Actividad 1. Shodan

¿Qué tipo de información indexa Shodan?

Se dedica a buscar y hacer un listado de dispositivos que están conectados a Internet. No busca páginas web como los buscadores, sino que encuentra equipos como servidores, routers, cámaras de seguridad, sistemas de control industrial, dispositivos de Internet de las cosas y hasta electrodomésticos inteligentes.

Analiza los puertos abiertos de cada dispositivo y guarda la información que estos devuelven, como los banners de respuesta, donde se pueden ver servicios activos, versiones de software y protocolos utilizados. De esta forma, permite conocer cómo están configurados y expuestos estos dispositivos en la red.

¿Qué diferencia hay entre Shodan y Google?

La principal diferencia está en lo que cada uno busca. Google se enfoca en indexar contenido de la web, como páginas HTML, documentos, imágenes o vídeos. El objetivo de es ayudar a los usuarios a encontrar información que ya está publicada en Internet.

Shodan, en cambio, no busca contenidos, sino la infraestructura que hay detrás de la red. En lugar de indexar páginas web, localiza dispositivos conectados a Internet y analiza sus puertos y protocolos para identificar qué servicios están activos y cómo están configurados. Mientras Google muestra lo que las personas publican, Shodan permite ver qué sistemas y dispositivos están expuestos y accesibles desde una dirección IP.

¿Qué tipos de dispositivos IoT aparecen con más frecuencia?

Los dispositivos que aparecen con más frecuencia suelen ser webcams, routers domésticos, impresoras y sistemas de almacenamiento en red (NAS). También es habitual encontrar dispositivos domóticos y equipos industriales como PLCs o sistemas SCADA que utilizan protocolos industriales como Modbus.

Las cámaras IP destacan especialmente entre los resultados, ya que en muchos casos están mal configuradas, utilizan credenciales por defecto o están expuestas directamente a Internet, lo que facilita su localización y acceso desde Shodan.

¿Qué información técnica muestra un resultado típico?

Muestra la dirección IP del dispositivo, su localización aproximada y el proveedor de servicios de Internet (ISP). La información más relevante suele ser la lista de puertos abiertos, como el 80, 443 o 502, junto con los servicios asociados a cada uno.

Muestra los banners de respuesta de esos servicios, donde se pueden identificar versiones de software, el sistema operativo del dispositivo y, en algunos casos, si mantiene configuraciones inseguras como credenciales por defecto o vulnerabilidades conocidas.

Actividad 2. Búsqueda de Shodan

He seleccionado el dispositivo con dirección IP 86.155.129.79, que aparece identificado como un equipo IoT.

Dispositivo:

- Dispositivo IoT de la marca TP-Link, concretamente un TP-Link Kasa P100, que es un enchufe inteligente.

Sector:

- Doméstico, ya que es un dispositivo de domótica pensado para el hogar.

información visible:

- Dirección IP pública.
- Ubicación aproximada (Reino Unido).
- Puertos abiertos: 80 (HTTP).
- Servicios: Servicio web accesible HTTP.
- Protocolos y datos técnicos: Versión de protocolo, tipo de cifrado KLAP.
- información del fabricante y dirección MAC.

¿Por qué es un riesgo que esta información sea publica?

Supone un riesgo de seguridad, ya que permite identificar dispositivos IoT concretos, su ubicación y los servicios abiertos. Un ataque podría utilizar esta información para intentar explotar vulnerabilidades conocidas, acceder al dispositivo o usarlo como punto de entrada a la red doméstica.

Actividad 3. Responde a estas cuestiones

¿En qué capa del IoT se sitúan los dispositivos encontrados?

Se sitúan principalmente en la capa de red o de comunicaciones del IoT, ya que es en esta capa donde se gestiona la conectividad y el intercambio de datos entre los dispositivos físicos y el exterior.

Esta ubicación se debe a que Shodan detecta los equipos porque responden a través de protocolos de red y puertos específicos, como Modbus en el puerto 502 o servicios de bases de datos como SQL Server, lo que evidencia que están expuestos a nivel de red.

Estos dispositivos actúan como un punto intermedio que permite que la información generada en la capa de percepción (sensores y actuadores) sea transmitida hacia la capa de aplicación, donde se gestionan interfaces de usuario, sistemas de control o bases de datos.

¿Pueden considerarse CPS? ¿Por qué?

Sí, los dispositivos que aparecen en este tipo de búsquedas pueden considerarse sistemas ciberfísicos (CPS), ya que combinan de forma directa el mundo digital con el mundo físico.

Integran una parte ciber, formada por el software, la conectividad y el procesamiento de datos, y, una parte física, que corresponde a los procesos reales que controlan o supervisan. En entornos industriales o de servicios, la información que circula por la red no se limita a transmitir datos, sino que puede provocar acciones reales, como abrir una barrera, detener una máquina o regular una válvula.

Estos sistemas suelen operar en tiempo real, tomando decisiones digitales que afectan inmediatamente al comportamiento de elementos físicos. Por ello, cuando Shodan detecta un dispositivo industrial o un sistema IoT expuesto, está identificando precisamente el componente cibernético que gobierna un proceso físico, lo que encaja plenamente con la definición de CPS.

¿Qué papel ha jugado la conectividad en su exposición?

Ha sido el factor determinante que ha permitido que estos dispositivos pasen de estar aislados a quedar expuestos en Internet. La necesidad de monitorización y gestión remota ha provocado que muchos sistemas, especialmente industriales o de servicios, se conecten directamente a la red, eliminando el aislamiento físico que antes actuaba como una barrera de seguridad.

Es la que hace posible que detecten e indexen los dispositivos, ya que al contar con direcciones IP públicas y servicios accesibles desde el exterior se vuelven visibles a nivel de red. En muchos casos se utilizan protocolos que no fueron diseñados originalmente para Internet, como Modbus, priorizando la facilidad de conexión frente a la seguridad.

El acceso remoto mal configurado, sin medidas de protección como VPN o firewalls, permite que servicios que deberían ser privados queden accesibles desde cualquier lugar del mundo, aumentando significativamente el riesgo de exposición y de accesos no autorizados.

¿Qué errores de diseño IoT detectas?

Se detectan, varios errores de diseño. El más crítico es la exposición directa de servicios sensibles a Internet, sin una capa intermedia de seguridad, lo que provoca que paneles de control, bases de datos o dispositivos industriales sean visibles públicamente.

Otro fallo importante es el uso de protocolos no cifrados o inseguros, como HTTP en lugar de HTTPS, o protocolos industriales antiguos que transmiten la información en texto plano, facilitando la interceptación y manipulación de los datos.

Se detecta una clara falta de segmentación de red, ya que sistemas internos aparecen accesibles desde direcciones IP públicas, lo que indica que no existe una separación adecuada entre la red interna y la red de Internet.

Actividad 4. Busca información y propone medidas de seguridad para prevenir que un sistema IoT industrial aparezca expuesto en Shodan

Para que un sistema IoT industrial no aparezca en buscadores como Shodan. Lo importante es quitar accesos que no se necesitan y aplicar medidas de seguridad desde el principio. Las medidas principales que hay que considerar son las siguientes:

1. Uso de VPN y eliminación de IPs públicas

No conectarlos directamente a internet con una dirección IP pública. Es mejor acceder a ellos de forma remota a través de una red privada virtual, o VPN, que tenga un cifrado seguro. De esta forma, solo las personas que tengan acceso a la red autorizada podrán llegar a los sistemas de control. Incluso si el dispositivo está conectado a internet, un servicio como Shodan solo podrá ver el servidor VPN y no los dispositivos que están dentro de la red.

2. Segmentación de red y uso de firewalls

Es importante mantener separadas la red de la oficina y la red industrial. Debemos utilizar firewalls especiales para la red industrial que tengan reglas muy estrictas. Estas reglas deben negar todo acceso por defecto y solo permitir el tráfico que sea absolutamente necesario. Es útil utilizar listas de direcciones IP que estén permitidas, lo que limita aún más el acceso a solo aquellos sistemas que conocemos y controlamos.

3. Fortalecimiento y configuración segura de los dispositivos (hardening)

Muchos dispositivos se muestran en Shodan porque comparten información que no es necesaria. Es importante apagar los servicios que no se utilizan, como servidores web que no se necesitan, cambiar siempre las claves de acceso que vienen por defecto y configurar los servicios para que no muestren información técnica sensible en los mensajes de bienvenida, como las versiones exactas del software que se utiliza.

4. Uso de gateways de seguridad

En lugar de conectar directamente cada sensor o PLC a la red, es recomendable utilizar gateways industriales como único punto de salida. Esto permite centralizar la seguridad, aplicar controles adicionales, facilitar la monitorización del tráfico y gestionar las actualizaciones de forma más eficiente.

Por último, es fundamental realizar auditorías y escaneos periódicos sobre los rangos de IP de la organización. De esta forma se pueden detectar dispositivos expuestos por error y corregir configuraciones inseguras antes de que sean indexadas por herramientas como Shodan.