

CURSO ONLINE DE CIBERSEGURIDAD

Especialidad Introducción a la
Ciberseguridad Industrial

Taller 1

Unidad 5. Introducción a la
ciberseguridad industrial



GOBIERNO
DE ESPAÑA
VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL

incibe_



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Contenidos

- | | | |
|---|--|----|
| 1 | USO DE SHODAN Y GOOGLE PARA EL DESCUBRIMIENTO DE SISTEMAS OT EXPUESTOS | 5 |
| 2 | CONSIDERACIONES PREVIAS | 7 |
| 3 | ACCESO Y REGISTRO EN LA PÁGINA WEB DE SHODAN | 9 |
| 4 | BÚSQUEDAS DESDE LA INTERFAZ WEB | 15 |
| 5 | BÚSQUEDAS DESDE LA INTERFAZ WEB:
SCREENSHOTS | 36 |
| 6 | BÚSQUEDAS DESDE LA CLI: COMANDO <i>INIT</i> | 52 |

Contenidos

7	BÚSQUEDAS DESDE LA CLI: COMANDO STATS	59
8	BÚSQUEDAS DESDE LA CLI: COMANDO COUNT	71
9	BÚSQUEDAS DESDE LA CLI: COMANDO SEARCH	84
10	BÚSQUEDAS DESDE LA CLI: UTILIZACIÓN CONJUNTA DE LOS COMANDOS COUNT, STATS Y SEARCH	98
11	BÚSQUEDAS DESDE LA CLI: COMANDO DOWNLOAD	112
12	BÚSQUEDAS DESDE LA CLI: COMANDO PARSE	126

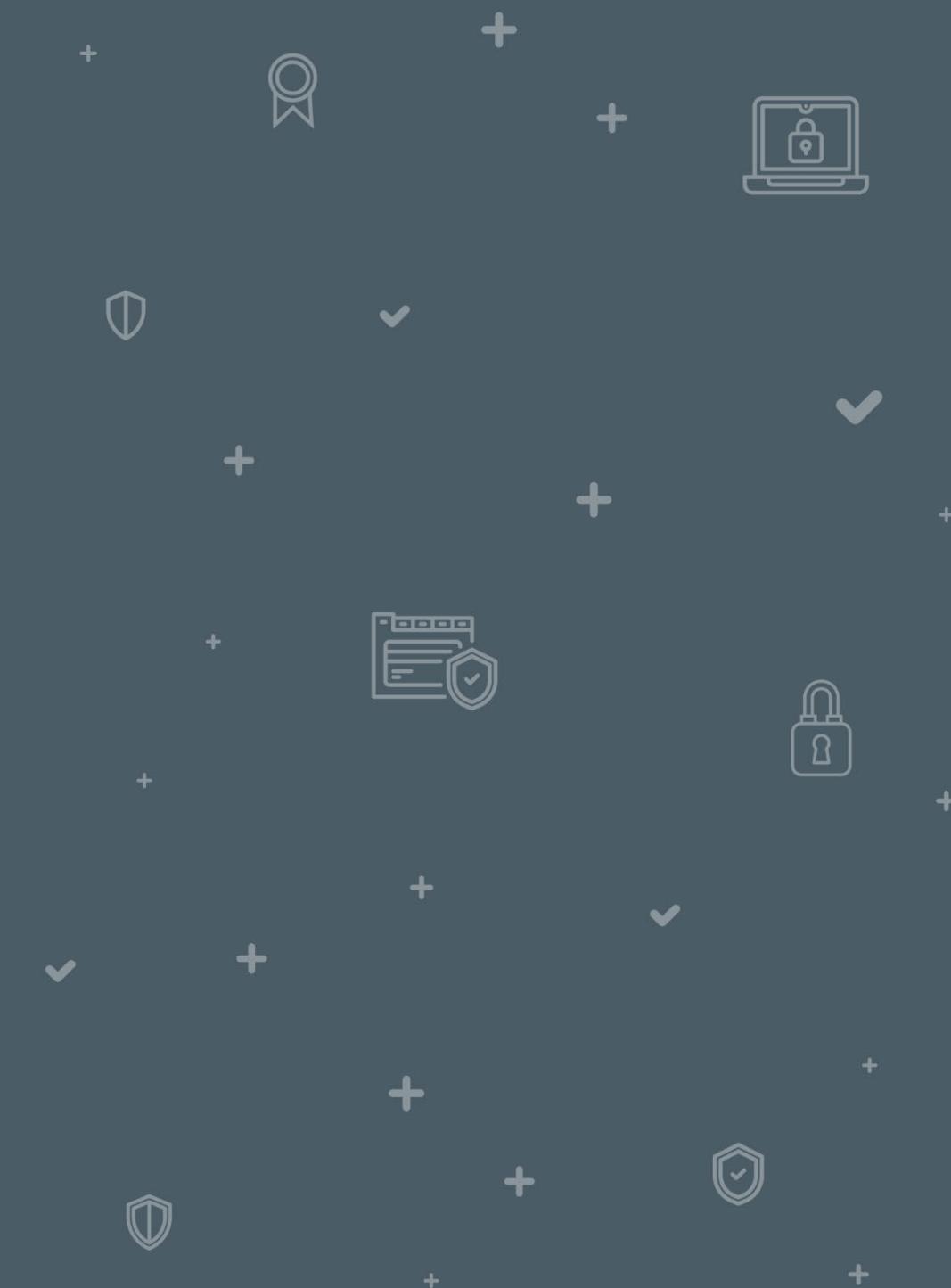
Contenidos

- | | | |
|----|--|-----|
| 13 | BÚSQUEDAS DESDE LA CLI: COMANDO CONVERT | 144 |
| 14 | BÚSQUEDAS DESDE LA CLI: COMANDOS HOST Y HONEYSCORE | 149 |
| 15 | EJERCICIO PRÁCTICO 1 | 162 |
| 16 | EJERCICIO PRÁCTICO 2 | 172 |

Duración total del taller: 3 horas y 30 minutos

USO DE SHODAN Y GOOGLE PARA EL DESCUBRIMIENTO DE SISTEMAS OT EXPUESTOS

1





USO DE SHODAN Y GOOGLE PARA EL DESCUBRIMIENTO DE SISTEMAS OT EXPUESTOS

Shodan es un motor de búsqueda, que, a diferencia de los buscadores de contenido como Google o Bing, es capaz de rastrear, detectar e identificar los dispositivos conectados a Internet (entre ellos, los dispositivos industriales), mediante la detección de los puertos abiertos, y clasificar e indexar estos dispositivos en función de la respuesta que da el servicio de que se trate, ante los escaneos e intentos de conexión que realiza Shodan.

Shodan permite realizar búsquedas de dispositivos utilizando filtros de búsqueda (es necesario estar registrado con una cuenta gratuita). También permite realizar búsquedas utilizando cadenas de texto.

En esta práctica vamos a aprender el uso de Shodan utilizando su interfaz gráfica desde la página web de Shodan, así como el uso de la herramienta CLI (*command-line interface* o interfaz de línea de comandos) Shodan para realizar las búsquedas directamente desde la terminal de tu máquina virtual donde tienes instalada la distribución Kali Linux.

CONSIDERACIONES PREVIAS

2

CONSIDERACIONES PREVIAS

Puesto que Shodan es un sistema de búsqueda dinámico y está continuamente actualizando su base de datos con los resultados de los sistemas que identifica conectados a Internet, es posible que cuando se realice esta práctica los resultados que obtenga el alumno no coincidan con los resultados que se muestran en este documento.

ACCESO Y REGISTRO EN LA PÁGINA WEB DE SHODAN

3



3 ACCESO Y REGISTRO EN LA PÁGINA WEB DE SHODAN

- En este apartado te registrarás en el motor de búsqueda Shodan y crearás una cuenta gratuita.
 - Para ello, accede a la pagina web oficial de [Shodan](#).
- Haz clic en el botón de «*Login*» y luego en el botón de «*Register*».

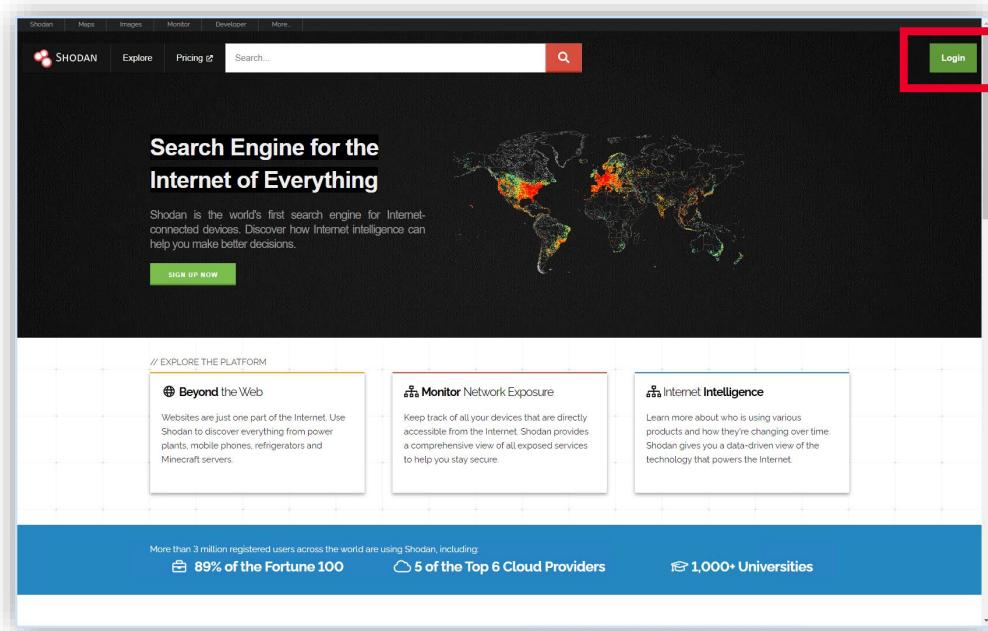


Ilustración 1: Acceso a la página de Shodan.

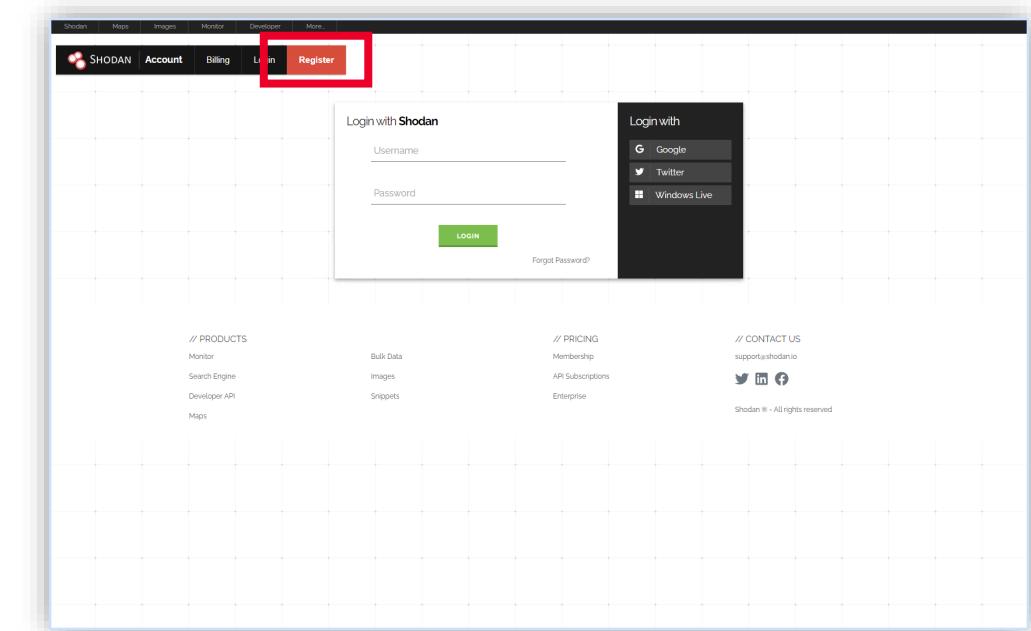


Ilustración 2: Registro.

3 ACCESO Y REGISTRO EN LA PÁGINA WEB DE SHODAN

- Rellena los datos para crear una cuenta y pulsa el botón «Create».

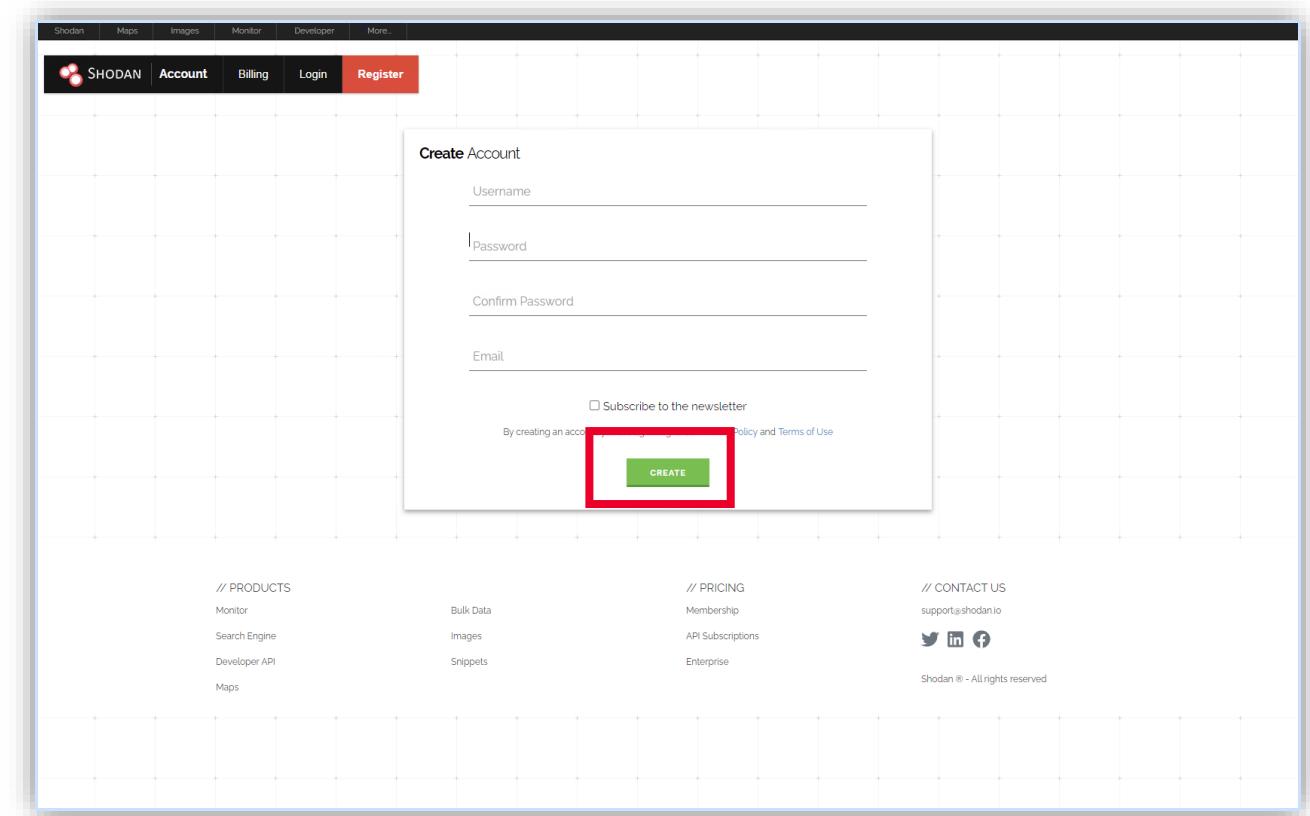


Ilustración 3: Imagen de la pantalla en la que se introducen los datos de acceso.

3 ACCESO Y REGISTRO EN LA PÁGINA WEB DE SHODAN

- Si todo ha ido correctamente, aparecerá una ventana emergente en color verde.

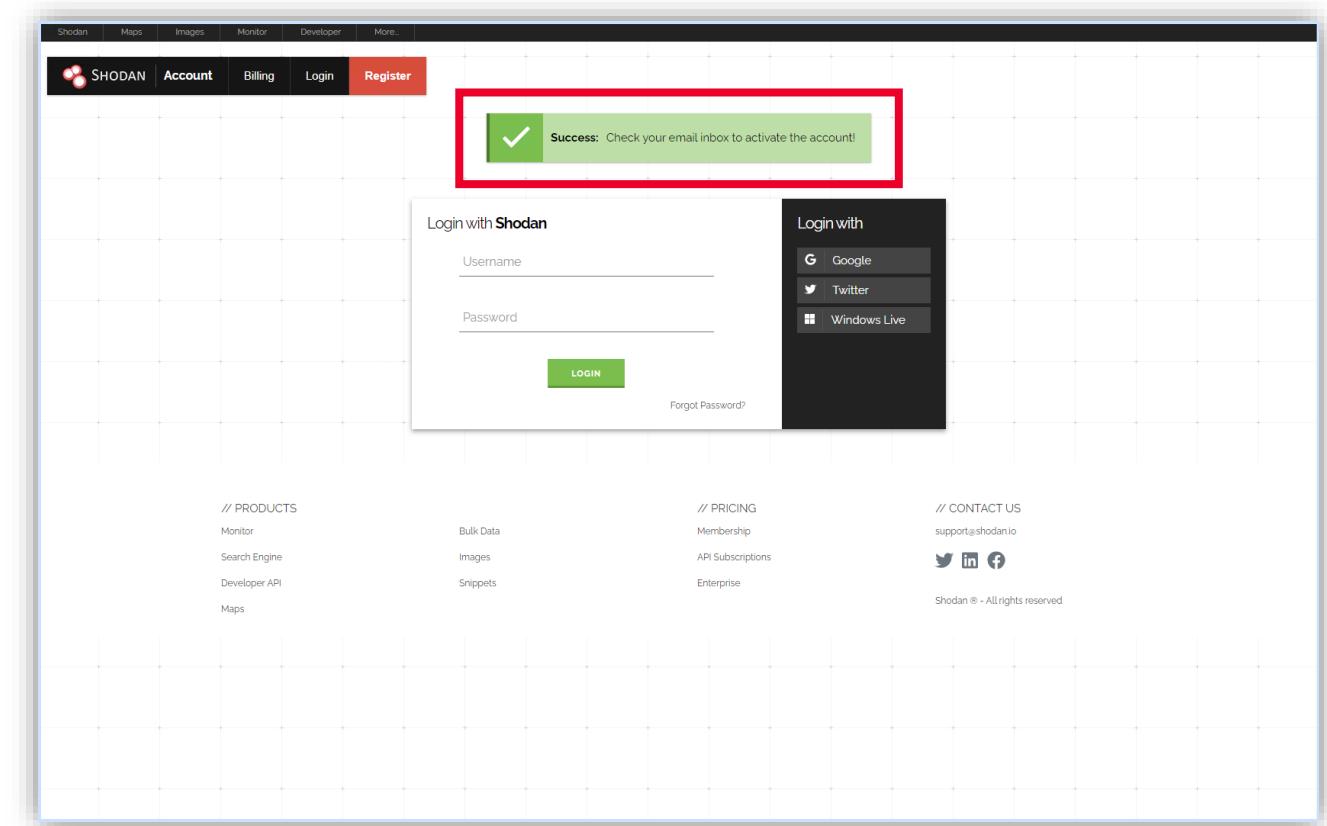


Ilustración 4: Aviso de confirmación.

3 ACCESO Y REGISTRO EN LA PÁGINA WEB DE SHODAN

- Accede a la dirección de correo que has proporcionado para activar la cuenta. Comprueba que has recibido un correo de la plataforma Shodan. Haz clic en la dirección que aparece en el correo para activar la cuenta de Shodan, de esta forma se abrirá directamente la web de Shodan y verás un mensaje donde se te informa de que la cuenta se ha activado con éxito.

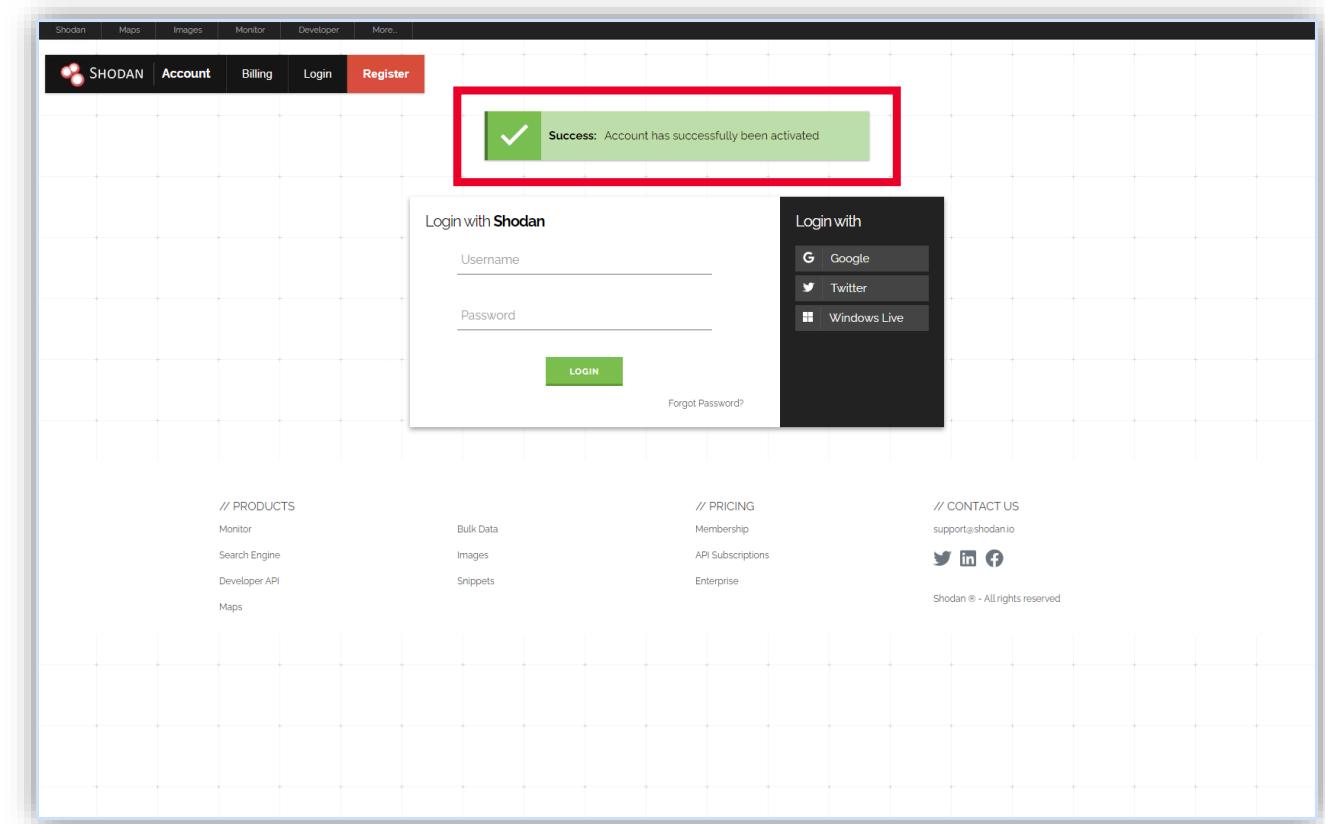


Ilustración 5: Activación del registro.

3 ACCESO Y REGISTRO EN LA PÁGINA WEB DE SHODAN

Nota: este tipo de cuenta gratuita tiene una serie de limitaciones:

- El número máximo de búsquedas diarias está limitado a unas 20.
- Solo se puede acceder a las dos primeras páginas de resultados de búsquedas.

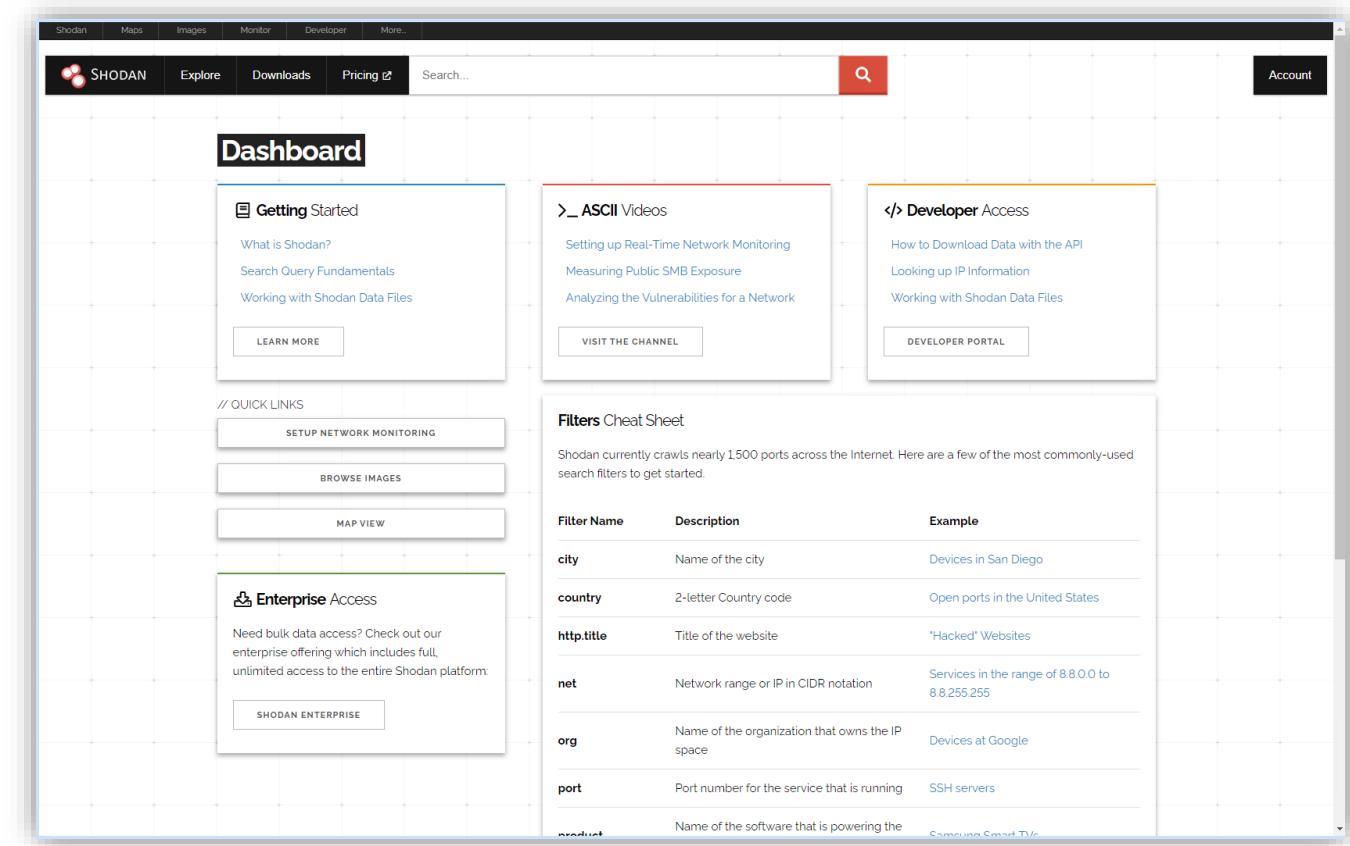
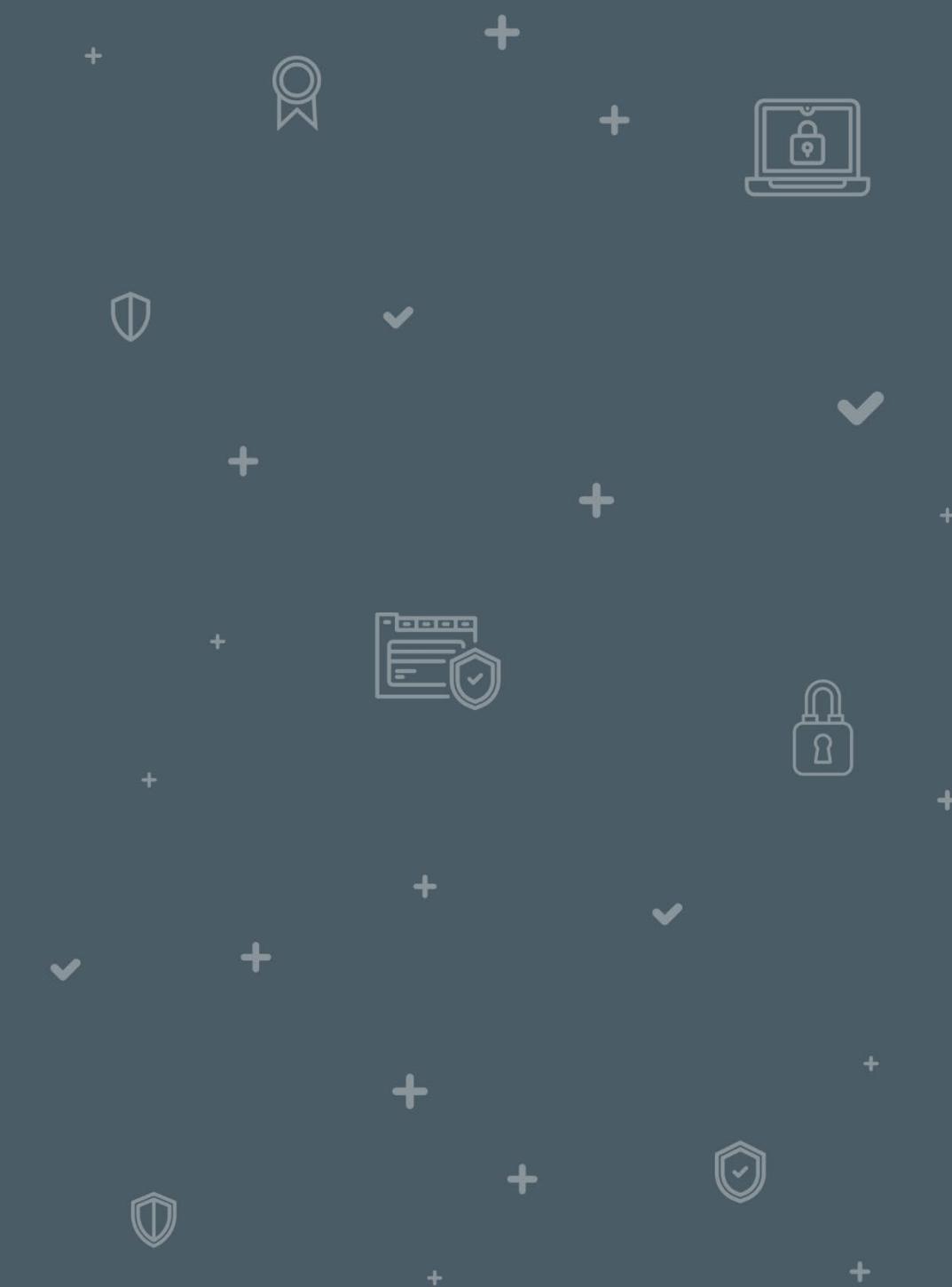


Ilustración 6: *Dashboard* de Shodan.

BÚSQUEDAS DESDE LA INTERFAZ WEB

4



4

BÚSQUEDAS DESDE LA INTERFAZ WEB

- Ahora, vamos a familiarizarnos con la interfaz web que proporciona Shodan y a realizar búsquedas de dispositivos industriales, como un PLC.
- Haz clic en el botón «Explore», que es la parte de la web donde se realizan las búsquedas.
 - En la página que se abre, haz clic en la imagen «*Industrial Control System*», que ofrece información sobre los sistemas ICS.

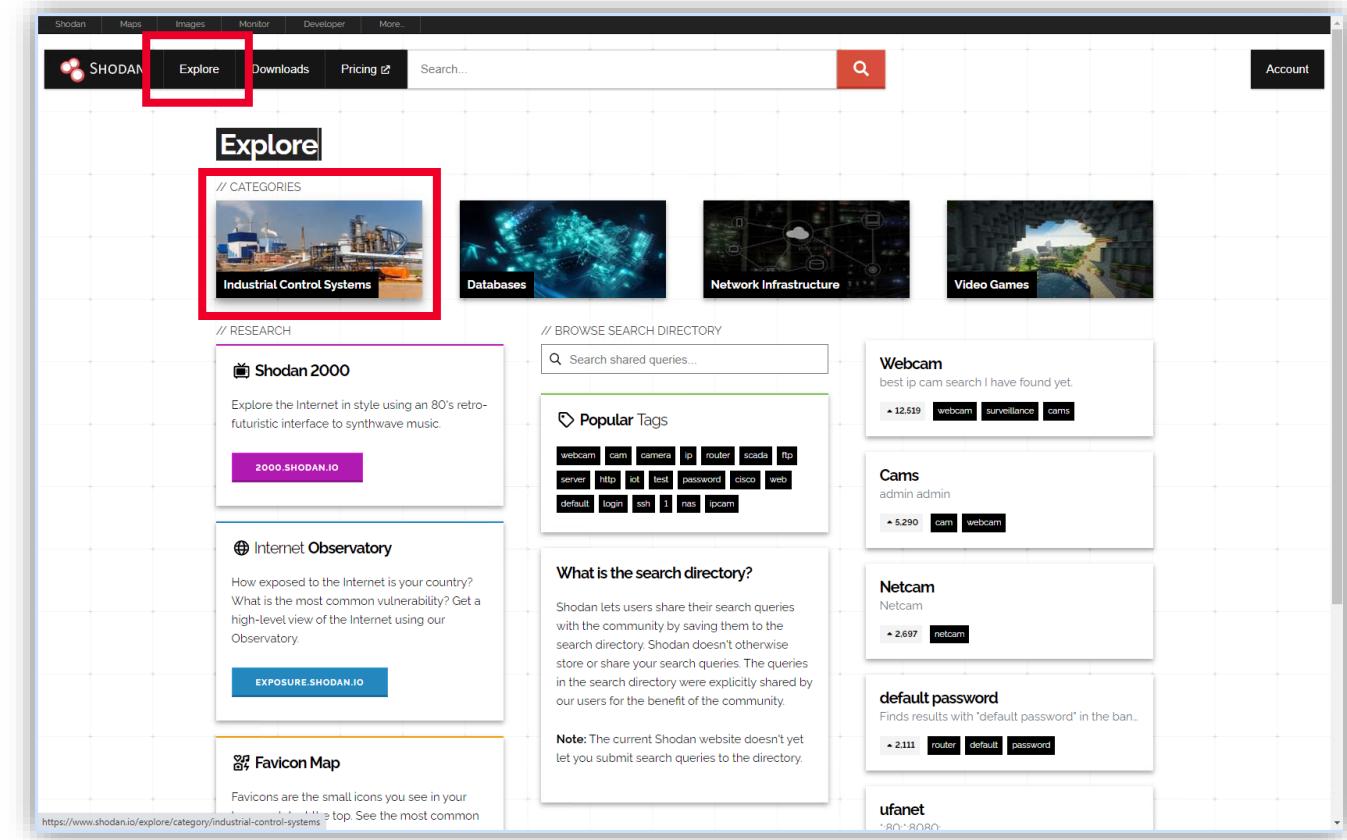


Ilustración 7: Búsquedas con el botón «Explore», se accede a la opción «*Industrial Control System*».

4

BÚSQUEDAS DESDE LA INTERFAZ WEB

- Si pulsas el botón «EXPLORE MODBUS», realiza una búsqueda preconfigurada del puerto 502 que corresponde al protocolo industrial Modbus.

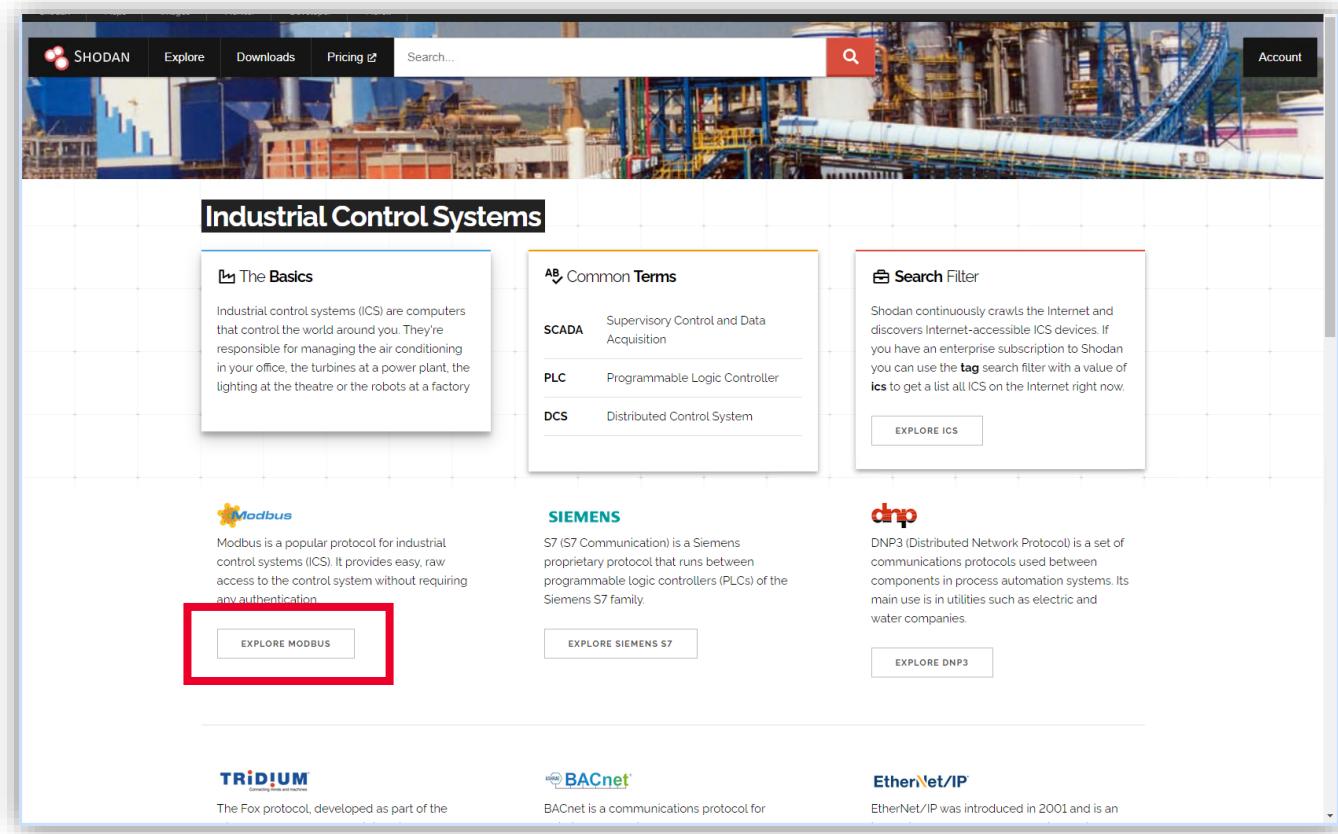


Ilustración 8: Pulsando en el botón «EXPLORE MODBUS» se realiza una búsqueda preconfigurada del puerto 502 correspondiente al protocolo industrial Modbus.

4

BÚSQUEDAS DESDE LA INTERFAZ WEB

- En el campo de búsqueda puedes observar el filtro que se ha aplicado: port:502.

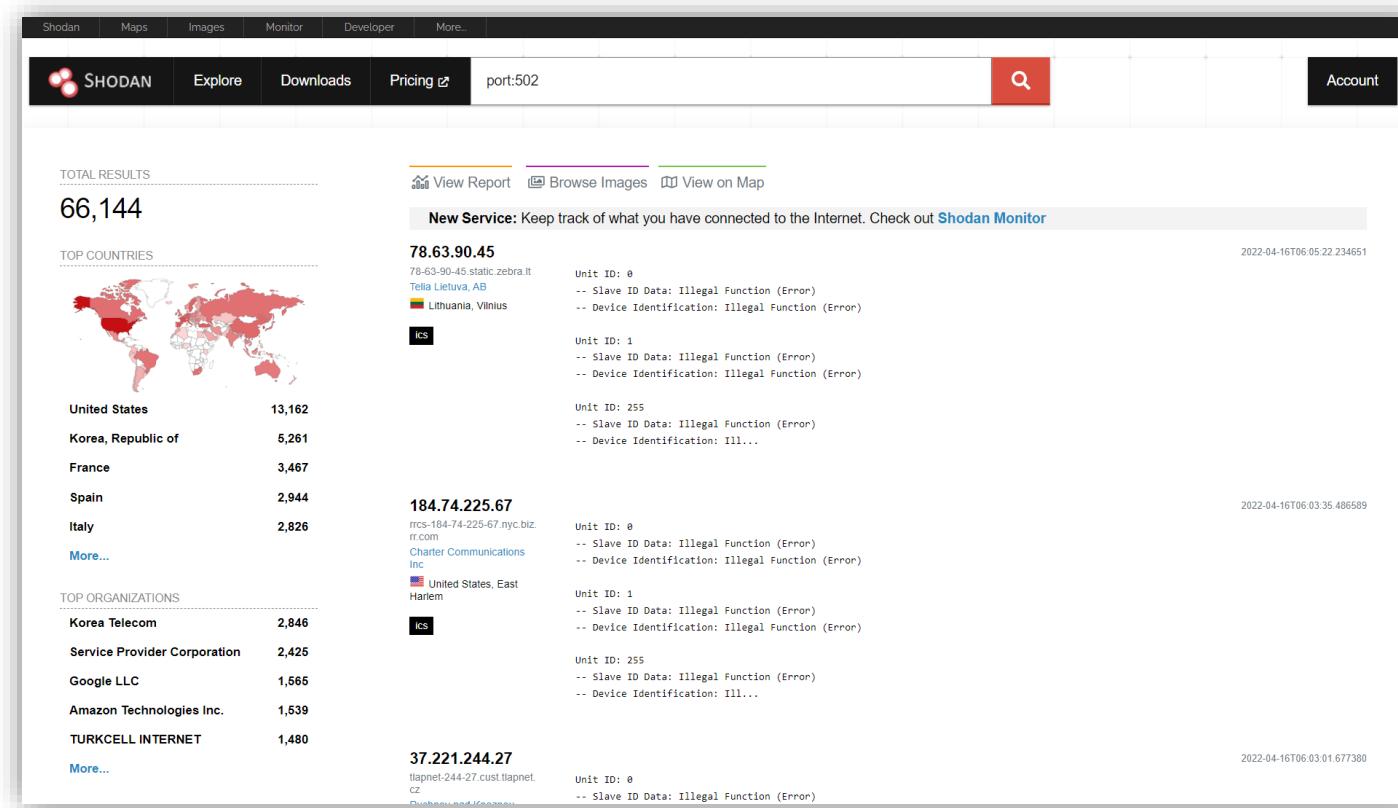


Ilustración 9: Resultados del filtro aplicado.

4

BÚSQUEDAS DESDE LA INTERFAZ WEB

- La página de resultados tiene la siguiente estructura, una columna a la izquierda donde en la parte superior se ve el total de resultados. Bajo esta entrada nos encontramos con una zona de estadísticas de resultados por países, por organizaciones, por dispositivos, etc. Luego se muestra una parte central con el listado de resultados.

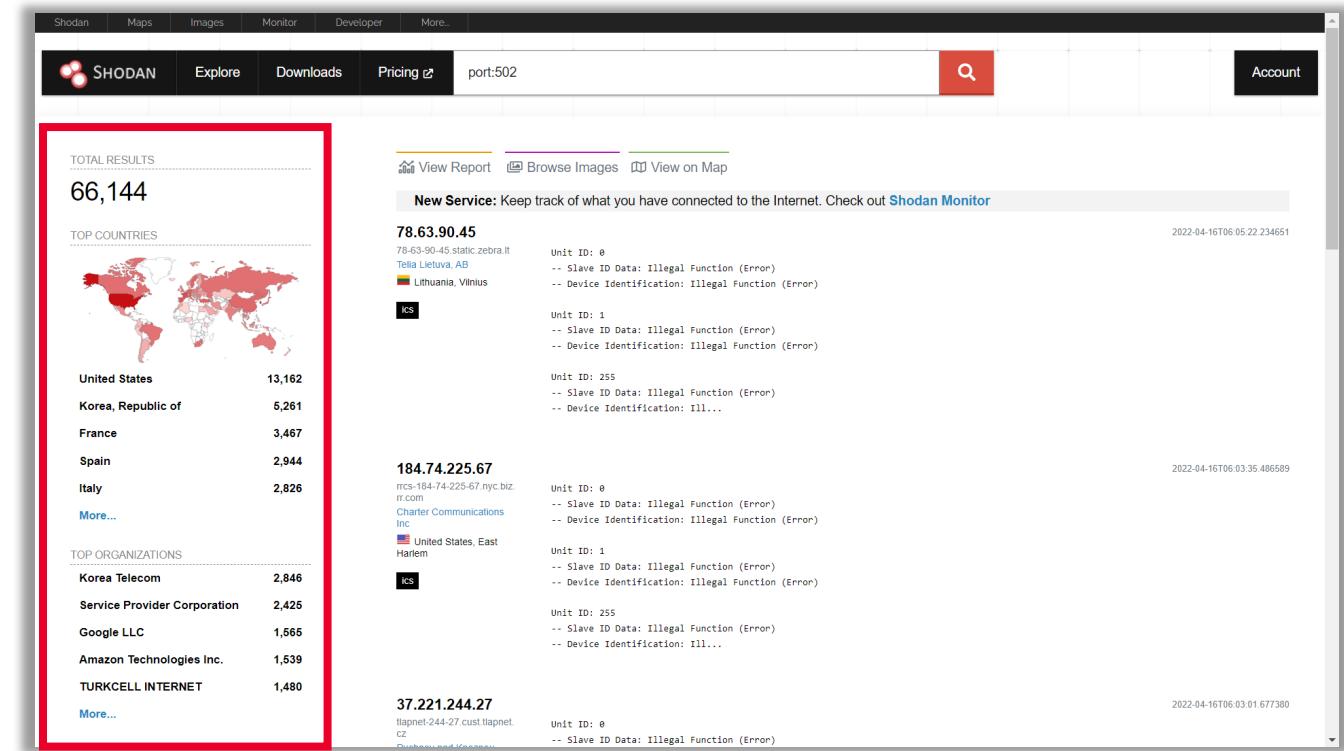


Ilustración 10: Página de resultados de búsqueda, destacada la zona de estadísticas de resultados por países, organizaciones, dispositivos, etc.

4

BÚSQUEDAS DESDE LA INTERFAZ WEB

- Si en la columna de la izquierda haces clic en cada uno de los resultados, se aplica un nuevo filtro de búsqueda, donde se va reduciendo el número de dispositivos encontrados.
- Volviendo a nuestro ejercicio, haz clic en la entrada «Spain» y «Madrid». Como puedes observar, el resultado de la búsqueda devuelve 867 dispositivos y, en el campo de búsqueda se han añadido los filtros país España y ciudad Madrid:
 - country:"ES" city:"Madrid"

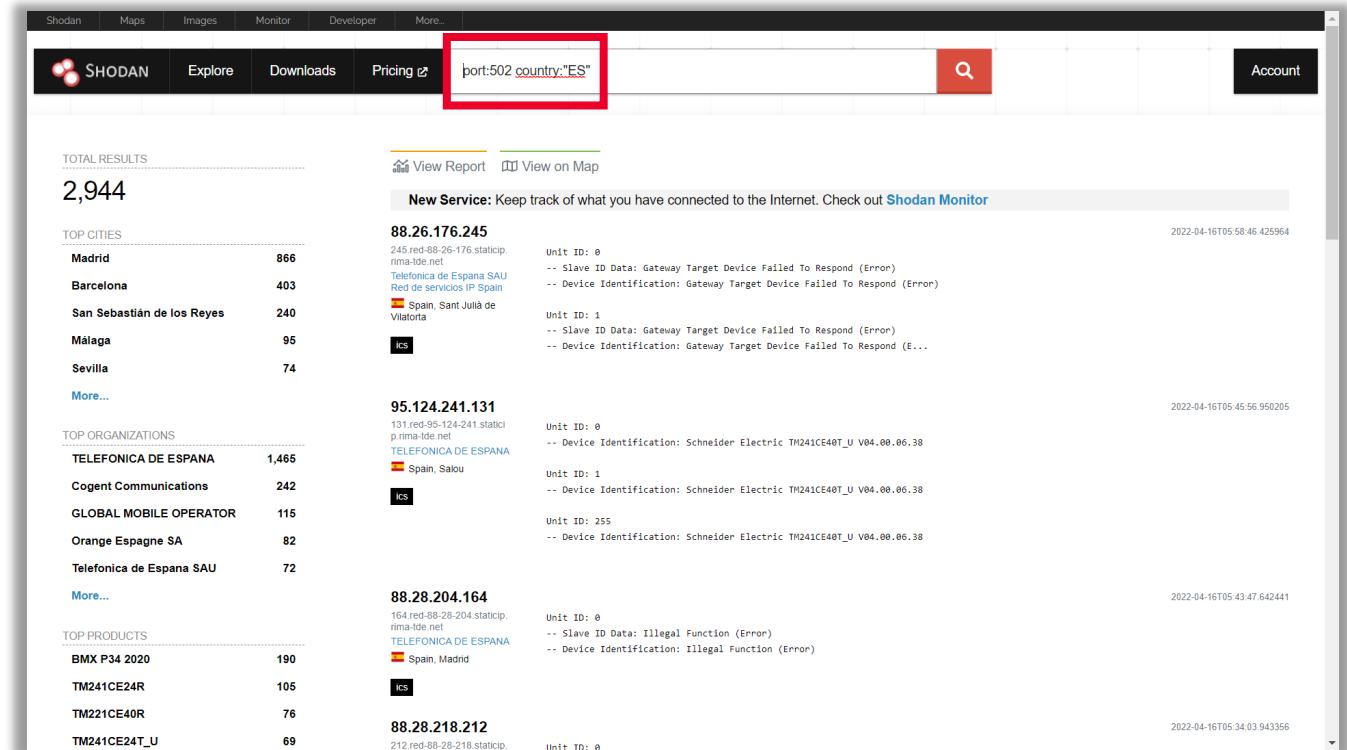


Ilustración 11: Resultado añadiendo como filtro el país España.

4

BÚSQUEDAS DESDE LA INTERFAZ WEB

The screenshot shows the Shodan search interface with a search query highlighted: "port:502 country:'ES' city:'Madrid'". The results page displays 867 total results. On the left, there are sections for TOP CITIES (Madrid: 866, Humanes de Madrid: 1) and TOP ORGANIZATIONS (TELEFONICA DE ESPANA: 575, Orange Espagne SA: 65, Mobile 4G Internet Plus Services: 38, Telefonica de Espana SAU: 23, Mobile HSDPA Internet Plus Services: 20). On the right, three specific device entries are listed:

- 88.28.204.164**: Unit ID: 0, Slave ID Data: Illegal Function (Error), Device Identification: Illegal Function (Error). Located in Spain, Madrid. (Last seen: 2022-04-16T05:43:47.642441)
- 88.28.218.212**: Unit ID: 0, Slave ID Data: Illegal Function (Error), Device Identification: Illegal Function (Error). Located in Spain, Madrid. (Last seen: 2022-04-16T05:34:03.943356)
- 88.31.198.108**: Unit ID: 0, Device Identification: Schneider Electric TM221CE16T V1.0, CPU module: TM221CE16T_V1. Unit ID: 1, Device Identification: Schneider Electric TM221CE16T V1.0. Located in Spain, Madrid. (Last seen: 2022-04-16T05:29:29.727214)

Below these, another entry for **81.36.155.87** is shown with Unit ID: 255, Device Identification: INVENTSYN 00AE_0401 01A7_001B.

Ilustración 12: Resultado añadiendo como filtros «Spain» y «Madrid». Devuelve 867 dispositivos.



BÚSQUEDAS DESDE LA INTERFAZ WEB

- Haz clic en la entrada de la izquierda TM251MESE, dentro de la agrupación «PRODUCTS», de esta forma se aplica un nuevo filtro de búsqueda, el de producto TME251MESE.
 - product:"TM251MESE"

The screenshot shows the Shodan search interface with the following search parameters: port:502 country:ES city:Madrid. The results page displays the following sections:

- TOTAL RESULTS:** 867
- TOP CITIES:** Madrid (866), Humanes de Madrid (1)
- TOP ORGANIZATIONS:** TELEFONICA DE ESPANA (575), Orange Espagne SA (65), Mobile 4G Internet Plus Services Coslada Site (38), Telefonica de Espana SAU (23), Mobile HSDPA Internet Plus Services Coslada Site (20)
- TOP PRODUCTS:** BMX P34 2020 (101), TM241CE24T U (50), TM251MESE (13), TM221CE16T (10), TM221CE16T (9)
- Result Details for TM251MESE:**
 - IP: 88.28.204.164
 - Unit ID: 0
 - Slave ID Data: Illegal Function (Error)
 - Device Identification: Illegal Function (Error)
- Result Details for TM221CE16T:**
 - IP: 88.28.218.212
 - Unit ID: 0
 - Slave ID Data: Illegal Function (Error)
 - Device Identification: Illegal Function (Error)
- Result Details for TM221CE16T:**
 - IP: 88.31.198.108
 - Unit ID: 0
 - Device Identification: Schneider Electric TM221CE16T V1.0
 - CPU module: TM221CE16T V1
- Result Details for TM221CE16T:**
 - IP: 81.36.155.87
 - Unit ID: 255
 - Device Identification: Schneider Electric TM221CE16T V1.0

Ilustración 13: Panel izquierdo donde se accede a la entrada TM251MESE en el apartado de productos.

4

BÚSQUEDAS DESDE LA INTERFAZ WEB

- Ahora, has localizado 13 dispositivos Modbus con el puerto 502 abierto, tipo producto TM251MESE (se trata de un modelo de PLC) que pertenece al fabricante Schneider Electric y localizados en Madrid. Para ello has aplicado la siguiente combinación de filtros de búsqueda:
 - port:502 country:"ES" city:"Madrid" product:"TM251MESE"

4

BÚSQUEDAS DESDE LA INTERFAZ WEB

Nota: Como puedes observar en los filtros de tipo cadena de texto, el texto de búsqueda va entre los caracteres dobles comillas. Es recomendable utilizarlas sobre todo cuando el término de búsqueda contenga espacios en blanco.

The screenshot shows the Shodan search interface with a search query highlighted in red: "port:502 country:'ES' city:'Madrid' product:'TM251MESE'". The search results page displays 13 total results. The first result is for IP 88.28.209.154, which is identified as a Schneider Electric TM251MESE device. The second result is for IP 88.28.218.253, also a Schneider Electric TM251MESE device. The third result is for IP 83.56.16.17, another Schneider Electric TM251MESE device. All three results are from Telefonica de Espana SAU in Madrid, Spain, and are categorized under the ICS (Industrial Control Systems) sector.

Ilustración 14: Resultado de 13 dispositivos Modbus con el puerto 502 abierto.

4

BÚSQUEDAS DESDE LA INTERFAZ WEB

- Si el número de resultados es mayor que 10, aparecerá al final de la página un botón «next», que, al pulsarlo, avanzaremos a la página 2 de resultados de búsqueda (como si fuera un buscador tipo Google).
- Haz clic sobre el primero para ver más información sobre el mismo.

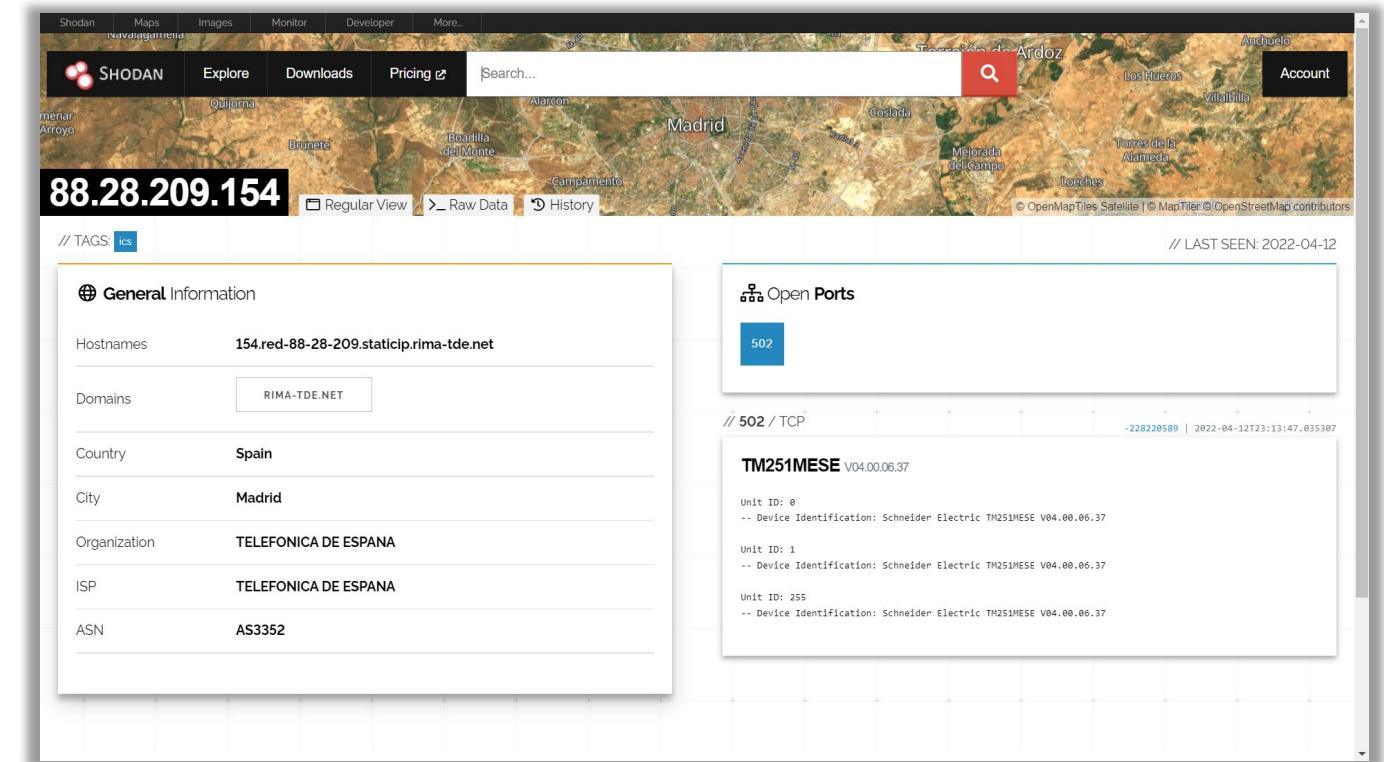


Ilustración 15: Acceso al primer resultado.

4

BÚSQUEDAS DESDE LA INTERFAZ WEB

- La página de resultados tiene la siguiente estructura, una columna a la izquierda donde en la parte superior se ve el total de resultados. Bajo esta entrada encontramos con una zona de estadísticas de resultados por países, por organizaciones, por dispositivos, etc. Luego se muestra una parte central con el listado de resultados.
- La zona central de cada una de las páginas de resultados es donde aparece el listado de dispositivos que has localizado.
- Haz clic en la entrada de la dirección IP accede a toda la información que Shodan ha recopilado de este dispositivo. En la página que se abre la información está estructurada de la siguiente manera:
 - En la parte superior muestra un mapa con información de la localización del dispositivo, en nuestro caso Madrid.
 - En la parte izquierda aparece información general del *host*.

4

BÚSQUEDAS DESDE LA INTERFAZ WEB

- En la parte derecha muestra información de los puertos abiertos, y cuando se detectó el dispositivo por última vez, así como el modelo de dispositivo detectado y la información que ha intercambiado el dispositivo cuando ha sido interrogado por Shodan.
- En nuestro caso, el primer resultado que devuelve la búsqueda con Shodan, muestra la siguiente información:
 1. Dirección IP: 88.28.209.154
 2. Compañía: Teléfonos S.A.
 3. Ubicación: España, Madrid
 4. Tag (etiqueta): ICS
 5. Información que ha devuelto el intercambio de información mediante el protocolo Modbus, donde se identifica el número de esclavo (UNIT ID: 0), el fabricante (Schneider Electric), el modelo de dispositivo o PLC (TM251MESE) y la versión de software o firmware detectada (V04.00.06.37).

4

BÚSQUEDAS DESDE LA INTERFAZ WEB

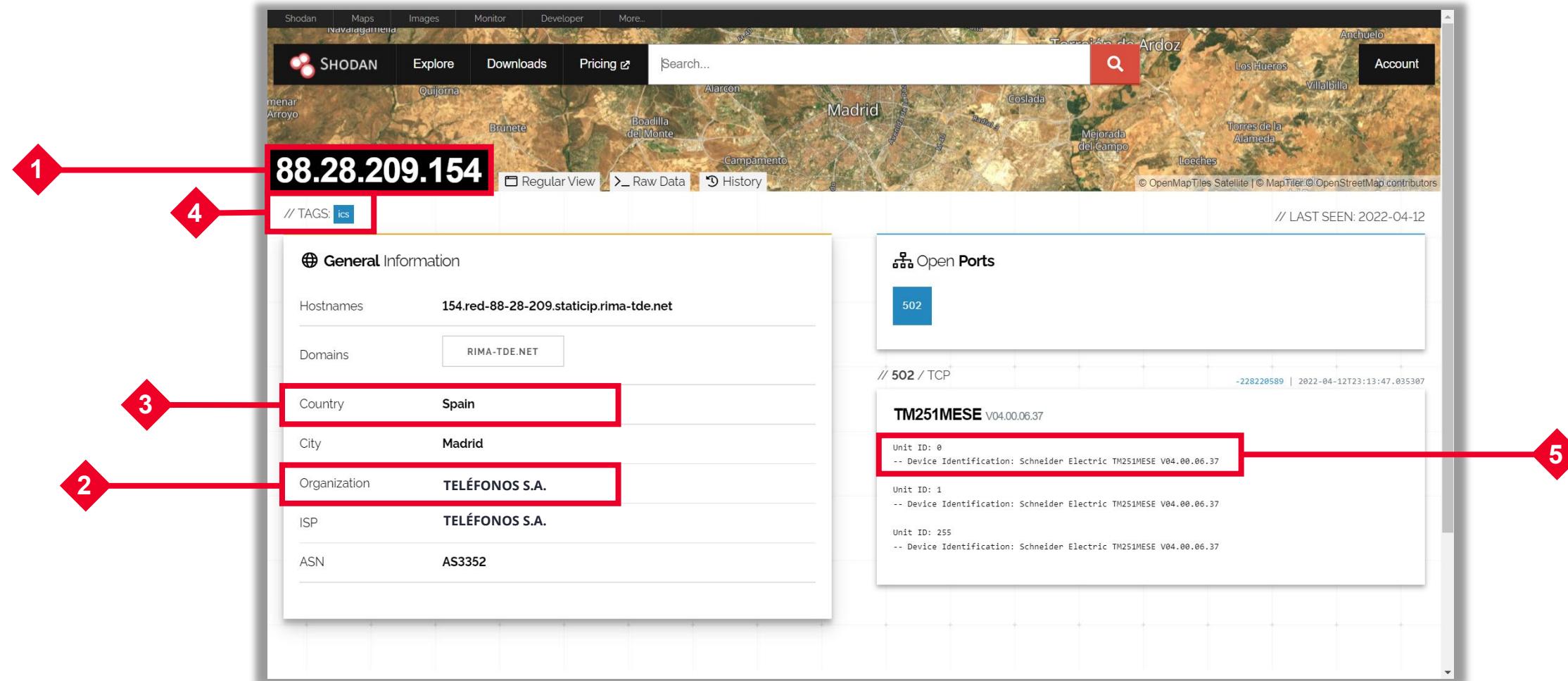


Ilustración 16: Información mostrada en el primer resultado.

4

BÚSQUEDAS DESDE LA INTERFAZ WEB

Nota: para realizar búsquedas utilizando el filtro *tag* (como, por ejemplo, *tag:ics*) es necesario contar con una suscripción de pago.

Nota: la pestaña que muestra toda esta información está identificada como *Regular View*. Las pestañas «*Raw Data*» y «*History*», requieren una suscripción de pago para poder ser utilizadas.

- Realiza una nueva búsqueda. En este caso, para localizar dispositivos que tengan el puerto 102 abierto (puerto que identifica comunicaciones de dispositivos del Fabricante Siemens), que contengan la palabra «*simatic*» (identifica la familia de dispositivos del Fabricante Siemens), y que estén ubicados en Madrid.

4 BÚSQUEDAS DESDE LA INTERFAZ WEB

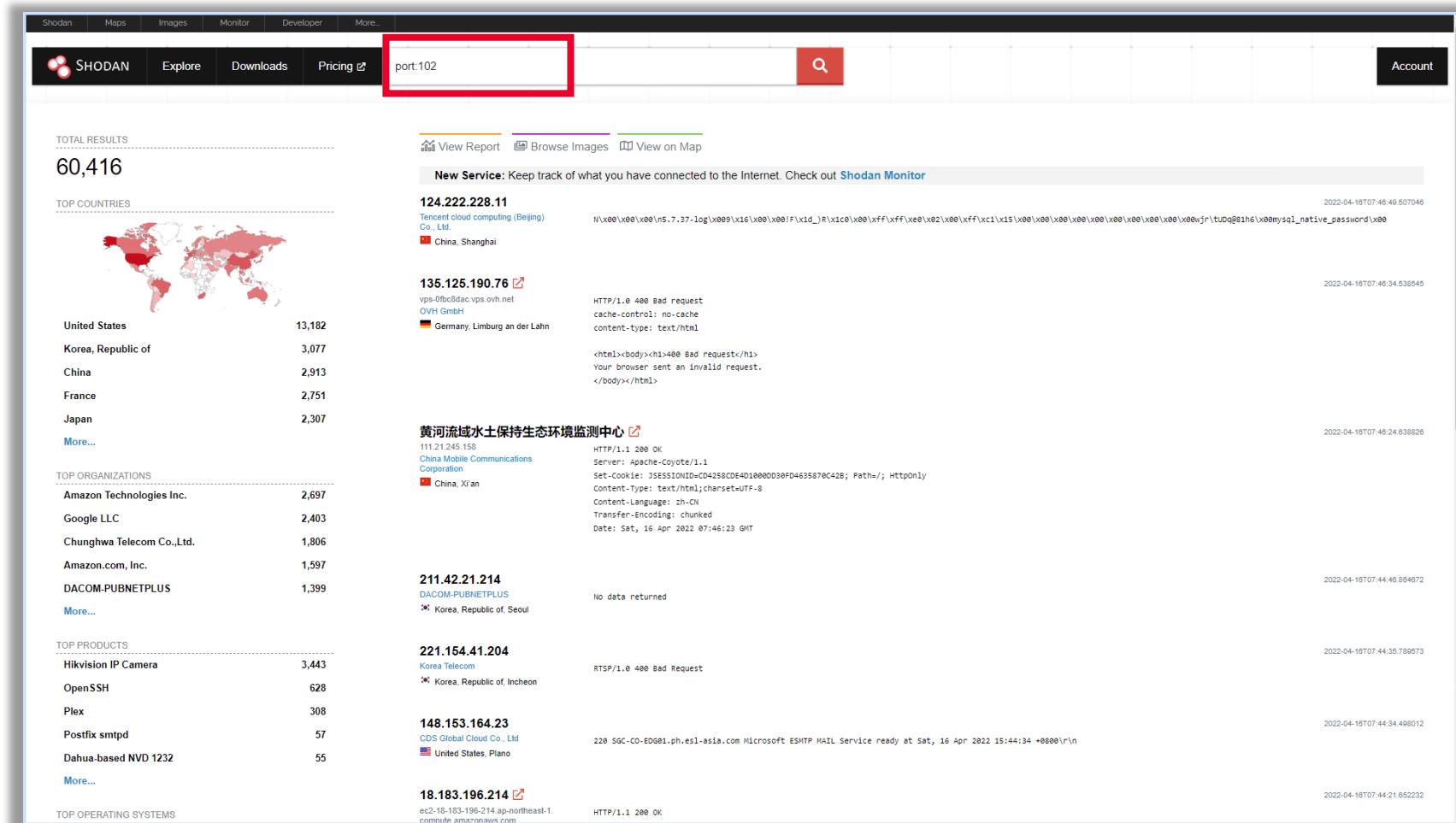


Ilustración 17: Nueva búsqueda para localizar dispositivos con el puerto 102 abierto.



BÚSQUEDAS DESDE LA INTERFAZ WEB

The screenshot shows the Shodan search interface with a red box highlighting the search bar containing the query "port:102 simatic". The results page displays 327 total findings. On the left, there are two sections: "TOP COUNTRIES" and "TOP ORGANIZATIONS", each listing countries or organizations along with their respective counts. The main area lists four specific IP addresses with their details:

- 91.123.183.172**: Located in Poland, Krakow. Copyright: Original Siemens Equipment. PLC name: SIMATIC 300 Station. Module type: CPU 315-2 DP. Unknown (129): Boot Loader. Module: 6ES7 315-2A01-0AB0 v.0.7. Basic Firmware: v.2.6.9. Module name: CPU 315-2 DP(1). Serial number of module: S C-X6VK79842869. Plant identification: Basic Hardw...
Date: 2022-04-16T07:23:12.688325
- 193.253.194.123**: Located in France, Puteaux. Copyright: Original Siemens Equipment. PLC name: SIMATIC 300 Station K1. Module type: CPU 315-2 PN/DP. Unknown (129): Boot Loader. Module: 6ES7 315-2EH14-0AB0 v.0.6. Basic Firmware: v.3.2.10. Module name: CPU315-2 PN/DP. Serial number of module: S C-E4V355072014. Plant identification: Basic...
Date: 2022-04-16T08:53:18.464187
- 194.213.63.30**: Located in Czechia, Prague. Copyright: Original Siemens Equipment. PLC name: SIMATIC 300(1). Module type: IM151-8 PN/DP CPU. Unknown (129): Boot Loader. Module: 6ES7 151-8AB01-0AB0 v.0.7. Basic Firmware: v.3.2.16. Module name: IM151-8 PN/DP CPU. Serial number of module: S LBM15309472020. Plant identification: Basic H...
Date: 2022-04-16T06:41:38.047188
- 80.14.53.224**: Located in France, Paris. Copyright: Original Siemens Equipment. PLC name: SIMATIC 300. Module type: CPU 314. Unknown (129): Boot loader.
Date: 2022-04-16T06:39:30.387742

Ilustración 18: Campo de búsqueda en el que además del puerto se pide que contenga la palabra «simatic».



BÚSQUEDAS DESDE LA INTERFAZ WEB

The screenshot shows the Shodan search interface with a search query highlighted in a red box: "port:102 simatic country:"ES"".

TOTAL RESULTS: 25

TOP CITIES:

Ciudad	Cantidad
Madrid	10
Vigo	3
Valencia	2
Carmona	1
Castelló de la Plana	1

TOP ORGANIZATIONS:

Organización	Cantidad
TELEFONICA DE ESPANA	12
Telefonica de Espana SAU	3
R Cable y Telecable Telecomunicaciones, S.A.U.	2
Bonarea Energia SLU	1
CAST-TELECOM SL	1

Search Results:

- 83.61.5.229**
Copyright: Original Siemens Equipment
PLC name: SIMATIC 300(1)
Module type: CPU 313C-2 DP
Unknown (129): Boot Loader A
Module: 6ES7 313-6CF03-0AB0 v.0.2
Basic Firmware: V.2.6.9
Module name: CPU 313C-2 DP
Serial number of module: S-C-X9VN37682009
Plant identification:
Basic Hardware: 6...
- 188.84.236.157**
Copyright: Original Siemens Equipment
PLC name: SIMATIC 300(1)
Module type: IM151-8 PN/DP CPU
Unknown (129): Boot Loader A
Module: 6ES7 151-8AB01-0AB0 v.0.2
Basic Firmware: V.3.1.3
Module name: IM151-8 PN/DP CPU
Serial number of module: S-C-B9V940782011
Plant identification:
Basic Har...
- 5.205.129.165**
Copyright: Original Siemens Equipment
PLC name: SIMATIC 300
Module type: IM151-8 PN/DP CPU
Unknown (129): Boot Loader A%
Module: 6ES7 151-8AB01-0AB0 v.0.6
Basic Firmware: V.3.2.11
Module name: IM151-8 PN/DP CPU
Serial number of module: S-C-H2DG70002016
Plant identification:
Basic Hard...
- 195.55.97.173**
Copyright: Original Siemens Equipment
PLC name: SIMATIC 300(1)
Module type: CPU 313C-2 DP
Unknown (129): Boot loader

Ilustración 19: País: España.

4

BÚSQUEDAS DESDE LA INTERFAZ WEB

- La búsqueda devuelve un resultado de 10 dispositivos en Madrid. Haz clic en el primer resultado, en la entrada de la dirección IP, para que Shodan muestre toda la información del dispositivo identificado. Como puedes observar tiene 6 puertos abiertos.

The screenshot shows the Shodan search interface with the query 'port:102 simatic country:"ES"'. The results page displays 25 total results. The first result, IP address 83.61.5.229, is highlighted with a red box. This result is associated with 'Madrid' and has 10 entries. The detailed information for this device includes:
Copyright: Original Siemens Equipment
PLC name: SIMATIC 300(1)
Module type: CPU 313C-2 DP
Unknown (129): Boot Loader A
Module: 6ES7 313-6CF03-0AE00 v.0.2
Basic Firmware: v.2.6.9
Module name: CPU 313C-2 DP
Serial number of module: S-C-X9VW07602009
Plant identification:
Basic Hardware: 6...
The IP address 83.61.5.229 is also listed under 'TOP CITIES'.

Ilustración 20: Resultado de la búsqueda.

4

BÚSQUEDAS DESDE LA INTERFAZ WEB

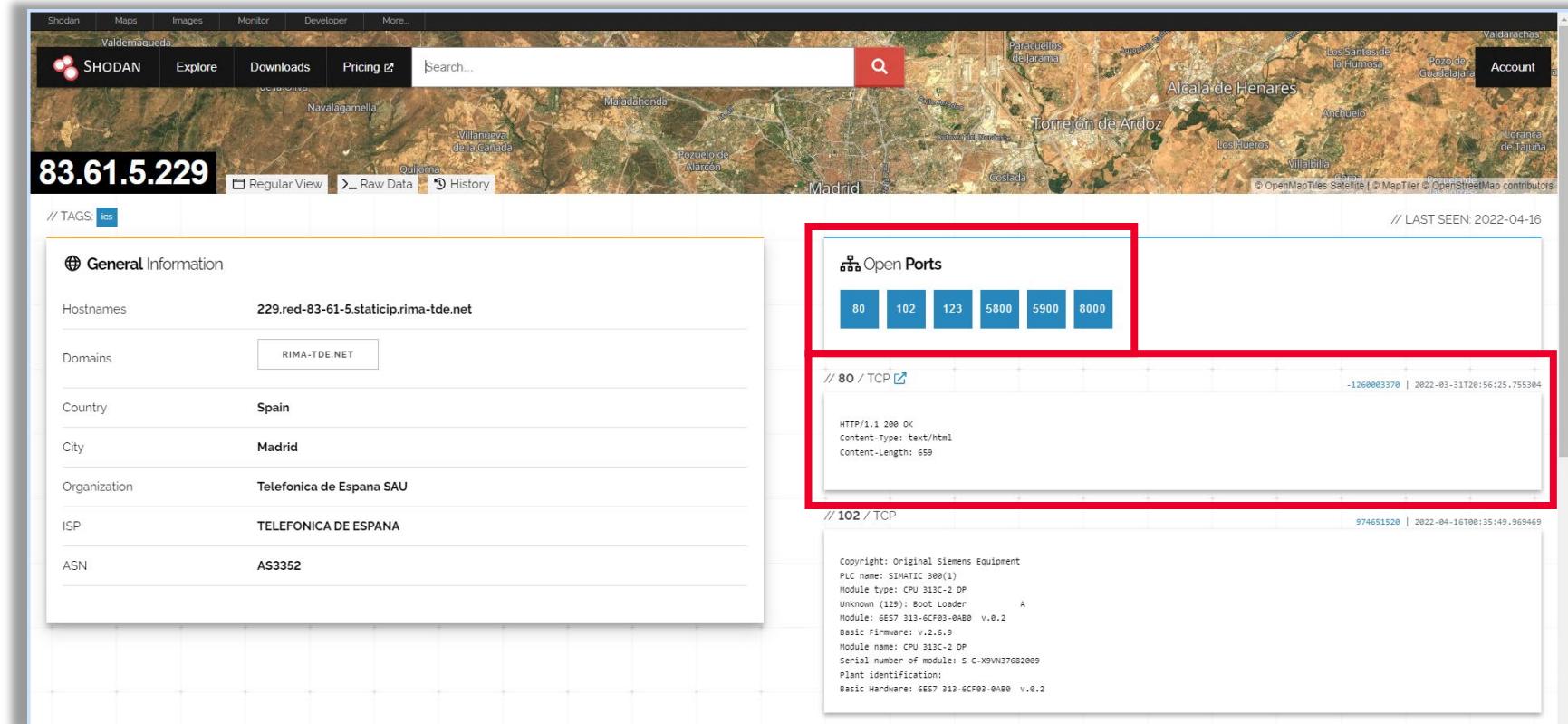


Ilustración 21: Datos de los puertos abiertos del primero de los resultados de la búsqueda anterior.

4

BÚSQUEDAS DESDE LA INTERFAZ WEB

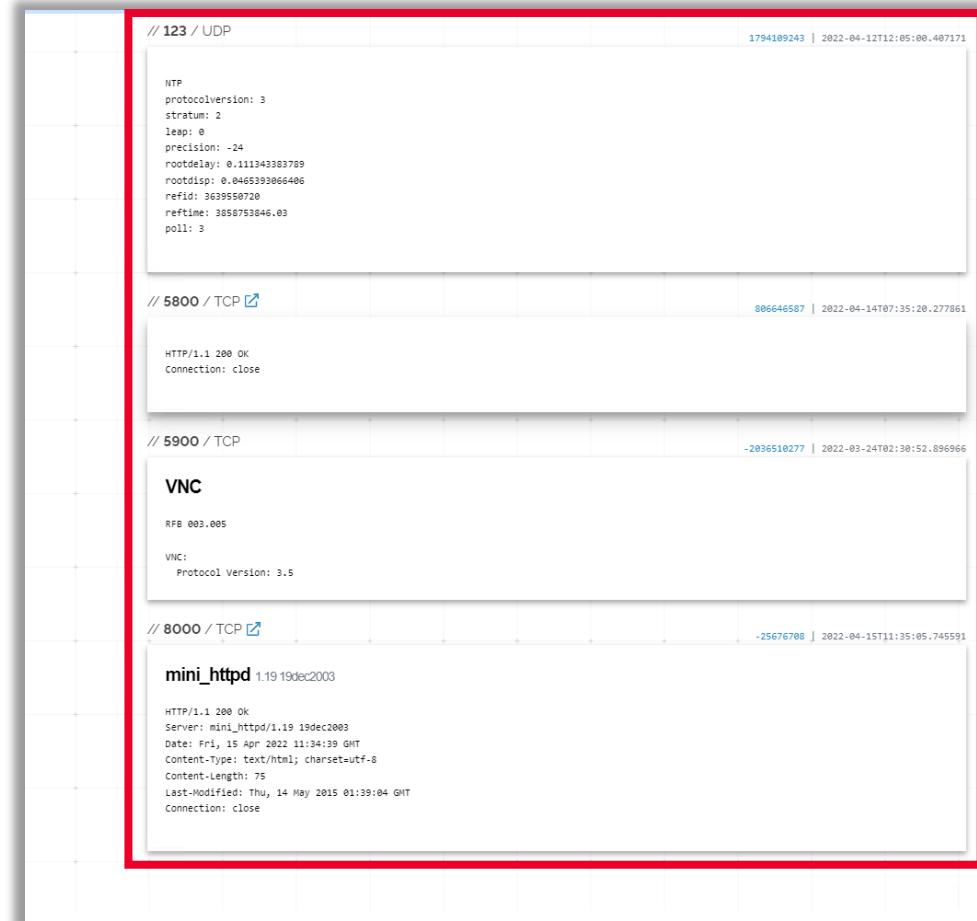
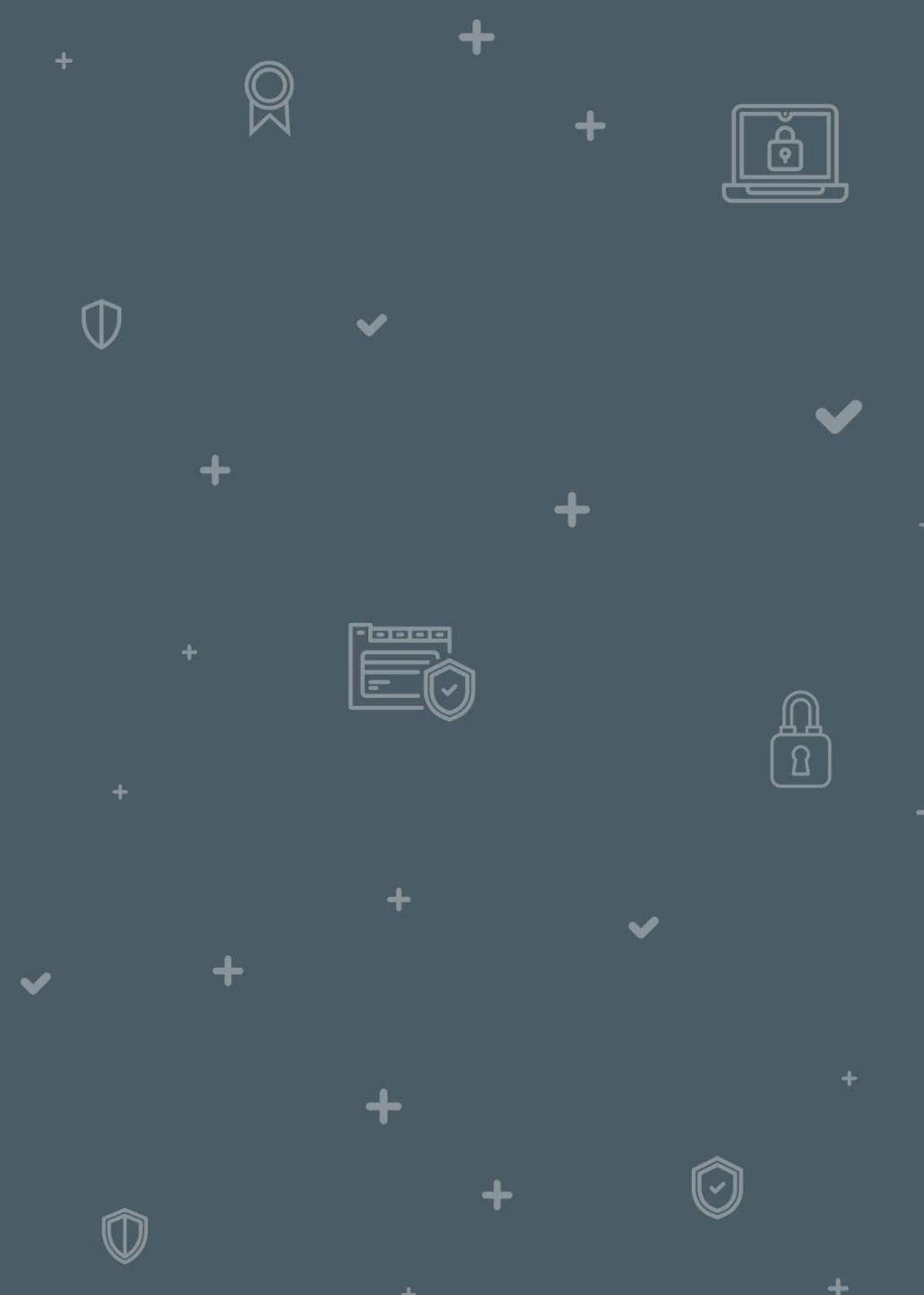


Ilustración 22: Otra información del dispositivo que ofrece Shodan.

BÚSQUEDAS DESDE LA INTERFAZ WEB: *SCREENSHOTS*

5





BÚSQUEDAS DESDE LA INTERFAZ WEB: SCREENSHOTS

- Ahora, vamos a realizar búsquedas tratando de identificar dispositivos con algún tipo de interfaz gráfica (como la pantalla que pide la introducción de credenciales utilizando los protocolos RDP (*Remote Desktop Protocol*) y VNC (*Virtual Network Computing*)) y que estas pantallas hayan sido registradas por Shodan durante los intentos de conexión contra estos dispositivos.
- Realiza una nueva búsqueda. En este caso para localizar dispositivos que hayan permitido realizar algún tipo de captura de pantalla por parte de Shodan, y que contengan la palabra «*wincc*» (que identifica el *software* de tipo SCADA del fabricante Siemens). Los términos de búsqueda utilizados son los siguientes:
 - ***wincc hasScreenshot:1***
- La búsqueda devuelve como resultado 5 dispositivos. En el primer resultado aparece una captura de pantalla que indica que se está ejecutando en ese *host* el *software* de tipo SCADA WinCC. Haz clic en su IP y se abre una página con toda la información del *host*.

5 BÚSQUEDAS DESDE LA INTERFAZ WEB: SCREENSHOTS

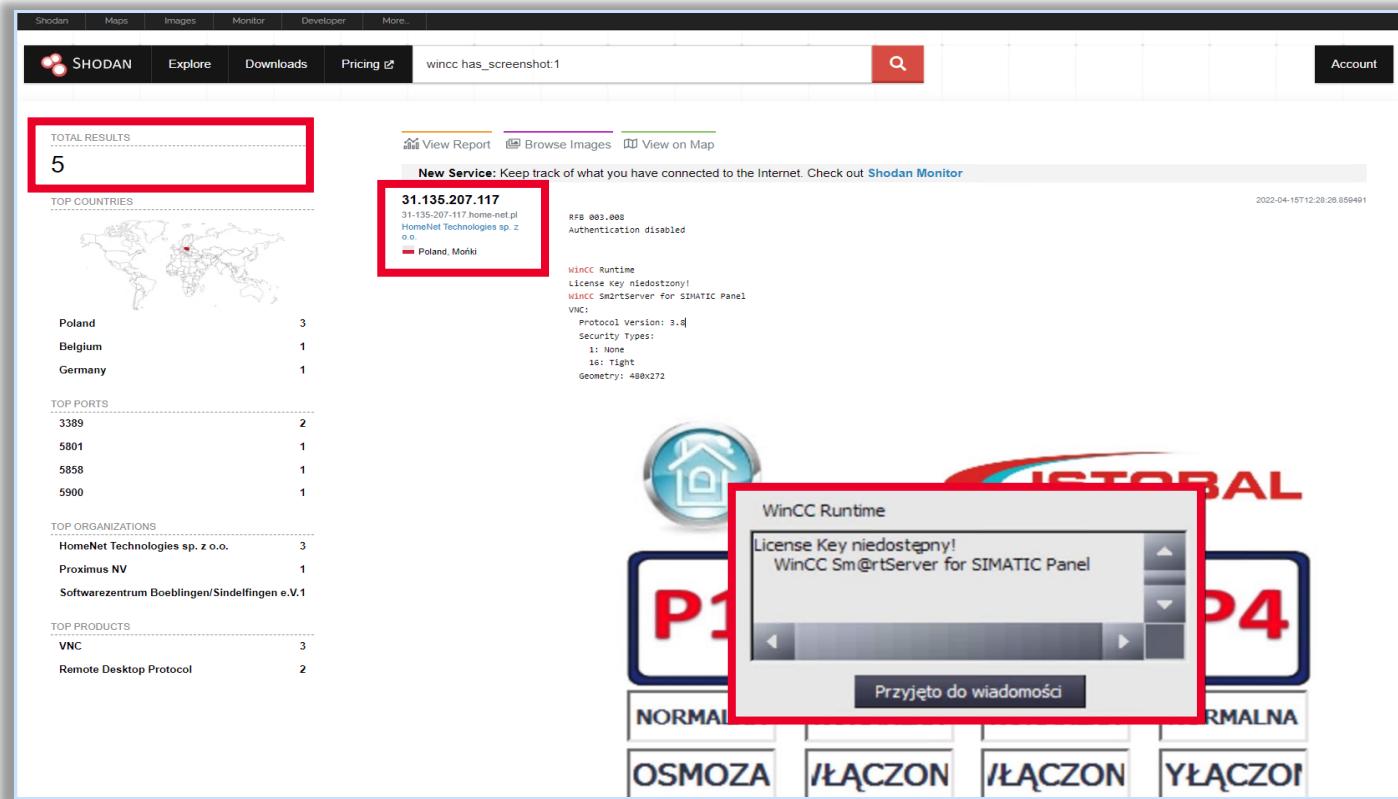


Ilustración 23: Nueva búsqueda. En este caso para localizar dispositivos que hayan permitido realizar algún tipo de captura de pantalla por parte de Shodan, y que contengan la palabra «wincc». Se accede al primer dispositivo del listado.

5 BÚSQUEDAS DESDE LA INTERFAZ WEB: SCREENSHOTS

- Como puedes observar en las siguientes imágenes, este dispositivo tiene una serie de puertos abiertos asociados al protocolo VNC que permitiría conectar a este sistema (si no hay ningún tipo de seguridad habilitada) y operar sobre él a través del entorno gráfico que se muestra.

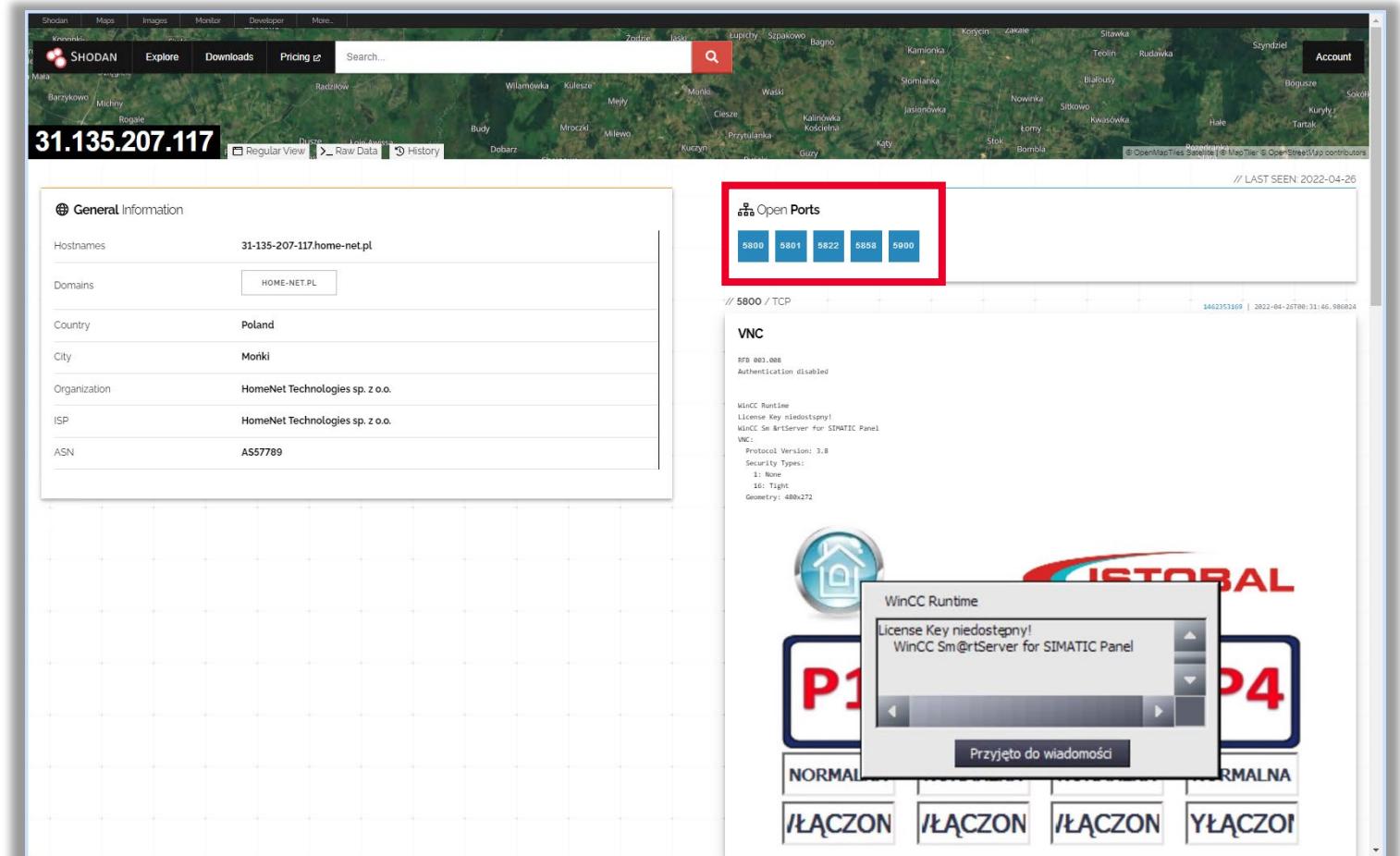


Ilustración 24: Puertos abiertos del dispositivo asociados al protocolo VNC.

5 BÚSQUEDAS DESDE LA INTERFAZ WEB: SCREENSHOTS

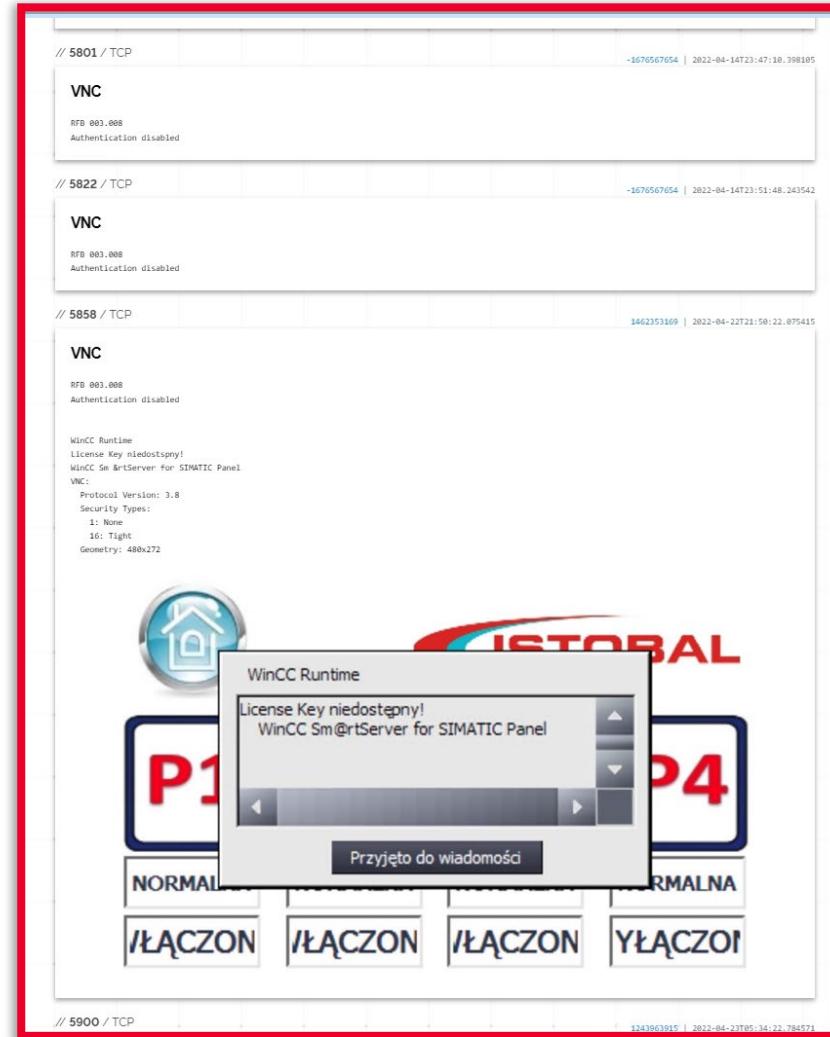


Ilustración 25: Puertos abiertos del dispositivo asociados al protocolo VNC.

5 BÚSQUEDAS DESDE LA INTERFAZ WEB: SCREENSHOTS

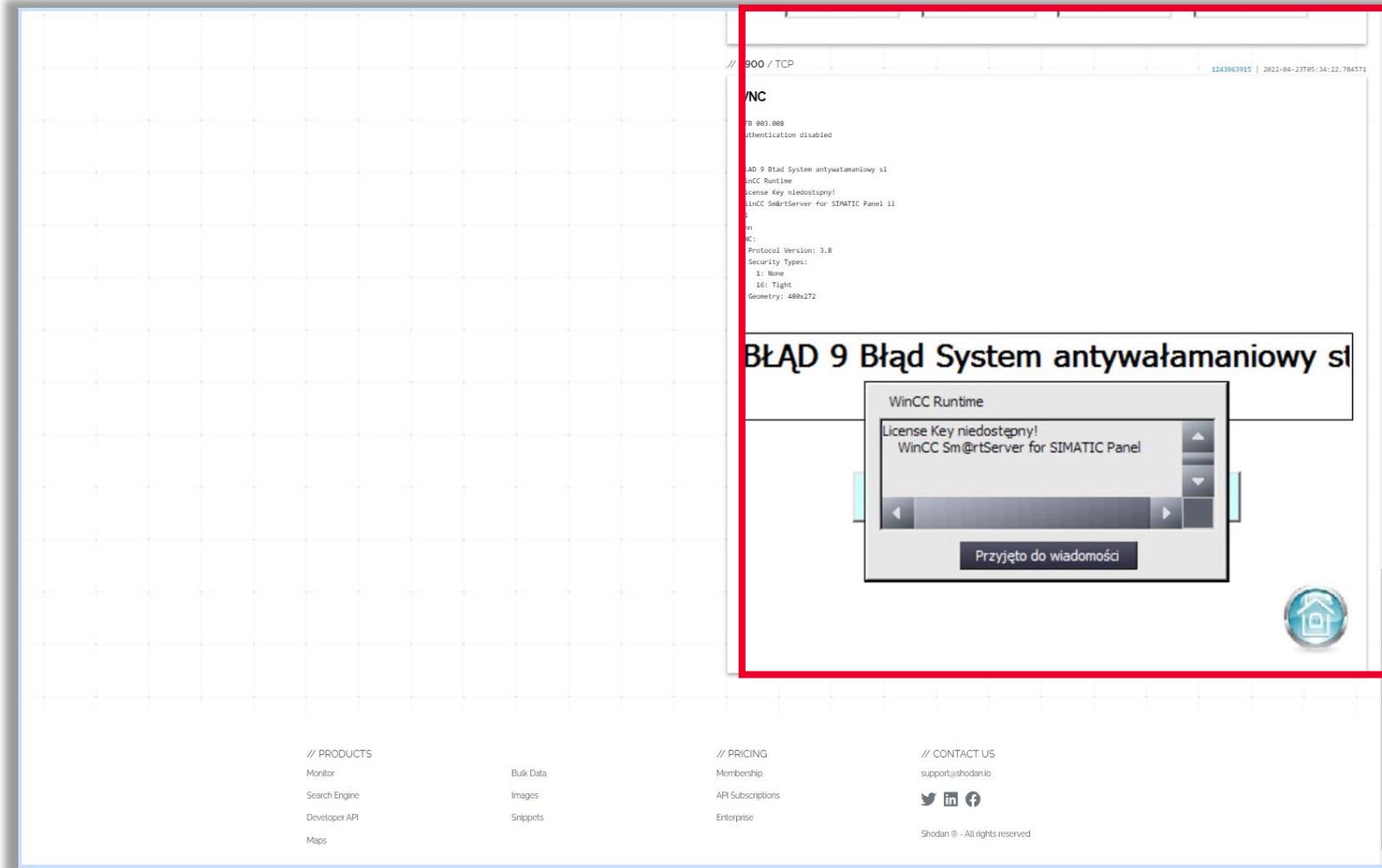


Ilustración 26: Puertos abiertos del dispositivo asociados al protocolo VNC.



BÚSQUEDAS DESDE LA INTERFAZ WEB: SCREENSHOTS

Modifica tu anterior búsqueda y ahora busca por el término «rdp», para tratar de localizar dispositivos que tengan habilitado la conexión por escritorio remoto a través del puerto RDP. Los términos de búsqueda son los siguientes:

- **rdp has_screenshot:1**
- La búsqueda devuelve un resultado de 461 dispositivos. En el primer resultado aparece una captura de pantalla donde se muestra la interfaz gráfica de un sistema Windows Server 2012 R2 que permitiría introducir las credenciales para conectar por escritorio remoto.

5 BÚSQUEDAS DESDE LA INTERFAZ WEB: SCREENSHOTS

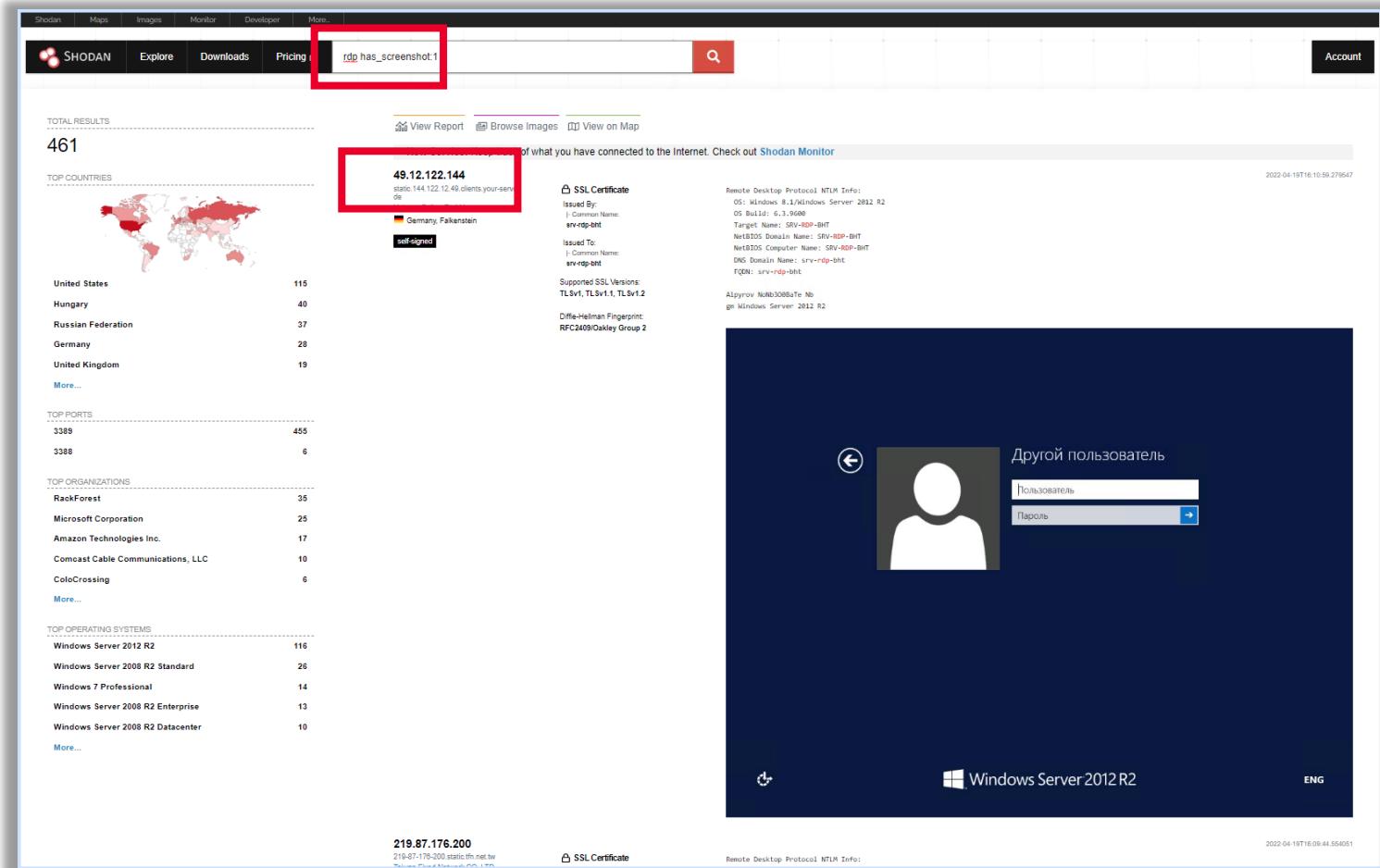


Ilustración 27: Modificación de la búsqueda anterior utilizando el término «rdp», para localizar dispositivos con la conexión por escritorio remoto a través del puerto RDP habilitada.

5 BÚSQUEDAS DESDE LA INTERFAZ WEB: SCREENSHOTS

- Haz clic en su IP y se abre una página con toda la información de este *host*. Como puedes observar, en el apartado «*Open Ports*» aparece el puerto 3389, que es el puerto que se suele utilizar en las conexiones por escritorio remoto en los sistemas Windows.

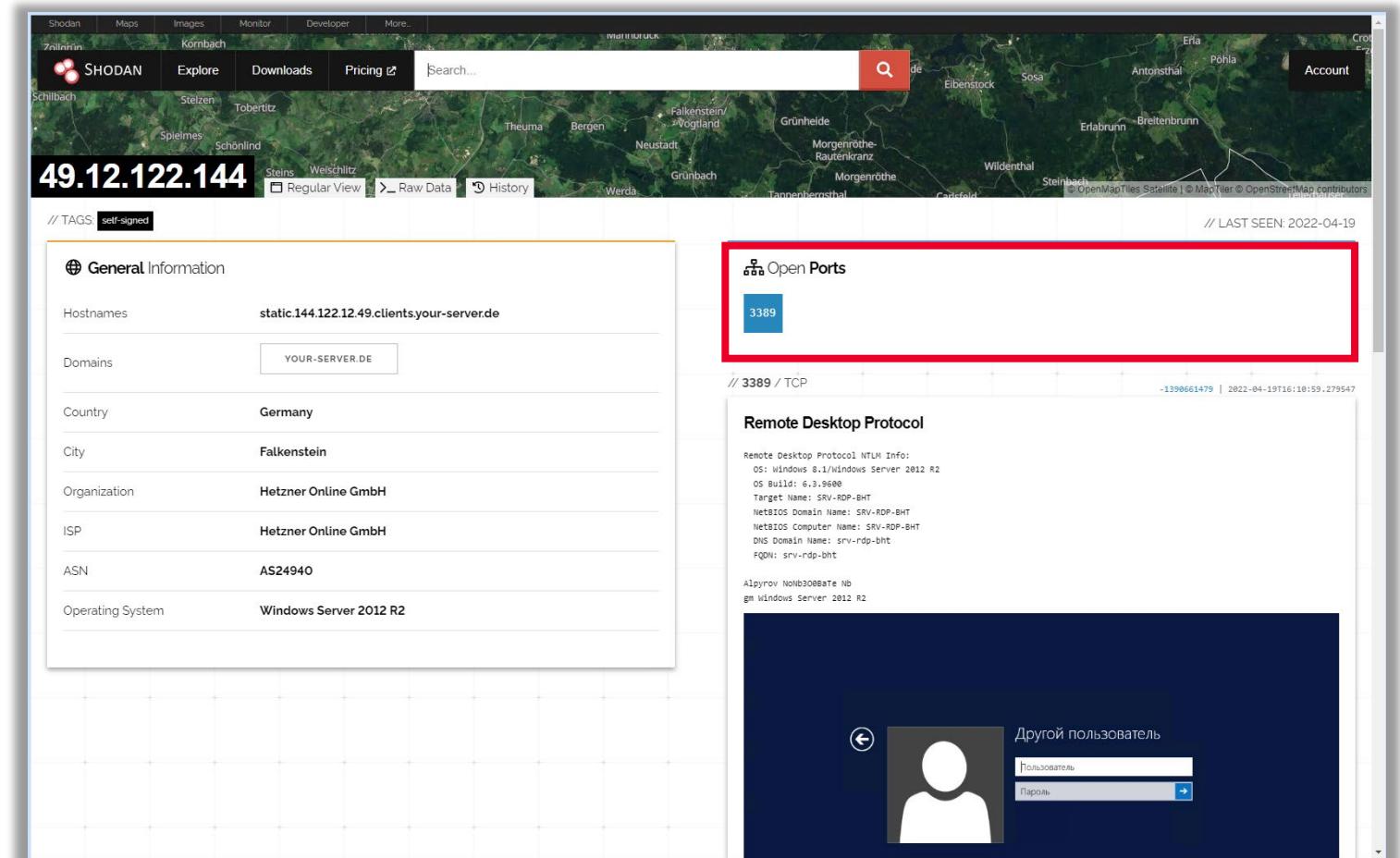


Ilustración 28: Dato que aparece en el apartado «*Open Ports*», puerto 3389.

5 BÚSQUEDAS DESDE LA INTERFAZ WEB: SCREENSHOTS

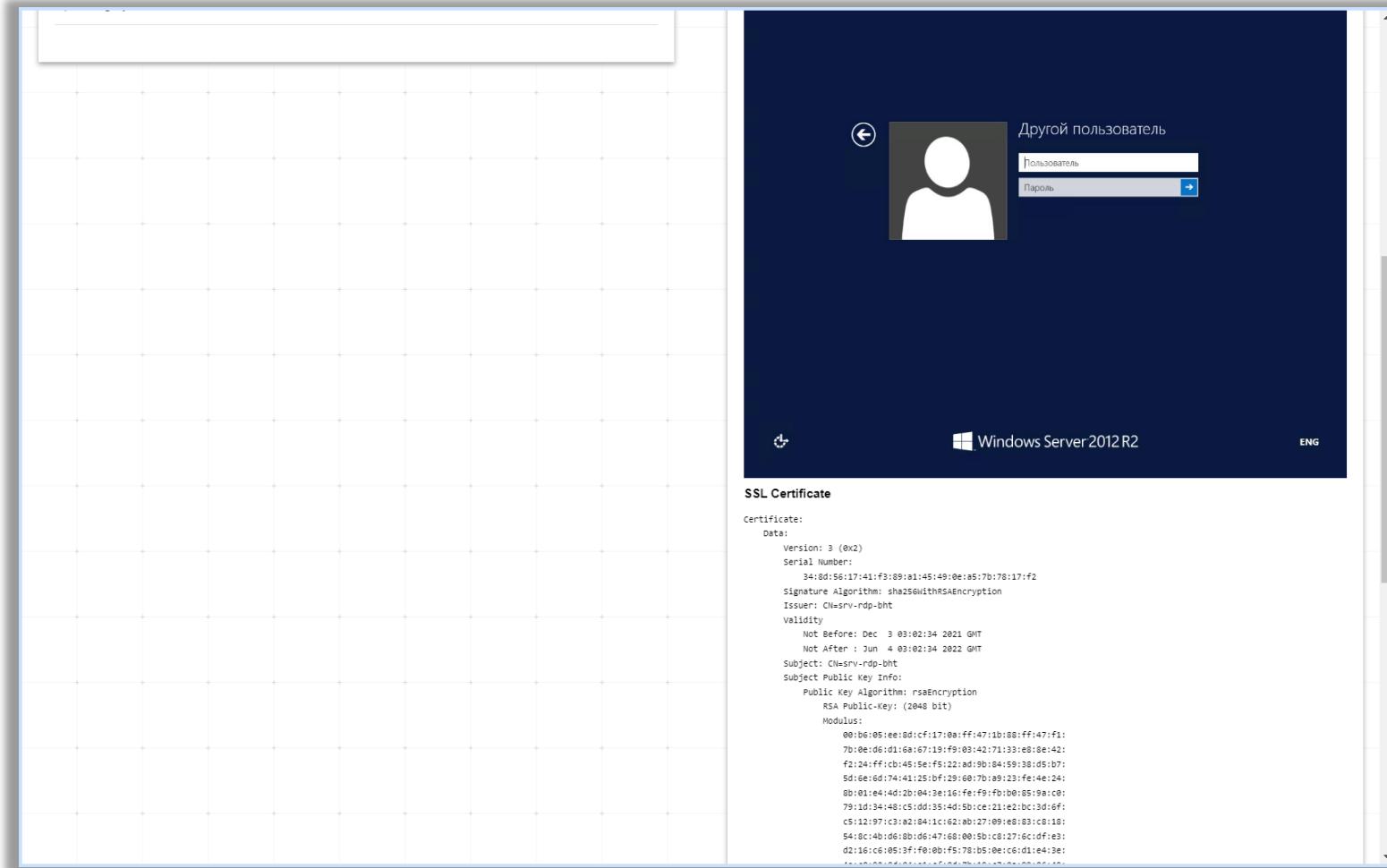


Ilustración 29: Puerto que se suele utilizar en las conexiones por escritorio remoto en los sistemas Windows.

5 BÚSQUEDAS DESDE LA INTERFAZ WEB: SCREENSHOTS

- Por último, realiza una búsqueda por el término «vnc» para localizar dispositivos que permitan la conexión a un escritorio remoto a través del protocolo VNC. Los términos de búsqueda son los siguientes:
 - **vnc has_screenshot:1**
- La búsqueda devuelve un resultado muy elevado de dispositivos (4944).

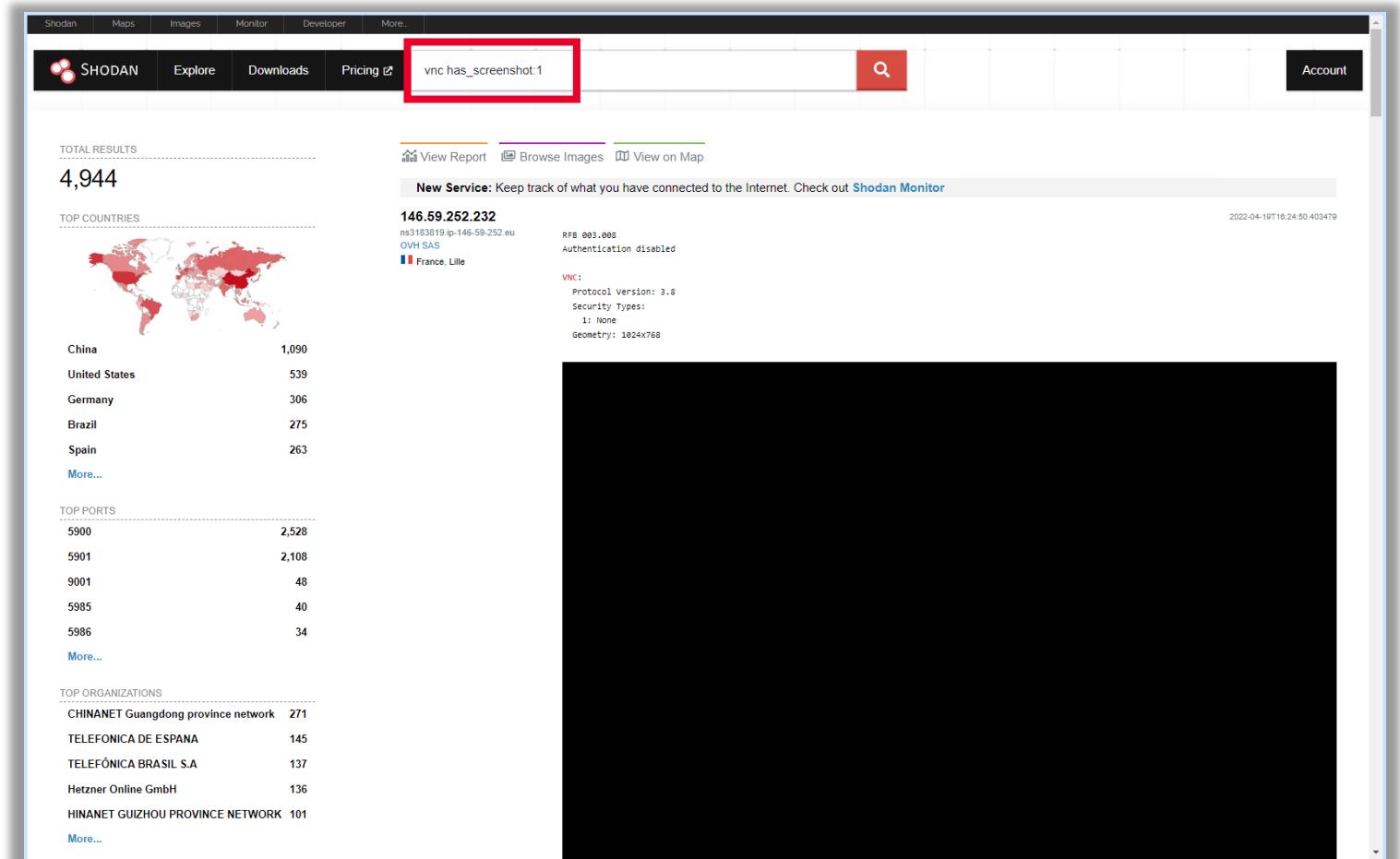


Ilustración 30: Nueva búsqueda por el término «vnc» para localizar dispositivos que permitan la conexión a un escritorio remoto a través del protocolo VNC.

5 BÚSQUEDAS DESDE LA INTERFAZ WEB: SCREENSHOTS

- Si haces scroll hacia abajo, podremos ver lo que parece un dispositivo SCADA, donde se está representando un proceso industrial.

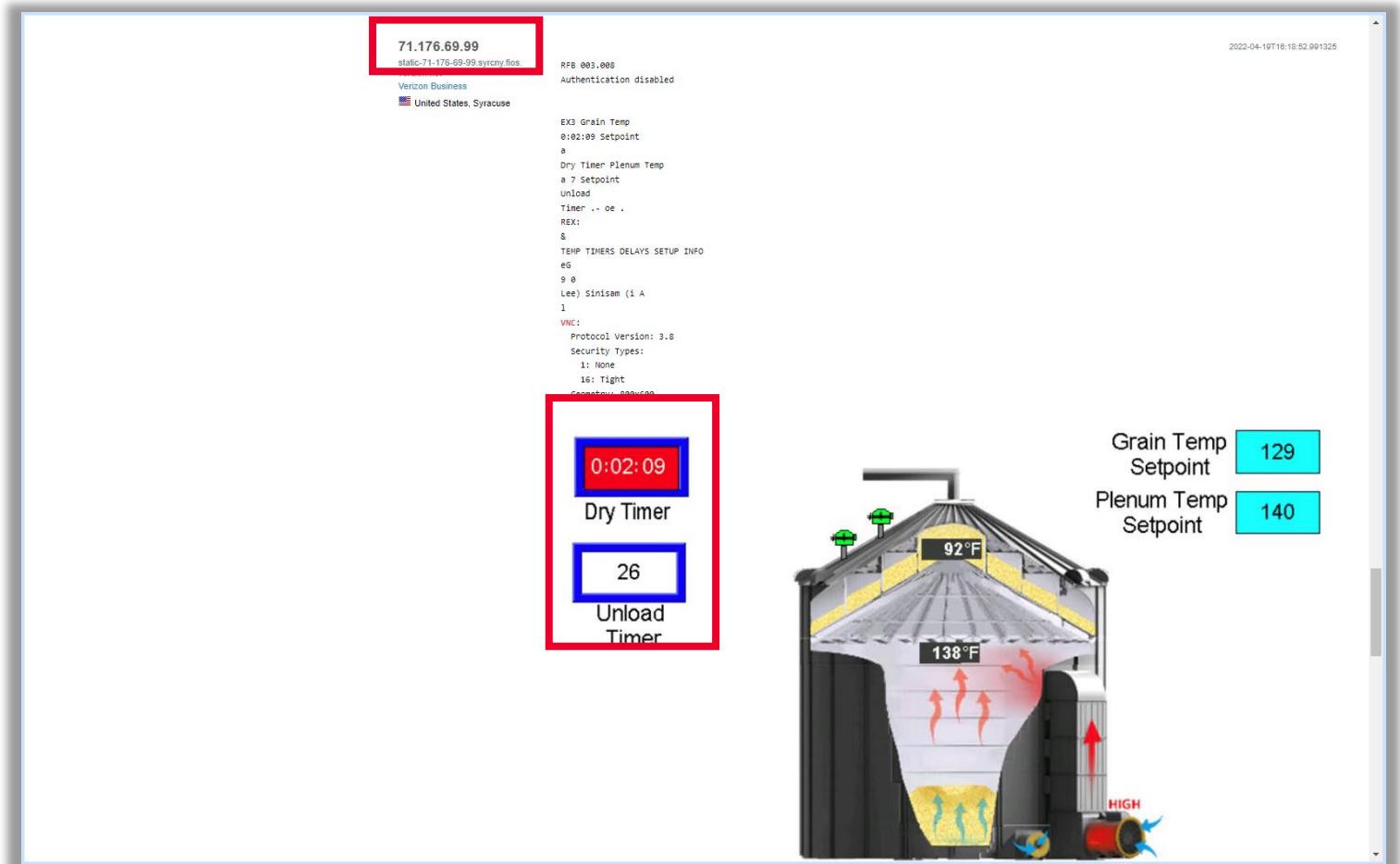


Ilustración 31: Dispositivo SCADA mostrando un proceso industrial.

5 BÚSQUEDAS DESDE LA INTERFAZ WEB: SCREENSHOTS

- Haz clic en su IP y se abre, como en anteriores ocasiones, una página con toda la información de este *host*. Como puedes observar en la imagen que se muestra, parece la interfaz gráfica de un sistema industrial, como podría ser un SCADA. En la imagen aparecen una serie de botones de control que permitirían a un posible atacante interactuar con el sistema industrial y provocar un incidente.

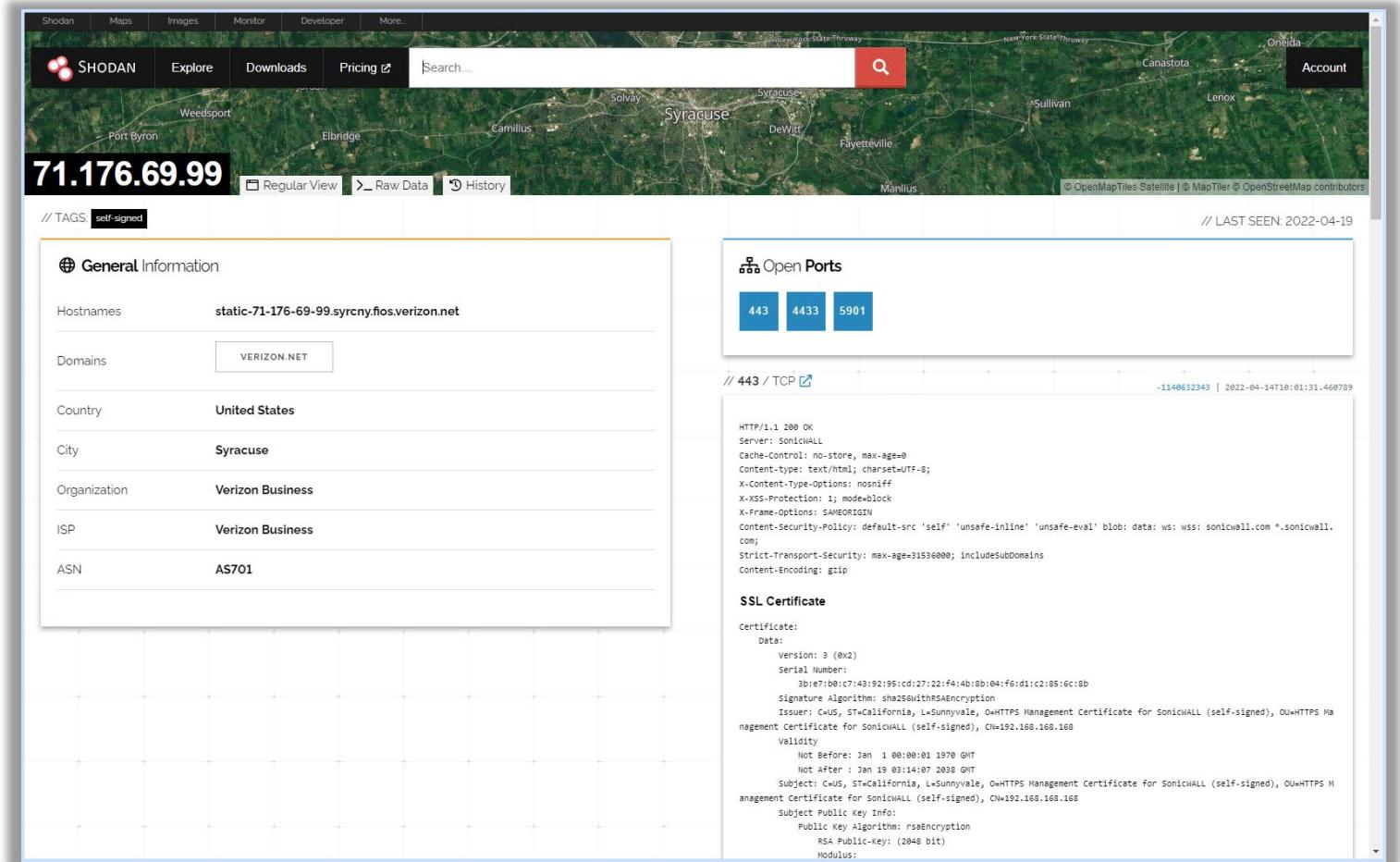
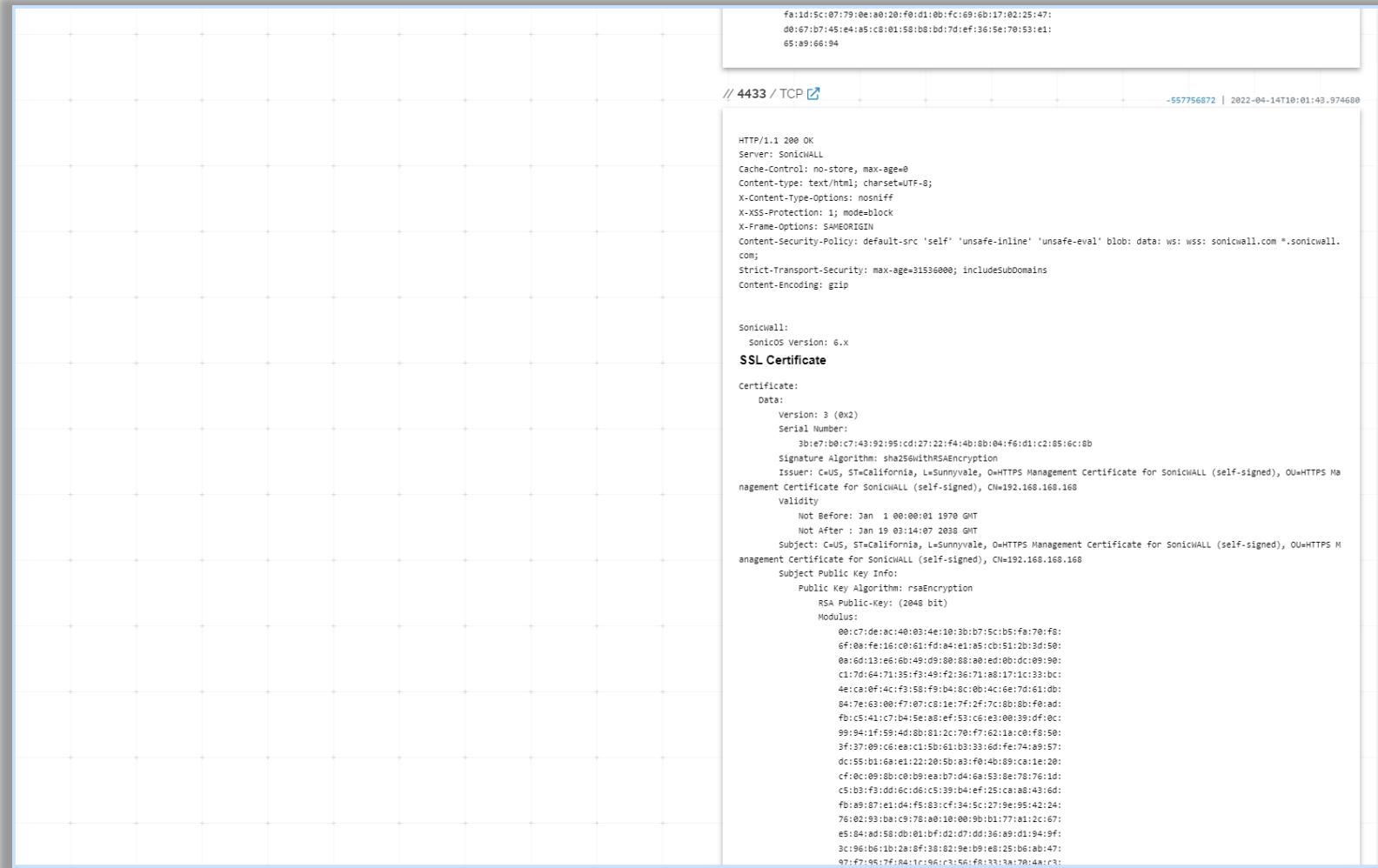


Ilustración 32: Datos del dispositivo.

5 BÚSQUEDAS DESDE LA INTERFAZ WEB: SCREENSHOTS



The screenshot shows a browser window with the URL `// 4433 / TCP`. The page content is a detailed SSL certificate for a SonicWALL device. The certificate includes the following details:

- HTTP/1.1 200 OK**
- Server:** SonicWALL
- Cache-Control:** no-store, max-age=0
- Content-type:** text/html; charset=UTF-8;
- X-Content-Type-Options:** nosniff
- X-XSS-Protection:** 1; mode=block
- X-Frame-Options:** SAMEORIGIN
- Content-Security-Policy:** default-src 'self' 'unsafe-inline' 'unsafe-eval' blob: data: ws: wss: sonicwall.com *.sonicwall.com;
- Strict-Transport-Security:** max-age=31536000; includeSubDomains
- Content-Encoding:** gzip

SonicWall:
sonicOS Version: 6.x
SSL Certificate

Certificate:

Data:

Version: 3 (0x2)
Serial Number:
3b:e7:b0:c7:43:92:95:cd:27:22:f4:4b:8b:04:f6:d1:c2:85:6c:8d
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, ST=California, L=Sunnyvale, O=HTTPS Management Certificate for SonicWALL (self-signed), OU=HTTPS Management Certificate for SonicWALL (self-signed), CN=192.168.168.168
Validity
Not Before: Jan 1 00:00:01 1970 GMT
Not After : Jan 19 03:14:07 2030 GMT
Subject: C=US, ST=California, L=Sunnyvale, O=HTTPS Management Certificate for SonicWALL (self-signed), OU=HTTPS Management Certificate for SonicWALL (self-signed), CN=192.168.168.168
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
00:c7:de:ac:40:03:4e:10:3b:b7:5c:b5:f0:70:f8:
6f:08:fe:16:c0:61:fd:a4:e1:a5:cb:51:2b:3d:50:
0a:6d:13:e6:6b:49:d9:90:88:a0:ed:00:dc:09:90:
c1:7d:64:71:35:f3:49:f2:36:71:a8:17:1c:33:bc:
4e:ca:0f:4c:f3:58:f9:b4:8c:0b:4c:6e:7d:61:db:
84:7e:83:00:f7:07:c8:1e:7f:2f:7c:80:80:f0:ad:
fb:c5:41:c7:04:5e:a8:ef:53:c6:e3:00:39:df:0c:
99:94:1f:59:4d:8b:81:2c:70:f7:62:1a:c0:f8:5e:
3f:37:09:c6:ea:c1:5b:61:b3:33:60:fe:74:a9:57:
dc:55:b1:68:e1:22:29:b9:a3:f0:4b:89:ca:1e:20:
cf:0c:09:80:c0:b9:ea:07:d4:68:53:8e:78:76:10:
c5:b3:f3:dd:6c:d6:c5:39:b4:ef:25:c8:a8:43:6d:
fb:a9:87:ea:04:f5:83:c7:34:5c:27:9e:95:42:24:
76:02:93:ba:c9:78:a0:01:00:9b:b1:77:a1:2c:67:
e5:84:ad:58:db:01:bf:02:d7:dd:36:a9:d1:94:9f:
3c:96:be:1b:2a:6f:38:62:9e:b9:e8:25:b6:ab:47:
97:f7:95:7f:84:1c:96:c3:56:f8:33:a7:70:4a:c9:

Ilustración 33: Más información del dispositivo.

5 BÚSQUEDAS DESDE LA INTERFAZ WEB: SCREENSHOTS

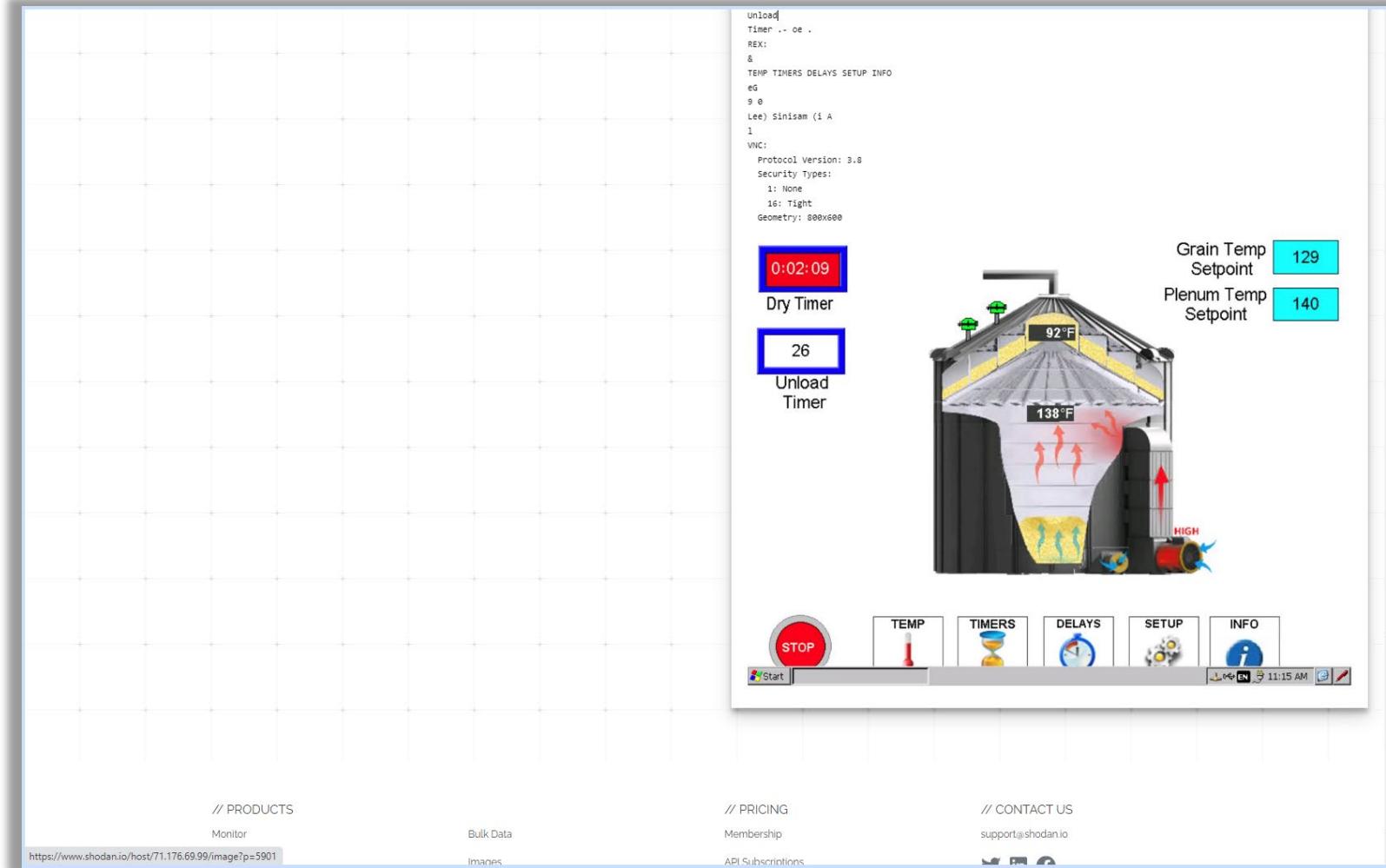


Ilustración 34: Botones de control que permitirían a un posible atacante interactuar con el sistema industrial y provocar un incidente.

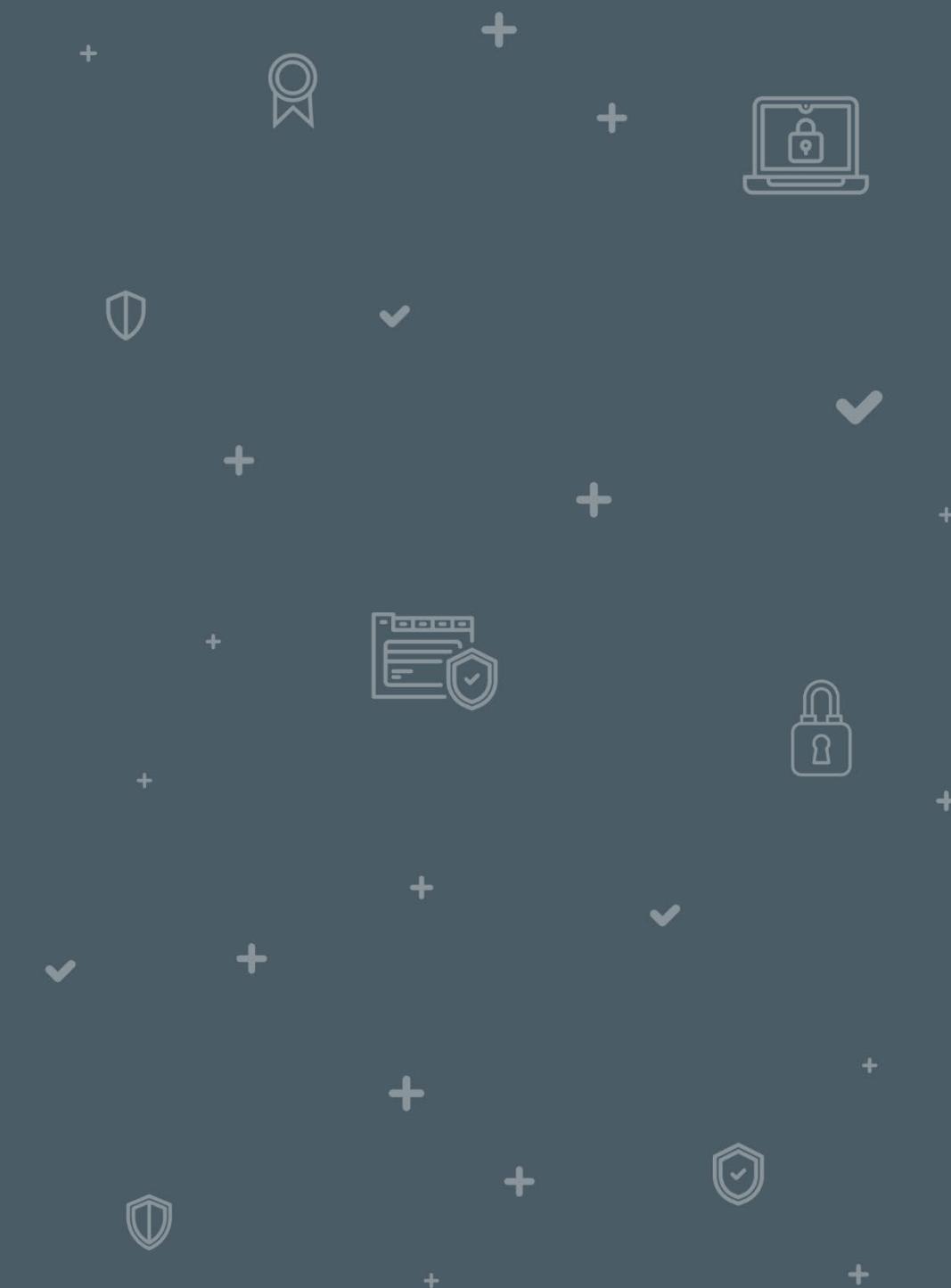
5 BÚSQUEDAS DESDE LA INTERFAZ WEB: SCREENSHOTS

Por lo que has comprobado, con el motor de búsqueda Shodan, es posible localizar dispositivos industriales. Sin embargo, no es que aparezcan todos los dispositivos, si no únicamente aquellos que se encuentran compartidos de forma pública en Internet. Suele tratarse de dispositivos que no cuentan con una adecuada protección, por lo que se recomienda siempre tomar medidas tales como cambiar los nombres de usuario y contraseñas por defecto, modificar las configuraciones por defecto o mantener actualizado el *firewall*, entre otras.



BÚSQUEDAS DESDE LA CLI: COMANDO *INIT*

6





BÚSQUEDAS DESDE LA CLI: COMANDO INIT

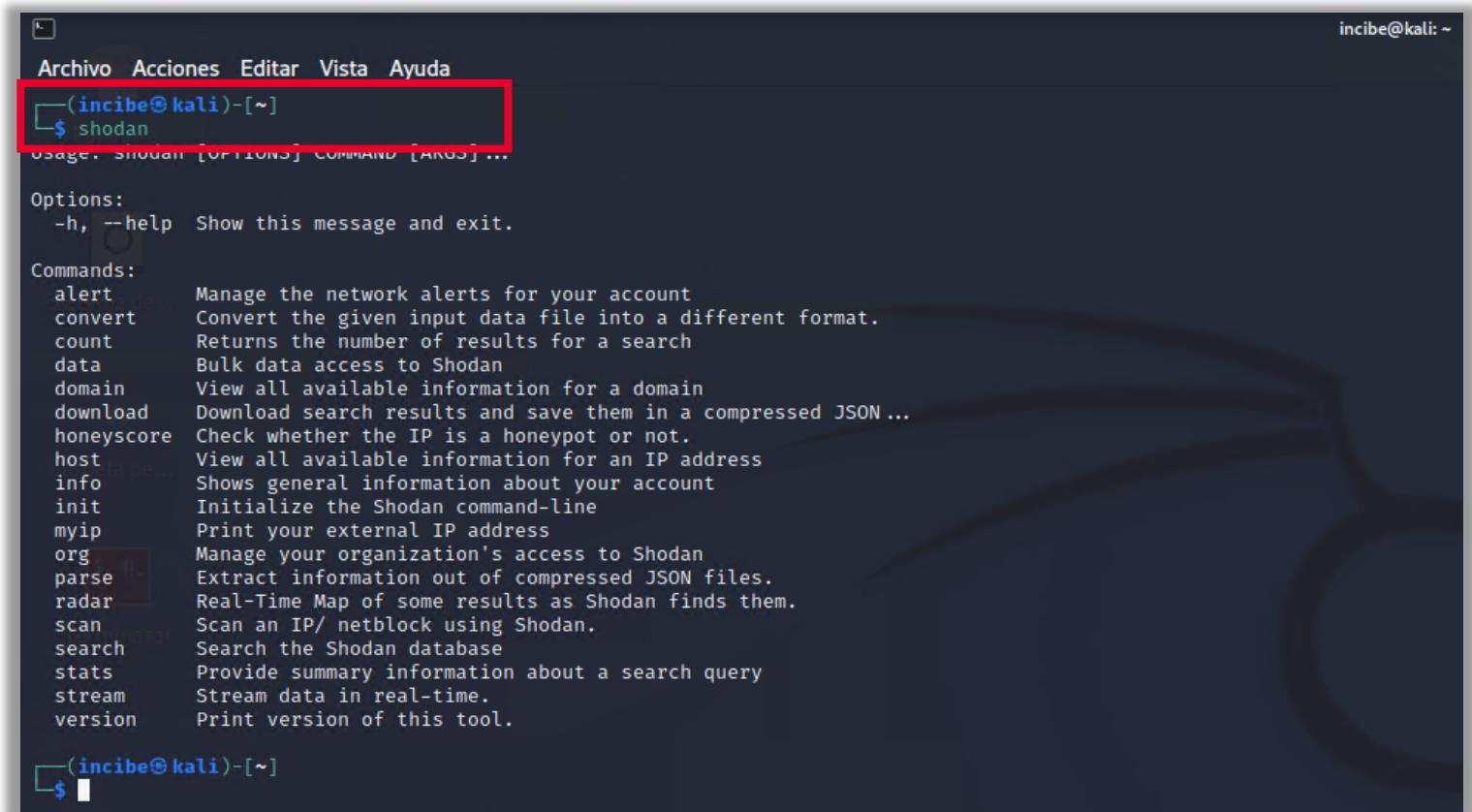
Ahora, vamos a utilizar la herramienta CLI (*Command Line Interface*) que proporciona Shodan para realizar las búsquedas directamente desde la terminal sin utilizar la interfaz web, con lo que conseguiremos acceder a una mayor cantidad de resultados y evitaremos algunas limitaciones que impone realizar búsquedas desde la interfaz web de Shodan.

Esta herramienta CLI ya viene instalada en la distribución Kali Linux de tu MV. Cuando ejecutes la herramienta por primera vez con el comando shodan, esta tardará un tiempo en responder y mostrar al final la información de la ayuda de los diferentes comandos que incorpora Shodan.

6

BÚSQUEDAS DESDE LA CLI: COMANDO INIT

- Desde tu MV Kali Linux abre una terminal y ejecuta el comando que invoca a la CLI de Shodan y muestra la ayuda de este comando: **shodan**



```
incibe@kali: ~
Archivo Acciones Editar Vista Ayuda
(incibe@kali)-[~]
$ shodan
Usage: shodan [OPTIONS] COMMAND [ARGS] ...
Options:
-h, --help Show this message and exit.
Commands:
alert Manage the network alerts for your account
convert Convert the given input data file into a different format.
count Returns the number of results for a search
data Bulk data access to Shodan
domain View all available information for a domain
download Download search results and save them in a compressed JSON ...
honeyscore Check whether the IP is a honeypot or not.
host View all available information for an IP address
info Shows general information about your account
init Initialize the Shodan command-line
myip Print your external IP address
org Manage your organization's access to Shodan
parse Extract information out of compressed JSON files.
radar Real-Time Map of some results as Shodan finds them.
scan Scan an IP/ netblock using Shodan.
search Search the Shodan database
stats Provide summary information about a search query
stream Stream data in real-time.
version Print version of this tool.

(incibe@kali)-[~]
$
```

Ilustración 35: Ejecuta el comando «shodan» desde tu MV Kali Linux para invocar a la CLI de Shodan.

6

BÚSQUEDAS DESDE LA CLI: COMANDO *INIT*

- Ejecuta el comando **shodan info** para verificar si la API Key está registrada. Como vemos, devuelve un error.

```
VERSION      PRINT VERSION OF THIS TOOL.  
[kali㉿kali)-[~]  
└─$ shodan info  
Error: Please run "shodan init <api key>" before using this command
```

Ilustración 36: Ejecuta el comando «shodan info» para verificar si la API Key está registrada.

- Esto es normal debido a que para utilizar la CLI de Shodan, primero debes registrar la API Key que se crea en la plataforma web cuando nos registramos como usuarios.

6

BÚSQUEDAS DESDE LA CLI: COMANDO INIT

- Tu API Key la puedes localizar en la web de Shodan. Para ello, accede a su página y haz clic en el botón «Account» (si es necesario vuelve a iniciar sesión) y, en la página que aparece, copia el texto (código) que aparece identificado en la entrada API Key.

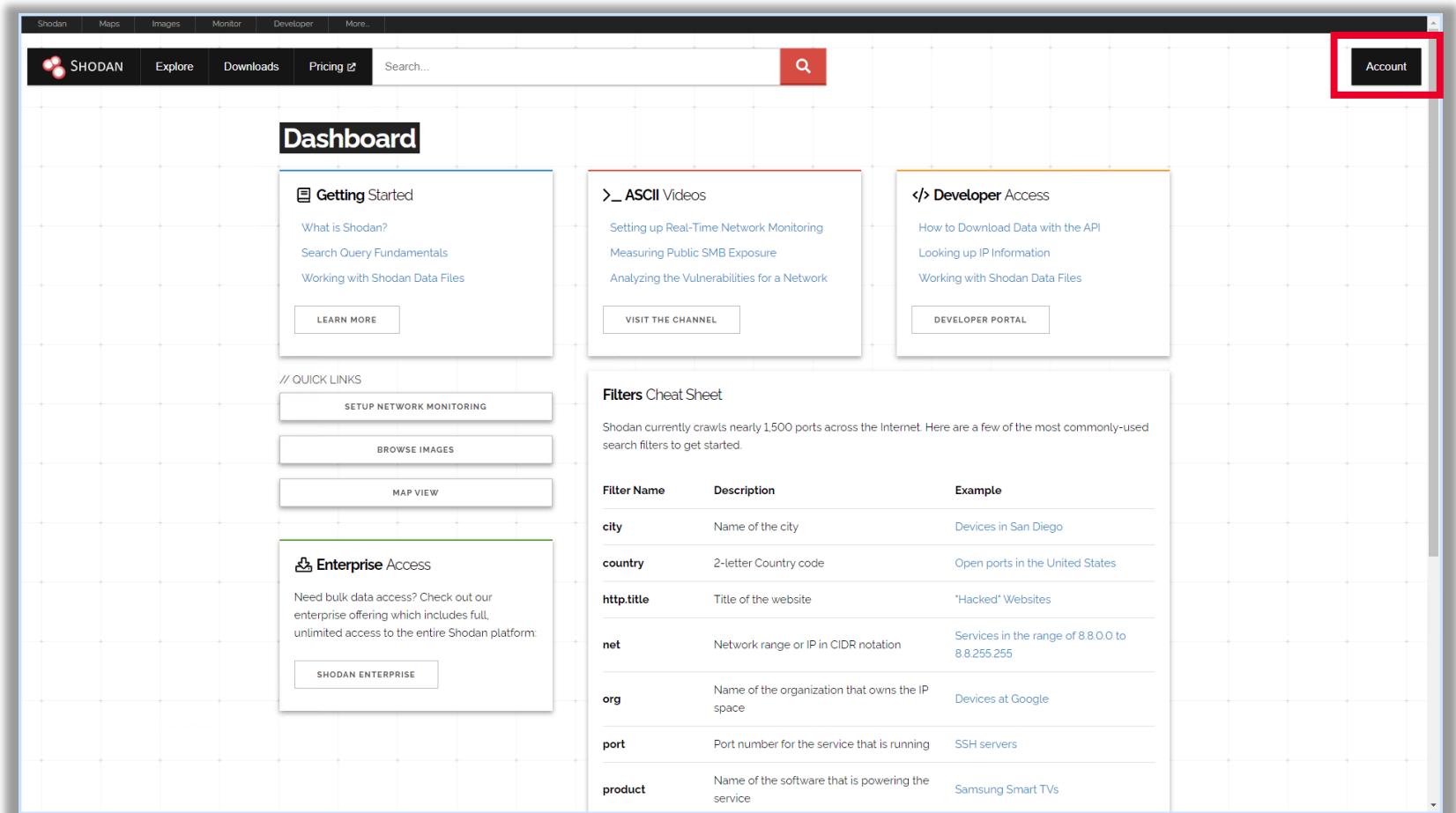


Ilustración 37: Acceso a la API Key a través del botón «Account» en la web de Shodan.

6

BÚSQUEDAS DESDE LA CLI: COMANDO INIT

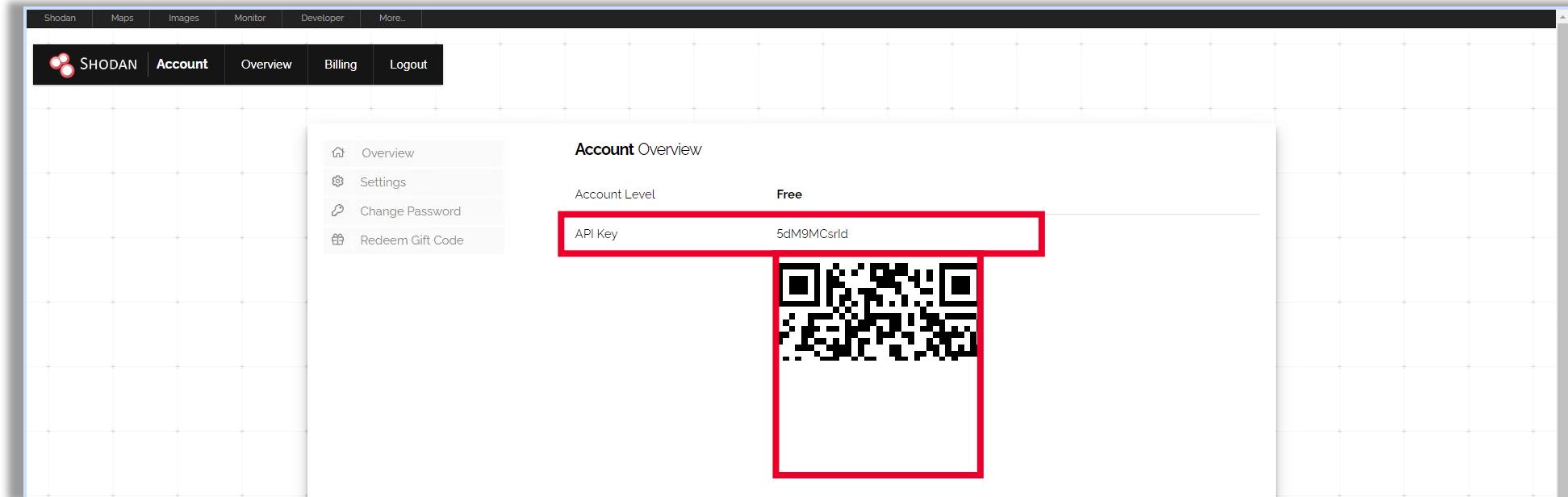
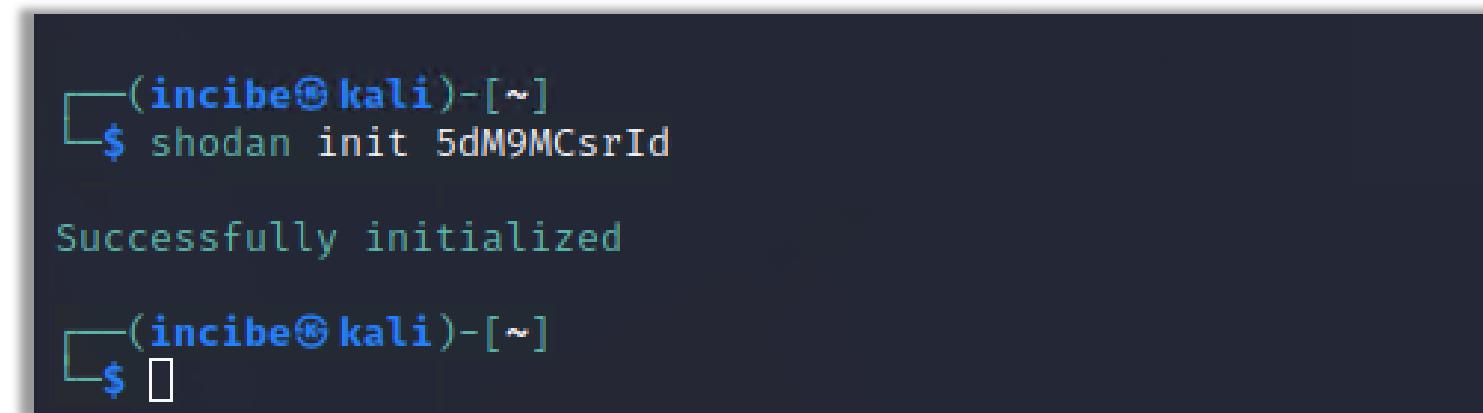


Ilustración 38: Página donde aparece el código que hay que copiar.

6

BÚSQUEDAS DESDE LA CLI: COMANDO *INIT*

- Regresa a la terminal de tu MV Kali Linux y ejecuta **shodan init** indicando tu API Key:



```
(incibe㉿kali)-[~]
$ shodan init 5dM9MCsrId

Successfully initialized

(incibe㉿kali)-[~]
$ 
```

A screenshot of a terminal window on a Kali Linux system. The user is at the prompt '(incibe㉿kali)-[~]'. They type 'shodan init 5dM9MCsrId' and press enter. The terminal then displays the message 'Successfully initialized' followed by another prompt '(incibe㉿kali)-[~]'.

Ilustración 39: MV Kali Linux donde ejecuta «shodan *init*» indicando el código copiado en el paso anterior.

BÚSQUEDAS DESDE LA CLI: COMANDO **STATS**

7





BÚSQUEDAS DESDE LA CLI: COMANDO STATS

Ahora, vamos a utilizar el comando **stats** para realizar tus primeras búsquedas en la terminal con la CLI de Shodan.

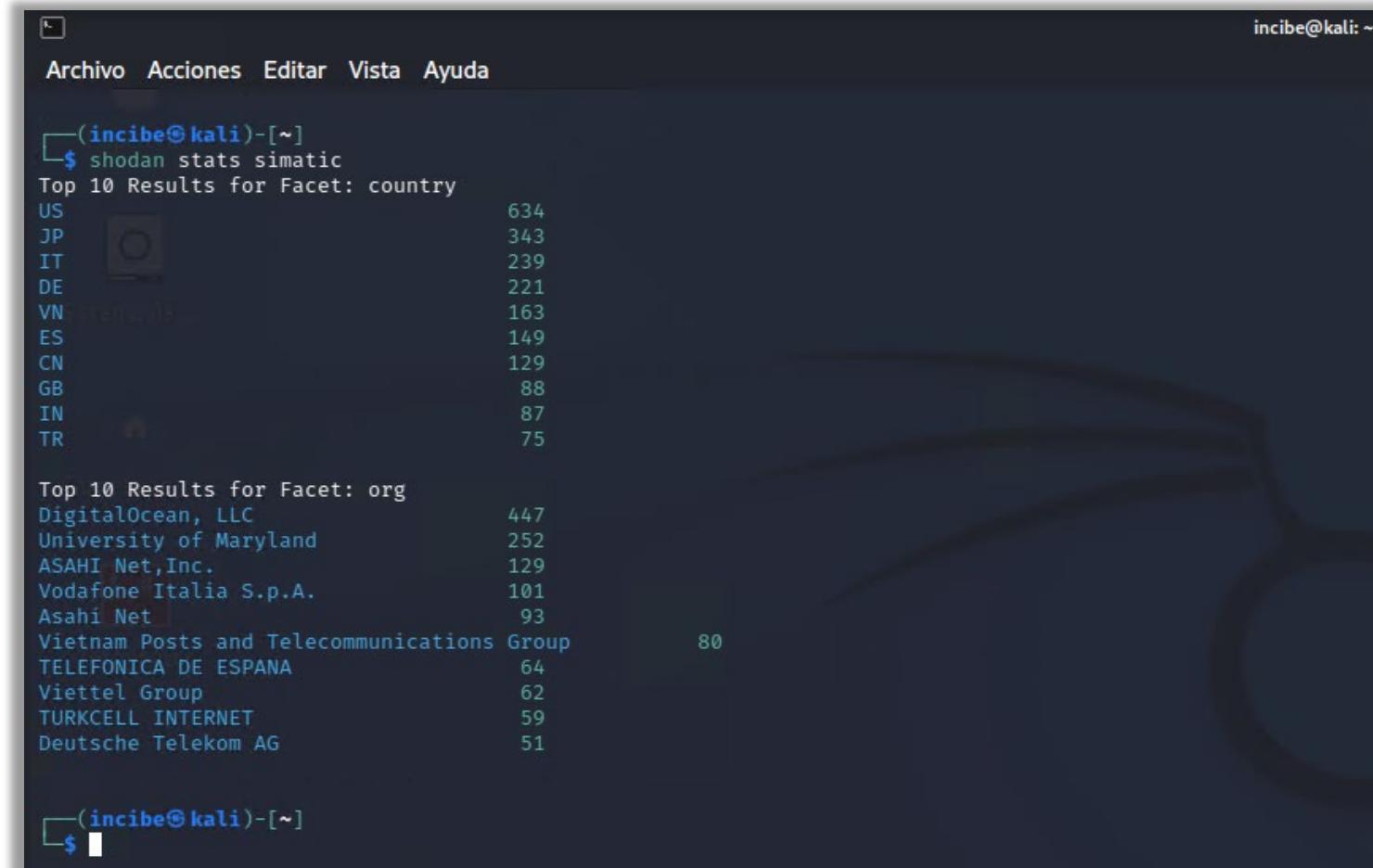
Este comando **stats** mostrará los principales resultados del término de búsqueda que introduzcas.

- Realiza la búsqueda del término «**simatic**». Verás que, por defecto, muestra el top 10 de resultados distribuidos por países y el top 10 de resultados distribuidos por organización. El comando utilizado es el siguiente:
 - **shodan stats simatic**

En general, en la segunda columna de resultados va a aparecer la cantidad de dispositivos identificados (en color verde claro).

7

BÚSQUEDAS DESDE LA CLI: COMANDO STATS



The screenshot shows a terminal window with the following content:

```
incibe@kali: ~
Archivo  Acciones  Editar  Vista  Ayuda
└──(incibe@kali)-[~]
$ shodan stats simatic
Top 10 Results for Facet: country
US          634
JP          343
IT          239
DE          221
VN          163
ES          149
CN          129
GB           88
IN           87
TR           75

Top 10 Results for Facet: org
DigitalOcean, LLC      447
University of Maryland  252
ASAHI Net, Inc.         129
Vodafone Italia S.p.A. 101
Asahi Net                93
Vietnam Posts and Telecommunications Group 80
TELEFONICA DE ESPANA    64
Viettel Group            62
TURKCELL INTERNET        59
Deutsche Telekom AG      51

└──(incibe@kali)-[~]
$
```

Ilustración 40: Búsqueda del término «simatic». Por defecto, muestra los resultados distribuidos por organización y por país. En la segunda columna aparecen el número de dispositivos.



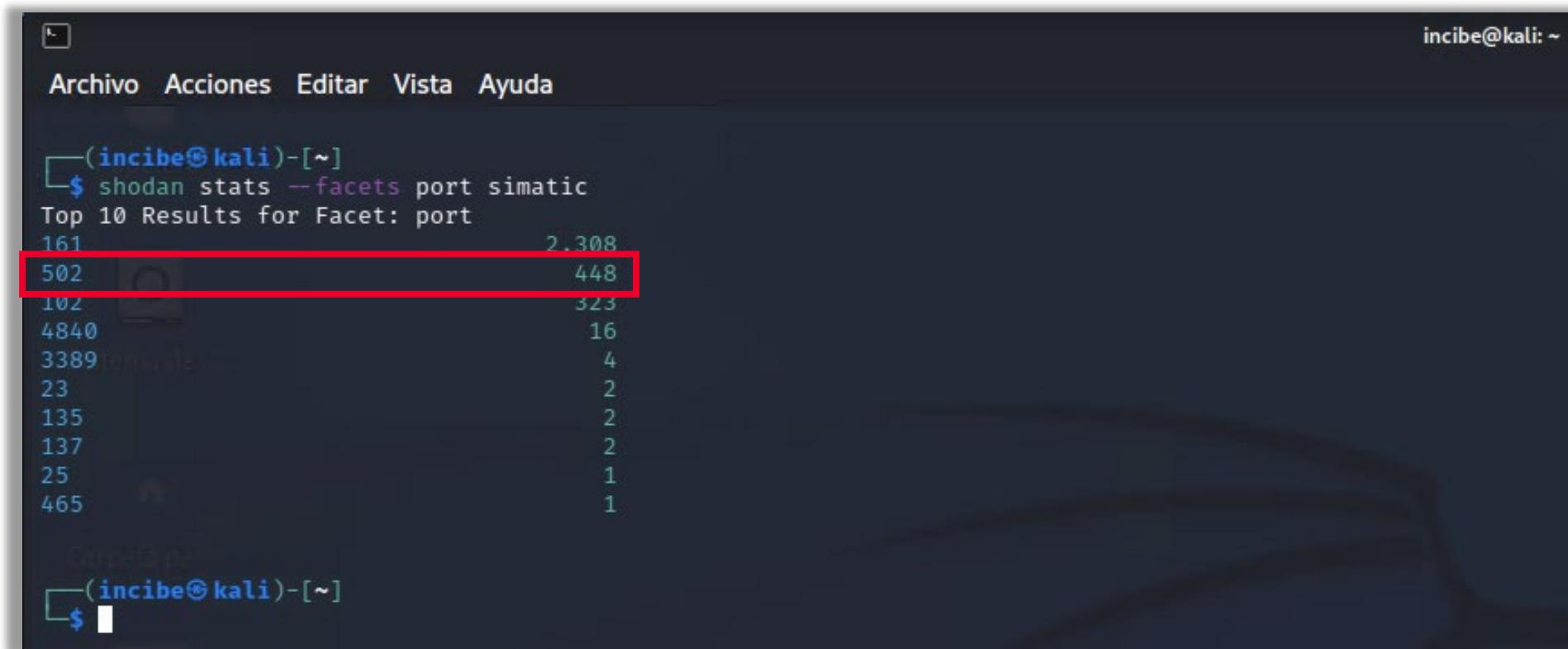
BÚSQUEDAS DESDE LA CLI: COMANDO STATS

- Para la siguiente búsqueda, utilizarás el parámetro *facets*, que es un concepto que muestra los primeros resultados sobre una propiedad (por ejemplo, el número de puerto de un dispositivo) para el término de búsqueda empleado.
 - El comando que utilizarás con el parámetro *facets port* (puerto) para el término de búsqueda «simatic» es el siguiente:
 - Shodan stats --facets port simatic**

7

BÚSQUEDAS DESDE LA CLI: COMANDO STATS

- Como puedes comprobar en la imagen, para el puerto 502 (que ya conoces de anteriores prácticas y que es utilizado por dispositivos industriales que utilizan el protocolo de comunicaciones Modbus TCP) aparecen 448 dispositivos.



The screenshot shows a terminal window with a dark background and light-colored text. At the top, it says "incibe@kali: ~". Below that is a menu bar with "Archivo", "Acciones", "Editar", "Vista", and "Ayuda". The main area of the terminal shows a command-line interface. The command entered is "\$ shodan stats --facets port simatic". The output is titled "Top 10 Results for Facet: port". The results are listed in a table format:

Port	Count
161	2.308
502	448
102	323
4840	16
3389	4
23	2
135	2
137	2
25	1
465	1

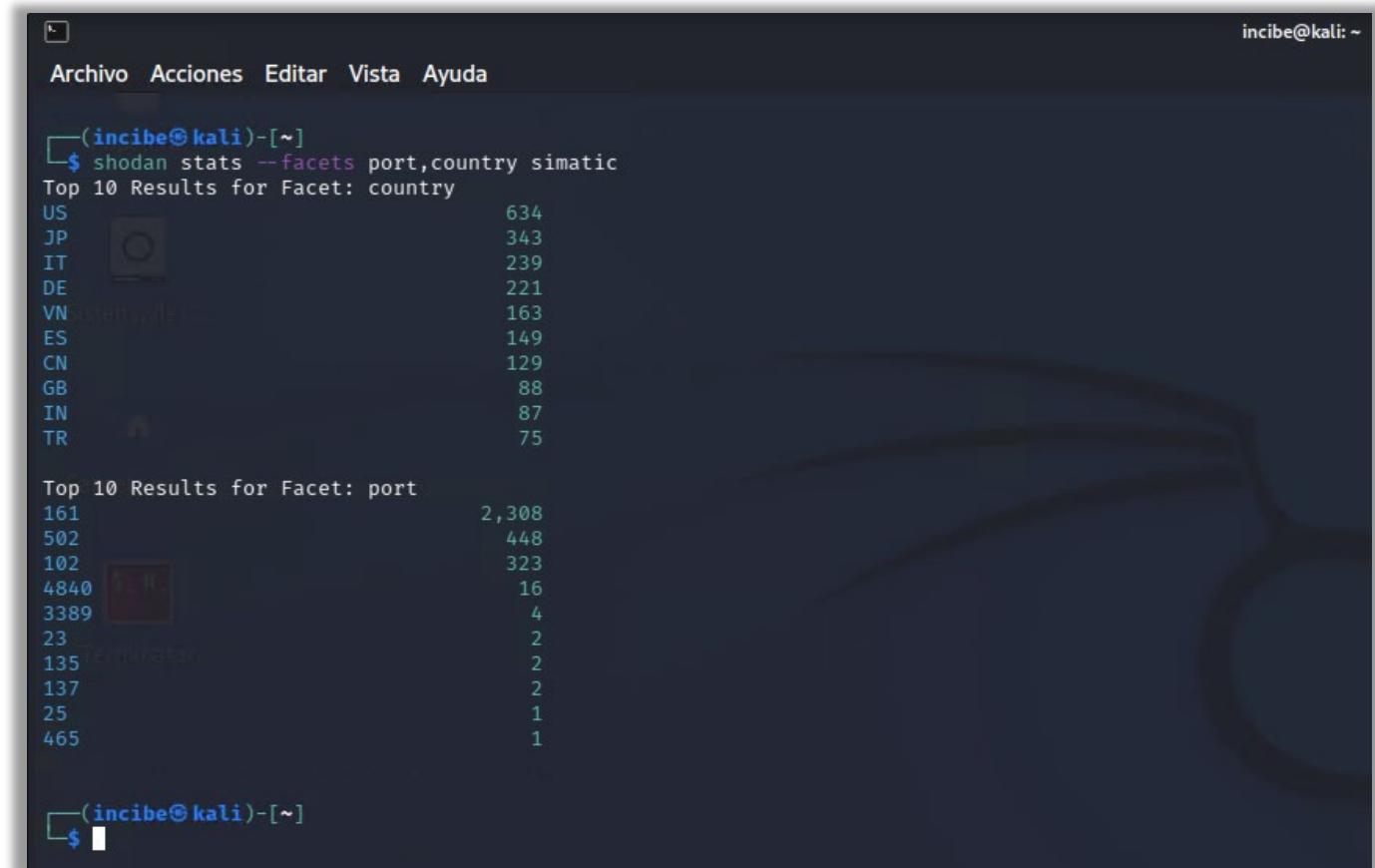
At the bottom of the terminal window, there is a prompt "(incibe@kali)-[~]" followed by a dollar sign (\$) and a blank line.

Ilustración 41: Resultados para el puerto 502.

7

BÚSQUEDAS DESDE LA CLI: COMANDO STATS

- Puedes utilizar más de un *facets* en tu búsqueda, en cuyo caso deberás separarlos por una coma. Por ejemplo, al comando anterior le puedes añadir el *facets country* para que muestre también los principales resultados distribuidos por países. El comando es el siguiente:
 - **shodan stats --facets port,country simatic**



A terminal window titled '(incibe㉿kali)-[~]' showing the output of the 'shodan stats' command. The command used was 'shodan stats --facets port,country simatic'. The output displays two sections of data: 'Top 10 Results for Facet: country' and 'Top 10 Results for Facet: port'. The 'country' facet shows results for US, JP, IT, DE, VN, ES, CN, GB, IN, and TR. The 'port' facet shows results for 161, 502, 102, 4840, 3389, 23, 135, 137, 25, and 465.

Facet	Result	Count
country	US	634
	JP	343
	IT	239
	DE	221
	VN	163
	ES	149
	CN	129
	GB	88
	IN	87
	TR	75
port	161	2,308
	502	448
	102	323
	4840	16
	3389	4
	23	2
	135	2
	137	2
	25	1
	465	1

Ilustración 42: Se puede añadir más de un *facets*. En este caso se añade uno para que muestre los resultados de la búsqueda anterior por países.

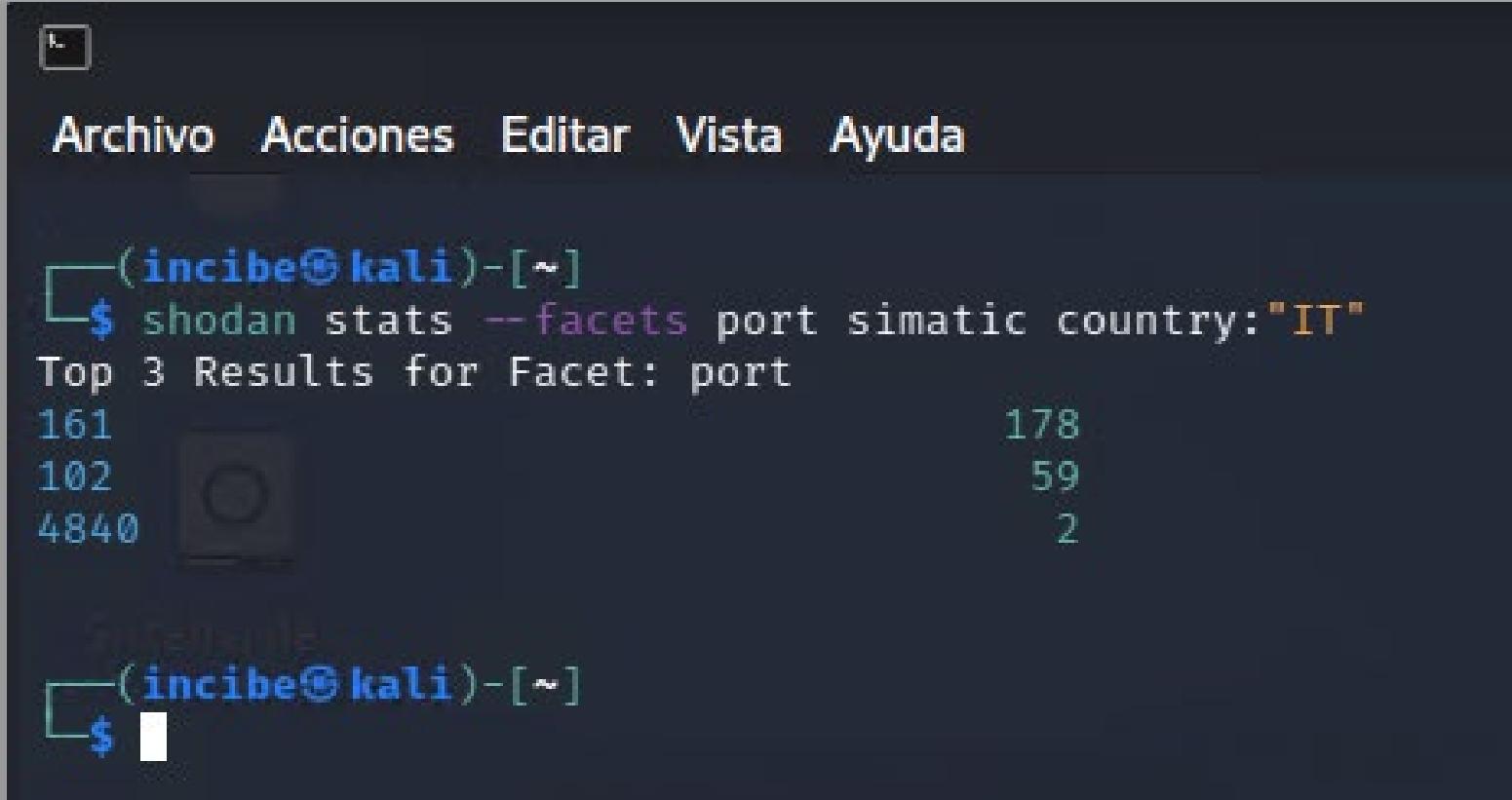


BÚSQUEDAS DESDE LA CLI: COMANDO STATS

- Puedes afinar la anterior búsqueda utilizando filtros, como ya hicimos desde la web de Shodan. En nuestro caso mantén el *facets port* y añade el filtro «country:"IT"», para que muestre el *top* de resultados de puertos abiertos, de dispositivos localizados en Italia. El comando utilizado es el siguiente:
 - **shodan stats --facets port,country simatic**
- Como puedes observar en Italia ha identificado para el término de búsqueda «simatic» tres entradas, que corresponden con los puertos 161 (utilizado por el protocolo SNMP), 102 (habitual de dispositivos de la familia Simatic, del fabricante Siemens) y el 4840 que se suele encontrar en sistemas OPC que usan la plataforma *software* de CodeSys. Asimismo, en la columna de la derecha puedes comprobar el número de dispositivos que tiene cada puerto.

7

BÚSQUEDAS DESDE LA CLI: COMANDO STATS



The screenshot shows a terminal window with a dark background and light-colored text. At the top, there's a menu bar with options: Archivo, Acciones, Editar, Vista, and Ayuda. Below the menu, the terminal prompt is shown as `(incibe㉿kali)-[~]`. The user then runs the command `$ shodan stats --facets port simatic country:"IT"`. The output displays the results for the 'port' facet, specifically for SIMATIC devices in Italy. It lists three entries with their respective counts:

Port	Count
161	178
102	59
4840	2

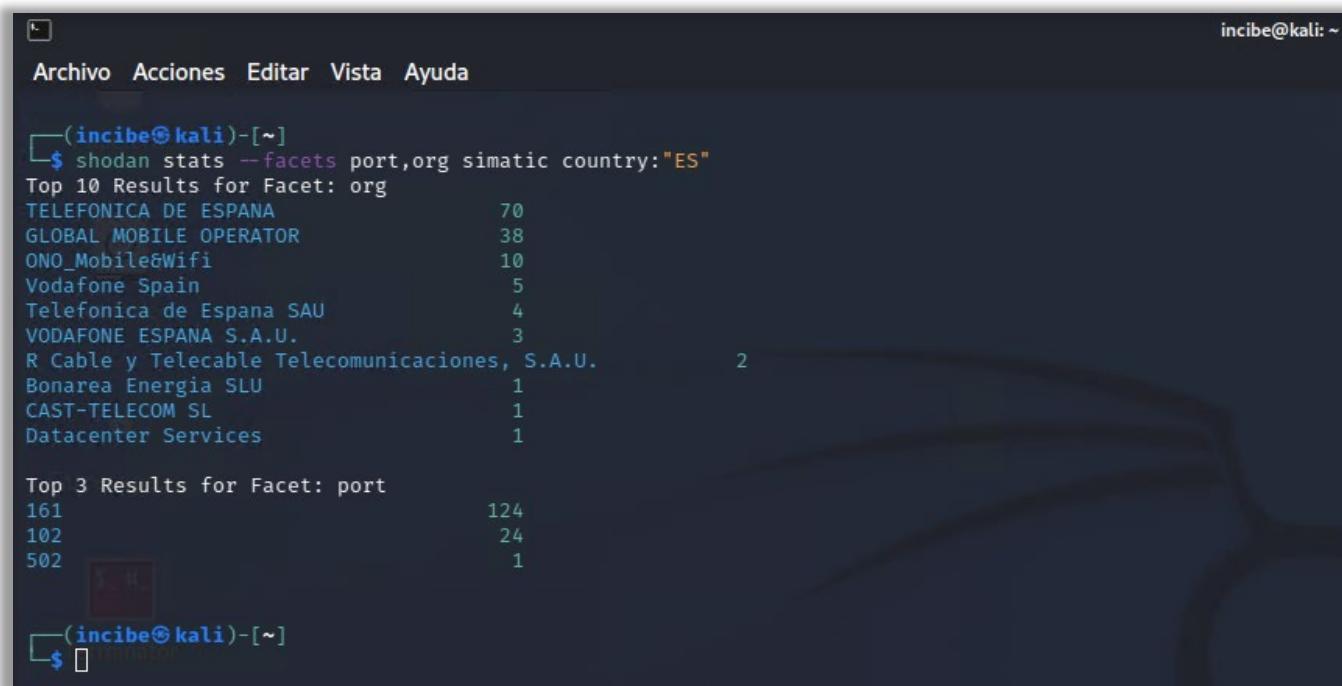
Ilustración 43: Búsqueda de dispositivos ubicados en Italia.



7

BÚSQUEDAS DESDE LA CLI: COMANDO STATS

- Modifica la anterior búsqueda añadiendo el *facets org* para que muestre no solo el *top* de puertos sino también el de organizaciones y pon como país España. El comando será el siguiente:
 - shodan stats --facets port,org simatic country:"ES"**



A terminal window titled 'Archivo Acciones Editar Vista Ayuda' with the command 'shodan stats --facets port,org simatic country:"ES"' entered. The output shows the top 10 organizations by count:

Organization	Count
TELEFONICA DE ESPANA	70
GLOBAL MOBILE OPERATOR	38
ONO_Mobile&Wifi	10
Vodafone Spain	5
Telefonica de Espana SAU	4
VODAFONE ESPANA S.A.U.	3
R Cable y Telecable Telecomunicaciones, S.A.U.	2
Bonarea Energia SLU	1
CAST-TELECOM SL	1
Datacenter Services	1

Below this, the top 3 ports are listed:

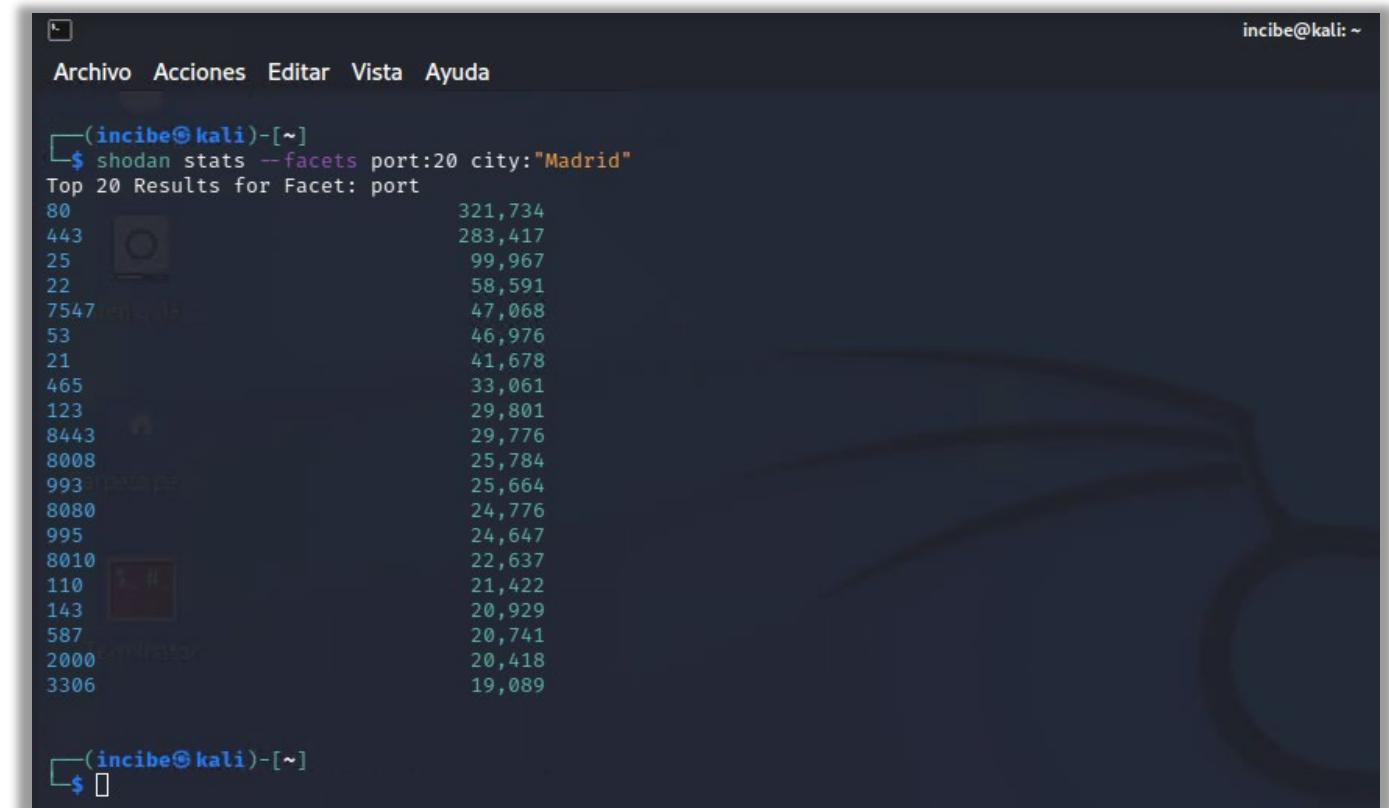
Port	Count
161	124
102	24
502	1

Ilustración 44: Edición de la búsqueda anterior para que arroje resultados de dispositivos ubicados en España.

7

BÚSQUEDAS DESDE LA CLI: COMANDO STATS

- Para indicar al *facets* que muestre más de 10 resultados, escribimos el carácter «`:`» seguido del valor máximo. Utilizando esta característica, con el siguiente comando muestras el *top 20* de resultados para el *facets port* en la ciudad de Madrid:
 - shodan stats --facets port:20 city:"Madrid"**
- Como puedes observar, para el puerto 443 (protocolo HTTPS), has obtenido 283.417 resultados.



A terminal window titled '(incibe㉿kali)-[~]' showing the output of the 'shodan stats --facets port:20 city:"Madrid"' command. The output lists the top 20 results for the 'port' facet, ordered by count. The results show various port numbers and their respective counts, with port 443 having the highest count of 283,417.

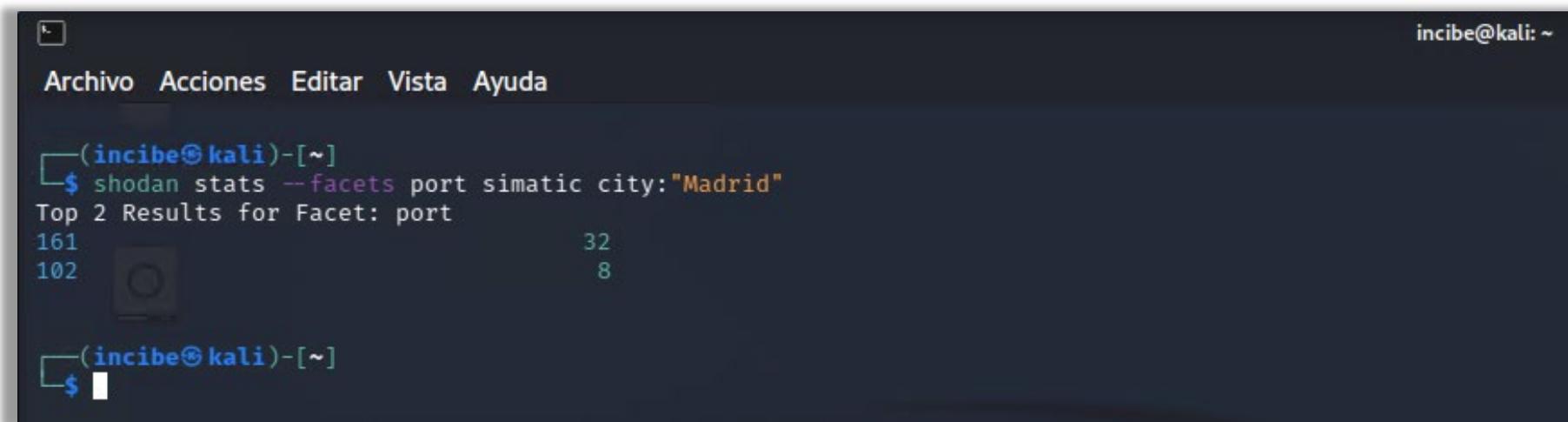
Port	Count
80	321,734
443	283,417
25	99,967
22	58,591
7547	47,068
53	46,976
21	41,678
465	33,061
123	29,801
8443	29,776
8008	25,784
993	25,664
8080	24,776
995	24,647
8010	22,637
110	21,422
143	20,929
587	20,741
2000	20,418
3306	19,089

Ilustración 45: Protocolo HTTPS.

7

BÚSQUEDAS DESDE LA CLI: COMANDO STATS

- Para mostrar el *top* de resultados por puertos en la ciudad de Madrid para los productos de Symantec utilizamos el siguiente comando:
 - shodan stats --facets port simatic city:"Madrid"



A terminal window titled 'Archivo Acciones Editar Vista Ayuda' with a user icon '(incibe@kali)-[~]'. The command '\$ shodan stats --facets port simatic city:"Madrid"' is entered. The output shows 'Top 2 Results for Facet: port' with two entries: '161' and '102'. Each entry has a small icon to its left. The terminal prompt '\$' is at the bottom.

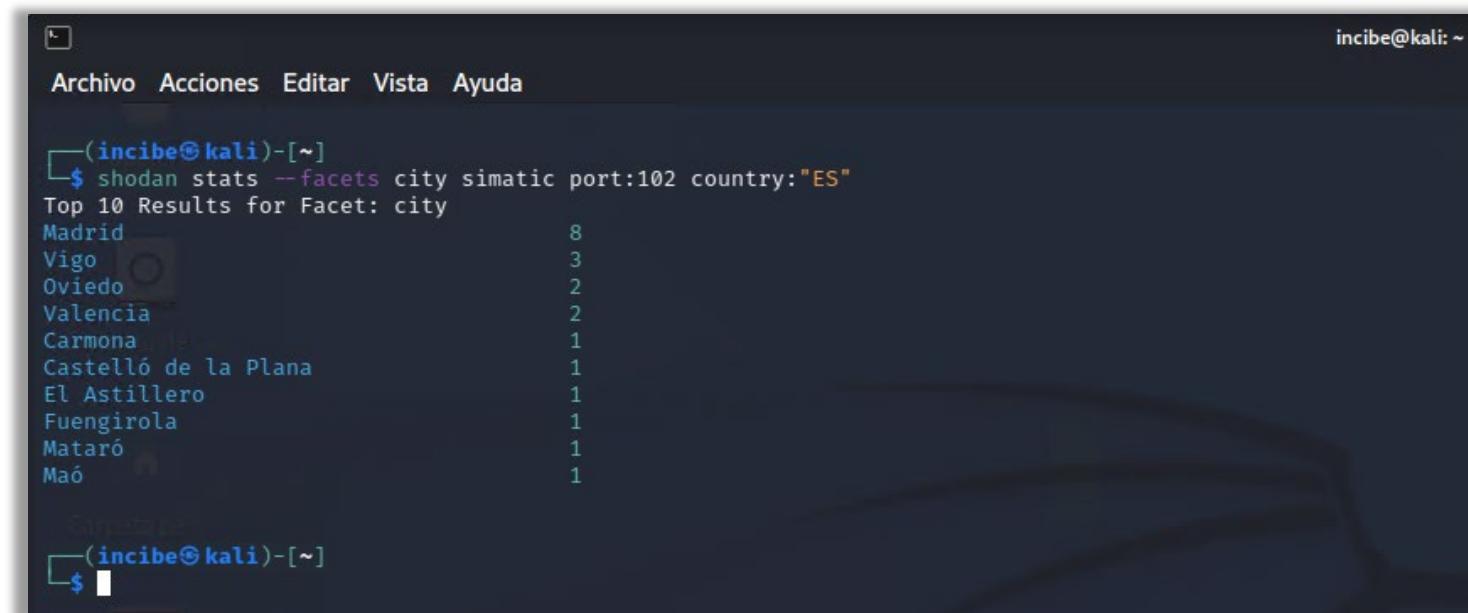
```
incibe@kali: ~
Archivo Acciones Editar Vista Ayuda
(incibe@kali)-[~]
$ shodan stats --facets port simatic city:"Madrid"
Top 2 Results for Facet: port
161
102
(incibe@kali)-[~]
```

Ilustración 46: Comando shodan *stats --facets port simatic city:"Madrid"* para obtener como resultado los puertos en Madrid.

7

BÚSQUEDAS DESDE LA CLI: COMANDO STATS

- Por último, utiliza el *facets city* (ciudad) y combínalo con los filtros *port* y *country*, obteniendo el *top* de resultados del término de búsqueda simatic, distribuidos por ciudad, filtrando por el puerto 102 en España:
 - shodan stats --facets city simatic port:102 country:"ES"



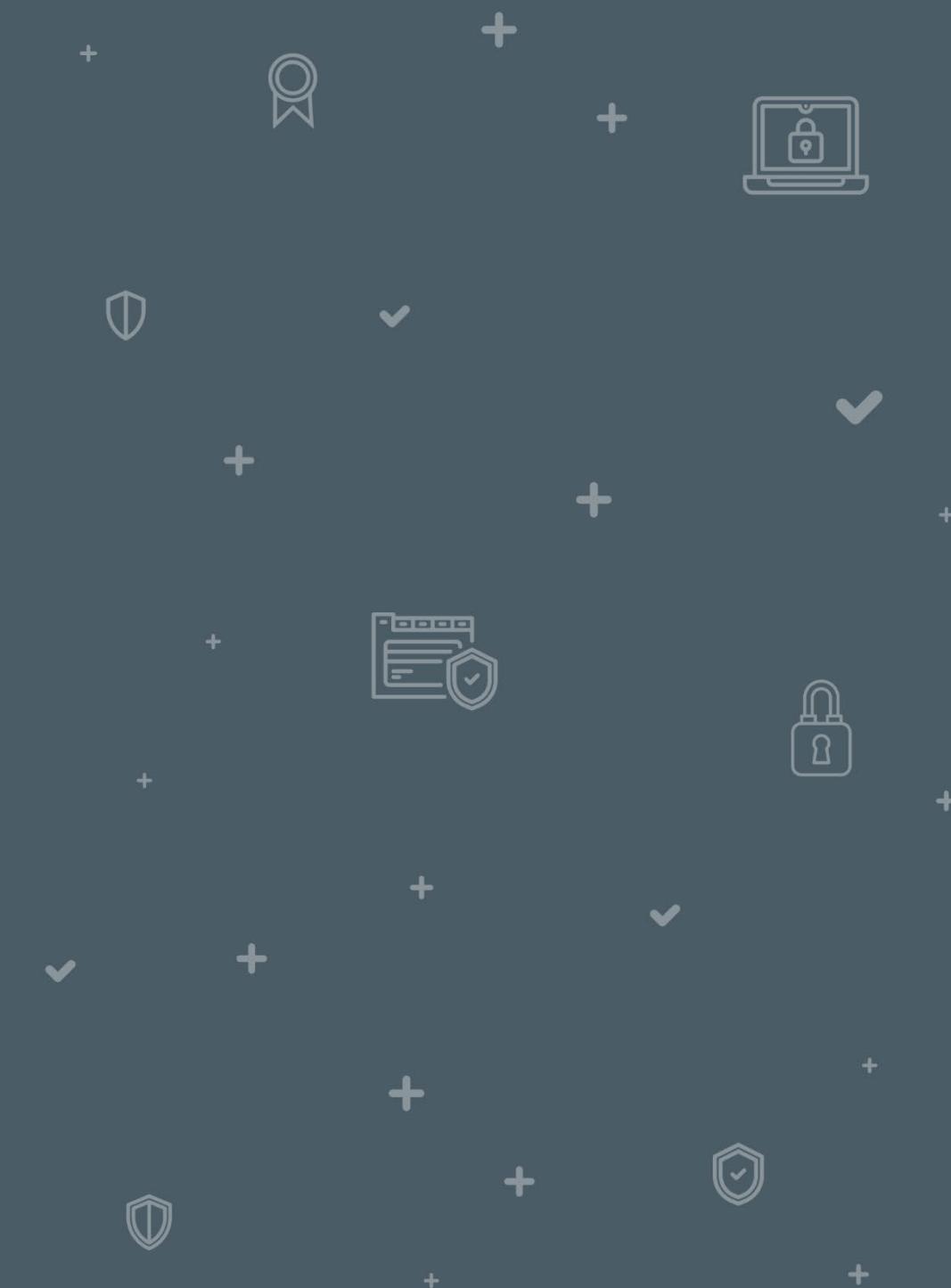
A terminal window titled '(incibe㉿kali)-[~]' showing the command \$ shodan stats --facets city simatic port:102 country:"ES". The output displays the top 10 results for the facet 'city', listing various Spanish cities and their counts. Madrid has the highest count at 8, followed by Vigo (3), Oviedo (2), Valencia (2), Carmona (1), Castelló de la Plana (1), El Astillero (1), Fuengirola (1), Mataró (1), and Maó (1).

City	Count
Madrid	8
Vigo	3
Oviedo	2
Valencia	2
Carmona	1
Castelló de la Plana	1
El Astillero	1
Fuengirola	1
Mataró	1
Maó	1

Ilustración 47: Combinación *facets city* con los filtros *port* y *country*.

BÚSQUEDAS DESDE LA CLI: COMANDO *COUNT*

8





BÚSQUEDAS DESDE LA CLI: COMANDO COUNT

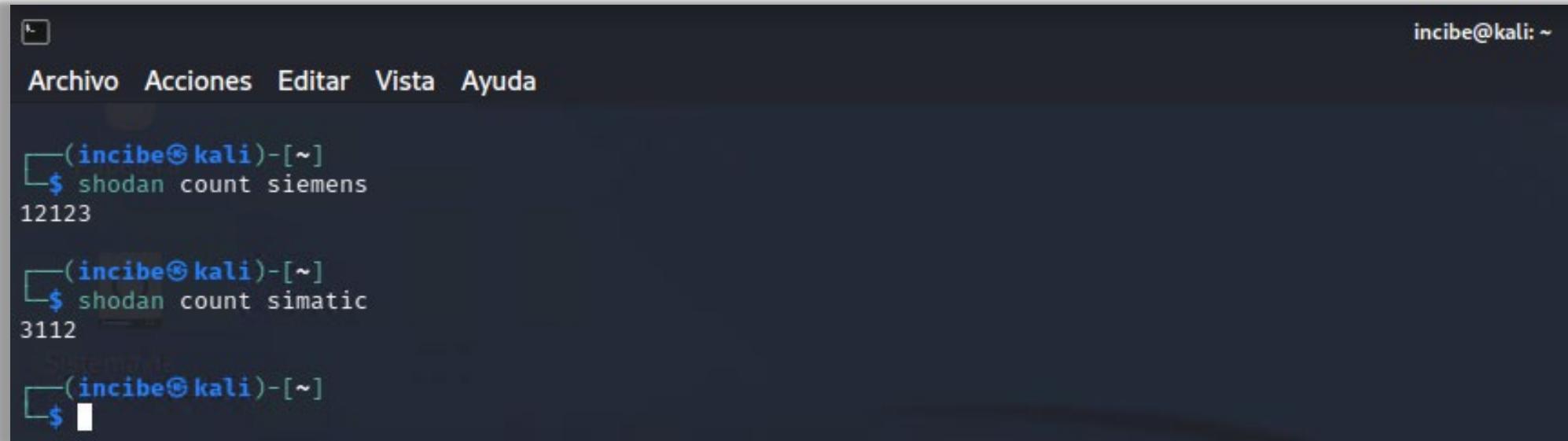
Ahora, vamos a utilizar el comando **count**. Este comando devuelve la cantidad de dispositivos en los que se ha identificado que contienen el término de búsqueda. Además, este comando permite utilizar filtros en la búsqueda, proporcionando resultados mucho más acotados. Las búsquedas las realizarás organizándolas por bloques, utilizando los nombres de fabricantes más famosos de dispositivos industriales de tipo PLC, como Siemens, Schneider Electric, etc.

- En este primer bloque, vas a realizar búsquedas relacionadas con el fabricante Siemens. Con los siguientes comandos, realiza una búsqueda del término siemens y del término simatic:
 - **shodan count siemens**
 - **shodan count simatic**

8

BÚSQUEDAS DESDE LA CLI: COMANDO COUNT

Como ves en el primer caso el buscador tiene localizados 12.123 dispositivos y para el segundo 3.112.



```
incibe@kali: ~
Archivo Acciones Editar Vista Ayuda
└──(incibe㉿kali)-[~]
    └──$ shodan count siemens
        12123

└──(incibe㉿kali)-[~]
    └──$ shodan count simatic
        3112

└──(incibe㉿kali)-[~]
    └──$ █
```

A terminal window titled 'incibe@kali: ~' showing two command executions. The first command is 'shodan count siemens' which returns the number 12123. The second command is 'shodan count simatic' which returns the number 3112. The terminal has a dark background with light-colored text and a standard Linux-style menu bar at the top.

Ilustración 48: Ejecución de comandos para buscar los términos siemens y simatic.



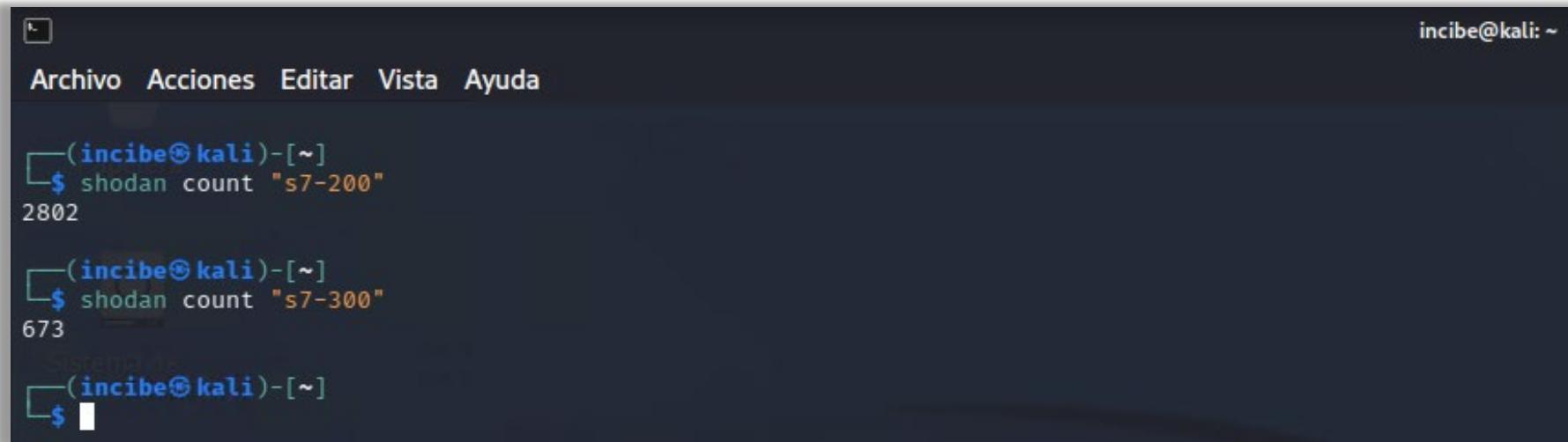
BÚSQUEDAS DESDE LA CLI: COMANDO COUNT

- Realiza una nueva búsqueda tratando de localizar dispositivos industriales s7-200 y s7-300, que identifican a PLC industriales del fabricante Siemens:
 - **shodan count “s7-200”**
 - **shodan count “s7-300”**

8

BÚSQUEDAS DESDE LA CLI: COMANDO COUNT

Como puedes observar, al realizar la búsqueda de dispositivos Siemens o Simatic, no utilizamos comillas al escribir el comando y, sin embargo, en este caso sí las hemos usado. Aunque se puede realizar utilizando o no comillas, y el comando funcionaría correctamente, en este segundo caso sí se han usado, ya que al realizar una búsqueda específica es una buena práctica el utilizar comillas dobles.



A terminal window titled 'incibe@kali: ~' showing Shodan search results for Siemens PLCs. The user has run two commands: 'shodan count "s7-200"' which returned 2802 results, and 'shodan count "s7-300"' which returned 673 results. Both commands use double quotes around the search term.

```
incibe@kali: ~
Archivo  Acciones  Editar  Vista  Ayuda
└──(incibe@kali)-[~]
    $ shodan count "s7-200"
2802
└──(incibe@kali)-[~]
    $ shodan count "s7-300"
673
└──(incibe@kali)-[~]
    $
```

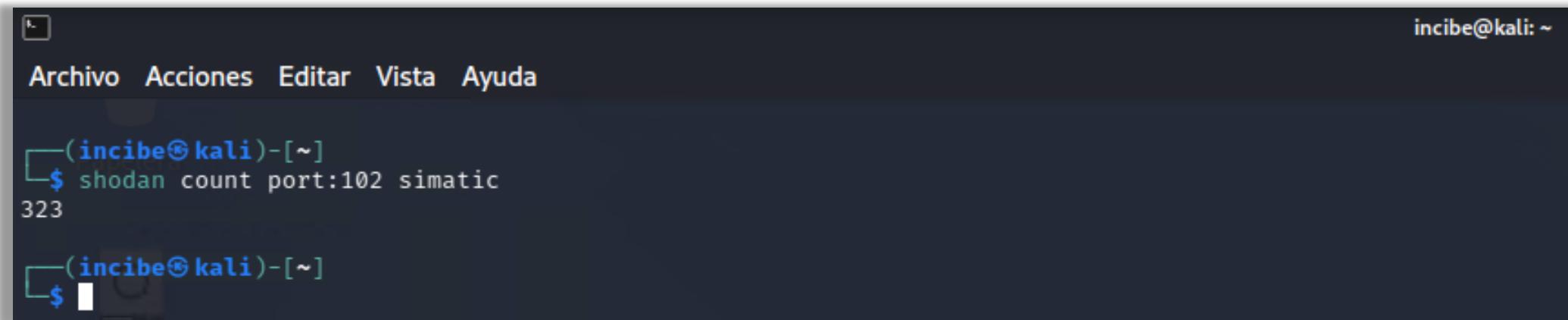
Ilustración 49: Nueva búsqueda de PLC industriales del fabricante Siemens.

8

BÚSQUEDAS DESDE LA CLI: COMANDO COUNT

- En esta nueva búsqueda utilizarás el filtro «port:102» con el término simatic, para localizar dispositivos industriales que utilizan este puerto de comunicaciones:
 - shodan count port:102 simatic

Como puedes observar en la imagen, la cantidad de dispositivos encontrados se ha reducido a 323.



The screenshot shows a terminal window with a dark background and light-colored text. At the top, it says 'incibe@kali: ~'. Below that is a menu bar with 'Archivo', 'Acciones', 'Editar', 'Vista', and 'Ayuda'. The main area of the terminal shows a command-line session:

```
(incibe㉿kali)-[~]$ shodan count port:102 simatic
323
(incibe㉿kali)-[~]$
```

Ilustración 50: Consola de búsqueda del término simatic bajo el filtro «port:102».



BÚSQUEDAS DESDE LA CLI: COMANDO COUNT

- Este hecho es muy interesante, ya que el objetivo es obtener resultados de búsquedas cerca a los 100 resultados para poder ser consultados y descargados con los comandos de Shodan **search** y **download**, como veremos más adelante.
- En este segundo bloque, realizarás búsquedas relacionadas con el fabricante Schneider Electric. Con las siguientes búsquedas tratas de localizar dispositivos del fabricante de PLC Schneider Electric y, posteriormente filtras por el puerto 502.
 - shodan count “schneider electric”**
 - shodan count port:502 “schneider electric”**

8

BÚSQUEDAS DESDE LA CLI: COMANDO COUNT



```
incibe@kali: ~
Archivo  Acciones  Editar  Vista  Ayuda
└──(incibe㉿kali)-[~]
    $ shodan count "schneider electric"
3859

└──(incibe㉿kali)-[~]
    $ shodan count port:502 "schneider electric"
3211
```

Ilustración 51: Búsqueda de dispositivos del fabricante Schneider Electric bajo el puerto 502.

Como puedes observar en la imagen el número de resultados devueltos es bastante elevado.

8

BÚSQUEDAS DESDE LA CLI: COMANDO COUNT

- Realiza una nueva búsqueda, primero del término modbus, y después filtrando por el puerto 502.
 - shodan count modbus**
 - shodan count port:502 modbus**

```
└─[incibe㉿kali)-[~]
└$ shodan count modbus
369

└─[incibe㉿kali)-[~]
└$ shodan count port:502 modbus
39

└─[incibe㉿kali)-[~]
└$ █
```

A terminal window showing two Shodan search commands. The first command, 'shodan count modbus', returns 369 results. The second command, 'shodan count port:502 modbus', returns 39 results. The terminal prompt is '@kali)'.

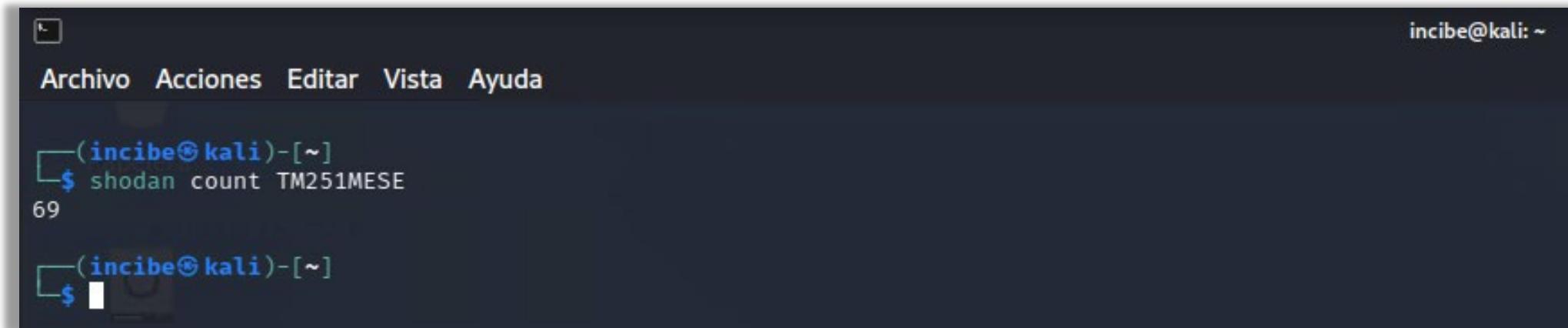
Ilustración 52: nuevo filtrado por el término modbus y puerto 502.

En este caso, el resultado devuelto es bastante inferior, como era tu objetivo.

8

BÚSQUEDAS DESDE LA CLI: COMANDO COUNT

- Por último, realiza una búsqueda para localizar dispositivos industriales del modelo TM251MESE (modelo de PLC):
 - **shodan count TM251MESE**



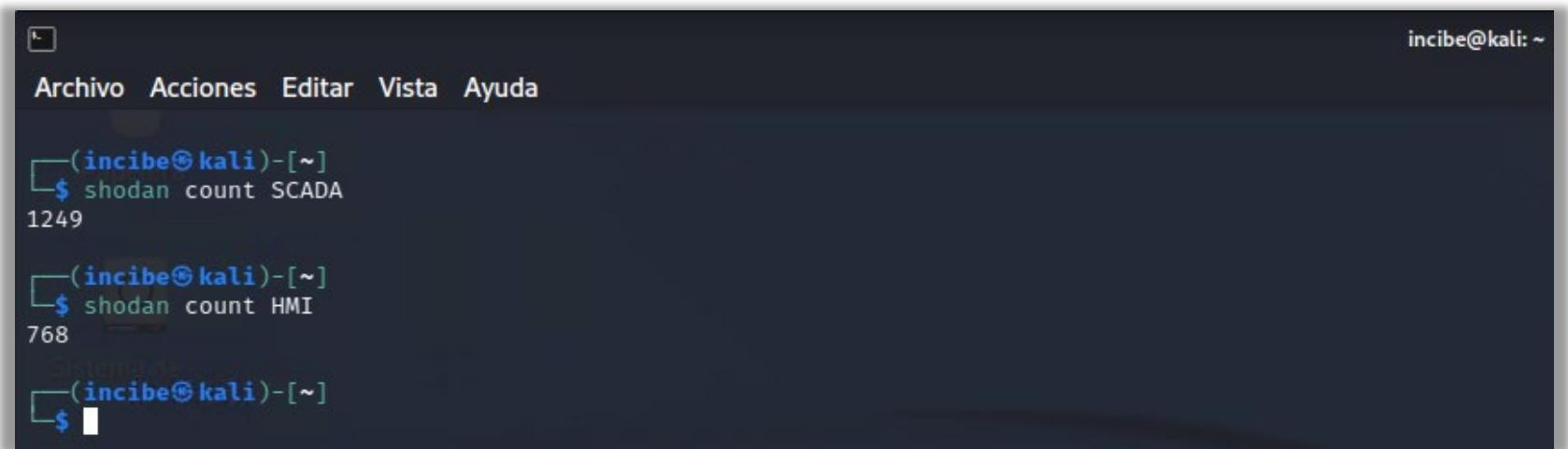
A screenshot of a terminal window titled '(incibe㉿kali)-[~]'. The window has a dark background and light-colored text. At the top, there's a menu bar with 'Archivo', 'Acciones', 'Editar', 'Vista', and 'Ayuda'. On the right side, the text 'incibe㉿kali: ~' is visible. In the center, the command '\$ shodan count TM251MESE' is typed, followed by the number '69' on the next line. Below this, another prompt '(incibe㉿kali)-[~]' is shown with a partially visible '\$' sign.

Ilustración 53: Nueva búsqueda para acotar más el resultado. Ahora bajo el modelo TM251MESE.

8

BÚSQUEDAS DESDE LA CLI: COMANDO COUNT

- Realiza nuevas búsquedas tratando de localizar el término SCADA y HMI, habitual en dispositivos industriales.
 - **shodan count SCADA**
 - **shodan count HMI**



A terminal window titled 'Archivo' with a dark background and light text. The user is at the prompt '\$'. The window shows two search results:

- Search for 'SCADA':
 - Result count: 1249
 - Command: shodan count SCADA
- Search for 'HMI':
 - Result count: 768
 - Command: shodan count HMI

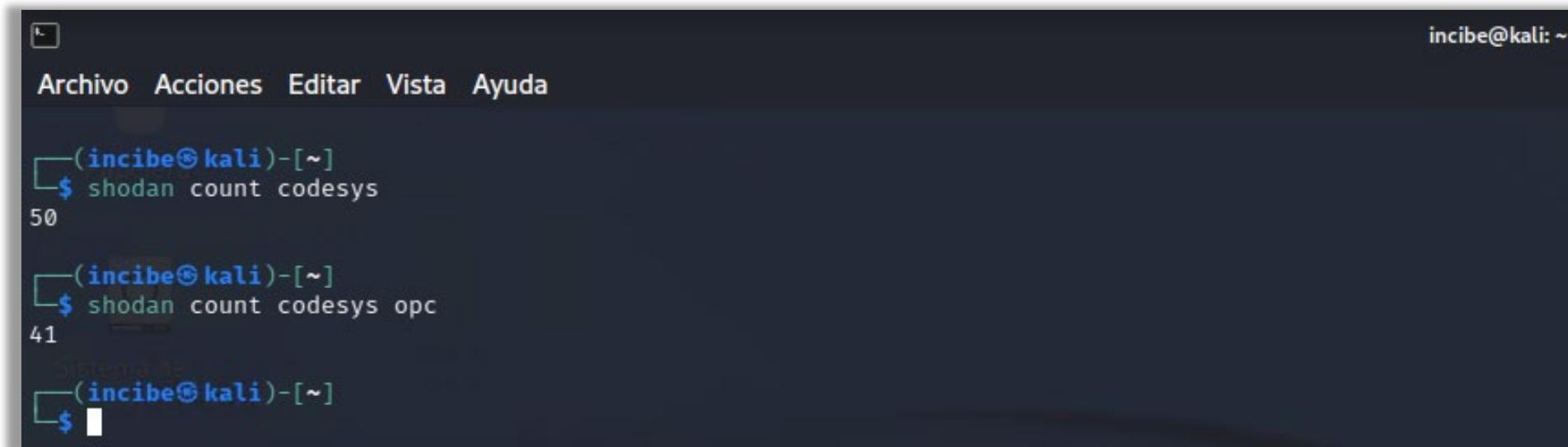
Ilustración 54: Búsqueda de los términos SCADA y HMI.

En este caso, los resultados devueltos son bastante elevados y al ser términos algo genéricos, es posible que algún resultado de las búsquedas no corresponda con dispositivos industriales.

8

BÚSQUEDAS DESDE LA CLI: COMANDO COUNT

- Ahora, realiza búsquedas para identificar dispositivos que utilizan la plataforma de software CoDeSys y del tipo OPC.
 - **shodan count codesys**
 - **shodan count codesys opc**



```
incibe@kali: ~
Archivo  Acciones  Editar  Vista  Ayuda

└─(incibe㉿kali)-[~]
    $ shodan count codesys
50

└─(incibe㉿kali)-[~]
    $ shodan count codesys opc
41

└─(incibe㉿kali)-[~]
    $ █
```

A terminal window titled 'incibe@kali: ~' showing two Shodan search commands. The first command, 'shodan count codesys', returns 50 results. The second command, 'shodan count codesys opc', returns 41 results. Both commands are run from a root shell on a Kali Linux system.

Ilustración 55: Búsquedas para identificar dispositivos que utilizan la plataforma de software CoDeSys y del tipo OPC.

8

BÚSQUEDAS DESDE LA CLI: COMANDO COUNT

- Para finalizar, realiza una búsqueda de dispositivos Rockwell/Allen-Bradley, que identifica a un fabricante de dispositivos industriales de tipo PLC:
 - shodan count “Rockwell Automation/Allen-Bradley”**



```
incibe@kali: ~
Archivo  Acciones  Editar  Vista  Ayuda
└──(incibe㉿kali)-[~]
    $ shodan count "Rockwell Automation/Allen-Bradley"
6513
└──(incibe㉿kali)-[~]
    $
```

A terminal window titled 'Archivo Acciones Editar Vista Ayuda' with a user prompt '(incibe㉿kali)-[~]'. The command 'shodan count "Rockwell Automation/Allen-Bradley"' is entered, followed by the output '6513'. The window title bar shows 'incibe@kali: ~'.

Ilustración 56: Imagen de nueva búsqueda de dispositivos PLC.

Como has podido comprobar, en algunas búsquedas los resultados devueltos son bastante elevados, por lo que habrá que intentar ser más preciso en los términos de búsqueda utilizados. Esto lo veremos en otro apartado donde combinaremos la utilización de los comandos **count**, **stats** y **search**.



BÚSQUEDAS DESDE LA CLI: COMANDO *SEARCH*

9



BÚSQUEDAS DESDE LA CLI: COMANDO **SEARCH**

Ahora, vamos a utilizar el comando **search**. Con este comando realizarás búsquedas en la base de datos del motor Shodan mostrando solo los campos que interesen.

- Para mostrar la salida del comando **search** de Shodan, conviene que utilices la herramienta del sistema operativo **less**.
- Para moverte por las pantallas de resultados que muestra esta herramienta, utilizaremos las teclas de movimiento:
 - Inicio, Fin, RePag y AvPag
- Para invocar la pantalla de ayuda ejecutaremos el comando que veremos a continuación y para salir de esta pantalla de ayuda o de la pantalla de resultados, pulsaremos la tecla «q».
- Ejecuta la ayuda del comando **search**:
 - **shodan search -h**



BÚSQUEDAS DESDE LA CLI: COMANDO SEARCH

The screenshot shows a terminal window with a dark background. At the top, there's a menu bar with options: Archivo, Acciones, Editar, Vista, Ayuda. Below the menu, the terminal prompt is `(incibe㉿kali)-[~]`. The user types `$ shodan search -h` and presses Enter. The terminal displays the help documentation for the `shodan search` command:

```
Usage: shodan search [OPTIONS] <search query>

Search the Shodan database

Options:
--color / --no-color           List of properties to show in the search results.
--fields TEXT                  The number of search results that should be returned.
--limit INTEGER                Maximum: 1000
--separator TEXT               The separator between the properties of the search
                               results.
-h, --help                      Show this message and exit.
```

At the bottom of the terminal window, the prompt `(incibe㉿kali)-[~]` appears again, followed by a dollar sign `$` and a blank line for input.

Ilustración 57: Búsqueda en Shodan desde la CLI.

9

BÚSQUEDAS DESDE LA CLI: COMANDO SEARCH

- De las opciones disponibles, utilizarás las siguientes:
 - Opción **--fields**: indica a Shodan los campos que quieras que muestre (separados por tabulaciones).

De todos los campos *fields (properties)* disponibles, los que van a proporcionar resultados más útiles son los siguientes:

Propiedad	Significado
timestamp	Muestra la fecha y la hora de recopilación de la información del dispositivo en cuestión.
ip_str	Dirección IP.
port	Puerto.
product	Producto/Servicio.
os	Sistema operativo.
tags	Etiquetas, como, por ejemplo, la que indica si un dispositivo es ICS.
hostnames	Hostnames.



BÚSQUEDAS DESDE LA CLI: COMANDO SEARCH

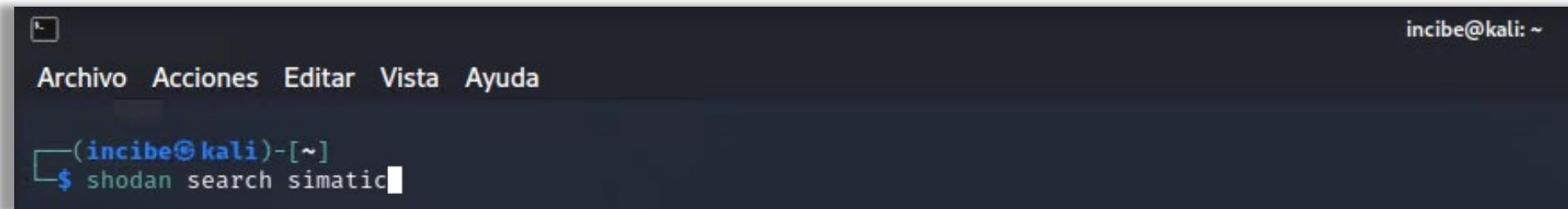
Propiedad	Significado
<code>transport</code>	Protocolo de transporte.
<code>domains</code>	Dominios.
<code>_shodan</code>	Muestra información relativa a cómo Shodan ha recopilado la información del dispositivo.
<code>_shodan.module</code>	Identifica el módulo utilizado por Shodan para recolectar la información del dispositivo.
<code>location</code>	Muestra todos los datos de ubicación.
<code>location.city</code>	Muestra la ciudad.
<code>location.country_code</code>	Muestra el código del país, como ES.
<code>location.country_name</code>	Muestra el nombre del país.
<code>org</code>	Muestra la organización.
<code>data</code>	Muestra información asociada al tipo de dispositivo, protocolo o puerto, que ha detectado Shodan.

- Opción `--limit`: limita el número máximo de resultados de búsqueda que va a devolver Shodan.

9

BÚSQUEDAS DESDE LA CLI: COMANDO SEARCH

- Realiza la primera búsqueda con este comando, buscando el término simatic.
 - shodan search simatic**



A screenshot of a terminal window on a Kali Linux system. The window title bar says 'incibe@kali: ~'. The menu bar includes 'Archivo', 'Acciones', 'Editar', 'Vista', and 'Ayuda'. Below the menu is a terminal prompt: '(incibe@kali)-[~] \$ shodan search simatic'.

Ilustración 58: Búsqueda del término «simatic» con el comando «shodan search simatic».



9 BÚSQUEDAS DESDE LA CLI: COMANDO SEARCH

- El resultado que devuelve es un listado de 100 resultados de búsqueda donde aparecen una serie de campos por defecto, que son los siguientes y en el orden aquí indicado:

- Dirección IP, puerto, *hostname*, y datos que contienen información asociada al tipo de dispositivo, protocolo o puerto, que ha detectado Shodan.

Como se observa en las imágenes la mayoría de los puertos que aparecen corresponden a dispositivos industriales (puertos 102 y 502).

```
Archivo Acciones Editar Vista Ayuda
139.59.98.244 161 0A\x02\x01\x00\x04\x06public\x24\x02\x04\xfbij"\x02\x01\x00\x02\x01\x00\x06$|x06\x08+\x05\x01\x02\x01\x01\x00\x04\x18siemens, SIMATIC, S7-200
129.2.27.81 502 129-2-27-81.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\nn
183.76.166.219 161 ab166219.ppp.asahi-net.or.jp 0-\x02\x01\x00\x04\x06public\x24\x02\x04\xfbij"\x02\x01\x00\x06$|x06\x08+\x05\x01\x02\x01\x01\x00\x04\x18siemens, SIMATIC S7, CPU-1200,
6EST 215-1AG40-0XB0, HW: 12, FW: V.4.4.1, S V-NIB37907
133.232.77.9 161 133-232-77-9.static.zoot.jp 0-\x02\x01\x00\x04\x06public\x24\x02\x04\xfbij"\x02\x01\x00\x02\x01\x00\x06$|x06\x08+\x05\x01\x02\x01\x01\x00\x04\x18siemens, SIMATIC S7, CPU-1200,
6EST 215-1AG40-0XB0, HW: 12, FW: V.4.4.1, S V-NIB3701
41.155.232.166 161 0}\x02\x01\x00\x04\x06public\x24\x02\x04\xfbij"\x02\x01\x00\x02\x01\x00\x06$|x06\x08+\x05\x01\x02\x01\x01\x00\x04\x18siemens, SIMATIC S7, CPU-1200, 6EST 212-1BE40-0XB0, HW:
7, FW: V.4.2.1, S V-K8CS2683
2.196.100.143 161 Siemens, SIMATIC NET, SCALANCE M876-4 EU, 6GK5 876-4AA00-2BA2, HW: Version 006.02.00, SVPM0144938
91.223.193.71 161 0A\x02\x01\x00\x04\x06public\x24\x02\x04\xfbij"\x02\x01\x00\x06$|x06\x08+\x05\x01\x02\x01\x01\x00\x04\x18siemens, SIMATIC, S7-300
185.109.109.1 161 0A\x02\x01\x00\x04\x06public\x24\x02\x04\xfbij"\x02\x01\x00\x06$|x06\x08+\x05\x01\x02\x01\x01\x00\x04\x18siemens, SIMATIC, S7-300
46.227.222.193 161 ip-46-227-222-193.en.viatel.net 0}\x02\x01\x00\x04\x06public\x24\x02\x04\xfbij"\x02\x01\x00\x02\x01\x00\x06$|x06\x08+\x05\x01\x02\x01\x01\x00\x04\x18siemens, SIMATIC S7, CPU-1200,
6EST 212-1HE40-0XB0, HW: 2, FW: V.4.1.1, S C-F2594986
129.2.27.13 502 129-2-27-13.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\nn
129.2.27.45 502 129-2-27-45.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\nn
129.2.27.105 502 129-2-27-105.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\nn
129.2.27.218 502 129-2-27-218.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\nn
45.219.102.207 161 Siemens, SIMATIC NET, SCALANCE M876-4 EU, 6GK5 876-4AA00-2BA2, HW: Version 1, FW: Version 006.01.00, SVP1134416
77.104.252.119 102 Copyright: Original Siemens Equipment\nPLC name: SIMATIC 300 (1)\nModule type: IM151-8 PN/DP CPU\nUnknown (129): Boot Loader A\\nModule: 6ES 151-8AB01-0AB0 v.0.7\\n
nBasis Firmware: v.3.2.14\\nModule name: IM151-8 PN/DP CPU\\nSerial number of module: S C-KORV022/2018\\nPlant identification: \\nBasic Hardware: 6ES 151-8AB01-0AB0 v.0.7\\n
165.232.136.159 161 0A\x02\x01\x00\x04\x06public\x24\x02\x04\xfbij"\x02\x01\x00\x06$|x06\x08+\x05\x01\x02\x01\x01\x00\x04\x18siemens, SIMATIC, S7-300
213.86.80.14 161 0A\x02\x01\x00\x04\x06public\x24\x02\x04\xfbij"\x02\x01\x00\x06$|x06\x08+\x05\x01\x02\x01\x01\x00\x04\x18siemens, SIMATIC, S7-300
129.2.27.162 502 129-2-27-162.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\nn
129.2.27.151 502 129-2-27-151.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\nn
81.23.178.175 102 host-81-23-178-175.tilt.ru Copyright: Original Siemens Equipment\nPLC name: SIMATIC 300 (1)\nModule type: CPU 314C-2 PN/DP\\nUnknown (129): Boot Loader A\\nModule: 6ES 7
314-6EH04-0AB0 v.0.2\\nBasic Firmware: v.3.3.7\\nModule name: CPU 314C-2 PN/DP\\nSerial number of module: S C-C0066225291\\nPlant identification: \\nBasic Hardware: 6ES 314-6EH04-0AB0 v.0.2\\n
129.2.27.74 502 129-2-27-74.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\nn
129.2.27.70 502 129-2-27-70.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\nn
129.2.27.150 502 129-2-27-150.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\nn
129.2.27.93 502 129-2-27-93.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\nn
133.232.82.246 161 133-232-82-246.static.zoot.jp 0-\x02\x01\x00\x04\x06public\x24\x02\x04\xfbij"\x02\x01\x00\x02\x01\x00\x06$|x06\x08+\x05\x01\x02\x01\x01\x00\x04\x18siemens, SIMATIC S7, CPU-1200,
6EST 215-1AG40-0XB0, HW: 12, FW: V.4.4.1, S V-NIB32175
129.2.27.169 502 129-2-27-169.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\nn
62.167.224.160 161 Siemens, SIMATIC NET, SCALANCE M876-4 EU, 6GK5 876-4AA00-2BA2, HW: Version 1, FW: Version 006.02.00, SVPK9148284
216.238.104.90 161 216-238-104.90.vultrusercontent.com 0A\x02\x01\x00\x04\x06public\x24\x02\x04\xfbij"\x02\x01\x00\x02\x01\x00\x06$|x06\x08+\x05\x01\x02\x01\x01\x00\x04\x18siemens, SIMATIC, S7
-300
222.114.104.52 161 0}\x02\x01\x00\x04\x06public\x24\x02\x04\xfbij"\x02\x01\x00\x02\x01\x00\x06$|x06\x08+\x05\x01\x02\x01\x01\x00\x04\x18siemens, SIMATIC, S7-200
W: 1, FW: V6.0.9, SVP061908
206.189.38.43 161 0A\x02\x01\x00\x04\x06public\x24\x02\x04\xfbij"\x02\x01\x00\x02\x01\x00\x06$|x06\x08+\x05\x01\x02\x01\x01\x00\x04\x18siemens, SIMATIC, S7-200
129.2.27.82 502 129-2-27-82.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\nn
62.94.102.211 102 ip-102-211.smn.cloudflair.com Copyright: Original Siemens Equipment\nPLC name: SIMATIC 300\\nModule type: CPU 315-2 DP\\nUnknown (129): Boot Loader A\\nModule: 6ES 315-2AG10-0AB0 v.0.7\\n
10-0AB0 v.0.7\\nBasic Firmware: v.2.6.6\\nModule name: CPU 315-2 DP\\nSerial number of module: S C-N3J990112021\\nPlant identification: \\nBasic Hardware: 6ES 315-2AG10-0AB0 v.0.7\\n
89.149.8.194 161 0A\x02\x01\x00\x04\x06public\x24\x02\x04\xfbij"\x02\x01\x00\x02\x01\x00\x06$|x06\x08+\x05\x01\x02\x01\x01\x00\x04\x18siemens, SIMATIC, S7-300
222.255.1.157 161 static.vnp7.vt 0A\x02\x01\x00\x04\x06public\x24\x02\x04\xfbij"\x02\x01\x00\x02\x01\x00\x06$|x06\x08+\x05\x01\x02\x01\x01\x00\x04\x18siemens, SIMATIC, S7-300
129.2.27.94 502 129-2-27-94.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\nn
129.2.27.24 502 129-2-27-24.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\nn
34.142.40.239 161 239-40-142-34.bc.googleusercontent.com 0A\x02\x01\x00\x04\x06public\x24\x02\x04\xfbij"\x02\x01\x00\x02\x01\x00\x06$|x06\x08+\x05\x01\x02\x01\x01\x00\x04\x18siemens, SIMATIC, S7
-300
35.131.239.2 102 035-131-239-002.biz.spectrum.com Copyright: Original Siemens Equipment\nPLC name: SIMATIC 300-Station\\nModule type: CPU 315F-2 PN/DP\\nUnknown (129): Boot Loader A\\n
nModule: 6ES 315-2FJ14-0AB0 v.0.10\\nBasic Firmware: v.3.2.17\\nModule name: CPU 315F-2 PN/DP\\nSerial number of module: S C-N3J990112021\\nPlant identification: \\nBasic Hardware: 6ES 315-2FJ14-0AB0 v.0.10
\n
:
```

Ilustración 59: Resultado del paso anterior para los puertos 102 y 502 (I).

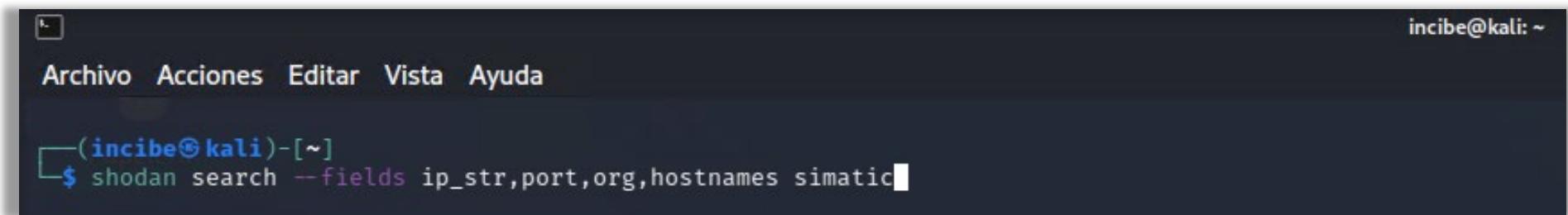
BÚSQUEDAS DESDE LA CLI: COMANDO *SEARCH*

Ilustración 60: Resultado del paso anterior para los puertos 102 y 502 (II).

9

BÚSQUEDAS DESDE LA CLI: COMANDO SEARCH

- Realiza de nuevo la búsqueda sobre el término simatic pero indicando que quieres que únicamente muestre la información de los campos dirección IP, puerto, organización y *hostname*.
 - shodan search --fields ip_str,port,org,hostnames simatic

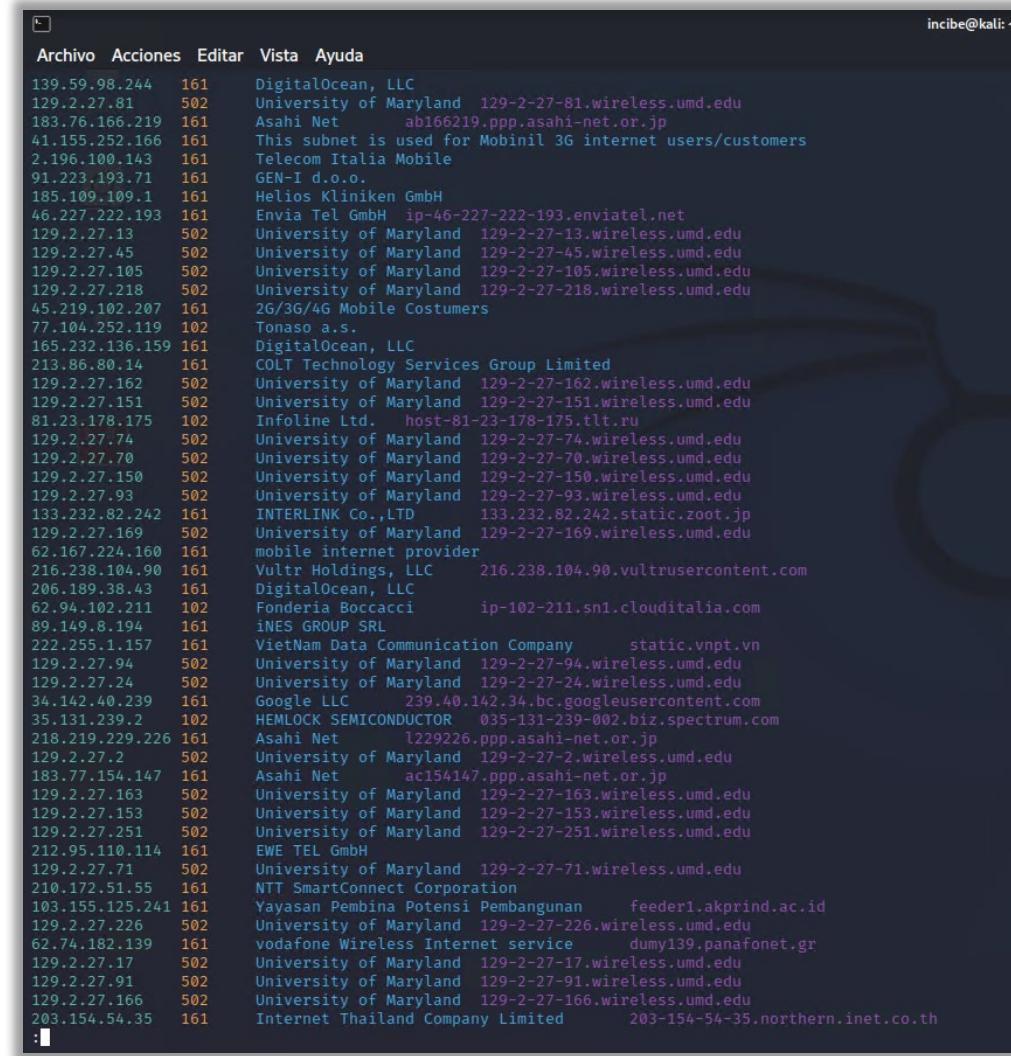


A screenshot of a terminal window titled 'incibe@kali: ~'. The window has a dark background and light-colored text. At the top, there's a menu bar with options: Archivo, Acciones, Editar, Vista, Ayuda. Below the menu, the terminal prompt shows '(incibe@kali)-[~]'. The user has typed the command '\$ shodan search --fields ip_str,port,org,hostnames simatic' and is waiting for the results.

Ilustración 61: Nueva búsqueda para la información dirección IP, puerto, organización y *hostname*.



BÚSQUEDAS DESDE LA CLI: COMANDO SEARCH

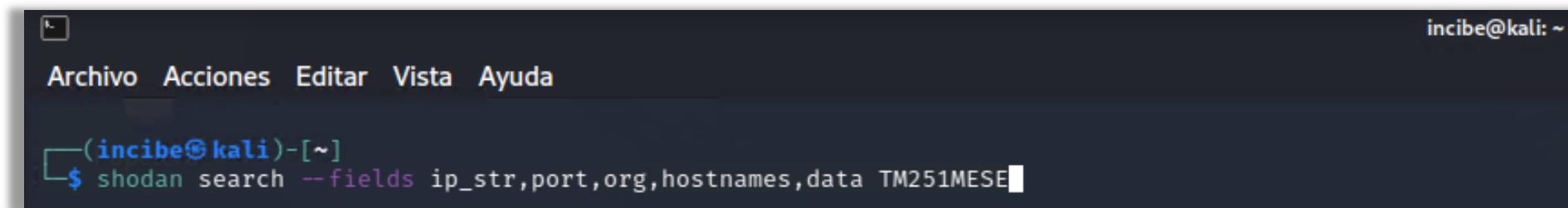


```
incibe@kali: ~
Archivo  Acciones  Editar  Vista  Ayuda
139.59.98.244  161  DigitalOcean, LLC
129.2.27.81    502  University of Maryland 129-2-27-81.wireless.umd.edu
183.76.166.219 161  Asahi Net      ab166219.ppp.asahi-net.or.jp
41.155.252.166 161  This subnet is used for Mobinil 3G internet users/customers
2.196.100.143  161  Telecom Italia Mobile
91.223.193.71  161  GEN-I d.o.o.
185.109.109.1  161  Helios Kliniken GmbH
46.227.222.193 161  Envia Tel GmbH ip-46-227-222-193.enviatele.net
129.2.27.13    502  University of Maryland 129-2-27-13.wireless.umd.edu
129.2.27.45    502  University of Maryland 129-2-27-45.wireless.umd.edu
129.2.27.105   502  University of Maryland 129-2-27-105.wireless.umd.edu
129.2.27.218   502  University of Maryland 129-2-27-218.wireless.umd.edu
45.219.102.207 161  2G/3G/4G Mobile Costumers
77.104.252.119 102  Tonaso a.s.
165.232.136.159 161  DigitalOcean, LLC
213.86.80.14   161  COLT Technology Services Group Limited
129.2.27.162   502  University of Maryland 129-2-27-162.wireless.umd.edu
129.2.27.151   502  University of Maryland 129-2-27-151.wireless.umd.edu
81.23.178.175  102  Infoline Ltd. host-81-23-178-175.tilt.ru
129.2.27.74    502  University of Maryland 129-2-27-74.wireless.umd.edu
129.2.27.70    502  University of Maryland 129-2-27-70.wireless.umd.edu
129.2.27.150   502  University of Maryland 129-2-27-150.wireless.umd.edu
129.2.27.93    502  University of Maryland 129-2-27-93.wireless.umd.edu
133.232.82.242 161  INTERLINK Co.,LTD 133.232.82.242.static.zoot.jp
129.2.27.169   502  University of Maryland 129-2-27-169.wireless.umd.edu
62.167.224.160 161  mobile internet provider
216.238.104.90 161  Vultr Holdings, LLC 216.238.104.90.vultrusercontent.com
206.189.38.43  161  DigitalOcean, LLC
62.94.102.211  102  Fonderia Boccacci ip-102-211.sm1.clouditalia.com
89.149.8.194   161  iNES GROUP SRL
222.255.1.157  161  VietNam Data Communication Company static.vnpt.vn
129.2.27.94    502  University of Maryland 129-2-27-94.wireless.umd.edu
129.2.27.24    502  University of Maryland 129-2-27-24.wireless.umd.edu
34.142.40.239  161  Google LLC 239.40.142.34.bc.googleusercontent.com
35.131.239.2   102  HEMLOCK SEMICONDUCTOR 035-131-239-002.biz.spectrum.com
218.219.229.226 161  Asahi Net l229226.ppp.asahi-net.or.jp
129.2.27.2    502  University of Maryland 129-2-27-2.wireless.umd.edu
183.77.154.147 161  Asahi Net ac154147.ppp.asahi-net.or.jp
129.2.27.163   502  University of Maryland 129-2-27-163.wireless.umd.edu
129.2.27.153   502  University of Maryland 129-2-27-153.wireless.umd.edu
129.2.27.251   502  University of Maryland 129-2-27-251.wireless.umd.edu
212.95.110.114 161  EWE TEL GmbH
129.2.27.71    502  University of Maryland 129-2-27-71.wireless.umd.edu
210.172.51.55  161  NTT SmartConnect Corporation
103.155.125.241 161  Yayasan Pembina Potensi Pembangunan feeder1.akprind.ac.id
129.2.27.226   502  University of Maryland 129-2-27-226.wireless.umd.edu
62.74.182.139  161  vodafone Wireless Internet service dummy139.panafonet.gr
129.2.27.17    502  University of Maryland 129-2-27-17.wireless.umd.edu
129.2.27.91    502  University of Maryland 129-2-27-91.wireless.umd.edu
129.2.27.166   502  University of Maryland 129-2-27-166.wireless.umd.edu
203.154.54.35  161  Internet Thailand Company Limited 203-154-54-35.northern.inet.co.th
:
```

9

BÚSQUEDAS DESDE LA CLI: COMANDO SEARCH

- Realiza una búsqueda más específica de un dispositivo industrial identificado como TM251MESE, que corresponde a un dispositivo industrial del fabricante Schneider Electric (como ya vimos anteriormente). Al querer que sea una búsqueda específica, añade dentro de las propiedades *data*.
 - **shodan search --fields ip_str,port,org,hostnames,data TM251MESE**



A screenshot of a terminal window on a Kali Linux system. The window title bar says 'incibe@kali: ~'. The menu bar includes 'Archivo', 'Acciones', 'Editar', 'Vista', and 'Ayuda'. Below the menu is a user prompt '(incibe@kali)-[~]'. The command '\$ shodan search --fields ip_str,port,org,hostnames,data TM251MESE' is entered at the prompt.

Ilustración 63: Búsqueda para dispositivo de la compañía Schneider Electric.

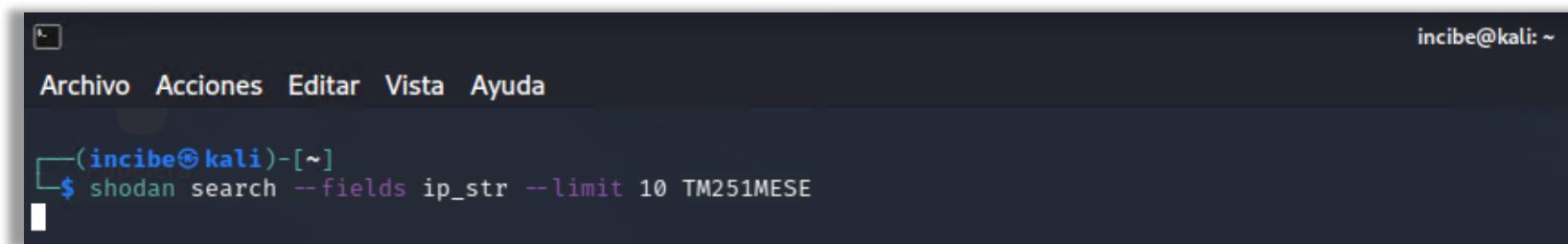
BÚSQUEDAS DESDE LA CLI: COMANDO *SEARCH*

Ilustración 64: Resultados de la búsqueda de dispositivos Schneider Electric.

9

BÚSQUEDAS DESDE LA CLI: COMANDO SEARCH

- Por último, limita la anterior búsqueda referente a dispositivos TM251MESE a únicamente 10 resultados, indicando en el comando que solo quieres visualizar el campo de la dirección IP.
- Realiza una búsqueda más específica de un dispositivo industrial identificado como TM251MESE, que corresponde a un dispositivo industrial del fabricante Schneider Electric (como ya vimos anteriormente). Al querer que sea una búsqueda específica, añade dentro de las propiedades *data*.
 - **shodan search --fields ip_str --limit 10 TM251MESE**

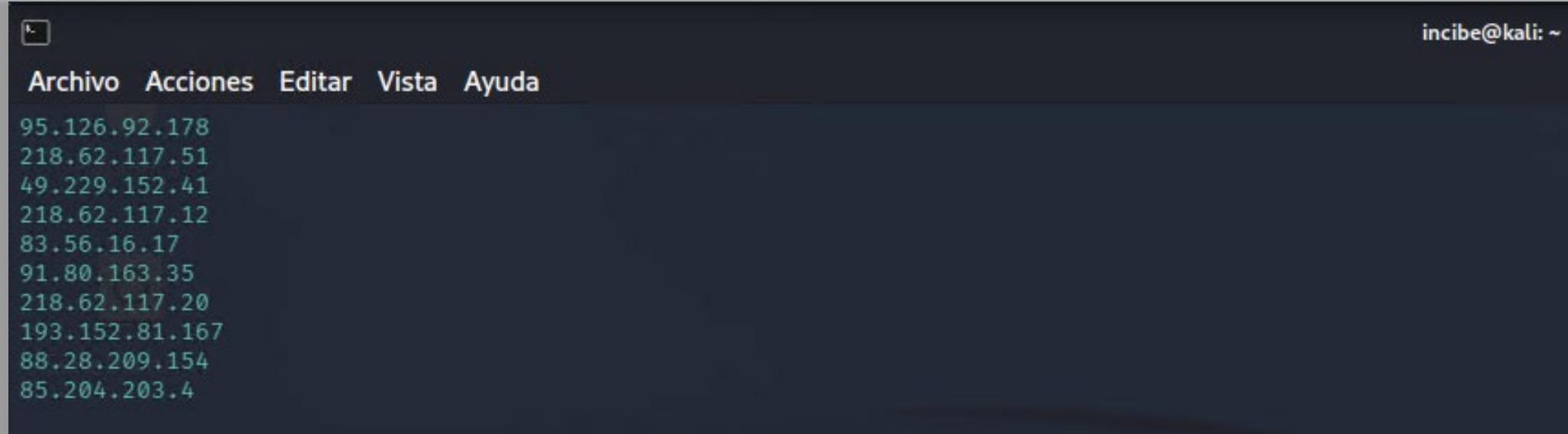


A screenshot of a terminal window titled 'incibe@kali: ~'. The window has a dark background and light-colored text. At the top, there's a menu bar with options: Archivo, Acciones, Editar, Vista, Ayuda. Below the menu, the terminal prompt shows '(incibe㉿kali)-[~] \$'. The user has typed the command 'shodan search --fields ip_str --limit 10 TM251MESE' into the terminal. The cursor is positioned at the end of the command line.

Ilustración 65: Limitación de la búsqueda anterior a solo diez resultados.



BÚSQUEDAS DESDE LA CLI: COMANDO SEARCH



A screenshot of a terminal window titled 'incibe@kali: ~'. The window has a dark background and a light-colored header bar. In the header bar, there is a small icon on the left, followed by the terminal title 'incibe@kali: ~' and a tilde symbol (~) on the right. Below the header bar, there is a menu bar with the following options: 'Archivo', 'Acciones', 'Editar', 'Vista', and 'Ayuda'. The main body of the terminal contains a list of IP addresses, each on a new line. The IP addresses listed are:

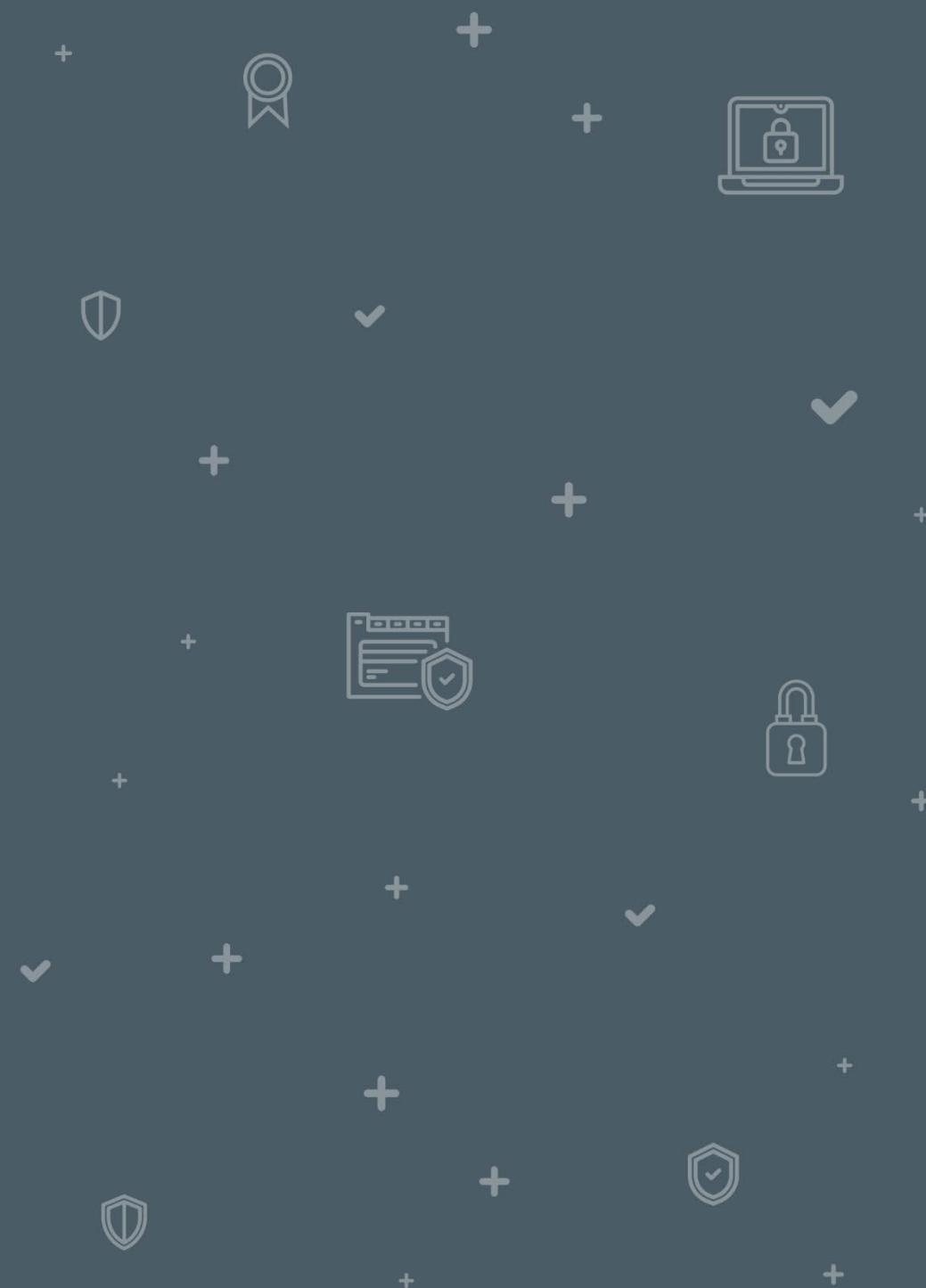
- 95.126.92.178
- 218.62.117.51
- 49.229.152.41
- 218.62.117.12
- 83.56.16.17
- 91.80.163.35
- 218.62.117.20
- 193.152.81.167
- 88.28.209.154
- 85.204.203.4

Ilustración 66: Resultados de la búsqueda anterior.

BÚSQUEDAS DESDE LA CLI: UTILIZACIÓN CONJUNTA DE LOS COMANDOS *COUNT*, *STATS* Y *SEARCH*

- 10.1 Búsqueda de dispositivos industriales del fabricante Siemens
- 10.2 Búsqueda de dispositivos industriales del fabricante Simatic
- 10.3 Búsqueda de dispositivos industriales del fabricante Rockwell/Allen-Bradley

10



BÚSQUEDAS DESDE LA CLI: UTILIZACIÓN CONJUNTA DE LOS COMANDOS *COUNT*, *STATS* Y *SEARCH*

Ahora vas a realizar búsquedas empleando de forma conjunta los comandos ***count***, ***stats*** y ***search***. No obstante, antes de empezar es importante que sepas que, debido a que utilizas una cuenta gratuita de Shodan, el comando ***search*** tiene las siguientes limitaciones:

- No puedes utilizar filtros de tipo **campo:valor**, para reducir el número de resultados devueltos.
- El número máximo de resultados devueltos en una búsqueda está limitado a 100.

Por lo que, para superar estas limitaciones utilizarás, con los diferentes comandos, términos de búsqueda mucho más específicos de dispositivos de fabricantes de PLC. Asimismo, también te apoyarás en el comando ***stats*** para averiguar los diferentes puertos utilizados que devuelve el término de búsqueda.

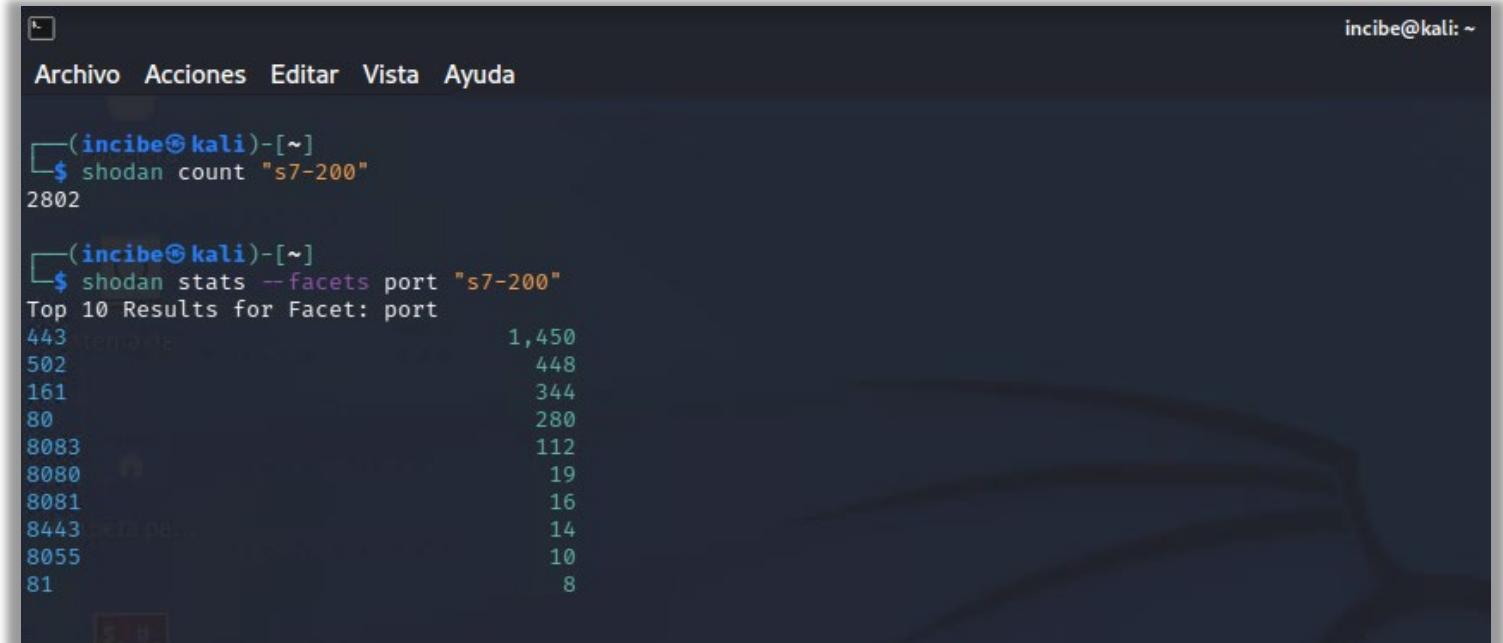
Por último, con el comando ***search*** mostrarás los resultados de búsqueda obtenidos.

Retomando el apartado donde realizas búsquedas con el comando ***count***, realizarás una serie de búsquedas agrupadas por fabricantes de dispositivos industriales de tipo PLC.

BÚSQUEDAS DESDE LA CLI: UTILIZACIÓN CONJUNTA DE LOS COMANDOS *COUNT*, *STATS* Y *SEARCH*

10.1 Búsqueda de dispositivos industriales del fabricante Siemens

- Realiza una primera búsqueda con el comando **count** para el dispositivo s7-200 y, después, para este mismo dispositivo utiliza el comando **stats** con el *facets port*:
 - shodan count “s7-200”**
 - shodan stats --facets port “s7-200”**



The terminal window shows the following session:

```
incibe@kali: ~
Archivo Acciones Editar Vista Ayuda
└(incibe@kali)-[~]
$ shodan count "s7-200"
2802

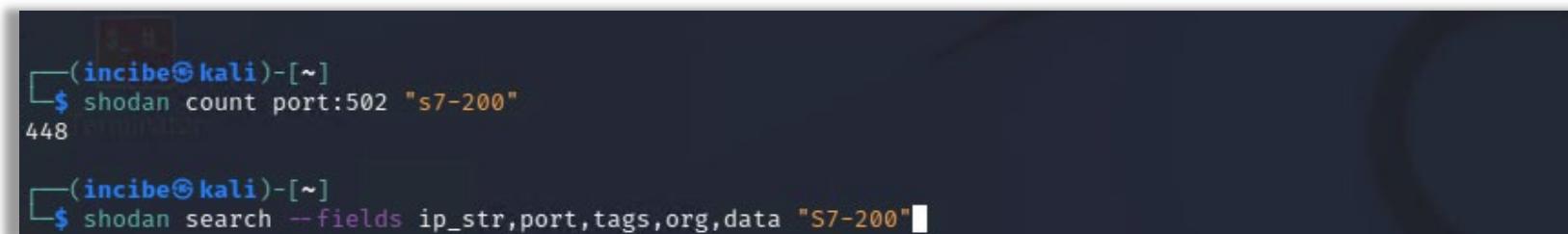
└(incibe@kali)-[~]
$ shodan stats --facets port "s7-200"
Top 10 Results for Facet: port
443              1,450
502              448
161              344
80               280
8083             112
8080             19
8081             16
8443             14
8055             10
81               8
```

Ilustración 67: Búsqueda con el comando *count* del término s7-200.

BÚSQUEDAS DESDE LA CLI: UTILIZACIÓN CONJUNTA DE LOS COMANDOS *COUNT*, *STATS* Y *SEARCH*

10.1 Búsqueda de dispositivos industriales del fabricante Siemens

- Añade a la búsqueda con el comando **count** el filtro «port:502», verás que aparece el mismo número de resultados que los obtenidos con el comando **stats** y la agrupación por puertos utilizando el **facets**, donde para el puerto 502, en número, en nuestro caso, es 448 resultados.



```
(incibe㉿kali)-[~]
└─$ shodan count port:502 "s7-200"
448

(incibe㉿kali)-[~]
└─$ shodan search --fields ip_str,port,tags,org,data "S7-200"
```

Ilustración 68: Búsqueda con el comando «shodan count port:502 “s7-200”».

BÚSQUEDAS DESDE LA CLI: UTILIZACIÓN CONJUNTA DE LOS COMANDOS COUNT, STATS Y SEARCH

10.1 Búsqueda de dispositivos industriales del fabricante Siemens

- Por último, realiza la búsqueda con el comando **search** indicando los campos que quieras que aparezcan en los resultados de búsqueda devueltos por Shodan. Estos campos serán dirección de IP, puerto, *tag* (etiquetas), organización y datos:
 - **shodan search --fields ip_str,port,tags,org,data "S7-200"**

El campo *tags* (etiquetas) muestra la categoría asignada por Shodan al dispositivo como, por ejemplo, la etiqueta «ics» que indica que Shodan ha identificado el dispositivo como industrial.

Nota: el término de búsqueda que has utilizado entrecomillado “S7-200” no es sensible a la utilización de mayúsculas o minúsculas.



BÚSQUEDAS DESDE LA CLI: UTILIZACIÓN CONJUNTA DE LOS COMANDOS COUNT, STATS Y SEARCH

10.1 Búsqueda de dispositivos industriales del fabricante Siemens

Ilustración 69: Primeros resultados de la búsqueda anterior.

BÚSQUEDAS DESDE LA CLI: UTILIZACIÓN CONJUNTA DE LOS COMANDOS COUNT, STATS Y SEARCH

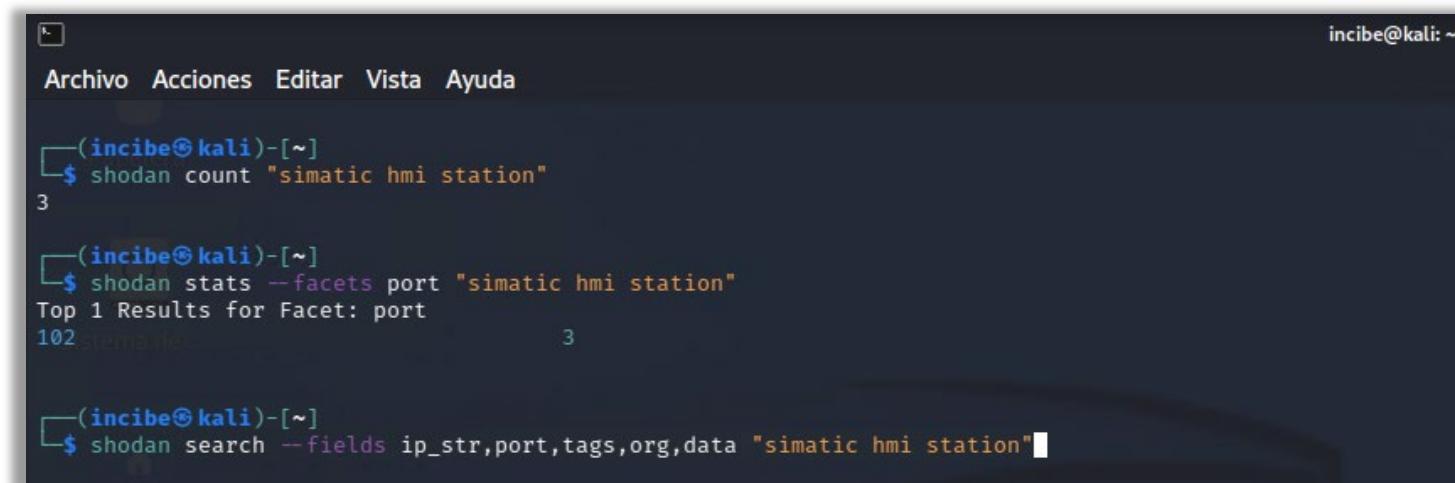
10.2 Búsqueda de dispositivos industriales del fabricante Simatic

- Con el primer comando **count**, realiza una búsqueda que contenga el nombre que identifica al dispositivo industrial, en este caso vamos a buscar un dispositivo HMI simatic escribiendo en nuestro comando **simatic hmi station**. Siempre es buena práctica ejecutar este comando porque, como hemos visto en Shodan, al usar la versión gratuita si son más de 100 resultados no se obtendrían todos ellos. En este caso, como veremos en la imagen de la siguiente diapositiva, aparecen 3. Pero recuerda, esta imagen es del momento en que se realizó este ejemplo, por lo que a ti te puede salir un resultado diferente.
- Con el segundo comando **stats**, identifica el puerto que es más probable que utilice este tipo de dispositivos industriales, en este caso, el puerto 102.
 - **shodan count “simatic hmi station”**
 - **shodan --facets port “simatic hmi station”**

BÚSQUEDAS DESDE LA CLI: UTILIZACIÓN CONJUNTA DE LOS COMANDOS COUNT, STATS Y SEARCH

10.2 Búsqueda de dispositivos industriales del fabricante Simatic

- Con estos comandos vas a poder visualizar que se han encontrados 3 dispositivos «simatic hmi station» y que los 3 se encuentran en el puerto 102.
- Por último, realiza la búsqueda con el comando **search** indicando los campos que quieras que aparezcan en los resultados de búsqueda devueltos por Shodan:
 - shodan search --fields ip_str,port,tags,org,data "simatic hmi station"**



```
incibe@kali: ~
Archivo Acciones Editar Vista Ayuda
└─(incibe㉿kali)-[~]
$ shodan count "simatic hmi station"
3

└─(incibe㉿kali)-[~]
$ shodan stats --facets port "simatic hmi station"
Top 1 Results for Facet: port
102

└─(incibe㉿kali)-[~]
$ shodan search --fields ip_str,port,tags,org,data "simatic hmi station"
```

Ilustración 70: Búsqueda realizada con los comandos *count* y *stats*.

BÚSQUEDAS DESDE LA CLI: UTILIZACIÓN CONJUNTA DE LOS COMANDOS COUNT, STATS Y SEARCH

10.2 Búsqueda de dispositivos industriales del fabricante Simatic

- Como puedes ver en la siguiente imagen, nos aparece la información que hemos buscado con el comando anterior (IP, puerto, etc.) de los 3 dispositivos HMI Siemens que hemos buscado. Esto no significa que Siemens únicamente haya fabricado 3 dispositivos de este tipo, si no que todos los que hay se encuentran en redes bien configuradas y protegidas y estos 3 son los únicos que se encuentran de forma pública en Internet.

```
62.141.26.135  102    ics    T-Mobile Czech Republic a.s.    Location designation of a module: \nCopyright: Original Siemens Equipment\nManufacturer and profile of a CPU module: *\nModule type: WinAC MP  
277\nPLC name: SIMATIC HMI Station\nModule: 6ES7 671-5EF01-0YA0 v.0.4\nPlant identification: \nModule name: WinAC MP 277\nSerial number of module: \nBasic Firmware: 6ES7 671-5EF01-0YA0 v.4.1.1\n85.163.71.12  102    ics    CETIN a.s.    Location designation of a module: \nCopyright: Original Siemens Equipment\nManufacturer and profile of a CPU module: *\nModule type: WinAC MP 277\nPLC name:  
SIMATIC HMI Station\nModule: 6ES7 671-5EF01-0YA0 v.0.4\nPlant identification: \nModule name: WinAC MP 277\nSerial number of module: \nBasic Firmware: 6ES7 671-5EF01-0YA0 v.4.1.1\n62.141.22.38  102    ics    T-Mobile Czech Republic a.s.    Location designation of a module: \nCopyright: Original Siemens Equipment\nManufacturer and profile of a CPU module: *\nModule type: WinAC MP  
277\nPLC name: SIMATIC HMI Station\nModule: 6ES7 671-5EF01-0YA0 v.0.4\nPlant identification: \nModule name: WinAC MP 277\nSerial number of module: \nBasic Firmware: 6ES7 671-5EF01-0YA0 v.4.1.1\n  
(END)
```

Ilustración 71: Búsqueda con el comando search indicando los campos que se quieren obtener.

BÚSQUEDAS DESDE LA CLI: UTILIZACIÓN CONJUNTA DE LOS COMANDOS *COUNT*, *STATS* Y *SEARCH*

10.3 Búsqueda de dispositivos industriales del fabricante Rockwell/Allen-Bradley

- Con este ejercicio vamos a realizar una búsqueda de dispositivos industriales del fabricante Rockwell / Allen-Bradley.
- Intenta realizar la búsqueda por ti mismo con los comandos que has aprendido teniendo en cuenta lo siguiente:
 - Busca por «**Rockwell Automation / Allen-Bradley**».
- Despues de descubrir el o los puertos y el número de dispositivos, comprueba realizando un **count** si en el puerto 44818 se encuentran el mismo número de dispositivos que aparece con la búsqueda **stats**.

BÚSQUEDAS DESDE LA CLI: UTILIZACIÓN CONJUNTA DE LOS COMANDOS *COUNT*, *STATS* Y *SEARCH*

10.3 Búsqueda de dispositivos industriales del fabricante Rockwell/Allen-Bradley

- Con el tercer comando **count** añade el filtro del puerto 44818 y confirma que el número de resultados devueltos coincide con el *top 10* de resultados devueltos por el comando **stats** con el *facets port*.
 - **shodan count “Rockwell Automation/Allen-Bradley”**
 - **shodan stats --facets port “Rockwell Automation/Allen-Bradley”**
 - **shodan count port:44818 “Rockwell Automation/Allen-Bradley”**

BÚSQUEDAS DESDE LA CLI: UTILIZACIÓN CONJUNTA DE LOS COMANDOS *COUNT*, *STATS* Y *SEARCH*

10.3 Búsqueda de dispositivos industriales del fabricante Rockwell/Allen-Bradley

The screenshot shows a terminal window with the following command history:

```
incibe@kali:~$ shodan count "Rockwell Automation/Allen-Bradley"
6513

incibe@kali:~$ shodan stats --facets port "Rockwell Automation/Allen-Bradley"
Top 10 Results for Facet: port
44818          6,484
2222           5
502            3
2016            3
2003            2
2013            2
2018            2
2000            1
2001            1
2004            1

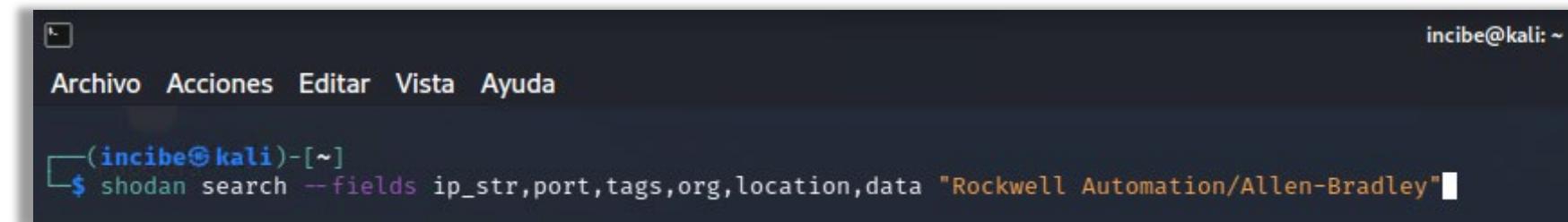
incibe@kali:~$ shodan count port:44818 "Rockwell Automation/Allen-Bradley"
6484
```

Ilustración 72: Búsqueda con los comandos *count*, *stats* y *search*.

BÚSQUEDAS DESDE LA CLI: UTILIZACIÓN CONJUNTA DE LOS COMANDOS COUNT, STATS Y SEARCH

10.2 Búsqueda de dispositivos industriales del fabricante Simatic

- Por último, realiza la búsqueda con el comando **search** indicando los campos que quieras que aparezcan en los resultados de búsqueda devueltos por Shodan:
 - **shodan search --fields ip_str,port,tags,org,data «Rockwell Automation/Allen-Bradley»**

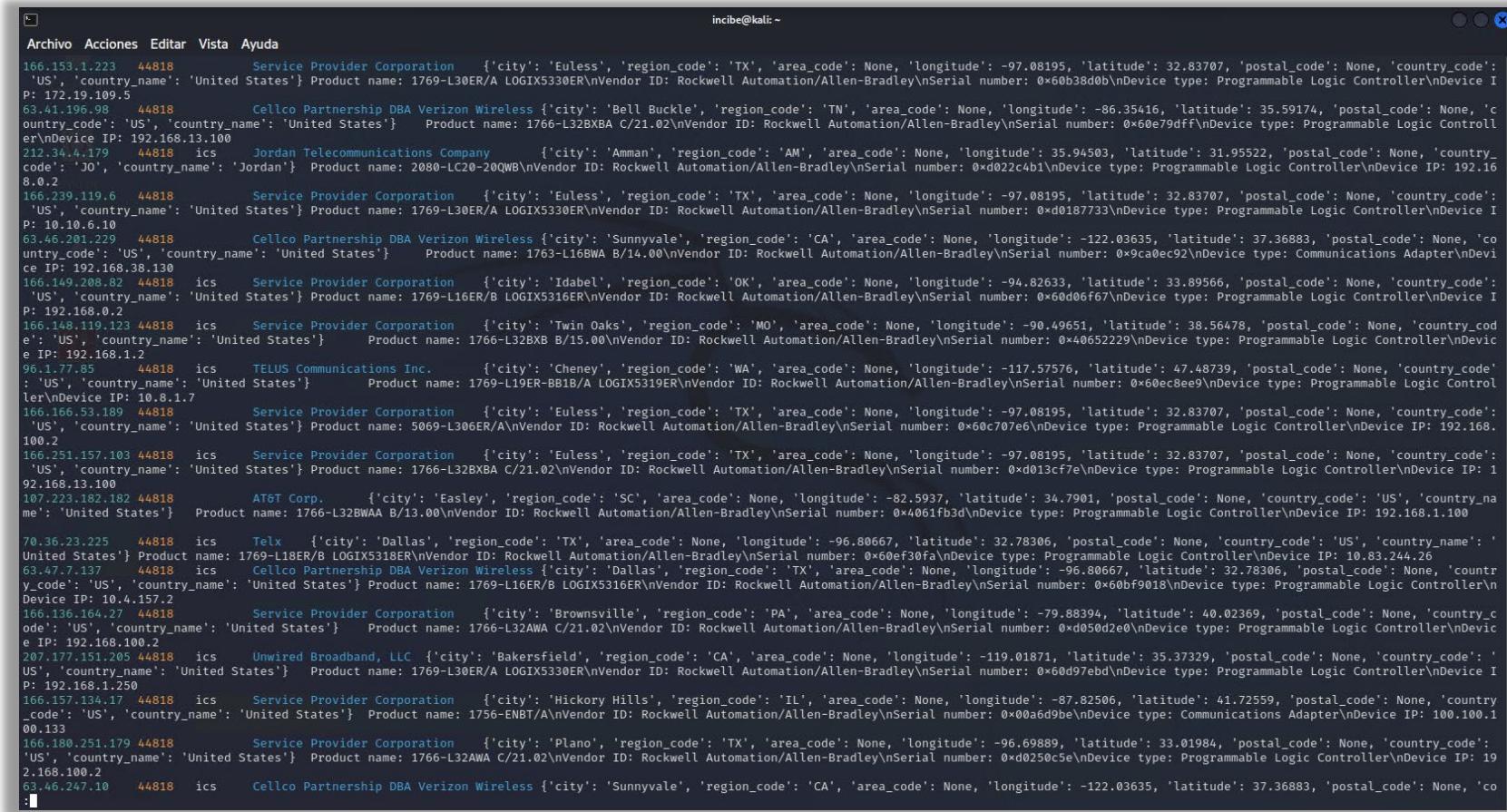


A screenshot of a terminal window titled 'Archivo Acciones Editar Vista Ayuda'. The window shows a command-line interface with the prompt '(incibe@kali)-[~]'. A user has typed the command '\$ shodan search --fields ip_str,port,tags,org,location,data "Rockwell Automation/Allen-Bradley"' into the terminal. The terminal is running on a Kali Linux system, as indicated by the desktop environment and the user's name.

Ilustración 73: Búsqueda con el comando *search*.

BÚSQUEDAS DESDE LA CLI: UTILIZACIÓN CONJUNTA DE LOS COMANDOS COUNT, STATS Y SEARCH

10.3 Búsqueda de dispositivos industriales del fabricante Rockwell/Allen-Bradley



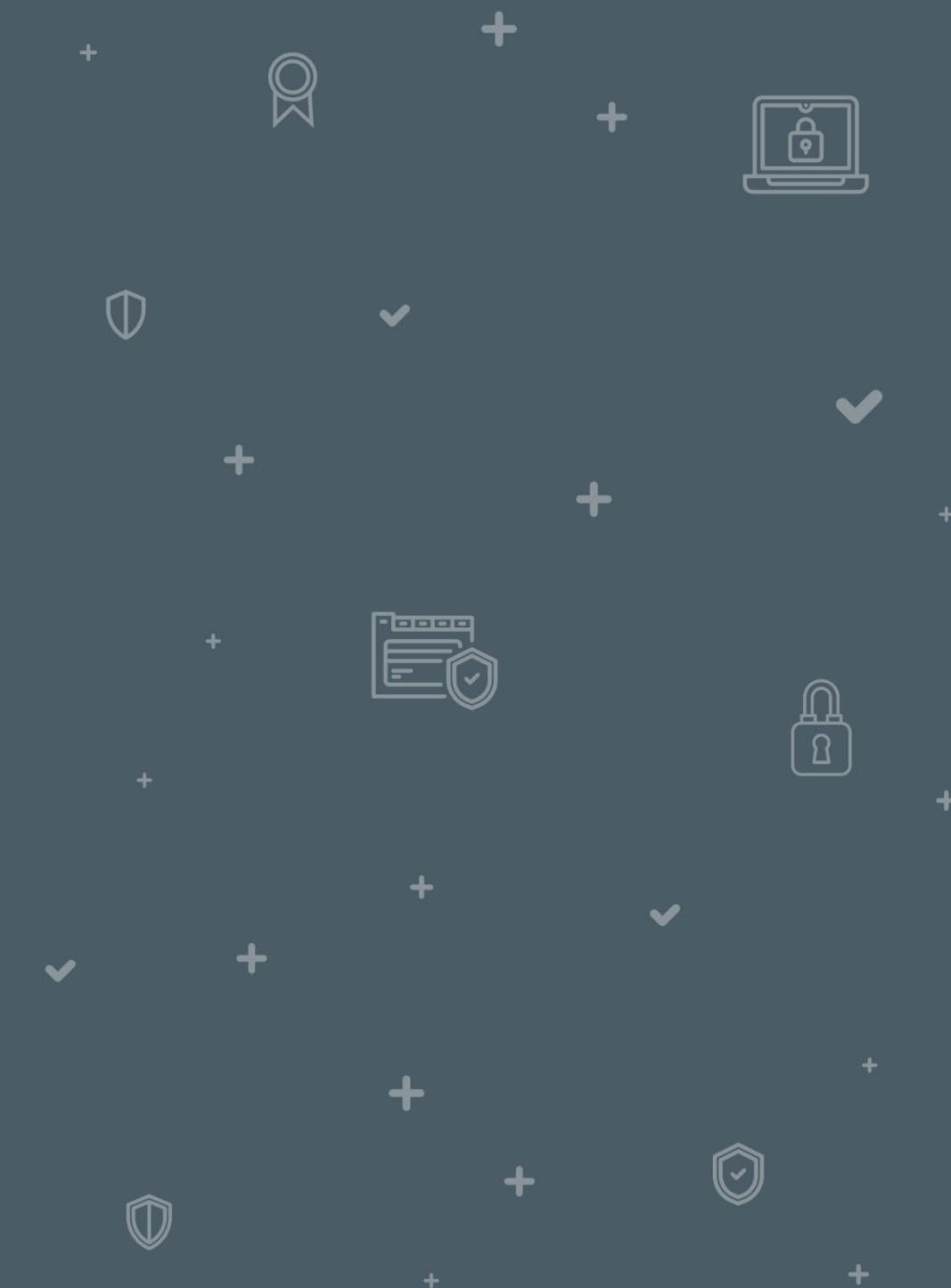
```

incibe@kali: ~
Archivo Acciones Editar Vista Ayuda
166.153.1.223 44818 Service Provider Corporation {'city': 'Euless', 'region_code': 'TX', 'area_code': None, 'longitude': -97.08195, 'latitude': 32.83707, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'} Product name: 1769-L30ER/A LOGIX5330ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60b38d0b\nDevice type: Programmable Logic Controller\nDevice IP: 172.19.109.5
63.41.196.98 44818 Cellco Partnership DBA Verizon Wireless {'city': 'Bell Buckle', 'region_code': 'None', 'area_code': None, 'longitude': -86.35416, 'latitude': 35.59174, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'} Product name: 1766-L32BXBA C/21.02\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60e79dff\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.13.100
212.34.4.179 44818 ics Jordan Telecommunications Company {'city': 'Amman', 'region_code': 'AM', 'area_code': None, 'longitude': 35.94503, 'latitude': 31.95522, 'postal_code': None, 'country_code': 'JO', 'country_name': 'Jordan'} Product name: 2080-LC20-20QWB\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0xd02c4b1\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.0.2
166.239.119.6 44818 Service Provider Corporation {'city': 'Euless', 'region_code': 'TX', 'area_code': None, 'longitude': -97.08195, 'latitude': 32.83707, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'} Product name: 1769-L30ER/A LOGIX5330ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x0187733\nDevice type: Programmable Logic Controller\nDevice IP: 10.10.6.10
63.46.201.229 44818 Cellco Partnership DBA Verizon Wireless {'city': 'Sunnyvale', 'region_code': 'CA', 'area_code': None, 'longitude': -122.03635, 'latitude': 37.36883, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'} Product name: 1763-L16BWA B/14.00\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x9ca0ec92\nDevice type: Communications Adapter\nDevice IP: 192.168.38.130
166.149.208.82 44818 ics Service Provider Corporation {'city': 'Idabel', 'region_code': 'OK', 'area_code': None, 'longitude': -98.82633, 'latitude': 33.89566, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'} Product name: 1769-L16ER/B LOGIX5316ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60d06f67\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.0.2
166.148.119.123 44818 ics Service Provider Corporation {'city': 'Twin Oaks', 'region_code': 'MO', 'area_code': None, 'longitude': -90.49651, 'latitude': 38.56478, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'} Product name: 1766-L32BXB B/15.00\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x4065229\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.1.2
96.1.77.85 44818 ics TELUS Communications Inc. {'city': 'Cheney', 'region_code': 'WA', 'area_code': None, 'longitude': -117.57576, 'latitude': 47.48739, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'} Product name: 1769-L19ER-BB1B/A LOGIX5319ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60ec8ee9\nDevice type: Programmable Logic Controller\nDevice IP: 10.8.1.7
166.166.53.189 44818 Service Provider Corporation {'city': 'Euless', 'region_code': 'TX', 'area_code': None, 'longitude': -97.08195, 'latitude': 32.83707, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'} Product name: 5069-L30ER/A\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60c707e6\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.100.2
166.251.157.103 44818 ics Service Provider Corporation {'city': 'Euless', 'region_code': 'TX', 'area_code': None, 'longitude': -97.08195, 'latitude': 32.83707, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'} Product name: 1766-L32BXBA C/21.02\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0xd013cf7e\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.13.100
107.223.182.182 44818 AT&T Corp. {'city': 'Easley', 'region_code': 'SC', 'area_code': None, 'longitude': -82.5937, 'latitude': 34.7901, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'} Product name: 1766-L32BWA B/13.00\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x4061fb3d\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.1.100
70.36.23.225 44818 ics Telx {'city': 'Dallas', 'region_code': 'TX', 'area_code': None, 'longitude': -96.80667, 'latitude': 32.78306, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'} Product name: 1769-L18ER/B LOGIX5318ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60ef30fa\nDevice type: Programmable Logic Controller\nDevice IP: 10.83.244.26
63.47.7.137 44818 ics Cellco Partnership DBA Verizon Wireless {'city': 'Dallas', 'region_code': 'TX', 'area_code': None, 'longitude': -96.80667, 'latitude': 32.78306, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'} Product name: 1769-L16ER/B LOGIX5316ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60bf9018\nDevice type: Programmable Logic Controller\nDevice IP: 10.4.157.2
166.136.164.27 44818 Service Provider Corporation {'city': 'Brownsville', 'region_code': 'PA', 'area_code': None, 'longitude': -79.88394, 'latitude': 40.02369, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'} Product name: 1766-L32AWA C/21.02\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0xd050d2e0\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.100.2
207.177.151.205 44818 ics Unwired Broadband, LLC {'city': 'Bakersfield', 'region_code': 'CA', 'area_code': None, 'longitude': -119.01871, 'latitude': 35.37329, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'} Product name: 1769-L30ER/A LOGIX5330ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60d97ebd\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.1.250
166.157.134.17 44818 ics Service Provider Corporation {'city': 'Hickory Hills', 'region_code': 'IL', 'area_code': None, 'longitude': -87.82506, 'latitude': 41.72559, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'} Product name: 1756-EBT/A\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x00ad6d9be\nDevice type: Communications Adapter\nDevice IP: 100.100.1.00.133
166.180.251.179 44818 Service Provider Corporation {'city': 'Plano', 'region_code': 'TX', 'area_code': None, 'longitude': -96.69889, 'latitude': 33.01984, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'} Product name: 1766-L32AWA C/21.02\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0xd0250c5e\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.100.2
63.46.247.10 44818 ics Cellco Partnership DBA Verizon Wireless {'city': 'Sunnyvale', 'region_code': 'CA', 'area_code': None, 'longitude': -122.03635, 'latitude': 37.36883, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'} Product name: 1769-L16BWA B/14.00\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x9ca0ec92\nDevice type: Communications Adapter\nDevice IP: 192.168.1.2
:
```

Ilustración 74: Resultados de la búsqueda del paso anterior.

BÚSQUEDAS DESDE LA CLI: COMANDO *DOWNLOAD*

11



Ahora, vas a descargar los resultados de las búsquedas que realices, esto se hace con el comando *download* de Shodan. Cada vez que se invoca este comando se guarda el resultado de la búsqueda en un archivo comprimido del tipo json.gz.

La descarga de resultados está limitada a un máximo de 100. Cuando el resultado de una búsqueda excede de 100 resultados, solo descarga los 100 primeros. Aunque esto es lo habitual, a veces sucede que la descarga se limita a 99 resultados o menos.

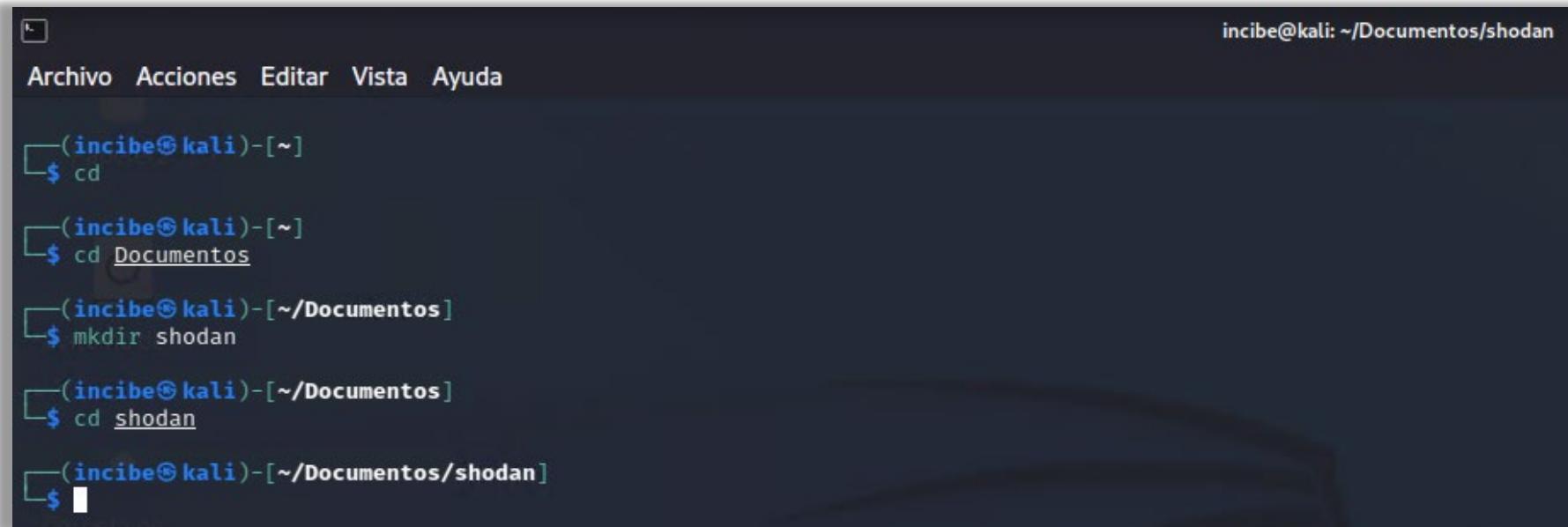
- En total descargarás 6 archivos para realizar esta práctica que veremos más adelante.

Para almacenar los archivos descargados, tienes que crear una carpeta. Para ello:

- Primero accede al directorio de usuario «incibe»
- Despues accede al directorio «Documentos»
- Ahí crea la carpeta «shodan»
- Accede a esta nueva carpeta.

Los comandos ejecutados son:

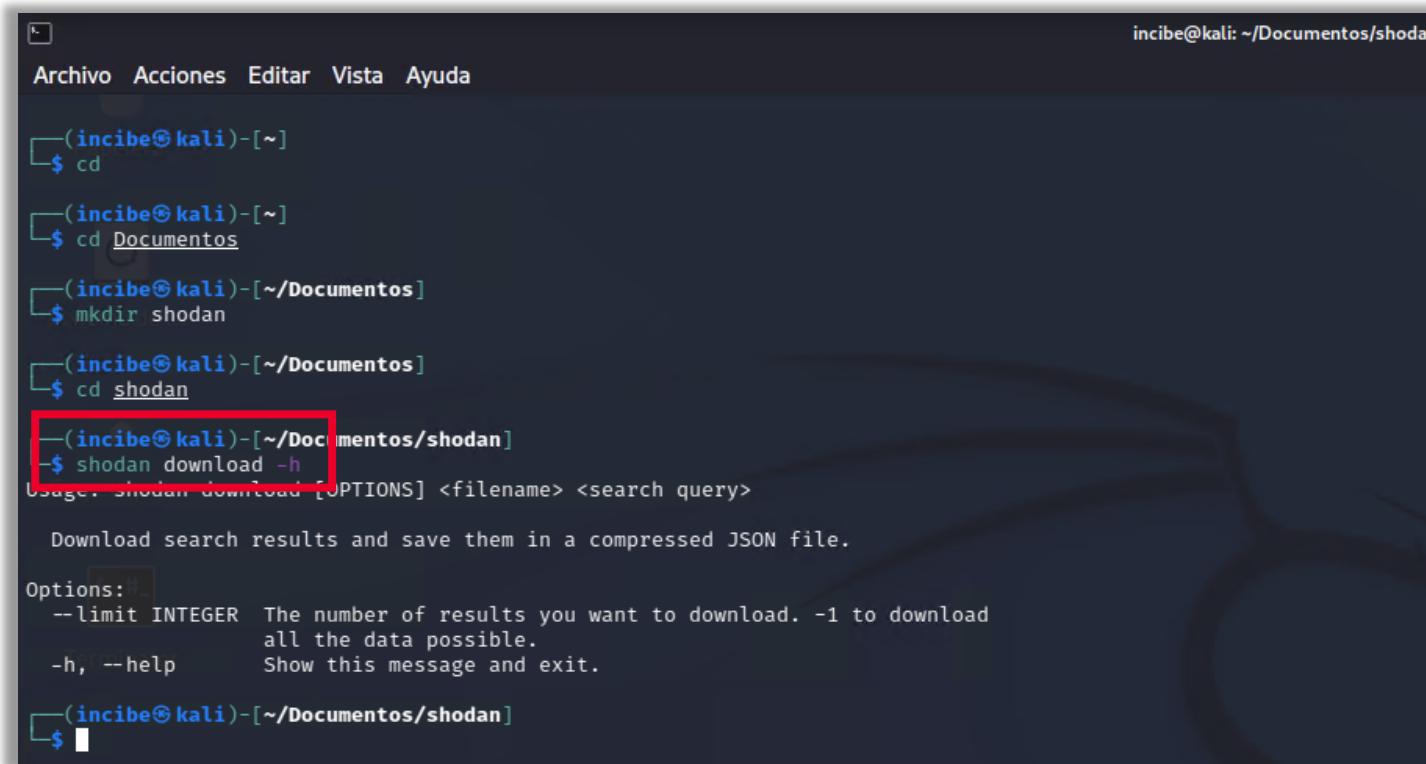
- **cd**
- **cd Documentos**
- **mkdir shodan**
- **cd shodan**



```
incibe@kali: ~/Documentos/shodan
Archivo  Acciones  Editar  Vista  Ayuda
└──(incibe㉿kali)-[~]
    $ cd
    └──(incibe㉿kali)-[~]
        $ cd Documentos
        └──(incibe㉿kali)-[~/Documentos]
            $ mkdir shodan
            └──(incibe㉿kali)-[~/Documentos]
                $ cd shodan
                └──(incibe㉿kali)-[~/Documentos/shodan]
                    $
```

Ilustración 75: Proceso de creación de la carpeta «shodan» en el directorio «Documentos» del usuario «incibe».

- Una vez has accedido a la carpeta shodan, muestra la ayuda del comando **download** de shodan como sigue:
 - shodan download -h**



```
incibe@kali: ~/Documentos/shodan
Archivo  Acciones  Editar  Vista  Ayuda
└─(incibe㉿kali)-[~]
    └─$ cd
      └─(incibe㉿kali)-[~]
          └─$ cd Documentos
            └─(incibe㉿kali)-[~/Documentos]
                └─$ mkdir shodan
                  └─(incibe㉿kali)-[~/Documentos]
                      └─$ cd shodan
                        └─(incibe㉿kali)-[~/Documentos/shodan]
                            └─$ shodan download -h
Usage: shodan download [OPTIONS] <filename> <search query>
Download search results and save them in a compressed JSON file.

Options:
  --limit INTEGER  The number of results you want to download. -1 to download
                   all the data possible.
  -h, --help       Show this message and exit.

└─(incibe㉿kali)-[~/Documentos/shodan]
    └─$
```

Ilustración 76: Ayuda del comando «shodan».

- En la primera descarga, vas a descargar todos los resultados de búsqueda devueltos (en este caso 69):
 - **shodan download resultados-TM251MESE_2.json.gz TM251MESE**
 - Este comando quiere decir que vamos a descargar los resultados de los dispositivos «TM251MESE_2», y los vamos a guardar en el archivo «resultados-TM251MESE_2.json.gz», donde «.gz» es una extensión de archivos comprimidos en zip específico de GNU, que es un sistema operativo de tipo Unix.
- Como puedes observar en la imagen de la siguiente diapositiva, hay 69 resultados, pero únicamente se han guardado 67. No te preocupes si esto también te ocurre a ti, puede ser que no se hayan podido guardar bien y por eso aparezca un número menor.

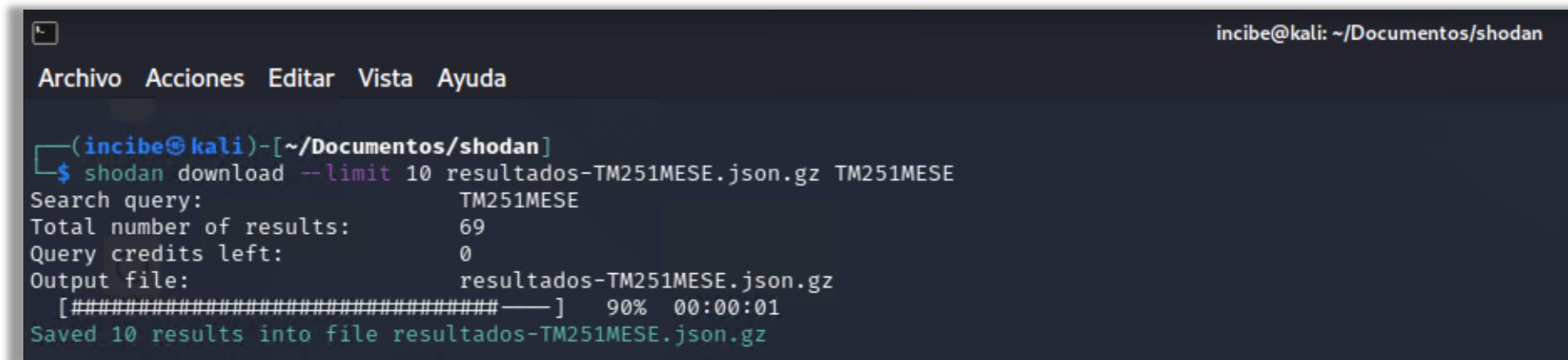
- Cuando el número de resultados es mayor a 100, ten en cuenta que únicamente se guardarán los 100 primeros resultados, pero como ya hemos mencionado, no te preocupes si te aparece que se han guardado menos.



```
(incibe㉿kali)-[~/Documentos/shodan]
$ shodan download resultados-TM251MESE_2.json.gz TM251MESE
Search query: TM251MESE
Total number of results: 69
Query credits left: 0
Output file: resultados-TM251MESE_2.json.gz
[#####--] 97% 00:00:04
Notice: fewer results were saved than requested
Saved 67 results into file resultados-TM251MESE_2.json.gz
```

Ilustración 77: Segunda descarga, sin limitación de resultados.

- Realiza la segunda descarga, limitando la cantidad de resultados descargados a 10 para el término de búsqueda «TM251MESE», que consiste en un modelo de dispositivo PLC Schneider, con el siguiente comando:
 - shodan download --limit 10 resultados-TM251MESE.json.gz TM251MESE**



```
incibe@kali: ~/Documentos/shodan
Archivo  Acciones  Editar  Vista  Ayuda

└─(incibe㉿kali)-[~/Documentos/shodan]
$ shodan download --limit 10 resultados-TM251MESE.json.gz TM251MESE
Search query:          TM251MESE
Total number of results: 69
Query credits left:    0
Output file:           resultados-TM251MESE.json.gz
[#####-----] 90% 00:00:01
Saved 10 results into file resultados-TM251MESE.json.gz
```

Ilustración 78: Descarga para el término de búsqueda «TM251MESE» limitada a diez resultados.

- Ahora realizaremos una nueva descarga, la tercera descarga, pero, en este caso, buscaremos por simatic:
 - **shodan download resultados-simatic.json.gz simatic**



```
(incibe㉿kali)-[~/Documentos/shodan]$ shodan download resultados-simatic.json.gz simatic
Search query: simatic
Total number of results: 3112
Query credits left: 0
Output file: resultados-simatic.json.gz
[###-----] 9% 00:23:18
Notice: fewer results were saved than requested
Saved 99 results into file resultados-simatic.json.gz
```

Ilustración 79: Descarga bajo el término de búsqueda «simatic».

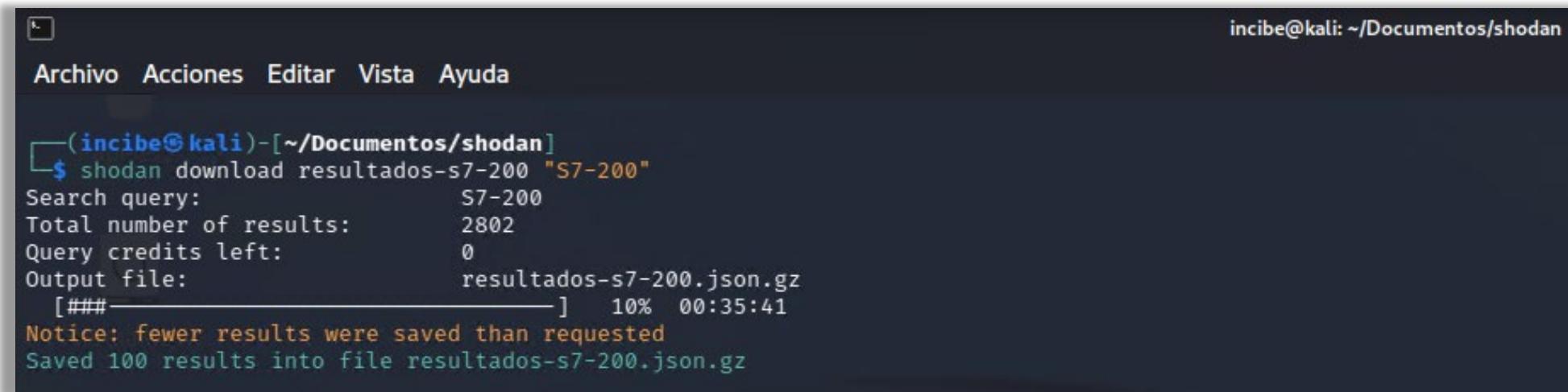
- Como puedes observar, de 3112 resultados que ha devuelto la búsqueda, ha descargado 99 en este caso.
- Puedes ver los archivos que se van generando con el comando **ls**. Si le añades el parámetro **-l** verás cada archivo en una fila.
 - **ls -l**

```
(incibe㉿kali)-[~/Documentos/shodan]
└─$ ls -l
total 36
-rw-r--r-- 1 incibe incibe 19643 abr 25 13:24 resultados-simatic.json.gz
-rw-r--r-- 1 incibe incibe  9699 abr 25 13:23 resultados-TM251MESE_2.json.gz
-rw-r--r-- 1 incibe incibe  1995 abr 25 13:22 resultados-TM251MESE.json.gz

(incibe㉿kali)-[~/Documentos/shodan]
└─$ █
```

Ilustración 80: Vista de los distintos archivos, que se generan con el comando **ls -l**, en filas.

- Genera una nueva descarga, esta vez para los dispositivos «S7-200».
 - **shodan download resultados-s7-200 "S7-200"**



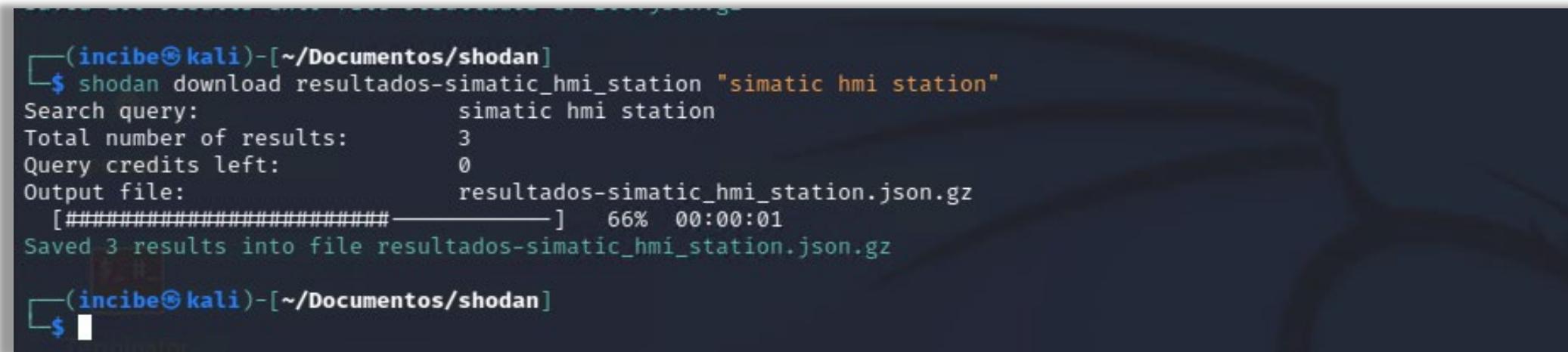
A terminal window titled 'incibe@kali: ~/Documentos/shodan' showing the output of the 'shodan download' command. The command is: \$ shodan download resultados-s7-200 "S7-200". The output includes search query (S7-200), total number of results (2802), query credits left (0), and the output file (resultados-s7-200.json.gz). A progress bar indicates 10% completion at 00:35:41. A notice states fewer results were saved than requested, and it shows 100 results saved into the file.

```
(incibe㉿kali)-[~/Documentos/shodan]
$ shodan download resultados-s7-200 "S7-200"
Search query: S7-200
Total number of results: 2802
Query credits left: 0
Output file: resultados-s7-200.json.gz
[###-----] 10% 00:35:41
Notice: fewer results were saved than requested
Saved 100 results into file resultados-s7-200.json.gz
```

Ilustración 81: Descarga para el término «S7-200».

Como puedes ver, aunque Shodan tiene identificados 2802 dispositivos de este tipo, en el archivo descargado ha almacenado únicamente 100.

- Descarga un nuevo archivo, el quinto, para los dispositivos «simatic hmi station».
 - **shodan download resultados-simatic_hmi_station "simatic hmi station"**



```
(incibe㉿kali)-[~/Documentos/shodan]$ shodan download resultados-simatic_hmi_station "simatic hmi station"
Search query: simatic hmi station
Total number of results: 3
Query credits left: 0
Output file: resultados-simatic_hmi_station.json.gz
[#####-----] 66% 00:00:01
Saved 3 results into file resultados-simatic_hmi_station.json.gz

(incibe㉿kali)-[~/Documentos/shodan]$
```

Ilustración 82: Descarga para el término «simatic hmi station».

- Para la última descarga, utiliza el término «Rockwell Automation/Allen-Bradley».
 - shodan download resultados-rockwell "Rockwell Automation/Allen-Bradley"**

```
(incibe㉿kali)-[~/Documentos/shodan]$ shodan download resultados-rockwell "Rockwell Automation/Allen-Bradley"

Search query: Rockwell Automation/Allen-Bradley
Total number of results: 6513
Query credits left: 0
Output file: resultados-rockwell.json.gz
[###-----] 9% 00:33:50
Notice: fewer results were saved than requested
Saved 99 results into file resultados-rockwell.json.gz

(incibe㉿kali)-[~/Documentos/shodan]$
```

Ilustración 83: Captura de la sexta descarga. En esta ocasión se hace para el término «Rockwell Automation/Allen-Bradley».

Nota: como has comprobado, si no especificamos la extensión del archivo «json.gz» descargado, Shodan la añade automáticamente.

Si ahora listamos los archivos que se encuentra en «Documentos/shodan», donde hemos almacenado todas las descargas, aparecen 6 archivos. Los generados con nuestras consultas. Para verlos escribe:

- **ls -l**

```
(incibe㉿kali)-[~/Documentos/shodan]
└─$ ls -l
total 596
-rw-r--r-- 1 incibe incibe 23371 abr 25 13:34 resultados-rockwell.json.gz
-rw-r--r-- 1 incibe incibe 543352 abr 25 13:31 resultados-s7-200.json.gz
-rw-r--r-- 1 incibe incibe 1225 abr 25 13:32 resultados-simatic_hmi_station.json.gz
-rw-r--r-- 1 incibe incibe 19643 abr 25 13:24 resultados-simatic.json.gz
-rw-r--r-- 1 incibe incibe 9699 abr 25 13:23 resultados-TM251MESE_2.json.gz
-rw-r--r-- 1 incibe incibe 1995 abr 25 13:22 resultados-TM251MESE.json.gz

(incibe㉿kali)-[~/Documentos/shodan]
└─$ █
```

Ilustración 84: Resultados de la búsqueda.

12

BÚSQUEDAS
DESDE LA CLI:
COMANDO *PARSE*

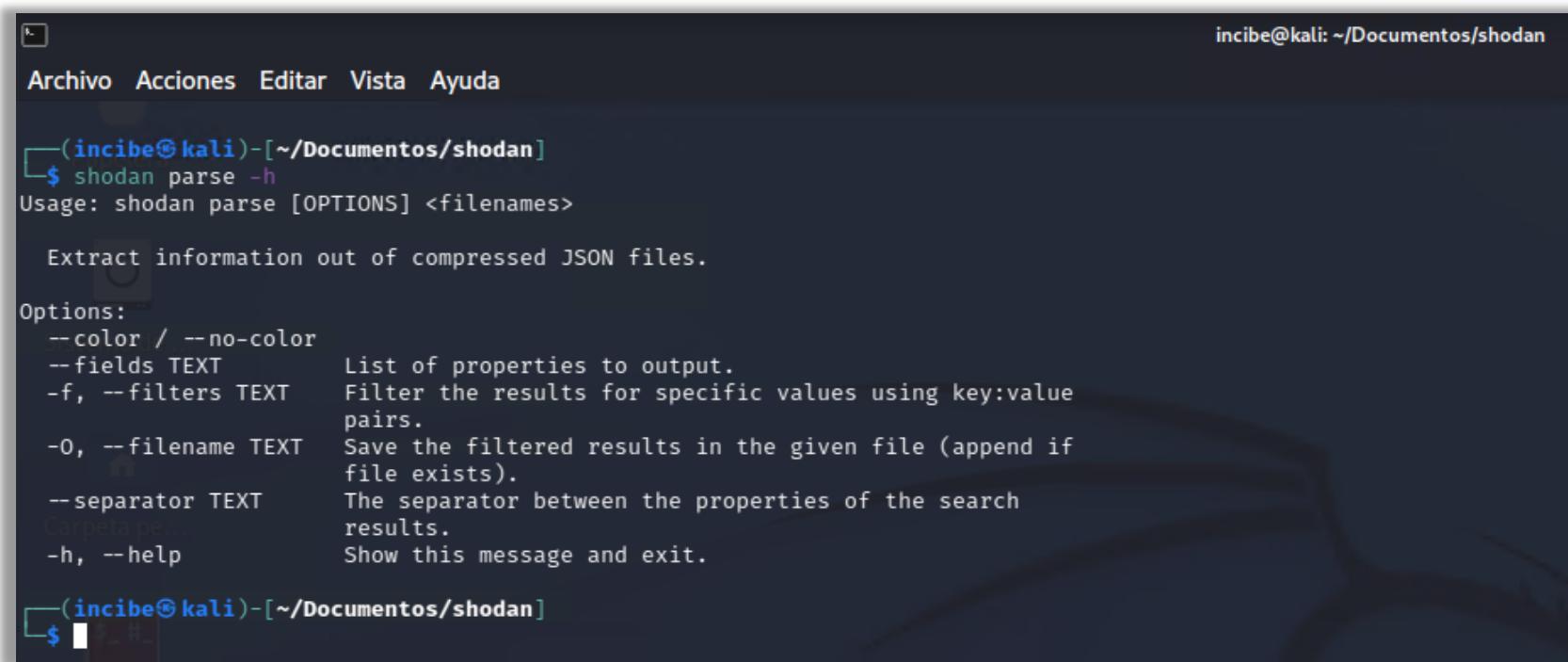
Estos archivos que hemos descargado almacenan toda la información disponible de los dispositivos que hemos buscado. Si recuerdas, antes hemos realizado búsquedas con el comando **search** y hemos buscado diferentes campos (como la IP, el puerto, etc.). Lo que hemos hecho, ha sido descargar toda la información en un archivo y ahora vamos a poder realizar otras acciones de búsqueda o filtrado de la información.

Ahora, vamos a utilizar el comando **Shodan parse**, que va a permitir extraer toda la información de los archivos descargados, indicando las propiedades o campos que quieras que muestre. Shodan también permite la utilización de filtros, para afinar más la búsqueda.

Nota: los campos o *properties* que puedes visualizar con este comando **parse** son los mismos que los indicados para el comando **search**.

- Ejecuta la ayuda del comando **parse**:
 - **shodan parse -h.**
 - Con la opción «**--fields**», indicas a Shodan los campos que quieras que muestre (separados por comas).
 - Con la opción «**-f**», indicas a Shodan que estas utilizando un filtro y especifica el tipo de filtro.
 - Con la opción «**--separator**», indicas a Shodan el texto que quieras utilizar para separar los campos.

- En cada ejecución del comando **parse**, irás especificando el archivo comprimido que corresponda, según los resultados de la búsqueda que quieras mostrar.



A terminal window titled 'Archivos' with the command 'shodan parse -h' entered. The output shows the usage of the command, its purpose (extracting information from compressed JSON files), and a detailed list of options:

```
(incibe㉿kali)-[~/Documentos/shodan]
$ shodan parse -h
Usage: shodan parse [OPTIONS] <filenames>

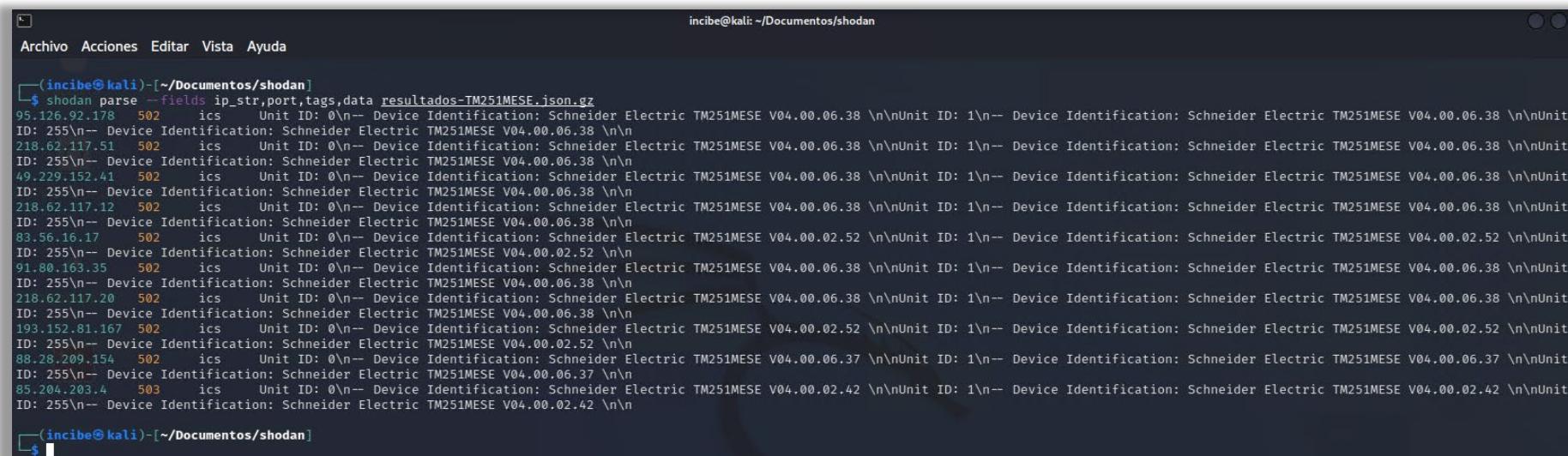
    Extract information out of compressed JSON files.

Options:
  --color / --no-color
  --fields TEXT      List of properties to output.
  -f, --filters TEXT Filter the results for specific values using key:value
                      pairs.
  -o, --filename TEXT Save the filtered results in the given file (append if
                      file exists).
  --separator TEXT   The separator between the properties of the search
                     results.
  -h, --help          Show this message and exit.

(incibe㉿kali)-[~/Documentos/shodan]
```

Ilustración 85: Ejecución de la ayuda del comando *parse*.

- Ahora realiza una extracción de la información del archivo «**resultados-TM251MESE.json.gz**».
 - Indica que quieres mostrar los campos *ip_str* (dirección IP), *port* (puerto), *tags* (etiqueta, como por ejemplo la que indica si un dispositivo es *ics*), *data* (muestra información asociada al tipo de dispositivo, protocolo o puerto, que ha detectado Shodan).
 - **shodan parse --fields ip_str,port,tags,data resultados-TM251MESE.json.gz**



The terminal window shows the command \$ shodan parse --fields ip_str,port,tags,data resultados-TM251MESE.json.gz being run. The output lists multiple entries, each representing a device found by Shodan. Each entry includes the IP address (e.g., 95.126.92.178), port (e.g., 502), tags (e.g., ics), and data (Device Identification: Schneider Electric TM251MESE V04.00.06.38). The data field contains detailed information about the device's model and version.

```
(incibe㉿kali)-[~/Documentos/shodan]$ shodan parse --fields ip_str,port,tags,data resultados-TM251MESE.json.gz
95.126.92.178 502 ics Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 218.62.117.51 502 ics Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 49.229.152.41 502 ics Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 218.62.117.12 502 ics Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 83.56.16.17 502 ics Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\nUnit ID: 91.80.163.35 502 ics Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 218.62.117.20 502 ics Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 193.152.81.167 502 ics Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\nUnit ID: 88.28.209.154 502 ics Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.37 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.37 \n\nUnit ID: 85.204.203.4 503 ics Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.42 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.42 \n\nUnit
```

Ilustración 86:
Extracción de
la información
del archivo
«**resultados-
TM251MESE.j
son.gz**».

BÚSQUEDAS DESDE LA CLI: COMANDO *PARSE*

A continuación, realiza una extracción de la misma información del archivo «**resultados-TM251MESE_2.json.gz**».

- Ejecuta el siguiente comando, indicando los campos que quieras mostrar:

- shodan parse --fields ip_str, port, tags, data resultados- TM251MESE_2.json.g

Ilustración 87: Extracción de resultados del archivo «resultados-TM251MESE_2.json.gz» con el comando «shodan parse --fields ip_str,port,tags,data resultados-TM251MESE_2.json.gz».



BÚSQUEDAS DESDE LA CLI: COMANDO PARSE

- Filtra en este caso para que solo muestre los resultados de búsqueda con el puerto 502.

```
incibe@kali: ~/Documentos/shodan
$ shodan parse --fields ip, str, port, tags, domains, data resultados-TM251MESE_2.json.gz
.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n
120.157.121.136 502 ics          Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.21 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.21 \n\n
193.248.231.219 502 ics  wanadoo.fr  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.05.11 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.05.11 \n\n
85.232.130.190 502 ics  telelanas.lt  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n
213.96.26.163 502 ics  rima-tde.net  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V05.00.08.04 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V05.00.08.04 \n\n
83.224.129.112 502 ics          Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V05.00.08.04 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V05.00.08.04 \n\n
185.205.255.150 44818 ics          Product name: TM251MESE\nVendor ID: Schneider Automation:Inc.\nSerial number: 0x00007e46\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.1.20
46.56.142.237 502 ics          Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.41 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.41 \n\n
218.62.116.254 502 ics  jlcpcptt.net.cn  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n
46.56.141.35 502 ics          Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.37 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.37 \n\n
218.62.117.19 502 ics  jlcpcptt.net.cn  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n
5.154.1.3 502 ics          Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.14 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.14 \n\n
109.167.48.60 502 ics          Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\n
2.118.194.22 502 ics  telecomitalia.it  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.21 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.21 \n\n
18.62.117.11 502 ics  jlcpcptt.net.cn  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n
.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n
91.80.148.172 502 ics          Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V05.00.08.04 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V05.00.08.04 \n\n
88.28.209.155 502 ics  rima-tde.net  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n
.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.14 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.14 \n\n
83.56.16.17 503 ics          Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\n
.02.52 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\n
88.28.203.30 502 ics  rima-tde.net  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\n
.02.52 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\n
207.255.184.108 502 ics  atlanticbb.net  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.14 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.14 \n\n
218.62.117.13 502 ics  jlcpcptt.net.cn  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n
.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n
91.80.154.153 502 ics          Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.41 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.41 \n\n
218.62.117.154 502 ics  jlcpcptt.net.cn  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n
.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n
109.166.175.2 502 ics  orangero.net  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.11 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.11 \n\n
.02.11 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.11 \n\n
218.62.117.52 502 ics  jlcpcptt.net.cn  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n
.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n
91.80.146.77 502 ics          Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\n
```

Ilustración 88: Inicio del listado de resultados para el puerto 502.

BÚSQUEDAS DESDE LA CLI: COMANDO PARSE

- shodan parse -f port:502 --

fields ip_str, port, tags, data

resultados-

TM251MESE_2.json.gz

```

Archivo  Acciones  Editar  Vista  Ayuda
(incibe@kali)-[~/Documentos/shodan]
$ shodan parse -f port:502 --fields ip_str, port, tags, data resultados-TM251MESE_2.json.gz
95.126.92.178 502  ics  rima-tde.net  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 218.62.117.51 502  ics  jlccptt.net.cn  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 49.229.152.41 502  ics  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 218.62.117.12 502  ics  jlccptt.net.cn  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 83.56.16.17 502  ics  rima-tde.net  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\nUnit ID: 91.80.163.35 502  ics  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 193.152.81.167 502  ics  rima-tde.net  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\nUnit ID: 88.28.209.154 502  ics  rima-tde.net  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.37 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.37 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.37 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.37 \n\nUnit ID: 88.28.218.253 502  ics  rima-tde.net  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.04.12 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.04.12 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 81.42.208.116 502  ics  rima-tde.net  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 120.157.121.136 502  ics  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.21 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.21 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.21 \n\nUnit ID: 193.248.231.219 502  ics  wanadoo.fr  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.05.11 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.05.11 \n\nUnit ID: 85.232.130.190 502  ics  telkanas.lt  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 213.96.26.163 502  ics  rima-tde.net  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V05.00.08.04 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V05.00.08.04 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V05.00.08.04 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V05.00.08.04 \n\nUnit ID: 83.224.129.112 502  ics  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V05.00.08.04 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V05.00.08.04 \n\nUnit ID: 46.56.142.237 502  ics  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.41 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.41 \n\nUnit ID: 218.62.116.254 502  ics  jlccptt.net.cn  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 46.56.141.35 502  ics  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.37 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.37 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.37 \n\nUnit ID: 218.62.117.19 502  ics  jlccptt.net.cn  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 5.154.1.3 502  ics  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.14 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.14 \n\nUnit ID: 109.167.40.60 502  ics  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.02.52 \n\nUnit ID: 2.118.194.22 502  ics  telecomitalia.it  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.21 \n\nUnit ID: 255\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.21 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V05.01.09.21 \n\nUnit ID: 218.62.117.11 502  ics  jlccptt.net.cn  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V04.00.06.38 \n\nUnit ID: 91.80.148.172 502  ics  Unit ID: 0\n-- Device Identification: Schneider Electric TM251MESE V05.00.08.04 \n\nUnit ID: 1\n-- Device Identification: Schneider Electric TM251MESE V05.00.08.04 
```

Ilustración 89: Ejecución del comando «shodan parse -f port:502 --fields ip_str, port, tags, data resultados-TM251MESE_2.json.gz».

Ahora realiza la extracción de la información del archivo: «**resultados-simatic.json.gz**».

- Con la ejecución del siguiente comando, indica que quieres mostrar los campos *ip_str* (dirección IP), *port* (puerto), *tags* (etiqueta, como por ejemplo la que indica si un dispositivo es ics), *_shodan* (muestra información interna del motor Shodan), *hostnames* (muestra el *hostname* detectado), *data* (muestra información asociada al tipo de dispositivo, protocolo o puerto, que ha detectado Shodan).
 - **shodan parse --fields ip_str,port,tags,_shodan,hostnames,data resultados-simatic.json.gz**



12 BÚSQUEDAS DESDE LA CLI: COMANDO PARSE

```
incibe@kali: ~/Documentos/shodan
$ shodan parse --fields ip_str,port,tags,_shodan,hostnames,data resultados-simatic.json.gz

139.59.98.244 161    cloud {'crawler': 'dfd12d70c30ccb3812bf26f89905deeb85e98c77', 'options': {}, 'id': '85a9bdal-97bc-47ed-8314-0a808cd319df', 'module': 'snmp', 'ptr': True} 0A\x02\x01\x00\x04\x06public\xaa24\x02\x04\xb1j^x02\x01\x00\x02\x01\x00050$x\x06\x08+\x06\x01\x02\x01\x01\x00\x04\x18Siemens, SIMATIC, S7-200
129.2.27.81 502    ics {'crawler': 'e96d8dd73faaa42bde09c7ce075d3c7146e67d0', 'options': {}, 'id': '40336983-ae5c-44d0-be26-e71cd1263935', 'module': 'modbus', 'ptr': True} 129-2-27-81.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n
183.76.166.219 161    {'crawler': '308515b6113c0645034fb8122d0ff0d5194e7e72', 'options': {}, 'id': '552c8491-bd3e-4464-9f5c-c07a15d5b299', 'module': 'snmp', 'ptr': True} ab166219.ppp.asahi-ne.t.or.jp 0\x02\x01\x00\x04\x06public\xaa2q\x02\x04\xb1j^x02\x01\x00\x02\x01\x000ca\x06\x08+\x06\x01\x02\x01\x01\x00\x04USiemens, SIMATIC S7, CPU-1200, 6E57 215-1AG40-0XB0, HW: 12, FW: V.4.4.1, S V-N1B37907
133.232.77.9 161    {'crawler': '78039f81a0245caa8ab71c98182f0eff0ce52aab', 'options': {}, 'id': '64747196-5be3-4db5-847b-37ef8f597b2b', 'module': 'snmp', 'ptr': True} 133.232.77.9.static.zoot.jp 0\x02\x01\x00\x04\x06public\xaa2q\x02\x04\xb1j^x02\x01\x00\x02\x01\x000ca\x06\x08+\x06\x01\x02\x01\x01\x00\x04USiemens, SIMATIC S7, CPU-1200, 6E57 215-1AG40-0XB0, HW: 12, FW: V.4.4.1, S V-N1B30701
41.155.252.166 161    {'crawler': 'cdd92e2d835a37d2798fa6c7105171f4d214012f', 'options': {}, 'id': '4df4ca837-1daa-4d74-9f44-9e2a2b705056', 'module': 'snmp', 'ptr': True} 0\x02\x01\x00\x04\x06public\xaa2p\x02\x04\xb1j^x02\x01\x00\x02\x01\x000b0\x06\x08+\x06\x01\x02\x01\x01\x00\x04TSiemens, SIMATIC S7, CPU-1200, 6E57 212-1E40-0XB0, HW: 7, FW: V.4.2.1, S V-K8CS2683
2.196.100.143 161    {'crawler': 'cdd92e2d835a37d2798fa6c7105171f4d214012f', 'options': {}, 'id': '12583319-b0d4-4f8d-beeb-9b098c71368b', 'module': 'snmp', 'ptr': True} Siemens, SIMATIC NET, SCALANCE M876-4 EU, 6GK5 876-4AA00-2BA2, HW: Version V06.02.00, SVPM014938
91.223.193.71 161    {'crawler': '90a359c2c5601dec86ee088ba89601ca8256a61', 'options': {'scan': 'WkM4g5VGFrbx3Jcf'}, 'id': 'b6d6a712-8740-4b5b-b737-6ee1a83e6eb8', 'module': 'snmp', 'ptr': True} 0A\x02\x01\x00\x04\x06public\xaa24\x02\x04\xb1j^x02\x01\x00\x02\x01\x0000\x05\x06\x08+\x06\x01\x02\x01\x01\x00\x04\x18Siemens, SIMATIC, S7-300
185.109.109.1 161    {'crawler': '8c108d59c1b65bba32b325a760b40705b85da', 'options': {'scan': 'SUgAA5NgwReWTUK'}, 'id': '8f6f61d1-b27f-45fd-b00d-75d3701c3510', 'module': 'snmp', 'ptr': True} 0A\x02\x01\x00\x04\x06public\xaa24\x02\x04\xb1j^x02\x01\x00\x02\x01\x0000\x05\x06\x08+\x06\x01\x02\x01\x01\x00\x04\x18Siemens, SIMATIC, S7-300
46.227.222.193 161    {'crawler': '90a359c2c5601dec86ee088ba89601ca8256a61', 'options': {'scan': '4j7QrSebg01fj35z'}, 'id': 'd28bf2c7-96bc-4873-8be6-7f3114268b0d', 'module': 'snmp', 'ptr': True} ip-46-227-222-193.enviatel.net 0\x02\x01\x00\x04\x06public\xaa2p\x02\x04\xb1j^x02\x01\x00\x02\x01\x0000\x05\x06\x08+\x06\x01\x02\x01\x01\x00\x04TSiemens, SIMATIC S7, CPU-1200, 6E57 212-1HE40-0XB0, HW: 2, FW: V.4.1.1, S C-F2594986
129.2.27.13 502    ics {'crawler': '90a359c2c5601dec86ee088ba89601ca8256a61', 'options': {'scan': 'b86YBkhWKFdhc9ZK'}, 'id': '510dd31a-bb68-4b95-a831-ab63ec2ffec8', 'module': 'modbus', 'ptr': True} e} 129-2-27-13.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n
129.2.27.45 502    ics {'crawler': '90a359c2c5601dec86ee088ba89601ca8256a61', 'options': {'scan': 'b86YBkhWKFdhc9ZK'}, 'id': '4d02eb2e-afb0-4342-8f22-30af6613a8d2', 'module': 'modbus', 'ptr': True} e} 129-2-27-45.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n
129.2.27.105 502    ics {'crawler': '42f86247b760542c0192b61c60405edc5db0d155', 'id': 'd87a87d4-4d81-4b81-4b04-3fc6cc', 'module': 'modbus', 'options': {}} 129-2-27-105.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n
129.2.27.218 502    ics {'crawler': '90a359c2c5601dec86ee088ba89601ca8256a61', 'options': {'scan': 'b86YBkhWKFdhc9ZK'}, 'id': 'faec2cd1-7ed4-475f-be44-8adc5184b4f5', 'module': 'modbus', 'ptr': True} e} 129-2-27-218.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n
45.219.102.207 161    {'crawler': '42f86247b760542c0192b61c60405edc5db0d155', 'options': {}, 'id': 'fc812a6d-6246-4d9d-ab7b-470f7d3556dc', 'module': 'snmp', 'ptr': True} Siemens, SIMATIC NET, SCALANCE M876-4 EU, 6GK5 876-4AA00-2BA2, HW: Version 1, FW: Version V06.01.00, SVPL1134416
77.104.252.119 102    ics {'crawler': 'bf213bc419cc8491376c12af31e32623c1b6f467', 'options': {}, 'id': 'a31602dc-905d-4460-88f9-fd005b7d22aa', 'module': 's7', 'ptr': True} Copyright: Original Siemens Equipment\PLC name: SIMATIC 300(1)\nModule type: IM151-8\nPN/DP CPU\nnSerial number of module: S C-KORV02242018\nnPlant identification: nBasic Hardware: 6E57 151-8AB01-0AB0 v.0.7\nn-8 PN/DP CPU\nnSerial number of module: S C-KORV02242018\nnPlant identification: nBasic Hardware: 6E57 151-8AB01-0AB0 v.0.7\nn
165.232.136.159 161    cloud {'crawler': '487814a778c983e2dcf234806292d8c5b52-457c-8c56-94b4c4180c8a', 'options': {'scan': 'UrIIXYF8IzieEWgS'}, 'id': '33ded76-42b5-457c-8c56-94b4c4180c8a', 'module': 'snmp', 'ptr': True} 0A\x02\x01\x00\x04\x06public\xaa24\x02\x04\xb1j^x02\x01\x00\x02\x01\x0000\x05\x06\x08+\x06\x01\x02\x01\x01\x00\x04\x18Siemens, SIMATIC, S7-300
213.86.80.14 161    {'crawler': '36f536ccfb8f2bed3f109d29ab93e2219065654', 'options': {'scan': 'UrIIXYF8IzieEWgS'}, 'id': '7edd9b0e-dc46-44e9-87b0-c4b5b870be0e', 'module': 'snmp', 'ptr': True} 0A\x02\x01\x00\x04\x06public\xaa24\x02\x04\xb1j^x02\x01\x00\x02\x01\x0000\x05\x06\x08+\x06\x01\x02\x01\x01\x00\x04\x18Siemens, SIMATIC, S7-300
129.2.27.162 502    ics {'crawler': '3b30ded3f602a16b2b9b094255050a05614063bc0', 'options': {'scan': 'm00ifx4406HmRaC7'}, 'id': 'fd2c07de-57b8-4635-ad62-cc859cd051c', 'module': 'modbus', 'ptr': True} e} 129-2-27-162.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n
129.2.27.151 502    ics {'crawler': '3b30ded3f602a16b2b9b094255050a05614063bc0', 'options': {'scan': 'm00ifx4406HmRaC7'}, 'id': 'ecc04e39-d587-4391-9e79-686396e9eff1', 'module': 'modbus', 'ptr': True} e} 129-2-27-151.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n
81.23.178.175 102    ics {'crawler': '28d3701d3332c9b20cb1649d936db665a4c57cde', 'options': {}, 'id': '01206439-38e-41f5-828c-e20a999d7f07', 'module': 's7', 'ptr': True} host-81-23-178-175.tl.tr Copyright: Original Siemens Equipment\PLC name: SIMATIC 300(1)\nModule type: CPU 314C-2 PN/DP\nnSerial number of module: S C-CU066225012\nnPlant identification: nBasic Hardware: 6E57 314-6EH04-0AB0 v.0.2\nnModule name: CPU 314C-2 PN/DP\nnSerial number of module: S C-CU066225012\nnPlant identification: nBasic Hardware: 6E57 314-6EH04-0AB0 v.0.2\nn
129.2.27.74 502    ics {'crawler': '3b30ded3f602a16b2b9b094255050a05614063bc0', 'options': {'scan': 'm00ifx4406HmRaC7'}, 'id': '3b548dfa-c084-42ec-b7bf-29112217330f', 'module': 'modbus', 'ptr': True} e} 129-2-27-74.wireless.umd.edu Unit ID: 1\n-- Slave ID Data: \t(110101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n
129.2.27.70 502    ics {'crawler': '3b30ded3f602a16b2b9b094255050a05614063bc0', 'options': {'scan': 'm00ifx4406HmRaC7'}, 'id': '484fc399-7444-4def-8fb9-3721e2f96bbe', 'module': 'modbus', 'ptr': True}
```

Ilustración 90: Ejecución del comando «shodan parse --fields ip_str,port,tags,_shodan,hostnames,data resultados-simatic.json.gz».



BÚSQUEDAS DESDE LA CLI: COMANDO PARSE

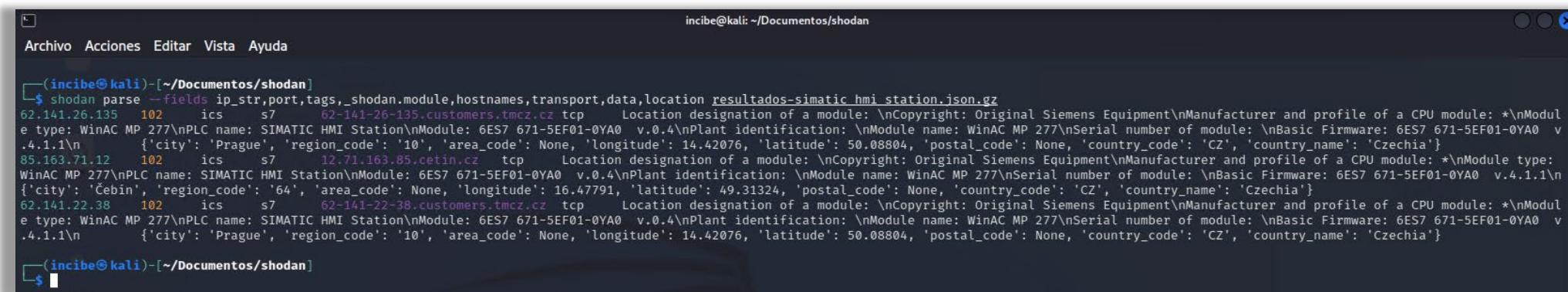
- Para que solo muestre resultados de búsqueda del puerto 102, utiliza el siguiente comando:
 - shodan parse -f port:102 --fields ip_str,port,tags,_shodan,hostnames,data resultados-simatic.json.gz**

```
incibe@kali:~/Documentos/shodan
$ shodan parse -f port:102 --fields ip_str,port,tags,_shodan,hostnames,data resultados-simatic.json.gz

77.104.252.119 102 ics {'crawler': 'bf213bc419cc8491376c12af31e32623c1b6f467', 'options': {}, 'id': 'a31602dc-905d-4460-88f9-fd005b7d2aa', 'module': 's7', 'ptr': True} Copyright: Original Siemens Equipment\nPLC name: SIMATIC 300(1)\nModule type: IM151-8 PN/DP CPU\nUnknown (129): Boot Loader A%\nModule: 6E57 151-8AB01-0AB0 v.0.7\nBasic Firmware: v.3.2.14\nModule name: IM151-8 PN/DP CPU\nSerial number of module: S C-KORY02242018\nPlant identification: \nBasic Hardware: 6E57 151-8AB01-0AB0 v.0.7\n81.23.178.175 102 ics {'crawler': '28d3701d3332c9b20cb1649d936db665a4c57cde', 'options': {}, 'id': '01206439-38e8-41f5-828c-e20a999d7f07', 'module': 's7', 'ptr': True} host-81-23-178.175.tl.t.ru Copyright: Original Siemens Equipment\nPLC name: SIMATIC 300(1)\nModule type: CPU 314C-2 PN/DP\nUnknown (129): Boot Loader A%\nModule: 6E57 314-6EH04-0AB0 v.0.2\nBasic Firmware: v.3.3.7\nModule name: CPU 314C-2 PN/DP\nSerial number of module: S C-CDU662252012\nPlant identification: \nBasic Hardware: 6E57 314-6EH04-0AB0 v.0.2\n62.94.102.211 102 ics {'crawler': '6d5195c331613d103027c23dc52e6d32fd2a74af', 'options': {'scan': 'PYSSzrxYxPPxdzLvf'}, 'id': 'bd5ae23c-555c-4a12-a4d1-6ef71c025814', 'module': 's7', 'ptr': True} i.p-102-211.snl.clouditalia.com Copyright: Original Siemens Equipment\nPLC name: SIMATIC 300\nModule type: CPU 315-2 DP\nUnknown (129): Boot Loader A%\nModule: 6E57 315-2AG10-0AB0 v.0.7\nBasic Firmware: v.2.6.6\nModule name: CPU 315-2 DP\nSerial number of module: S C-W6V981202008\nPlant identification: \nBasic Hardware: 6E57 315-2AG10-0AB0 v.0.7\n35.131.239.2 102 ics {'crawler': 'cdd92e2d835a37d2798fa6c7105171f4d214012f', 'options': {}, 'id': '737ee9f-4498-48f9-a04a-ied63b0dba03', 'module': 's7', 'ptr': True} 035-131-239-002.biz.spectrum.com Copyright: Original Siemens Equipment\nPLC name: SIMATIC 300-Station\nModule type: CPU 315F-2 PN/DP\nUnknown (129): Boot Loader A%\nModule: 6E57 315-2FJ14-0AB0 v.0.10\nBasic Firmware: v.3.2.17\nModule name: CPU 315F-2 PN/DP\nSerial number of module: S C-N3J990112021\nPlant identification: \nBasic Hardware: 6E57 315-2FJ14-0AB0 v.0.10\n151.0.238.98 102 ics {'crawler': 'ada8582d54117e5eb7c72186882e76f0854a54ae', 'options': {}, 'id': 'f1bf8997-9be6-4056-a8c1-cb51f599a1b6', 'module': 's7', 'ptr': True} Copyright: Original Siemens Equipment\nPLC name: SIMATIC 300(1)\nModule type: CPU 317-2 DP\nUnknown (129): Boot Loader A%\nModule: 6E57 317-2AJ10-0AB0 v.0.5\nBasic Firmware: v.2.6.10\nModule name: CPU 317-2 D\nP\nSerial number of module: S C-X6UG26832009\nPlant identification: \nBasic Hardware: 6E57 317-2AJ10-0AB0 v.0.5\n93.240.48.210 102 ics {'crawler': '85a5be66a1913a867d4f8cd62bd10fb79f410a2a', 'options': {}, 'id': '9f377bc1-aec4-4c79-9921-1a159309015d', 'module': 's7', 'ptr': True} p5df030d2.dip0.t-ipconnect.de Copyright: Original Siemens Equipment\nPLC name: SIMATIC 300(1)\nModule type: CPU 315-2 PN/DP\nUnknown (129): Boot Loader A%\nModule: 6E57 315-2EH14-0AB0 v.0.7\nModule name: CPU 315-2 PN/DP\nSerial number of module: S C-FNC412002015\nPlant identification: \nBasic Hardware: 6E57 315-2EH14-0AB0 v.0.7\n187.121.199.154 102 ics {'crawler': '1e4769fde0b9dbe1f84ba3a427cb5b0e415246c1', 'options': {}, 'id': '1160108f-6e5f-4143-a967-d7fa8829fc30', 'module': 's7', 'ptr': True} 187-121-199-154.nucleo.com.br Location designation of a module: Porta Ferreira / SP\nCopyright: Original Siemens Equipment\nManufacturer and profile of a CPU module: *\nModule type: WinAC RTX\nPLC name: Simatic PC\nModule: 6E57 611-4SB00-0YB7 v.4.6.0\n109.164.243.35 102 ics {'crawler': '487814a778c983e2cef234806292d88c5cbf3ec', 'options': {}, 'id': '7f633df0-1fd5-41a4-a0e0-850d6f5bd08c', 'module': 's7', 'ptr': True} smtp365.tegometall.com Copyright: Original Siemens Equipment\nPLC name: SIMATIC 300(RBG01)\nModule type: CPU 315F-2 PN/DP\nUnknown (129): Boot Loader A%\nModule: 6E57 315-2FJ14-0AB0 v.0.6\nModule name: HRL-CPU-201\nSerial number of module: S C-E3VC49142014\nPlant identification: \nBasic Hardware: 6E57 315-2FJ14-0AB0 v.0.6\n
```

Ilustración 91: Búsqueda de resultados del puerto 102.

- A continuación, realiza la extracción de la información de la IP, puerto, la etiqueta que tenga, información de Shodan, el nombre del *host*, el modo de transporte, los datos y la localización del archivo «**resultados-simatic_hmi_station**» con el siguiente comando:
 - **shodan parse --fields ip_str,port,tags,_shodan.module,hostnames,transport,data,location resultados-simatic_hmi_station.json.gz**



The screenshot shows a terminal window titled "incibe@kali: ~/Documentos/shodan". The user has run the command:

```
shodan parse --fields ip_str,port,tags,_shodan.module,hostnames,transport,data,location resultados-simatic_hmi_station.json.gz
```

The output displays several entries of SIMATIC HMI Station modules found in the specified JSON file. Each entry includes fields such as IP address, port, tags, module details, hostnames, transport type (tcp), data, and location information (city, region_code, area_code, longitude, latitude, postal_code, country_code, country_name).

Ilustración 92: Extracción de la información del archivo «**resultados-simatic_hmi_station**»

BÚSQUEDAS DESDE LA CLI: COMANDO *PARSE*

- Realiza la extracción de la información de la IP, puerto, la etiqueta que tenga, información de Shodan, el nombre del *host*, el modo de transporte, los datos y la localización, del archivo «resultados-s7-200.json.gz», con el siguiente comando:

- **shodan parse --fields**
*ip_str, port, tags, _shodan, host
names, transport, data, location*
resultados-s7-200.json.gz

Ilustración 93: Extracción de resultados «resultados-s7-200.json.gz».



12 BÚSQUEDAS DESDE LA CLI: COMANDO PARSE

- shodan parse -f port:502 –

fields

ip_str, port, tags, _shodan, hostnames, transport, data, location

resultados-s7-200.json.gz

- En este caso, estamos realizando una extracción de información únicamente del puerto 502.

```
incibe@kali:~/Documentos/shodan
$ shodan parse -f port:502 --fields ip_str,port,tags,_shodan,hostnames,transport,data,location resultados-s7-200.json.gz
[...]
```

Ilustración 94: Ejecución del comando «shodan parse -f port:502 –fields ip_str, port, tags, _shodan, hostnames, transport, data, location resultados-s7-200.json.gz».



12 BÚSQUEDAS DESDE LA CLI: COMANDO PARSE

- Con esta siguiente búsqueda, debes buscar con la etiqueta «ics» los campos IP, puerto, tags, _shodan, hostnames, transport, data y location.

■ **shodan parse -f tags:ics --fields ip_str,port,tags,_shodan,hostnames,transport,data,location resultados-s7-200.json.gz**

```
incibe@kali: ~/Documentos/shodan
$ shodan parse -f tags:ics --fields ip_str, port, tags, _shodan, hostnames, transport, data, location resultados-s7-200.json.gz
129.2.27.81      502    ics  {'crawler': 'e69d8d673faaa42bde089c7ce075d3c7146e67d0', 'options': {}, 'id': '40336983-aec-44d0-be26-e71cd1263935', 'module': 'modbus', 'ptr': True}  129-2-27-81.wireless.umd.edu  tcp  Unit ID: 1\n-- Slave ID Data: \t(t(10101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n\t{'city': 'College Park', 'region_code': 'MD', 'area_code': None, 'longitude': -76.93692, 'latitude': 38.98067, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'}
129.2.27.13      502    ics  {'crawler': '90a359c2c5601dedc86ee088ba89601ca8256a61', 'options': {'scan': 'BB6YBkhWKFdhc9ZX'}, 'id': '510dd31a-bb68-4b95-a831-ab63ec2ffec8', 'module': 'modbus', 'ptr': True}  129-2-27-13.wireless.umd.edu  tcp  Unit ID: 1\n-- Slave ID Data: \t(t(10101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n\t{'city': 'College Park', 'region_code': 'MD', 'area_code': None, 'longitude': -76.93692, 'latitude': 38.98067, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'}
129.2.27.45      502    ics  {'crawler': '90a359c2c5601dedc86ee088ba89601ca8256a61', 'options': {'scan': 'BB6YBkhWKFdhc9ZX'}, 'id': '4d02eb2e-afb0-4342-8f22-30af6613a8d2', 'module': 'modbus', 'ptr': True}  129-2-27-45.wireless.umd.edu  tcp  Unit ID: 1\n-- Slave ID Data: \t(t(10101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n\t{'city': 'College Park', 'region_code': 'MD', 'area_code': None, 'longitude': -76.93692, 'latitude': 38.98067, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'}
129.2.27.105     502    ics  {'crawler': '42f86247b760542c0192b61c60405edc5db01d55', 'id': 'd87a87af-d891-4da8-bb14-b0b46c3f6cc4', 'module': 'modbus', 'options': {}}  129-2-27-105.wireless.umd.edu  tcp  Unit ID: 1\n-- Slave ID Data: \t(t(10101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n\t{'city': 'College Park', 'region_code': 'MD', 'area_code': None, 'longitude': -76.93692, 'latitude': 38.98067, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'}
129.2.27.218     502    ics  {'crawler': '90a359c2c5601dedc86ee088ba89601ca8256a61', 'options': {'scan': 'BB6YBkhWKFdhc9ZX'}, 'id': 'faec2cd1-7ed4-475f-be44-8adc5184b4f5', 'module': 'modbus', 'ptr': True}  129-2-27-218.wireless.umd.edu  tcp  Unit ID: 1\n-- Slave ID Data: \t(t(10101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n\t{'city': 'College Park', 'region_code': 'MD', 'area_code': None, 'longitude': -76.93692, 'latitude': 38.98067, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'}
129.2.27.162     502    ics  {'crawler': '3b30ded3f602a16b2b9b09425b50a05614063bc0', 'options': {'scan': 'M00ifx4406HmRaC7'}, 'id': 'fdc207de-57b8-4635-ad62-cc859cd05dic', 'module': 'modbus', 'ptr': True}  129-2-27-162.wireless.umd.edu  tcp  Unit ID: 1\n-- Slave ID Data: \t(t(10101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n\t{'city': 'College Park', 'region_code': 'MD', 'area_code': None, 'longitude': -76.93692, 'latitude': 38.98067, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'}
129.2.27.151     502    ics  {'crawler': '3b30ded3f602a16b2b9b09425b50a05614063bc0', 'options': {'scan': 'M00ifx4406HmRaC7'}, 'id': 'ec04e39-d587-4391-9e79-6863969eff1', 'module': 'modbus', 'ptr': True}  129-2-27-151.wireless.umd.edu  tcp  Unit ID: 1\n-- Slave ID Data: \t(t(10101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n\t{'city': 'College Park', 'region_code': 'MD', 'area_code': None, 'longitude': -76.93692, 'latitude': 38.98067, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'}
129.2.27.74      502    ics  {'crawler': '3b30ded3f602a16b2b9b09425b50a05614063bc0', 'options': {'scan': 'M00ifx4406HmRaC7'}, 'id': '3b548dfa-c084-42ec-b7bf-29112217330f', 'module': 'modbus', 'ptr': True}  129-2-27-74.wireless.umd.edu  tcp  Unit ID: 1\n-- Slave ID Data: \t(t(10101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n\t{'city': 'College Park', 'region_code': 'MD', 'area_code': None, 'longitude': -76.93692, 'latitude': 38.98067, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'}
129.2.27.166     502    ics  {'crawler': '3b30ded3f602a16b2b9b09425b50a05614063bc0', 'options': {'scan': 'M00ifx4406HmRaC7'}, 'id': '135c3578-34f3-444c-bed4-ef04a63678d', 'module': 'modbus', 'ptr': True}  129-2-27-166.wireless.umd.edu  tcp  Unit ID: 1\n-- Slave ID Data: \t(t(10101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n\t{'city': 'College Park', 'region_code': 'MD', 'area_code': None, 'longitude': -76.93692, 'latitude': 38.98067, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'}
129.2.27.150     502    ics  {'crawler': '90a359c2c5601dedc86ee088ba89601ca8256a61', 'options': {'scan': 'BB6YBkhWKFdhc9ZX'}, 'id': '65f0febd-31le-4607-9720-ca1d258414f9', 'module': 'modbus', 'ptr': True}  129-2-27-150.wireless.umd.edu  tcp  Unit ID: 1\n-- Slave ID Data: \t(t(10101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n\t{'city': 'College Park', 'region_code': 'MD', 'area_code': None, 'longitude': -76.93692, 'latitude': 38.98067, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'}
129.2.27.182     502    ics  {'crawler': '3b30ded3f602a16b2b9b09425b50a05614063bc0', 'options': {'scan': 'M00ifx4406HmRaC7'}, 'id': '2a3183bb-1b02-4e0b-9f07-788983111c93', 'module': 'modbus', 'ptr': True}  129-2-27-182.wireless.umd.edu  tcp  Unit ID: 1\n-- Slave ID Data: \t(t(10101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n\t{'city': 'College Park', 'region_code': 'MD', 'area_code': None, 'longitude': -76.93692, 'latitude': 38.98067, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'}
129.2.27.94      502    ics  {'crawler': '3b30ded3f602a16b2b9b09425b50a05614063bc0', 'options': {'scan': 'M00ifx4406HmRaC7'}, 'id': 'a0962280-8302-4a68-8b21-aaca5f4cca63', 'module': 'modbus', 'ptr': True}  129-2-27-94.wireless.umd.edu  tcp  Unit ID: 1\n-- Slave ID Data: \t(t(10101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n\t{'city': 'College Park', 'region_code': 'MD', 'area_code': None, 'longitude': -76.93692, 'latitude': 38.98067, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'}
129.2.27.24      502    ics  {'crawler': '36f536ccfb8f2bed3f4109d29ab93e6221906564', 'options': {'scan': 'BB6YBkhWKFdhc9ZX'}, 'id': 'fdb3b165-8733-411e-a832-52ee6ad275b2', 'module': 'modbus', 'ptr': True}  129-2-27-24.wireless.umd.edu  tcp  Unit ID: 1\n-- Slave ID Data: \t(t(10101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n\t{'city': 'College Park', 'region_code': 'MD', 'area_code': None, 'longitude': -76.93692, 'latitude': 38.98067, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'}
129.2.27.27      502    ics  {'crawler': '36f536ccfb8f2bed3f4109d29ab93e6221906564', 'options': {'scan': 'BB6YBkhWKFdhc9ZX'}, 'id': '5de56318-1fd8-406b-abd8-d0124b9a936a', 'module': 'modbus', 'ptr': True}  129-2-27-27.wireless.umd.edu  tcp  Unit ID: 1\n-- Slave ID Data: \t(t(10101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n\t{'city': 'College Park', 'region_code': 'MD', 'area_code': None, 'longitude': -76.93692, 'latitude': 38.98067, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'}
129.2.27.163     502    ics  {'crawler': '3b30ded3f602a16b2b9b09425b50a05614063bc0', 'options': {'scan': 'M00ifx4406HmRaC7'}, 'id': '4b6e95c7-f487-4e25-b6f8-5e3340a2ab95', 'module': 'modbus', 'ptr': True}  129-2-27-163.wireless.umd.edu  tcp  Unit ID: 1\n-- Slave ID Data: \t(t(10101ff)\n-- Device Identification: Siemens SIMATIC S7-200 \n\nUnit ID: 255\n\n\t{'city': 'College Park', 'region_code': 'MD', 'area_code': None, 'longitude': -76.93692, 'latitude': 38.98067, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'}
```

Ilustración 95: Ejecución del comando «shodan parse -f tags:ics --fields ip_str, port, tags, _shodan, hostnames, transport, data, location resultados-s7-200.json.gz».



BÚSQUEDAS DESDE LA CLI: COMANDO PARSE

- Por último, para la extracción de la información del archivo «resultados-rockwell» ejecuta el siguiente comando:

▪ **shodan parse –fields ip_str,port,tags,_shodan.module,hostnames,transport,data,os,location.city,location.country_code,location.country_name resultados-rockwell.json.gz**

```
(incibe㉿kali)-[~/Documentos/shodan]$ shodan parse --fields ip_str,port,tags,_shodan.module,hostnames,transport,data,os,location.city,location.country_code,location.country_name resultados-rockwell.json.gz
[{"ip": "166.153.1.223", "port": 44818, "tags": "ethernetip-udp", "module": "shodan", "hostnames": "223.sub-166-153-1.myvzw.com", "transport": "udp", "os": "Product name: 1769-L30ER/A LOGIX5330ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60b38d0b\nDevice type: Programmable Logic Controller\nDevice IP: 172.19.109.5", "city": "Euless", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "63.41.196.98", "port": 44818, "tags": "ethernetip-udp", "module": "shodan", "hostnames": "host98.sub-63-41-196.myvzw.com", "transport": "udp", "os": "Product name: 1766-L32BXBA C/21.02\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60e79dff\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.13.100", "city": "Bell Buckle", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "212.34.4.179", "port": 44818, "tags": "ics", "module": "shodan", "hostnames": "tcp", "os": "Product name: 2080-LC20-20QWB\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0xd022c4b1\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.0.2", "city": "Amman", "country_code": "JO", "country_name": "Jordan", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "166.239.119.6", "port": 44818, "tags": "ethernetip-udp", "module": "shodan", "hostnames": "6.sub-166-239-119.myvzw.com", "transport": "udp", "os": "Product name: 1769-L30ER/A LOGIX5330ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0xd0187733\nDevice type: Programmable Logic Controller\nDevice IP: 10.10.6.10", "city": "Euless", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "63.46.201.229", "port": 44818, "tags": "ethernetip-udp", "module": "shodan", "hostnames": "host198.sub-63-46-201.myvzw.com", "transport": "udp", "os": "Product name: 1763-L16BWA B/14.00\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x9ca0ec92\nDevice type: Communications Adapter\nDevice IP: 192.168.38.130", "city": "Sunnyvale", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "166.149.208.82", "port": 44818, "tags": "ics", "module": "shodan", "hostnames": "82.sub-166-149-208.myvzw.com", "transport": "tcp", "os": "Product name: 1769-L16ER/B LOGIX5316ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60d06f67\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.0.2", "city": "Idabel", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "166.148.119.123", "port": 44818, "tags": "ics", "module": "shodan", "hostnames": "123.sub-166-148-119.myvzw.com", "transport": "tcp", "os": "Product name: 1766-L32BXBA B/15.00\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x40652229\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.1.2", "city": "Twin Oaks", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "96.1.77.85", "port": 44818, "tags": "ics", "module": "shodan", "hostnames": "96-1-77-85-staticipwest.wireless.telus.com", "transport": "tcp", "os": "Product name: 1769-L19ER-BB1B/A LOGIX5319ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60e8ee9\nDevice type: Programmable Logic Controller\nDevice IP: 10.83.1.7", "city": "Cheney", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "166.166.53.189", "port": 44818, "tags": "ethernetip-udp", "module": "shodan", "hostnames": "189.sub-166-166-53.myvzw.com", "transport": "udp", "os": "Product name: 5069-L306ER/A\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60c707e6\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.100.2", "city": "Euless", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "166.251.157.183", "port": 44818, "tags": "ics", "module": "shodan", "hostnames": "103.sub-166-251-183.myvzw.com", "transport": "tcp", "os": "Product name: 1766-L32BXBA C/21.02\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0xd013cf7e\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.13.100", "city": "Euless", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "107.223.182.182", "port": 44818, "tags": "ethernetip-udp", "module": "shodan", "hostnames": "107-223-182-182.lightspeed.gnvlsc.sbcglobal.net", "transport": "udp", "os": "Product name: 1766-L32BWAA B/13.00\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x406fb3d\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.1.100", "city": "Easley", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "70.36.23.225", "port": 44818, "tags": "ics", "module": "shodan", "hostnames": "61fb3d\nDevice type: Programmable Logic Controller\nDevice IP: 10.83.244.26", "transport": "tcp", "os": "Product name: 1769-L18ER/B LOGIX5318ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60ef30fa\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.100.2", "city": "Dallas", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "63.47.7.137", "port": 44818, "tags": "ics", "module": "shodan", "hostnames": "63-47-7.myvzw.com", "transport": "tcp", "os": "Product name: 1769-L16ER/B LOGIX5316ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60bf9018\nDevice type: Programmable Logic Controller\nDevice IP: 10.4.157.2", "city": "Dallas", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "166.136.164.27", "port": 44818, "tags": "ethernetip-udp", "module": "shodan", "hostnames": "mobile-166-136-164-027.myingular.net", "transport": "udp", "os": "Product name: 1766-L32AWA C/21.02\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0xd050d2e0\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.100.2", "city": "Brownsville", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "207.177.151.205", "port": 44818, "tags": "ics", "module": "shodan", "hostnames": "static-207-177-151-205.wireless.unwiredbb.net", "transport": "tcp", "os": "Product name: 1769-L30ER/A LOGIX5330ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60d97ebd\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.1.250", "city": "Bakersfield", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "166.157.134.17", "port": 44818, "tags": "ics", "module": "shodan", "hostnames": "17.sub-166-157-134.myvzw.com", "transport": "tcp", "os": "Product name: 1756-ENBT/A\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x00a6d9be\nDevice type: Communications Adapter\nDevice IP: 100.100.100.133", "city": "Hickory Hills", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "166.180.251.179", "port": 44818, "tags": "ethernetip-udp", "module": "shodan", "hostnames": "179.qarestr.sub-166-180-251.myvzw.com", "transport": "udp", "os": "Product name: 1766-L32AWA C/21.02\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0xd0250c5e\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.100.2", "city": "Plano", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "63.46.247.10", "port": 44818, "tags": "ics", "module": "shodan", "hostnames": "host10.sub-63-46-247.myvzw.com", "transport": "tcp", "os": "Product name: 1763-L16AWA B/16.00\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x16a6da57\nDevice type: Communications Adapter\nDevice IP: 192.168.0.10", "city": "Sunnyvale", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "74.213.224.43", "port": 44818, "tags": "ethernetip-udp", "module": "shodan", "hostnames": "host137.sub-63-47-7.myvzw.com", "transport": "tcp", "os": "Product name: PanelView Plus_7 Standard 600\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x6013ec22\nDevice type: Human-Machine Interface\nDevice IP: 192.168.10.2", "city": "Los Angeles", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "66.244.168.125", "port": 44818, "tags": "ethernetip-udp", "module": "shodan", "hostnames": "125.168.244.66.biz.sta.worldgci.net", "transport": "udp", "os": "Product name: 1769-L35E Ethernet Port\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x403d8a0\nDevice type: Communications Adapter\nDevice IP: 192.168.1.99", "city": "Chicago", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "173.181.136.204", "port": 44818, "tags": "ethernetip-udp", "module": "shodan", "hostnames": "173-181-136-204-ent-barlow-staticipwest.wireless.telus.com", "transport": "udp", "os": "Product name: 2080-LC20-20QWB\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60d47d9e\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.1.152", "city": "Lloydminster", "country_code": "CA", "country_name": "Canada", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "184.151.239.119", "port": 44818, "tags": "ics", "module": "shodan", "hostnames": "184-151-239-119.myvzw.com", "transport": "tcp", "os": "Product name: 1766-L32BXBA B/11.00\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x4060f9ef\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.1.152", "city": "Toronto", "country_code": "CA", "country_name": "Canada", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "212.166.151.87", "port": 44818, "tags": "ethernetip-udp", "module": "shodan", "hostnames": "192.168.1.2", "transport": "udp", "os": "Product name: 1766-L32BXBA B/10.00\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x404fedfc\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.13.100", "city": "Valencia", "country_code": "ES", "country_name": "Spain", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "166.251.171.55", "port": 44818, "tags": "ics", "module": "shodan", "hostnames": "55.sub-166-251-171.myvzw.com", "transport": "tcp", "os": "Product name: 1766-L32BXBA C/21.02\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0xd01414ae\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.10.100", "city": "Euless", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}, {"ip": "174.90.191.84", "port": 44818, "tags": "ethernetip-udp", "module": "shodan", "hostnames": "174-90-191-84.myvzw.com", "transport": "udp", "os": "Product name: 2080-LC20-20QWB\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60690952\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.10.100", "city": "Euless", "country_code": "US", "country_name": "United States", "location": "Rockwell Automation/Allen-Bradley"}]
```

Ilustración 96: Extracción de la información del archivo «resultados-rockwell».

Debido a que la localización de la información puede resultar un poco complicada, en especial cuando se tienen varios campos, el parámetro `--separator` permite definir una cadena para separar campos. Por ejemplo, la cadena «----».

- **shodan parse --fields**
ip_str,port,tags,_shodan.module,hostnames,transport,data,os,location.city,location.country_code,location.country_name --separator ----- resultados-rockwell.json.gz



BÚSQUEDAS DESDE LA CLI: COMANDO PARSE

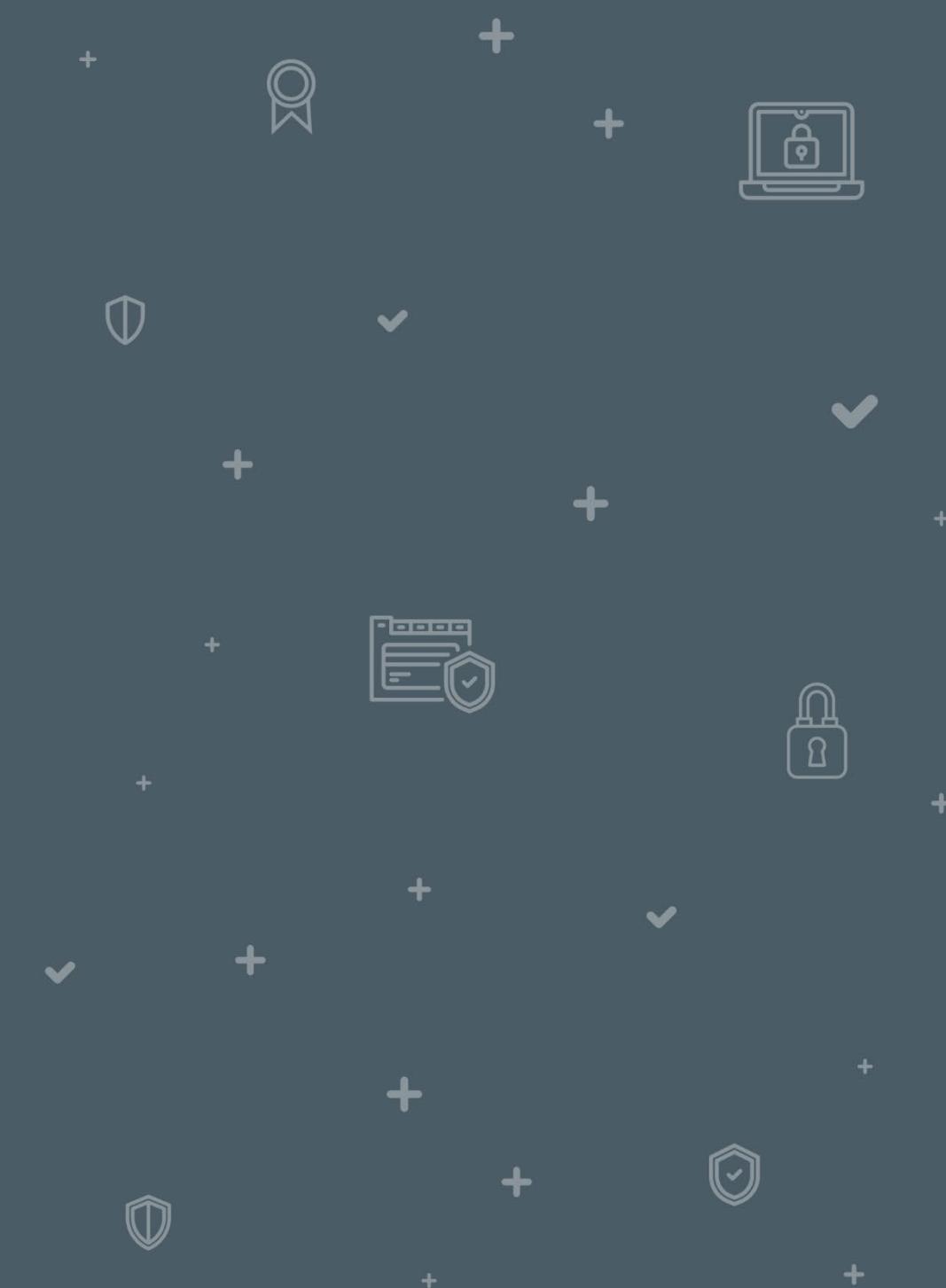
The screenshot shows a terminal window titled "incibe@kali: ~/Documentos/shodan". The command entered is "shodan parse --fields ip, port, tags, _shodan.module, hostnames, transport, data, os, location.city, location.country_code, location.country_name --separator ----- resultados-rockwell.json.gz". The output lists numerous network devices, their details, and their geographical locations. The output is very long and contains many entries like:

```
$ shodan parse --fields ip, port, tags, _shodan.module, hostnames, transport, data, os, location.city, location.country_code, location.country_name --separator ----- resultados-rockwell.json.gz
166.153.1.223--44818--ethernetip-udp--223.sub-166-153-1.myvzw.com--udp--Product name: 1769-L30ER/A LOGIX5330ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60b38d0b\nDevice type: Programmable Logic Controller\nDevice IP: 172.19.109.5--Euless--US--United States
63.41.196.98--44818--ethernetip-udp--host98.sub-63-41-196.myvzw.com--udp--Product name: 1766-L32BXBA C/21.02\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60e79dff\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.13.100--Bell Buckle--US--United States
212.34.4.179--44818--ics--ethernetip--tcp--Product name: 2080-LC20-20QWB\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0xd022c4b1\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.0.2--Amman--Jordan
166.239.119.6--44818--ethernetip-udp--6.sub-166-239-119.myvzw.com--udp--Product name: 1769-L30ER/A LOGIX5330ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0xd0187733\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.1.2--Euless--US--United States
63.46.201.229--44818--ethernetip-udp--host229.sub-63-46-201.myvzw.com--udp--Product name: 1763-L16BWA B/14.00\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x9ca0ec92\nDevice type: Communications Adapter\nDevice IP: 192.168.38.130--Sunnyvale--US--United States
166.149.208.82--44818--ics--ethernetip--82.sub-166-149-208.myvzw.com--tcp--Product name: 1769-L16ER/B LOGIX5316ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60d06f67\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.0.2--Idabel--US--United States
166.148.119.123--44818--ics--ethernetip--123.sub-166-148-119.myvzw.com--tcp--Product name: 1766-L32BXB B/15.00\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x40652229\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.1.2--Twin Oaks--US--United States
96.1.77.85--44818--ics--ethernetip--96-1-77-85-statisticwest.wireless.telus.com--tcp--Product name: 1769-L19ER-BB1B/A LOGIX5319ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60ec8ee9\nDevice type: Programmable Logic Controller\nDevice IP: 10.8.1.7--Cheney--US--United States
166.166.53.189--44818--ethernetip-udp--189.sub-166-166-53.myvzw.com--udp--Product name: 5069-L30ER/A\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60c707e6\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.100.2--Euless--US--United States
166.251.157.103--44818--ics--ethernetip--103.sub-166-251-157.myvzw.com--tcp--Product name: 1766-L32BXBA C/21.02\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0xd013cf7e\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.100--Euless--US--United States
107.223.182.182--44818--ethernetip-udp--107-223-182-182.lightspeed.gnvisc.sbcglobal.net--udp--Product name: 1766-L32BWA B/13.00\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x4061fb3d\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.1.100--Easley--US--United States
70.36.23.225--44818--ics--ethernetip--tcp--Product name: 1769-L18ER/B LOGIX5318ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60ef30fa\nDevice type: Programmable Logic Controller\nDevice IP: 10.83.244.26--Dallas--US--United States
63.47.7.137--44818--ics--ethernetip--host137.sub-63-47-7.myvzw.com--tcp--Product name: 1769-L16ER/B LOGIX5316ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60bf9018\nDevice type: Programmable Logic Controller\nDevice IP: 10.4.157.2--Dallas--US--United States
166.136.164.27--44818--ethernetip-udp--mobile-166-136-164-027.mycingular.net--udp--Product name: 1766-L32AWA C/21.02\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0xd050d2e0\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.100.2--Brownsville--US--United States
207.177.151.205--44818--ics--ethernetip--static-207-177-151-205.wireless.unwireddb.net--tcp--Product name: 1769-L30ER/A LOGIX5330ER\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60d97ebd\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.1.250--Bakersfield--US--United States
166.157.134.17--44818--ics--ethernetip--17.sub-166-157-134.myvzw.com--tcp--Product name: 1756-ENBT/A\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x00a6d9be\nDevice type: Communications Adapter\nDevice IP: 100.100.100.133--Hickory Hills--US--United States
166.180.251.179--44818--ethernetip-udp--179.garestr.sub-166-180-251.myvzw.com--udp--Product name: 1766-L32AWA C/21.02\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0xd0250c5e\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.100.2--Plano--US--United States
63.46.247.10--44818--ics--ethernetip--host10.sub-63-46-247.myvzw.com--tcp--Product name: 1763-L16AWA B/16.00\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x16a6da57\nDevice type: Communications Adapter\nDevice IP: 192.168.0.10--Sunnyvale--US--United States
74.213.224.43--44818--ethernetip-udp--tcp--Product name: PanelView Plus_7 Standard 600\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x6013ec22\nDevice type: Human-Machine Interface\nDevice IP: 192.168.10.2--Los Angeles--US--United States
66.244.168.125--44818--ethernetip-udp--125.168.244.66.biz.sta.networkgci.net--udp--Product name: 1769-L35E Ethernet Port\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x403d8a03\nDevice type: Communications Adapter\nDevice IP: 192.168.1.99--Chicago--US--United States
173.181.136.204--44818--ethernetip-udp--173-181-136-204-ent-barlow-staticipwest.wireless.telus.com--udp--Product name: 2080-LC20-20QWB\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60d47d9e\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.1.152--Lloydminster--CA--Canada
184.151.239.119--44818--ics--ethernetip--tcp--Product name: 1766-L32BXBA B/11.00\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x4060f9ef\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.1.152--Toronto--CA--Canada
212.166.151.87--44818--ethernetip-udp--tcp--Product name: 1766-L32BXB B/10.00\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x404fedfc\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.1.2--Valencia--ES--Spain
166.251.171.55--44818--ics--ethernetip--55.sub-166-251-171.myvzw.com--tcp--Product name: 1766-L32BXBA C/21.02\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0xd01414ae\nDevice type: Programmable Logic Controller\nDevice IP: 192.168.13.100--Euless--US--United States
174.90.191.84--44818--ethernetip-udp--tcp--Product name: 2080-LC20-20QWB\nVendor ID: Rockwell Automation/Allen-Bradley\nSerial number: 0x60690952\nDevice type: Programmable Logic Controller
```

Ilustración 97: Parámetro --separator el texto que utilizamos para separación de campos es el «-----».

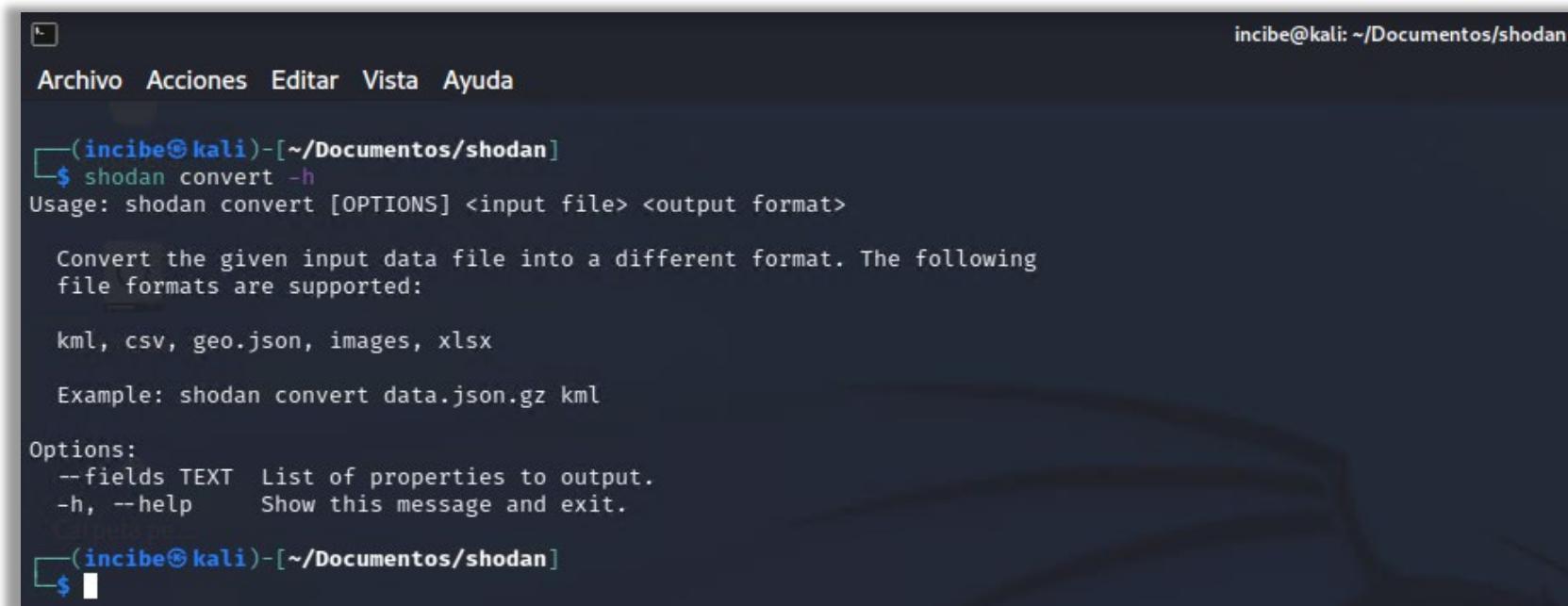
BÚSQUEDAS DESDE LA CLI: COMANDO *CONVERT*

13



Ahora, vamos a utilizar el comando de **shodan convert** para convertir el archivo comprimido «json.gz» que has descargado previamente, en un archivo con un formato diferente como «csv».

- Ejecuta la ayuda del comando:
 - **shodan convert -h**



The terminal window shows the user 'incibe' at a Kali Linux terminal. The command 'shodan convert -h' is entered, and the output provides usage information for the 'shodan convert' command. It details supported file formats (kml, csv, geo.json, images, xlsx) and examples of usage, such as 'shodan convert data.json.gz kml'. It also lists options like '--fields' and '-h'.

```
incibe@kali: ~/Documentos/shodan
Archivo Acciones Editar Vista Ayuda
(incibe㉿kali)-[~/Documentos/shodan]
$ shodan convert -h
Usage: shodan convert [OPTIONS] <input file> <output format>

Convert the given input data file into a different format. The following
file formats are supported:

kml, csv, geo.json, images, xlsx

Example: shodan convert data.json.gz kml

Options:
--fields TEXT  List of properties to output.
-h, --help      Show this message and exit.

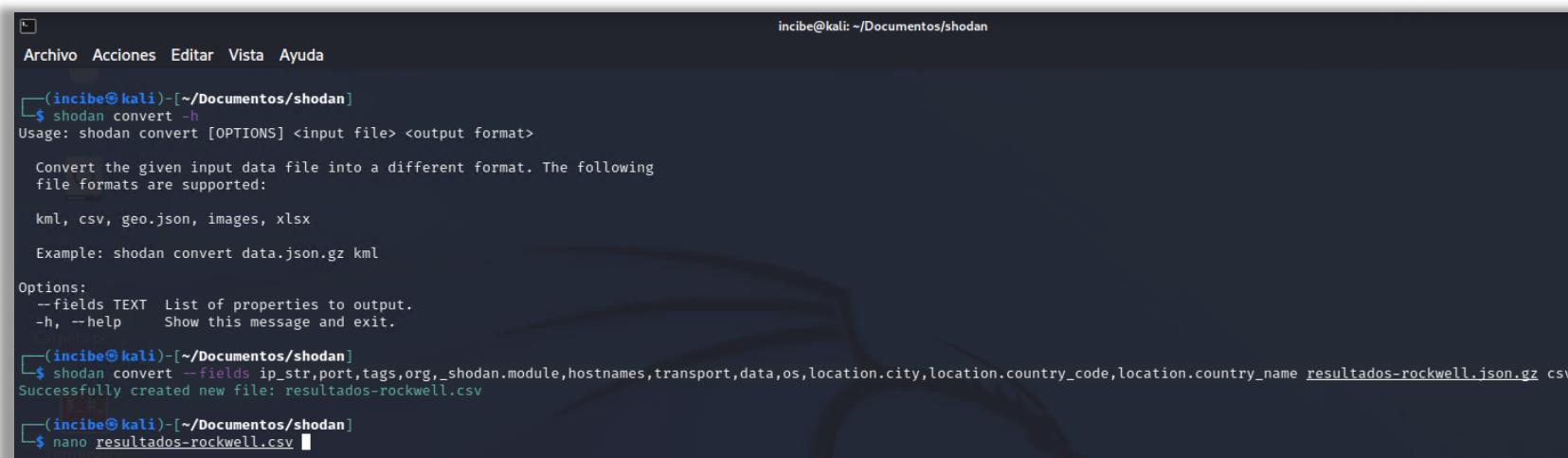
(incibe㉿kali)-[~/Documentos/shodan]
$
```

Ilustración 98:
Ejecución de
la ayuda con
«shodan
convert -h».

13

BÚSQUEDAS DESDE LA CLI: COMANDO CONVERT

- Convierte el archivo «resultados-rockwell.json.gz» descargado previamente, en un archivo con formato «CSV» con indicación de los campos que debe de contener. El archivo se creará en la misma carpeta en la que estaba el archivo anterior (carpeta «Shodan») y se creará con la extensión que hemos marcado (.csv).
 - **shodan convert --fields ip_str,port,tags,org,_shodan.module,hostnames,transport,data,os,location.city,location.country_code,location.country_name resultados-rockwell.json.gzcsv**



The terminal window shows the following session:

```
incibe@kali: ~/Documentos/shodan
$ shodan convert -h
Usage: shodan convert [OPTIONS] <input file> <output format>

Convert the given input data file into a different format. The following
file formats are supported:

kml, csv, geo.json, images, xlsx

Example: shodan convert data.json.gz kml

Options:
--fields TEXT List of properties to output.
-h, --help Show this message and exit.

incibe@kali:~/Documentos/shodan
$ shodan convert --fields ip_str,port,tags,org,_shodan.module,hostnames,transport,data,os,location.city,location.country_code,location.country_name resultados-rockwell.json.gz csv
Successfully created new file: resultados-rockwell.csv

incibe@kali:~/Documentos/shodan
$ nano resultados-rockwell.csv
```

Ilustración 99:
Conversión del
archivo
«resultados-
rockwell.json.gz»
descargado en un
archivo con
formato «CSV»

- El archivo generado tiene el nombre «resultados-rockwell.csv». Estos archivos .csv (*Comma Separated Values*), implica que son archivos de textos cuyos caracteres están separados por comas, convirtiéndolo en una especie de tabla en filas y columnas. Por ello, los archivos .csv son fáciles de ver y visualmente con una hoja de cálculo como Excel o Calc.

Este archivo puedes visualizarlo con el editor de texto *nano* (como ya hiciste en anteriores ocasiones), con el siguiente comando:

- ***nano resultados-rockwell.csv***

13

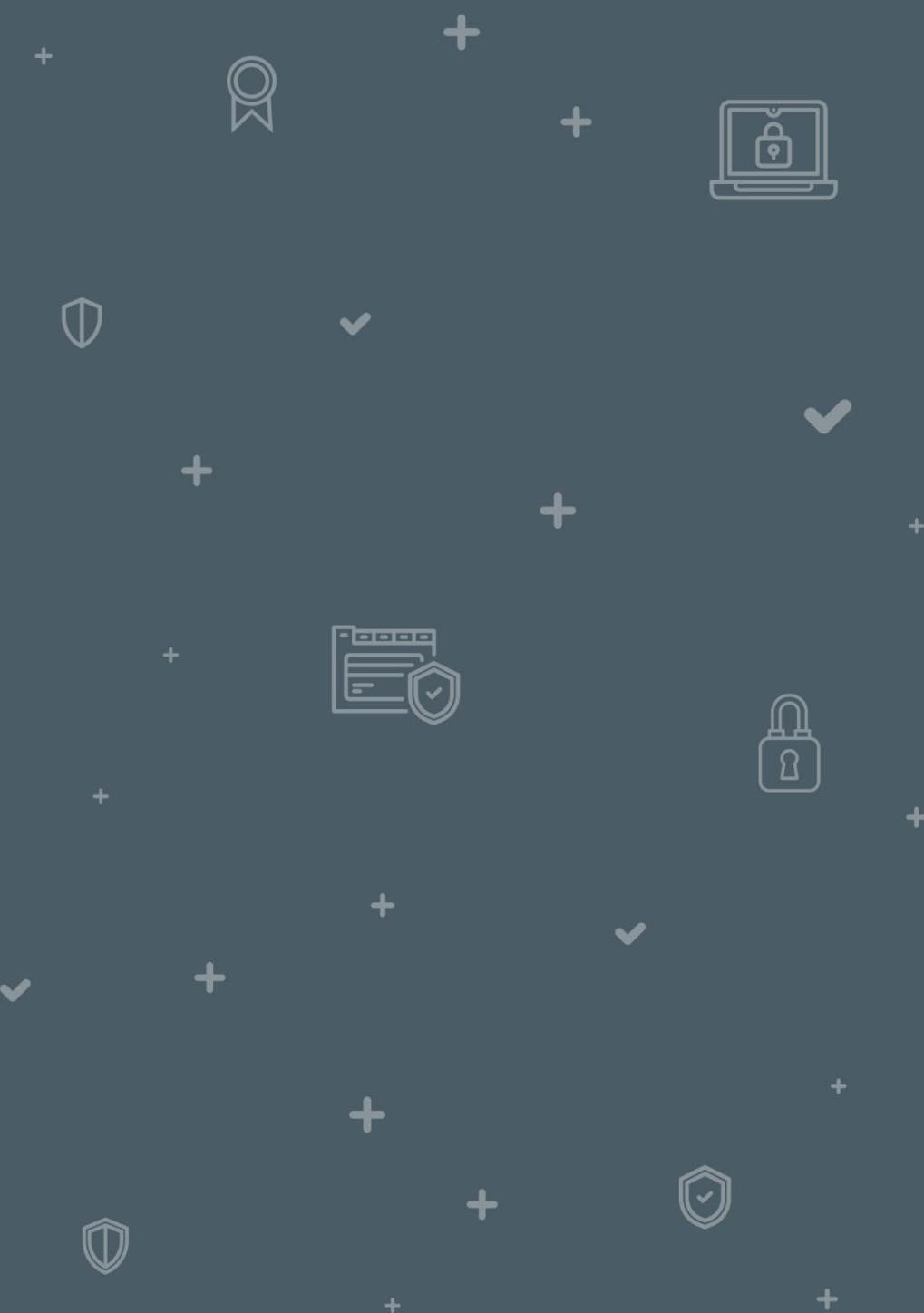
BÚSQUEDAS DESDE LA CLI: COMANDO CONVERT

```
incibe@kali: ~/Documentos/shodan
Archivo Acciones Editar Vista Ayuda
GNU nano 6.2
resultados-rockwell.csv
166.153.1.223,44818,,Service Provider Corporation,ethernetip-udp,223.sub-166-153-1.myvzw.com,udp,"Product name: 1769-L30ER/A LOGIX5330ER
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x60b38d0b
Device type: Programmable Logic Controller
Device IP: 172.19.109.5,,Euless,US,United States
63.41.196.98,44818,,Cellco Partnership DBA Verizon Wireless,ethernetip-udp,host98.sub-63-41-196.myvzw.com,udp,"Product name: 1766-L32BXBA C/21.02
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x60e79dff
Device type: Programmable Logic Controller
Device IP: 192.168.13.100,,Bell Buckle,US,United States
212.34.4.179,44818,ics,Jordan Telecommunications Company,ethernetip,,tcp,"Product name: 2080-LC20-20QWB
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x0022c4b1
Device type: Programmable Logic Controller
Device IP: 192.168.0.2,,Amman,JO,Jordan
166.239.119.6,44818,,Service Provider Corporation,ethernetip-udp,6.sub-166-239-119.myvzw.com,udp,"Product name: 1769-L30ER/A LOGIX5330ER
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x0187733
Device type: Programmable Logic Controller
Device IP: 10.10.6.10,,Euless,US,United States
63.46.201.229,44818,,Cellco Partnership DBA Verizon Wireless,ethernetip-udp,host229.sub-63-46-201.myvzw.com,udp,"Product name: 1763-L16BWA B/14.00
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x9ca0ec92
Device type: Communications Adapter
Device IP: 192.168.38.130,,Sunnyvale,US,United States
166.149.208.82,44818,ics,Service Provider Corporation,ethernetip,82.sub-166-149-208.myvzw.com,tcp,"Product name: 1769-L16ER/B LOGIX5316ER
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x60d06f67
Device type: Programmable Logic Controller
Device IP: 192.168.0.2,,Idabel,US,United States
166.148.119.123,44818,ics,Service Provider Corporation,ethernetip,123.sub-166-148-119.myvzw.com,tcp,"Product name: 1766-L32BXB B/15.00
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x40652229
Device type: Programmable Logic Controller
Device IP: 192.168.1.2,,Twin Oaks,US,United States
96.1.77.85,44818,ics,TELUS Communications Inc.,ethernetip,96-1-77-85-staticipwest.wireless.telus.com,tcp,"Product name: 1769-L19ER-BB1B/A LOGIX5319ER
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x0ec8ee9
Device type: Programmable Logic Controller
Device IP: 10.8.1.7,,Cheney,US,United States
166.166.53.189,44818,,Service Provider Corporation,ethernetip-udp,189.sub-166-166-53.myvzw.com,udp,"Product name: 5069-L306ER/A
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x60c707e6
Device type: Programmable Logic Controller
Device IP: 192.168.100.2,,Euless,US,United States
166.251.157.103,44818,ics,Service Provider Corporation,ethernetip,103.sub-166-251-157.myvzw.com,tcp,"Product name: 1766-L32BXBA C/21.02
Vendor ID: Rockwell Automation/Allen-Bradley
[ 496 líneas leídas ]
^G Ayuda      ^O Guardar     ^W Buscar      ^K Cortar      ^E Ejecutar      ^C Ubicación      M-U Deshacer      M-A Poner marca      M-] A llave      M-Q Anterior      ^B Atrás      ^P Palabr ant
^X Salir      ^R Leer fich.   ^Y Reemplazar   ^U Pegar       ^J Justificar    ^/ Ir a linea     M-E Rehacer      M-6 Copiar       M-Q Buscar atrás  M-W Siguiente    ^F Adelante    ^D Palabr sig
```

Ilustración 100: Editor de texto *nano* utilizado para ver el archivo CSV.

BÚSQUEDAS DESDE LA CLI: COMANDOS *HOST* Y *HONEYSCORE*

14



Ahora, vas a cambiar la búsqueda. En lugar de obtener información sobre dispositivos, vas a consultar qué información tiene Shodan sobre una determinada dirección IP. Para ello se utiliza el comando ***host***. También utilizaremos el comando ***honeyscore***, que va a ayudar a tratar de identificar si una determinada dirección IP o *host*, es un *honeypot* (sistema trampa o señuelo que simula ser un dispositivo determinado).

- Con el siguiente comando, consultas la información que la base de datos de Shodan contiene sobre una determinada dirección IP. Con este comando vamos a poder ver información sobre el *hostname*, la organización, país, ciudad y los puertos abiertos, pudiendo ver primero el número de puertos y luego el listado de ellos.
 - **shodan host 5.183.108.29**



incibe@kali: ~/Documentos/shodan

Archivo Acciones Editar Vista Ayuda

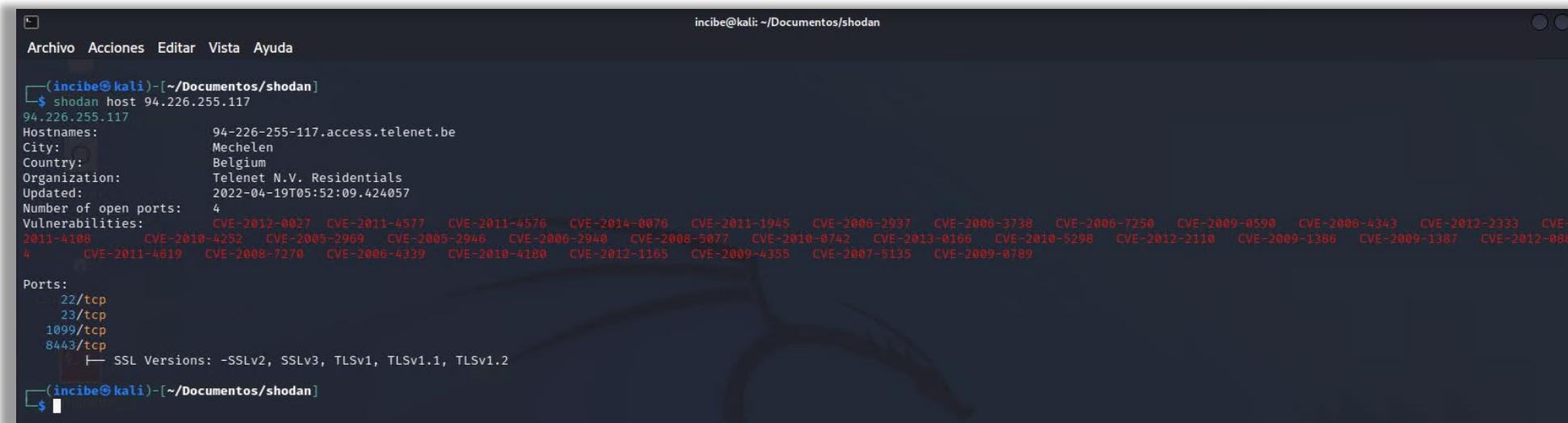
```
└─(incibe㉿kali)-[~/Documentos/shodan]
  └─$ shodan host 5.183.108.29
  5.183.108.29
    Hostnames:          108-29.customer.connextra.it
    City:               Rome
    Country:            Italy
    Organization:       CONNEXTRA S.R.L
    Updated:            2022-04-25T12:01:50.373319
    Number of open ports: 5

    Ports:
      22/tcp Dropbear sshd (2017.75)
      80/tcp
      81/tcp
      102/tcp
      161/udp

  └─(incibe㉿kali)-[~/Documentos/shodan]
  └─$
```

Ilustración 101: Búsqueda con Shodan sobre información una determinada dirección IP.

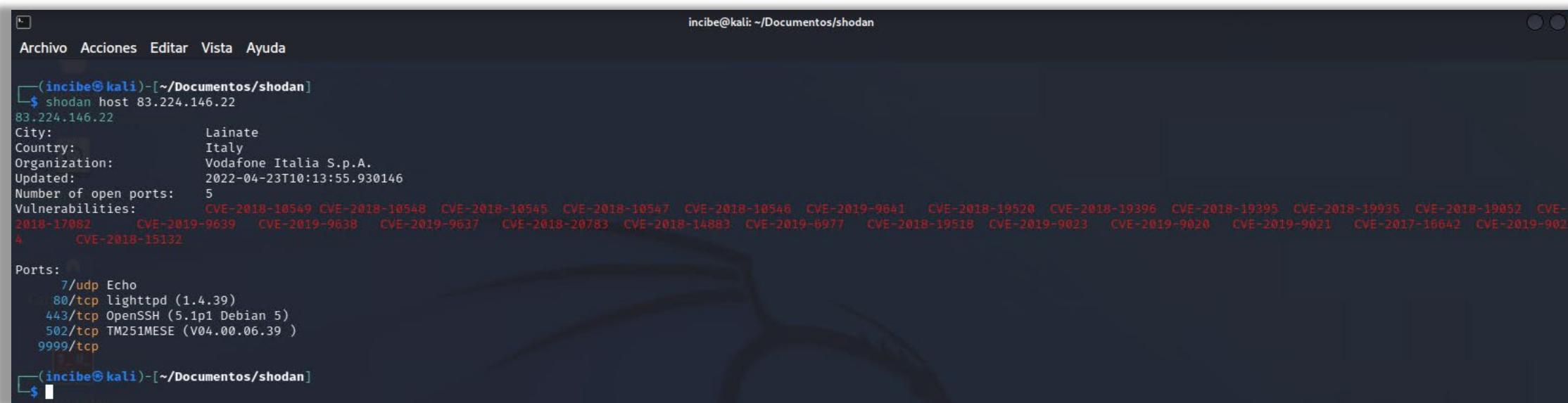
- En el caso de que a ese *host* se le haya identificado alguna vulnerabilidad, aparecerán estas en color rojo indicando el CVE de la vulnerabilidad identificada. Esto lo puedes observar con la ejecución del siguiente comando:
 - shodan host 94.226.255.117



```
incibe@kali: ~/Documentos/shodan
$ shodan host 94.226.255.117
94.226.255.117
Hostnames: 94-226-255-117.access.telenet.be
City: Mechelen
Country: Belgium
Organization: Telenet N.V. Residential
Updated: 2022-04-19T05:52:09.424057
Number of open ports: 4
Vulnerabilities: CVE-2012-0027 CVE-2011-4577 CVE-2011-4576 CVE-2014-0076 CVE-2011-1945 CVE-2006-2937 CVE-2006-3738 CVE-2006-7250 CVE-2009-0590 CVE-2006-4343 CVE-2012-2333 CVE-2011-4108 CVE-2010-4252 CVE-2005-2959 CVE-2005-2946 CVE-2006-2940 CVE-2008-5077 CVE-2010-0742 CVE-2012-0166 CVE-2010-5298 CVE-2012-2110 CVE-2009-1386 CVE-2009-1387 CVE-2012-0884 CVE-2011-4619 CVE-2008-7270 CVE-2006-4339 CVE-2010-4180 CVE-2012-1165 CVE-2009-4355 CVE-2007-5135 CVE-2009-0789
Ports:
 22/tcp
 23/tcp
 1099/tcp
 8443/tcp
  └-- SSL Versions: -SSLv2, SSLv3, TLSv1, TLSv1.1, TLSv1.2
incibe@kali: ~/Documentos/shodan
$
```

Ilustración 102: La vulnerabilidad aparece en color rojo.

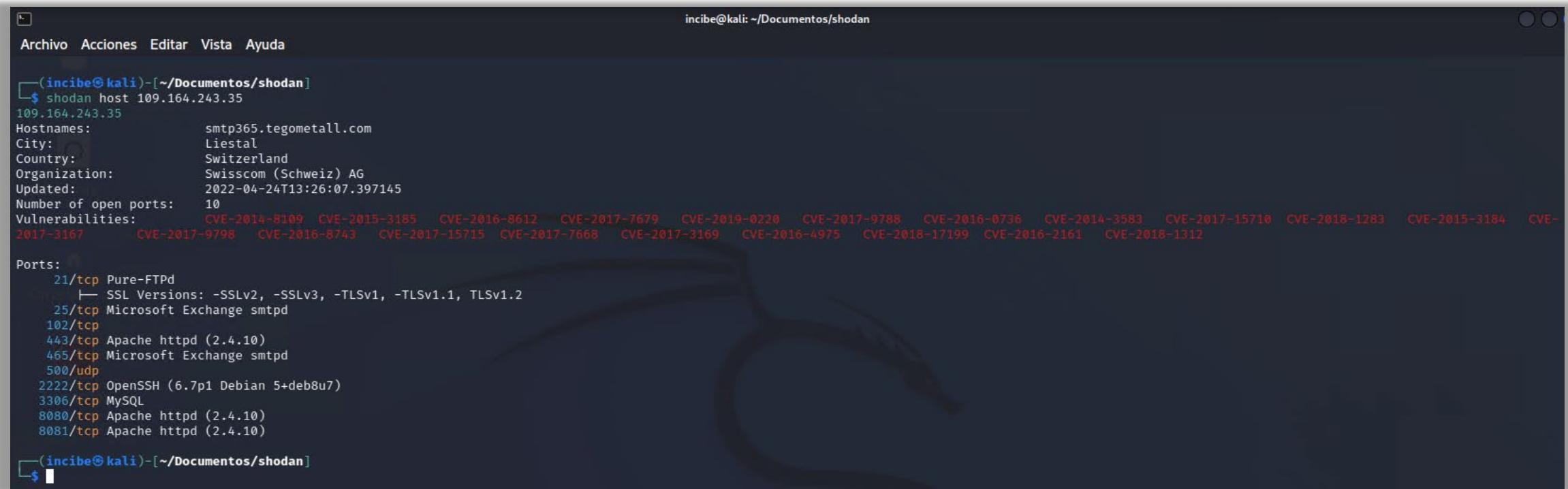
- En las siguientes imágenes se muestra información de diferentes *hosts* a los que se les ha detectado puertos abiertos utilizados normalmente por protocolos industriales (puertos como el 102, 502, 44818, etc.) y, en algunos casos, también se muestran vulnerabilidades detectadas en el *host*.



The screenshot shows a terminal window on a Kali Linux system. The user has run the command `shodan host 83.224.146.22`. The output provides detailed information about the host:

- Address:** 83.224.146.22
- Location:** Lainate, Italy, Vodafone Italia S.p.A.
- Updated:** 2022-04-23T10:13:55.930146
- Open ports:** 5 (including 7/udp Echo, 80/tcp lighttpd (1.4.39), 443/tcp OpenSSH (5.1p1 Debian 5), 502/tcp TM251MESE (V04.00.06.39), 9999/tcp)
- Vulnerabilities:** A long list of CVE IDs including CVE-2018-10549, CVE-2018-10548, CVE-2018-10545, CVE-2018-10547, CVE-2018-10546, CVE-2019-9641, CVE-2018-19520, CVE-2018-19396, CVE-2018-19395, CVE-2018-19935, CVE-2018-19052, CVE-2018-17082, CVE-2019-9639, CVE-2019-9638, CVE-2019-9637, CVE-2018-20783, CVE-2018-14883, CVE-2019-6977, CVE-2018-19518, CVE-2019-9023, CVE-2019-9020, CVE-2019-9021, CVE-2017-16642, CVE-2019-9024, and CVE-2018-15132.

Ilustración 103: *Host* a los que se les ha detectado puertos abiertos utilizados normalmente con protocolos industriales. País: Italia.



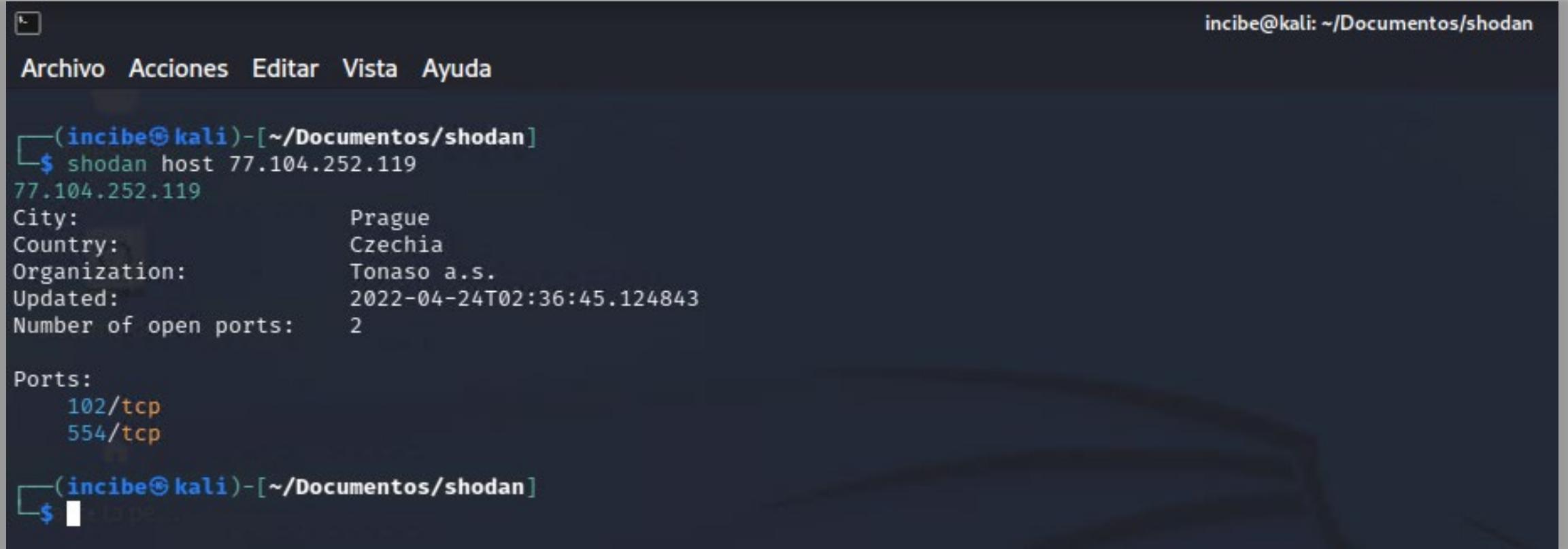
```
(incibe㉿kali)-[~/Documentos/shodan]
$ shodan host 109.164.243.35
109.164.243.35
Hostnames: smtp365.tegometall.com
City: Liestal
Country: Switzerland
Organization: Swisscom (Schweiz) AG
Updated: 2022-04-24T13:26:07.397145
Number of open ports: 10
Vulnerabilities: CVE-2014-8109 CVE-2015-3185 CVE-2016-8612 CVE-2017-7679 CVE-2019-0220 CVE-2017-9788 CVE-2016-0736 CVE-2014-3583 CVE-2017-15710 CVE-2018-1283 CVE-2015-3184 CVE-2017-3167 CVE-2017-9798 CVE-2016-8743 CVE-2017-15715 CVE-2017-7668 CVE-2017-3169 CVE-2016-4975 CVE-2018-17199 CVE-2016-2161 CVE-2018-1312

Ports:
21/tcp Pure-FTPd
└─ SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, TLSv1.2
25/tcp Microsoft Exchange smtpd
102/tcp
443/tcp Apache httpd (2.4.10)
465/tcp Microsoft Exchange smtpd
500/udp
2222/tcp OpenSSH (6.7p1 Debian 5+deb8u7)
3306/tcp MySQL
8080/tcp Apache httpd (2.4.10)
8081/tcp Apache httpd (2.4.10)

(incibe㉿kali)-[~/Documentos/shodan]
```

Ilustración 104: *Hosts* a los que se les ha detectado puertos abiertos utilizados normalmente con protocolos industriales. País: Suiza.

14 BÚSQUEDAS DESDE LA CLI: COMANDOS HOST Y HONEYSCORE



```
incibe@kali: ~/Documentos/shodan
Archivo  Acciones  Editar  Vista  Ayuda

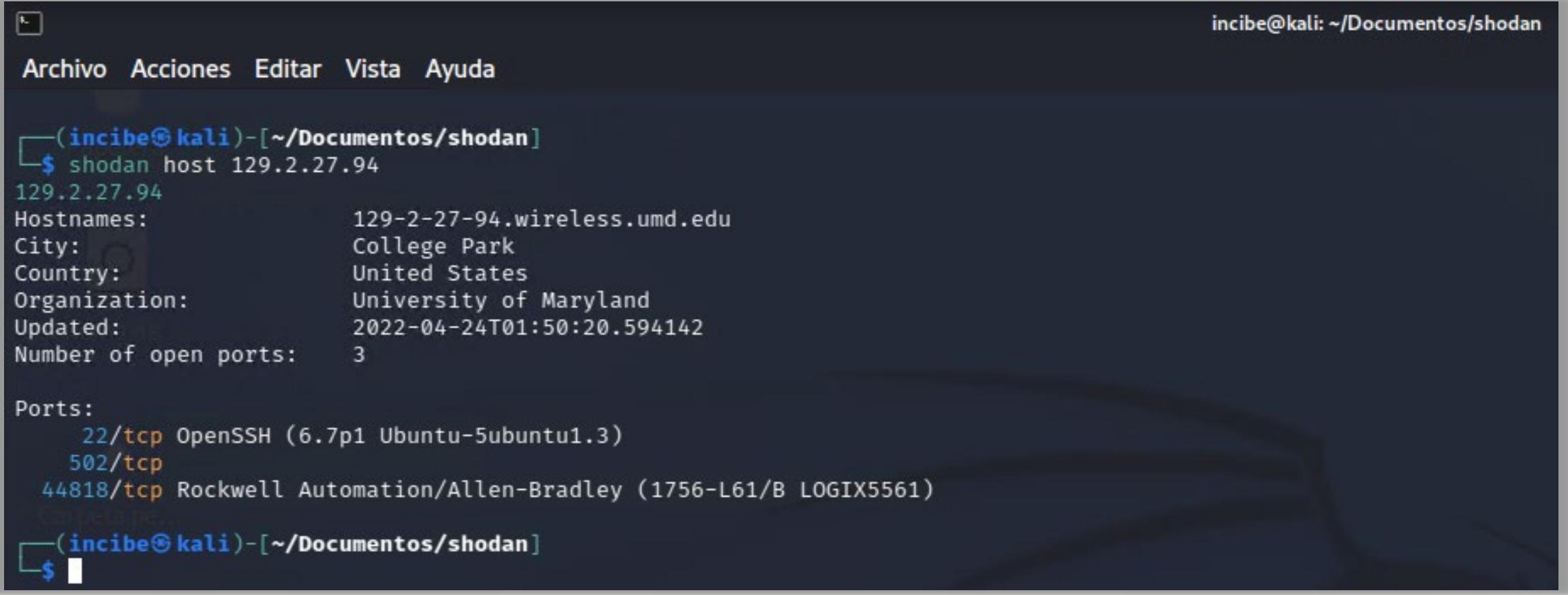
└──(incibe㉿kali)-[~/Documentos/shodan]
$ shodan host 77.104.252.119
77.104.252.119
City: Prague
Country: Czechia
Organization: Tonaso a.s.
Updated: 2022-04-24T02:36:45.124843
Number of open ports: 2

Ports:
  102/tcp
  554/tcp

└──(incibe㉿kali)-[~/Documentos/shodan]
$
```

Ilustración 105: *Hosts* a los que se les ha detectado puertos abiertos utilizados normalmente con protocolos industriales. País: República Checa.

14 BÚSQUEDAS DESDE LA CLI: COMANDOS HOST Y HONEYSCORE



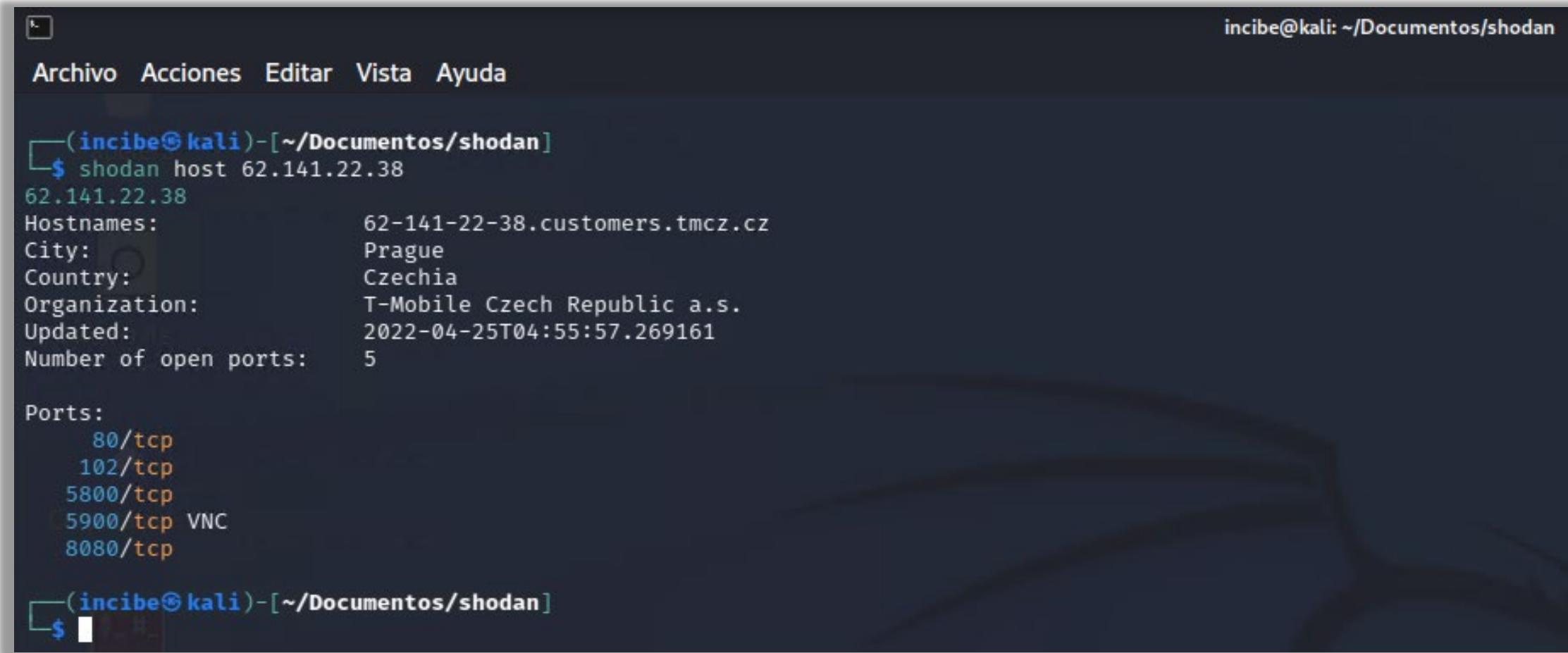
```
incibe@kali: ~/Documentos/shodan
Archivo Acciones Editar Vista Ayuda

└─(incibe㉿kali)-[~/Documentos/shodan]
$ shodan host 129.2.27.94
129.2.27.94
Hostnames: 129-2-27-94.wireless.umd.edu
City: College Park
Country: United States
Organization: University of Maryland
Updated: 2022-04-24T01:50:20.594142
Number of open ports: 3

Ports:
  22/tcp OpenSSH (6.7p1 Ubuntu-5ubuntu1.3)
  502/tcp
  44818/tcp Rockwell Automation/Allen-Bradley (1756-L61/B LOGIX5561)

└─(incibe㉿kali)-[~/Documentos/shodan]
$
```

Ilustración 106: Hosts a los que se les ha detectado puertos abiertos utilizados normalmente con protocolos industriales. País: Estados Unidos.



incibe@kali: ~/Documentos/shodan

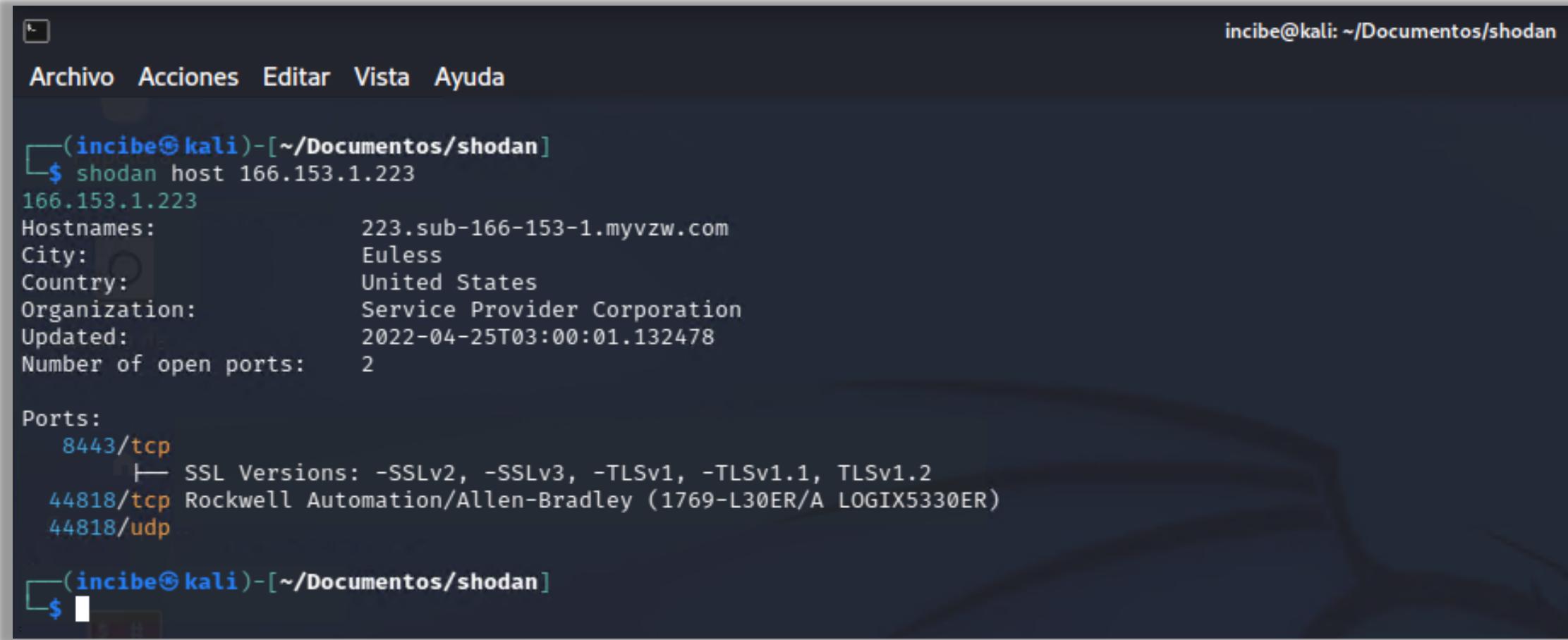
Archivo Acciones Editar Vista Ayuda

```
└──(incibe㉿kali)-[~/Documentos/shodan]
  └─$ shodan host 62.141.22.38
  62.141.22.38
    Hostnames:          62-141-22-38.customers.tmcz.cz
    City:               Prague
    Country:            Czechia
    Organization:       T-Mobile Czech Republic a.s.
    Updated:            2022-04-25T04:55:57.269161
    Number of open ports: 5

    Ports:
      80/tcp
      102/tcp
      5800/tcp
      5900/tcp VNC
      8080/tcp

  └──(incibe㉿kali)-[~/Documentos/shodan]
  └─$
```

Ilustración 107: *Hosts* a los que se les ha detectado puertos abiertos utilizados normalmente con protocolos industriales. País: República Checa.

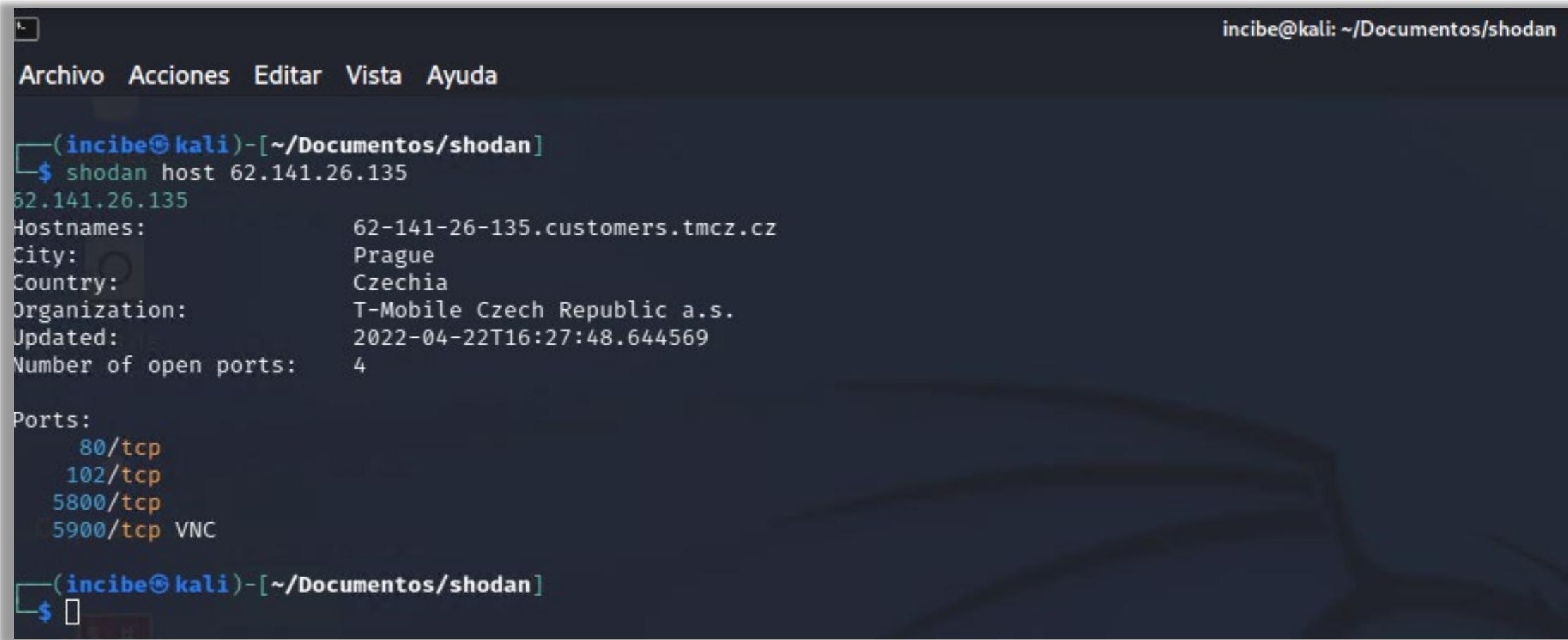


```
incibe@kali: ~/Documentos/shodan
Archivo  Acciones  Editar  Vista  Ayuda
└──(incibe㉿kali)-[~/Documentos/shodan]
    $ shodan host 166.153.1.223
166.153.1.223
Hostnames:          223.sub-166-153-1.myvzw.com
City:               Euless
Country:            United States
Organization:       Service Provider Corporation
Updated:            2022-04-25T03:00:01.132478
Number of open ports: 2

Ports:
  8443/tcp
    └── SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, TLSv1.2
  44818/tcp Rockwell Automation/Allen-Bradley (1769-L30ER/A LOGIX5330ER)
  44818/udp

└──(incibe㉿kali)-[~/Documentos/shodan]
    $
```

Ilustración 108: *Hosts* a los que se les ha detectado puertos abiertos utilizados normalmente con protocolos industriales. País: Estados Unidos.



```
incibe@kali: ~/Documentos/shodan
Archivo  Acciones  Editar  Vista  Ayuda

└──(incibe㉿kali)-[~/Documentos/shodan]
    $ shodan host 62.141.26.135
62.141.26.135
Hostnames:          62-141-26-135.customers.tmcz.cz
City:               Prague
Country:            Czechia
Organization:       T-Mobile Czech Republic a.s.
Updated:            2022-04-22T16:27:48.644569
Number of open ports: 4

Ports:
      80/tcp
      102/tcp
      5800/tcp
      5900/tcp VNC

└──(incibe㉿kali)-[~/Documentos/shodan]
    $ 
```

Ilustración 109: *Hosts* a los que se les ha detectado puertos abiertos utilizados normalmente con protocolos industriales. País: República Checa.

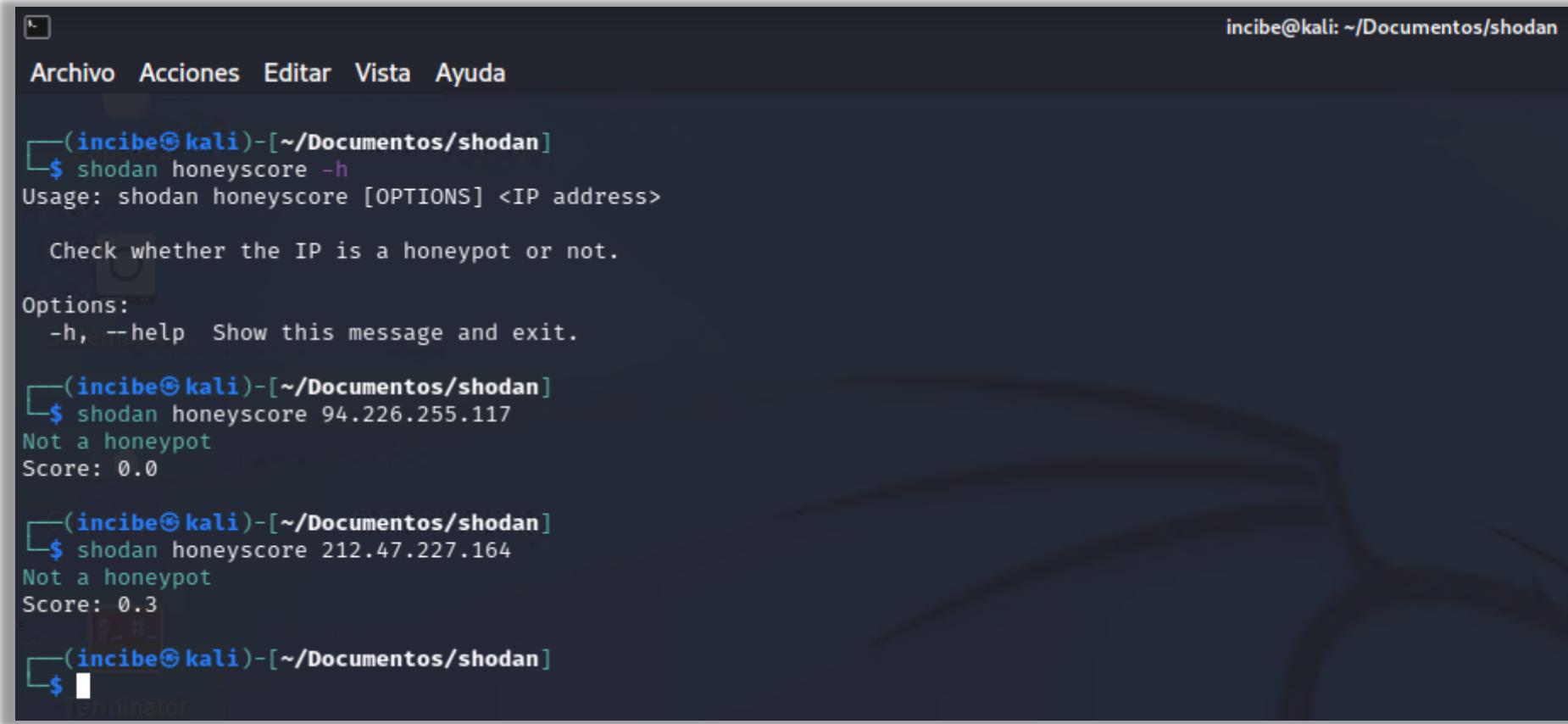
14 BÚSQUEDAS DESDE LA CLI: COMANDOS *HOST* Y *HONEYSCORE*

Por otro lado, para detectar si un sistema es un *honeypot* y simula ser un dispositivo (como por ejemplo un PLC industrial), se utiliza el siguiente comando:

- **shodan honeyscore dirección IP**
- En la imagen que verás en la siguiente diapositiva, puedes observar la ejecución del comando **Shodan honeyscore -h**, que nos muestra más información del comando que podemos utilizar. Luego hemos ejecutado el comando anterior para dos *hosts* diferentes, donde uno de ellos alcanza una puntuación de 0.3 (aunque Shodan no lo identifica como un *honeypot*). El rango puede ir desde 0.0 a 1.0, donde si llega a 1.0 es que se considera un *honeypot*.

14

BÚSQUEDAS DESDE LA CLI: COMANDOS *HOST* Y *HONEYSCORE*



```
incibe@kali: ~/Documentos/shodan
Archivo  Acciones  Editar  Vista  Ayuda

└──(incibe㉿kali)-[~/Documentos/shodan]
$ shodan honeyscore -h
Usage: shodan honeyscore [OPTIONS] <IP address>

    Check whether the IP is a honeypot or not.

Options:
  -h, --help  Show this message and exit.

└──(incibe㉿kali)-[~/Documentos/shodan]
$ shodan honeyscore 94.226.255.117
Not a honeypot
Score: 0.0

└──(incibe㉿kali)-[~/Documentos/shodan]
$ shodan honeyscore 212.47.227.164
Not a honeypot
Score: 0.3

└──(incibe㉿kali)-[~/Documentos/shodan]
$ █
Terminator
```

Ilustración 110: Detectar si un sistema es un *honeypot* y simula ser un dispositivo.

15

EJERCICIO PRÁCTICO 1

- 15.1 Enunciado
- 15.2 Solución



15 EJERCICIO PRÁCTICO 1

15.1 Enunciado ejercicio práctico 1



Con todo lo aprendido anteriormente, realiza una búsqueda de dispositivos industriales Omron utilizando la herramienta CLI de Shodan desde Kali Linux, siguiendo los siguientes pasos.

- Enumera los dispositivos que contienen el término de búsqueda «Omron», indicando la cantidad de dispositivos encontrados.
- Muestra la estadística del *Top* de puertos más utilizados para la anterior búsqueda e indica cuál es el puerto más utilizado.
- Continuando con la misma búsqueda, de todos los resultados obtenidos, muestra los 100 primeros resultados que contengan los siguientes campos: *ip_str*, *port*, *tags*, *hostnames*, *data* y *location*.

15 EJERCICIO PRÁCTICO 1

15.1 Enunciado ejercicio práctico 1

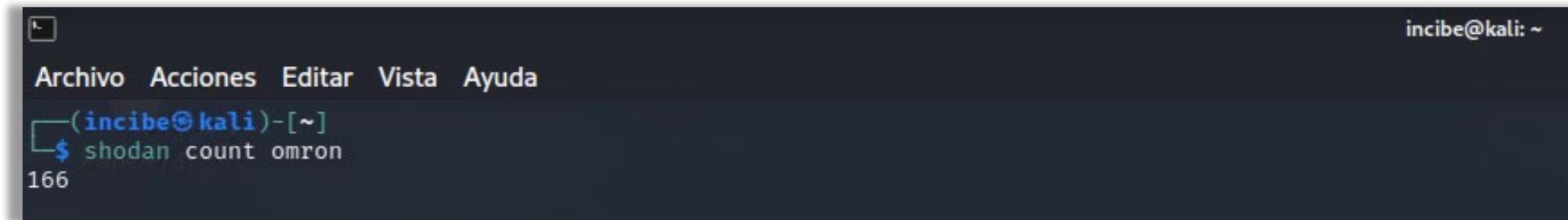
- Descarga los 100 primeros resultados de la búsqueda de dispositivos Omron, en la carpeta «shodan» (creada anteriormente).
- Realiza una búsqueda local, utilizando el archivo descargado, filtrando por el puerto más utilizado que identificamos en el segundo punto y muestra solo los siguientes campos: *ip_str, port, tags, _shodan.module, hostnames, transport, data, os, location.city, location.country_code, location.country_name*.

Nota: es posible que no obtengamos información de todos los campos (algo habitual en dispositivos industriales).

15 EJERCICIO PRÁCTICO 1

15.2 Solución ejercicio práctico 1

- Enumera los dispositivos que contienen el término de búsqueda «Omron», indicando la cantidad de dispositivos encontrados.
 - **shodan count Omron**



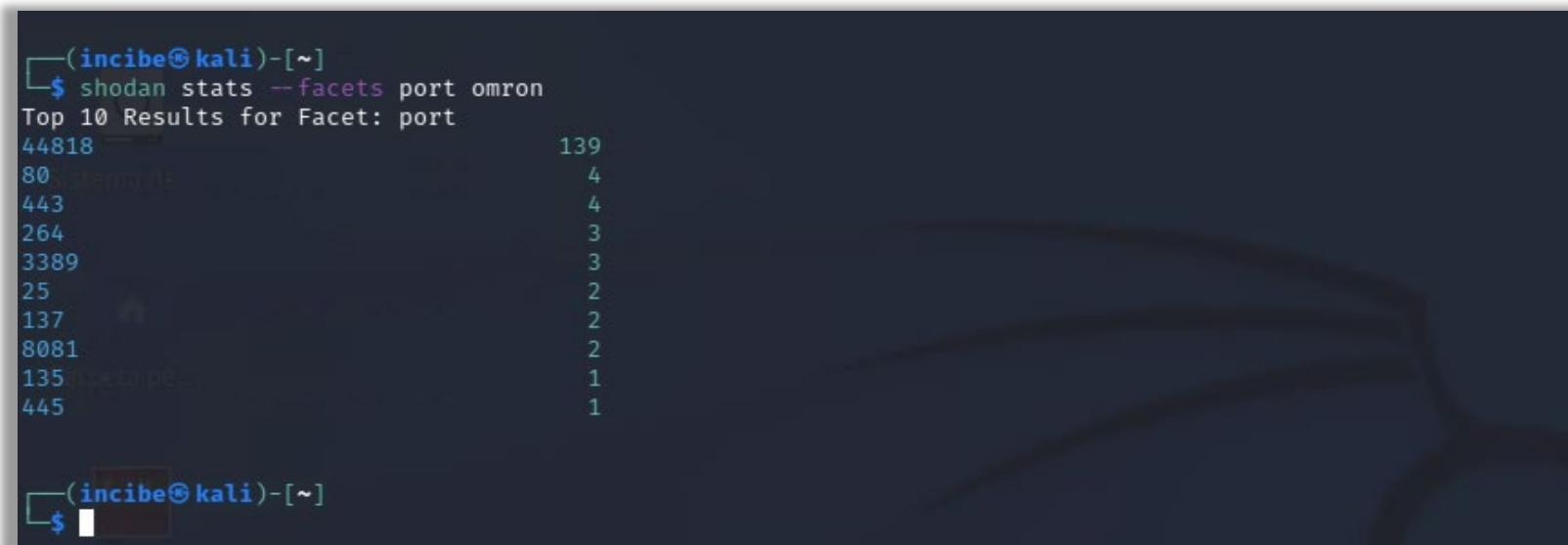
A terminal window with a dark background and light-colored text. The window title bar says 'incibe@kali: ~'. The menu bar includes 'Archivo', 'Acciones', 'Editar', 'Vista', and 'Ayuda'. Below the menu is a command-line interface with a blue cursor. The command entered is '\$ shodan count omron'. The output of the command is '166'.

Ilustración 111: Término de búsqueda «Omron» y del número de dispositivos encontrados.

15 EJERCICIO PRÁCTICO 1

15.2 Solución ejercicio práctico 1

- Muestra la estadística del *top* de puertos más utilizados para la anterior búsqueda e indica cual es el puerto más utilizado.
 - shodan *stats --facets port Omron*



```
(incibe㉿kali)-[~]
└─$ shodan stats --facets port omron
Top 10 Results for Facet: port
44818          139
80              4
443             4
264             3
3389            3
25              2
137             2
8081            2
135             1
445             1

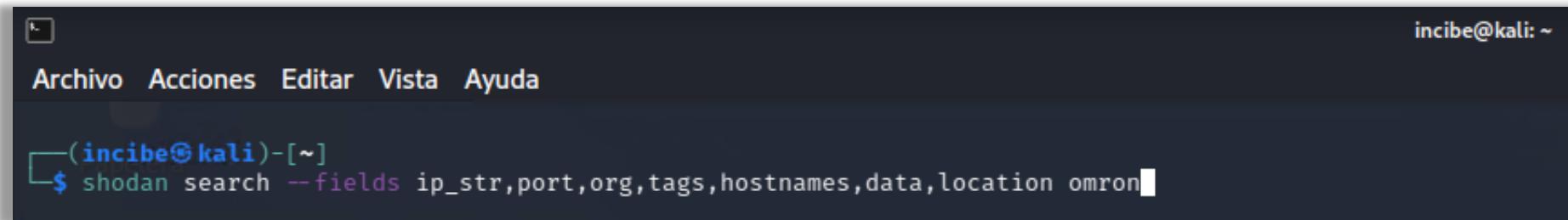
(incibe㉿kali)-[~]
└─$
```

Ilustración 112: Estadística de los puertos más utilizados.

15 EJERCICIO PRÁCTICO 1

15.2 Solución ejercicio práctico 1

- Continuando con la misma búsqueda, de todos los resultados obtenidos, muestra los 100 primeros resultados que contengan los siguientes campos: *ip_str, port, tags, hostnames, data* y *location*.
 - shodan **search --fields ip_str, port, org, tags, hostnames, data, location Omron**



A screenshot of a terminal window titled 'incibe@kali: ~'. The window has a dark background and light-colored text. At the top, there's a menu bar with options: Archivo, Acciones, Editar, Vista, Ayuda. Below the menu, the terminal prompt shows '(incibe@kali)-[~]'. A command is being typed into the terminal: '\$ shodan search --fields ip_str, port, org, tags, hostnames, data, location omron'. The cursor is positioned at the end of the command.

Ilustración 113: Campos *ip_str, port, tags, hostnames, data* y *location*.

15 EJERCICIO PRÁCTICO 1

15.2 Solución ejercicio práctico 1

```
incibe@kali:~  
Archivo Acciones Editar Vista Ayuda  
166.250.81.162 44818 Service Provider Corporation ics 162.sub-166-250-81.myvzw.com Product name: NJ101\nVendor ID: Omron Corporation\nSerial number: 0x01662ae5\nDevice type: Communications Adapter\nDevice IP: 192.168.0.3 {'city': 'Evergreen', 'region_code': 'CO', 'area_code': None, 'longitude': -105.31721, 'latitude': 39.63332, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'}  
220.130.225.22 44818 Chunghwa Telecom Co.,Ltd. ics 220-130-225-22.hinet-ip.hinet.net Product name: CJ2M-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x00f8553b\nDevice type: Communications Adapter\nDevice IP: 220.130.225.22 {'city': 'Taoyuan City', 'region_code': '04', 'area_code': None, 'longitude': 121.29696, 'latitude': 24.99368, 'postal_code': None, 'country_code': 'TW', 'country_name': 'Taiwan'}  
2.83.16.238 44818 PT Comunicaciones S.A. bl22-16-238.dsl.telepac.pt Product name: CJ2M-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x019ceb9d\nDevice type: Communications Adapter\nDevice IP: 192.168.82.9 {'city': 'Barcouço', 'region_code': '01', 'area_code': None, 'longitude': -8.4967, 'latitude': 40.2989, 'postal_code': None, 'country_code': 'PT', 'country_name': 'Portugal'}  
194.158.12.38 80 BWISE BV randstad-test.bwise.net HTTP/1.1 301 Moved Permanently\r\nDate: Sun, 24 Apr 2022 01:39:51 GMT\r\nServer: Apache\r\nLocation: https://omron-test.bwise.net:443/\r\nContent-Length: 241\r\nContent-Type: text/html; charset=iso-8859-1\r\n\r\n{'city': 'Amsterdam', 'region_code': 'NH', 'area_code': None, 'longitude': 4.88969, 'latitude': 52.37403, 'postal_code': None, 'country_code': 'NL', 'country_name': 'Netherlands'}  
220.128.138.124 44818 Chunghwa Telecom Co.,Ltd. ics 220-128-138-124.hinet-ip.hinet.net Product name: CJ2M-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x00fb8e91\nDevice type: Communications Adapter\nDevice IP: 220.128.138.124 {'city': 'Taipei', 'region_code': '04', 'area_code': None, 'longitude': 121.53185, 'latitude': 25.04776, 'postal_code': None, 'country_code': 'TW', 'country_name': 'Taiwan'}  
77.18.159.245 44818 Telenor Norge AS 77.18.159.245.telenormobil.no Product name: NX102-1000\nVendor ID: Omron Corporation\nSerial number: 0x016a2944\nDevice type: Communications Adapter\nDevice IP: 192.168.1.90 {'city': 'Sandsls', 'region_code': '46', 'area_code': None, 'longitude': 5.28554, 'latitude': 60.30323, 'postal_code': None, 'country_code': 'NO', 'country_name': 'Norway'}  
130.238.122.253 44818 Swedish University of Agricultural Sciences plc001.vhi.slu.se Product name: NJ101\nVendor ID: Omron Corporation\nSerial number: 0x01097b6c\nDevice type: Communications Adapter\nDevice IP: 130.238.122.253 {'city': 'Uppsala', 'region_code': 'C', 'area_code': None, 'longitude': 17.63889, 'latitude': 59.85882, 'postal_code': None, 'country_code': 'SE', 'country_name': 'Sweden'}  
46.66.175.106 44818 Telenor Norge AS 46.66.175.106.telenormobil.no Product name: NX102-1000\nVendor ID: Omron Corporation\nSerial number: 0x016a2949\nDevice type: Communications Adapter\nDevice IP: 192.168.1.90 {'city': 'Sandsls', 'region_code': '46', 'area_code': None, 'longitude': 5.28554, 'latitude': 60.30323, 'postal_code': None, 'country_code': 'NO', 'country_name': 'Norway'}  
210.242.156.74 44818 Chunghwa Telecom Co.,Ltd. 210-242-156-74.hinet-ip.hinet.net Product name: CJ2M-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x00f93be3\nDevice type: Communications Adapter\nDevice IP: 210.242.156.74 {'city': 'Taipei', 'region_code': '04', 'area_code': None, 'longitude': 121.53185, 'latitude': 25.04776, 'postal_code': None, 'country_code': 'TW', 'country_name': 'Taiwan'}  
125.227.227.249 44818 Chunghwa Telecom Co.,Ltd. ics 125-227-227-249.hinet-ip.hinet.net Product name: NX1P2\nVendor ID: Omron Corporation\nSerial number: 0x01339ac3\nDevice type: Communications Adapter\nDevice IP: 125.227.227.249 {'city': 'Kaohsiung', 'region_code': 'KHH', 'area_code': None, 'longitude': 120.31333, 'latitude': 22.61626, 'postal_code': None, 'country_code': 'TW', 'country_name': 'Taiwan'}  
46.66.183.164 44818 Telenor Norge AS ics 46.66.183.164.telenormobil.no Product name: NX102-9000\nVendor ID: Omron Corporation\nSerial number: 0x016a3845\nDevice type: Communications Adapter\nDevice IP: 192.168.1.90 {'city': 'Oslo', 'region_code': '03', 'area_code': None, 'longitude': 10.74609, 'latitude': 59.91273, 'postal_code': None, 'country_code': 'NO', 'country_name': 'Norway'}  
142.112.0.93 44818 Bell Canada ipagstacip-6afla8e5-f36a-7ab8-6f86-1d6dbf7dc360.sdsbell.ca Product name: CJ2M-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x00fa83f6\nDevice type: Communications Adapter\nDevice IP: 192.168.4.20 {'city': 'Québec', 'region_code': 'QC', 'area_code': None, 'longitude': -71.2453, 'latitude': 46.7933, 'postal_code': None, 'country_code': 'CA', 'country_name': 'Canada'}  
61.219.241.219 44818 Data Communication Business Group, 61-219-241-219.hinet-ip.hinet.net Product name: NX1P2\nVendor ID: Omron Corporation\nSerial number: 0x01339ab7\nDevice type: Communications Adapter\nDevice IP: 61.219.241.219 {'city': 'Taipei', 'region_code': '04', 'area_code': None, 'longitude': 121.53185, 'latitude': 25.04776, 'postal_code': None, 'country_code': 'TW', 'country_name': 'Taiwan'}  
61.219.241.81 44818 Data Communication Business Group, ics 61-219-241-81.hinet-ip.hinet.net Product name: NX1P2\nVendor ID: Omron Corporation\nSerial number: 0x01339ac7\nDevice type: Communications Adapter\nDevice IP: 61.219.241.81 {'city': 'Kaohsiung', 'region_code': 'KHH', 'area_code': None, 'longitude': 120.31333, 'latitude': 22.61626, 'postal_code': None, 'country_code': 'TW', 'country_name': 'Taiwan'}  
223.200.72.4 44818 Government Service Network (GSN) ics 223-200-72-4.hinet-ip.hinet.net Product name: CJ2M-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x00fce87c\nDevice type: Communications Adapter\nDevice IP: 223.200.72.4 {'city': 'Fengshan', 'region_code': 'KHH', 'area_code': None, 'longitude': 120.36126, 'latitude': 22.62659, 'postal_code': None, 'country_code': 'TW', 'country_name': 'Taiwan'}  
166.250.81.161 44818 Service Provider Corporation 161.sub-166-250-81.myvzw.com Product name: NJ101-9000\nVendor ID: Omron Corporation\nSerial number: 0x0109583b\nDevice type: Communications Adapter\nDevice IP: 192.168.0.3 {'city': 'Evergreen', 'region_code': 'CO', 'area_code': None, 'longitude': -105.31721, 'latitude': 39.63332, 'postal_code': None, 'country_code': 'US', 'country_name': 'United States'}  
77.16.8.77 44818 Telenor Norge AS 77.16.8.77.telenormobil.no Product name: NX102-1000\nVendor ID: Omron Corporation\nSerial number: 0x016a2944\nDevice type: Communications Adapter\nDevice IP: 192.168.1.90 {'city': 'Volda', 'region_code': '15', 'area_code': None, 'longitude': 6.07108, 'latitude': 62.146, 'postal_code': None, 'country_code': 'NO', 'country_name': 'Norway'}
```

Ilustración 114: Resultados de la búsqueda anterior.

15 EJERCICIO PRÁCTICO 1

15.2 Solución ejercicio práctico 1

- Descarga el resultado de la búsqueda de dispositivos Omron, en la carpeta «shodan» (creada anteriormente).
 - **shodan download resultados-ejercicio.json.gz omron**



```
incibe@kali: ~/Documentos/shodan
Archivo  Acciones  Editar  Vista  Ayuda
└──(incibe㉿kali)-[~]
    $ cd Documentos/shodan

└──(incibe㉿kali)-[~/Documentos/shodan]
    $ shodan download resultados-ejercicio.json.gz omron
Search query:          omron
Total number of results: 166
Query credits left:      0
Output file:            resultados-ejercicio.json.gz
                         [#####] 59% 00:05:44
Notice: fewer results were saved than requested
Saved 99 results into file resultados-ejercicio.json.gz

└──(incibe㉿kali)-[~/Documentos/shodan]
    $
```

Ilustración 115: Descarga del resultado de la búsqueda de dispositivos Omron, en la carpeta «shodan».

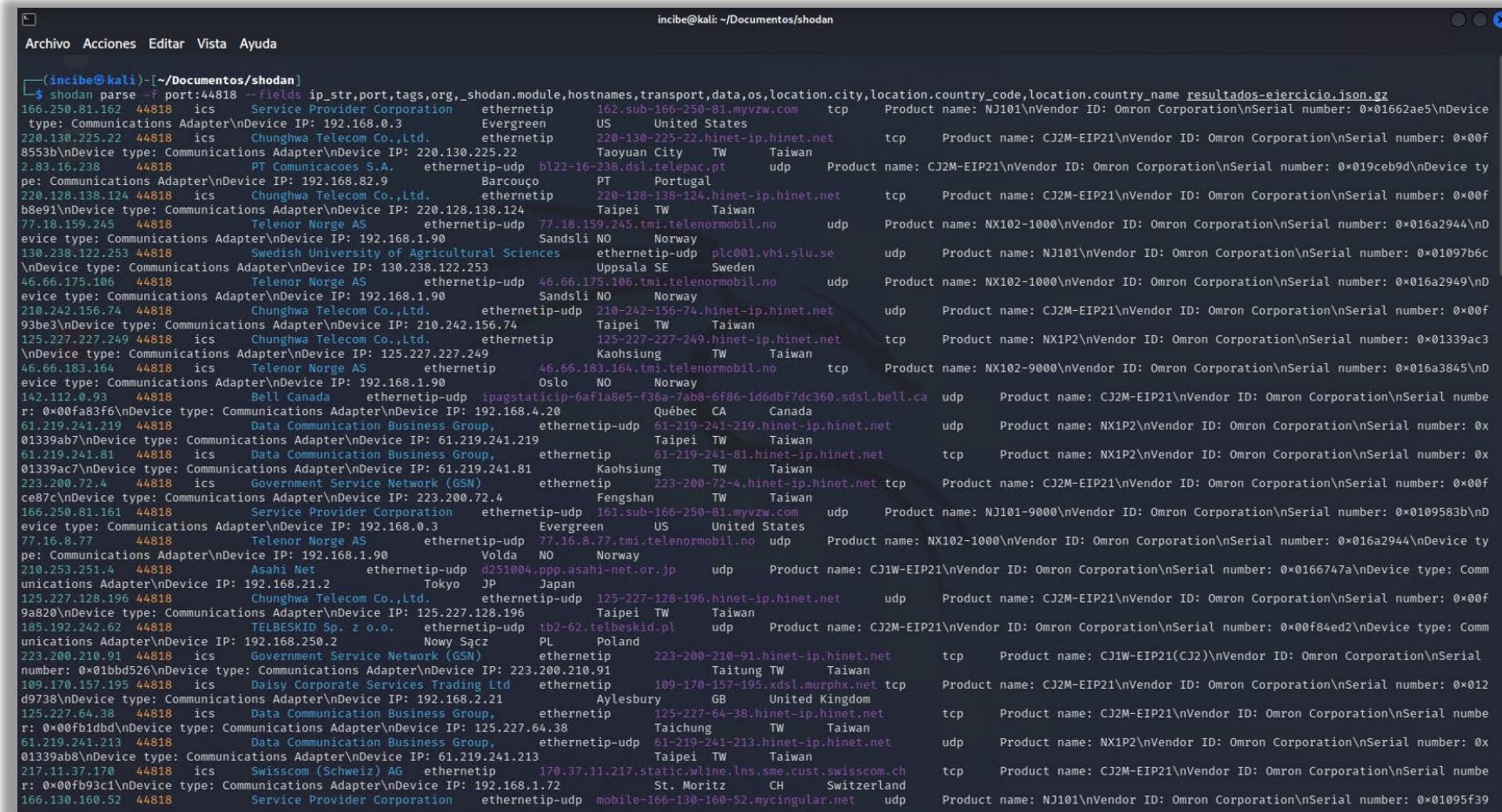
15 EJERCICIO PRÁCTICO 1

15.2 Solución ejercicio práctico 1

- Realiza una búsqueda local, utilizando el archivo descargado, filtrando por el puerto más utilizado que identificamos en el segundo punto y muestra solo los siguientes campos: *ip_str, port, tags, _shodan.module, hostnames, transport, data, os, location.city, location.country_code, location.country_name*.
 - **shodan parse -f port:44818 --fields ip_str,port,tags,org,_shodan.module,hostnames,transport,data,os,location.city,location.country_code,location.country_name resultados-ejercicio.json.gz**

15 EJERCICIO PRÁCTICO 1

15.2 Solución ejercicio práctico 1



The screenshot shows a terminal window titled "incibe@kali: ~/Documentos/shodan". The command run was "shodan parse -f port:44818 -fields ip_str, port, tags, org, _shodan.module, hostnames, transport, data, os, location.city, location.country_code, location.country_name resultados-ejercicio.json.gz". The output lists numerous network devices, primarily Communications Adapters, from various manufacturers and locations. Key details include IP addresses, device types, and vendor information like Omron Corporation and their serial numbers.

```
incibe@kali: ~/Documentos/shodan
$ shodan parse -f port:44818 -fields ip_str, port, tags, org, _shodan.module, hostnames, transport, data, os, location.city, location.country_code, location.country_name resultados-ejercicio.json.gz
166.250.81.162 44818 ics Service Provider Corporation ethernetip 162.sub-166-250-81.myvzw.com tcp Product name: NJ101\nVendor ID: Omron Corporation\nSerial number: 0x01662ae5\nDevice type: Communications Adapter\nDevice IP: 192.168.0.3 Evergreen US United States
220.130.225.22 44818 ics Chungwha Telecom Co.,Ltd. ethernetip 220-130-225-22.hinet-ip.hinet.net tcp Product name: CJ2M-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x00f8553b\nDevice type: Communications Adapter\nDevice IP: 220.130.225.22 Taoyuan City TW Taiwan
2.83.16.238 44818 PT Comunicacoes S.A. ethernetip-udp bl22-16-238.dsl.telepac.pt udp Product name: CJ2M-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x019ceb9d\nDevice type: Communications Adapter\nDevice IP: 192.168.82.9 Barcouço PT Portugal
220.128.138.124 44818 ics Chungwha Telecom Co.,Ltd. ethernetip 220-128-138-124.hinet-ip.hinet.net tcp Product name: CJ2M-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x00fb8e91\nDevice type: Communications Adapter\nDevice IP: 220.128.138.124 Taipei TW Taiwan
77.18.159.245 44818 Telenor Norge AS ethernetip-udp 77.18.159.245.tmi.telenormobil.no udp Product name: NX102-1000\nVendor ID: Omron Corporation\nSerial number: 0x016a2944\nDevice type: Communications Adapter\nDevice IP: 192.168.1.90 Sandsli NO Norway
130.238.122.253 44818 Swedish University of Agricultural Sciences ethernetip-udp plc001.whi.slu.se udp Product name: NJ101\nVendor ID: Omron Corporation\nSerial number: 0x01097b6c\nDevice type: Communications Adapter\nDevice IP: 130.238.122.253 Uppsala SE Sweden
46.66.175.106 44818 Telenor Norge AS ethernetip-udp 46.66.175.106.tmi.telenormobil.no udp Product name: NX102-1000\nVendor ID: Omron Corporation\nSerial number: 0x016a2949\nDevice type: Communications Adapter\nDevice IP: 192.168.1.90 Sandsli NO Norway
210.242.156.74 44818 Chungwha Telecom Co.,Ltd. ethernetip-udp 210-242-156-74.hinet-ip.hinet.net udp Product name: CJ2M-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x00f93be3\nDevice type: Communications Adapter\nDevice IP: 210.242.156.74 Taipei TW Taiwan
125.227.227.249 44818 ics Chungwha Telecom Co.,Ltd. ethernetip 125-227-227-249.hinet-ip.hinet.net tcp Product name: NX1P2\nVendor ID: Omron Corporation\nSerial number: 0x01339ac3\nDevice type: Communications Adapter\nDevice IP: 125.227.227.249 Kaohsiung TW Taiwan
46.66.183.164 44818 ics Telenor Norge AS ethernetip 46.66.183.164.tmi.telenormobil.no tcp Product name: NX102-9000\nVendor ID: Omron Corporation\nSerial number: 0x016a3845\nDevice type: Communications Adapter\nDevice IP: 192.168.1.90 Oslo NO Norway
142.112.0.93 44818 Bell Canada ethernetip-udp ipagstaticip-6af1a8e5-f36a-7ab8-6f86-1dddbf7dc36.sdsl.bell.ca udp Product name: CJ2M-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x00fa83f6\nDevice type: Communications Adapter\nDevice IP: 192.168.4.20 Québec CA Canada
61.219.241.219 44818 Data Communication Business Group, ethernetip-udp 61-219-241-219.hinet-ip.hinet.net udp Product name: NX1P2\nVendor ID: Omron Corporation\nSerial number: 0x01339ab7\nDevice type: Communications Adapter\nDevice IP: 61.219.241.219 Taipei TW Taiwan
61.219.241.81 44818 ics Data Communication Business Group, ethernetip 61-219-241-81.hinet-ip.hinet.net tcp Product name: NX1P2\nVendor ID: Omron Corporation\nSerial number: 0x01339ac7\nDevice type: Communications Adapter\nDevice IP: 61.219.241.81 Kaohsiung TW Taiwan
223.200.72.4 44818 ics Government Service Network (GSM) ethernetip 223-200-72-4.hinet-ip.hinet.net tcp Product name: CJ2M-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x00fce87c\nDevice type: Communications Adapter\nDevice IP: 223.200.72.4 Fengshan TW Taiwan
166.250.81.161 44818 Service Provider Corporation ethernetip-udp 161.sub-166-250-81.myvzw.com udp Product name: NJ101-9000\nVendor ID: Omron Corporation\nSerial number: 0x0109583b\nDevice type: Communications Adapter\nDevice IP: 192.168.0.3 Evergreen US United States
77.16.8.77 44818 Telenor Norge AS ethernetip-udp 77.16.8.77.tmi.telenormobil.no udp Product name: NX102-1000\nVendor ID: Omron Corporation\nSerial number: 0x016a2944\nDevice type: Communications Adapter\nDevice IP: 192.168.1.90 Volda NO Norway
210.253.251.4 44818 Asahi Net ethernetip-udp d251004.ppp.asahi-net.or.jp udp Product name: CJ1W-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x0166747a\nDevice type: Communications Adapter\nDevice IP: 192.168.21.2 Tokyo JP Japan
125.227.128.196 44818 Chungwha Telecom Co.,Ltd. ethernetip-udp 125-227-128-196.hinet-ip.hinet.net udp Product name: CJ2M-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x00f9a820\nDevice type: Communications Adapter\nDevice IP: 125.227.128.196 Taipei TW Taiwan
185.192.242.62 44818 TELBESKID Sp. z o.o. ethernetip-udp tb2-62.teleskid.pl udp Product name: CJ2M-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x00f84ed2\nDevice type: Communications Adapter\nDevice IP: 192.168.250.2 Nowy Sącz PL Poland
223.200.210.91 44818 ics Government Service Network (GSM) ethernetip 223-200-210-91.hinet-ip.hinet.net tcp Product name: CJ1W-EIP21(CJ2)\nVendor ID: Omron Corporation\nSerial number: 0x01bb5d26\nDevice type: Communications Adapter\nDevice IP: 223.200.210.91 Taitung TW Taiwan
109.170.157.195 44818 ics Daisy Corporate Services Trading Ltd ethernetip 109-170-157-195.xdsl.murphx.net tcp Product name: CJ2M-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x012d9738\nDevice type: Communications Adapter\nDevice IP: 192.168.2.21 Aylesbury GB United Kingdom
125.227.64.38 44818 ics Data Communication Business Group, ethernetip 125-227-64-38.hinet-ip.hinet.net tcp Product name: CJ2M-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x00fb1fdb\nDevice type: Communications Adapter\nDevice IP: 125.227.64.38 Taichung TW Taiwan
61.219.241.213 44818 ics Data Communication Business Group, ethernetip-udp 61-219-241-213.hinet-ip.hinet.net udp Product name: NX1P2\nVendor ID: Omron Corporation\nSerial number: 0x01339ab8\nDevice type: Communications Adapter\nDevice IP: 61.219.241.213 Taipei TW Taiwan
217.11.37.170 44818 ics Swisscom (Schweiz) AG ethernetip 170.37.11.217.static.wline.lns.sme.cust.swisscom.ch tcp Product name: CJ2M-EIP21\nVendor ID: Omron Corporation\nSerial number: 0x00fb93c1\nDevice type: Communications Adapter\nDevice IP: 192.168.1.72 St. Moritz CH Switzerland
166.130.160.52 44818 Service Provider Corporation ethernetip-udp mobile-166-130-160-52.mycingular.net udp Product name: NJ101\nVendor ID: Omron Corporation\nSerial number: 0x01095f39
```

Ilustración 116: Resultado de una búsqueda local, utilizando el archivo descargado, filtrando por el puerto más utilizado.

16

EJERCICIO PRÁCTICO 2

- 16.1 Enunciado
- 16.2 Solución



16 EJERCICIO PRÁCTICO 2

16.1 Enunciado ejercicio práctico 2



Muestra toda la información que proporciona
Shodan del *host* 166.250.81.162.

Nota: si Shodan no muestra información de ese *host*, (debido por ejemplo a que la IP ya no está disponible en la base de datos de Shodan) se utilizará algún otro de los *hosts* que ha devuelto la búsqueda anterior.

16 EJERCICIO PRÁCTICO 2

16.2 Solución ejercicio práctico 2

- Muestra toda la información que proporciona Shodan del host 166.250.81.162.
 - shodan *host 166.250.81.162*

```
(incibe㉿kali)-[~/Documentos/shodan]
└─$ shodan host 166.250.81.162
166.250.81.162
Hostnames:          162.sub-166-250-81.myvzw.com
City:               Evergreen
Country:            United States
Organization:       Service Provider Corporation
Updated:            2022-04-25T17:28:37.884151
Number of open ports: 7
Vulnerabilities:   CVE-2014-2324  CVE-2014-2323  CVE-2010-0295  CVE-2013-4560  CVE-2013-4559  CVE-2011-4362  CVE-2018-19052  CVE-2013-1427

Ports:
  80/tcp lighttpd (1.4.23)
  443/tcp Apache Tomcat/Coyote JSP engine (1.1)
    └─ SSL Versions: -SSLv2, -TLSv1.1, -TLSv1.2, -TLSv1.3, SSLv3, TLSv1
  3260/tcp
  8080/tcp
  8443/tcp
    └─ SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, TLSv1.2
  9600/tcp NJ101-9000 (1.18.00)
  44818/tcp Omron Corporation (NJ101)
  44818/udp

(incibe㉿kali)-[~/Documentos/shodan]
└─$
```

Ilustración 117: Información aportada por Shodan.

¡GRACIAS!



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL

 incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

