

## EJERCICIOS SHODAN

## Prerrequisitos

Registrarse en:

<https://www.shodan.io/>

Utilizar filtros para acotar las siguientes búsquedas y responder las preguntas.

## Ejercicio 1

Busca una webcam e intenta acceder a ella usando el nombre de usuario y la contraseña por defecto. Entrega una captura de pantalla donde se vea la localización de la cámara, el país, el proveedor de internet, los puertos abiertos...

Lista de contraseñas y/o nombre de usuario predeterminado de IP's de cámaras:

<https://netviewcctv.co.uk/blog/ipcampassword/>

General Information

eisenbahn.dyndns.tv  
fritz.box  
www.fritz.box  
**myfrizt**.box  
www.**myfrizt**.box  
wzxcrgkwaljfd4**z-myfrizt.net**  
p508bb78.dip0.t-ipconnect.de

// 443 / TCP 🔒

Domains

DYNDNS.TVFRITZ.BOXMYFRIZT.BOX  
MYFRIZT.NETT.IPCONNECT.DE

Country

Germany

City

Willich

Organization

Deutsche Telekom AG

ISP

Deutsche Telekom AG

ASN

AS3320

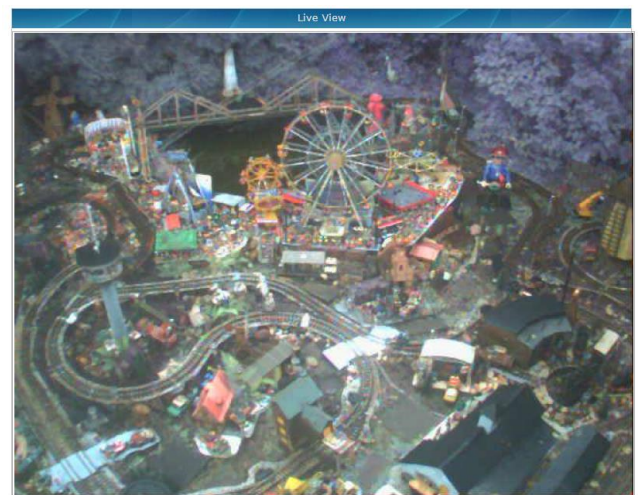
Operating System

Windows

HTTP/1.1 200 OK  
Cache-Control: no-cache  
Cache-control: no-cache  
Connection: close  
Content-type: text/html  
Date: Sat, 23 Sep 2023  
Expires: -1  
Pragma: no-cache  
X-Frame-Options: SAMEORIGIN  
X-XSS-Protection: 1; mode=block  
X-Content-Type-Options: nosniff  
Content-Security-Policy: script-src https://fritzhelpehttps://clickonce.asrc'self' https://\*.de unsafe-inline'; style-

SSL Certificate

Certificate:  
Data:  
Version: 3 (R)  
Serial Number:  
4a:a4:b:c:d:e:f  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: O=CERT...  
Validity:



**Localización:** Alemania

**Puertos abiertos: 443; 8080**

Aparece cómo funciona la noria

## Ejercicio 2

Intenta acceder a un router con el nombre de usuario y la contraseña por defecto. No hagas ninguna modificación. Razona tu respuesta: ¿crees que es legal hacer una modificación a la configuración de un router al que puedes acceder?

Pricing ↗
product: "MikroTik"

View Report
 View on Map

**Access Granted:** Want to get more out of your existing Shodan account? Check out our [pricing page](#).

**181.115.46.12**

SERCOM de Honduras

Honduras, Tegucigalpa

```

220 MikroTik FTP server (MikroTik 6.45.8) ready
530 Login incorrect
500 'HELP': command not understood
500 'FEAT': command not understood
    
```

**45.188.233.66**

EDWIN SALAZAR  
ORDÓÑEZ EDSAOR CIA.  
LTD.A(FIBRATELECOM)

Ecuador, Riobamba

```

220 MikroTik FTP server (MikroTik 6.49.6) ready
530 Login incorrect
500 'HELP': command not understood
500 'FEAT': command not understood
    
```

45.188.233.66 Regular View Raw Data

**General Information**

Country	Ecuador
City	Riobamba
Organization	EDWIN SALAZAR ORDOÑEZ EDSAOR CIA. LTDA.(FIBRATELECOM)
ISP	WIFITELECOM
ASN	AS264744

**Open Ports**

21 22 80 2000 8291 8728

// 21 / TCP

**MikroTik router ftpd 6.49.6**

```

220 MikroTik FTP server (MikroTik 6.49.6) ready
530 Login Incorrect
580 'HELP': command not understood
500 'FEAT': command not understood
  
```

**RouterOS v6.45.8**

You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.

**WebFig Login:**

Login:  Login

Password:

Authentication failed: invalid username or password.

**MikroTik**

He intentado acceder a este router con las contraseñas por defecto que aparecen en internet y no se autentifica.

Sí, es legal realizar modificaciones en la configuración de un router, siempre que seas el propietario de este o tengas permiso del propietario para hacerlo. Si tienes acceso legítimo, puedes modificar la configuración del router según tus necesidades. En función del país, acceder a redes o dispositivos sin autorización puede considerarse ilegal y estar sujeto a sanciones.

## Ejercicio 3

Comprueba si hay algún sistema con "Windows XP" conectado a internet, ¿en qué país?, ¿qué puerto está exponiendo?. Razona tu respuesta: ¿qué problemas de seguridad puede tener?, ¿por qué?

downloads Pricing windowsXP

View Report Browse Images View on Map

Access Granted: Want to get more out of your existing Shodan account? Check out everyth

39.107.242.130

Alpaca Computing Co., LTD

China, Beijing

HTTP/1.1 404 Not Found

Date: Tue, 3 Oct 2023 03:57:08 GMT

Content-Type: text/plain

Content-Length: 8

Cobalt Strike Beacon:

ids:

beacon\_type: HTTP

dns.beacon.strategy\_fall\_seconds: -1

dns.beacon.strategy\_fall\_in: -1

82.200.108.82 Regular View Raw Data

// TAGS: self-signed starttls

**General Information**

Hostnames	gw-spkill-omsk.zsttk.ru
Domains	ZSTTK.RU
Country	Russian Federation
City	Omsk
Organization	JSC Zap-Sib TransTeleCom
ISP	Joint Stock Company TransTeleCom
ASN	AS21127
Operating System	Windows

**Open Ports**

25 53 80 1701

// 25 / TCP

**Postfix smtpd**

```

220 spk.ru ESMTP Postfix windowsXP
250-SPK.RU
250-PIPELINING
250-SIZE 38721528
250-ETRN
250-STARTTLS
250-AUTH LOGIN NTLM PLAIN DIGEST-MD5 CRAM-MD
250-AUTH-LOGIN NTLM PLAIN DIGEST-MD5 CRAM-MD
250-ENHANCEDSTATUSCODES
250-RESTRICTED
250 OK

SMTP NTLM Info:
Target Name: SPK.RU
  
```

Al buscar WindowsXP aparecen una serie de países conectados a este sistema operativo, decido escoger uno concretamente de Rusia que tiene los puertos 25, 53, 80, 1701 abiertos. Pude contabilizar 53 tipos diferentes de vulnerabilidades, esto ocurre debido a que al ser un OS tan antiguo no ha parcheado estos problemas debido a que no existen actualizaciones para este mismo.

## Ejercicio 4

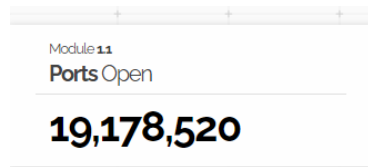
El siguiente enlace nos muestra el estado de la seguridad informática de España, según Shodan:

<https://exposure.shodan.io/#/ES>

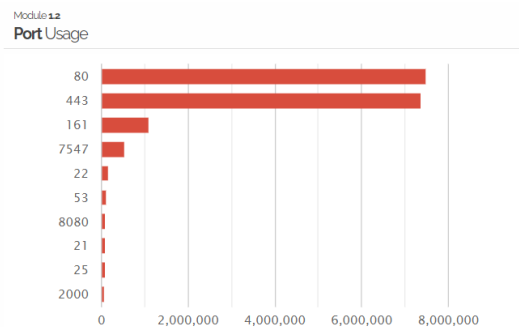
Interpretando el mapa indica la siguiente información:

¿Cuántos puertos abiertos hay en España?, ¿cuál es el más usado?, ¿a qué servicio corresponde?

- Numero de puertos abiertos:

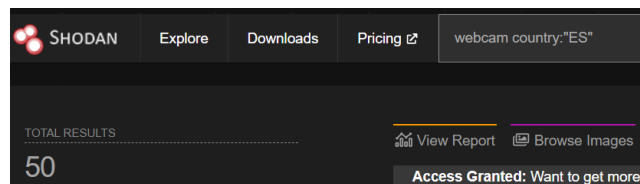


- Puerto más utilizado: 80



- HTTP

¿Cuántas webcam están abiertas en la actualidad en España?



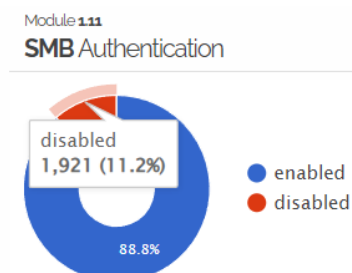
¿Cuántos sistemas de control industriales están conectados a internet?



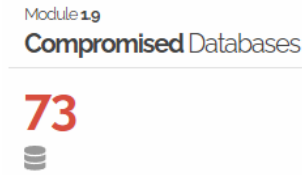
¿Cuántas páginas web utilizan el protocolo obsoleto SSLv2 en el protocolo https?



¿Qué porcentaje de servidores SAMBA no tienen habilitados un sistema de autenticación?



¿Cuántas bases de datos están comprometidas?



¿Cuál es la vulnerabilidad más detectada? A qué fallo corresponde.

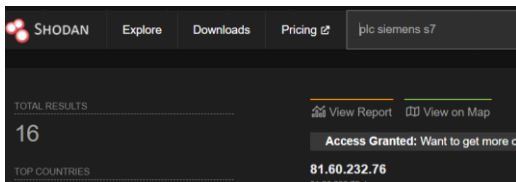


permite a servidores SSL remotos llevar a cabo ataques de degradación y facilitar el descifrado de fuerza bruta

## Ejercicio 5

La ciberseguridad industrial es cada vez más importante. ¿Cómo buscarías PLCs de Siemens del modelo S7 que estén conectados a Internet usando Google y usando Shodan? Una vez que los hubieras encontrado, ¿cuál es el usuario y contraseña por defecto de este tipo de dispositivos? NOTA: Sólo puedes realizar las búsquedas, no entres en ninguno de los paneles que encuentres.

Shodan: Existen 16 dispositivos conectados a internet según Shodan



Google: Existen distintos tipos de modelos, en distintos foros exponen que en los modelos 300 no existe autenticación, los modelos 1200 y 1500 sí que tendrían pero por defecto es user: admin y password: empty

**S7-300 Default password**

Created by: [vorapob](#) at: 9/21/2018 2:37 PM (2 Replies)

Rating: ★★★★★ (1)  
Thanks: 0

► Actions **New post**

3 Entries

9/21/2018 2:37 PM ► Rate ★★★★★ (0)

**vorapob**

Dear Experts,  
What is the default password of S7-300 cpu ?  
Can I use it if I forgot password ?  
Best Regards,  
Vorapob

**Attachment**  
↓ S7 315F Default Password.jpg (229 Downloads)

Joined: 1/17/2013  
Last visit: 9/29/2023  
Posts: 1047  
Rating: ★★★★★ (6)

► Suggestion ► To thank Answer Quote

9/21/2018 4:02 PM ► Rate ★★★★★ (0)

**Hati**

There is no default password for PLC's.

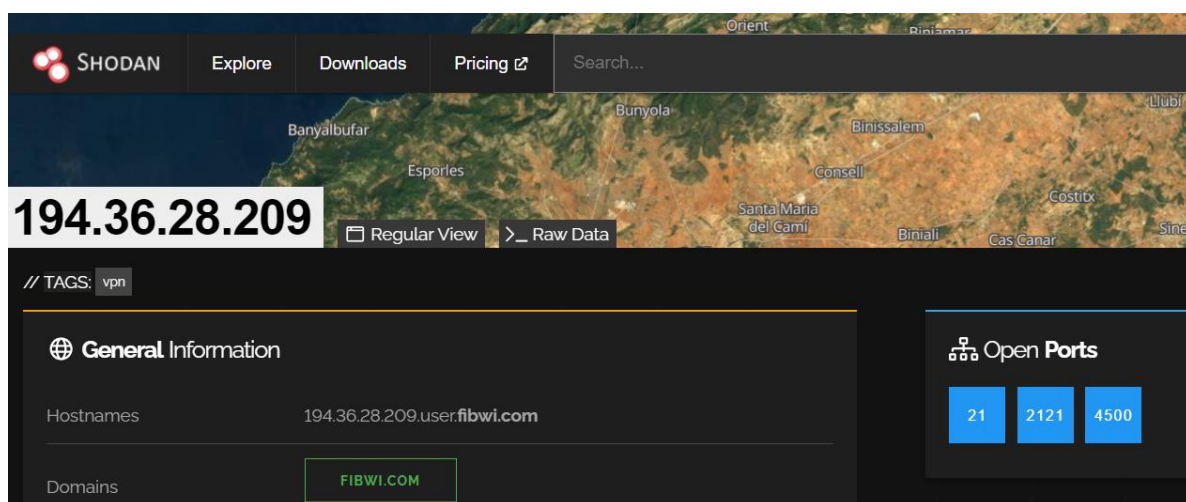
## Ejercicio 6

¿Cómo podrías saber qué software se ha utilizado para montar un servidor web determinado (Apache, IIS, etc.)? ¿Y su versión específica?

Existen distintas formas

1. **Buscar en robots.txt:** Algunos sitios web incluyen información en sus archivos **robots.txt**. Esto se ejecuta sumándolo al URL del dominio.
2. **Utilizar herramientas de escaneo de seguridad:** Herramientas de escaneo de seguridad como Nmap y Nikto, estas herramientas analizan los banners y las respuestas del servidor para determinar qué software y versión se están utilizando.
3. **Utilizando páginas web:** como BuiltWith (<https://builtwith.com/>) y Wappalyzer (<https://www.wappalyzer.com/>).
4. **Examinar las cabeceras HTTP:** utilizando el comando `curl` → `curl -I http://example.com`
5. Una forma sencilla de identificar el software y la versión de un servidor web es utilizando un servicio en línea como "Netcraft" ([https://toolbar.netcraft.com/site\\_report](https://toolbar.netcraft.com/site_report)) o "SecurityHeaders" (<https://securityheaders.com/>).

Utilizando el filtro de búsqueda country:es server podemos conocer ips de dispositivos. En función de la sobreexposición de información podremos visualizar la versión específica de cada tipo. En este caso el puerto 2121 utiliza Apache 2.4.48



SHODAN Explore Downloads Pricing Search...

194.36.28.209 Regular View Raw Data

// TAGS: vpn

**General Information**

Hostnames 194.36.28.209.user.fibwi.com

Domains FIBWI.COM

**Open Ports**

21 2121 4500

```
// 2121 / TCP


HTTP/1.1 200 OK
Date: Thu, 05 Oct 2023 13:12:24 GMT
Server: Apache/2.4.48 (Win64)
Last-Modified: Mon, 11 Jun 2007 18:53:14 GMT
ETag: "2d-432a5e4a73a80"
Accept-Ranges: bytes
Content-Length: 45
Content-Type: text/html
```

## Ejercicio 7

¿Cómo podrías localizar los puertos en los que un servidor emplea SSL ó TLS? ¿Y cómo podrías saber si el cifrado que se está usando es débil?

1. **Abre el Sitio Web:**
2. **Comprobación de la Conexión Segura:** Observa la barra de direcciones del navegador. Si el sitio utiliza SSL/TLS correctamente, verás un candado o alguna otra indicación de conexión segura. Haz clic en el candado o en el icono para obtener detalles.
3. **Información de Certificado:** Dentro de los detalles de seguridad, generalmente encuentras información sobre el certificado SSL/TLS del sitio, incluyendo el cifrado utilizado y la versión del protocolo.
4. **Comprobación de Cifrados Fuertes:** Idealmente, el sitio debería utilizar TLS 1.2 o superior y cifrados fuertes como AES-GCM o ChaCha20. Si ves menciones a SSL o a cifrados antiguos como RC4, DES, o 3DES, esto indica una configuración insegura.

Esta forma de verificar la conexión SSL/TLS es simple y no requiere herramientas adicionales.

```
// 443 / TCP 

nginx

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 04 Oct 2023 15:46:19 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
Content-Language: ca
X-Frame-Options: SAMEORIGIN
X-Generator: Drupal 7 (http://drupal.org)
Link: </content/inici>; rel="canonical",</node/147>; rel="shortlink"
X-Httpd-Modphp: 1
Host-Header: 6b7412fb82ca5edfd0917e3957f05d89
X-Proxy-Cache: MISS
X-Proxy-Cache-Info: 0 NC:000000 UP:

SSL Certificate

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      03:4d:a9:28:d0:4f:4d:85:88:ca:58:7b:57:49:57:90:d7:47
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, O=Let's Encrypt, CN=R3
    Validity
      Not Before: Sep 26 12:09:04 2023 GMT
      Not After : Dec 25 12:09:03 2023 GMT
    Subject: CN=*.bibliotecabalmes.cat
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
```

Se puede observar que la clave publica del puerto 443 es de 2048 bit, además utiliza sha256 por tanto tiene un cifrado fuerte

