Shodan

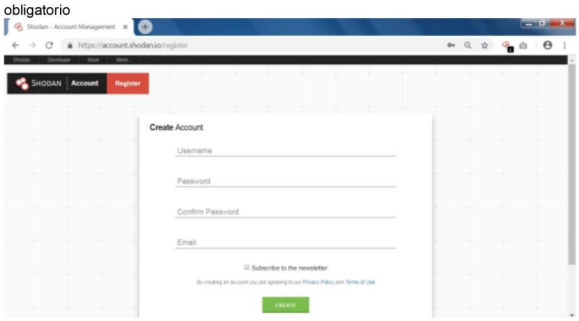
Shodan es un escáner que encuentra dispositivos conectados a través de Internet, puede encontrar dispositivos como semáforos, cámaras de seguridad, aparatos de calefacción para el hogar y monitores para bebés. Este escáner web también puede encontrar sistemas SCADA en estaciones de gas, centrales nucleares, etc. Shodan informa la ubicación física de los dispositivos conectados a través de Internet.

Investigadores en hacking ético del Instituto Internacional de Seguridad Cibernética mencionan que Shodan puede crear una violación en la privacidad de los usuarios porque encuentra casi en cualquier dispositivo conectado a través de Internet sin que el dueño del dispositivo exprese su consentimiento.

Para utilizar Shodan vaya a: https://www.shodan.io/

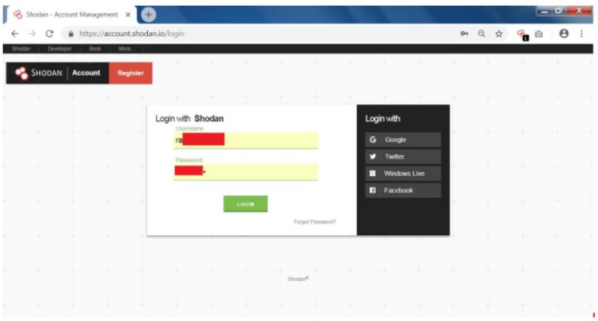
Para crear una cuenta, vaya a ***https://account.shodan.io/register***

- El motor de búsqueda Shodan también se puede utilizar sin registrarse; el registro no es obligatorio

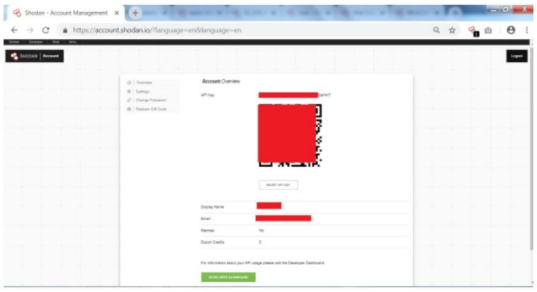


- Ingrese los detalles necesarios: su nombre de usuario, contraseña y correo electrónico para registrarse en Shodan

- Después de crear una cuenta inicie sesión con sus credenciales



- Después de ingresar, Shodan se abrirá. Ahora puede explorar Shodan

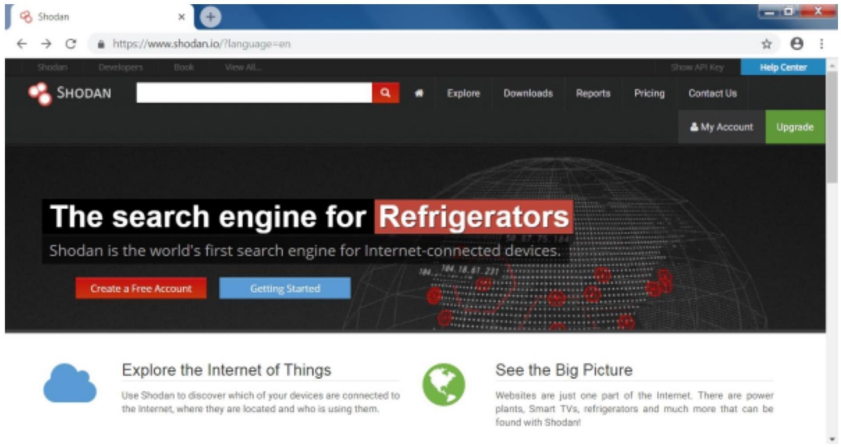


- Después de crear su cuenta en Shodan, inicie sesión en su cuenta y Shodan mostrará la clave de

API de su cuenta. Por razones de seguridad, la clave se ha ocultado en este ejemplo

(ZoxxxxxxPFmYHJvSWhKixxxxxxxxxxHmT)

-

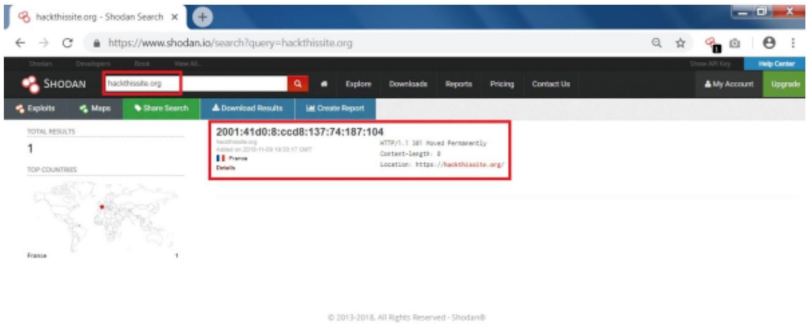


- También puede buscar cualquier sitio web/dirección IP, simplemente ingrese el nombre de su

También puede usar la clave API en recon-ng para el reconocimientoç objetivo y, como se ve a continuación, Shodan mostrará los detalles

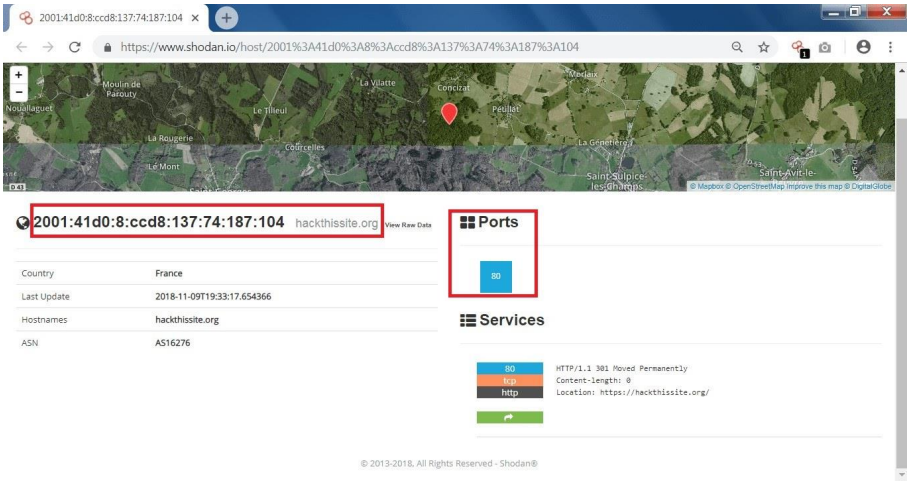
Diversión con Shodan

El sitio mostrado en la siguiente captura de pantalla es el más popular para probar sus habilidades de hacking (hackthissite.org).



- Después de buscar este sitio web, se muestran los puertos abiertos y la dirección IP encontraron

que se puede usar para el footprinting y el reconocimiento



Características de Shodan

Shodan ofrece muchas características excelentes para buscar. El usuario normal puede explorar fácilmente Shodan. La mayoría de los pentesters usan Shodan para encontrar vulnerabilidades.

Hay muchas palabras clave para buscar en Shodan, aquí están algunas que se han usado para mostrar cómo funciona Shodan:

VSAT: funciona principalmente en barcos/rastreador de barcos para detectar barcos/ubicación de barcos

Cameras: muestra las IP abiertas de las cámaras web que se utilizan en la vigilancia

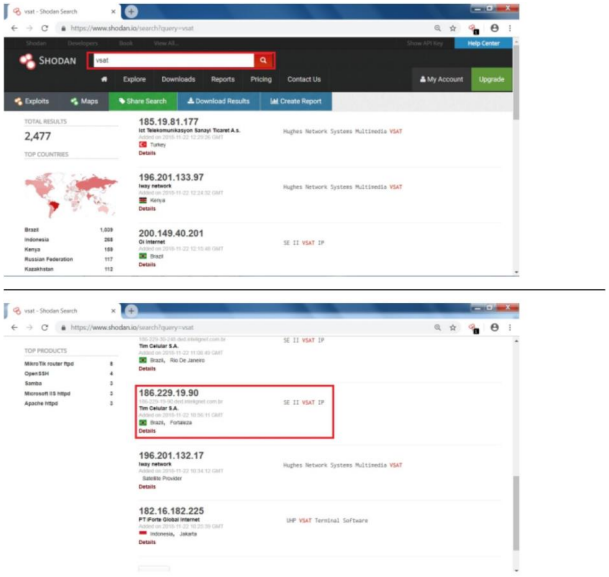
Databases: muestra las bases de datos con falta de seguridad

Video game servers: muestra los servidores abiertos en ejecución de los juegos

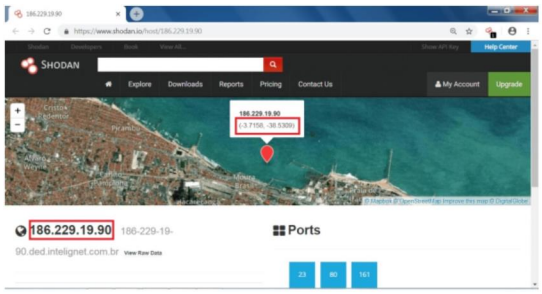
ICS (Sistema de control industrial): muestra los sistemas ICS abiertos vulnerables

Buscar botes con Shodan

Los barcos/embarcaciones utilizan ***VSAT*** (terminal de muy pequeña apertura) que utiliza la comunicación por satélite para comunicarse con el mundo exterior. VSAT utiliza IPv4 para la comunicación. Como Shodan escanea todas las direcciones IP a través de Internet, en este proceso Shodan también enumera las IP asociadas con la comunicación VSAT en el barco. Ahora, en las siguientes capturas de pantalla, verá cómo un usuario normal de Internet puede buscar los barcos en el mar.



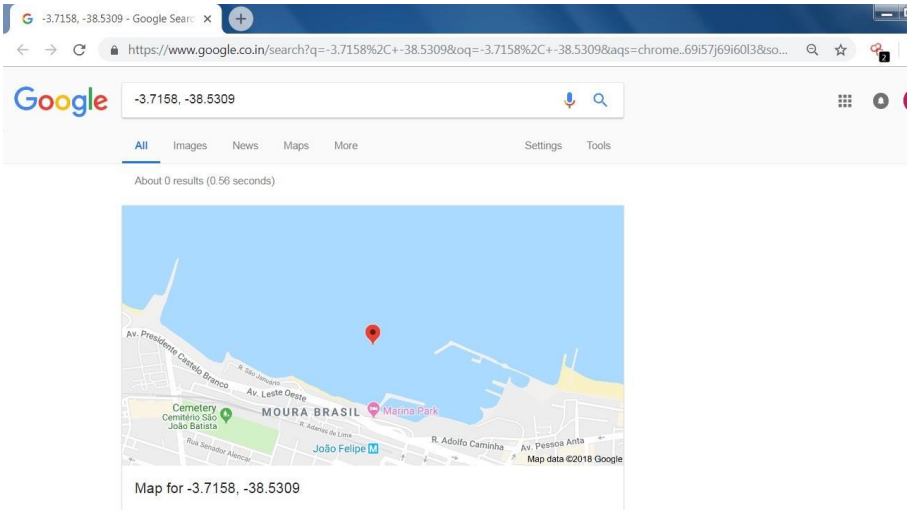
- Si escribe ***VSAT*** en el motor de búsqueda de Shodan, encontrará que hay muchas IPs desprotegidas del barco



- Puede ver en las capturas de pantalla anteriores, puertos abiertos y la dirección IP del barco, que

se pueden usar en otras actividades de hacking

También puede verificar la ubicación del barco escribiendo la longitud y la latitud del barco en el motor de búsqueda de Google

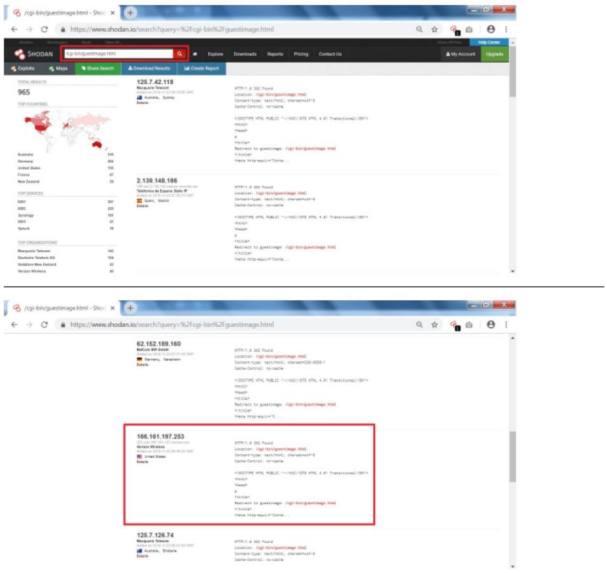


Buscar cámaras de transmisión en vivo

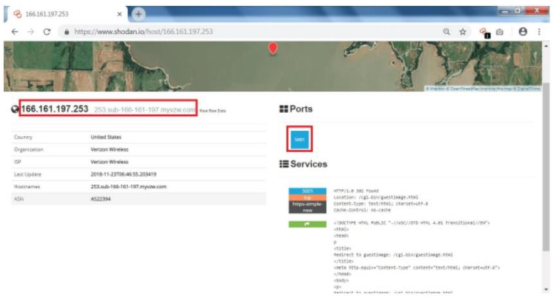
Puede buscar las cámaras en vivo con puertos abiertos. Para buscar en las cámaras web en vivo, vaya al buscador de Shodan y teclee ***webcams*** Por ejemplo:

Para buscar cámaras web, puede escribir ***webcams*** o la consulta de la cámara web que, en su mayoría, es la ruta URL utilizada por la cámara IP Así que buscaremos en ***/cgi-bin/guestimage.html***

- La ruta de la URL anterior es normalmente utilizada por la compañía ***Mobotix***



- Después de buscar en la consulta, hay una IP (166.161.197.253) que examinaremos más a fondo

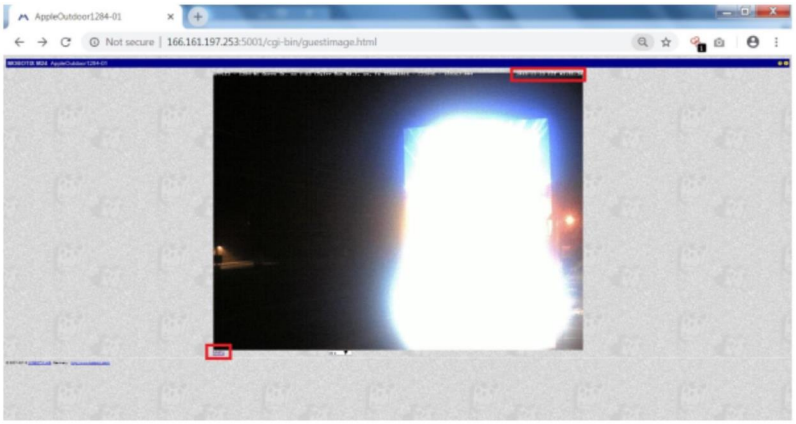


- Después de hacer clic en la IP, puede ver el puerto abierto y la dirección IP de ***com*** desde la

organización ***verizon wireless***

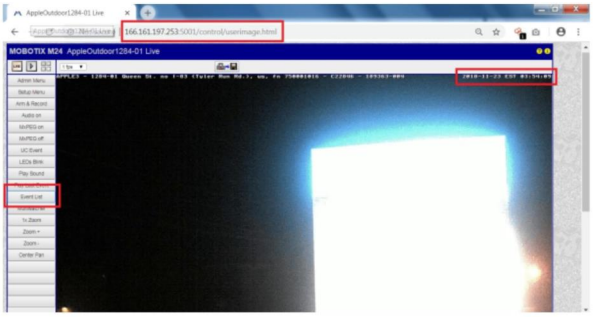
Ahora, para abrir la dirección IP, escriba la dirección IP anterior con el puerto en su navegador

161.197.253:5001 como se muestra a continuación

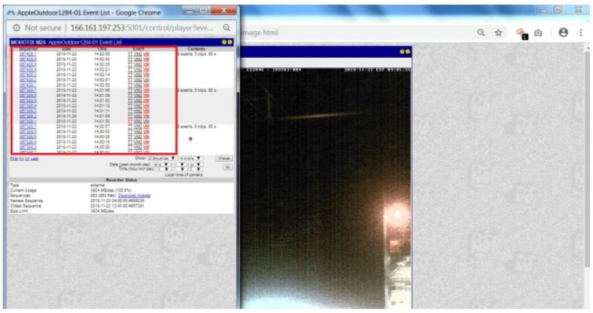


- Como puedes ver, la cámara IP está funcionando pero es de noche. Ahora intentaremos encontrar

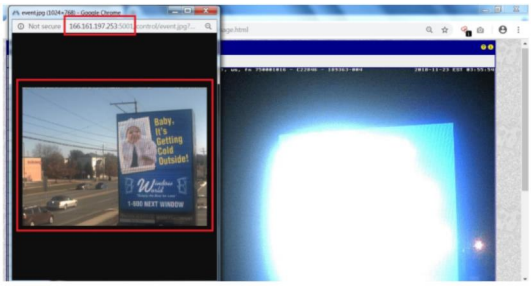
algunas grabaciones previas para verificar si la cámara está funcionando Haga clic en el menú de mercado rojo en la captura de pantalla anterior



- Ir a la lista de eventos



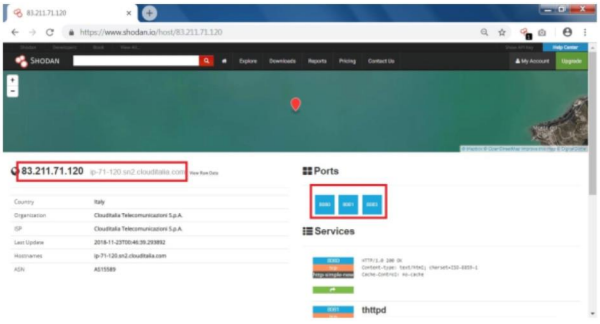
- Como hay muchos registros anteriores, uno de los registros te mostrará el modo de día



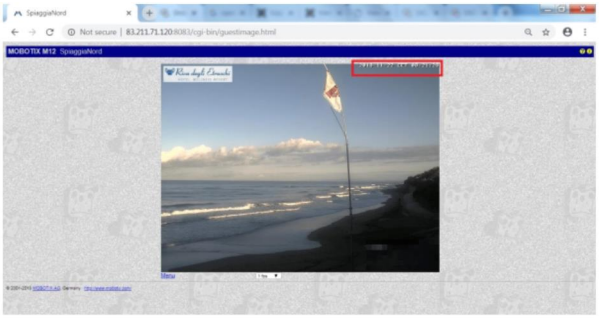
- Uno de los registros anteriores como se puede ver que esta cámara de vigilancia está abierta para

explotar

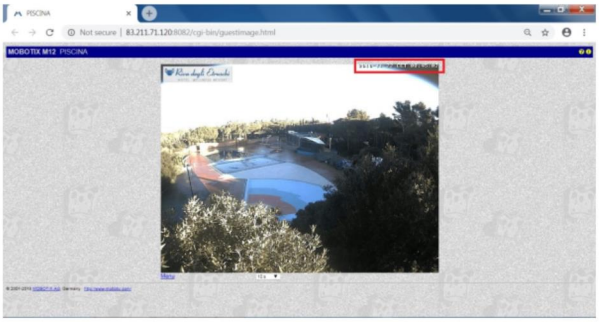
Otra cámara de vigilancia que se encuentra en la lista.



- Cuando abrimos la dirección IP con los puertos listados, encontramos que:

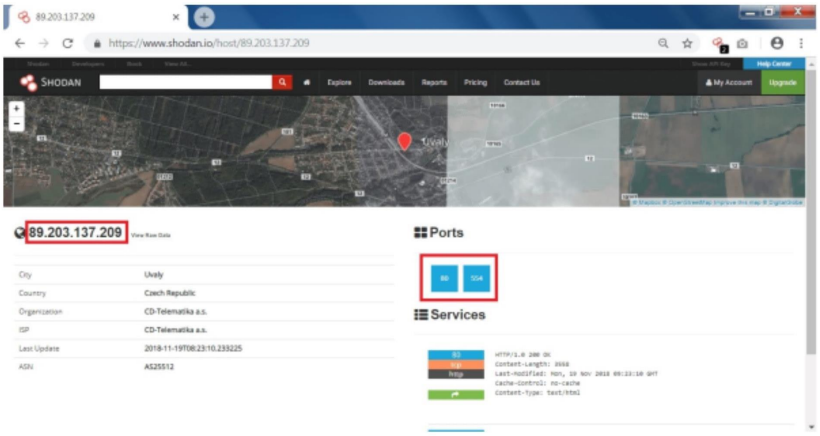


- Cámara de vigilancia de playa

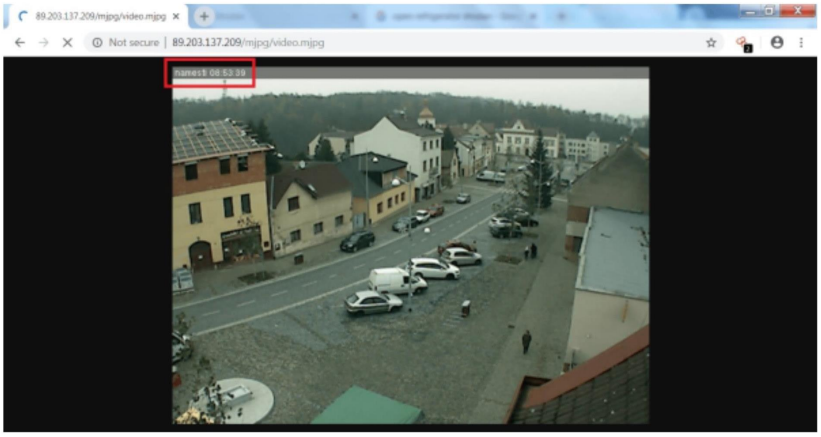


Las capturas de pantalla anteriores son del Hotel Wellness (riva degli etruschi).

Otro ejemplo:



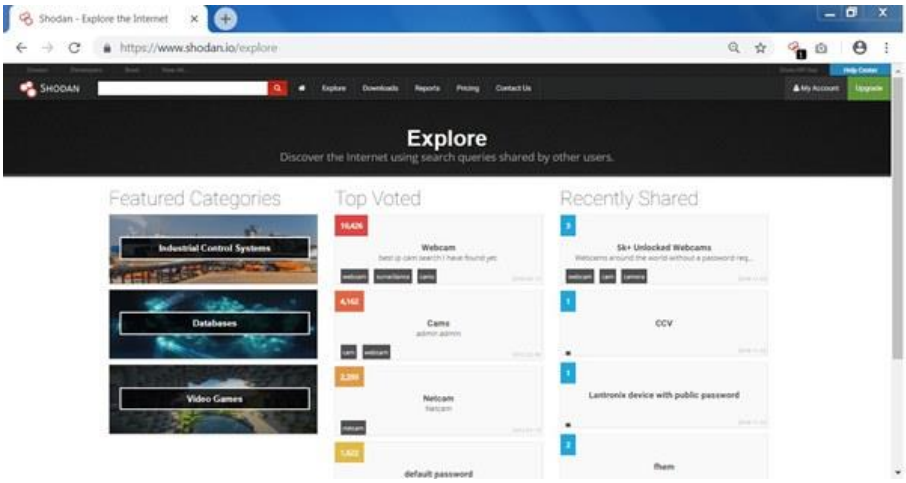
- La apertura de la dirección IP 89.203.117.200 muestra vigilancia en vivo



- La captura de pantalla de arriba es de la República Checa. Una ubicación de la calle local de la cámara en vivo

Otras características de Shodan

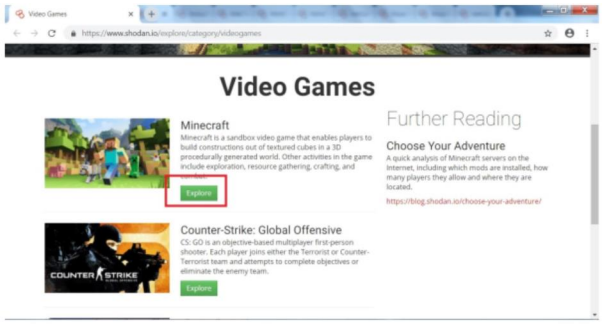
Shodan ofrece múltiples opciones para explorar.



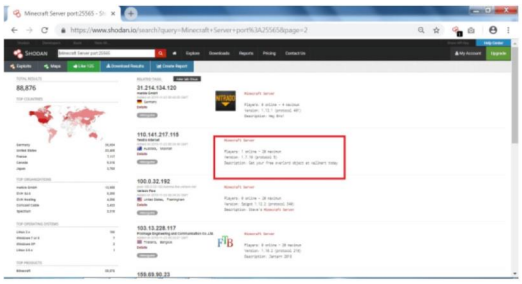
Al hacer clic en explorar, puede encontrar las búsquedas más populares que otros usuarios han realizado en shodan. Se mostrarán las búsquedas más comunes y recientes.

Estas búsquedas comunes se pueden utilizar fácilmente para explotarlas, ya que carecen de seguridad.

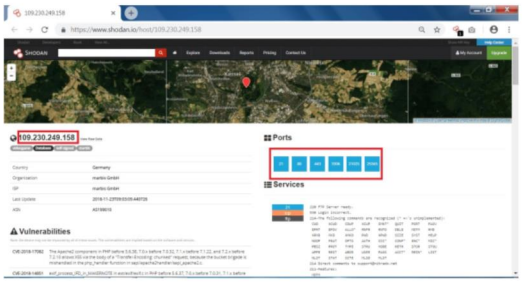
Buscar video juegos

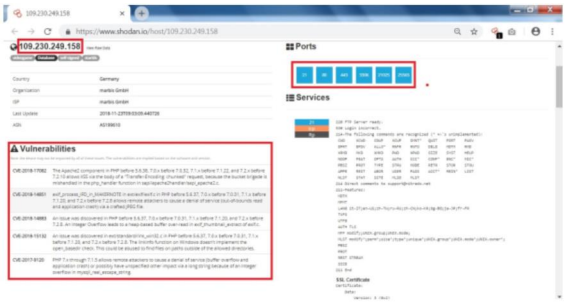


- Puedes abrir los servidores de juegos listados para verificar las direcciones IP



- Aquí hemos elegido el objetivo



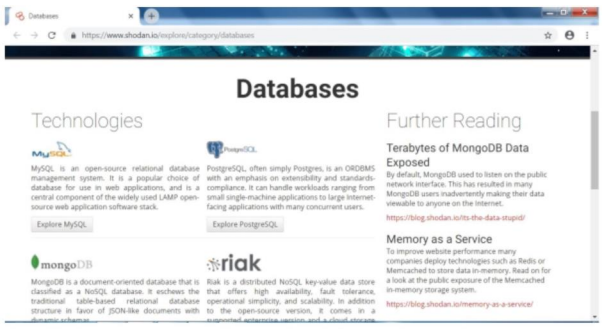


- El servidor de Minecraft se puede utilizar en el escaneo de puertos y en otras actividades de

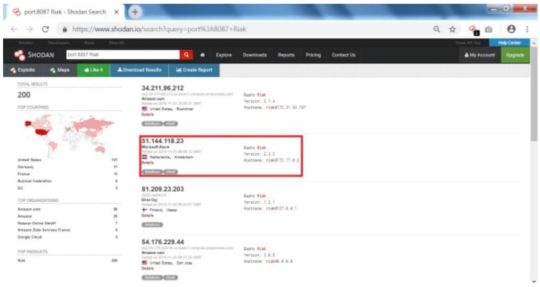
hacking

Los atacantes remotos pueden usar las vulnerabilidades mencionadas anteriormente para causar un ataque de denegación de servicio. Y la vulnerabilidad podría permitir entrar en los directorios

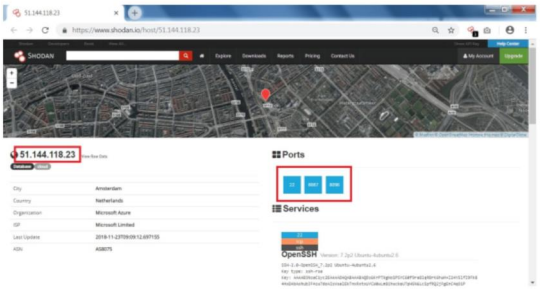
Buscar bases de datos



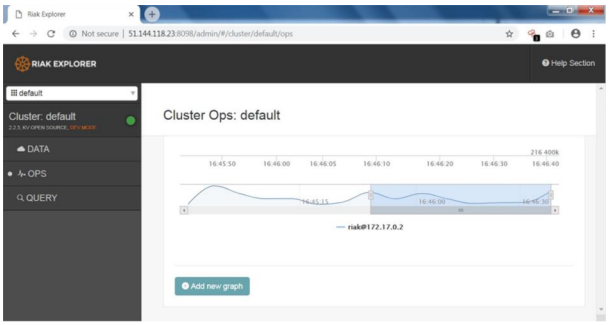
- Escoger la base de datos

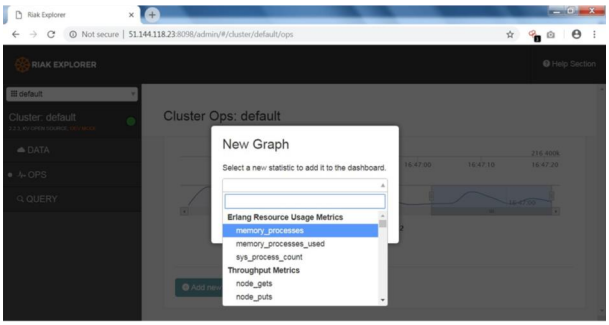


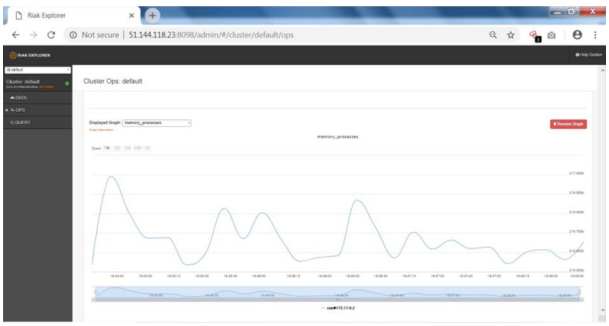
- Seleccionar el objetivo



- En la captura de pantalla anterior, puede usar la dirección IP con los puertos listados para abrir la página db



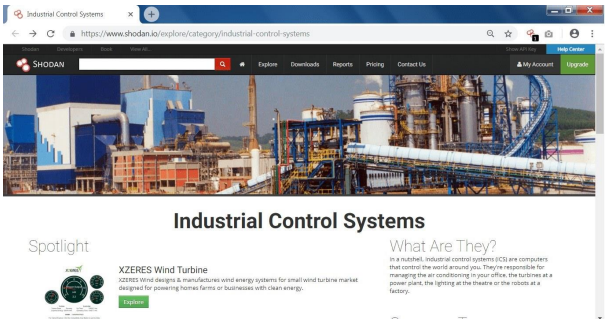


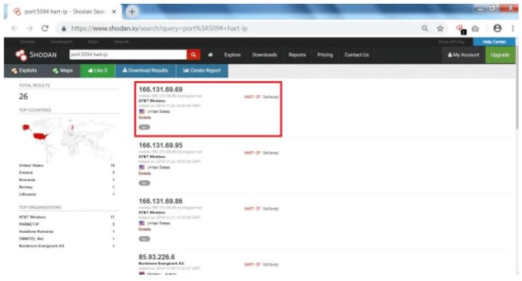


Muestra la gráfica del proceso de memoria que se puede utilizar en la fase inicial de las pruebas de penetración

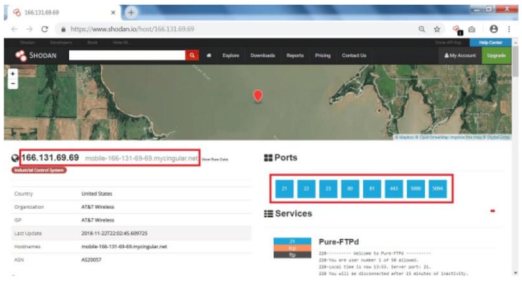
- Como puede ver las capturas de pantalla anteriores, los detalles de administración anteriores se pueden usar en otras actividades de hacking

Buscar sistemas de control industrial





- Seleccionar el objetivo



- La dirección IP anterior y los puertos abiertos se pueden usar en la exploración de puertos
- En las capturas de pantalla anteriores, las vulnerabilidades enumeradas pueden provocar ataques

masivos al objetivo. Los atacantes pueden usar el ataque de denegación de servicio. La ejecución remota también se puede hacer en este sitio web vulnerable

Usar la extensión de Google Chrome

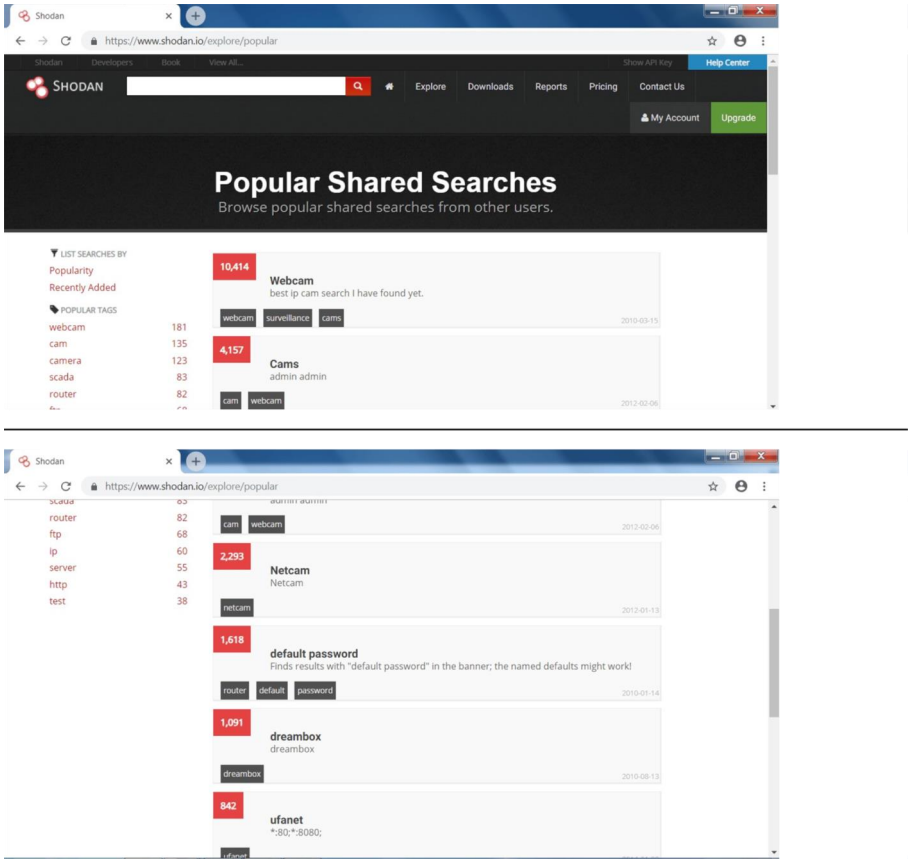
Para obtener información rápida, también puede usar el complemento de Google Chrome, que está disponible en la tienda de aplicaciones de Chrome. Para instalar el complemento para Shodan en Chrome, vaya a:

https://chrome.google.com/webstore/detail/shodan/jjalcfnidlmpjhdfepjhjbhnhkbgleap?utm_source=chrome-ntp-icon

Después de instalar el complemento, siempre que abra el sitio de destino se iniciará el complemento de Shodan e iniciará su consulta y mostrará los puertos abiertos/dirección IP del sitio web objetivo

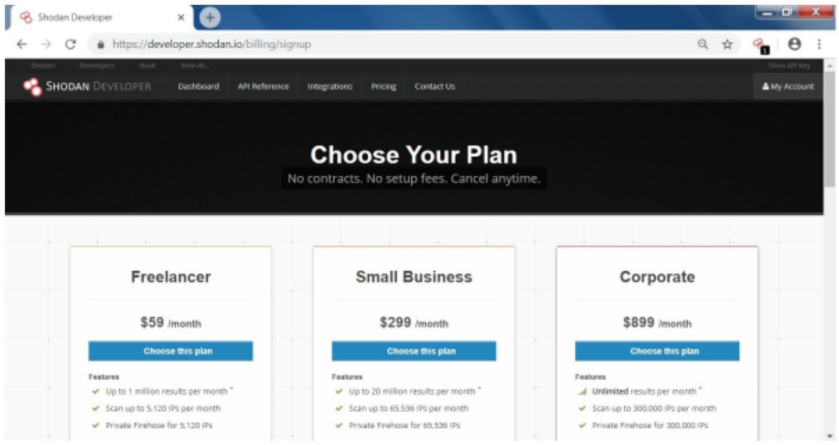
Búsquedas populares

Shodan ofrece muchas funciones como buscar cualquier cámara abierta o buscar enrutadores con de seguridad predeterminada.



En la captura de pantalla anterior están algunos de los dispositivos abiertos enumerados que se pueden usar en actividades de hacking. Las búsquedas más populares son fáciles de encontrar y también pueden ser explotadas por script kiddie.

Planes de pago



- También puede usar los planes pagados si trabaja como pentester profesional porque Shodan

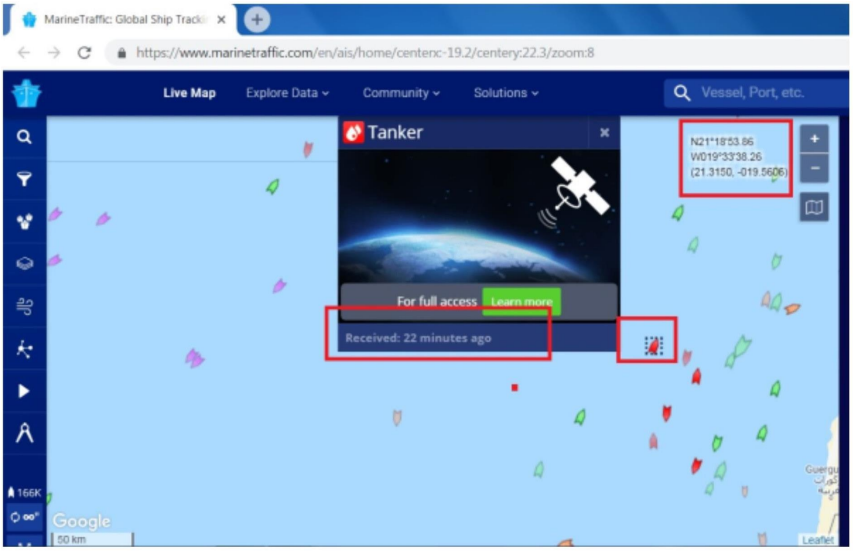
proporciona información detallada para el objetivo

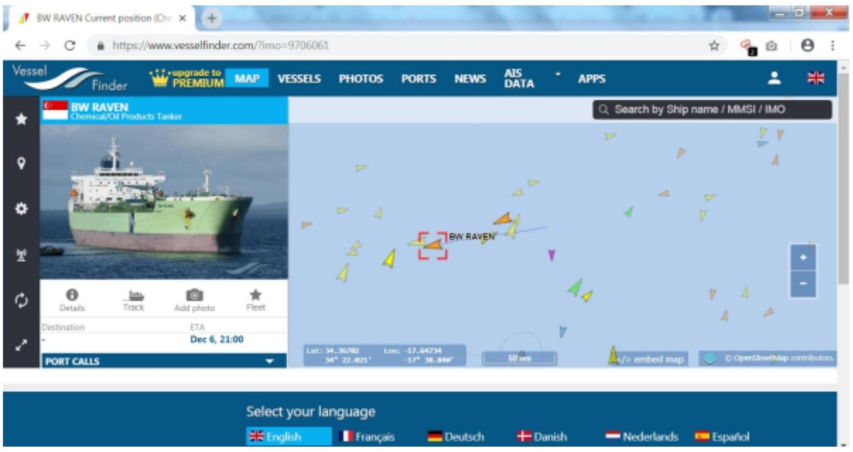
Otros recursos

También puede utilizar algunos otros recursos para verificar la latitud y longitud del barco.

https://shiptracker.shodan.io https://www.vesselfinder.com https://www.marinetraffic.com

Estos sitios web proporcionan AIS (sistema de identificación automática) que usa un dispositivo transpondedor para recibir la señal al satélite y luego transmitir esas señales al receptor para indicar su ubicación, pero el rastreador de Shodan es más que eso.





- Como puede ver en las capturas de pantalla anteriores, hay dos sitios web que muestran la

ubicación del envío utilizando el sistema AIS. El usuario normal puede verificar la ubicación del sitio web. Estos dos sitios web muestran la longitud y latitud de la nave

Búsquedas intesantes

Dispositivos IoT

- title:"WebcamXP" - Cámaras web públicas
- port:554 has_screenshot:true - Cámaras IP accesibles

- netcam.dlink.com - Cámaras D-Link
- server:SQ-WEBCAM - Cámaras con servidor SQ-WEBCAM

Redes y Dispositivos de Comunicaciones

- port:21 "220" - Servidores FTP abiertos
- port:22 "SSH" - Servidores SSH
- port:161 "public" - Dispositivos SNMP sin protección
- port:5060 - Sistemas VoIP expuestos

Servidores Web

- http.title:"index of" - Directorios abiertos
- http.html:"It works!" - Servidores Apache por defecto
- http.title:"Admin Login" - Portales de administración web
- http.favicon.hash:116323821 - Páginas de inicio de sesión de Cisco

Cámaras de Vigilancia

- title:"Hikvision" - Cámaras Hikvision
- port:80 Server:AVTech - Cámaras AVTech
- html:"ViewerFrame?Mode=" - Cámaras de acceso directo
- server:"GWS/2.4" - Cámaras GoAhead

Bases de Datos

- port:27017 "MongoDB Server Information" - Servidores MongoDB abiertos
- port:3306 - Servidores MySQL sin protección
- port:9200 "Elastic" - Elasticsearch sin seguridad
- port:5432 PostgreSQL - Servidores PostgreSQL

Sistemas de Control Industrial (ICS/SCADA)

- port:502 - Dispositivos Modbus
- port:1911 - Sistemas BACnet
- port:102 - Sistemas Siemens S7
- port:20000 "DNP3" - Dispositivos DNP3

Domótica y Hogares Inteligentes

- port:8883 - Dispositivos MQTT sin autenticación
- port:8083 - Puertas abiertas en Smart Hubs
- title:"Sonoff" - Dispositivos de automatización Sonoff
- http.html:"Welcome to Home Assistant" - Servidores Home Assistant expuestos

Sistemas de Videovigilancia

- port:8000 - Servidores DVR Hikvision
- port:37777 - Sistemas Dahua
- port:554 - Transmisión RTSP pública
- http.html:"Network Camera" - Cámaras de red expuestas

Infraestructura Crítica

- port:502 "modbus" - Controladores industriales
- port:47808 - Controladores BACnet
- port:9600 "grid" - Sistemas de energía
- port:20000 - Dispositivos SCADA

Sistemas de Acceso y Seguridad

- http.title:"Login" - Paneles de inicio de sesión
- http.html:"admin" - Páginas administrativas
- port:8080 "webmin" - Interfaces Webmin abiertas
- port:8443 - Consolas de administración de seguridad

Claro, aquí tienes un listado ampliado de búsquedas para cámaras IP accesibles:

Búsquedas Generales de Cámaras IP

- port:554 has_screenshot:true - Cámaras IP accesibles con capturas de pantalla disponibles
- port:80 http.html:"Network Camera" - Cámaras de red accesibles
- port:8080 http.html:"Live View" - Cámaras con vista en vivo habilitada
- port:8000 "video stream" - Flujos de video accesibles

Cámaras Específicas por Marca

- title:"IP Camera Viewer" - Cámaras genéricas

- server:"GoAhead-Webs" - Cámaras GoAhead
- server:"uc-httpd" - Cámaras Trendnet
- server:"IPCam" - Cámaras IP genéricas
- title:"AXIS" - Cámaras Axis
- html:"MOBOTIX" - Cámaras MOBOTIX
- server:"NetSurveillance" - Cámaras NetSurveillance (genéricas)
- title:"webcamXP" - Cámaras utilizando webcamXP

Búsquedas por Protocolo o Servicios

- port:554 rtsp - Cámaras con RTSP habilitado
- port:8080 "Server: IP Webcam" - Cámaras Android con IP Webcam
- port:81 "video.cgi" - Flujos de video en CGI
- port:8888 - Cámaras accesibles en el puerto 8888

Combinaciones de Títulos y URL

- title:"Live View / - AXIS" - Cámaras AXIS con vista en vivo
- http.title:"D-Link DCS-" - Cámaras D-Link
- http.html:"AVTech" - Cámaras AVTech
- http.html:"ViewerFrame?Mode=" - Cámaras con visualización directa

Búsquedas Adicionales

- title:"Hikvision - Webs" - Cámaras Hikvision accesibles
- port:85 has_screenshot:true - Cámaras accesibles en puertos alternativos
- html:"realmonitor" - Flujos de cámaras Dahua
- http.html:"VIVOTEK" - Cámaras Vivotek