

INSTITUTO TECNOLÓGICO SUPERIOR "HUAQUILLAS"

Manual Shodan

Manual Técnico

Tecnología:

• Superior en Redes y Telecomunicaciones

Autora:

Alejandro Becerra, Jessica Pilar

Huaquillas – Ecuador

2019

Índice de contenido

Ind	ice de contenido	2		
Ind	ndice de figuras3			
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.	Responsable1	4		
4.	Referencias1	5		

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".

						strar clave de API	Pruebe el nuevo sitio web b	etal Cen	itro de ayuda
Shodan		Q 🏶 Explora	r Descargas	Informes	Precios	Acceso empresari	al	🛓 Mi cuenta	Potencia
El bi	uscador de Cán	naras web				67.20.69.105			
Shodan e	es el primer motor de búsqueda	i del mundo para di	spositivos c	onectado	s a Inter	net.			
					184.18.61.23	0	<i>7</i> 0 , 0		
Cn	ear una cuenta Primeros pasos gratuita					<i>7 - 0</i>	<u>6</u>		
					0	í ø			
				7 -			//		
	Explore el Internet de las co	osas	C	V	er la ima	agen complet	a		
	Use Shodan para descubrir cuáles de sus Internet, dónde están ubicados y quién los es	dispositivos están conectado stá utilizando.	s a	LC te	os sitios web levisores intel on Shodan!	o son solo una par ligentes, refrigerador	te de Internet. ¡Hay plant as y mucho más que se pu	as de energía, eden encontrar	
	Monitorear la seguridad de l	la red	50		btenga u	una ventaja c	ompetitiva		
	Mantenga un registro de todas las computad	doras de su red a las que se pu	ede	i C	uién está usa	ando tu producto? ¿D	ónde están ubicados? Utilio	ce Sh <mark>oda</mark> n para	1

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

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

\leftrightarrow \rightarrow C \triangle \triangleq shodan.io/explore		题 🕁 🎈	G 🔏 🖃 🌸 :
Descubra Internet	Explorar utilizando consultas de búsqueda compartic	las por otros usuarios.	- -
Categorías Destacadas	Más votados 11.850	Compartido recientemente	
Sistemas de control industrial	Cámara web mejor búsqueda de cámara IP que he encontrado todavia. cámara web vigilancia lexas 2010-03-15	1 VMware vSphere Web Client VMware vSphere Web Client vmware	2020-04-22
Bases de datos	Levas admin admin leva camara web 2012-02-05	1 VMware vCloud Director VMware vCloud Director	2020-04-22
Videojuegos	Netcam Netcam netcam 2012-01-13	3 contraseña predeterminada	
	1,931	1	- LOLO OFFIC

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

Ecuador	18 años	400 00 44 005 5		
MEJORES CIUDADES Guayaquil Quito Inaquito Cuenca Dtavalo	66 55 2 2 1	186.68,444,235 L 255.geni 804-46 yes astinct net Sataret Gye Coorp CM Anadio ei 1504/2020 11:229-46 GMT de Ecuador , Guayaquil	HTTP / 1.1 401 no autorizado Tipo de contenido: texto / html Conexión: cerrar Pregma: sin cache Autenticación WWM: <mark>Reino básico = " netcam</mark> " Longitud del contenido: 17	
SERVICIOS SUPERIORES				
HTTP (83) HTTP (8080) 5005 HTTP (82) HTTP	55 3 2 2 2	191.99.157,139	HTTP / 1.1 401 no autorizado Tipo de contenido: texto / html Conexión: mantener vivo Autenticación WW: Reino básico = " netcam " Longitud del contenido: 17	
ORGANIZACIONES SUPERIORES				
Vetifie Satnet ErAP EP Corporación Nacional De Telec Claro Ecuador	77 44 2 2 2	186.101.235.242 ☑ has-108-101-235.242.nellfie.eo Nellfie Afaddio el 2025-04-14 02-45:12 GMT ■ Ecuador , Guayaqui	HTTP / 1.1 401 no autorizado Tipo de contenido: texto / html Conexión: cerrar Pragma: sin caché Autenticación WMM: Reino básico = " Netcam " Longitud del contenido: 17	
1 235 242-8080		190.130.237.193 C Claro Ecuador Afadido el 1504.2020 09:27:29 GMT Ecuador, Culto	HTTP / 1.1 401 no autorizado Tipo de contenido: texto / html Conexión: mantener vivo Autenticación VMW: Reino básico = " netcam "	

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

Iniciar sesión http://190.152.166.121.83 Tu conexión con este sitio web no es privada
Contraseña 2Quieres guardar Nombre de usuario Contraseña



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



Q 186.101.235.242 host-186-101-235-242.netlife.ec Ver datos sin procesar



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

Guayaquil

Ciudad



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.

← → C ☆ 🗱 IE	Tab chrome-extension://	hehijbfgiekmjfkfjpbkbar	mmjbdenadd/nhc.htm#url=http://186.101.235.242
Address: http://186.101.23	5.242:8080/admin/setup.cgi?pa	ge=network	
)net		Wireless Internet Camera Server TV-IP110W Location: entrada 2007/01/28 07:47:34
· Ö Live View	Network » Network	ĸ	
OP Setup	Network		
	IP Settings:		
Smart Wizard		 Static IP 	
		IP:	192 . 168 . 0 . 222
Basic		Subnet Mask:	255 . 255 . 255 . 0
Network		Default Gateway:	192 . 168 . 0 . 1
Network		Primary DNS:	192 . 168 . 0 . 1
• IP Filter • Wireless		Secondary DNS:	186 . 5 . 11 . 18
Video		O PPPoE	
		User Name:	
Event Server		Password:	
Motion Detect	DDNS Setting:		
Event Config		Enable Provider:	members dyndas org
Tools		Host Name:	
		User Name:	
Information		Password:	

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:

Shodan	Desarrolladores	Monitor Ver	todo			Mos	strar clave de API	Pruebe el nuevo sitio web beta!	Centro	de ayuda
🔏 Ѕнос	DAN hikvisi	ion country:"ec"	۹ 🐐	Explorar Descarga	s Informes	Precios	Acceso empresari	al 🚨 🗛	di cuenta	Potencia
Exploits	🔧 Mapas	💊 Compartir búsque	eda 📥 Descargar resultados	Lul Crear reporte						
RESULTADOS	TOTALES		Nuevo servicio: realice un segui	imiento de lo que ha con	ectado a Internet	. Echa un vist	azo a <mark>Shodan Monit</mark>	or		
863			181.198.31.84							
PRINCIPALES	PAÍSES		host-181-108-31-84 telconet.net Metifio Afadido el 2020-04-22 18:46:12 GMT Cusador, Guayaquil	RTSP / 1.0 40 CSeq: 1 Autenticación Autenticación	1 no autorizado WWW: Reino impli WWW: Reino bésic	cito = " Hikv o = "/"	ision ", nonce = "fe	3b2ed44ef21e41fddb9672e2782130	", obsoleto =	"FALSO"
Ecuador	₽ ÷	863	181.112.63.154 154.03.112.101.static.anycast.ont-grms.ec Corporación Nacional De Telecomunicacion E	RTSP / 1.0 40 CSeq: 1	1 no autorizado					
MEJORES CIU	DADES	204	Añadido el 2020-04-22 17:25:15 GMT	Autenticación Autenticación	WWW: Reino impli WWW: Reino básic	cito = " Hikv o = "/"	ision ", nonce = "lb	4eb8d235fecbcf0283e1e835a5cdc	", obsoleto =	"FALSO"
Guayaquil		258								
Cuenca		60 60								
Machala		15								
Inaquito		12	191.100.80.168 168.191-100-80.etapanet.net ETAPA EP	RTSP / 1.0 48	1 no autorizado					
SERVICIOS SU	PERIORES		Añadido el 22/04/2018 18:48:29 GMT	Autenticación	WWW: Reino impli	cito = " Hikv	ision ", nonce = "17	a6a104618d018a7cdaae527533feb	", obsoleto =	"FALSO"
554		674		Autenticación	WWW: Reino básic	o = "/"				
HTTP		78								
2000		17								
HTTP (8080)		dieciséis								
Qconn		8	157.100.237.3 host-157-100-237-3.ecua.net.ec Netlife	RTSP / 1.0 40	1 no autorizado					

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.

→ C 🏠 🔒 si	hodan.io/host/181.112.63.154	🔤 🖈 🎈 🤤 😤 🖡					
cesar PN		554 1723 2000					
liudad	Ambato						
aís	Ecuador						
rganización	Corporación Nacional De Telecomunicaciones - Cnt E	554					
5P	Corporación Nacional De Telecomunicaciones - Cnt E						
ltima actualización	2020-04-22T17: 25: 15.103773	RTSP / 1.0 401 no autorizado					
Nombres de host 154.63.112.181.static.anycast.cnt-grms.ec		Autenticación WWH: Reino implícito = "Hikvision", nonce = "1be4eb8d235fecbcf0283e1e835 c" chicalato = "FALSO"					
SN	AS28006	Autenticación WWW: Reino básico = "/"					
		1723 Firmware: 1					
		tcp Nombre de host: prueba pptp Vendedor: MikroTik					
		2000 Pégina HTTP / 1.1 400 no encontrada \ r \ n tcp ikettle					
		e					

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	A\$27947
ciudad	Quito
código de país	CE
country_code3	nulo
nombre del país	Ecuador
data.0shodan.crawler	ff4c1113c29fd057c5712a8b31ff786a10e9cafb
data.0shodan.id	0273528a-115d-4e3e-b05b-38871982799F
data.0shodan.module	http-simple-new
data.0. shodan.ntr	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:

audraß

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., Ropero, J., Sánchez, G., & Sivianes, F. (2014). *Redes locales.* Madrid: Parainfo.
- Shodan. (05 de 01 de 2013). shodan. Obtenido de https://www.shodan.io/