



INSTITUTO TECNOLÓGICO SUPERIOR “HUAQUILLAS”

Manual Shodan

Manual Técnico

Tecnología:
<ul style="list-style-type: none">• Superior en Redes y Telecomunicaciones

Autora:

Alejandro Becerra, Jessica Pilar

Huaquillas – Ecuador

2019

Índice de contenido

Índice de contenido	2
Índice de figuras	3
1. Introducción.....	4
1.1. Objetivo General	5
1.2. Objetivos Específicos	5
2. Contenido técnico.	6
2.1. Shodan	6
2.1.1. Uso de Shodan.....	6
3. Responsable	14
4. Referencias	15

Índice de figuras

Figura 1. Interfaz Shodan	7
Figura 2. Interfaz Explorador de Shodan	7
Figura 3. Interfaz Parámetros	8
Figura 4. Resultados de búsqueda.....	9
Figura 5. Interfaz Datos cámara	9
Figura 6. Geolocalización de la cámara.....	10
Figura 7. Visión de la cámara	10
Figura 8. Interfaz configuración de la cámara.....	11
Figura 9. Cámaras Hikvisión	11
Figura 10. Interfaz de configuración cámara Hickvisión.....	12
Figura 11. Parámetros de configuración de la cámara Hickvision.....	13

1. Introducción

La seguridad de la infraestructura tecnológica es un tema de interés para todo administrador de dichos recursos, para ello es necesario usar diferentes herramientas existentes en el mercado, algunas de ellas son de pago otras libres. De acuerdo a las necesidades de cada institución se seleccionará la más adecuada.

La finalidad de realizar el presente documento es presentar el uso de una de los buscadores web que sirven para identificar servicios y sistemas conectados a internet, el cual permite identificar información cómo las IP's de los dispositivos tecnológicos conectados a la web, permitiendo determinar las vulnerabilidades que estos pueden presentar. En el presente manual se explica la utilidad en las cámaras IP.

El documento está compuesto por la descripción de los objetivos, que determinan la razón de ser del documento, seguido a ello se indica con el contenido del manual el cual describe brevemente la herramienta y los pasos para su uso; en las últimas secciones se encontrará información sobre la responsable del documento, así como glosario y bibliografía usada.

1.1. Objetivo General

Identificar vulnerabilidades en las cámaras IP usando el motor de búsqueda Shodan.io difundiendo los beneficios de usar esta herramienta a los administradores de redes de datos.

1.2. Objetivos Específicos

- Investigar los fundamentos de la herramienta
- Analizar la seguridad de las cámaras IP ubicadas en el territorio ecuatoriano usando Shodan.io.
- Difundir el presente documento para que sea usado como una guía para los administradores de redes.

2. Contenido técnico.

2.1. Shodan

Se lo conoce como el motor de búsqueda de los hackers, con el objetivo de realizar tareas de investigación de nuevas vulnerabilidades. No obstante, esta herramienta puede usarse con fines maliciosos a razón de la cantidad de información detallada que se proporciona con cada búsqueda realizada. Auditores, investigadores y toda persona que necesite información sobre dispositivos en general, puede recibir información muy útil en cuestión de minutos. (Mendoza, 2018)

“Este motor de búsqueda está enfocado únicamente a buscar sistemas y servicios conectados a internet “ (Rizaldos, 2018).

A raíz de la evolución de la tecnología existen muchos dispositivos conectados a la red, pudiendo ser identificados por herramientas como Shodan, las cuáles pueden identificar todas los equipos inteligentes conectados a la red, de tal manera que si no se encuentran configurados de forma adecuada se puede acceder a sus datos de conectividad, convirtiéndolos en vulnerables a personas inadecuadas, por ello la importancia de monitorear frecuentemente la seguridad de dichos dispositivos e implementar mecanismos de defensa o simplemente realizar las configuraciones adecuadas. Así como esta herramienta puede ser usada para fines maliciosos, también puede ser usada para monitorear dicha seguridad, ya que al usar diferentes parámetros se puede establecer el grado de vulnerabilidad de los equipos conectados a la web.

2.1.1. Uso de Shodan

1- Dirigirse al navegador e ingresar a la página oficial de Shodan:

<https://www.shodan.io/>

2- En la parte superior, en el menú selecciona “Explorar”.



Figura 1. Interfaz Shodan
Fuente: (Shodan, 2013)

3- A continuación, haga doble clic en la opción de “Netcam”.

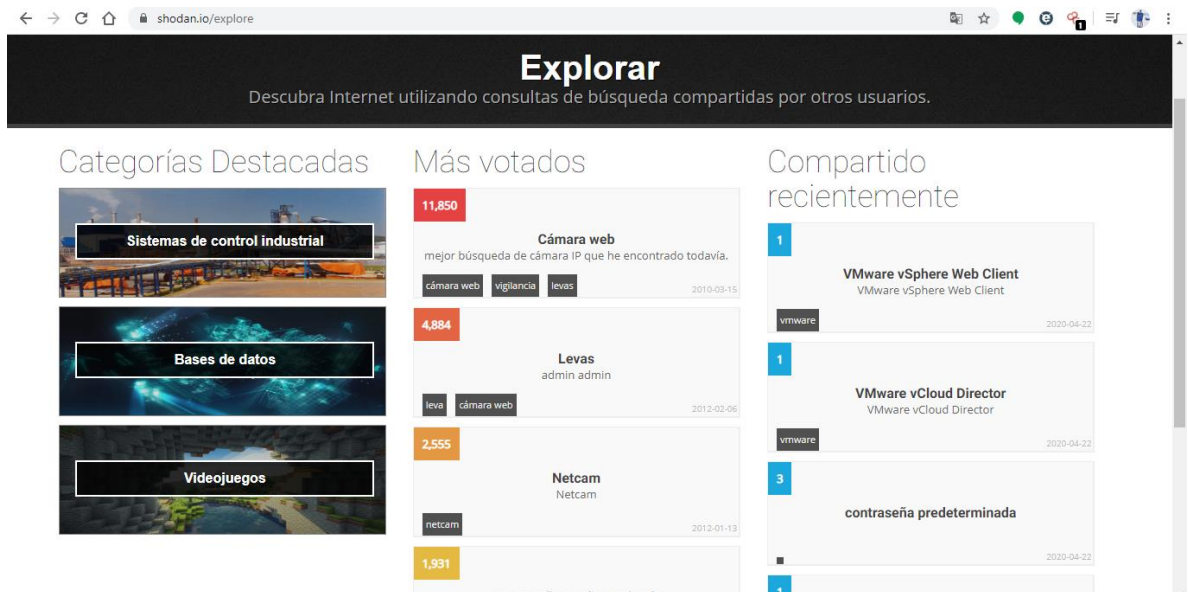


Figura 2. Interfaz Explorador de Shodan
Fuente: (Shodan, 2013)

- 4- Aparece todas las cámaras que son Netcam en todo el mundo. Para ser más específicos en la barra superior, en el buscador se le añade "Country" y entre comillas el país donde se quiere buscar "netcam country: "EC"
- 5- Con este comando se muestra todas las cámaras netcam en el Ecuador.

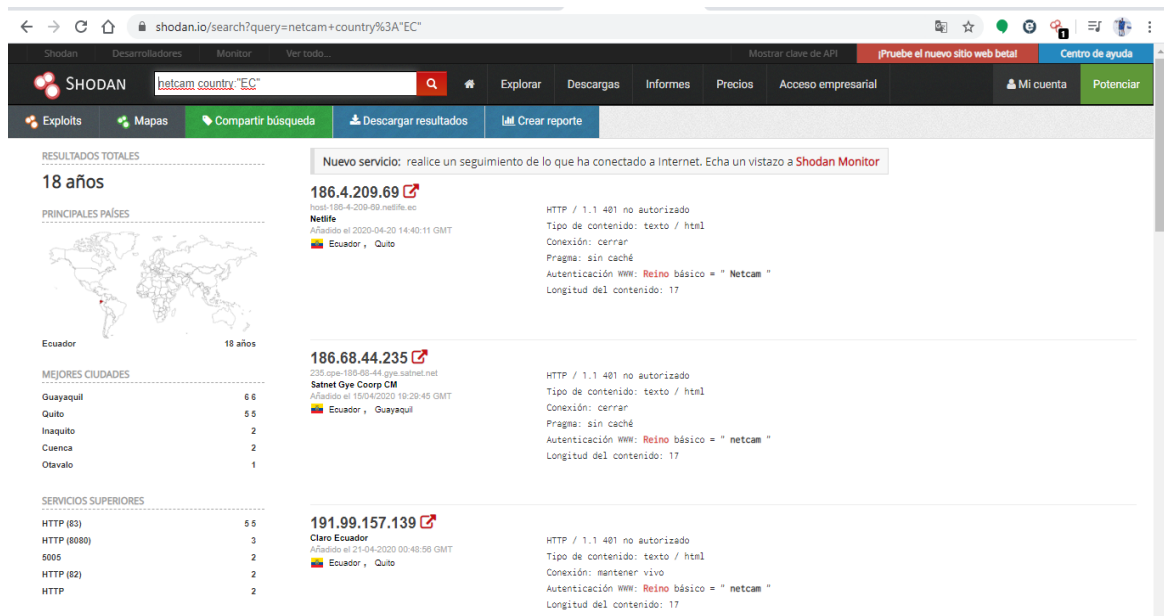


Figura 3. Interfaz Parámetros
Fuente: (Shodan, 2013)

- 6- Clic en el cuadro que esta alado de una de las direcciones ip de cualquier cámara . Se escoge la cámara con ip 186.101.235.242

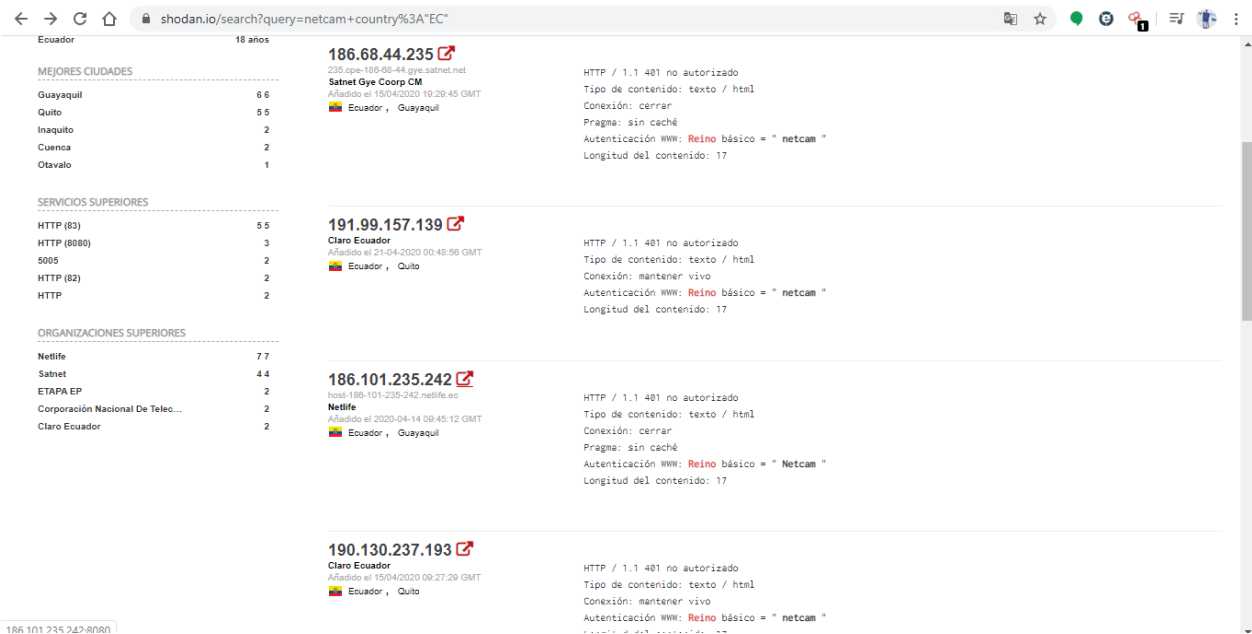


Figura 4. Resultados de búsqueda
Fuente: (Shodan, 2013)

Pedirá usuario y contraseña, pero este tipo de cámara es vulnerable a su uso ya que tiene la contraseña por defecto que es admin y contraseña admin

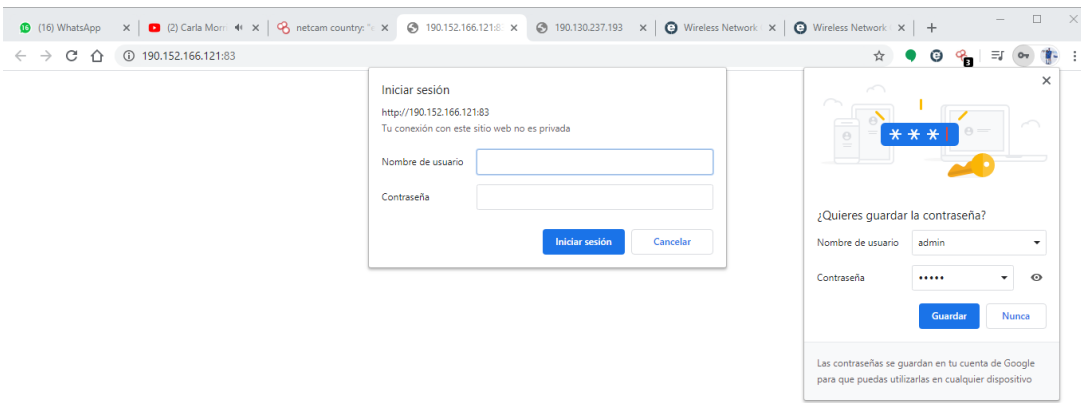


Figura 5. Interfaz Datos cámara
Fuente: (Shodan, 2013)

7- Se ingresa y muestra lo que está grabando en ese lugar en este caso es una cámara ubicada en el corredor de una vivienda en la ciudad de Guayaquil

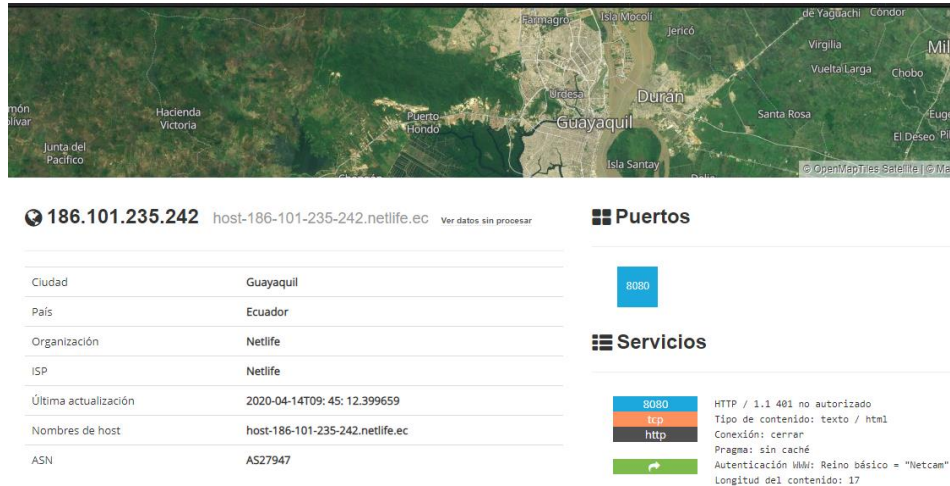


Figura 6. Geolocalización de la cámara
Fuente: (Shodan, 2013)

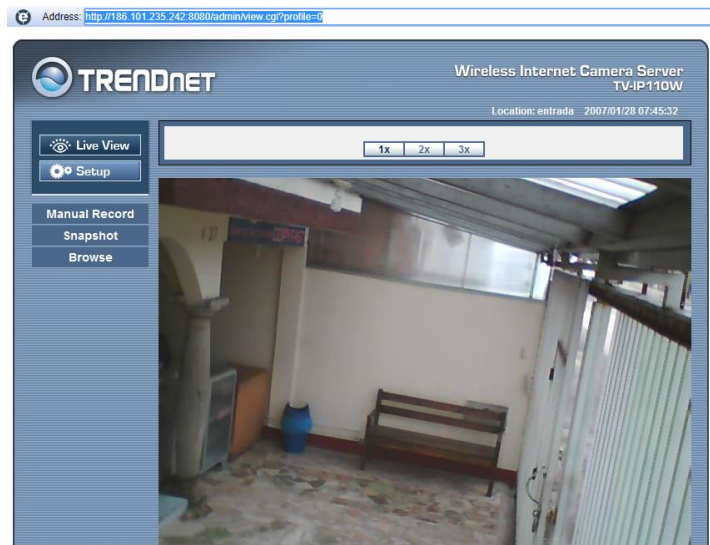


Figura 7. Visión de la cámara
Fuente: (Shodan, 2013)

Como tenemos el acceso total de la cámara se puede configurar cualquier parámetro de ella.

8- Para realizar cambios se dará clic en “Setup” logrando verificar las configuraciones que tiene el dispositivo.

Uno de los datos de la configuración que se puede modificar es la dirección ip la cual si se cambia del rango puesto aquí la cámara se dejaría de emitir video al usuario y nadie podría acceder a ella.

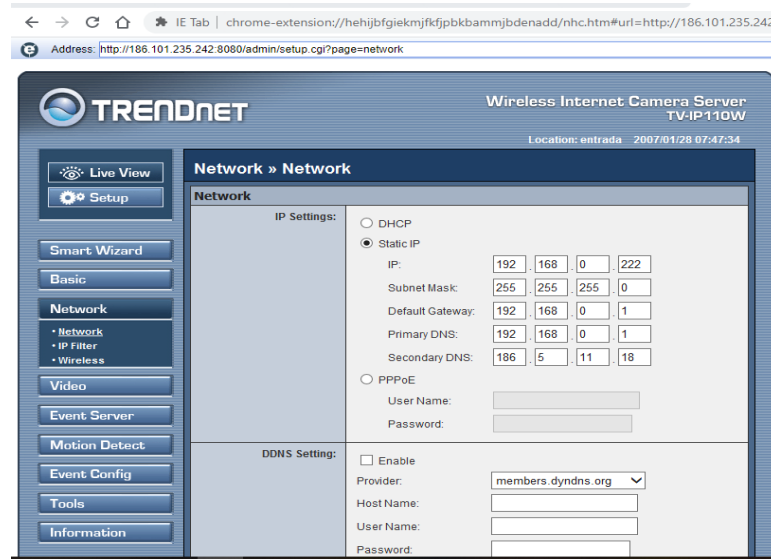


Figura 8. Interfaz configuración de la cámara
Fuente: (Shodan, 2013)

9- También se puede realizar la búsqueda con una marca de sistema de videovigilancia más conocida como la de Hikvision ejemplo:

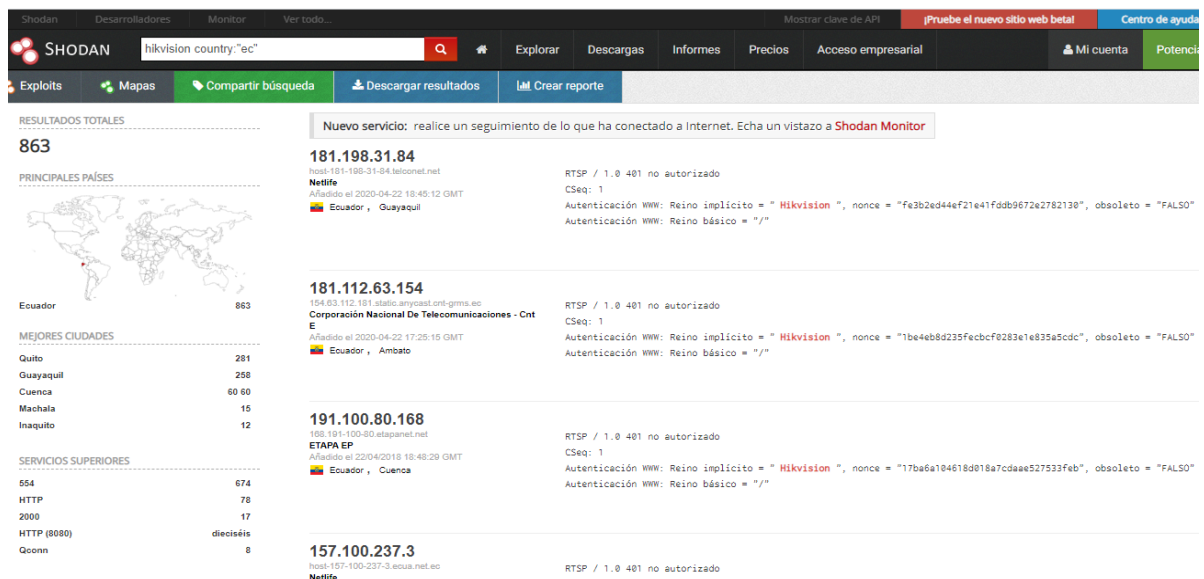


Figura 9. Cámaras Hikvisión
Fuente: (Shodan, 2013)

Se muestra los resultados de la búsqueda con esta marca en Ecuador en la parte izquierda muestra las ciudades que se encuentran.

10- Se dará clic en la dirección ip y mostrará a detalle la ubicación de la cámara, puertos que usa, además el servidor de internet al que está conectado.

The screenshot shows the Shodan web interface. On the left, there is a table with the following data:

Ciudad	Ambato
País	Ecuador
Organización	Corporación Nacional De Telecomunicaciones - Cnt E
ISP	Corporación Nacional De Telecomunicaciones - Cnt E
Última actualización	2020-04-22T17:25:15.103773
Nombres de host	154.63.112.181.static.anycast.cnt-grms.ec
ASN	AS28006

On the right, under the 'Servicios' section, there are three entries:

- 554**: tcp, rtsp-tcp. RTSP / 1.0 401 no autorizado. CSeq: 1. Autenticación WWW: Reino implícito = "Hikvision", nonce = "1be4eb8d235fecbcf0283e1e835a5cd", obsoleto = "FALSO". Autenticación WWW: Reino básico = "/"
- 1723**: tcp, pptp. Firmware: 1. Nombre de host: prueba. Vendedor: MikroTik
- 2000**: tcp, ikettle. Página HTTP / 1.1 400 no encontrada \ r \ n

A green arrow button is located at the bottom of the services section.

Figura 10. Interfaz de configuración cámara Hickvisión
Fuente: (Shodan, 2013)

11- Se selecciona la flecha verde en la parte inferior derecha y le enviará a la página de ingreso de esta cámara.

Estas cámaras no son tan vulnerables ya que esta no se puede acceder con las contraseñas por defecto como se lo realizó anteriormente.

Lo interesante de Shodan es que muestra a detalle los parámetros que pueden ser muy útiles para un hacker así como: la ubicación precisa con latitud y longitud, puertos que usa, puertos libres, servidor de internet que usa, entre otros.

186.4.209.69

Nombre de la propiedad	Valor
codigo de AREA	nulo
asn	AS27947
ciudad	Quito
código de país	CE
country_code3	nulo
nombre del país	Ecuador
data.0._shodan.crawler	ff4c1113c29f0957c5712a8b31ff786a10e9caf8
data.0._shodan.id	0273528a-115d-4e3e-b05b-38871982799f
data.0._shodan.module	http-simple-new
data.0._shodan.ntf	Cierto

Figura 11. Parámetros de configuración de la cámara Hickvision
Fuente: (Shodan, 2013)

3. Responsable

Ingeniera en sistemas

Formación:

- Universidad del Azuay - Certificación en Administración de Base de Datos y Herramientas Ofimáticas

Experiencia:

- Docente en educación tecnológica por 7 años - Asesora en proyectos de titulación - Coordinación académica del Instituto Huaquillas por 3 años - Coordinación de vinculación por 1 año.

Responsable:



Ing. Jessica Alejandro Becerra

Revisado y Aprobado por:



Ing. Jorge David Herrera Sarango

4. Referencias

- Giménez, V. (25 de 09 de 2011). *Hacking y ciberdelito*. Obtenido de <https://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf>
- Jara, H., & Pacheco, F. (2012). *Ethical Hacking*. Buenos Aires: RedUsers.
- Mendoza, J. (09 de Julio de 2018). *Mundo Hackers*. Obtenido de <https://www.redeszone.net/tutoriales/seguridad/shodan-busqueda-hacking/>
- Rizaldos, H. (17 de 09 de 2018). *Qué es Shodan y para qué usarlo*. Obtenido de <https://openwebinars.net/blog/que-es-shodan/>
- Romero, M., Conce, J., Mondé, J., Rivera, O., Roper, J., Sánchez, G., & Sivianes, F. (2014). *Redes locales*. Madrid: Parainfo.
- Shodan. (05 de 01 de 2013). *shodan*. Obtenido de <https://www.shodan.io/>