

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/>

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 puedas acceder?

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?

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?
 - ¿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.

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.

Ejercicio 6

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

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?