

Seguridad en infraestructuras críticas

Hacking con SHODAN

Dr. Manuel Sánchez Rubio



<https://www.linkedin.com/in/sanchezrum>

Estado del arte

Actualmente se estima que unos 250 dispositivos se conectan a internet cada segundo.

Este aumento viene dado por la mayor interconectividad de todos los dispositivos, y terminos como *Internet of Things* ó *Smart Cities* son comunes en la actualidad.

A primera vista esto supone un avance la hora de usabilidad e información pero implica la conexión de todos estos elementos en internet. Por esa razón ha de realizarse de forma razonada y teniendo en cuenta la seguridad de cada uno de estos nuevos dispositivos.

Si todo este proceso no se realiza correctamente se dará acceso remoto no solo al usuario legítimo sino a cualquiera que encuentre ese dispositivo en internet.

... y aquí empiezan los problemas.

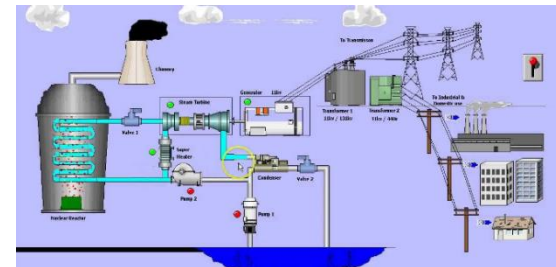
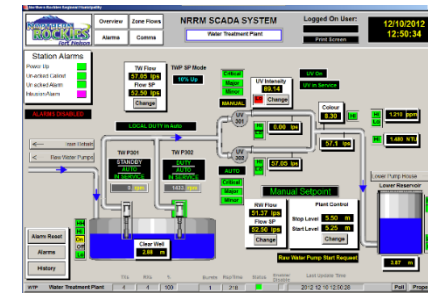
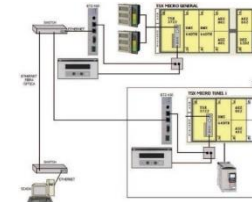
Qué son infraestructuras críticas



- Son aquellos activos esenciales para el funcionamiento de los servicios.
 - Redes de telecomunicaciones
 - Depuradoras, energías eléctricas.
 - Hospitales, aeropuertos
- Los servicios que sirven a la sociedad dependen de ellos.
- La interrupción o mal funcionamiento de estos activos pueden suponer una interrupción de los servicios o convertirse en amenazas.

Qué es SCADA

- ***Supervisory Control And Data Acquisition:*** Sistemas para comunicarse y operar con elementos industriales
- Elemento más extendido a la hora de gestionar infraestructuras críticas.
- Principal ventaja: permite el control remoto de las estructuras en **tiempo real**



¿Están asegurados los entornos críticos?

- No nos engañemos, hay de todo.
- Muchos de estos desarrollos están más pensados en las funcionalidades, dejando a un lado elementos clave como la seguridad del entorno.
- Muchos entornos se despliegan de forma insegura y predecible (ejemplo: credenciales “admin / admin”...)
- Principales elementos de un entorno seguro: VPN, Credenciales fuertes, sistema de roles, ...

Qué es Shodan

Es un motor de búsqueda de servicios.

A diferencia de los buscadores convencionales, Shodan busca más allá de servicios con interfaz web: edificios, cámaras web refrigeradores, plantas de energía...

Se puede utilizar de manera gratuita (registrado), pero la compra de una licencia amplía los horizontes:

- Acceso a la API de Shodan.
- Vista de todos los resultados de búsqueda.
- Ninguna limitación de consultas diarias.
- Acceso a todos los filtros de búsqueda.



Qué es Shodan

Like living on the edge? Try out the beta website for Shodan.

SHODAN Search


EXPOSE ONLINE DEVICES.


WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

[TAKE A TOUR](#) [FREE SIGN UP](#)

Popular Search Queries: default password - Finds results with "default password" in the banner; the named defaults might work!


**DEVELOPER API**
Find out how to access the Shodan database with Python, Perl or Ruby.

**LEARN MORE**
Get more out of your searches and find the information you need.

**FOLLOW ME**
Contact me and stay up to date with the latest features of Shodan.

IN THE PRESS


Shodan pinpoints shoddy industrial controls.



It greatly lowers the technical bar needed to canvas the Internet...



'Shodan for Penetration Testers' presented at DEF CON 18



It's a reminder to many to know what's on your network...



Shodan is the Google for hackers.



Shodan vereinfacht die Suche nach SCADA-Systeme erheblich...



Firmen öffnen Stuxnet und Co. selbst die Tür.



Computerangriffe werden einfacher. Zumindest für die Nutzer von Shodan.



[Privacy Policy](#) | [Terms of Service](#) © SHODAN

Qué es Shodan

Consulta realizada

Resultado coincidente con la consulta

Server Banner

Datos relacionados con el resultado obtenido

The screenshot displays the Shodan search engine interface. At the top, the Shodan logo is on the left, and a search bar contains the text 'minecraft' with a 'Search' button to its right. Below the search bar is a navigation menu with links: Home, Search Directory, Data Analytics/ Exports, Developer Center, and Labs. Under the 'Search Directory' link, there are two buttons: 'Add to Directory' and 'Export Data'. The main content area shows search results. On the left, there are two sections: 'Services' and 'Top Countries'. The 'Services' section lists various protocols and their counts: None (30,909), SMB (258), NetBIOS (199), HTTP (165), and FTP (155). The 'Top Countries' section lists countries and their counts: United States (15,473), Germany (6,185), France (2,234), Netherlands (1,818), and Canada (1,450). The main search results are displayed in a list. The first result is for a 'Minecraft Server' located in 'Belpre' with IP '173.81.4-235.pkbgcmk02.res.dyn.suddenlink.net'. It shows '0 online - 20 maximum' players, 'CraftBukkit 1.7.5 (protocol 4)' version, and a description 'Just another day in Derpvile'. The second result is also for a 'Minecraft Server' with '0 online - 8 maximum' players, 'Spigot 1.7.10 (protocol 5)' version, and a description 'Yes We Craft Realms'. Red boxes and arrows highlight specific elements: a box around the search bar with an arrow pointing to it labeled 'Consulta realizada'; a box around the first search result with an arrow pointing to it labeled 'Resultado coincidente con la consulta'; a box around the 'Server Banner' section of the first result with an arrow pointing to it labeled 'Server Banner'; and a box around the 'Services' and 'Top Countries' sections with an arrow pointing to it labeled 'Datos relacionados con el resultado obtenido'.

Services	
None	30,909
SMB	258
NetBIOS	199
HTTP	165
FTP	155

Top Countries	
United States	15,473
Germany	6,185
France	2,234
Netherlands	1,818
Canada	1,450

Minecraft Server	
Belpre	
Details	
173.81.4-235.pkbgcmk02.res.dyn.suddenlink.net	
Players:	0 online - 20 maximum
Version:	CraftBukkit 1.7.5 (protocol 4)
Description:	Just another day in Derpvile

Minecraft Server	
Details	
Players:	0 online - 8 maximum
Version:	Spigot 1.7.10 (protocol 5)
Description:	Yes We Craft Realms

Qué es Shodan

Cada dispositivo se muestra de la siguiente manera:

1 **13.214.178.28**

2 **ec2-13-214-178-28.ap-southeast-1.compute.amazonaws.com**

3 **Amazon Data Services Singapore**

4 **2022-06-18T08:53:51.950194**

5 **Singapore, Singapore**

cloud
honeypot

6 **HTTP/1.1 200 OK
Date: Sat, 18 Jun 2022 08:53:51 GMT
X-Powered-By: Express
Server: dcv 2wire Gateway 4D_WebSTAR_S/5.0 4D_WebSTAR_S/5.102.1 5.1.2600 2/Service Pack**

1. Dirección IP
2. Nombre del host
3. Proveedor de servicios de internet
4. Fecha de la entrada en la base de datos de Shodan
5. País
6. El banner creado por Shodan

Funcionamiento

- El buscador lee las cabeceras de los servicios para obtener información relevante:
 - Cabecera (ISP, hostname, Country, etc.)
 - Puerto/s por los que operan
 - Servicio y protocolos que ejecuta
- De forma histórica, el buscador muestra el resultado de histórico para cada vez que éste ha preguntado al servidor por la cabecera.
- Toda esta información es publicada en las bases de datos de Shodan.

Hacking con Shodan

- Para toda fase de recopilación de información, es interesante comprobar la información que puede ofrecer Shodan sobre un entorno a estudiar.
- Más allá del pentesting, Shodan es ampliamente utilizado para footprinting (recopilación de información de forma no activa de un objetivo).
- El acceso a Shodan no es delito, pero sí el acceso no permitido a los resultados que éste ofrece.

SHODAN DORKS

Filtros de localización

City


- Busca todos aquellos terminales cuya localización coincida con la de la ciudad especificada.
- Ejemplo: city:"Madrid"

Country

- Busca todos aquellos terminales cuya localización esté dentro del país buscado(escrito por código según ISO).
- Ejemplo: country:ES

SHODAN DORKS

Filtros de localización

 SHODAN

city:"Madrid" country:ES

Q

Explore

Contact Us

Blog

Enterprise Access


Exploits

Maps

Download Results

Create Report

TOP COUNTRIES



Spain 238,208


TOP CITIES

Madrid	236,970
Las Rozas De Madrid	939
Humanes De Madrid	298
Rozas De Madrid	1


TOP SERVICES

SSH	42,943
Modem Web Interface	40,181
HTTP	31,759
UPnP	17,250
SMTP	4,936



Showing results 1 - 10 of 238,203


rma-ide.net
Spain, Madrid
[Details](#)

HTTP/1.1 404 Not Found
Server: gSOAP/2.7
Content-Type: text/xml; charset=utf-8
Content-Length: 488
Connection: close


www-ide.net
Spain, Madrid
[Details](#)

HTTP/1.1 200 OK
Cache-Control: max-age=1800
ST: upnp:rootdevice
USN: uuid:63041253-1019-2006-1228-001915d51216::upnp:rootdevice
EXT:
Server: OS 1.0 UPnP/1.0 Realtek/V1.0
Location: http://192.168.1.1:53683/simplecfg.xml


Microsoft Internet Information Services 8


HTTP/1.1 200 OK

SHODAN DORKS

Filtros de localización

Geo

- Busca direcciones IP registradas en Shodan según geolocalización.
- Necesita 2 (3) valores: Latitud, longitud, (radio de km de búsqueda, por defecto 5).
- Útil para la búsqueda no aleatoria de estructuras críticas.

SHODAN DORKS

Filtros de terminal hostname

- Busca el valor escrito en el nombre del host
- Ejemplo: `hostname:"universidad"`

OS

- Busca por un sistema operativo especificado

port

- Busca por un número de puerto indicado en el filtro.

SHODAN DORKS

Filtros de terminal net

- Busca en Shodan la información vinculada a una IP dada.
- Puede ser de diferentes formas:
 - IP directa: net:111.22.33.44
 - Rango de subred: net:111.22.33.0/24
 - Puede bajarse a rangos superiores: net:111.0.0.0/8

before/after

- Busca a partir o hasta una fecha según el filtro utilizado
- Ejemplos:
 - Before:12/09/2014
 - After:11/09/2014

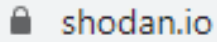
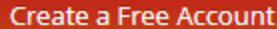
SHODAN DORKS

Código	Descripción	Ejemplo
Country	Permite seleccionar el país de búsqueda, con el código del país.	Country:"ES"
State	Búsqueda de un estado dentro del país.	State:"Texas"
City	Búsqueda de una ciudad.	Citi:"Madrid"
Postal	Búsqueda según el código postal	Postal:"27394"
Org	Buscar organizaciones por nombre	Org:"Google"
Net	Busca direcciones ip individuales o rangos	Net:10.0.0.0/8
Hostname	Búsqueda parcial o completa de dominios	Hostname:"Jazztel.es"
Port	Busca puertos específicos abiertos	Port:445
Title	Búsqueda por palabras clave en el título	Title:"camera"
Html	Busca una cadena en el código html de una página web	Html:"Bank"
Os	Búsqueda por sistema operativo	Os:"Linux"
Product	Busca por producto o fabricante	Product:"Cisco"
Version	Versión específica de un software o servicio	Version:"sslv3"
Geo	Búsqueda por geolocalización.	Geo:29.45,50.71

Ejemplo: "country:ES product:Apache Org:Telefonica Port:80"

SHODAN DORKS

- Crear una cuenta

The logo for Shodan.io, featuring a small padlock icon followed by the text "shodan.io".A red rectangular button with the text "Create a Free Account" in white.

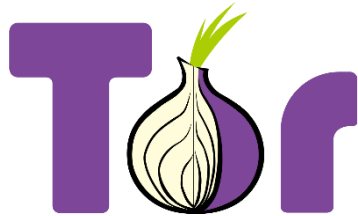
- Download up to 10,000 results per month
- Scan up to 100 IPs per month
- Network monitoring for 16 IPs
- The ability to use the "vuln" search filter on the website
- All add-ons (HTTPS, Telnet, view up to 2,000 search results)
- Improved API plan: <https://developer.shodan.io>
- Shodan Maps (<https://maps.shodan.io>)
- Shodan Images (<https://images.shodan.io>)
- Shodan Monitor (<https://monitor.shodan.io>)
- Shodan Book

Solicita a academic@shodan.io una mejora de la cuenta con un correo de una institución educativa, incluye:

SHODAN Responsabilidades



Solución



Caso práctico con Shodan



Shodan Scannhub Developers View all

SHODAN

Explore Membership Contact Us Blog Enterprise Access

Download Results Create Report

Exploits Maps

TOP COUNTRIES

Showing results 1 - 2 of 2

Spain, Details

Added on 2015-10-26 15:39:38 GMT

Basic Hardware: 6ES7 214-1BE30-0XB0 v.0.1
Module: 6ES7 214-1BE30-0XB0 v.0.1
Basic Firmware: 6ES7 214-1BE30-0XB0 v.2.2.0

Spain

TOP CITIES

Spain, Details

Added on 2015-10-15 18:35:30 GMT

Basic Hardware: 6ES7 211-1BE31-0XB0 v.0.1
Module: 6ES7 211-1BE31-0XB0 v.0.1
Basic Firmware: 6ES7 211-1BE31-0XB0 v.3.0.1

TOP ORGANIZATIONS

Caso práctico con Shodan

Shodan Scanhub Developers View All...

SHODAN

Explore Membership Contact Us Blog Enterprise Access

Logout

City

Country Spain

Organization

ISP

Last Update 2015-11-03T22:38:17.140536

Hostnames

ASN

Ports

80 102 443

Services

80 tcp http HTTP/1.1 302 Object Moved Content-Type: text/html Content-Length: 0 Location: /Default.mws1

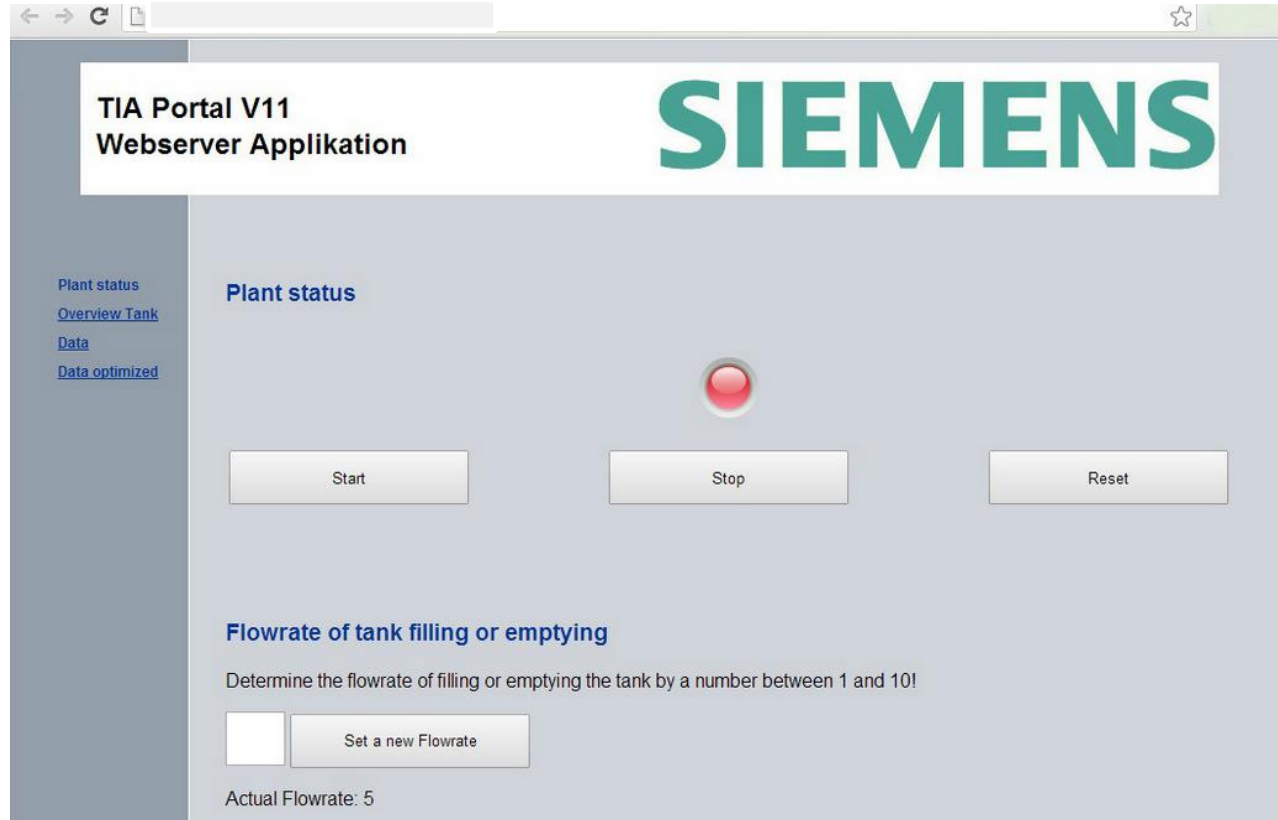
102 tcp s7 Basic Hardware: 6ES7 214-1BE30-0XB0 v.0.1 Module: 6ES7 214-1BE30-0XB0 v.0.1 Basic Firmware: 6ES7 214-1BE30-0XB0 v.2.2.0

Caso práctico con Shodan

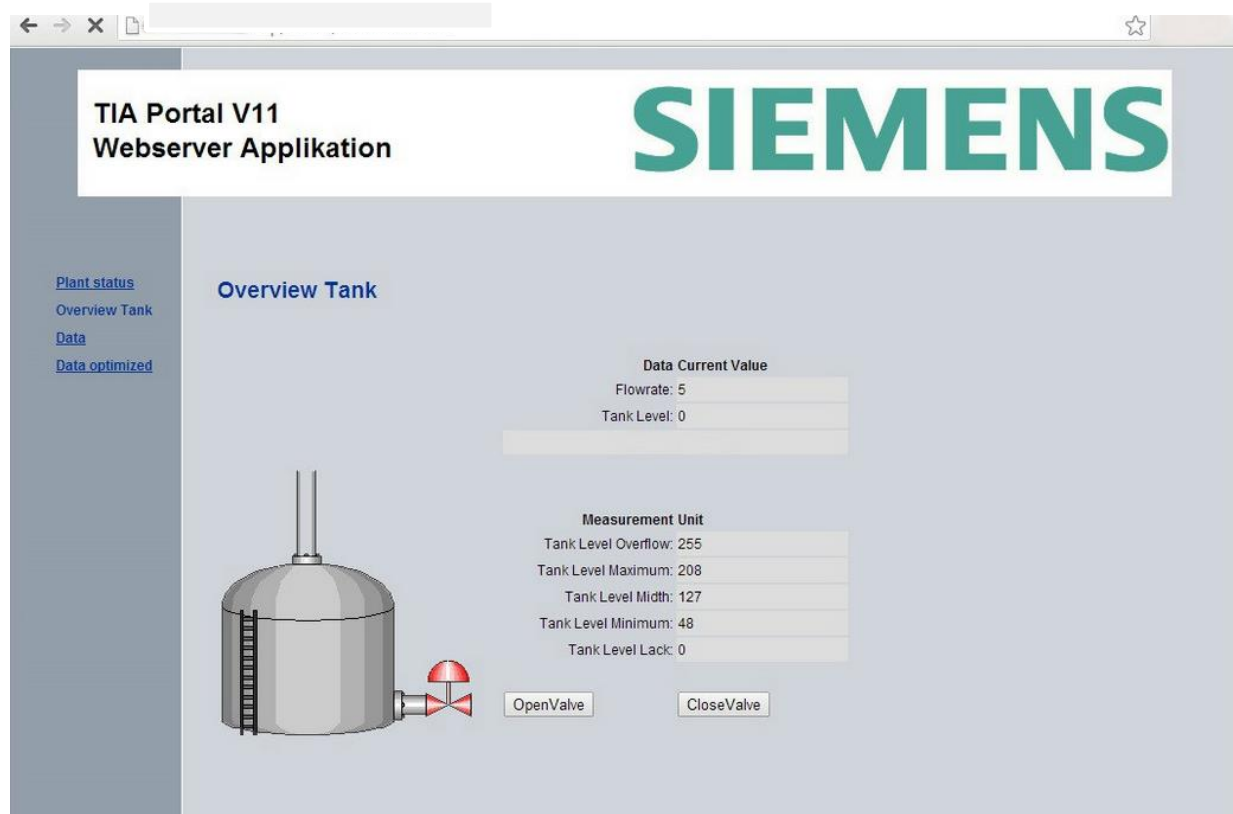
The screenshot displays the Siemens SIMATIC Manager interface for a SIMATIC 1200 station_1/PLC_1. The interface is divided into several sections:

- Header:** Displays "SIEMENS" and "SIMATIC 1200 station_1/PLC_1".
- Left Navigation Panel:** Contains a list of menu items: Start Page, Identification, Diagnostic Buffer, Module Information, Communication, Variable Status, Data Logs, User Pages, and Introduction.
- Top Bar:** Includes fields for "Name" and "Password", a "Login" button, and a status indicator showing "Off".
- Main Content Area:**
 - General:** Displays the following information:
 - Station name: SIMATIC 1200 station_1
 - Module name: PLC_1
 - Module type: CPU 1214C ACDCRly
 - IP Address: 192.168.1.2
 - Status:** Displays the following information:
 - Operating Mode: RUN
 - Status: ✔ OK

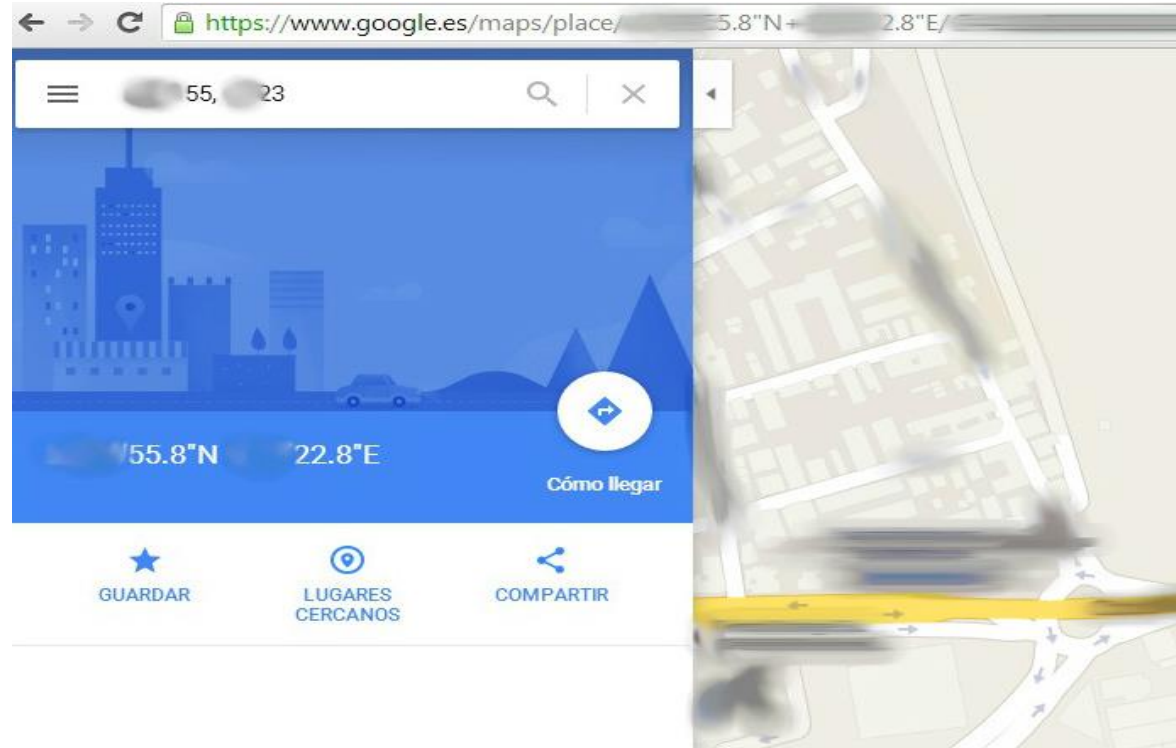
Caso práctico con Shodan



Caso práctico con Shodan



Caso práctico con Shodan



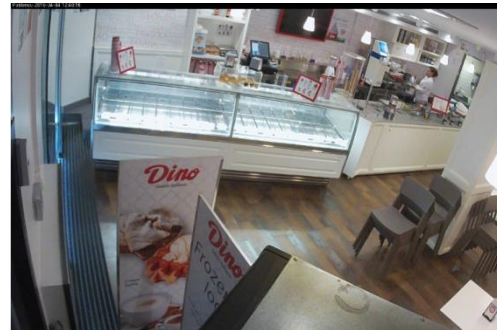
Caso práctico con Shodan



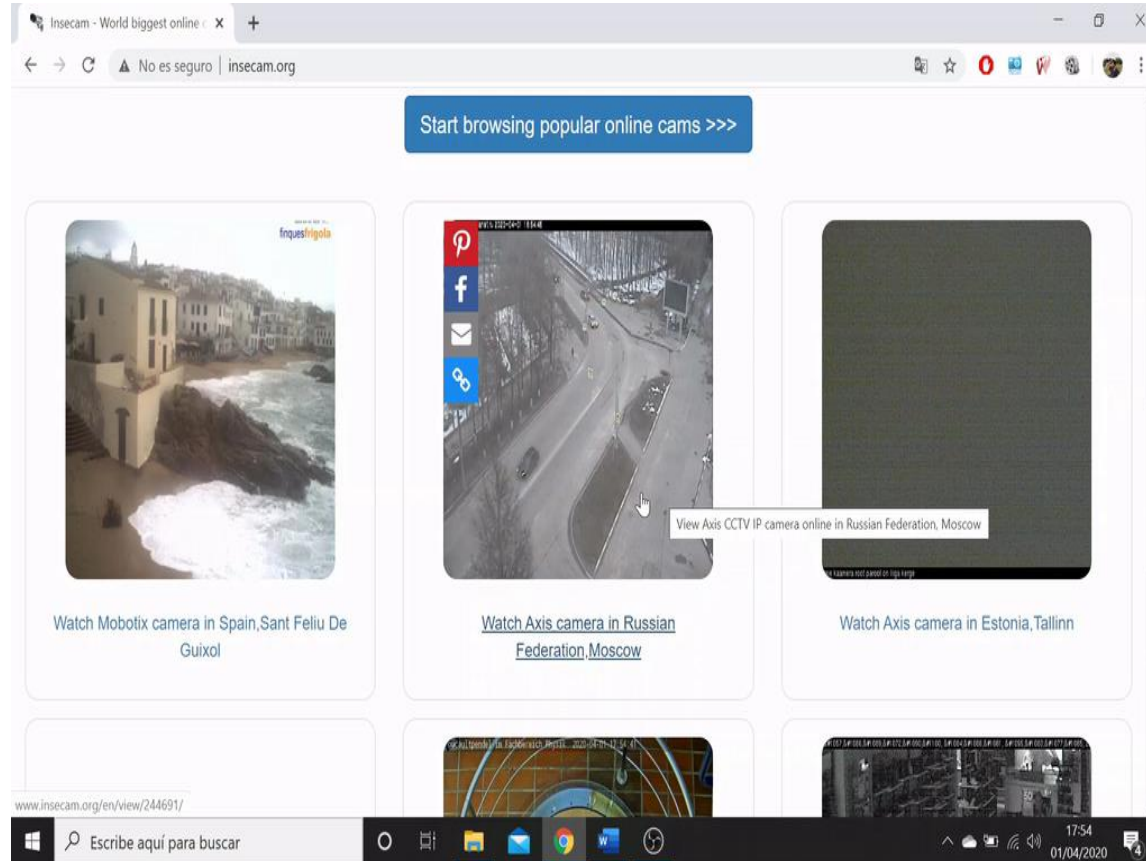
Cámaras en abierto

<http://insecam.org/>

→ Por países, por temática...



Cámaras en abierto. Insecam



Prueba de concepto I

Cisco

- Durante el rastreo que realiza Shodan puede encontrarse con distintas respuestas HTTP
- Determinadas configuraciones permiten acceder a la configuración de un dispositivo Cisco sin autenticación (respuesta HTTP 200 = OK)

```
HTTP/1.0 401 Unauthorized
Date: Tue, 01 Dec 2009 16:09:46 GMT
WWW-authenticate: Basic realm="level_15 or view_access"
Connection: close
Accept-ranges: none
Server: cisco-IOS
```

```
HTTP/1.0 200 OK
Transfer-encoding: chunked
Accept-ranges: none
Expires: Tue, 08 Jun 1993 06:55:45 GMT
Server: cisco-IOS
Last-modified: Tue, 08 Jun 1993 06:55:45 GMT
Connection: close
Cache-control: no-store, no-cache, must-revalidate
Date: Tue, 08 Jun 1993 06:55:45 GMT
Content-type: text/html
```

Prueba de concepto I

Cisco

Acceso sin
autenticación

The screenshot shows the Cisco IOS Series AP - Home page in a Mozilla Firefox browser. The page displays the Cisco Aironet 350 Series Access Point configuration interface. A red box highlights the text "Acceso sin autenticación".

Cisco Aironet 350 Series Access Point

Home: Summary Status

[Association](#)

Clients: 0 Repeater: 0

[Network Identity](#)

IP Address: [redacted]
MAC Address: [redacted]

[Network Interfaces](#)

Interface	MAC Address	Transmission Rate
FastEthernet	[redacted]	100Mb/s
Radio0-802.11B	[redacted]	11.0Mb/s

[Event Log](#)

Time	Severity	Description
Dec 7 20:33:53.718	Warning	Packet to client 0021.c510.b576 reached max retries, removing the client
Dec 7 20:33:49.495	Information	Interface Dot11Radio0, Deauthenticating Station 0023.6c83.3f41 Reason: Sending station has left the BSS
Dec 7 20:33:40.830	Information	Interface Dot11Radio0, Station 0021.c510.b576 Associated KEY_MGMT[NONE]

Prueba de concepto II

Granja de energía solar



Diferentes cabeceras de página web denotan un servicio

Showing results 1 - 3 of 3	
Solar Farm Web Scada Login TOT Added on 2015-05-18 01:21:57 GMT Thailand Details	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/7.5 Set-Cookie: ASP.NET_SessionId=tom4lazwat2p5h55tep3mzb; path=/; HttpOnly X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Date: Mon, 18 May 2015 01:21:08 GMT Content-Length: 3270
Solar Farm Web Scada Login TOT Added on 2015-05-14 05:17:40 GMT Thailand Details	HTTP/1.1 200 OK Cache-Control: private Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/7.5 X-AspNet-Version: 4.0.30319 Set-Cookie: ASP.NET_SessionId=415x5h4uk4jkd3h2dg2mp4kq; path=/; HttpOnly X-Powered-By: ASP.NET Date: Thu, 14 May 2015 05:14:53 GMT Content-Length: 3214

Prueba de concepto II

Granja de energía solar



Prueba de concepto III

Depuradoras

Country: ES

Explore Contact Us Blog Enterprise Access

aps Download Results Create Report

Showing results 1 - 3 of 3

500 Internal Error

Spain, Madrid

Details

HTTP/1.0 500 Internal Error
Server: LabVIEW/7.1
Connection: close
Date: Wed, 20 May 2015 01:48:06 GMT
Content-type: text/html
Content-length: 320

403 Forbidden

Spain, Vigo

Details

HTTP/1.0 403 Forbidden
Server: LabVIEW/7.1
Connection: close
Date: Fri, 8 May 2015 15:41:13 GMT
Content-type: text/html
Content-length: 317

LabVIEW Web Server Examples

Spain, Zaragoza

Details

HTTP/1.0 200 OK
Server: LabVIEW/8.2.1
Connection: close
Date: Fri, 8 May 2015 07:03:36 GMT
Last-modified: Thu, 22 Jun 2006 12:21:48 GMT

Prueba de concepto III

Depuradoras

Misma situación que antes

Se requiere autenticación

El servidor [REDACTED] requiere un nombre de usuario y una contraseña. Mensaje del servidor: (Tram Water-Base)

Nombre de usuario:


Contraseña:

Control de la calidad del agua



Prueba de concepto IV

Gasolineras

 SHODAN

port:10001 country:es

Q

10001

Automated Tank Gauge

I20100
04-05-15 23:58
816680
J07201431605011
INVENTARIO EN TANQUE

9999

Telnet (Lantronix)

MAC address
Software version V6.8.0.2 (120628) XPTEXE
Press Enter for Setup Mode

PRODUCTO	TANQ	VOL	VOL CT	POR LL	ALTURA	AGUA	TEMP
1	OPTIMA DIESEL	7672	7668	21828	672.7	0.0	15.76
2	OPTIMA 95	3826	3826	25673	439.3	0.0	15.37
3	GASOLINA 95	11722	11714	17778	965.6	0.0	15.90
4	GASOLEO A	11707	11691	17807	1020.8	0.0	16.88
5	GASOLEO A	16979	16949	12520	1308.3	0.0	17.61
6	GASOLINA 98	7270	7270	22229	693.4	0.0	15.41
7	GASOLEO C	5174	5174	24326	543.6	0.0	15.45

1. Acceder vía Telnet
2. Modificar datos del gestor de tanque
3. Parar servicio de una gasolinera por falsa señal de falta de stock
4. Eliminar avisos por aumento de temperatura...

Ejemplos

Ataques

Tenemos que elegir...



VS.





vs.



168.205.146.85

168-205-146-85.netuai-internet.com.br

Net-Uai Internet Provider LTDA ME

Added on 2018-08-26 11:53:23 GMT



Brazil

Details

Shodan puede ayudar a las empresas a realizar y controlar su exposición en internet

Unicomp Networks Device
IP: 168.205.146.85

MAC: 44:d9:e7:72:b2:13

Alternate IP: 192.168.2.1

Alternate MAC: 44:d9:e7:73:b2:13

Hostname: **HACKED**-ROUTER-HELP-SOS-HAD-DUPE-PASSWORD

Product: LB5

Version: XW.ar934x.v6.0.30097.161219.1705



vs.



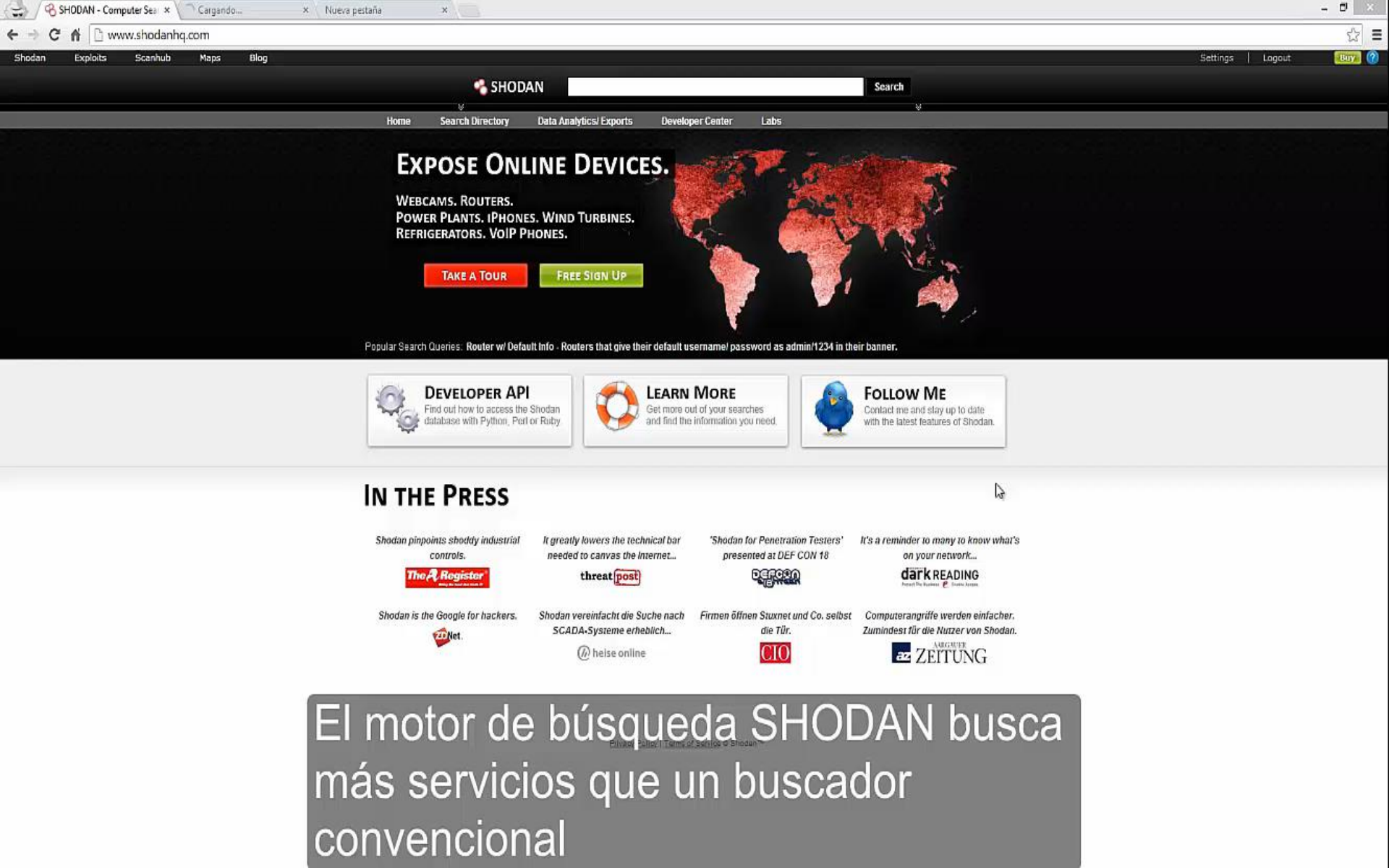
Product	Price	Quantity
Small job, for example: Email and Facebook hacking, installing trojans, small DDOS	250 EUR = 0.043 ₿	<input type="text" value="1"/> X Buy now
Medium-large job, ruining people, espionage, website hacking, DDOS for big websites Venta de nuevas vulnerabilidades (zero-days)	500 EUR = 0.087 ₿	<input type="text" value="1"/> X Buy now
Large job which takes a few days or multiple smaller jobs, DDOS for protected sites Ataques DDOS Acceso a sistemas	900 EUR = 0.156 ₿	<input type="text" value="1"/> X Buy now
UPGRADE: INSTANT reply within 30-60 minutes instead of 24-36 hours for urgent cases. If i need longer this will get refunded. Only buy this together with one of the other options. Acceso a cuentas personales de redes sociales Secuestro de dispositivos (Ransomware)	200 EUR = 0.035 ₿	<input type="text" value="1"/> X Buy now

... son las prácticas más comunes que motivan y financian a los ciberdelincuentes.

¡Empezamos!

... que la fuerza os acompañe

Abriendo boca...



EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

TAKE A TOUR

FREE SIGN UP

Popular Search Queries: Router w/ Default Info - Routers that give their default username/ password as admin/1234 in their banner.



DEVELOPER API

Find out how to access the Shodan database with Python, Perl or Ruby



LEARN MORE

Get more out of your searches and find the information you need.



FOLLOW ME

Contact me and stay up to date with the latest features of Shodan.

IN THE PRESS

Shodan pinpoints shoddy industrial controls.



It greatly lowers the technical bar needed to canvas the Internet...



'Shodan for Penetration Testers' presented at DEF CON 18



It's a reminder to many to know what's on your network...



Shodan is the Google for hackers.



Shodan vereinfacht die Suche nach SCADA-Systeme erheblich...



Firmen öffnen Stuxnet und Co. selbst die Tür.



Computerangriffe werden einfacher. Zumindest für die Nutzer von Shodan.



El motor de búsqueda SHODAN busca más servicios que un buscador convencional

Atacando a Sistemas de Control industrial (Parte I)

¿Cómo?

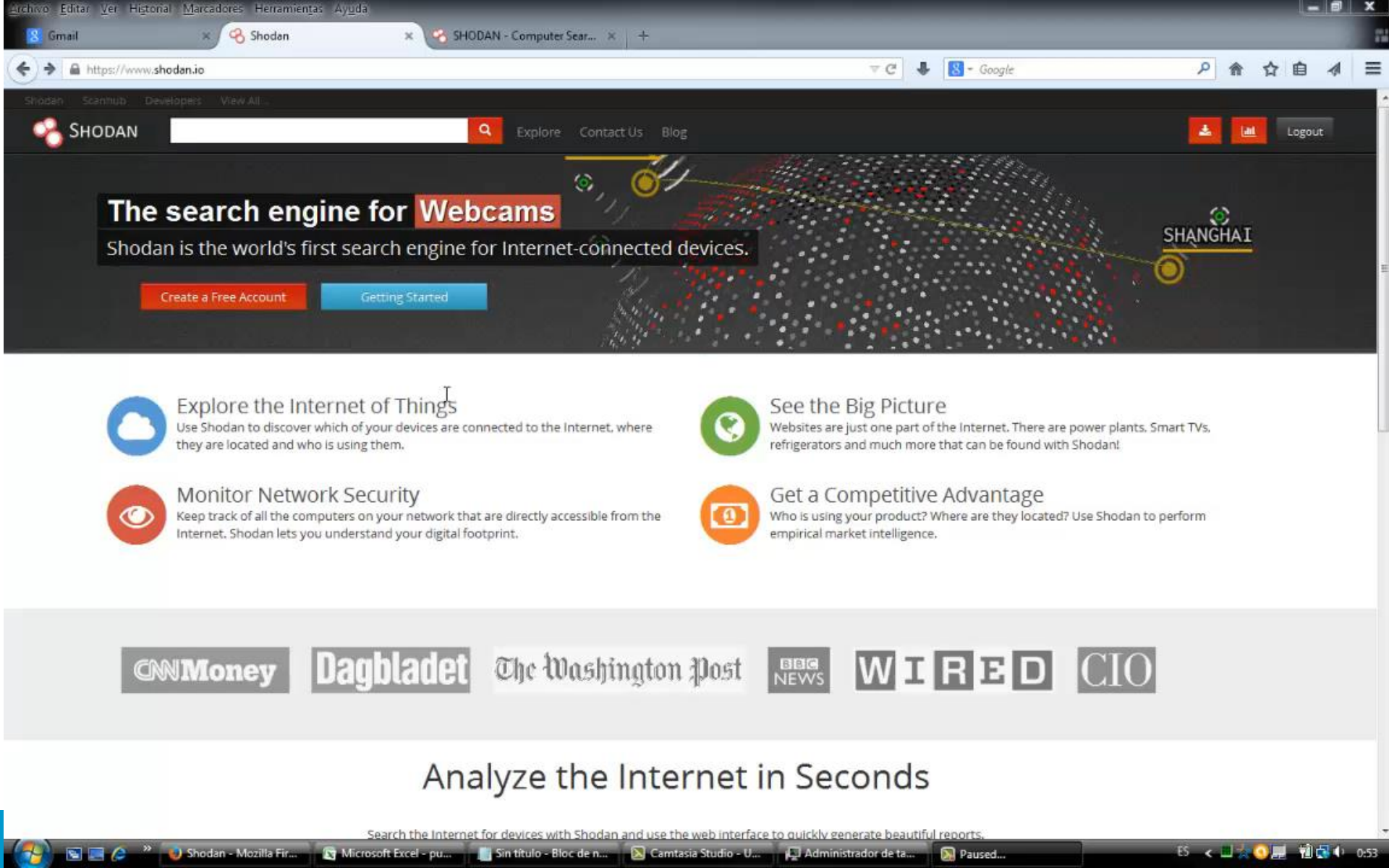
Puertos Industriales.

La siguiente tabla recoge los principales puertos de comunicación utilizados en protocolos industriales.

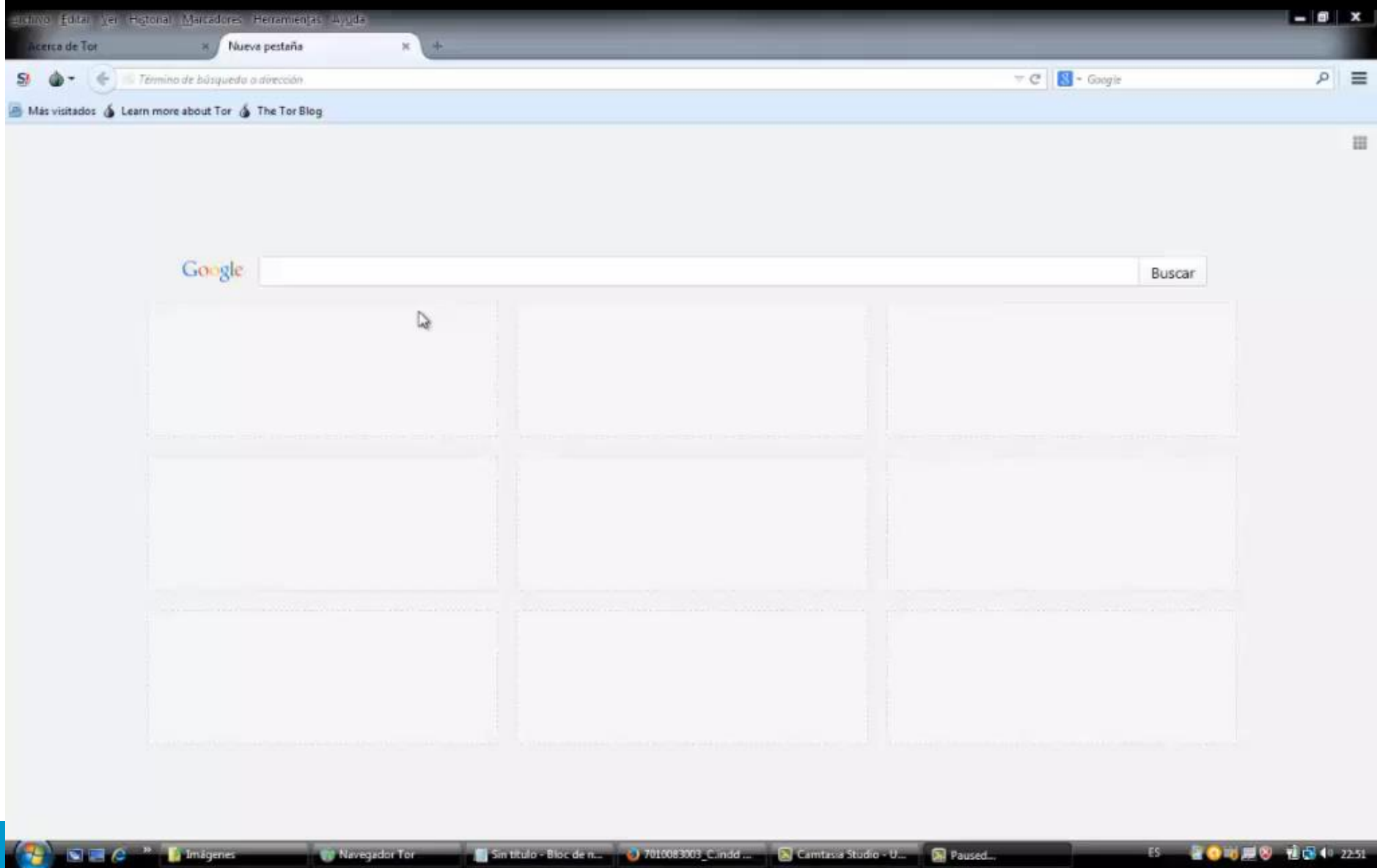
Protocolo	Puerto
Modbus	TCP/502
Vendor	Device
ABB	AC 800M
ABB	SREA-01
Adcon Telemetry	Telemetry Gateway A840 and Wireless Modem A440
Adcon Telemetry Fieldbus	addVANTAGE Pro 6.1, 6.5
OPC UA	3480
DNP	TCP/19999
DNP3	TCP/20000
PROFINET	TCP/34692-34964
BACNET/IP	TCP/47808
SIEMENS S7	TCP/102

Listado de passwords por defecto.

Vendor	Device	Default password	Port	Device type	Protocol
ABB	AC 800M	service:ABB800xA		Controller	
ABB	SREA-01	admin:admin	80/tcp	Ethernet Adapter Module	http
Adcon Telemetry	Telemetry Gateway A840 and Wireless Modem A440	root:840sw	terminal program	Base Station	
Adcon Telemetry	addVANTAGE Pro 6.1, 6.5	root:root	8080/tcp	HMI	HTTP
Advantech	SNMP-1000, MIC-3924	advantech:admin	serial port	system management module, intelligent chassis	
Argus	Argus Address Manager	argus:argus		Address Manager Software	
Astute Medical	ASTUTE140 Meter	1234:1234		analyzer	
B&B ELECTRONICS	CR10 v2	root:root	80/tcp	Industrial router	http
B&B ELECTRONICS	Conel 4.0.1	root:root	80/tcp	Industrial router	http
B&B ELECTRONICS	SPECTRE Router	root:root	80/tcp	Router	http
B&B ELECTRONICS	ER75/ER 75i DUO/ER 75i SL/ER75i v2	root:root	80/tcp	Industrial router	http
B&B ELECTRONICS	LR77 v2 Libratum/LR77 v2	root:root	80/tcp	Industrial router	http
B&B ELECTRONICS	UR5i v2	root:root	80/tcp	Industrial router	http
B&B ELECTRONICS	UCR11-v2/UCR11 v2 SL	root:root	80/tcp	Industrial router	http
B&B ELECTRONICS	XR5i v2/ER5i v2/ER5i/SL	root:root	80/tcp	Industrial router	http
B&B ELECTRONICS	ES1A	root:dbps	80/tcp	Converter	HTTP
B&B ELECTRONICS	Vlinx VESR4x4	<blank>		SERIAL SERVER	
B&B ELECTRONICS	Vlinx MESR9xx Modbus Gateway	<blank>		Modbus Gateway	
Barco	MediCal QAWeb Agent	Advanced:advanced		client application	
Beckhoff Automation GmbH	CX5020	webguest:1	23/tcp	PLC	Telnet
Beckhoff Automation GmbH	TwinCAT	Administrator:1		Software for the Windows control and automation technology	
Beck IPC	Ä IPC@CHIP	PPP:SERVER., ppps:ppps		PLC	paploha p



Atacando a Sistemas de Control industrial (Parte II)



Ataque de diccionario de datos

Sabéis atacar a un Sistemas de Control industrial

Sabéis hacer un ataque de diccionario de datos

...sabéis mucho

⚙ API DOCUMENTATION

Requirements

Introduction

Clients

REST API Documentation

Streaming API Documentation

⚙ EXPLOITS API DOCUMENTATION

Introduction

REST API Documentation

📄 APPENDIX

Banner Specification

Exploit Specification

REST API Documentation

The base URL for all of these methods is:

https://api.shodan.io

Note: All API methods are rate-limited to 1 request/ second.

Shodan Search Methods

GET	/shodan/host/{ip}
GET	/shodan/host/count
GET	/shodan/host/search
GET	/shodan/host/search/facets
GET	/shodan/host/search/filters
GET	/shodan/host/search/tokens
GET	/shodan/ports

Shodan On-Demand Scanning

FUNDAMENTOS DE SEGURIDAD

No olvidéis que nosotros no estamos en el lado oscuro



¿Preguntas?