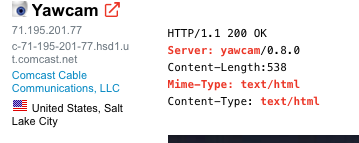
EJERCICIOS SHODAN

**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/>



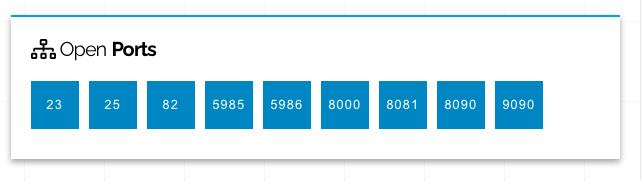
**2. Intenta acceder a un router con el nombre de usuario y la contraseña por defecto. No hagas ninguna modificación. Razona tu respuesta: ¿crees que es legal**

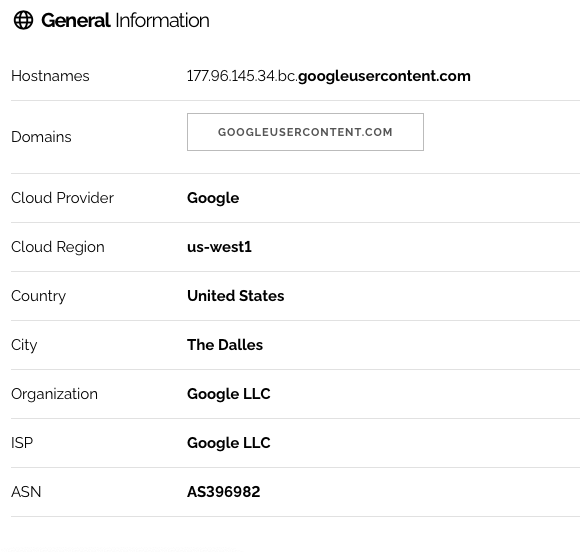
**hacer una modificación a la configuración de un router al que puedas acceder?**

No, que haya una puerta abierta no significa que puedas entrar

**3. Comprueba si hay algún sistema con “Windows XP” conectado a internet, ¿en qué país?, ¿qué puerto está exponiendo?.**

Está en USA y está exponiendo estos puertos:





**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?**

5,915,851, el puerto más usado es el 161. El puerto 161 es el puerto predeterminado de los dispositivos de red a los que se envían consultas SNMP durante los procesos de descubrimiento y supervisión.

**¿Cuántas webcam están abiertas en la actualidad en España?**

Alrededor de 512 mil puertos 80 están abiertos y 85 mil puertos 8080, estos puertos se suele corresponder con camaras IP

**¿Cuántos sistemas de control industriales están conectados a internet?**

8175

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

7,7%

**¿Cuántas bases de datos están comprometidas?**

109

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

## CVE-2015-0204

## Permite a servidores SSL remotos llevar a cabo ataques de degradación de RSA-to-EXPORT\_RSA y facilitar el descifrado de fuerza bruta al ofrecer una clave RSA efímera débil en un rol no compatible, relacionado con el problema "FREAK".

**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.**

En google

inurl:"S7" intitle:"Siemens"

Esto buscará páginas que contengan "S7" en la URL y "Siemens" en el título, lo que puede ayudarte a encontrar interfaces web de PLCs Siemens S7.

En shodan

"Siemens S7"

o

port:102 "Siemens"

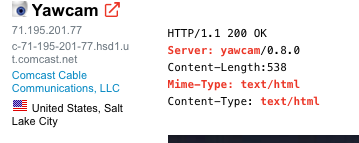
El puerto 102 es el que suelen usar los PLCs Siemens para la comunicación.

Para los dispositivos PLC Siemens S7, los valores por defecto para el usuario y contraseña suelen ser:

user: admin

contraseña admin o 1234

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



Usando la foto del ejercicio 1, vemos cómo el server está indicado ahí junto con la versión específica.