

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 escanea o acceda a las redes que posee o tiene permiso de acceso.

Recursos necesarios

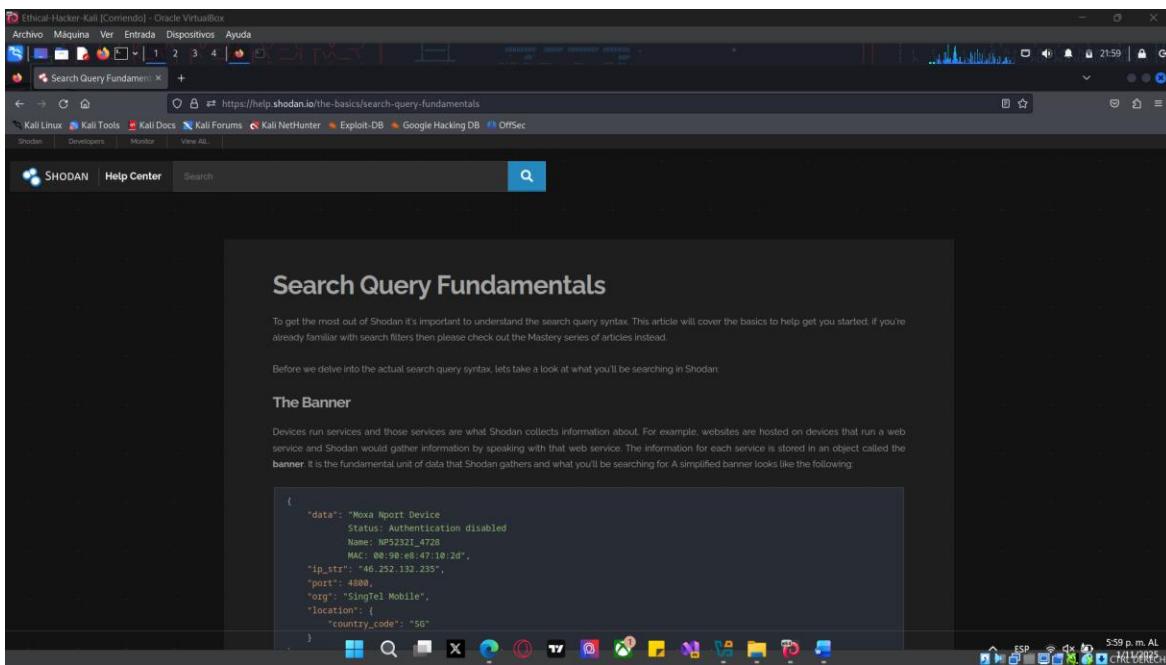
- Kali VM personalizada para el curso de Ethical Hacker
- Acceso a Internet

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**.



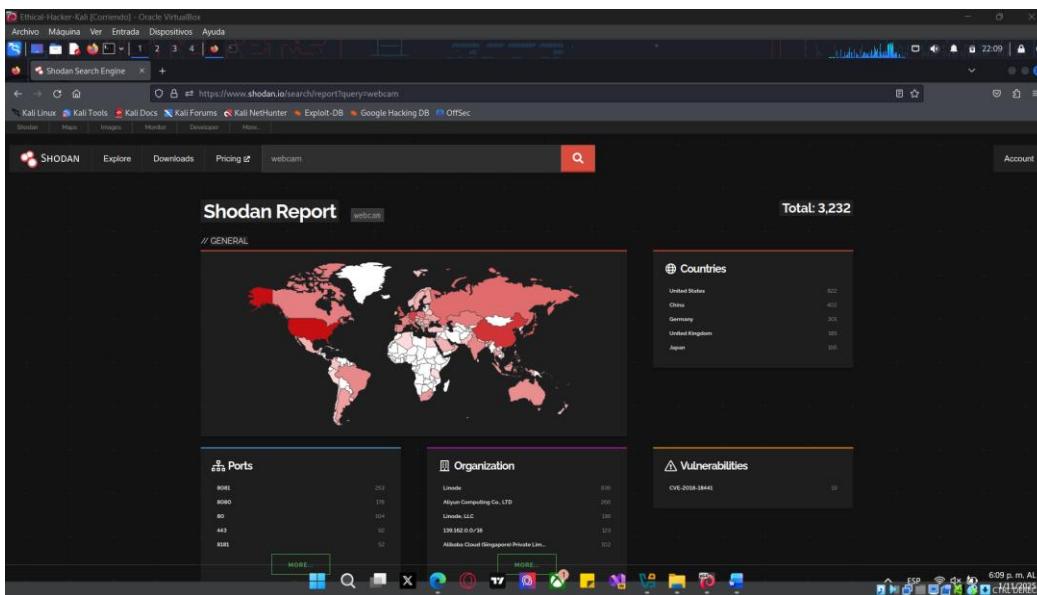
Parte 2: Utilice el sitio web de Shodan para buscar dispositivos de IoT vulnerables

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

- 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.
- 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?

Práctica de laboratorio: Búsquedas de Shodan

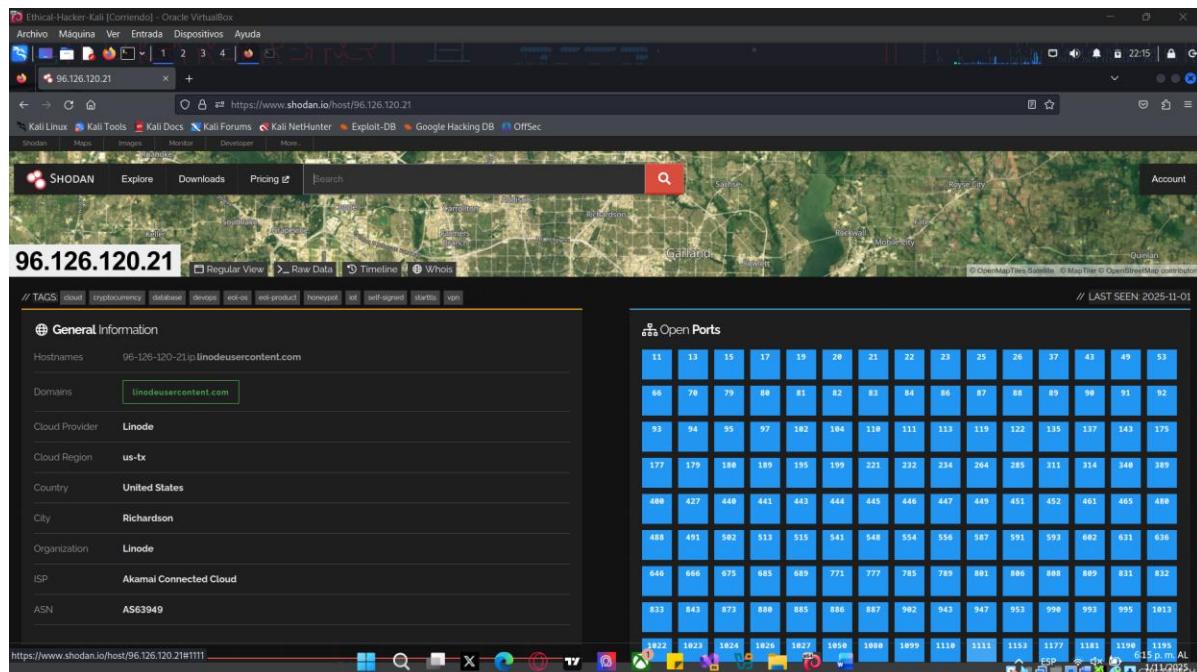


Estados Unidos es el primer país.

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

Práctica de laboratorio: Búsquedas de Shodan

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?

Open Ports															
11	13	15	17	19	20	21	22	23	25	26	37	43	49	53	
66	70	79	80	81	82	83	84	86	87	88	89	90	91	92	
93	94	95	97	102	104	110	111	113	119	122	135	137	143	175	
177	179	180	189	195	199	221	232	234	264	285	311	314	340	389	
400	427	440	441	443	444	445	446	447	449	451	452	461	465	480	
488	491	502	513	515	541	548	554	556	587	591	593	602	631	636	
646	666	675	685	689	771	777	785	789	801	806	808	809	831	832	
833	843	873	880	885	886	887	902	943	947	953	990	993	995	1013	
1022	1023	1024	1026	1027	1050	1080	1099	1110	1111	1153	1177	1181	1196	1195	

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?

The screenshot shows a Shodan search result for an open port. The top part of the interface shows a grid of ports from 11 to 53. Below this, a specific port (port 2064) is selected, displaying a detailed list of vulnerabilities. The vulnerabilities listed include:

- CVE-2024-22201: Jetty is a Java based web server and servlet engine. An HTTP/2 SSL connection that is established and TCP congested will be leaked when it times out. An attacker can cause many connections to end up in this state, and the server may run out of file descriptors, eventually causing the server to stop accepting new connections from valid clients. The vulnerability is patched in 9.4.54, 10.0.20, 11.0.20, and 12.0.6.
- CVE-2024-13009: In Eclipse Jetty versions 9.4.0 to 9.4.56 a buffer can be incorrectly released when confronted with a gzip error when inflating a request body. This can result in corrupted and/or inadvertent sharing of data between requests.
- CVE-2024-10006: A vulnerability was identified in Consul and Consul Enterprise ("Consul") such that using Headers in L7 traffic intentions could bypass HTTP header based access rules.
- CVE-2024-10005: A vulnerability was identified in Consul and Consul Enterprise ("Consul") such that using URL paths in L7 traffic intentions could bypass HTTP request path-based access rules.
- CVE-2024-9823: There exists a security vulnerability in Jetty's DosFilter which can be exploited by unauthorized users to cause remote denial-of-service (DoS) attack on the server using DosFilter. By repeatedly sending crafted requests, attackers can trigger OutOfMemory errors and exhaust the server's memory finally.
- CVE-2024-8184: There exists a security vulnerability in Jetty's ThreadLimitHandler.getRemote() which can be exploited by unauthorized users to cause remote denial-of-service (DoS) attack. By repeatedly sending crafted requests, attackers can trigger OutOfMemory errors and exhaust the server's memory.

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 CORRESPONDIENTE 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

The screenshot shows the Shodan search interface with the query "webcam city:Toronto". The results page lists 36 devices. The first result is a DD-WRT (build 44715) device located at 172.105.97.164. The banner for this device includes the text "DD-WRT (build 44715) - Info" and "DD-WRT 3.0". Other results include 192.53.123.104 and 172.105.97.164, both of which also have banners for DD-WRT.

Práctica de laboratorio: Búsquedas de Shodan

- 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?

The screenshot shows a terminal window titled "Ethereal-Hacker-Kali [Corriendo] - Oracle VirtualBox". The URL in the address bar is <https://www.shodan.io/search?query=port%3A21+country%3AU+region%3ACA+city%3A%22San+Jose%22+230>. The search results page displays 440 results. The first result is for IP 64.6.173.88, which is identified as a Microsoft IIS server in the United States, San Jose. The second result is for IP 192.9.235.226, also a Microsoft IIS server in the United States, San Jose. The third result is for IP 139.28.232.165, another Microsoft IIS server in the United States, San Jose. The fourth result is for IP 64.62.12.229, a Microsoft IIS server in the United States, San Jose. The results list various organizations, top products (Pure-FTPD, Microsoft IIS), and operating systems (Windows, Unix, FreeBSD). The interface includes a sidebar with filters for organization, product, and operating system, and a bottom navigation bar with links like "Shodan", "Maps", "Images", "Monitor", "Developer", and "More...".

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"

The screenshot shows a terminal window titled "Ethereal-Hacker-Kali [Corriendo] - Oracle VirtualBox". The URL in the address bar is <https://www.shodan.io/search?query=Apache+port%3A80+city%3A%22santiago%22+country%3A%22DO%22>. The search results page displays 175 results. The first result is for IP 204.157.254.00, which is a Compañía Dominicana de Teléfonos S.A. server in the Dominican Republic, Santiago de los Caballeros. The second result is for IP 154.88.129.178, also a Compañía Dominicana de Teléfonos S.A. server in the Dominican Republic, Santiago de los Caballeros. The results list various organizations, top products (TELEFONICA, GROTE VREUGDE NV, TELERY NETWORKS, S.R.L.), and top operating systems (Windows, Unix). The interface includes a sidebar with filters for organization, product, and operating system, and a bottom navigation bar with links like "Shodan", "Maps", "Images", "Monitor", "Developer", and "More...".