Práctica de laboratorio: Búsquedas de Shodan

Objetivos

Shodan es un motor de búsqueda para dispositivos de IoT desarrollado por John Matherly en 2009. Shodan puede descubrir todo tipo de "cosas" conectadas a Internet, desde teléfonos móviles hasta dispositivos inteligentes y plantas de energía. Es una herramienta poderosa para determinar qué dispositivos están conectados actualmente a la red y cómo se conectan.

- Cree una cuenta de usuario de Shodan y regístrese para obtener una clave de API
- Utilice el sitio web de Shodan para buscar dispositivos de IoT vulnerables
- Usar Shodan de la CLI para realizar una búsqueda

Aspectos básicos/Situación

Los dispositivos de IoT se utilizan ampliamente. Los crean, instalan y mantienen los gobiernos, las empresas y los propietarios de viviendas. Estos dispositivos no suelen estar protegidos por el fabricante. Es responsabilidad del usuario final garantizar que estos dispositivos no introduzcan riesgos adicionales para la seguridad de la red.

Puede realizar algunas búsquedas en Shodan sin obtener una suscripción. Las búsquedas más extensas requieren una suscripción paga.

En esta práctica de laboratorio, realizará una búsqueda en Shodan de dispositivos vulnerables dentro de su red privada, así como dentro de un rango definido de direcciones IP. Como con la mayoría de las herramientas que está utilizando en este curso, solo escanee o acceda a las redes que posee o tiene permiso de acceso.

Recursos necesarios

- Kali VM personalizada para el curso de Ethical Hacker
- Acceso a Internet

Instrucciones

Parte 1: Cree una cuenta de Shodan y regístrese para obtener una clave de API

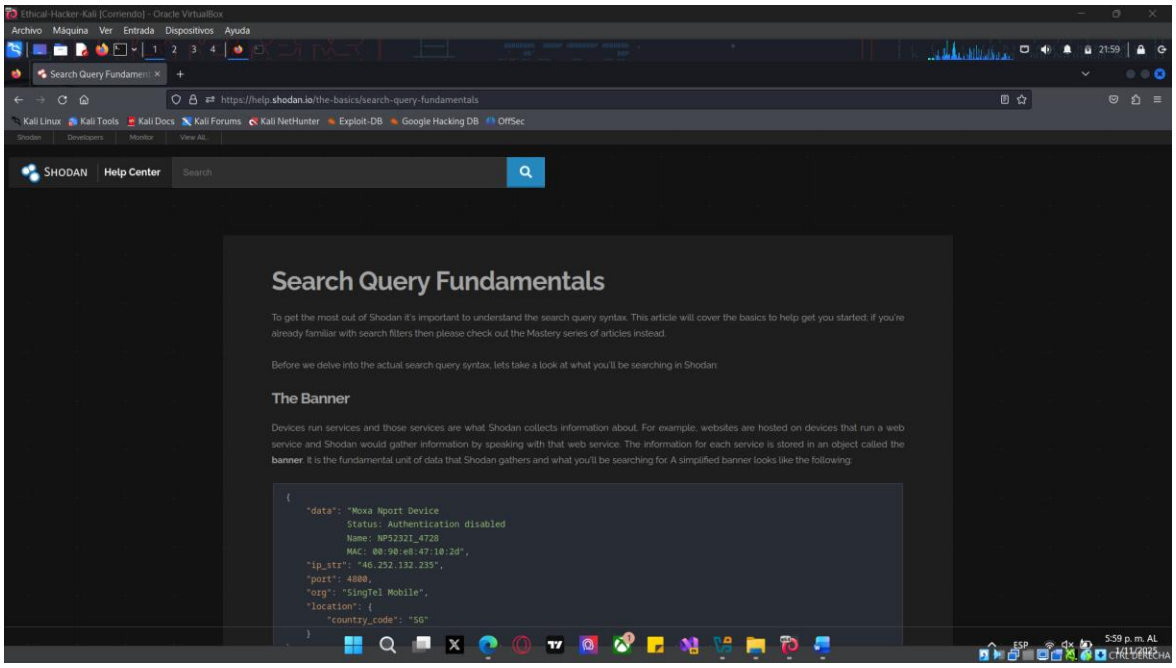
Paso 1: Regístrese para obtener una cuenta de Shodan.

a. Inicie sesión en su VM Kali Linux.

b. Abra el navegador Firefox y vaya a https://www.shodan.io/.

c. Haga clic en el botón **Login** en la parte superior derecha. En la siguiente pantalla, haga clic en el botón **Register** de la barra de menús. Complete su información para crear una cuenta de Shodan. Recibirá un correo electrónico para activar su cuenta.

d. Cuando se complete su registro, inicie sesión en su cuenta de Shodan. Esta es una cuenta gratuita que tiene varias restricciones, incluida la cantidad de resultados que se mostrarán de cada búsqueda. Inicie sesión y vaya a la página de inicio de Shodan. Revise la sección **Getting Started** , especialmente el enlace **Search Query Fundamentals** .



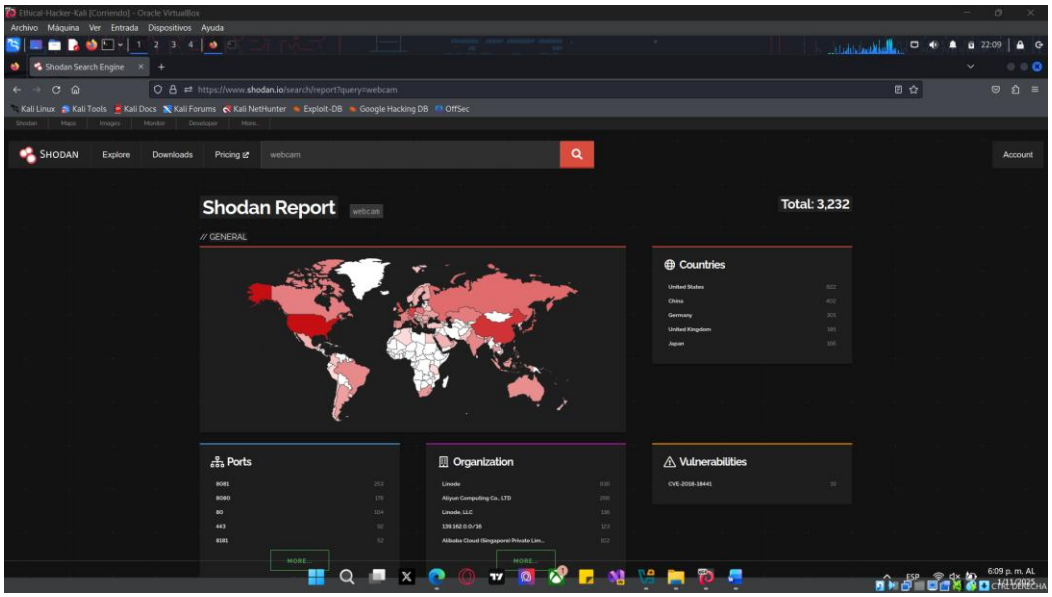
Parte 2: Utilice el sitio web de Shodan para buscar dispositivos de IoT vulnerables

Paso 1: Utilice la barra de búsqueda de Shodan para detectar dispositivos de IoT.

a. En la página de inicio de Shodan, ingrese **webcam** en la barra de búsqueda cerca de la parte superior de la pantalla y presione Intro.

b. Aparecerá una página que muestra los resultados de la búsqueda. En el lado izquierdo de la pantalla hay estadísticas de resumen. Las estadísticas muestran la cantidad total de anuncios de dispositivos que incluyen el término “cámara web”, los principales países donde se encontraron los resultados, las principales organizaciones, los principales productos y los principales sistemas operativos. Puede ver hasta 10 resultados sin un inicio de sesión de Shodan. Los usuarios registrados pueden acceder a 50 resultados de forma gratuita. Los servicios adicionales están disponibles con una suscripción paga.

¿Cuál es el principal país con cámaras web encontrado por Shodan?

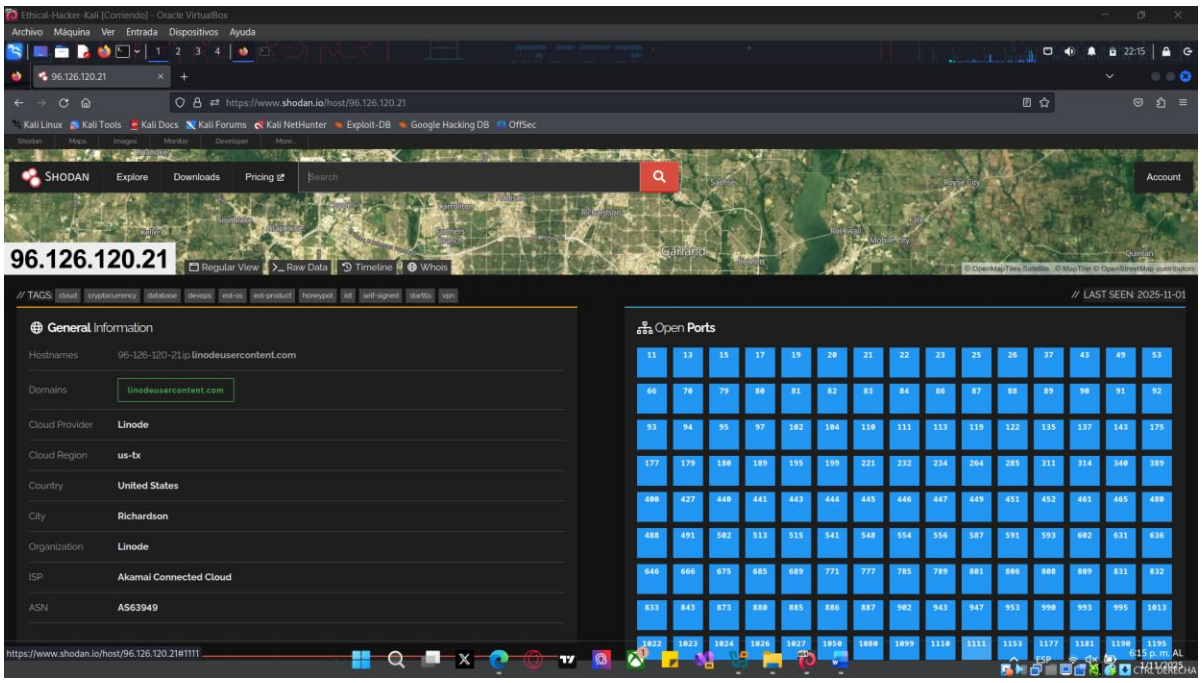


Estados Unidos es el primer país.

HACER CAPTURA DE PANTALLA DONDE SE PUEDA VER LO MENCIONADO

c. Haga clic en una de las direcciones IP que aparecen en los resultados de la búsqueda. Se abre una página con información más detallada. En la parte superior de la página, hay un mapa que muestra la ubicación aproximada del resultado de la búsqueda que seleccionó. Explore la información de varios de los dispositivos que se descubrieron.

¿Qué información se incluye en la sección Información general?

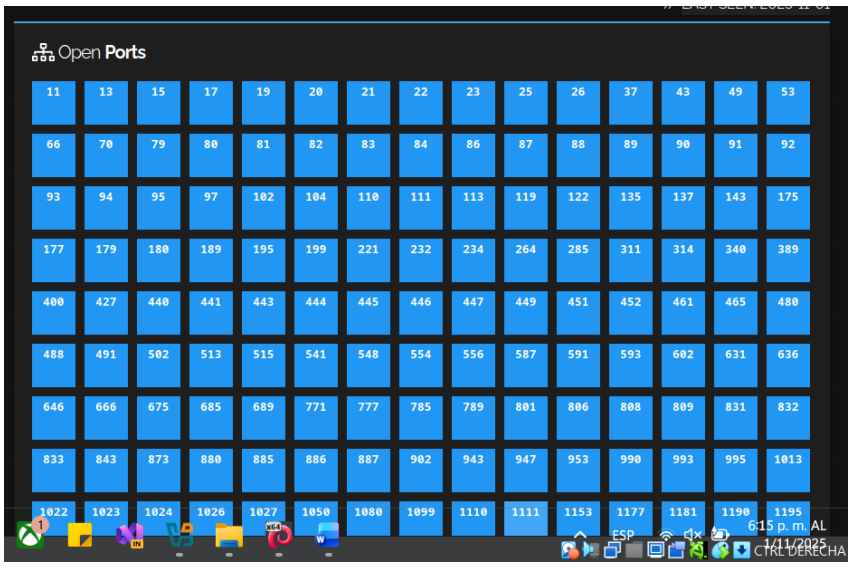


Nombres de host, dominios, país, ciudad, organización, ISP, ASN

HACER CAPTURA DE PANTALLA DONDE SE PUEDA VER LO MENCIONADO

d. En el lado derecho de la salida hay una lista de puertos abiertos que Shodan encontró en el dispositivo.

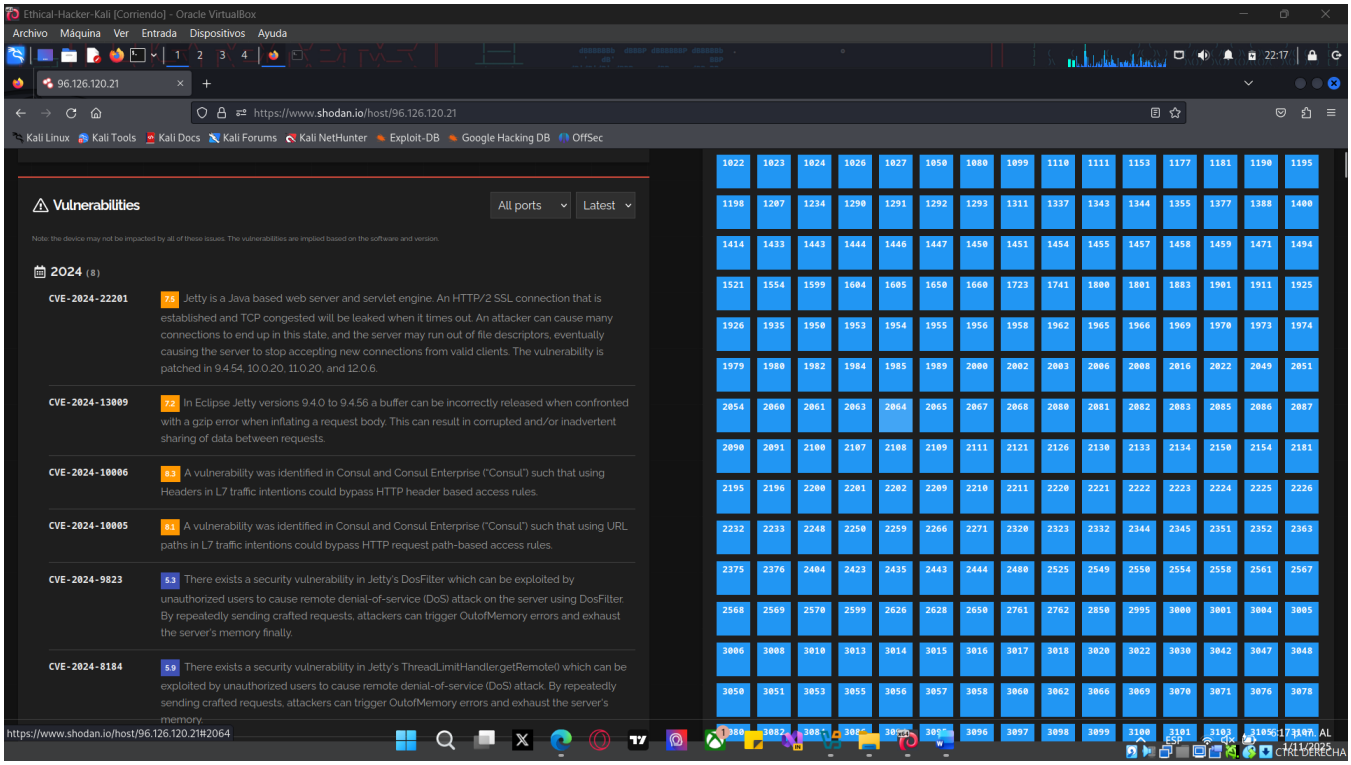
¿Qué puertos están abiertos en la dirección IP que seleccionó?



Las respuestas pueden variar. Los puertos comunes para cámaras web son 8081, 8088 y 80.

HACER CAPTURA DE PANTALLA DONDE SE PUEDA VER LO MENCIONADO

¿Qué información está disponible para los puertos abiertos?



Encabezados, páginas web, certificados y otra información para cada puerto según el servicio.

HACER CAPTURA DE PANTALLA DONDE SE PUEDA VER LO MENCIONADO

Nota: No todos los dispositivos descubiertos son en realidad cámaras web. Son dispositivos que tienen la palabra “webcam” en algún lugar de sus anuncio de servicio.

e. Busque en la web “fabricantes de cámaras web vulnerables”. Con frecuencia, los anuncios del dispositivo nombrarán al fabricante del dispositivo. Intente buscar algunos nombres de fabricantes en Shodan. A partir de los resultados, puede definir mejor los resultados de la búsqueda, a veces con números de modelo específicos del fabricante. Además, busque los inicios de sesión predeterminados utilizados por el modelo de cámara. Es posible que el propietario de la cámara no haya cambiado la contraseña predeterminada. **NO** intente iniciar sesión en dispositivos que no son de su propiedad o que no tienen permiso de acceso.

Paso 2: Utilice filtros de Shodan para refinar los resultados.

Shodan proporciona un método para filtrar los resultados de la búsqueda mediante la sintaxis ***filtro:valor*** sin espacios. Si el valor contiene espacios, como **city:"los angeles&**, debe encerrar el valor entre comillas dobles. Algunos de los filtros de búsqueda más populares son:

PRUEBE CADA UNO DE LOS SIGUIENTES FILTROS UTILIZANDO INFORMACIÓN CORRSPONDIENTE A REPUBLICA DOMINICANA

`país: XX` busca un código de país de 2 dígitos

`ciudad: nombre de la ciudad` Busca una ciudad por nombre

`región: nombre-de-región-o-estado` Busca un estado o región específicos

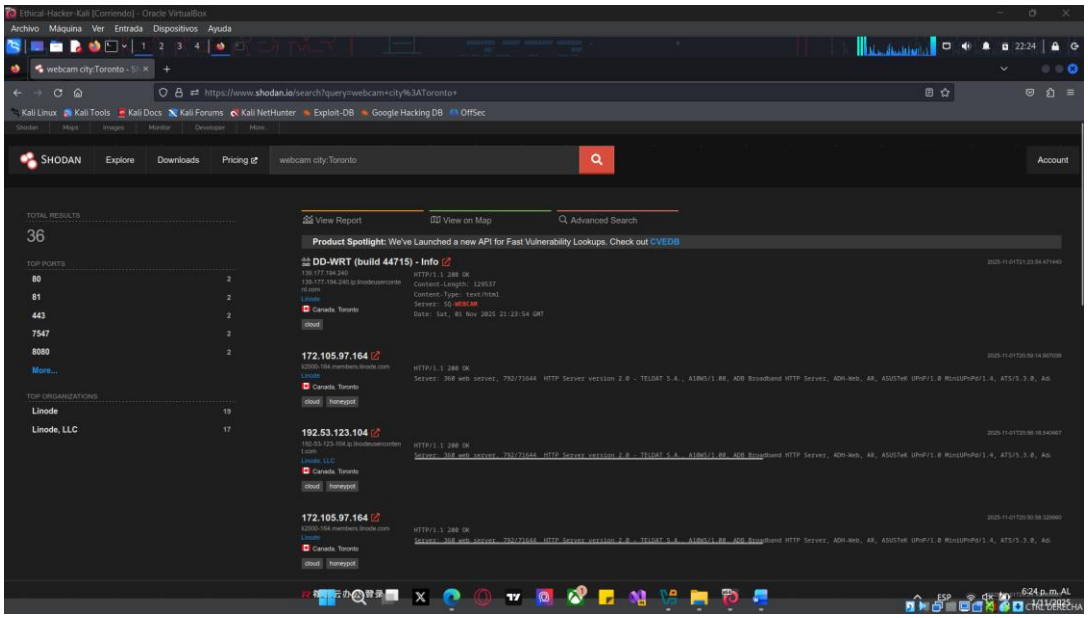
`product: product-name` Busca un producto específico por nombre

`versión:` `XX` busca una versión específica del producto

`vuln: XX` Busca vulnerabilidades que coincidan con un número CVE específico

a. Introduzca un filtro en la barra de búsqueda de Shodan. Este ejemplo devuelve todos los dispositivos con “webcam” en un banner que Shodan encuentra en la ciudad de Toronto.

`webcam city:Toronto`

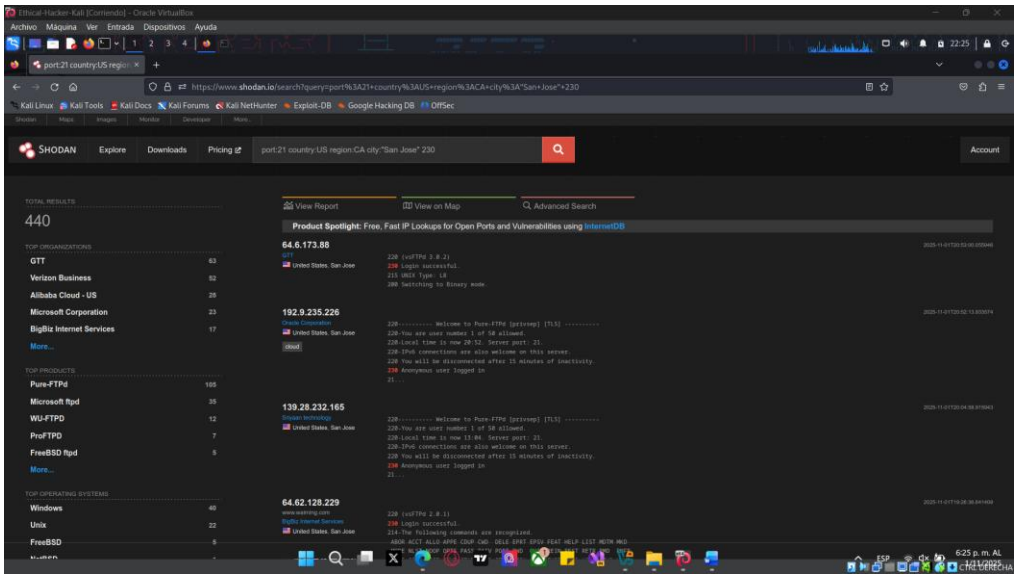


b. Un problema de configuración común que se encuentra en Internet son los servidores FTP que permiten inicios de sesión anónimos. Utilice la cadena de búsqueda para encontrar los servidores FTP en San José, California.

```
port:21 country:US region:CA city:"San Jose" 230
```

Esta búsqueda utiliza el puerto FTP TCP 21 estándar, con filtros de ubicación y una búsqueda de texto para 230. 230 es el código de respuesta de inicio de sesión correcto de FTP.

¿Cuántos servidores FTP encontró Shodan en San José que permitían inicios de sesión anónimos?



Las respuestas pueden variar. En el momento de redactar este informe, había 847.

Paso 3: Utilice Shodan para buscar un producto o servicio específico.

Puede utilizar Shodan para buscar un producto específico, como servidores Apache abiertos en el puerto 80. Formule una consulta para encontrar los servidores Apache en su ciudad.

```
Apache port:80 city:"your-city"
```