sistema IoT con numerosos puertos abiertos y acceso web directo desde Internet incrementa la superficie de ataque; si además el servicio corresponde a un servidor de cámaras <code>webcamxp</code> , un atacante podría intentar localizar credenciales débiles para acceder a las imágenes de videovigilancia o a la consola de administración.

ExacqVision

Descripción	Sistemas de videovigilancia/NVR corporativos ExacqVision, utilizados para la grabación y gestión centralizada de cámaras IP a través de servicios web y acceso remoto.
Parámetros de búsqueda	ExacqVision
# de resultados	<i>4 resultados para ExacqVision</i>
Parámetros de acceso por defecto	Acceso mediante servicios expuestos en Internet, típicamente un servidor web IIS en el puerto 80/tcp y acceso remoto al servidor Windows mediante RDP en el puerto 3389/tcp, donde se aloja el software de videovigilancia ExacqVision.

IP:	13.91.106.128
Organización:	Microsoft Corporation (AzureCloud)
Localización:	San Jose, United States (región WestUS de Azure)
Puerto:	80/tcp (Microsoft IIS) y 3389/tcp (Remote Desktop Protocol)
URL:	http://13.91.106.128/ (servidor web IIS sobre Windows Server 2012 R2; error 500 según el banner)
Observación:	El host es una máquina virtual en Azure con sistema operativo Windows Server 2012 R2 que ejecuta IIS en el puerto 80/tcp y expone RDP en el puerto 3389/tcp; el banner de RDP identifica el dominio y nombre de equipo EXACQVISION, lo que indica que se trata de un servidor asociado a la plataforma de videovigilancia ExacqVision.
Evidencias:	Captura de pantalla de Shodan donde se observa la IP 13.91.106.128, la organización Microsoft Corporation (AzureCloud), la información de sistema operativo Windows Server 2012 R2, el servicio Microsoft IIS httpd en el puerto 80/tcp con código 500 Internal Server Error y el banner RDP del puerto 3389/tcp mostrando el nombre de host y dominio relacionados con ExacqVision.
Observación	Desde el punto de vista de seguridad, el servidor de videovigilancia está expuesto a Internet con RDP abierto y con un sistema operativo antiguo (Windows Server 2012 R2), lo que incrementa la superficie de ataque; un atacante podría intentar explotación de vulnerabilidades de RDP o IIS, así como ataques de fuerza bruta sobre credenciales de acceso remoto para comprometer la infraestructura de videovigilancia.

JUNG KNX

Descripción	Pasarela/dispositivo de automatización de edificios basado en tecnología JUNG KNX, que actúa como KNX/IP Router para integrar el bus KNX con redes IP y permitir el control remoto de funciones domóticas (iluminación, clima, etc.).
Parámetros de búsqueda	"JUNGKNX" (por ejemplo, filtrando dispositivos cuyo banner del puerto 3671/UDP se identifica como IP Router JUNG).
# de resultados	<i>4 resultados para JUNG KNX</i>
Parámetros de acceso por defecto	Acceso KNXnet/IP en puerto 3671/UDP e interfaz web en puertos HTTP (8080/tcp); autenticación básica con credenciales por defecto permite gestionar automatización desde Internet.

IP:	88.19.44.142
Organización:	Telefonica de Espana SAU Red de servicios IP Spain
Localización:	Madrid, Spain
Puerto:	3671/UDP (KNX Gateway), 8080/tcp, 8081/tcp, 8083/tcp, 8123/tcp
URL:	http://88.19.44.142:8080/ (servidor <code>thttpd/2.19</code> ; responde 401 Unauthorized con autenticación básica "MOBOTIX Camera User").
Observación:	El puerto 3671/UDP se identifica como KNX Gateway con nombre de dispositivo IP Router JUNG; el banner muestra información de Siemens AG y servicios soportados, confirmado que es una pasarela KNX/IP JUNG en un entorno de automatización.
Evidencias:	Captura de Shodan donde se observa el dominio <code>rima-tde.net</code> , el servidor web <code>thttpd</code> en los puertos 8080/8081/8083/8123, el error HTTP 401 Unauthorized con cabecera <code>WWW-Authenticate: Basic realm="MOBOTIX Camera User"</code> , así como el banner detallado del puerto 3671/UDP describiendo el dispositivo como KNX Gateway y IP Router JUNG.
Observación	La exposición de una pasarela KNX/IP a Internet con autenticación básica puede permitir a un atacante acceder al sistema de cámaras y automatización, especialmente si las credenciales son débiles o por defecto.