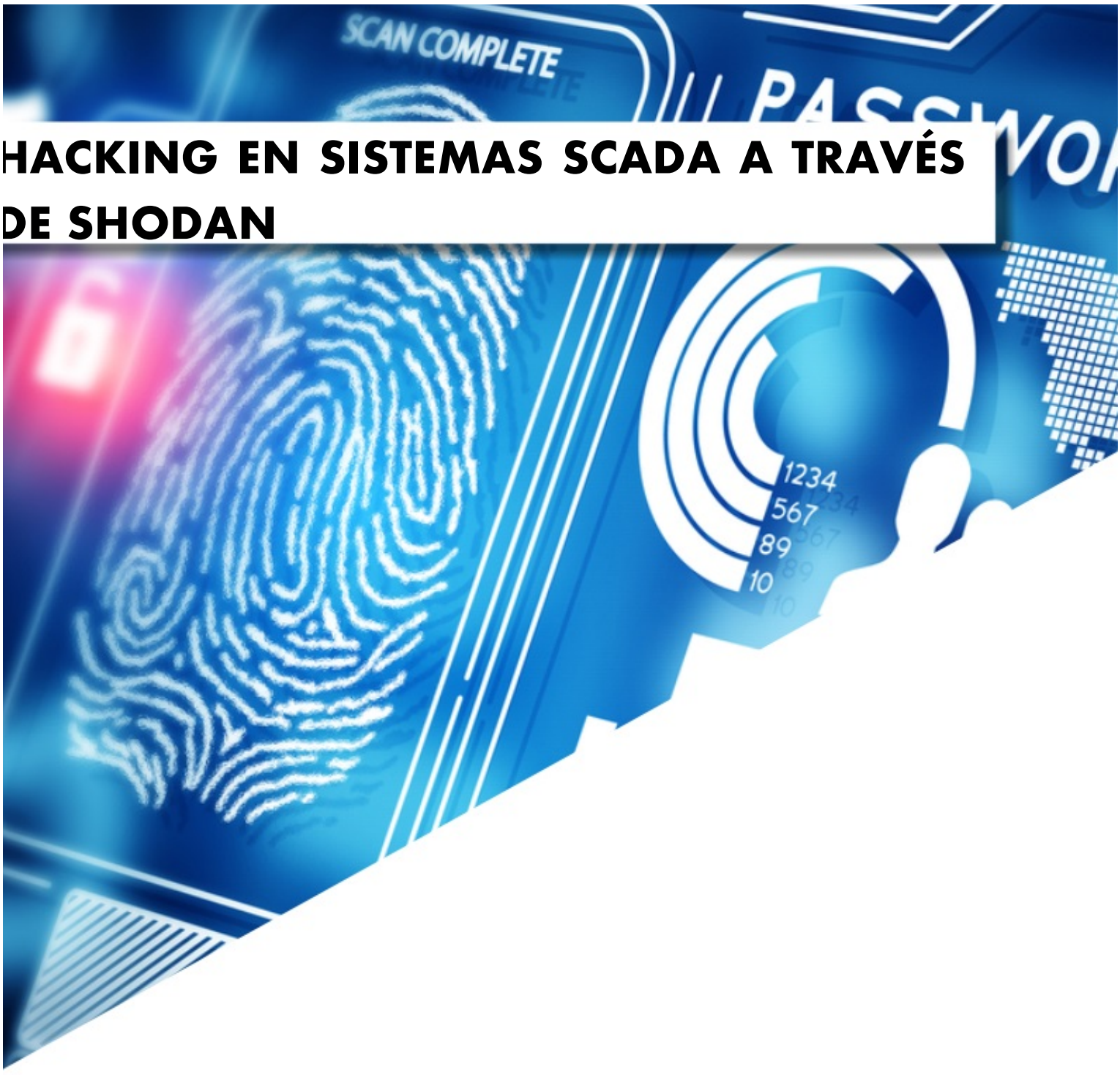



# HACKING EN SISTEMAS SCADA A TRAVÉS DE SHODAN

Trabajo Fin de Máster

Autor: Jesús Madrid del Val

Tutor: Manuel Sánchez Rubio

Máster en Ciberdefensa

MCD

Universidad de Alcalá

Fundación IN-NOVA Centro de Innovación

Trabajo Fin de Máster
HACKING EN SISTEMAS SCADA A TRAVÉS DE SHODAN

Autor: Jesús Madrid del Val
Tutor: Manuel Sánchez Rubio

Fecha de Presentación: Abril 2018
Máster en Ciberdefensa, 2ª edición
Universidad de Alcalá

Contenido

1. RESUMEN EJECUTIVO ..... 6
2. INTRODUCCIÓN ..... 7
3. OBJETIVOS ..... 8
4. METODOLOGÍA PARA EL DESARROLLO DEL TFM ..... 9
5. FUNDAMENTACIÓN TEÓRICA. ESTADO DEL ARTE ..... 11
5.1. ANALISIS DE LAS PARTICULARIDADES DE LAS REDES O.T. Y SISTEMAS SCADAS ..... 11
5.1.1. Que son las Redes OT y los Sistemas SCADA ..... 11
5.1.2. Particularidades de los sistemas SCADA, ICS y Redes OT. ..... 13
5.2. LISTADO DE SISTEMAS SCADA Y SUS PUERTOS ..... 15
5.2.1. Protocolos de Comunicaciones SCADA ..... 15
5.2.2. Protocolo MODBUS. Un referente en entornos SCADA ..... 15
5.3. SHODAN. PRINCIPIOS Y FUNCIONALIDADES ..... 16
5.3.1. APIs DE SHODAN ..... 19
5.3.2. Librerias de entornos de programación ..... 21
5.3.3. Plug-ins de SHODAN ..... 21
5.4. OTRAS HERRAMIENTAS DE POSIBLE APLICACIÓN ..... 22
6. FASES DE HACKING DE SIST. SCADA ..... 24
6.1. DESCRIPCION DEL PROCESO GLOBAL DE HACKING ..... 24
6.1.1. Fase de actuación Pasiva ..... 24
6.1.2. Fase de Actuación Activa ..... 24
6.2. HACKING CON SHODAN ..... 25
7. PROCEDIMIENTOS DE HACKING DE SIST. SCADA CON SHODAN ..... 27
7.1. USO DE FILTROS Y CLAVES DE BUSQUEDA EN SHODAN ..... 27
7.2. BUSQUEDAS COMPLEMENTARIAS CON GOOGLE DORKS Y GHDB ..... 29
7.2.1. Búsqueda con Google DORKS ..... 29
7.2.2. Búsqueda en repositorio GHDB ..... 32
7.3. ACCESO A SISTEMAS SCADAS ..... 34
7.3.1. ACCESO A SIST. SCADA CON PROTOCOLO *MODBUS* ..... 35
7.3.2. ACCESO A SIST. SCADA MODUWEB ..... 38
7.3.3. GEOLOCALIZACIÓN DE SISTEMAS SCADA ..... 41
7.4. ACCESO A DISPOSITIVOS CON CONTRASEÑAS POR DEFECTO ..... 43
7.5. ACCESO A ROUTERS ..... 44

7.5.1. ACCESO A ROUTERS CISCO ..... 44
7.6. BUSQUEDA DE SERVIDORES DE FTP ..... 46
7.7. BUSQUEDA DE BASES DE DATOS MONGODB ..... 47
7.8. ACCESO A SERVICIOS DE CÁMARAS IP ..... 50
Acceso a cámaras Web de seguridad genéricas ..... 50
Acceso a cámaras AvTech ..... 52
Acceso a WebCams Android sin autentificación ..... 56
Acceso a Cámaras D-link sin autenticación ..... 58
7.9. ACCESO A SERVICIOS DE DOMÓTICA ..... 60
7.10. BUSQUEDAS AUTOMÁTICAS CON SELENIUM-JAVA ..... 61
7.10.1. Análisis automático de conexiones TELNET ..... 61
8. TOOLBOX PARA HACKING DE SCADA CON SHODAN ..... 67
8.1. HERRAMIENTAS SW ..... 67
8.1.1. SHODAN ..... 67
8.1.2. APIs y Plug-ins ..... 68
8.1.3. Buscadores de Información en la Web (Surface web) ..... 69
8.1.4. Inspección de paginas Web (ACUNETIX) ..... 73
8.1.5. Buscadores de Información en la Deepweb ..... 74
8.1.6. Herramientas OSINT ..... 75
8.1.7. Automatizacion de busquedas ..... 76
8.1.8. Aplicaciones de bases de datos ..... 77
8.1.9. Descifradores de contraseñas ..... 77
8.1.10. Geolocalización ..... 77
8.2. INFORMACIÓN TÉCNICA ..... 77
8.2.1. Listado de puertos y sistemas objetivo ..... 77
8.3. NORMATIVA APLICABLE Y GUÍAS ..... 79
8.3.1. ISA99 ..... 79
8.3.2. IEC 62443 ..... 79
8.3.3. NIST SP 800-82 ..... 80
8.3.4. NIST SP 800-53 ..... 81
8.3.5. RG 5.71 ..... 81
8.3.6. NERC CIP ..... 81
8.3.7. IEC 62351 ..... 82

8.3.8. IEEE 1711-2010 ..... 82
8.3.9. IEEE 1686-2007 ..... 82
9. RESULTADOS ..... 83
9.1. LISTADO DE PUERTOS Y SISTEMAS ..... 83
9.2. NORMATIVA APLICABLE ..... 84
9.3. TOOLBOX HACKING de SIST. SCADA ..... 85
10. CONCLUSIONES Y TRABAJO FUTURO ..... 87
10.1. CONCLUSIONES ..... 87
10.2. TRABAJO FUTURO ..... 87
Referencias Bibliográficas ..... 88
Trabajos citados ..... 88
Anexo ..... 89

# 1. RESUMEN EJECUTIVO

Multitud de infraestructuras críticas (de ámbito público o industrial), tienen conectados a la red sus sistemas SCADA. Se ha demostrado que éstos, así como las Infraestructuras críticas (IC), son altamente vulnerables a los ciberataques.

En la actualidad existen algunas herramientas como SHODAN especialmente diseñadas para buscar en la red de Internet e identificar equipos que presentan vulnerabilidades de seguridad por errores de configuración, como pueden ser los servidores o nodos que forman los sistemas SCADA.

El presente trabajo tiene por objeto analizar y documentar cómo se pueden llevar a cabo las tareas de Hacking a Sistemas SCADA mediante el empleo de SHODAN (combinaciones de filtros y palabras clave) así como identificar que otras posibles herramientas o aplicaciones auxiliares (APIs o Herramientas libres) pueden combinarse con la anterior aumentando la efectividad del proceso.

El presente trabajo tiene por tanto un enfoque holístico que no se queda en el análisis técnico de las aplicaciones sino que pretende cubrir a su vez los aspectos normativos y de procedimiento que afectan a la forma de trabajar con dichas aplicaciones a lo largo del proceso de Hacking de Sistemas SCADA.

El empleo combinado de otras herramientas con Shodan permitiría poder hacer una explotación avanzada de los datos que se obtiene de las búsquedas, permitiendo incluso la automatización del proceso de búsqueda y reporting.

La disponibilidad de una suite de herramientas compatibles con Shodan, entre sí e incluso integrables entre ellas permitiría no solo identificar fácilmente aquellos equipos SCADA vulnerables sino poder acceder posteriormente a los mismos explotando dichas vulnerabilidades.

Por consiguiente el presente trabajo trata de describir y estructurar los siguientes aspectos del Hacking de Sistemas SCADA con SHODAN:

- Análisis de las particularidades de las redes OT y Sistemas SCADA.
- Listado de Sistemas SCADA y sus puertos
- Fases del proceso de Hacking con SHODAN
- Diferentes procedimientos de Hacking de SCADAS con SHODAN
- Identificación de Herramientas adicionales que constituyan una suite (ToolBox) concebida para Labores de Pentesting sobre sistemas SCADA de ICS.

Finalmente se propone, como posible proyecto futuro, la implementación de todas las aplicaciones identificadas y probadas aquí en una suite de herramientas (tipo Kali Linux) concebida para labores de Pentesting de Sistemas SCADA.

# 2. INTRODUCCIÓN

Multitud de infraestructuras críticas (de ámbito público o industrial), tienen conectados a la red sus sistemas SCADA. Se ha demostrado que éstos así como las Infraestructuras críticas (IC), son altamente vulnerables a los ciberataques y constituyen uno de los principales objetivos de las operaciones en el ciberespacio de cualquier país, (desde la energía como gas, hidrocarburos, electricidad, energía nuclear hasta las finanzas) ya que dependen de los sistemas de información y control que poseen vulnerabilidades explotables, parte de ellas comunes a las Tecnologías de Información y Comunicaciones (TIC), por agentes maliciosos.

A través del buscador SHODAN, se pretende que el alumno, desarrolle técnicas de búsqueda de dispositivos SCADA, que tengan algún tipo de vulnerabilidad.

La herramienta web SHODAN permite buscar dispositivos conectados a Internet que tienen configuraciones erróneas de seguridad. Se puede utilizar para buscar servidores vulnerables. Recoge información de dispositivos conectados a Internet de forma continua como por ejemplo: cámaras de seguridad, sistemas VoIP, sistemas de calefacción, plantas de energía y sistemas de automatización industriales.

SHODAN dispone de una amplia gama de filtros para caracterizar las búsquedas así como una extensa librería de APIs para poder hacer una explotación avanzada de los datos que obtiene de las búsquedas, la automatización del proceso y reporting. El trabajo pretenderá ahondar en el uso avanzado de filtros y la configuración de algunas APIs para poder llevar a cabo la explotación intensiva y customizada de la información que captura SHODAN con el objeto último de identificar las vulnerabilidades de los sistemas SCADA (direcciones IP, puertos, etc.) bajo estudio.

El propósito del trabajo sería desarrollar una serie de configuraciones con las APIs de SHODAN y valiéndonos de una serie de herramientas Opensource que nos permitieran generar una suite de herramientas específicamente concebida para llevar a cabo Auditorias de Pentesting sobre Sistemas SCADA de Infraestructuras críticas (ICS), bien sean de entorno industrial o de ámbito público.

# 3. OBJETIVOS

Los principales objetivos perseguidos mediante la elaboración del presente Trabajo Fin de Master son:

- Aprender a buscar dispositivos SCADA a través de SHODAN de forma sistematizada, para lo cual se identificarán:
  - Fases del proceso de hacking con SHODAN
  - Diferentes procedimientoas de Hacking con SHODAN
- Comprobar la vulnerabilidad de sistemas SCADA
- Definir una suite de herramientas (ToolBox) concebida para Labores de Pentesting sobre sistemas SCADA de ICS.

El presente trabajo desarrolla áreas de conocimiento que tienen una estrecha relación con otras asignaturas del MCD impartido por la UAH, como son:

- CIC – Ciberamenazas a las infraestructuras críticas
- CIB – Ciberinteligencia y fuentes abiertas

# 4. METODOLOGÍA PARA EL DESARROLLO DEL TFM

La Metodología seguida para el desarrollo del presente proyecto se fundamenta en las actividades y fases descritas a continuación:

1. Análisis del Estado del Arte

Constituye la primera actividad del trabajo y tiene como objetivo analizar el estado de la tecnología actual para lo cual se profundiza sobre las siguientes áreas:

- Análisis de las particularidades de las redes OT y sistemas SCADA.
- Identificación de los diferentes sistemas SCADA y sus puertos mas habituales.
- Análisis de las capacidades de la aplicación Shodan y de sus procedimientos de uso.
- Análisis de otras Herramientas complementarias a Shodan para e Hacking de SCADAS

En el trabajo se incluyen todas aquellas referencias bibliográficas que han sido consultadas para su elaboración, indicando autor, fecha y link de la fuente consultada.

2. Descripción de las fases del proceso de Hacking de Sistemas SCADA

En dicho apartado se analiza la secuencia de actividades genéricas y fases en el proceso de hacking de un sistema SCADA.
Ello permitirá definir una sistematización de tareas a lo largo del proceso de hacking con Shodan que sirva de guía para el experto de ciberseguridad.

3. Descripción de los diferentes procedimientos de hacking de Sist. SCADA con Shodan

Inicialmente se describe como se puede utilizar Shodan como herramienta para la identificación de equipos vulnerables mediante la configuración de los filtros y claves de búsqueda adecuados.

Posteriormente se describen otros procedimientos mas complejos donde se pueden combinar dichos resultados obtenidos con Shodan con otras aplicaciones para llegar a acceder a los equipos vulnerables (webcams, routers inhalambricos, servidores ftp, accesos via telnet, etc.) y reconfigurar éstos o bien extraer de ellos información.

Para cada procedimiento se hacen una serie de pruebas, cuyos resultados son documentados y resumidos en una tabla de resultados.

4. Identificación de aplicaciones complementarias para composición de una suite de herramientas (Toolbox) para Pentesting de Sist. SCADA

Como parte del trabajo se identifican y caracterizan un conjunto herramientas y elementos que, empleados de forma combinada con Shodan, permiten hacer una explotación avanzada y optimizada de los resultados ofrecidos por Shodan, permitiendo la automatización de búsquedas y del reporting.
Esta suite de herramientas (Toolbox) recogería todos aquellos elementos necesarios para optimizar el proceso de Auditoria de Pentesting de sistemas SCADA, estando compuesta por:

- Aplicaciones: APIs, Bases de Datos, etc.
- Información técnica: Links, Filtros shodan, Puertos SCADA, etc.
- Normativa aplicable y guías: ANSI/ISA99, CCN-STIC-480, IEC, IEEE, NERC, NIST SP-800, etc.

## 5. Resultados del trabajo

A lo largo del trabajo, y como consecuencia de las pruebas realizadas con las diversas herramientas para los distintos procedimientos de hacking se obtienen unos resultados que han sido llevados a unas tablas resumen. Dichas tablas se desglosan por tipología de sistema atacado.

## 6. Conclusiones y Trabajo Futuro

Finalmente en el presente documento se extractan las conclusiones del trabajo que son llevadas al apartado correspondiente al final del mismo.

Como parte de las conclusiones finales se propone una posible actividad de continuación del presente trabajo.

# 5. FUNDAMENTACIÓN TEÓRICA. ESTADO DEL ARTE

## 5.1. ANALISIS DE LAS PARTICULARIDADES DE LAS REDES O.T. Y SISTEMAS SCADAS

### 5.1.1. Que son las Redes OT y los Sistemas SCADA

Las Redes O.T. y los Sistemas SCADA son los encargados de la Gestion y Control de las instalaciones Industriales (ICS) y por consiguientes están presentes en cualquier tipo de Infraestructura Crítica (IC), como pueden ser: Aeropuertos, Instalaciones de generación y transformación de energía, Centros de comunicaciones, Instalaciones de investigación, Sistemas Bancarios, etc.

Las infraestructuras críticas (IC) se definen como '*Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas*' y constituyen hoy en dia uno de los principales objetivos de las operaciones en el ciberespacio.

Los ICS se componen de los siguientes elementos, si bien todos ellos comúnmente son conocidos bajo el término de SCADA:

- **Sistemas de Control de Supervisión y Adquisición de Datos (SCADA).**
- **Sistemas de Control Distribuido (DCS).**
- **Interfaces Hombre-Máquina (IHM).**
- **Unidades Terminal Maestras (MTU**
- **Controladores lógicos programables (PLCs).**
- **Unidades Terminales Remotas (RTU).**
- **Dispositivos Electrónicos Inteligentes (IEDs).**
- **Componentes de comunicaciones de la Red ICS**.
    - Fieldbus..
    - Red de Control.
    - Routers.
    - Firewall.
    - Modems.
    - Puntos de acceso remoto.

Los Sistemas SCADA están diseñados para recopilar información de entornos industriales, plantas distribuidas y activos dispersos, y transferirla a un sistema central de proceso a través de un sistema de comunicaciones, procesarla y mostrarla al operador de forma gráfica o textual en un interfaz hombre máquina que permite supervisar o controlar las numerosas entradas y salidas de los procesos a controlar de un sistema desde una ubicación central en tiempo real, mediante operaciones automáticas o manuales realizada mediante comandos.

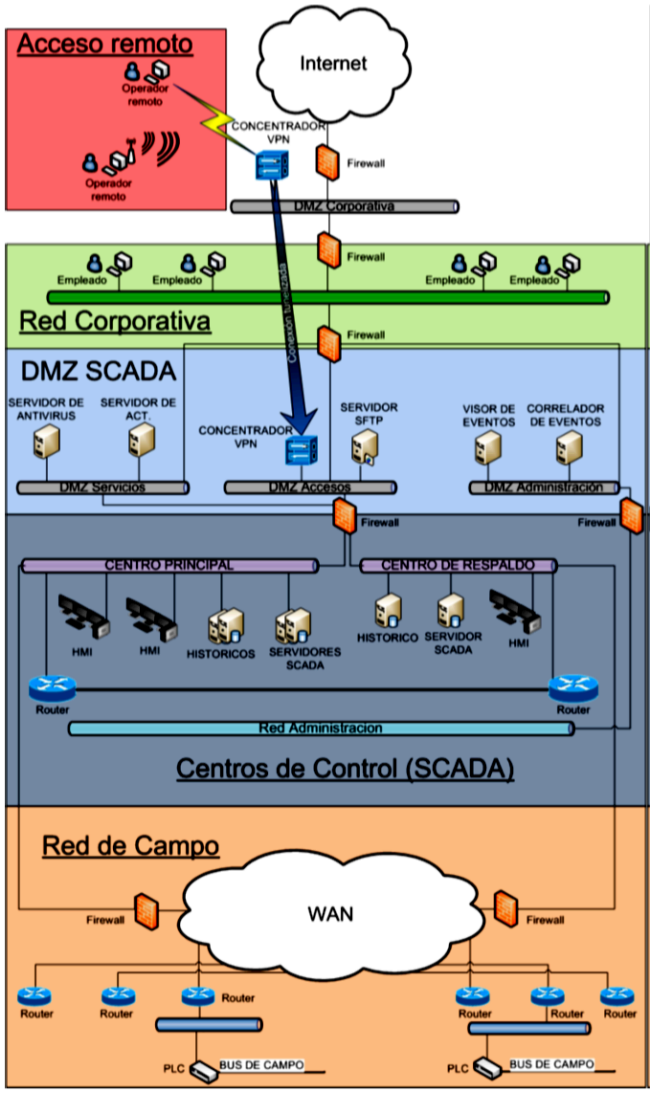
Ofrecen las siguientes prestaciones:

- Gestión centralizada de alarmas.
- Funcionamiento distribuido en red, lo que permite una mayor disponibilidad,
- redundancia, fiabilidad, tolerancia a fallos, etc.
- Posibilidad de adaptación a las necesidades concretas de los usuarios debido al elevado grado de configuración que poseen.
- Interfaces gráficos que permiten la supervisión de los sistemas de una forma rápida y visual.
- Capacidad de analizar tendencias de determinadas variables (históricos), así como la incorporación de funciones SPC (Control Estadístico de Procesos).
- Capacidad de programar acciones sobre las instalaciones de carácter periódico o a partir de los valores instantáneos de variables.
- Diagnóstico de fallos en instalaciones mediante sistemas expertos.
- Supervisión inteligente de procesos, tratamiento de datos (hojas de cálculo y bases
- de datos).
- Gestión y archivo de datos
- Creación de informes y elaboración de documentación.

Un sistema SCADA de tipo genérico está estructurado en base a los siguientes subsistemas:

- **Centros de control.**
    - Consola. Proporciona el interfaz hombre máquina que permite su operación.
    - Servidor.
    - MTU.
    - Servidor de históricos.
    - IHM.
- **Comunicaciones de campo.**
- **Posiciones de campo**
    - Adquisición de Datos.
    - DCS, RTUs, PLCs e IEDs.
    - Actuadores electromecánicos.

A continuación se muestra un esquema lógico de un sistema SCADA.




### 5.1.2. Particularidades de los sistemas SCADA, ICS y Redes OT.

En líneas generales se puede concluir que hoy en día los Sistemas de Control Industrial no constituyen una infraestructura con altos niveles de seguridad como veremos a continuación. Ello hace que resulte particularmente efectivo el hacking con herramientas de tipo Shodan.

Unos de los beneficios que conllevan los sistemas SCADA es el hecho de utilizar ordenadores, servidores y software de base (sistemas operativos, gestores de bases de datos, etc.) de uso general en las TIC. Por otro lado se tiene el inconveniente de heredar todas las vulnerabilidades asociadas con este tipo de tecnologías.

Las causas que han contribuido a la actual deficitaria seguridad de las IC son múltiples y variadas, aunque se pueden destacar las siguientes:

- *Exceso de confianza en la seguridad por oscuridad*. Deriva del hecho de que algunos profesionales del sector de las TIC consideran que la ausencia de información pública sobre una tecnología o producto ofrece altos niveles de seguridad al mismo.
- *Minimización de riesgos y amenazas*. Muchos responsables de sistemas SCADA consideran que sus instalaciones carecen de interés para potenciales atacantes, lo que reduce a su juicio la necesidad de seguridad de las mismas.
- *Ampliación de visibilidad*. Los sistemas SCADA no fueron pensados para ser interconectados con redes externas no confiables, como por ejemplo, Internet o las redes corporativas, lo que ha provocado la aparición de nuevos riesgos o amenazas para los que estos sistemas no estaban diseñados.
- *Ausencia de concienciación del personal*. La concienciación del personal en todos los niveles jerárquicos, tanto del personal operativo como de la alta dirección, es esencial.
- *Interconexión de los sistemas SCADA con redes externas*. Actualmente, los sistemas SCADA se han integrado y conectado a redes no confiables como Internet, o en el mejor de los casos una red controlada de tipo corporativo, factor que incrementa el riesgo de ataques.
- *Uso de tecnologías y soluciones de propósito general*. La adopción las TIC conlleva un riesgo intrínseco a las mismas, la incorporación de todas las vulnerabilidades que se descubren y, en algunos de los casos, publican antes de su corrección.
- *Generalización y expansión del uso de sistemas de monitorización y control*. Este tipo de sistemas nacieron para ser empleados en grandes procesos e instalaciones, como puede ser áreas de generación y transmisión de energía, procesos industriales, etc. Sin embargo, con el auge de las TIC, este tipo de sistemas comenzaron a implantarse para la monitorización y control de procesos menos críticos y más reducidos
- *Escasa evolución*. Debido a que su objetivo principal es la disponibilidad, los sistemas SCADA suelen sufrir muy pocas modificaciones a lo largo del tiempo, ya que se suelen considerar peligrosas al poder introducir algún fallo o problema que afecte negativamente en su rendimiento.
- *Configuraciones por defecto*. Muchos sistemas poseen en producción configuraciones por defecto en los equipos y dispositivos, lo que genera una situación de riesgo que puede provocar problemas de seguridad.
- *Arquitecturas de red poco seguras*. Muchos sistemas SCADA no mantienen una arquitectura de red segura, es decir, una disposición de los diferentes componentes y sus comunicaciones de forma que se dificulten las intrusiones o la intercepción/suplantación de comunicaciones.
- *Creciente interconexión entre las redes OT de las ICS*. Ello permite que el ataque en una de ellas tenga una rápida y gran afectación en otras. Esto es especialmente sensible en el caso de las infraestructuras críticas lo que puede derivar en la ocurrencia de fallos en cascada.

## 5.2. LISTADO DE SISTEMAS SCADA Y SUS PUERTOS

### 5.2.1. Protocolos de Comunicaciones SCADA

Existen múltiples protocolos de comunicación utilizados en SCADA o en los Sistemas de Control Industrial (ICS). A diferencia de los protocolos de Ethernet o Internet (IP), la industria usa múltiples protocolos, a menudo exclusivos del fabricante de los controladores lógicos programables (PLC). Aunque hay muchos protocolos, algunos de los protocolos de comunicación más populares dentro de estos sistemas son:

- **modbus** **port 502**
- **dnp** **port 19999**
- **dnp3** **port 20000**
- **fieldbus** **port 1089-91**
- **ethernet/IP** **port 2222**
- **etherCAT** **port 34980**
- **profinet** **port 34962-64**
- **Otros:** **ports: 19999, 20000, 1089-1091, 2222, 34980 y 34962-34964**

Conocer los puertos en los que opera cada sistema nos puede ayudar a identificar las vulnerabilidades de los sistemas SCADA

### 5.2.2. Protocolo MODBUS. Un referente en entornos SCADA

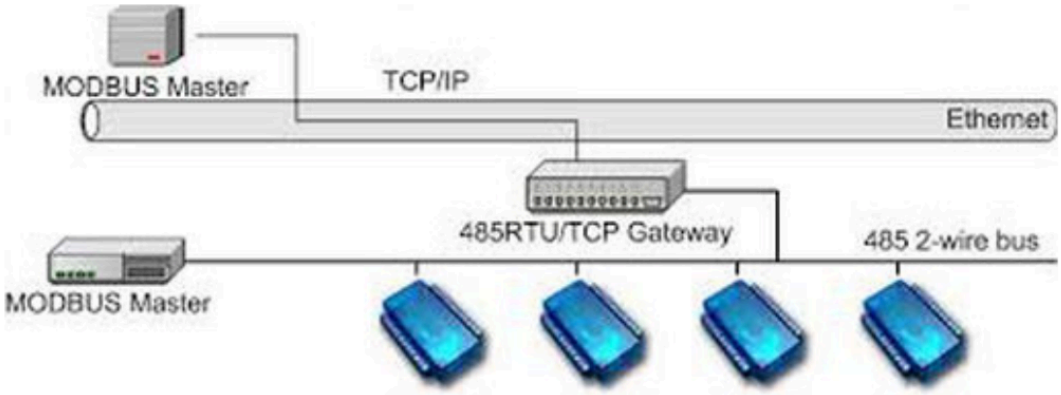
*Modbus* es uno de los protocolos más comunes en los sistemas ICS y SCADA. El Protocolo Modbus usa el puerto 502.

*Modbus* es un protocolo de comunicaciones en serie publicado originalmente por Modicon (ahora Schneider Electric) en 1979 para su uso con sus controladores lógicos programables (PLC). *Modbus* se ha convertido en un protocolo de comunicación estándar de facto en los sistemas SCADA / ICS por los siguientes motivos principalmente:

- desarrollado con aplicaciones industriales en mente
- abiertamente publicada y libre de regalías
- fácil de implementar y mantener.
- mueve bits o palabras sin poner muchas restricciones en los vendedores

*Modbus* permite la comunicación entre muchos dispositivos conectados a la misma red, por ejemplo, un sistema que mide la temperatura y la humedad y comunica los resultados a una computadora. *Modbus* se usa a menudo para conectar una computadora de supervisión con

una unidad terminal remota (RTU) en sistemas de control de supervisión y adquisición de datos (SCADA).




## 5.3. SHODAN. PRINCIPIOS Y FUNCIONALIDADES

Shodan nos permite rastrear por la web cualquier equipo (Desktops, Servers, Routers, Switches, IPcams, IoTs, etc.) que dispongan de un banner y se encuentre conectado a la web. Shodan rastrea y obtiene asi los banners y la información de los parámetros que éstos revelan (metadatos).

El tipo de metadatos que es capaz de obtener de los banners son los siguientes:

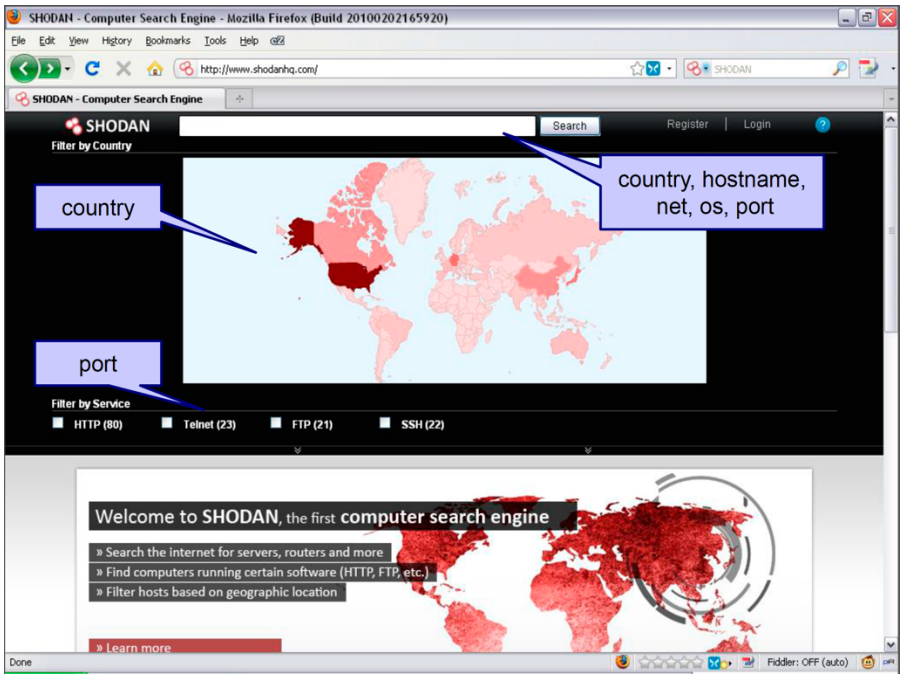
| | |
|---|---|
| **asn** | [String] El número de sistema autónomo (ex. "AS4837"). |
| **datos** | [String] Contiene la información de bandera para el servicio. |
| **ip** | [Entero] La dirección IP de la máquina como un entero. |
| **ip_st es** | [String] La dirección IP de la máquina como una cadena. |
| **ipv6** | [String] La dirección IPv6 del host como una cadena. Si está presente, entonces el "IP" y los campos "ip_str" no será. |
| **Puerto** | [Entero] El número de puerto que el servicio está funcionando con. |
| **fecha y hora** | [String] La marca de tiempo para cuando la bandera era descabellada desde el dispositivo en la zona UTC. Ejemplo: "2014-01-15T05: 49: 56.283713" |
| **nombres de host** | [String []] Una matriz de cadenas que contienen todos los nombres de host que se han asignado a la dirección IP para este dispositivo. |
| **dominios** | [String []] Una matriz de cadenas que contienen los dominios de nivel superior para los nombres de host del dispositivo. Esta es una propiedad de utilidad en caso de que quiera filtrar por TLD en lugar de subdominio. Es lo suficientemente inteligente como para manejar dominios de primer nivel mundial, con varios puntos en el dominio (ej. "Co.uk") |
| **ubicación** | [Objeto] Un objeto que contiene toda la información de ubicación para el dispositivo. |
| **location.area_code** | [Entero] El código de área de ubicación del dispositivo. Sólo está disponible para los EE.UU.. |
| **location.city** | [Cadena] El nombre de la ciudad donde se encuentra el dispositivo. |
| **location.country_code** | [Cadena] El código de país de 2 letras para la ubicación del dispositivo. |
| **location.country_code3** | [Cadena] El código de país de 3 letras para la ubicación del dispositivo. |
| **location.country_name** | [Cadena] El nombre del país donde se encuentra el dispositivo. |
| **location.dma_code** | [Entero] El código de área de mercado designado para la zona donde se encuentra el dispositivo. Sólo está disponible para los EE.UU.. |
| **location.latitude** | [Doble] La latitud de la localización geográfica del dispositivo. |
| **location.longitude** | [Doble] La longitud de la geolocalización del dispositivo. |
| **location.postal_code** | [Cadena] El código postal de la ubicación del dispositivo. |
| **location.region_code** | [String] El nombre de la región donde se encuentra el dispositivo. |
| **opta** | [Objeto] Contiene datos experimentales y complementarias para el servicio. Esto puede incluir el certificado SSL, robots.txt y otra información en bruto que aún no se ha formalizado en la Especificación de la bandera. |
| **org** | [Cadena] El nombre de la organización que se asigna el espacio IP para este dispositivo. |
| **isp** | [String] El ISP que está proporcionando la organización con el espacio de IP para este dispositivo. Considere esto, el "padre" de la organización en términos de propiedad intelectual. |
| **la** | [Cadena] El sistema operativo que alimenta el dispositivo. |
| **transporte** | [String] Cualquiera de "UDP" o "tcp" para indicar qué protocolo de transporte IP se utiliza para buscar la información |

La aplicación Shodan permite el empleo de una serie de Filtros de selección que pueden ser utilizados en el campo de búsqueda.

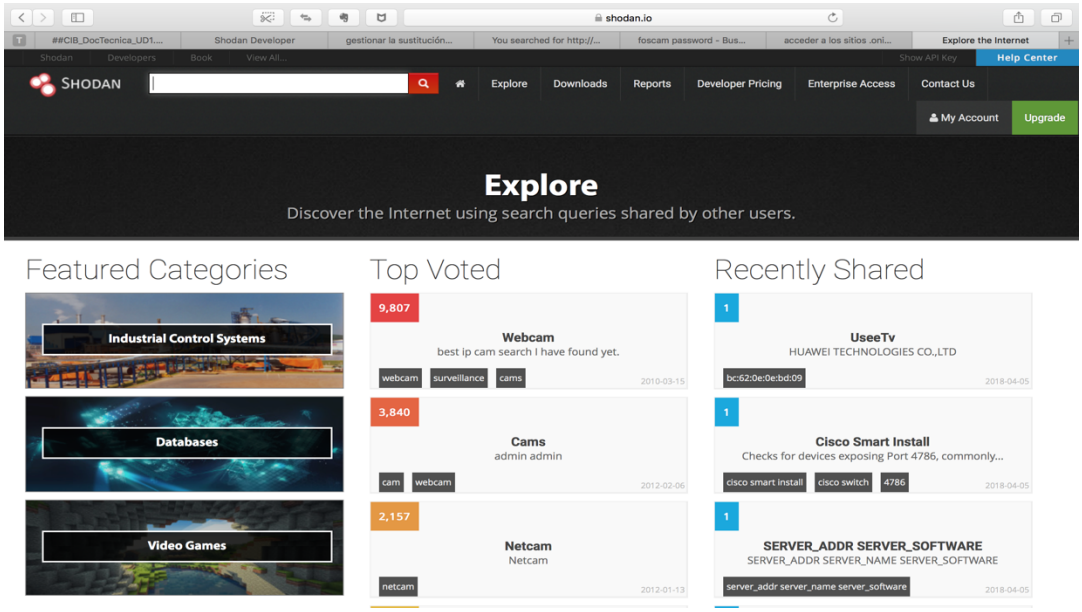
Los filtros que admite Shodan y su significado se muestran en la siguiente tabla:

| Filtro | Descripción | Ejemplo |
|---|---|---|
| **country** | Búsqueda de un país concreto | country:hn VOIP |
| **city** | Búsqueda por ciudad. | city:Madrid Apache |
| **port** | Búsqueda por puerto o servicio. | port:21 city:Ceiba |
| **net** | Búsqueda ip especifica o rangos de ip. | net:186.65.127.0/24 |
| **hostname** | Búsqueda del texto indicado en hostname. | hostname:Prensa |

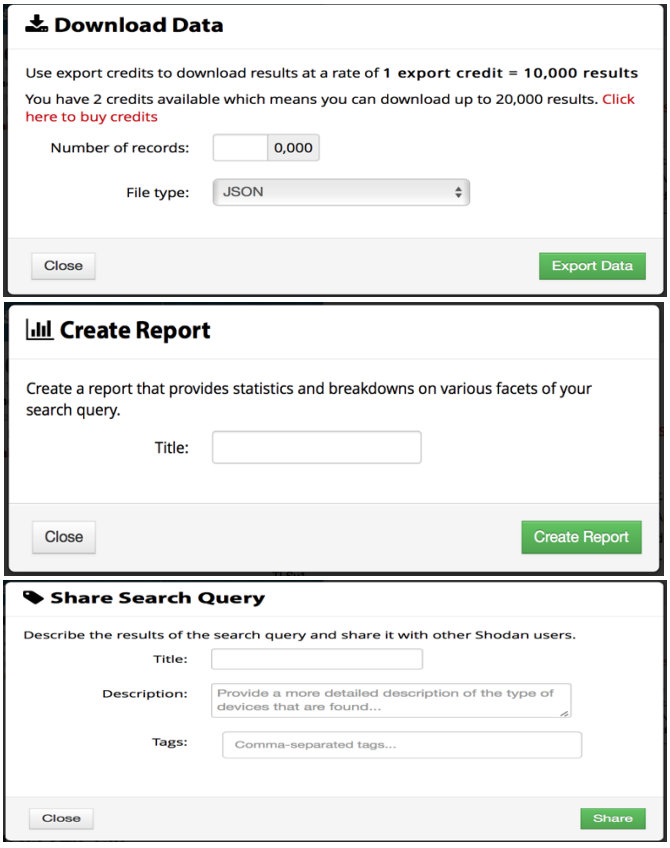
La aplicación ofrece la posibilidad de Loggeo. El usuario no está obligado a logarse, pero si no lo hace no podrá acceder a las funcionalidades de filtrado por los parámetros *country* ni *net*. Asi mismo tampoco podrá exportar los resultados obtenidos de las búsquedas.




El usuario puede acceder a un conjunto de búsquedas pre-configuradas desde la pantalla principal (menú Explore) por tipos de dispositivos o entornos e ir posteriormente refinando la búsqueda por otros parámetros (Pais, etc.)




Igualmente Shodan ofrece la posibilidad al usuario (logado previamente) de exportar los resultados de las búsquedas en diferentes formatos (csv, json, etc.), de generar informes y de compatir los resultados con otros usuarios de shodan.



### 5.3.1. APIs DE SHODAN

Con el objeto de poder hacer un uso avanzado de las funcionalidades de Shodan existen las dos siguientes familias de APIs que pueden ser empleadas en un gran numero de lenguajes diversos de programación:

#### APIs REST

**API REST** proporciona métodos para hacer búsquedas avanzadas en Shodan, búsqueda de hosts, obtención de información resumida de consultas asi como una variedad de métodos de utilidad para hacer más fácil el desarrollo.

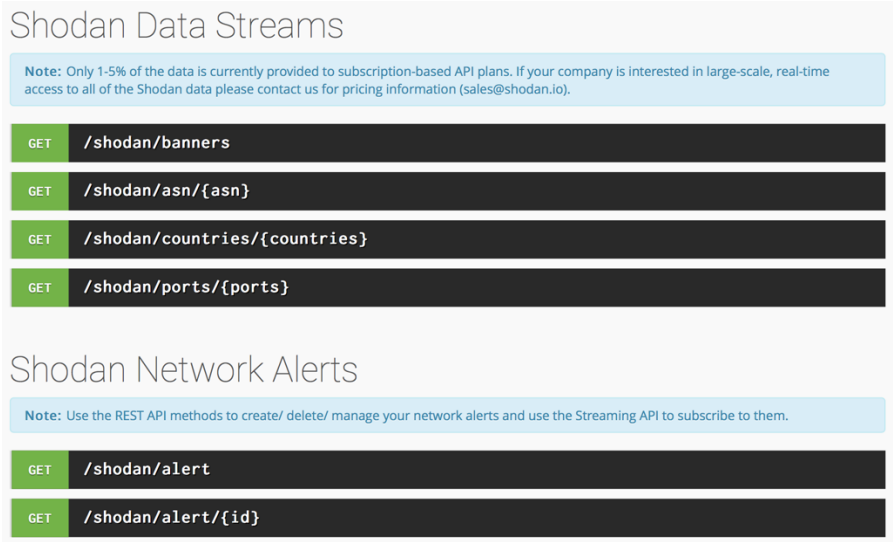
Las APIs disponibles son las siguientes:


## APIs Streaming

**API de Streaming** proporciona los datos en bruto en tiempo real que están siendo recogidos por shodan. Existen varias fuentes de datos en bruto a las que subscribirse, pero no es posible hacer búsquedas sobre dichos datos en tiempo real ya que se trata de una transmisión en vivo de un gran volumen de datos para aplicaciones de consumo de una cantidad ingente de datos.

La API de Streaming es un servicio basado en HTTP que devuelve una secuencia en tiempo real de los datos recogidos por Shodan. El feed devuelve la información como una cadena JSON codificados utilizando 2 formatos de salida distintos.

Las APIs disponibles son las siguientes:




### 5.3.2. Librerias de entornos de programación

Existe un conjunto de librerías para los lenguajes de programación mas extendidos al objeto de facilitar el acceso a las APIs de Shodan.

Actualmente existen librerías disponibles para los siguientes entornos de programación:

- Python
- Ruby
- PHP
- C#
- Go
- Haskell
- Java
- Node.js
- Perl
- Powershell
- Rust

### 5.3.3. Plug-ins de SHODAN

Con el objeto de poder acceder directamente a la funcionalidad de shodan desde los exploradores o aplicaciones mas habituales existen un conjunto de plug-ins.

Los pluggins mas relevantes actualmente están disponibles son para:

- Chrome
- Mozilla

- Maltego
- Metasploit
- Recon-ng

El Plug-in de Shodan te dice, entre otros, dónde está alojado el sitio web (país, ciudad), a quién pertenece el IP y qué otros servicios / puertos están abiertos.

El complemento de Shodan para Chrome o Mozilla comprueba automáticamente si Shodan tiene información para el sitio web actual (ejecución de servicios FTP, DNS, SSH o algún servicio inusual). Con este complemento puedes ver toda la información que Shodan ha recopilado en un determinado sitio web / dominio.


## 5.4. OTRAS HERRAMIENTAS DE POSIBLE APLICACIÓN

Adicionalmente existen en el mercado ya un conjunto de herramientas (en su mayoría libres) que pueden complementar la funcionalidad de Shodan. A continuación se citan las mas importantes:

<u>Buscadores de información en la web (Surface web)</u>

- Google Dorks
- Google Hacking Data Base (GHDB)
- Bing

## Explorador y Buscadores de información en la web (Deep web)

- Explorador: TOR Browser
- Buscadores: Onion.City, Onion.to, Not Evil, Memex Deep Web Search Engine

## Aplicaciones de inspección de páginas

- Acunetix
- Internet Archive

## Herramientas de OSINT e Ingeniería Social

- Análisis y Volcado de paginas Web
- Busqueda de personas
- Obtencion de Logs

## Herramientas de automatización de Busquedas

- TYFYP
- Selenium IDE
- Java unit4

## Aplicaciones de Gestión de Bases de Datos

- Robo Mongo
- MongoDB
- ElasticSearch
- Kibana

## Descifradores de contraseñas

- www.md5-hash.com
- Widows:  Lophtcrack
- Fuerza bruta sobre un cjto. de hashes: John the Ripper, hashcat, 10phtcrack
- Fuerza bruta sobre proceso de logging: Brutus, Hydra

## Aplicaciones de Geolocalización de IP

- IPLocation.net

# 6. FASES DE HACKING DE SIST. SCADA

## 6.1. DESCRIPCION DEL PROCESO GLOBAL DE HACKING

A continuación se describen los pasos necesarios que compondrían el proceso integro de hacking de una organización, donde se pueden distinguir fundamentalmente una primera fase *pasiva* y una segunda fase *activa*.

### 6.1.1. Fase de actuación Pasiva

Esta fase básicamente engloba las actuaciones pasivas (sin interacción detectable por los sistemas del objetivo) propias de OSINT encaminadas a la Recolección de información pública (Surface web o Deep web) para la caracterización de la infraestructura IT del objetivo. Las subfases habituales son:

a) Recolección de información pública.
Obtención de información publica accesible al publico (web, teléfonos, etc.)

Un punto de partida lo constituye el análisis de la página web. Algunas de las cosas que se pueden obtener son la localización, infraestructura con la que cuenta, adquisiciones o fusiones, números de teléfono, nombres de empleados y correos electrónicos así como enlaces hacia y desde otros sitios.

b) Google Hacking.
Obtención de información a través de la web (Surface web y Darkweb).

En esta fase **se utilizará SHODAN asi como** la mayoría de **herramientas auxiliares descritas** en este documento (Google Dorks, GHDB, Bing, etc.)

c) Obtención de información del DNS.
Implementar WHOIS y búsqueda inversa de DNS.

d) Obtención de metadatos.
Obtención de infprmacion de los Metadatos contenidos en los archivos capturados (usuarios, posiciones gps, timestamp, versiones de aplicaciones, etc.)

e) Reconocimiento pasivo de la red.
Reconocimiento y análisis de la red (topologías y rutas de acceso)

### 6.1.2. Fase de Actuación Activa

Esta fase implica la interacción con la infraestructura IT del objetivo, lo que permitirá obtener una gran cantidad de información de forma rápida, pero por el contrario abrirá la posibilidad de ser detectados por sus sistemas de Detección de intrusismos (IDS).

En esta fase **utilizaremos SHODAN para acceder directamente a las URLs de las paginas web, servidores vulnerables de ftp, telnet, ssh, etc. del objetivo** y que han sido previamente identificados por ésta.

Una vez identificados los citados servicios, la tarea consistirá en tratar de acceder mediante el forzado de las credenciales de acceso.

## 6.2. HACKING CON SHODAN

SHODAN es en sí un motor de búsqueda de equipos conectados al internet, funciona por medio de crawlers o robots que van haciendo consultas sobre internet y preguntando si la dirección corresponde a un dispositivo. En caso afirmativo lo almacena en sus bases de datos junto que los metadatos que pueda recoger de cada dispositivo, que son sobre los que los usuarios de Shodan buscan posteriormente información.

El proceso de consulta mediante Shodan no es intrusivo sino pasivo, ya que solo se está leyendo y guardando la información que estos dispositivos tienen expuesta en la red. Únicamente se convierte en activo en el momento en que nosotros accedemos a la URL o Link de cualquiera de los servicios asociados al equipo objetivo.

El proceso de Hacking con Shodan se fundamenta en:

1. Exploración e Identificación de equipos con vulnerabilidades de seguridad.
2. Busqueda en la web de contraseñas débiles o por defecto vinculadas a los equipos identificados
3. Intento de acceso a sus diferentes servicios o puertas de acceso vulnerables asociados mediante logeo empleando contraseñas débiles (contraseñas por defecto) o por mecanismos de fuerza bruta.

Las diferentes vulnerabilidades de los sistemas que pueden ser explotadas a través de SHODAN tienen su origen principalmente en tres errores de configuración de seguridad:

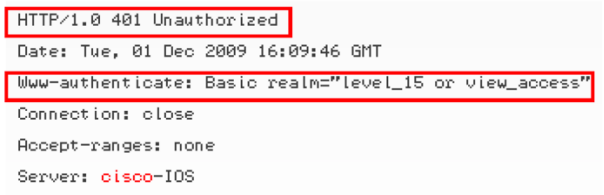
1. Usuarios por defecto o de fácil identificación programadamente.
2. Contraseñas por defecto o contraseñas débiles, que pueden ser fácilmente adivinables por medio de wordlist o listas de palabras.
3. Falta de mecanismo de bloqueo de cuenta al detectar cierto número de intentos fallidos.

El procedimiento de Hacking pues se fundamenta en introducir claves en el campo de búsqueda con arreglo a los contenidos de los banners que nos interesa localizar.

Para ello es interesante conocer los códigos de estado HTTP que nos indican los requerimientos de autentificación de cada nodo. Estos son los siguientes:

| Status Code | Description |
|---|---|
| 200 OK | Request succeeded |
| 401 Unauthorized | Request requires authentication |
| 403 Forbidden | Request is denied regardless of authentication |

En el siguiente banner perteneciente a un router CISCO podemos ver que el código de estado HTTP es de tipo 401. Además si observamos la línea Www-aunthenticate ya nos está indicando que se nos requewrirá un usuario y una password para logeado.



# 7. PROCEDIMIENTOS DE HACKING DE SIST. SCADA CON SHODAN

El presente apartado tuvo como objeto describir la forma general de uso de Shodan en el proceso de hacking de sistemas SCADA.

En el siguiente apartado 7.1. se describe como se puede utilizar Shodan como herramienta para la identificación de equipos vulnerables mediante la configuración de los filtros y claves de búsqueda adecuados.

En los apartados siguientes dentro de este capítulo describiremos otros procedimientos mas complejos donde se pueden combinar dichos resultados obtenidos con Shodan con otras aplicaciones para llegar a acceder a los equipos vulnerables y reconfigurar éstos o bien extraer de ellos información.

Partiendo de las búsquedas más comunes empecé a explorar y hacer pruebas para acabar encontrando dispositivos con huecos de seguridad, encontrando diversos hallazgos, desde acceso a cámaras hasta acceso a routers, para lo cual una vez identificado el equipo a analizar y el tipo de acceso posible (telnet, http, ftp, ssh, etc.) traté de buscar las claves por defecto.

## 7.1. USO DE FILTROS Y CLAVES DE BUSQUEDA EN SHODAN

Siguiendo los pasos para análisis de vulnerabilidades, dentro de este trabajo empezamos buscando los dispositivos más comunes o más frecuentemente expuesto a la red, para lo cual hicimos una búsqueda en internet apoyados en Google y así también en la propia página de Shodan, obteniendo de dicha investigación la siguiente información:

| Tipo | Descripción | Parámetros de búsqueda | Link | Resultados |
|---|---|---|---|---|
| WebCam | Cámaras de seguridad | Server: SQ-WEBCAM | URL | 124 |
| Cams | Cámara Universal Plug and Play AvTech | linux upnp avtech | URL | 112.362 |
| Dreambox | Decodificadores de España → Linux-powered DVB satellite, terrestrial and cable digital television receivers (set-top box) | Dreambox country:ES | URL | 568 |

| | | | | |
|---|---|---|---|---|
| Default password | Dispositivos que dentro de sus metadatos tengan relación con las palabras claves “default password” | "default password" | URL | 77.804 |
| Netgear | Routers inalámbricos NetGear | Netgear | URL | 237.959 |
| Router w/ Default Info | Routers con información en mensaje de autenticación o en banner de admin/1234 | admin+1234 | URL | 8.818 |
| Android Webcam | Webcams Android sin clave | Android Webcam Server -Authenticate | URL | 37 |
| D-Link Internet Camera | Cámaras D-link sin autenticación | d-Link Internet Camera, 200 OK | URL | 168 |
| | | | | |

*Tabla 1. Búsquedas populares extraídas del sitio web de Shodan, al 14 de junio de 2015*

De las búsquedas Shodan presentadas anteriormente, podemos observar que la mayoría buscan por el nombre o alguna identificación relacionada al dispositivo, como son su marca (d-link), tipo (camera), sistema operativo (linux), pudiendo de aquí desprender otras búsquedas según los que podamos buscar, por ejemplo: podría buscar equipos Polycom (equipos de video conferencia), router cisco, y luego complementar esto con los filtros que permite Shodan como son:

- **Ciudad** → city:Cuenca , para buscar equipos que estén en la ciudad de Cuenca
- **País** → country:EC , para buscar equipos en Ecuador
- **Puerto** → port:23 , para buscar equipos que tengan habilitado o estén a la escucha del puerto 23 generalmente asociado a Telnet
- **Fechas, antes de o desde de (dd/mm/yyyy)** → before:01/01/2015 , para equipos indexados antes del 01 de enero de este año; after:01/01/2015, para equipos indexados por Shodan a partir del inicio de este año. Estos parámetros no los considero relevantes, pues dada la limitación de Shodan (sin pago) de permitir consultar solo hasta 5 paginas (50 resultados) y estos al presentarse ordenados descendentemente por orden de indexación, estaríamos obteniendo los más recientes equipos con posibles huecos de seguridad y ya de fecha anteriores serian de menos importancia pues es posible que ya hayan sido corregidas sus fallas y por eso no se los ha detectado últimamente.
- **Nombre del equipo** → hostname:etapa , para equipos cuyo nombre de equipo o dominio tenga la palabra etapa (Empresa Municipal de Telefonía Agua Potable y Alcantarillado)
- **Dirección de red** → net: 200.55.224.68, para buscar equipos enlazados o públicos sobre una determina dirección de red, útil cuando conocemos la IP y queremos consultar los equipos atados a dicha IP.
- **Sistema operativo** → os:linux, para equipos con sistema operativo Linux

## 7.2. BUSQUEDAS COMPLEMENTARIAS CON GOOGLE DORKS Y GHDB

### 7.2.1. Búsqueda con Google DORKS

Google Dorks constituye un servicio basado en el buscador de Google que permite hacer una búsqueda avanzada de información mediante el empleo de una serie de filtros.

A continuación relaciono una serie de casos de uso que recogen combinaciones de filtros de Google Dorks que pueden ofrecer información de gran utilidad para las labores posteriores de Hacking con SHODAN.

**allinurl: tsweb / default.htm**

- *Objetivo perseguido:* Obtener páginas web que contengan el término 'tsweb / default.htm' en su url, lo que devuelve páginas diseñadas para permitir el acceso a su servidor de forma remota (mediante el servicio de Windows *Remote Desktop Web Connection*)
- *Tipo de información:* el hacker podría obtener los datos de logado del usuario (password y contraseña)
- *Vulnerabilidades (CVE):* Alguna páginas indican la dirección IP del servidor, la cual puede ser explotada para obtener un acceso externo ilícito.

**inurl:passlist.txt filetype:txt**

- *Objetivo perseguido:* Obtener páginas web que contienen el término 'passlist.txt' en el título.
- *Tipo de información:* Se puede descargar archivos .txt que contienen listados de nombres de usuario y contraseñas.
- *Vulnerabilidades (CVE):* Con ellos se pueden tratar de desarrollar ataques de fuerza bruta.

**intitle: index.of.etc**

- *Objetivo perseguido:* Obtener páginas web que contienen listados de directorios que contiene ficheros de todo tipo. 'Index of' nos muestra directorios presentándolos emn un índice.
- *Tipo de información:* Se puede visionar y descargar cualquier tipo de fichero que se encuentre archivado y accesible al exterior.
- *Vulnerabilidades (CVE):* Los servidores web que devuelven los archivos almacenados en sus directorios ante esta petición, no están protegiendo adecuadamente la información almacenada, pues están mostrando la estructura de carpetas y archivos, permitiendo incluso la descarga de los mismos.

**intitle:"Index of" passwd passwd.bak**

- *Objetivo perseguido:* Obtener páginas web que contienen listados de directorios que contiene ficheros antiguos de contraseñas.
- *Tipo de información:* El hacker puede obtener contraseñas antiguas asociadas a nombres de usuarios. Si bucea un poco mas en la información de la web correspondiente, mediante la búsqueda de páginas de conexión remota a escritorio (*p.ej. allinurl: tsweb / default.htm)* podría probar con cualquiera de estas contraseñas y conseguir el acceso al servidor.

- *Vulnerabilidades (CVE):* La vulnerabilidad en este caso consiste en mantener ficheros antiguos de contraseñas accesibles desde la red, en vez de encontrarse archivados en un dispositivo no conectado a una red con conexión al exterior.

**intitle:"Index of" ".htpasswd" "htgroup" -**

- *Objetivo perseguido*: Obtener páginas web que contienen listados de directorios que contienen ficheros ocultos (empiezan por un punto) de contraseñas de usuarios y grupos de estos, dado que .htpasswd es un fichero plano que almacena usuarios y sus contraseñas de autenticación para los servidores http de Apache. 'htgroup' contiene los grupos de usuarios.
- *Tipo de información*: En caso de que el hacker tenga acceso a dichos archivos dispondría de acceso total a los pares de contraseñas (user:password) contenidas en los archivos htpasswd (véase ejemplo de archivo htpasswd).
    - `root:root`
    - `John:john123`
    - `Dave Smith:dave123`
    - `Mike:mike123`
    - `Jane:jane123`
    - `Dawn:dawn123`
    - `Ruth Smith:ruth123`
- *Vulnerabilidades (CVE):* En servidores Apache el usuario local podría ganar privilegios a través del empleo de meta caracteres Shell como argumentos el línea de comandos. Esta vulnerabilidad es la CVE-2006-1079

**intitle:"dist" -apache -htpasswd.c**

- *Objetivo perseguido*: Buscar las webs que incluyan en el título "dist", (podría ser el archivo de configuración) y excluyan los que tengan "apache" y "htpasswd.c". La realidad es que encuentra infinidad de URL que tienen "dist" y que no parecen ser el resultado de la búsqueda.
- *Tipo de información:* Búsqueda de archivos de configuración que no sea el servidor apache ni los passwords de este.
- *Vulnerabilidades (CVE):* Archivos de configuración disponibles a partir de búsqueda en el título de la URL.

**intitle:"Index of" ".htpasswd" "htgroup" -"dist" -apache -htpasswd.c**

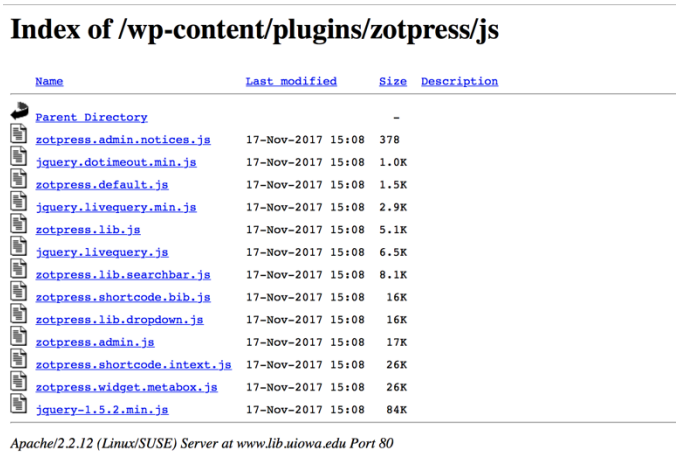
- *Objetivo perseguido:* Buscará URL's que tienen el título de la página web (intitle) los directorios/ficheros que contiene .htpasswd y/o "htgroup", excluyendo de esta búsqueda a los que contengan dist, sean "apache" o "htpasswd.c"
- *Tipo de información:* Información de contraseñas cifradas y grupos de usuarios excluyendo las enumeradas.
- *Vulnerabilidades en web:* Vulnerabilidad para encontrar contraseñas y grupos de usuarios en servidores Apache de forma exclusiva.

**intitle: index.of "Apache.2.2.12" "server at**

- *Objetivo perseguido:* Buscará URL's que tienen el título de la página web (intitle) los directorios que contiene "Apache.2.2.12" y "server at" en dicha url poniéndolo en un

índice. Es decir, te dará las URL's que tienen los listados con las cadenas mencionadas.

- *Tipo de información:* Listados que residen en los servidores apache citados y servido por un dominio X.
- *Vulnerabilidades en web:* Visibilidad de la versión del servidor Apache y quien lo sirve, así como su contenido.



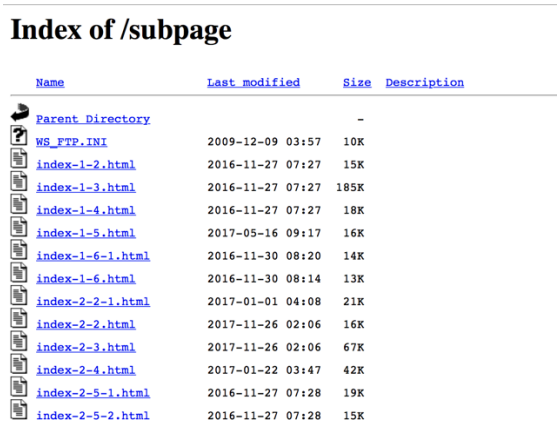
**Index of /wp-content/plugins/zotpress/js**

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| zotpress.admin.notices.js | 17-Nov-2017 15:08 | 378 | |
| jquery.dotimeout.min.js | 17-Nov-2017 15:08 | 1.0K | |
| zotpress.default.js | 17-Nov-2017 15:08 | 1.5K | |
| jquery.livequery.min.js | 17-Nov-2017 15:08 | 2.9K | |
| zotpress.lib.js | 17-Nov-2017 15:08 | 5.1K | |
| jquery.livequery.js | 17-Nov-2017 15:08 | 6.5K | |
| zotpress.lib.searchbar.js | 17-Nov-2017 15:08 | 8.1K | |
| zotpress.shortcode.bib.js | 17-Nov-2017 15:08 | 16K | |
| zotpress.lib.dropdown.js | 17-Nov-2017 15:08 | 16K | |
| zotpress.admin.js | 17-Nov-2017 15:08 | 17K | |
| zotpress.shortcode.intext.js | 17-Nov-2017 15:08 | 26K | |
| zotpress.widget.metabox.js | 17-Nov-2017 15:08 | 26K | |
| jquery-1.5.2.min.js | 17-Nov-2017 15:08 | 84K | |

*Apache/2.2.12 (Linux/SUSE) Server at www.lib.uiowa.edu Port 80*

**intitle:index.of ws_ftp.ini**

- *Objetivo perseguido:* Buscará URL's que tienen el título de la página web (intitle) los directorios que contiene "ws_ftp.ini". Búsqueda de contraseñas en el archivo de configuración de FTP win32.
- *Tipo de información:* Nombres de usuario y contraseña débilmente codificadas.
- *Vulnerabilidades en web:* Esta búsqueda utiliza el "directorio padre" para evitar resultados que no sean listados de directorio. "WS_FTP.ini" es un archivo de configuración para un popular cliente "FTP win32" que almacena nombres de usuario y contraseñas que están débilmente codificadas.



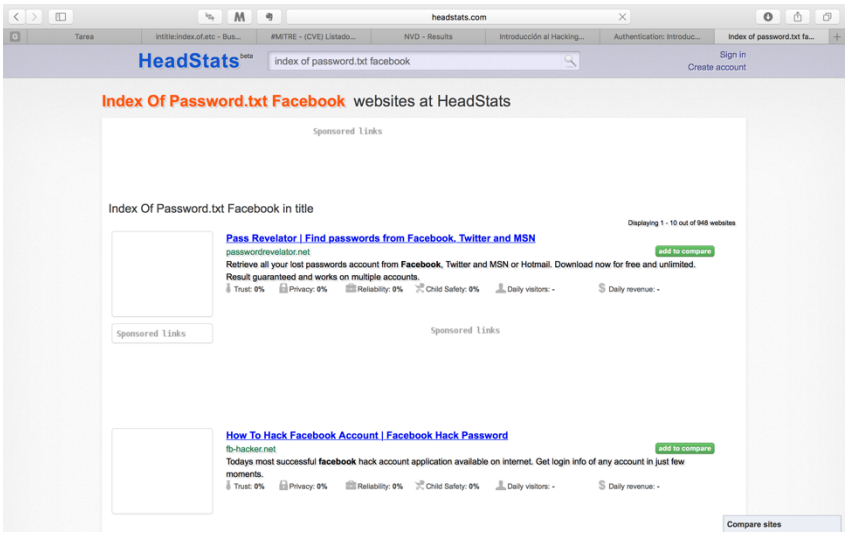
**Index of /subpage**

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| WS_FTP.INI | 2009-12-09 03:57 | 10K | |
| index-1-2.html | 2016-11-27 07:27 | 15K | |
| index-1-3.html | 2016-11-27 07:27 | 185K | |
| index-1-4.html | 2016-11-27 07:27 | 18K | |
| index-1-5.html | 2017-05-16 09:17 | 16K | |
| index-1-6-1.html | 2016-11-30 08:20 | 14K | |
| index-1-6.html | 2016-11-30 08:14 | 13K | |
| index-2-2-1.html | 2017-01-01 04:08 | 21K | |
| index-2-2.html | 2017-11-26 02:06 | 16K | |
| index-2-3.html | 2017-11-26 02:06 | 67K | |
| index-2-4.html | 2017-01-22 03:47 | 42K | |
| index-2-5-1.html | 2016-11-27 07:28 | 19K | |
| index-2-5-2.html | 2016-11-27 07:28 | 15K | |

**inurl:index.of.password site: .cl**

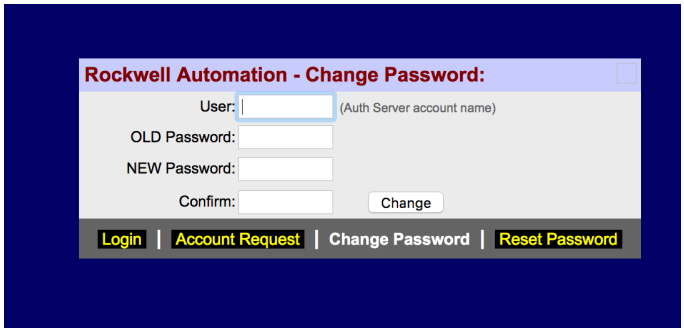
- *Objetivo a perseguir:* El objetivo de este comando es encontrar URLs asignadas al país de chile que contuvieran listados de archivos o directorios con el término 'password'.
- *Tipo de información:* Un indice de passwords.

- *Vulnerabilidades en web:* La vulnerabilidad en este caso consiste en mantener ficheros antiguos de contraseñas accesibles desde la red, en vez de encontrarse archivados en un dispositivo no conectado a una red con conexión al exterior.




**inurl:changepassword.cgi -cvs**

- *Objetivo a perseguir:* El objetivo de este comando es encontrar en las webs un término llamado "changepassword.cgi" en su URL excluyendo los resultados que tengan "cvs", es decir, los que incluyan controles de versiones para dar con la que está activa.
- *Tipo de información:* Muestra ventanas de cambio de contraseña.
- *Vulnerabilidades en web:* Permite a un usuario cambiar su contraseña para la autenticación en el sistema.




### 7.2.2. Búsqueda en repositorio GHDB

La base de datos "Google Hacking Database" (GHDB) de Johnny Long, recopila búsquedas especiales de Google Dorks permitiéndonos encontrar gran cantidad de información filtrada en internet sobre una determinada web o sobre un objetivo concreto (como una persona o una organización).

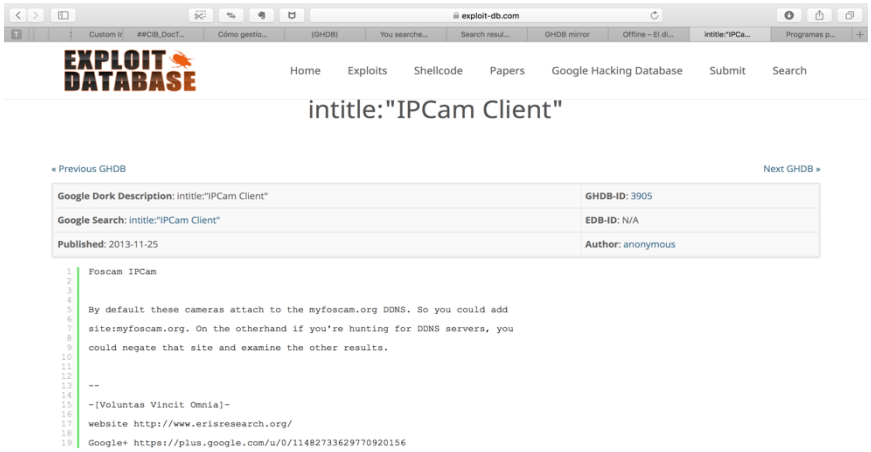
Vamos a buscar dispositivos de tipo cámaras web IP del fabricante FOSCAM vulnerables por errores de configuración.

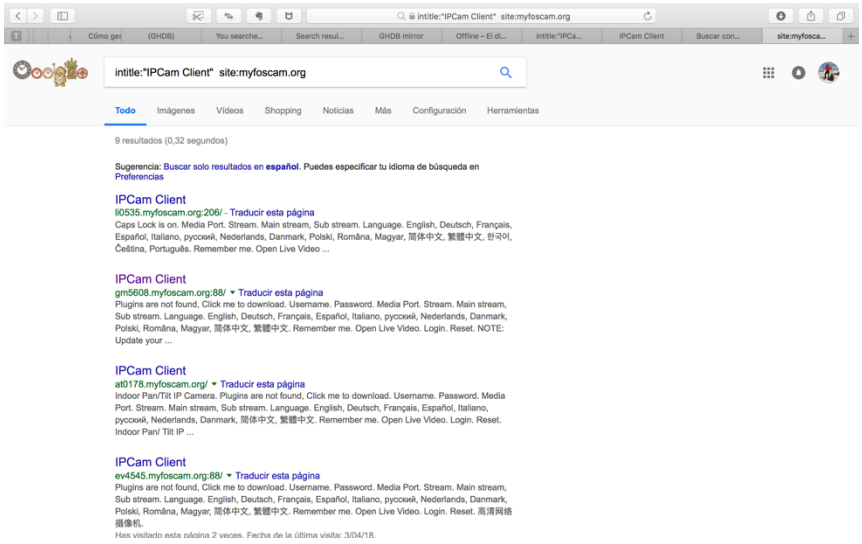
1.- En primer lugar nos dirigimos al sistio web https://www.exploit-db.com/google-hacking-database/

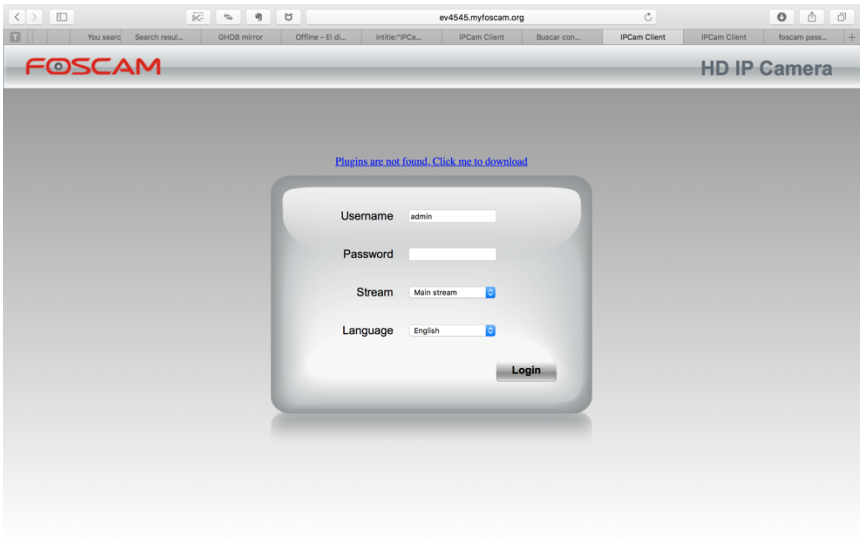
2.- A continuación seleccionamos en el menú desplegable la categoría de elemento a buscar. En nuestro ejemplo hemos seleccionado 'Dispositivos varios on-line'.

3.- Seguidamente introducimos como término de búsqueda 'IP FOSCAM' y obtenemos un resultado de google dorks.


4.- Si pinchamos en el enlace vemos una descripción mas detallada del Dorks y vemos además que podemos buscar en Google dorks filtrando por dos términos de búsqueda simultáneos, lo que nos devuelve una serie de enlaces a servicios de Camaras IP FOSCAM desde lo cuales podemos forzar un logado.






## 7.3. ACCESO A SISTEMAS SCADAS

Desde la pagina principal de SHODAN se puede seleccionar diferentes repositorios o instalaciones objetivo (Data Bases, Video Games, etc). Entre ellas se puede seleccionar Sistemas de Control Industrial (ICS) lo cual nos lleva a un repositorio de Equipos ICS vulnerables clasificados según los fabricantes de SCADA y sus protocolos propietarios.

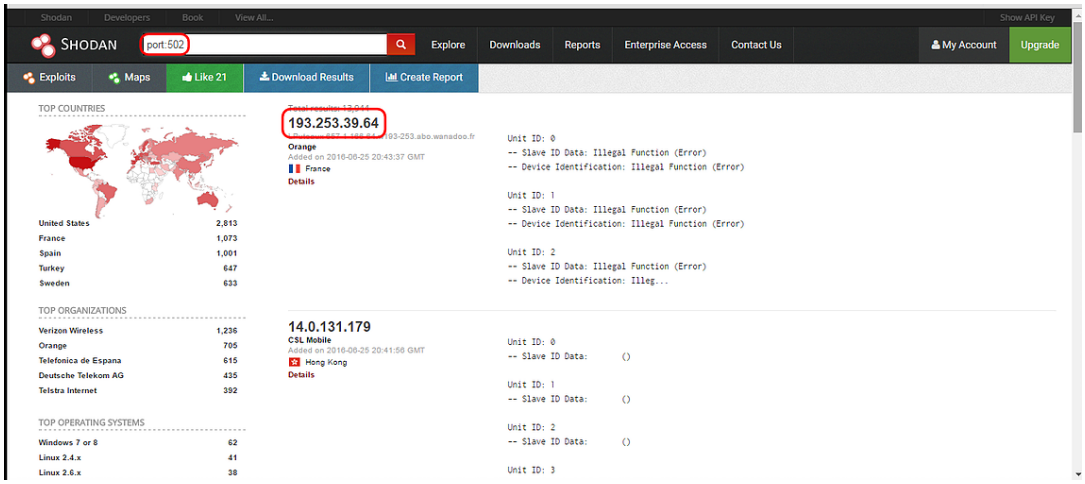

## 7.3.1. ACCESO A SIST. SCADA CON PROTOCOLO *MODBUS*

En este caso vamos a mostrar el modo de uso de Shodan basándonos en el protocolo *Modbus*, que constituye uno de los protocolos de referencia en entornos ICS.
Como sabemos que *Modbus* se ejecuta en el puerto 502, simplemente podríamos buscar en Shodan cualquier IP que tenga ese puerto abierto a Internet. Muy probablemente los equipos identificados formen parte de alguna estructura SCADA de alguna instalación industrial.

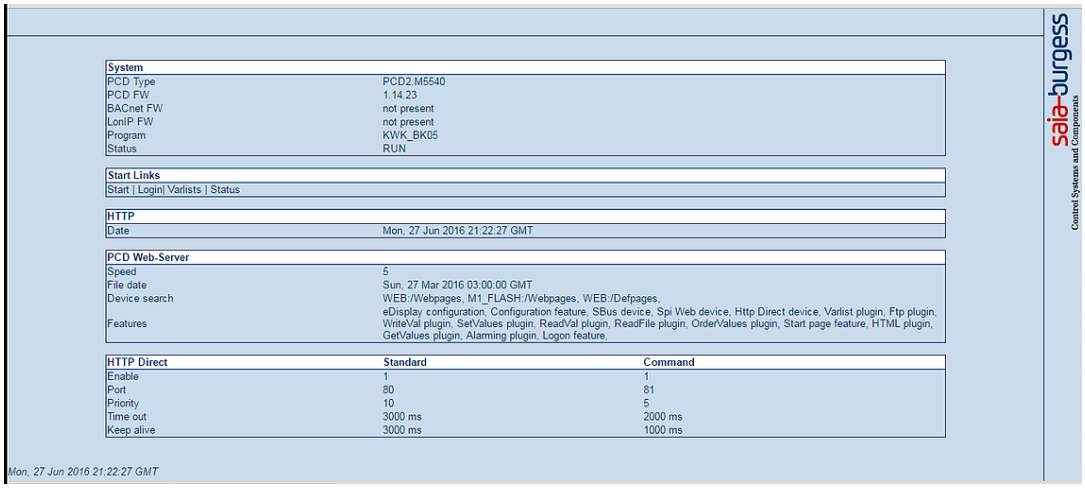
Vamos a abrir shodan y a buscar equipos con el puerto 502 abierto. Para ello escribiremos en la ventana de búsqueda (port: 502)

Tenga en cuenta que en Shodan, primero escribimos el parámetro que estamos buscando (port), seguido de dos puntos (:) y finalmente el valor (502). Cuando lo hacemos, ¡encontramos más de 13,000 resultados! Aunque no hay ninguna garantía de que todas estas IP estén ejecutando Modbus, es probable que la mayoría si, ya que el puerto 502 no es un puerto popular.

Podemos ver la primera página de resultados de nuestra búsqueda de Shodan a continuación.




Tenga en cuenta que el primer resultado tiene una dirección IP 192.253.39.64. Debajo del IP podemos ver que está basado en Francia y está conectado a través del sistema de telecomunicaciones Orange (anteriormente llamado France Telecom). Cuando hacemos clic en la IP, nos lleva directamente a la interfaz de administración de este dispositivo usando *modbus*.



| System | |
|---|---|
| PCD Type | PCD2.M5540 |
| PCD FW | 1.14.23 |
| BACnet FW | not present |
| LonIP FW | not present |
| Program | KWK_BK05 |
| Status | RUN |

| Start Links |
|---|
| Start \| Login\| Varlists \| Status |

| HTTP | |
|---|---|
| Date | Mon, 27 Jun 2016 21:22:27 GMT |

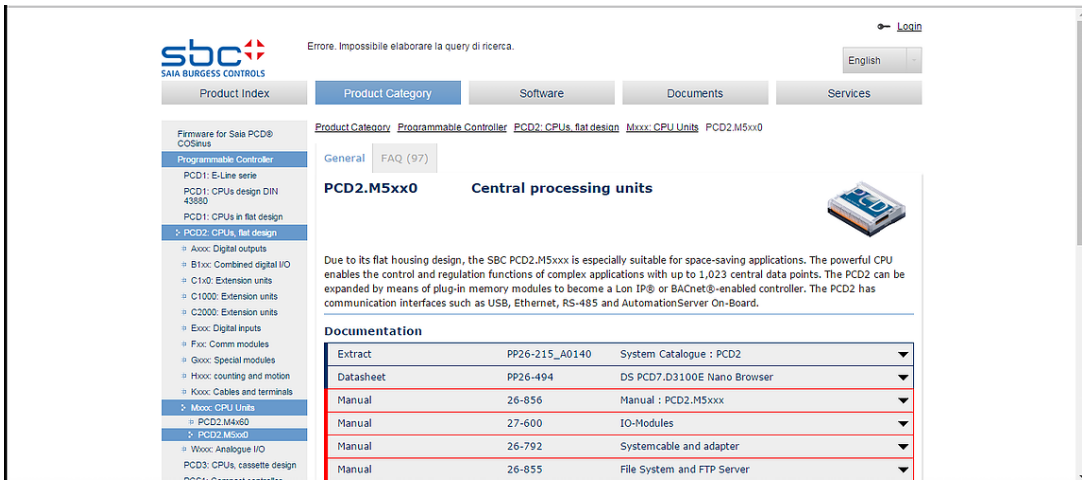
| PCD Web-Server | |
|---|---|
| Speed | 5 |
| File date | Sun, 27 Mar 2016 03:00:00 GMT |
| Device search | WEB:/Webpages, M1_FLASH:/Webpages, WEB:/Defpages, |
| Features | eDisplay configuration, Configuration feature, SBus device, Spi Web device, Http Direct device, Varlist plugin, Ftp plugin, WriteVal plugin, SetValues plugin, ReadVal plugin, ReadFile plugin, OrderValues plugin, Start page feature, HTML plugin, GetValues plugin, Alarming plugin, Logon feature, |

| HTTP Direct | Standard | Command |
|---|---|---|
| Enable | 1 | 1 |
| Port | 80 | 81 |
| Priority | 10 | 5 |
| Time out | 3000 ms | 2000 ms |
| Keep alive | 3000 ms | 1000 ms |

Mon, 27 Jun 2016 21:22:27 GMT

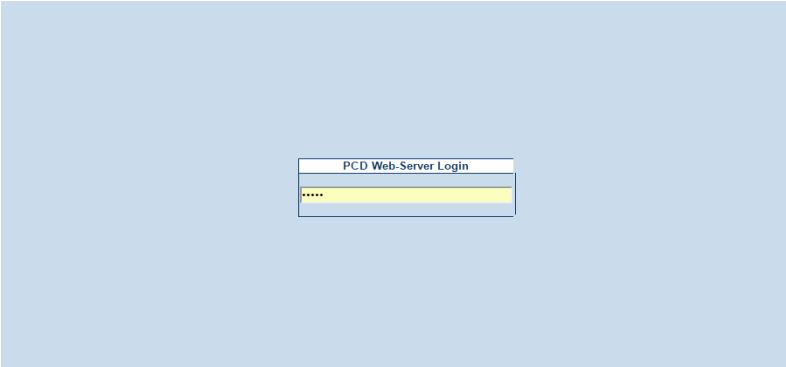
saia-burgess Control Systems and Components

Con una pequeña investigación en Internet, podemos decir que este PLC está fabricado por SAIA-Burgess, una empresa suiza. Principalmente fabrican PLC programables en el campo para los mercados de calefacción y refrigeración.




Cuando hacemos clic en el inicio de sesión, llegamos a un inicio de sesión de servidor web PCD. Si pudiéramos acceder aquí, tendríamos acceso a los controles de este PLC y controlaríamos la temperatura y la eficiencia energética de esta instalación.

Después de varios intentos fallidos de inicio de sesión, continué recibiendo esta página de inicio de sesión, lo que indica que no hay mecanismo de bloqueo de seguridad en esta página, por lo que es susceptible de intentos de fuerza bruta en su contraseña.



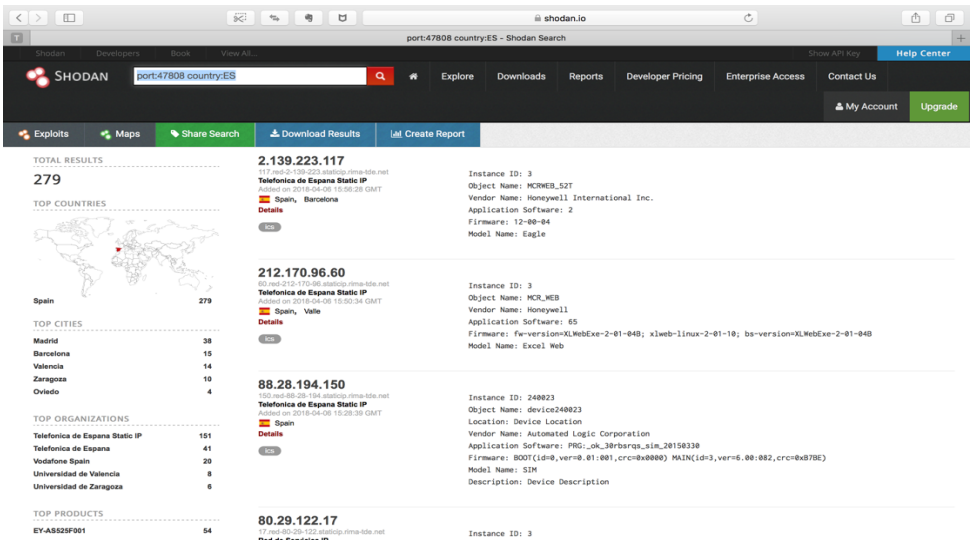

Además, dado que sabemos que este dispositivo está utilizando el puerto 502 para la comunicación *Modbus*, es probable que sea susceptible de falsificación de *modbus* y/o ataque DoS en ese puerto.

Este es un buen ejemplo de cómo los sistemas SCADA pueden ser identificados por Shodan. A menudo sus defensas son débiles y limitadas y los ataques simples como el crackeo de contraseñas de fuerza bruta y los ataques DoS pueden ser ejecutados con facilidad.

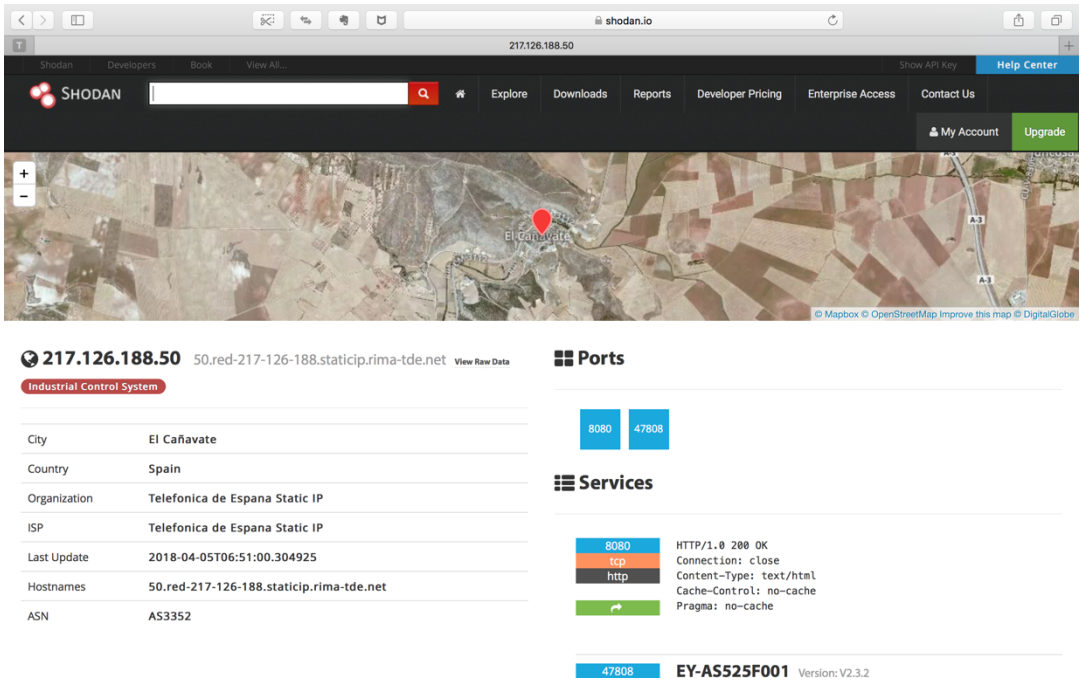
### 7.3.2. ACCESO A SIST. SCADA MODUWEB

SAUTER moduWeb es una plataforma de control industrial especializada en sistema de Climaticación (HVAC) ampliamente extendida en el mercado.

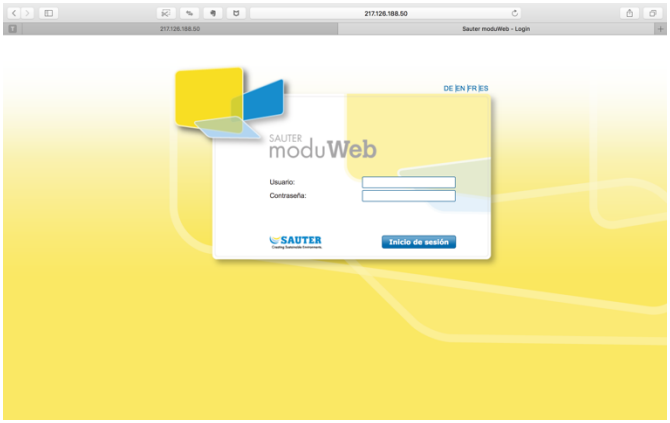
Para identificar servidores de MODUWEB estableceríamos como filtro de búsqueda el parámetro ‘port: 47808’. Para acotar mas la búsqueda especificaremos que nos devuelva únicamente los sistemas en territorio nacional, ello nos devolvería los nodos con el puerto 47808 abiertos en España.



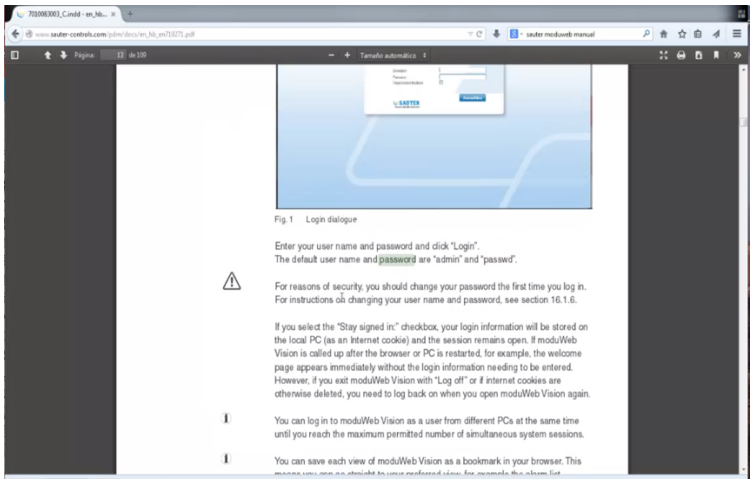
Si el nodo dispone de un Servicio Web de MODUWEB, entonces SHODAN nos permite acceder a través del navegador y por tanto tratar de forzar las credenciales de logeo y acceder así al sistema de control del SCADA.



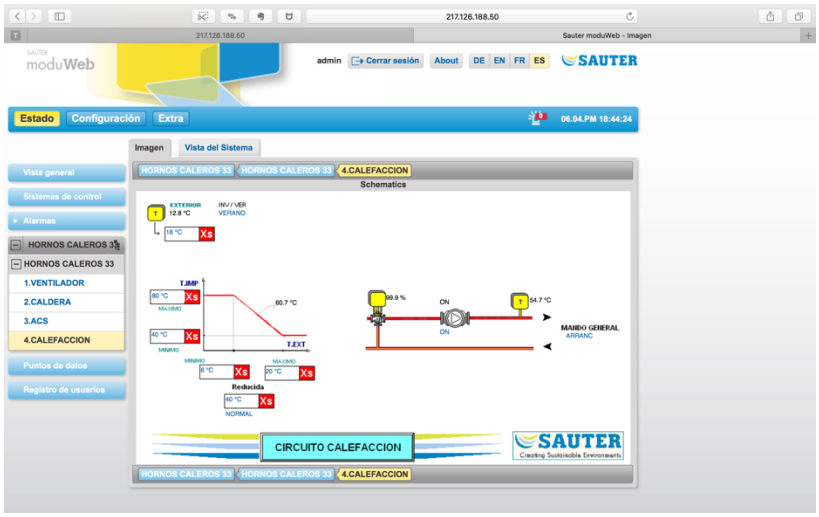

A continuación accedemos al enlace del servicio (https://www.shodan.io/host/217.126.188.50) y obtenemos la ventana de logado.

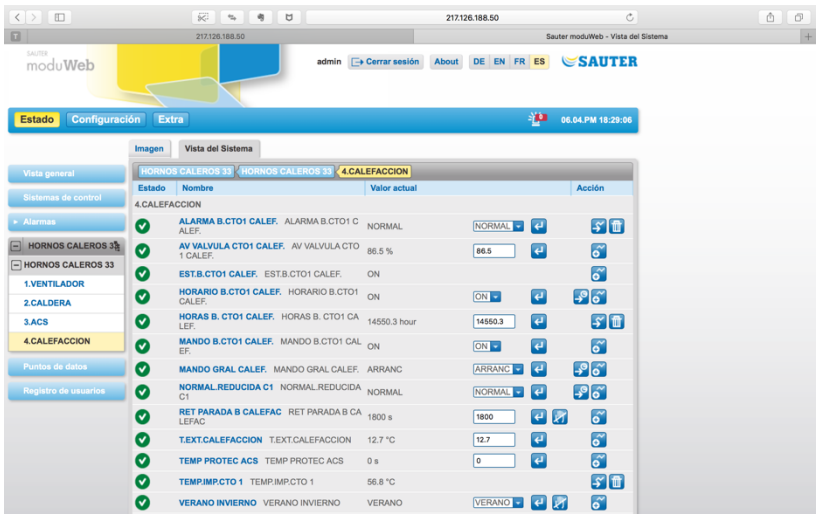


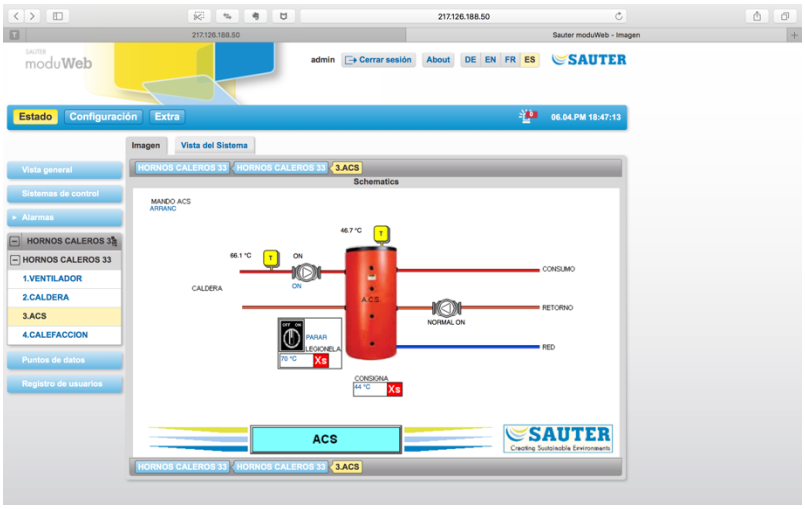

Busqué en Internet las credenciales por defecto de los sistemas moduWeb de la empresa SAUTER y ví que eran admin: passwd.

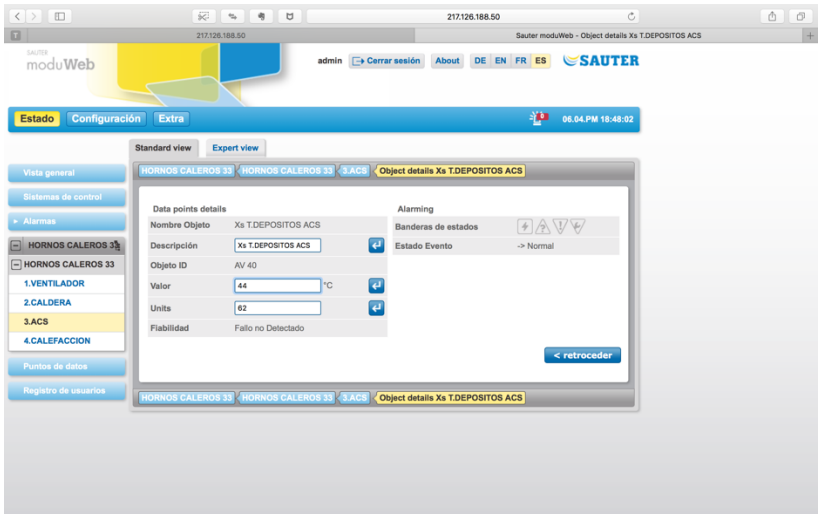



Probé suerte y conseguí acceder al sistema SCADA. Hice unas cuantas pruebas para chequear que efectivamente tenía acceso de modificación de los parámetros del sistema para concluir que el hacking había sido exitoso.





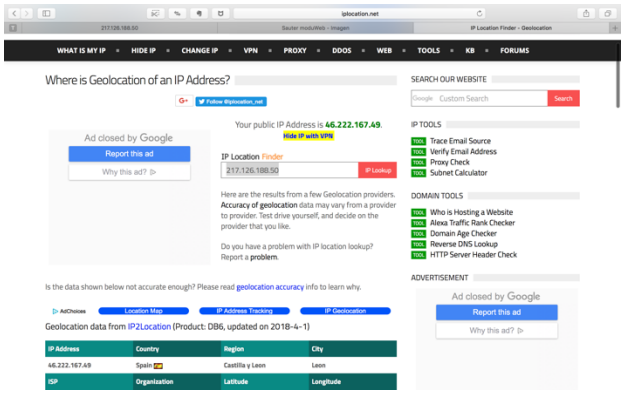

## 7.3.3. GEOLOCALIZACIÓN DE SISTEMAS SCADA

En SHODAN podemos acometer búsquedas introduciendo nombres comerciales de sistemas SCADAS (p.ej. las cadenas 'Schneider Electric BMX P34' o 'SCADA') y la aplicación nos devuelve la información disponible de los nodos que coincidan con la búsqueda, entre la que se encuentra la dirección IP.

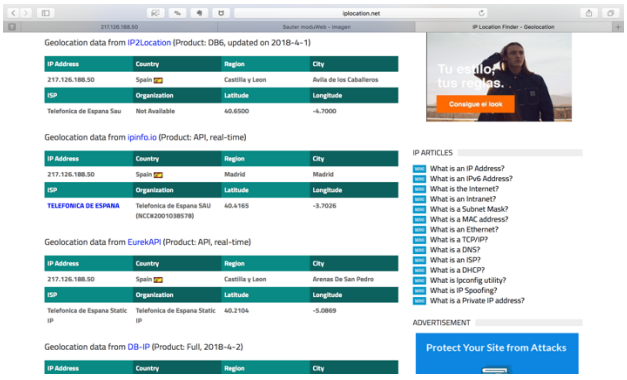
Posteriormente podemos filtrar en SHODAN, en el panel de la parte izqda., por modelos de SCADA e incluso versiones.

Shodan siempre ofrece por defecto la dirección IP de cada nodo asi como una geolocalización aproximada de dicha IP. Pero si deseamos obtener una posición exacta determinada por coordenadas podemos recurrir a aplicaciones como ***IPLocation*** para determinar geográficamente su ubicación y las características de su entorno.

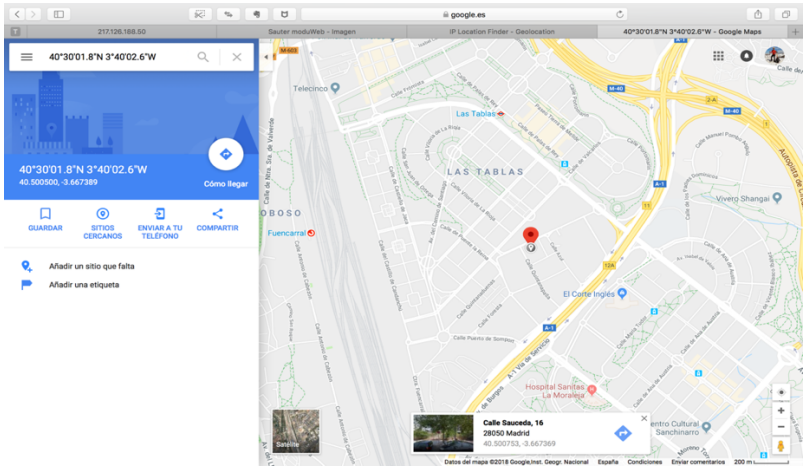
Vamos a hacer la prueba con el SCADA de moduWeb del caso anterior, cuya IP era 217.1126.188.50. Introducimos la dirección IP en el campo de búsqueda de IPLocation.




La aplicación ofrece varias posibles ubicaciones (si bien todas ellas determinadas por coordenadas de precisión).




Finalmente introducimos las coordenadas en el campo de búsqueda de una aplicación GIS como p.ej Google Maps y ya tenemos georeferenciado el nodo que corresponde a dicha IP.



## 7.4. ACCESO A DISPOSITIVOS CON CONTRASEÑAS POR DEFECTO

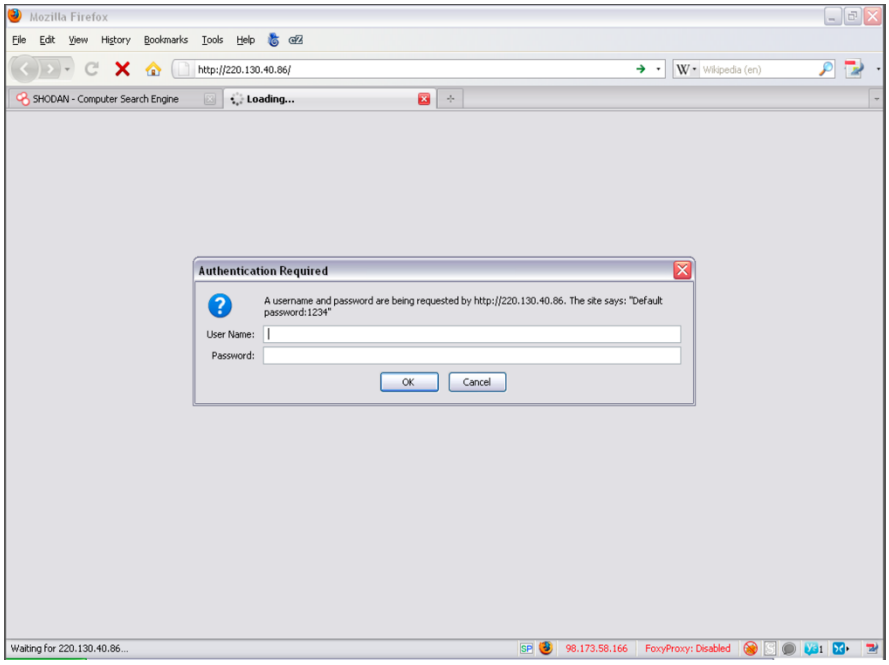
Si planteamos búsquedas introduciendo el término 'default password' SHODAN nos devolverá servidores SHODAN que tiene ese parámetro en sus banners.

Ello no nos asegura que dichos dispositivos no requieran posteriormente acreditarse pero al menos nos servirá para centrar bastante la búsqueda.

Abajo vemos un ejemplo del banner de un servidor devuelto por SHODAN (aparentemente se trata de un servidor de impresión) en el que aparece el código de estado 401 que nos indica que se nos requerirá acreditarnos pero que muy probablemente las claves requeridas sean aquellas por defecto.

```
HTTP/1.0 401
Date: Sat, 21 Dec 1996 12:00:00 GMT
Www-authenticate: Basic realm="Default password:1234"
Server: PrintSir WEBPORT 1.1
```

El hecho de que el banner no recoja el parámetro de 'username' nos recomienda dejar en blanco el campo o bien introducir 'admin'.



## 7.5. ACCESO A ROUTERS

### 7.5.1. ACCESO A ROUTERS CISCO

En primer lugar hay que tener en cuenta que los códigos de estado HHTP relativos a autenticación pueden ser de tres tipos:

- 200 OK → No requerirán autenticación
- 401 Unauthorized → Requerirá autenticación con user y password
- 403 Forbidden → El acceso es denegado con independencia de la autenticación.

Para acceder a los router de CISCO hay que conocer primeramente la configuración de sus banners.

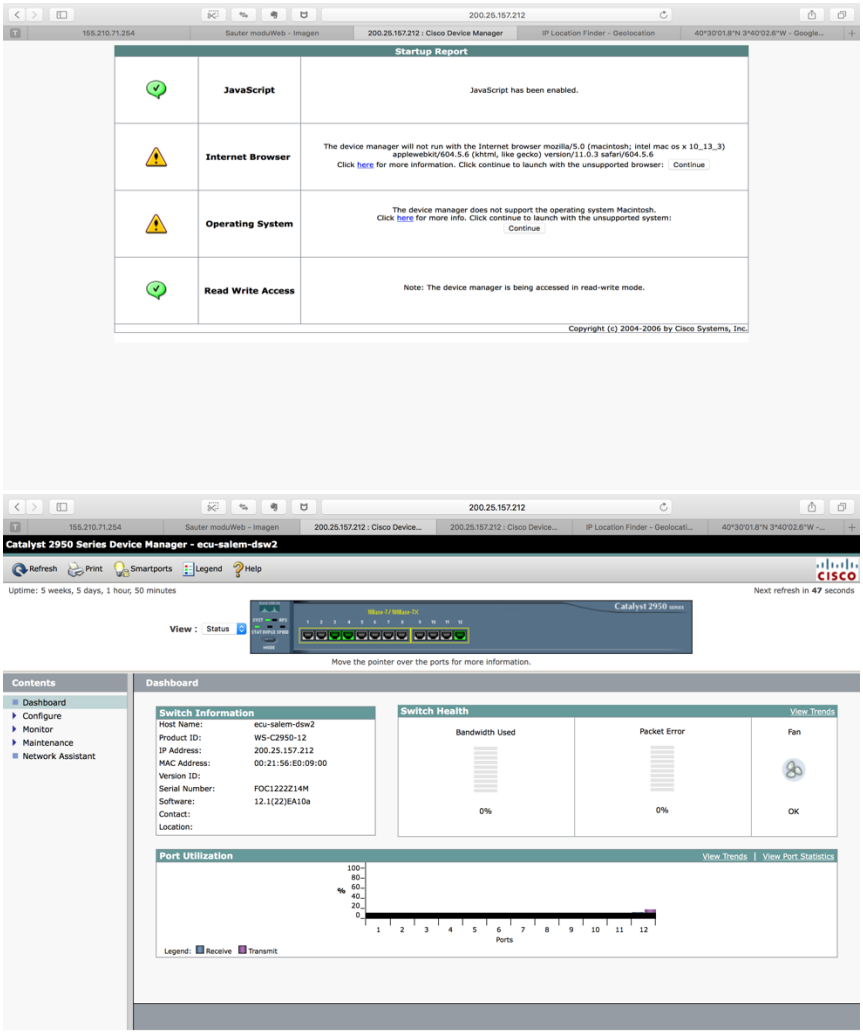
En el siguiente banner perteneciente a un router CISCO podemos ver que el código de estado HTTP es de tipo *401 Unauthorized*. Además si observamos la línea *Www-aunthenticate* ya nos está indicando que se nos requerirá un usuario y una password para logueado.

```
HTTP/1.0 401 Unauthorized
Date: Tue, 01 Dec 2009 16:09:46 GMT
Www-authenticate: Basic realm="level_15 or view_access"
Connection: close
Accept-ranges: none
Server: cisco-IOS
```

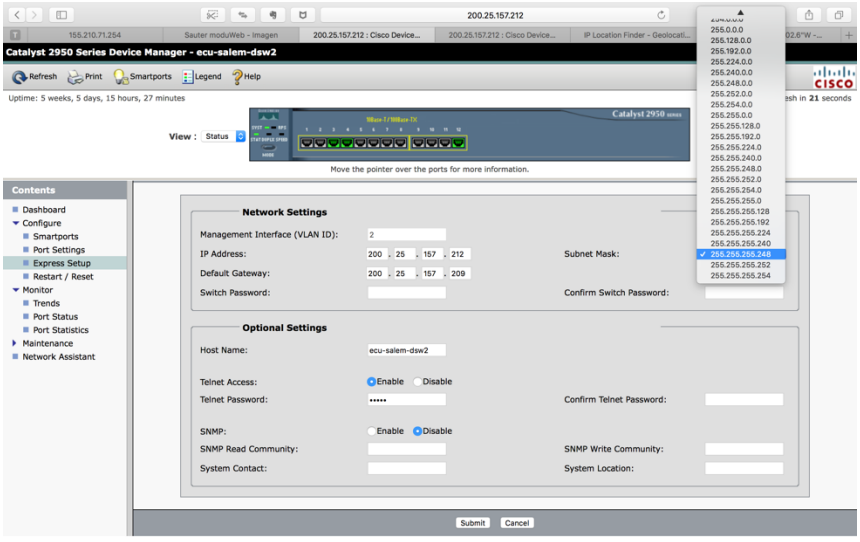
En este otro router de CISCO observamos que el cod. de estado indicado en el banner es *200 OK* y que la línea *Www-authenticate* es sustituida por la línea *'Last-modified: XXX..'*.Ello ya nos está indicando que posiblemente no se nos requiera acreditación para el acceso.

```
HTTP/1.0 200 OK
Transfer-encoding: chunked
Accept-ranges: none
Expires: Tue, 08 Jun 1993 06:55:45 GMT
Server: cisco-IOS
Last-modified: Tue, 08 Jun 1993 06:55:45 GMT
Connection: close
Cache-control: no-store, no-cache, must-revalidate
Date: Tue, 08 Jun 1993 06:55:45 GMT
Content-type: text/html
```

Para esta prueba se combinó palabras claves: Cisco-IOS, código de respuesta 200 OK y country:EC (Ecuador) para acotar la búsqueda a dispositivos router CISCO en ecuador con interfaz de acceso sin autentificación.




Como se puede apreciar dispongo de acceso a la configuración del router con privilegios de edición, lo que confirma el éxito del hacking al dispositivo.



## 7.6. BUSQUEDA DE SERVIDORES DE FTP

SHODAN nos puede servir para obtener las direcciones de IP a través de Servidores de FTP abiertos.

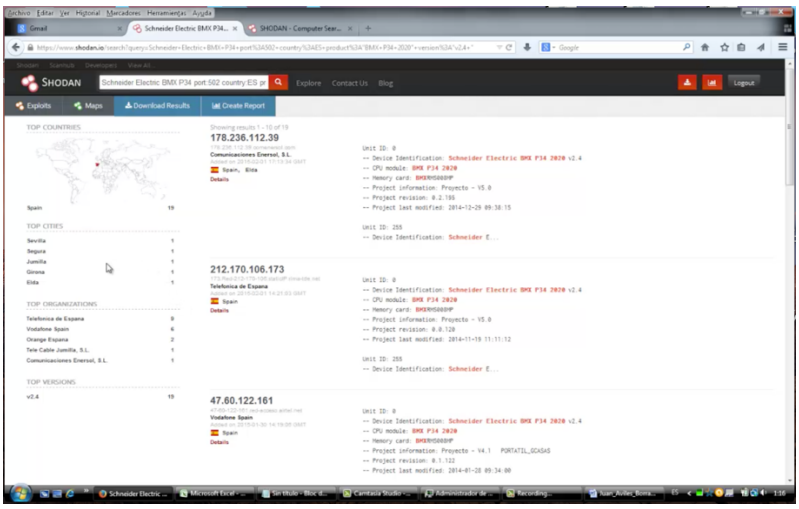
Para ello seleccionamos en campo de búsqueda aquellos nodos con el puerto FTP abierto (puertos:20, 21, 2121, etc.).

Algunas claves de búsqueda podrían ser: 'ftp server ready', 'ftp server ready anonymous@', 'port:21', etc.

A continuación apuntariamos en el navegador directamente a la dirección IP y al puerto 2121 (ftp//:213.97.84.23:2121) y accederíamos al directorio ftp de archivos.

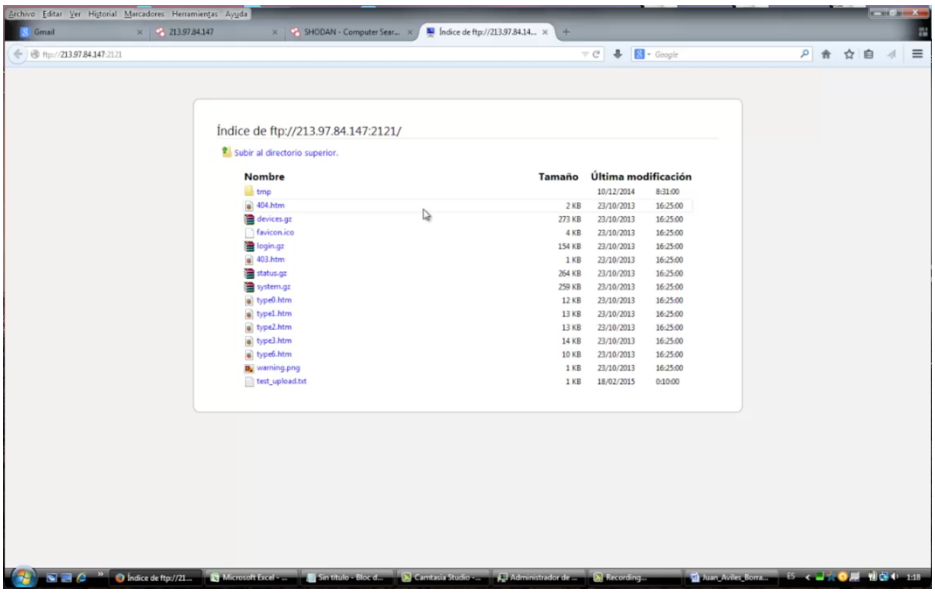
Vamos a ver un ejemplo accediendo al servidor ftp de un sistema SCADA de Schneider.

Inicialmente buscamos servidores del fabricante Schneider que emplean el protocolo Modbus, osea el puerto 502.




Vemos que uno de los dispositivos encontrados dispone del puerto ftp 2121 abierto y además no parece requerir autenticación pues en el banner aparece 'ftp server ready'.


Probamos suerte apuntando en el explorador a la dirección obtenida (ftp://213.97.84.147:2121) y vemos que nos da acceso directamente sin logueado previo.

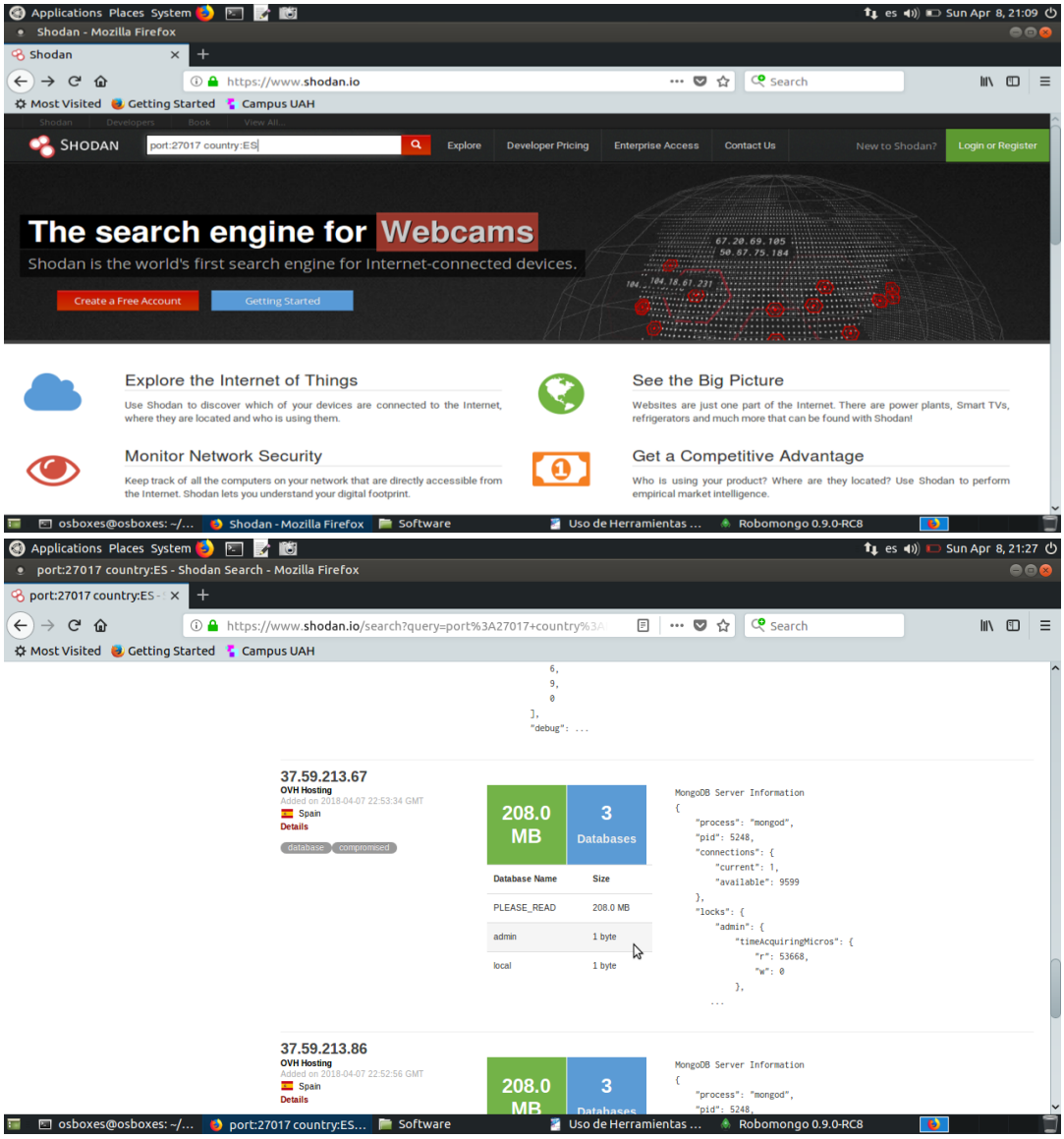



## 7.7. BUSQUEDA DE BASES DE DATOS MONGODB

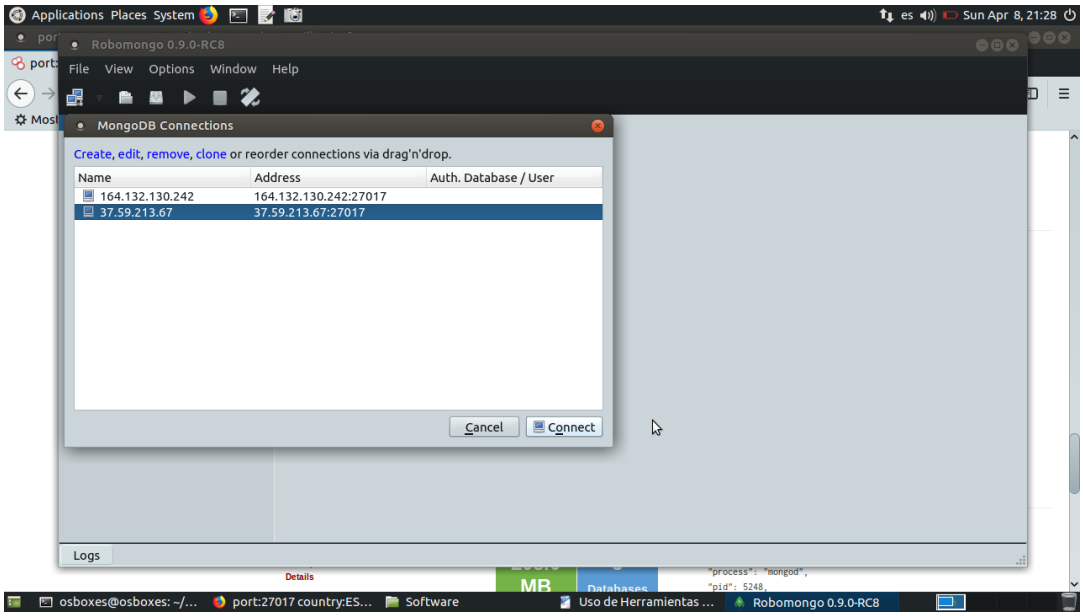
Para identificar servidores de bases de datos de tipo MongoDB estableceríamos como filtro de búsqueda el parámetro 'port: 27017'. Ello nos devolvería los nodos con el puerto 27017 abierto.

Una vez accedida a la Base de Datos Mongo DB podríamos tratar de extraer información valiosa, entre la que se encuentra la de los usuarios de la base de datos.

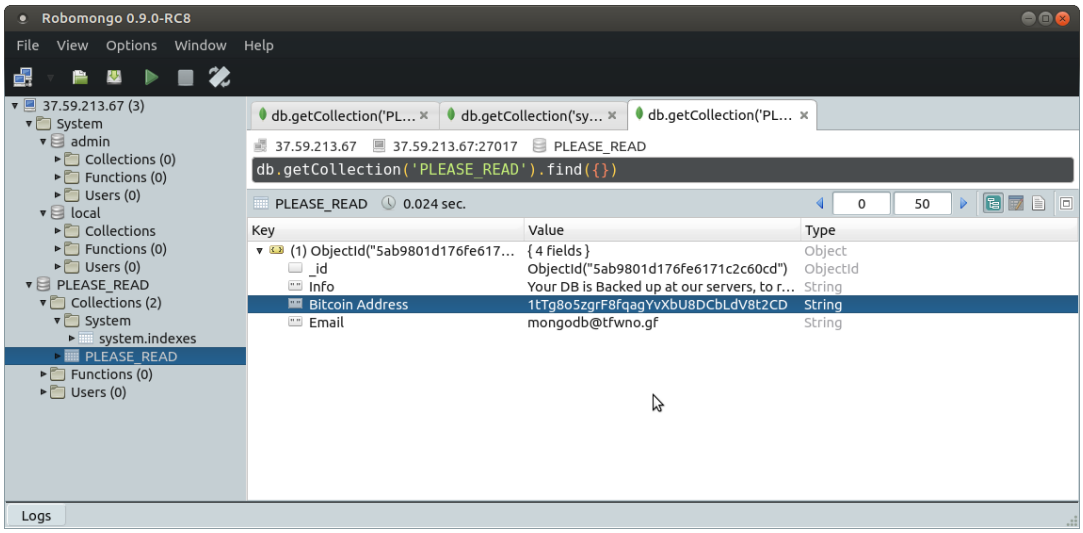
En primer lugar buscaremos Bases de Datos de tipo MongoDB en España filtrando por el puerto 27017 y seleccionaremos una cuya ultima actualización sea razonablemente reciente.




Probamos suerte con la BD seleccionada corriendo la aplicación Robomongo en una MV de Linux (Ubuntu Mate 16.04) y creando en ella una nueva BD con la IP seleccionada (37.59.213.67).




….y eureka! Conseguimos acceder a la citada BD de Robomongo. Fuimos surfeando por las diferentes carpetas y confirmando la total accesibilidad a los datos.



## 7.8. ACCESO A SERVICIOS DE CÁMARAS IP

SHODAN nos permite acceder a servicios de cámaras IP introduciendo en el campo de búsqueda comandos como p.ej 'ipcam' que nos devuelve el listado de nodos que disponen de un servicio de cámaras IP activo.

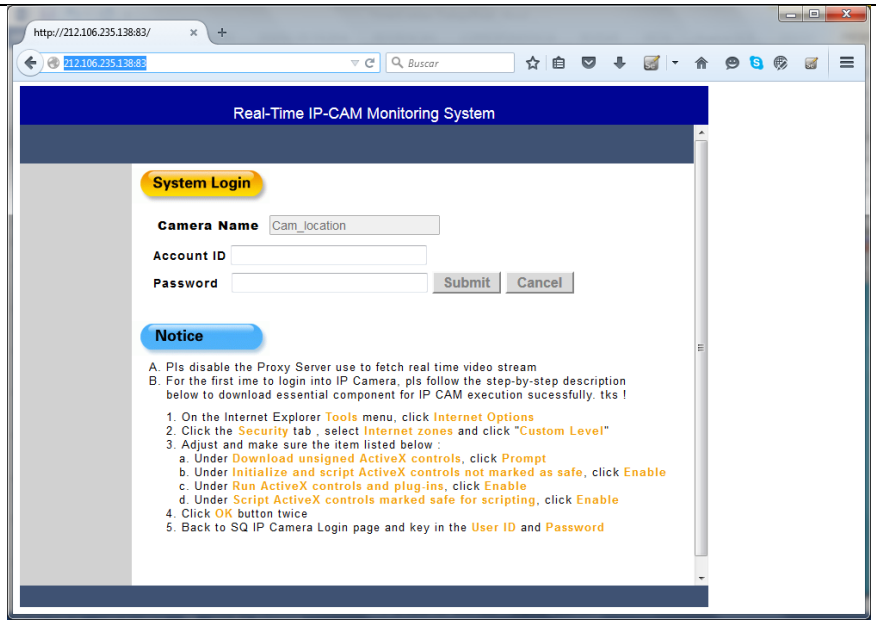
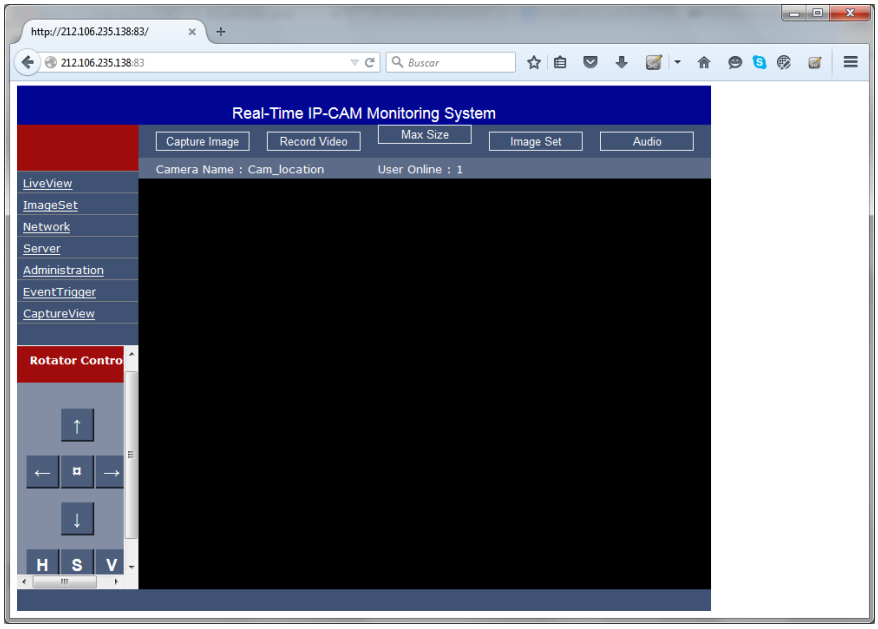
Una vez identificado el nodo de interés se puede intentar acceder mediante la ventana de logeado a través de las contraseñas por defecto de administrador. Para ello investigaríamos a través de la web sobre los valores por defecto de user/password de cada sistema de gestión de cámaras IP.

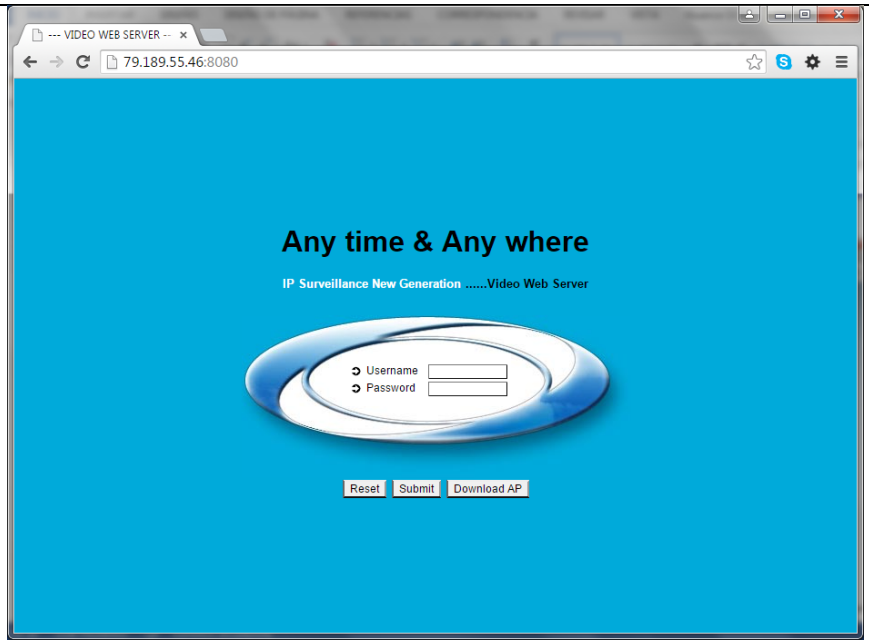
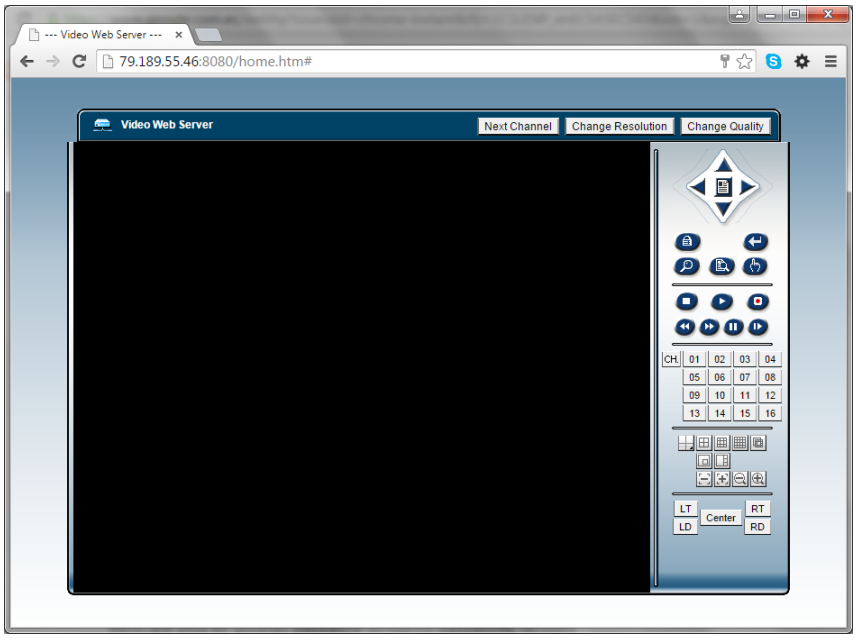
### Acceso a cámaras Web de seguridad genéricas

| | |
|---|---|
| Descripción | Cámaras de seguridad WEBCAM |
| Parámetros de búsqueda | Server: SQ-WEBCAM |
| # de resultados | 513 |
| Parámetros de acceso por defecto | Usuario: admin<br>Contraseña: admin / password |

*Hallazgos*

| | |
|---|---|
| IP: | 212.106.235.138 |
| Organización: | Jazz Telecom S.A. |
| Localización: | España |
| Puerto: | 83 |
| URL: | http:// 212.106.235.138:83 |
| Observación | Se puede acceder a un sistema de monitoreo en tiempo real de una cámara IP, pero no se puede visualizar nada, lo cual puede ser por que desconozco el funcionamiento del software y como activar la cámara o por qué falta algún plugin para su visualización. |

| | |
|---|---|
| Evidencias: |  <br>Usuario: admin - clave: password<br>  |
| | |
| IP: | 79.189.55.46 |
| Organización: | Orange Polska |
| Localización: | Solec Kujawski - Polonia |
| Puerto: | 8080 |
| URL: | http://79.189.55.46:8080/ |

| | |
|---|---|
| Observación | Se puede acceder a un sistema Video Web Server, pero no se puede visualizar nada, lo cual puede ser por que desconozco el funcionamiento del software y como activar la cámara o por qué falta algún plugin para su visualización. |
| Evidencias: |  <br>Usuario: admin - clave: admin<br>  |

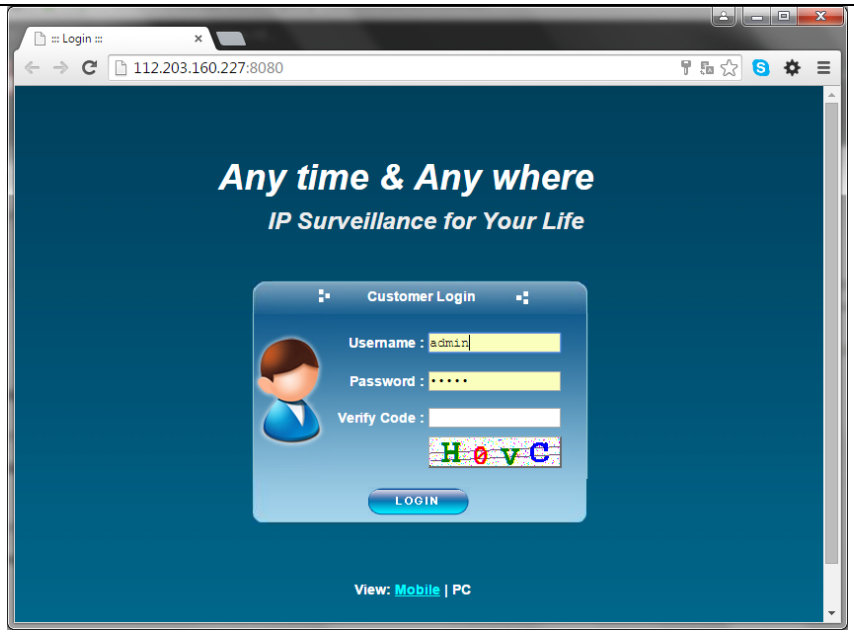
Se intentó hacer filtro para mi país Ecuador, pero no se obtuvo resultados.

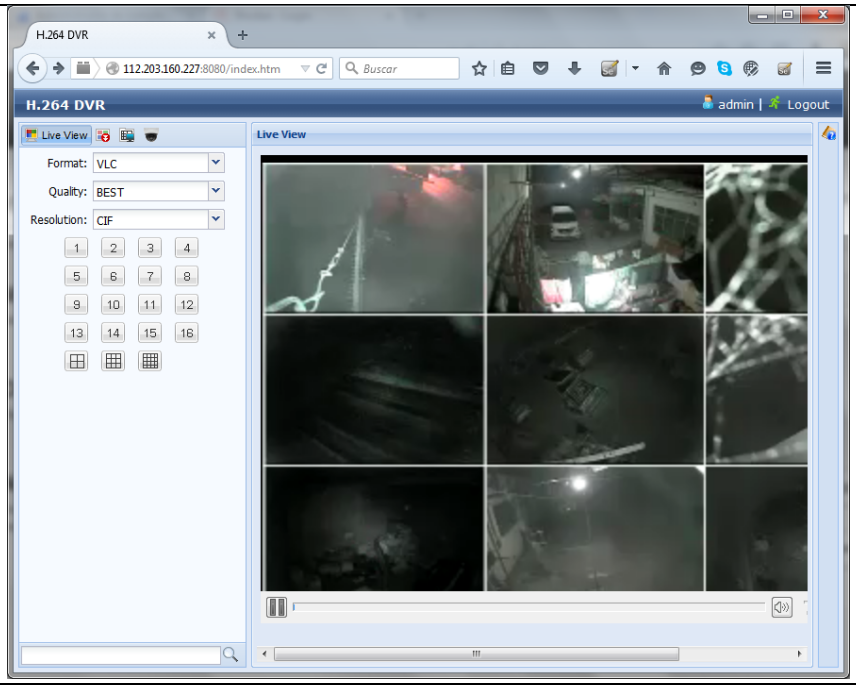
## Acceso a cámaras AvTech

| | |
|---|---|
| Descripción | Cámara Universal Plug and Play AvTech |

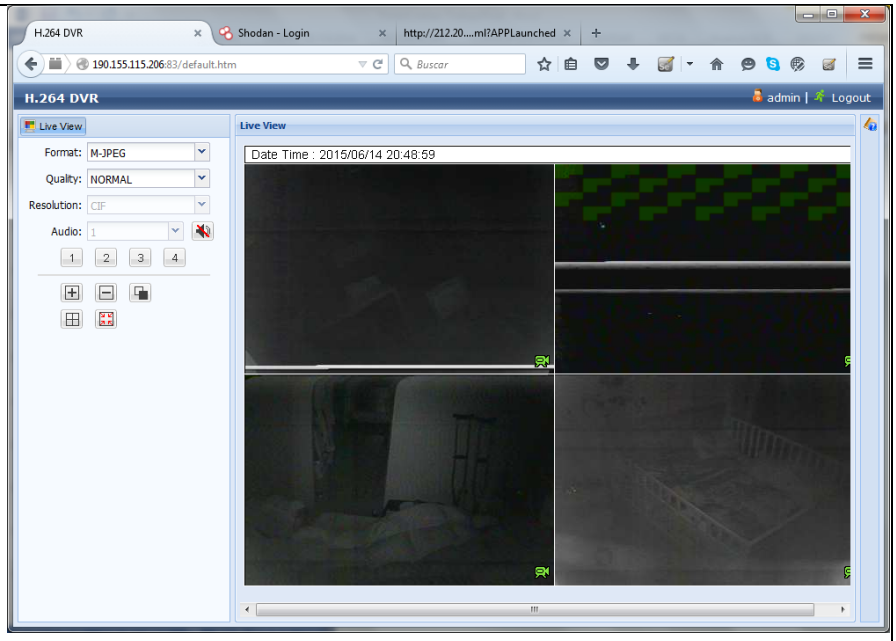
| | |
|---|---|
| Parámetros de búsqueda | linux upnp avtech |
| # de resultados | 154,959 |
| Procedimiento | De los resultados se toma aleatoriamente equipos y se hace clic sobre el URL del mismo, al ver que corresponde a un acceso web con usuario y clave, buscamos en internet los parámetros de acceso por defecto, partiendo de información del formulario de login, por ejemplo "Any time & Any where" http://kontech-blog.blogspot.com/2011/05/any-time-any-where-ip-surveillance-for.html Y probamos el acceso. |
| Parámetros de acceso por defecto | Usuario: admin<br>Contraseña: admin |

*Hallazgos*

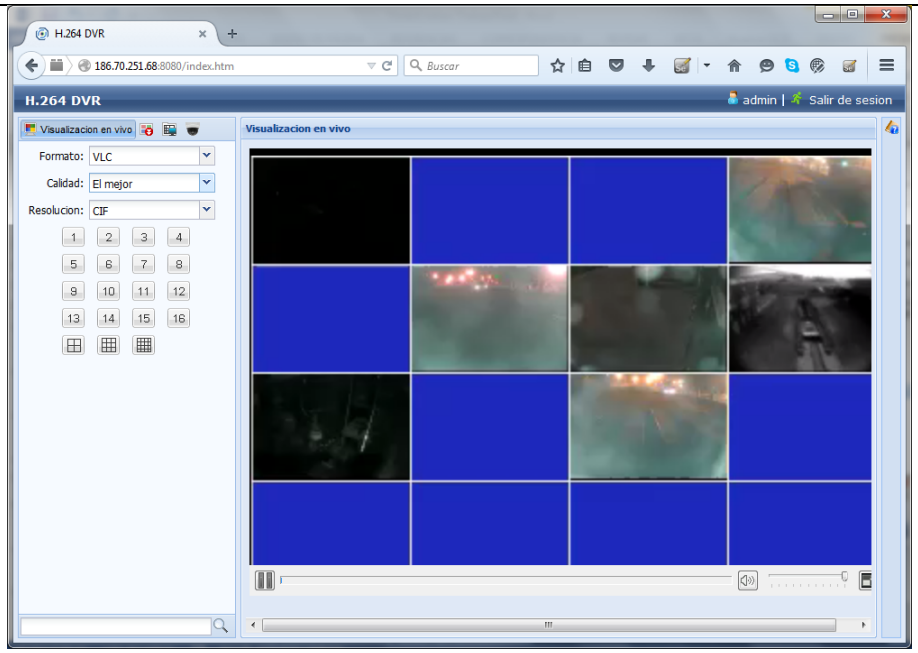
| | |
|---|---|
| IP: | 112.203.160.227 |
| Organización: | Philippine Long Distance Telephone |
| Localización: | Philippines |
| Puerto: | 8080 |
| URL: | http://112.203.160.227:8080 |
| Observación | Se puede acceder a un sistema DVR el cual presenta 9 cámaras de monitoreo. |
| Evidencias: |  |

| | |
|---|---|
| |  |

| | |
|---|---|
| IP: | 190.155.115.206 |
| Organización : | Satnet |
| Localización: | Guayaquil - Ecuador |
| Puerto: | 83 |
| URL: | http://190.155.115.206:83 |
| Observación | Para este hallazgo se hizo una variación en el filtro de búsqueda, ahora para buscar equipos con estas vulnerabilidades pero de mi país:<br>Parámetros: linux upnp avtech country:EC<br>URL: https://www.shodan.io/search?query=linux+upnp+avtech+country%3AEC<br># de resultados: 199<br><br>Se puede acceder a un sistema DVR el cual presenta 4 cámaras de monitoreo. |

| | |
|---|---|
| Evidencias: |  |

| | |
|---|---|
| IP: | 186.70.251.68 |
| Organización: | Satnet, al parecer esta empresa es la que proveer internet a domicilios por lo que presumo que es de una persona natural o empresa pequeña razón por la de su poca seguridad |
| Localización: | Cuenca - Ecuador |
| Puerto: | 8080 |
| URL: | http://186.70.251.68:8080 |
| Observación | Para este hallazgo se hizo una variación en el filtro de búsqueda, ahora para buscar equipos con estas vulnerabilidades de mi país y de mi ciudad:<br>Parámetros: linux upnp avtech country:EC city:Cuenca<br>URL:<br>https://www.shodan.io/search?query=linux+upnp+avtech+country%3AEC+city%3ACuenca<br># de resultados: 12<br><br>Se puede acceder a un sistema DVR el cual presenta 7 cámaras de monitoreo. |

| | |
|---|---|
| Evidencias: |  |

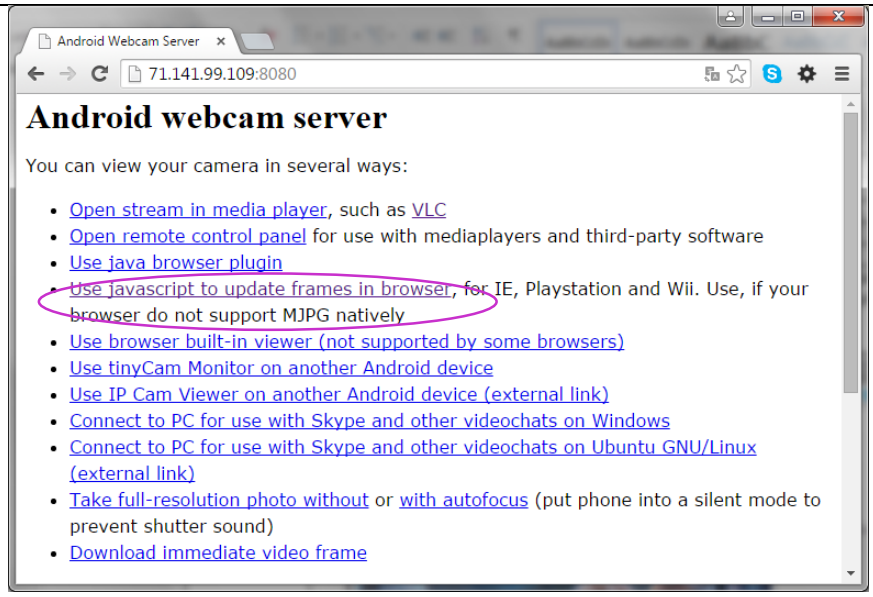
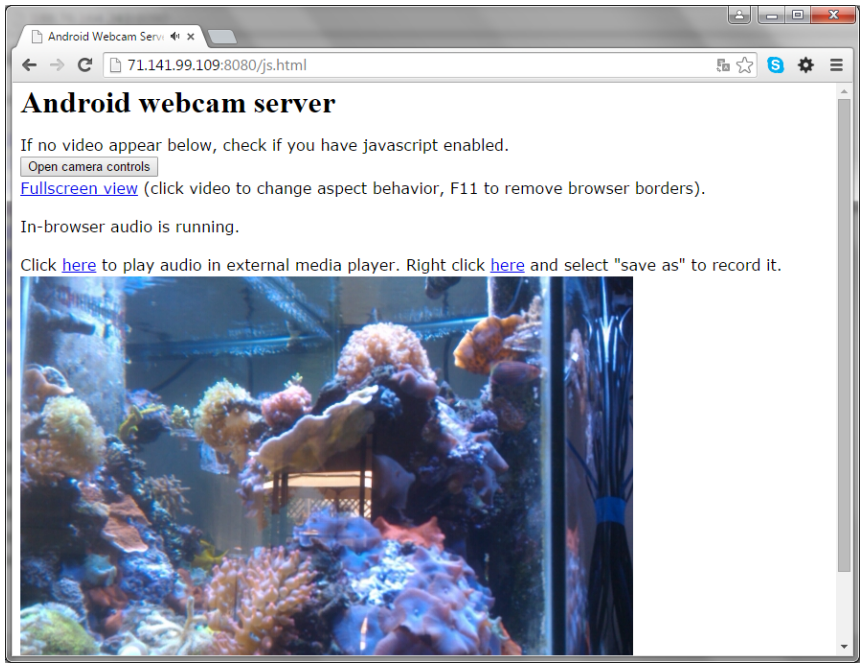
## Acceso a WebCams Android sin autentificación

En este caso no se aplicó un filtro adicional por la poca cantidad de resultados.

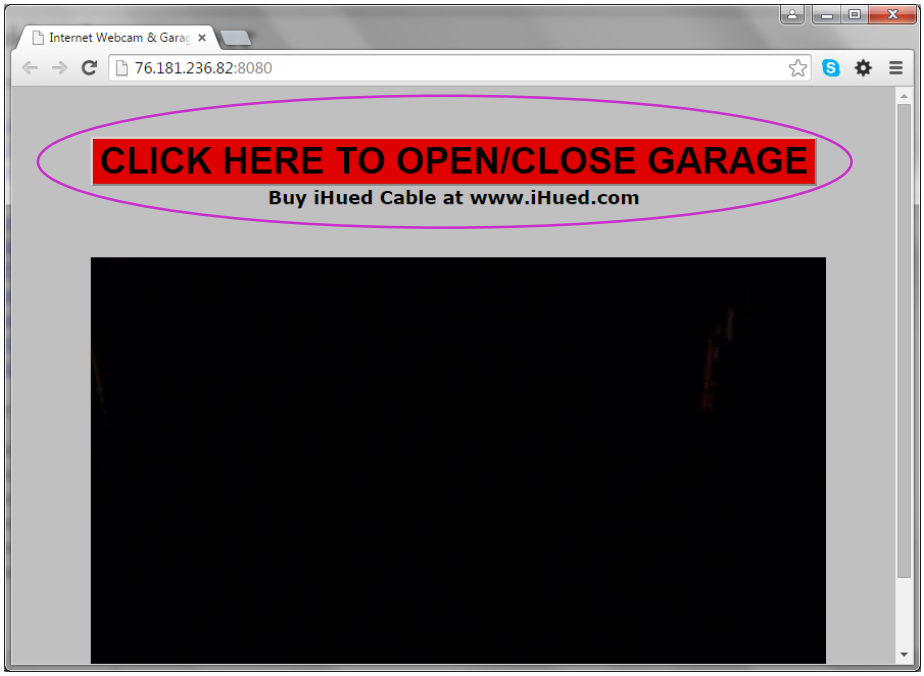
| | |
|---|---|
| Descripción | WebCams Android |
| Parámetros de búsqueda | Android Webcam Server –Authenticate https://www.shodan.io/search?query=Android+Webcam+Server+-Authenticate |
| # de resultados | 61 |
| Procedimiento | En este caso de consulta de Shodan se puede destacar la aparición del símbolo "-", el cual nos permite quitar algo de la búsqueda, la consulta buscaría algo con coincidencia a un parámetro pero así también que dentro de esos resultados no se incluya los que tengan el parámetro negado ("-") |
| Parámetros de acceso por defecto | No hay autenticación |

### *Hallazgos*

| | |
|---|---|
| IP: | 71.141.99.109 |
| Organización: | AT&T Internet Services |
| Localización: | Foster – Estados Unidos |
| Puerto: | 8080 (http) |
| URL: | http:// 71.141.99.109:8080/ |
| Observación | Sin necesidad de claves, se obtiene acceso a la interfaz de monitoreo de la cámara. En la cual existen varias formas poder monitorear, pero se depende de un plugin, por lo que hemos usado el que es dependiente de JavaScript |

| | |
|---|---|
| Evidencias: |  <br>  <br>En tipo de webcams también captura audio. El resultado presentado apuntaba a una pecera, pero cuando se activó el audio se empezó a escuchar una conversación, por lo que inmediatamente salimos de la interfaz. |

| | |
|---|---|
| IP: | 76.181.236.82 |
| Organización: | Time Warner Cable |
| Localización: | Colombus – Estados Unidos |
| Puerto: | 8080 (http) |
| URL: | http://76.181.236.82:8080/ |

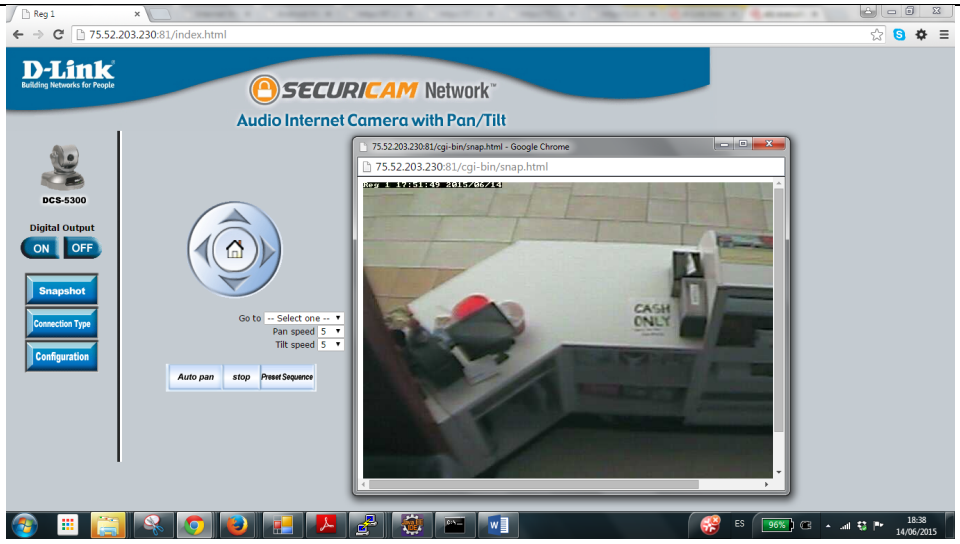
| | |
|---|---|
| Observación | Sin necesidad de claves, se obtiene acceso a la interfaz de monitoreo de una cámara y también una funcionalidad que permite abrir o cerrar la puerta de un garaje (lo cual no se probó). |
| Evidencias: |  |

## Acceso a Cámaras D-link sin autenticación

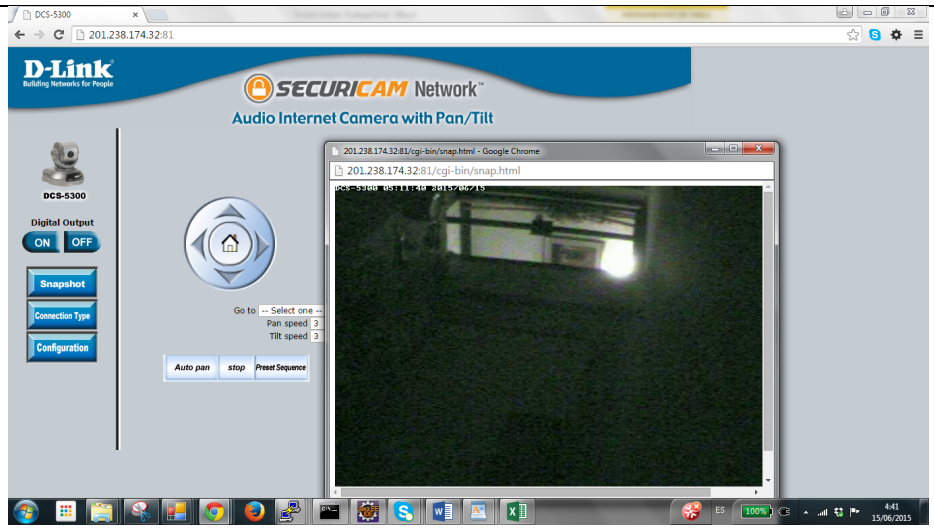
| | |
|---|---|
| Descripción | Cámaras D-Link |
| Parámetros de búsqueda | d-Link Internet Camera, 200 OK<br>https://www.shodan.io/search?query=d-Link+Internet+Camera%2C+200+OK |
| # de resultados | 61 |
| Procedimiento | El acceso se lo hacer sin credenciales, como se puede ver en los parámetros se busca que en las solicitudes el sistema haya respondido con un código 200 de conexión satisfactoria |
| Parámetros de acceso por defecto | No hay autenticación |

### *Hallazgos*

| | |
|---|---|
| IP: | 75.52.203.230 |
| Organización: | AT&T Internet Services |
| Localización: | Estados Unidos |
| Puerto: | 81 (http) |
| URL: | http://75.52.203.230:8080 |

| | |
|---|---|
| Observación | Sin necesidad de claves, se obtienen acceso a la interfaz de control y configuración de la cámara, de la cual para evidencia se obtiene únicamente un snapshot, esto por razones de ética profesional. |
| Evidencias: |  |

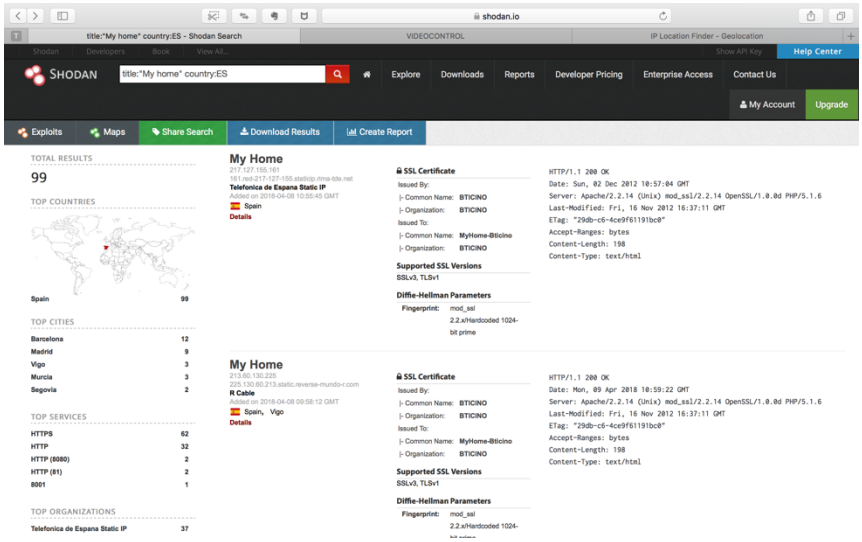
Posterior analizamos añadiendo un filtro destinado a obtener resultados de Ecuador, y obtenemos un solo resultado, el cual nos sorprende pues es de la Empresa Municipal de Telefonía, Agua Potable y Alcantarillado.

| | |
|---|---|
| IP: | 201.238.174.32 |
| Organización: | ETAPA EP |
| Localización: | Cuenca - Ecuador |
| Puerto: | 81 (http) |
| URL: | http://201.238.174.32:81 |
| Observación | Sin necesidad de claves, se obtienen acceso a la interfaz de control y configuración de la cámara, de la cual para evidencia se obtiene únicamente un snapshot, esto por razones de ética profesional. |
| Evidencias: |  |

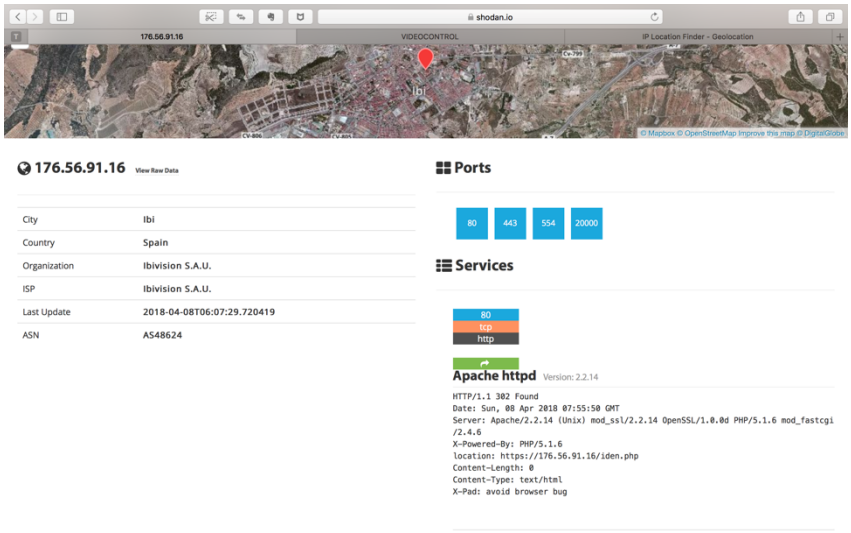
## 7.9. ACCESO A SERVICIOS DE DOMÓTICA

SHODAN nos permite acceder a servicios de Gestion de Domótica via Web introduciendo en el campo de búsqueda comandos como p.ej 'Myhome' que nos devuelve el listado de nodos que disponen de un servicio de domótica doméstico.

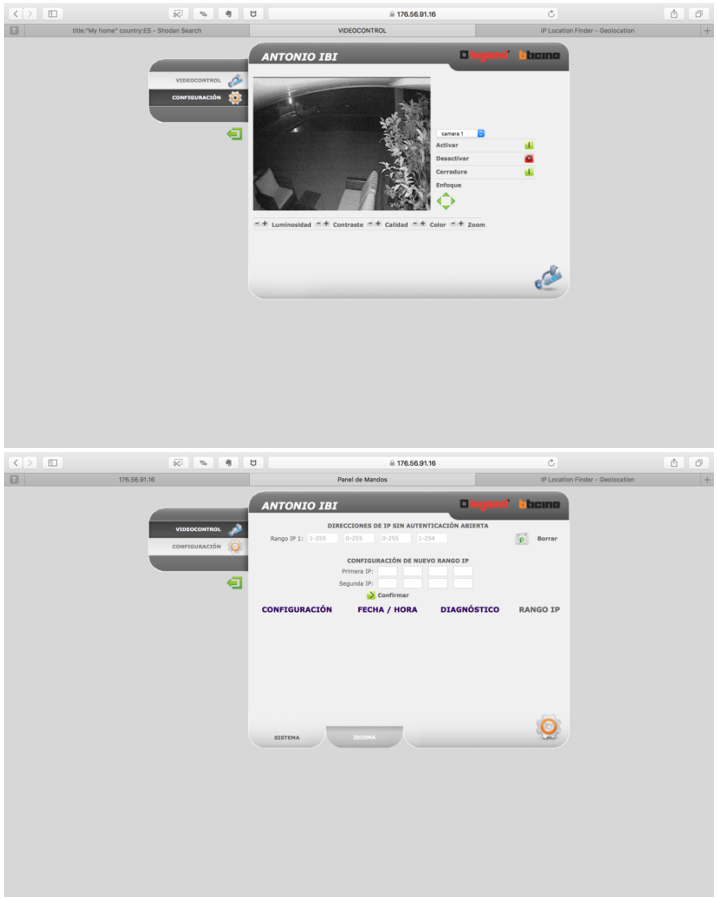
Buscamos con SHODAN sistemas de Domótica en el territorio español mediante la combinación de filtros 'Title:"My home" country:ES'




Una vez identificado el nodo de interés intentamos acceder al sistema logándonos con las claves por defecto 'User:admin password:admin' y eureka!, conseguimos acceso.




Vemos como hemos obtenido acceso al sistema y podemos visualizar las cámaras CCTV y reconfigurar el sistema.




## 7.10. BUSQUEDAS AUTOMÁTICAS CON SELENIUM-JAVA

### 7.10.1. Análisis automático de conexiones TELNET

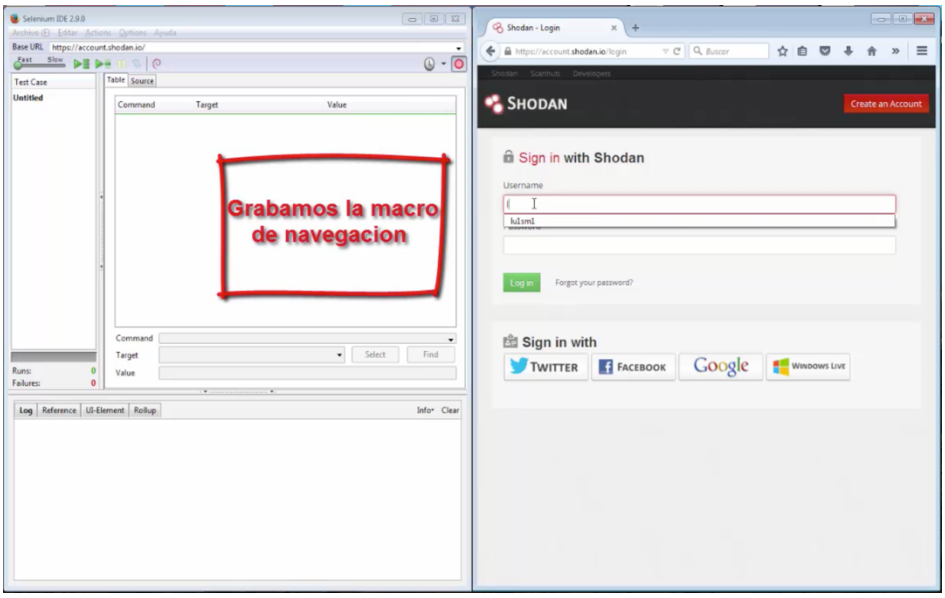
Este método está basado en la exploración del DOM HTML. Se propone y valida un método para chequear el acceso de forma automática de conexiones TELNET vulnerables que han sido previamente identificadad por SHODAN.

El método se basa en procesar el response de la solicitud HTTP hecha sobre el servidor Shodan cuando le pedimos que nos devuelva todos los servidores TELNET vulnerables por medio de la API Java JSoup (Java HTML Parser) que permita procesar un documento HTML a través de su DOM. El código Java es generado automáticamente con la aplicación Selenium IDE. Los resultados con las direcciones IPs obtenidas son archivados en varios ficheros y posteriormente con la ayuda de la herramienta de test de conexiones TELNET (TYFYP) son chequeadas todas ellas de forma automática determinándose asi las que están activas.

Los pasos del proceso serían los siguientes:

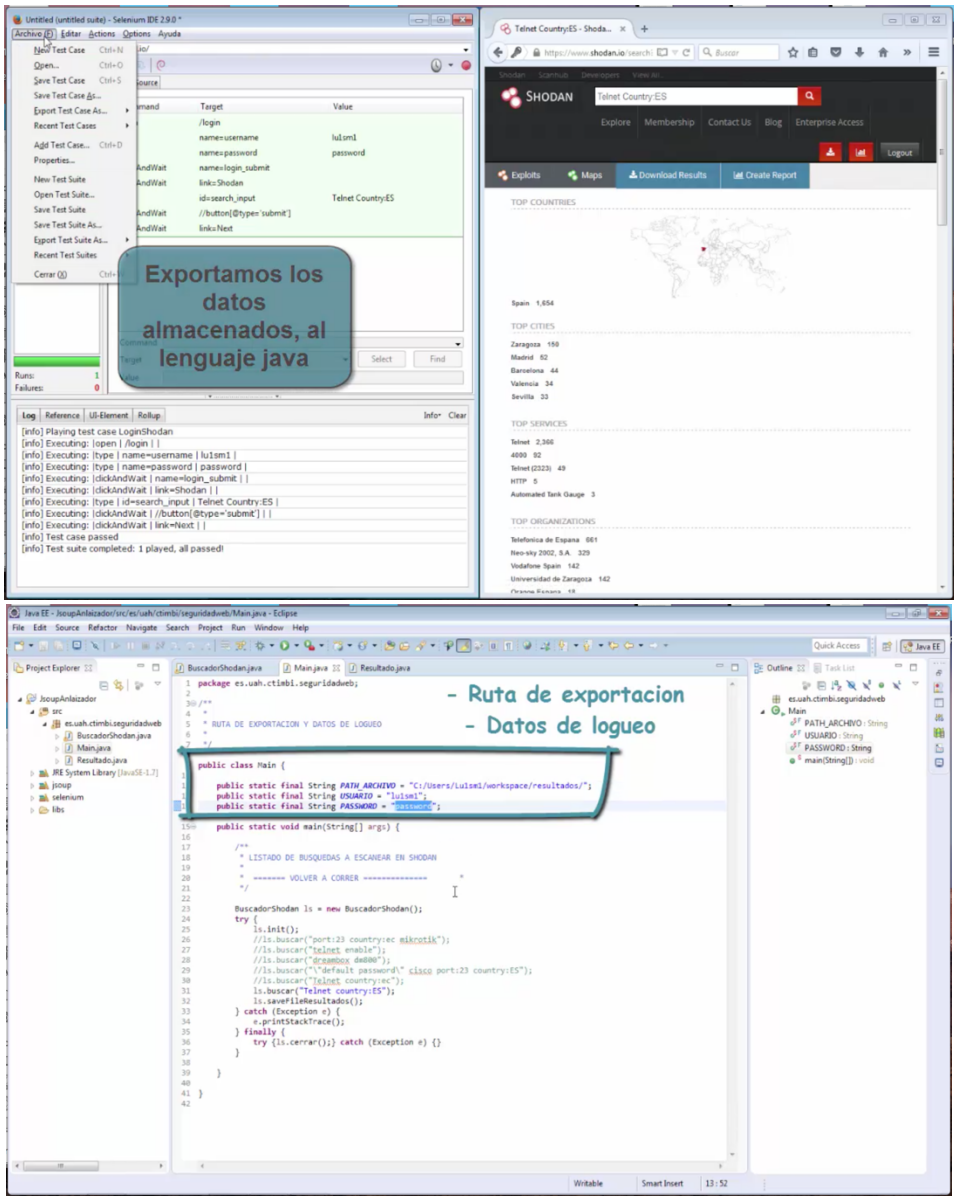
### *Paso 1. Grabar macro de navegación*

Mediante la herramienta Selenium IDE, que se ejecuta como complemento del Navegador, grabamos un macro de la navegación que deseamos (logueado y términos de búsqueda), la cual va a ir grabando cada uno de los pasos que se hacen sobre el navegador, para luego exportarlo a código fuente Java para posteriormente desarrollar la funcionalidad deseada




### *Paso 2. Generar código fuente para lenguaje Java*

Desde el mismo Selenium IDE podemos exportar el macro grabado previamente a lenguaje de programación Java mediante la opción ‘export to Java/Junit4’




*Paso 3. Adaptar código fuente a necesidades para recuperar el código HTML de las páginas de resultados*

Básicamernte se modifica el Java para que pueda capturar todas las páginas de resultados (Shodan version free solo da acceos a las 5 primeras páginas).

```java
/**
 *
 * AQUI ADAPTAMOS EL JAVA CREADO CON SELENEIUM IDE
 * PARA QUE HAGA LAS BUSQUEDAS INTRODUCIDAS EN MAIN()
 *
 */

public List<Resultado> buscar(String params) throws Exception {
    this.params = params;

  driver.get(baseUrl + "/login");
  driver.findElement(By.name("username")).clear();
  driver.findElement(By.name("username")).sendKeys(Main.USUARIO);
  driver.findElement(By.name("password")).clear();
  driver.findElement(By.name("password")).sendKeys(Main.PASSWORD);
  driver.findElement(By.name("login_submit")).click();
  driver.get("https://www.shodan.io/search?query="+params);

  String html = driver.getPageSource();
  int numeroPaginas = getNumeroResultados(html)/10;
  if(numeroPaginas>5)     //número máximo de resultados
      numeroPaginas=5;
  for(int i=0; i<numeroPaginas; i++){
      leerDOM(html);
      try{
          driver.findElement(By.linkText("Next")).click();
          html = driver.getPageSource();
      }catch(Exception e){}
  }

  return resultados;
}
```

Codigo java, exportado mediante Selenium IDE...

Modificado para poder capturar todas las paginas de resultados

### *Paso 4. Procesar DOM HTML con Jsoup*

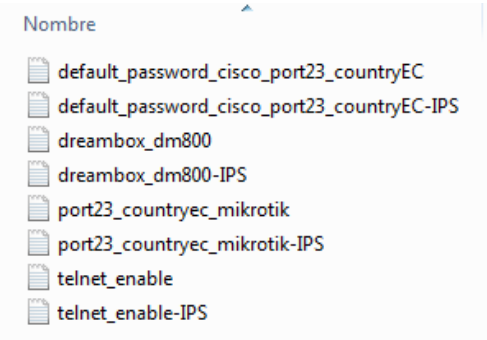
Partiendo del código HTML obtenido con Selenium parseamos el archivo XML y mediante la exploración del DOM vamos creando objetos que registren la IP y demás datos (host, organización, banner).

```java
        System.out.println("Resultados" + numeroResultados);
        return Integer.parseInt(numeroResultados);

    }

/**
 *
 * USAMOS JSOUP PARA PARSEAR EL ARCHIVO XML DEVUELTO
 * POR EL WEB SERVICES DE SHODAN
 *
 */

public void leerDOM(String html){
      Document doc = Jsoup.parse(html);

      String numeroResultados = doc.getElementsByClass("results-count").first().text();

      Elements resultados = doc.getElementsByClass("search-result");
      for (Element resultado : resultados) {
          Resultado server = new Resultado();
          server.setIp(resultado.getElementsByClass("ip").first().text());
          server.setTexto(resultado.getElementsByClass("search-result-summary").first().text());
          this.resultados.add(server);
      }
}
/**
 *
 * EXPORTAMOS LOS DATOS OBTENIDOS A DOS FICHERO DE TEXTO
 * UNA VERSION CON LA INFORMACION DETALLADA
 * OTRA VERSION CON DIRECCION IP PARA PROBAR CREDENCIALES
 *
```

Parseamos el documento devuelto mediante jsoup

### *Paso 5. Guardar resultados en Archivo*

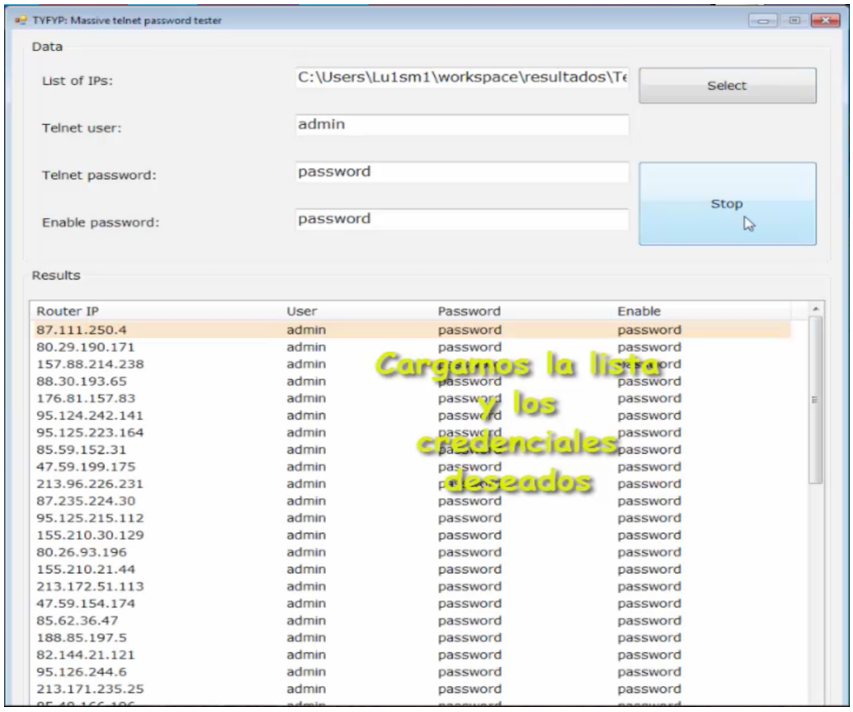
Posteriormente se crean dos archivos; uno para todos los datos obtenidos de detalle (IP y datos), y un segundo archivo solo con las IPS, IPS que luego serán usadas para automatizar los test de conexión por clientes determinados.



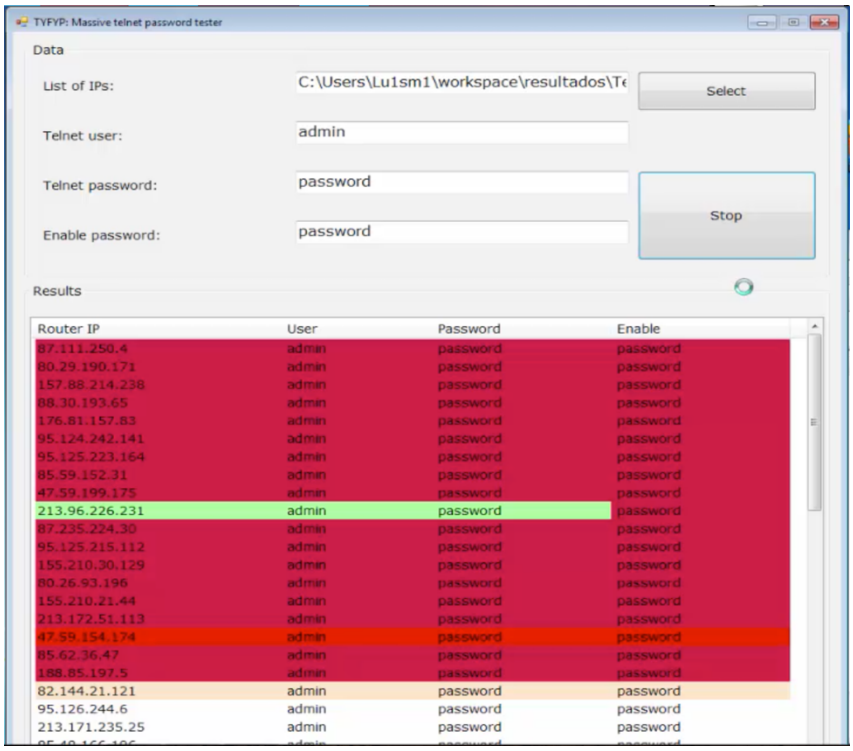

*Paso 6. Automatización del Test de conexión TELNET*

Con el fin de automatizar los test de conexión para un gran conjunto de equipos, se utilizó la aplicación [TYFYP-telnet-password-tester](), la cual parte de un archivo plano de direcciones IP de equipos a testear y el usuario y clave (en este caso genéricas) con el que validar el acceso.

En la primera pantalla de la aplicación cargamos el Archivo de lista de IPs, usuario y clave a testear (genéricas), y una segunda clave usada para probar el comando enable en routers




Una vez que corre el programa, va testeando todas las conexiones por telnet con las credenciales indicadas, y de ser conexión satisfactoria marca el registro con color verde.


TYFYP: Massive telnet password tester
Data
List of IPs:
C:\Users\Lu1sm1\workspace\resultados\Te
Select
Telnet user:
admin
Telnet password:
password
Enable password:
password
Stop
Results
Router IP
User
Password
Enable
87.111.250.4 admin password password
80.29.190.171 admin password password
157.88.214.238 admin password password
88.30.193.65 admin password password
176.81.157.83 admin password password
95.124.242.141 admin password password
95.125.223.164 admin password password
85.59.152.31 admin password password
47.59.199.175 admin password password
213.96.226.231 admin password password
87.235.224.30 admin password password
95.125.215.112 admin password password
155.210.30.129 admin password password
80.26.93.196 admin password password
155.210.21.44 admin password password
213.172.51.113 admin password password
47.59.154.174 admin password password
85.62.36.47 admin password password
188.85.197.5 admin password password
82.144.21.121 admin password password
95.126.244.6 admin password password
213.171.235.25 admin password password

# 8. TOOLBOX PARA HACKING DE SCADA CON SHODAN

En el presente apartado se identifican y caracterizan un conjunto de herramientas e información que, empleadas de forma combinada con Shodan permiten hacer una explotación avanzada de los resultados ofrecidos por Shodan, permitiendo la automatización de búsquedas y del reporting.
Esta suite de herramientas (Toolbox) recoge todos aquellos elementos necesarios para optimizar el proceso de Auditoria de Pentesting de sistemas SCADA, estando compuesta por:

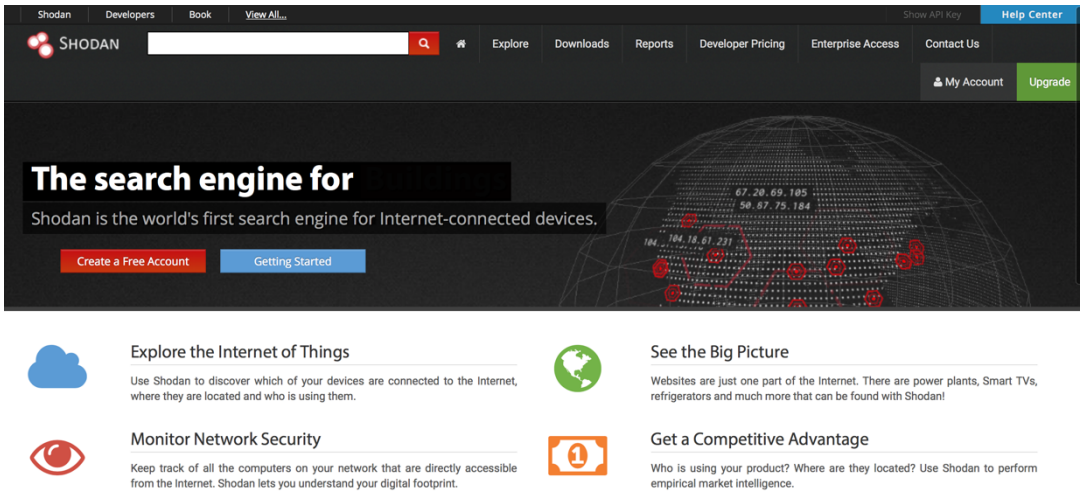
- Aplicaciones SW: APIs, Bases de Datos, etc.
- Información técnica: Links, Filtros shodan, Puertos SCADA, etc.
- Normativa aplicable y guías: ANSI/ISA99, CCN-STIC-480, IEC, IEEE, NERC, NIST SP-800, etc.

## 8.1. HERRAMIENTAS SW

### 8.1.1. SHODAN

Link: https://www.shodan.io

Esta aplicación es descrita en detalle en el apartado 5.3. 'SHODAN. Principios y funcionalidades'.



### 8.1.2. APIs y Plug-ins

Con el objeto de poder hacer un uso avanzado de las funcionalidades de Shodan existen las dos siguientes familias de APIs que pueden ser empleadas en un gran numero de lenguajes diversos de programación:

#### APIs REST

**API REST** proporciona métodos para hacer búsquedas avanzadas en Shodan, búsqueda de hosts, obtención de información resumida de consultas asi como una variedad de métodos de utilidad para hacer más fácil el desarrollo.

#### APIs Streaming

**API de Streaming** proporciona los datos en bruto en tiempo real que están siendo recogidos por shodan. Existen varias fuentes de datos en bruto a las que subscribirse, pero no es posible hacer búsquedas sobre dichos datos en tiempo real ya que se trata de una transmisión en vivo de un gran volumen de datos para aplicaciones de consumo de una cantidad ingente de datos.

La API de Streaming es un servicio basado en HTTP que devuelve una secuencia en tiempo real de los datos recogidos por Shodan. El feed devuelve la información como una cadena JSON codificados utilizando 2 formatos de salida distintos.

#### Librerias de entornos de programación

Existe un conjunto de librerías para los lenguajes de programación mas extendidos al objeto de facilitar el acceso a las APIs de Shodan.

Actualmente existen librerías disponibles para los siguientes entornos de programación:

- Python
- Ruby
- PHP
- C#
- Go
- Haskell
- Java
- Node.js
- Perl
- Powershell
- Rust

### Plug-ins de SHODAN

Con el objeto de poder acceder directamente a la funcionalidad de shodan desde los exploradores o aplicaciones mas habituales existen un conjunto de plug-ins.

Los pluggins mas relevantes actualmente están disponibles son para:

- Chrome
- Mozilla
- Maltego
- Metasploit
- Recon-ng

El Plug-in de Shodan te dice, entre otros, dónde está alojado el sitio web (país, ciudad), a quién pertenece el IP y qué otros servicios / puertos están abiertos.

El complemento de Shodan para Chrome o Mozilla comprueba automáticamente si Shodan tiene información para el sitio web actual (ejecución de servicios FTP, DNS, SSH o algún servicio inusual). Con este complemento puedes ver toda la información que Shodan ha recopilado en un determinado sitio web / dominio.

## 8.1.3. Buscadores de Información en la Web (Surface web)

### Google DORKS

Google es el motor de búsqueda más popular. Posee una gran variedad de comandos que hacen que nuestra búsqueda sea más fácil y eficaz para obtener información sobre un objetivo u organización, Google puede ayudar a descubrir y obtener datos sensibles sin que el objetivo en cuestión registre un solo paquete enviado desde nuestra dirección.

Para ello Google Dorks dispone de una extensa familia de filtros que nos permite orientas o restringir las búsquedas. Los mas importantes son los siguientes:

*Consultas Básicas*

- Consultas de palabras
- Consultas de Frases
- Operadores Buleanos (AND, OR, NOT)
- Caracteres especiales

| Operators | Description |
|---|---|
| - | Inverse search operator (hide results) |
| ~ | synonyms |
| [#]..[#] | Number range |
| * | Wildcard to put something between something when searching with "quotes" |
| + | Used to force stop words |
| OR | Boolean operator, must be uppercase |
| \| | Same as OR |
| | |

*Consultas Avanzadas*

| Filtro | Descripción | Ejemplo |
|---|---|---|
| site | Consultar palabras clave en dominio particular. | "exploits site:hackingspirits.com" |
| allinurl | Páginas que tengan el término en la URL. | allinurl: passwd.txt |
| inurl | Páginas que contienen una palabra en el título. | intitle: login password |
| filetype | Busca archivos con extensión. pdf, doc, .xls... | filetype:xls password site:.mil |
| index of | Búsqueda de directorios en la web. | "index of /admin" |
| allintitle | Búsqueda dentro del título de la web. | allintitle: "index of/admin" |
| intitle | Búsqueda webs que contienen ese término. | intitle: "index of" "Termino" |
| cache | Buscar páginas o textos eliminados. | cache:www.elhost.com/pass.txt |
| link | Páginas que tengan un enlace a cierta web. | |
| related | Páginas relacionadas con una página. | |
| info | Información en google de la página de inicio | |

Según el tipo de búsqueda a realizar se pueden emplear las combinaciones de términos siguientes:

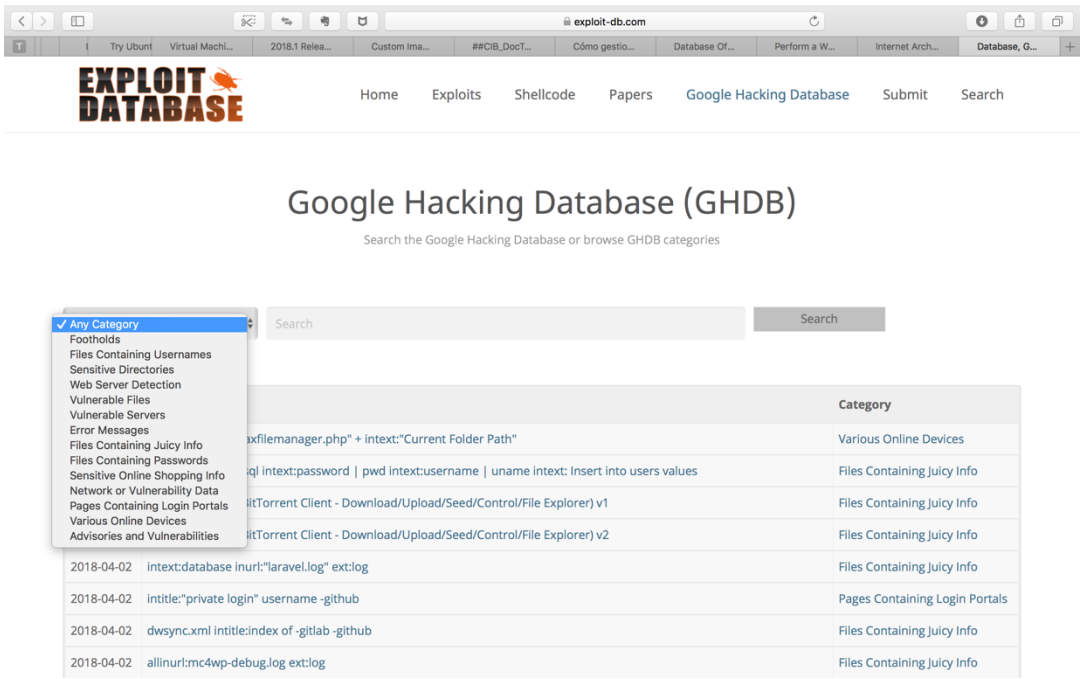
| Search Service | Search Operators |
|---|---|
| Web Search | allinanchor:, allintext:, allintitle:, allinurl:, cache:, define:, filetype:, id:, inanchor:, info:, intext:, intitle:, inurl:, link:, related:, site: |
| Image Search | allintitle:, allinurl:, filetype:, inurl:, intitle:, site: |
| Groups | allintext:, allintitle:, author:, group:, insubject:, intext:, intitle: |
| Directory | allintext:, allintitle:, allinurl:, ext:, filetype:, intext:, intitle:, inurl: |
| News | allintext:, allintitle:, allinurl:, intext:, intitle:, inurl:, location:, source: |
| Product Search | allintext:, allintitle: |

## Google Hacking Data Base (GHDB)

Link: https://www.exploit-db.com/google-hacking-database/

La base de datos "Google Hacking Database" (GHDB) de Johnny Long, recopila búsquedas especiales para Google. Permite encontrar mucha información filtrada en internet, sobre una determinada web o sobre un objetivo concreto (como una persona o una organización).

El proyecto fue creado hace algunos años por Johnny Long y luego ha sido continuado por el equipo de exploit-db.com.



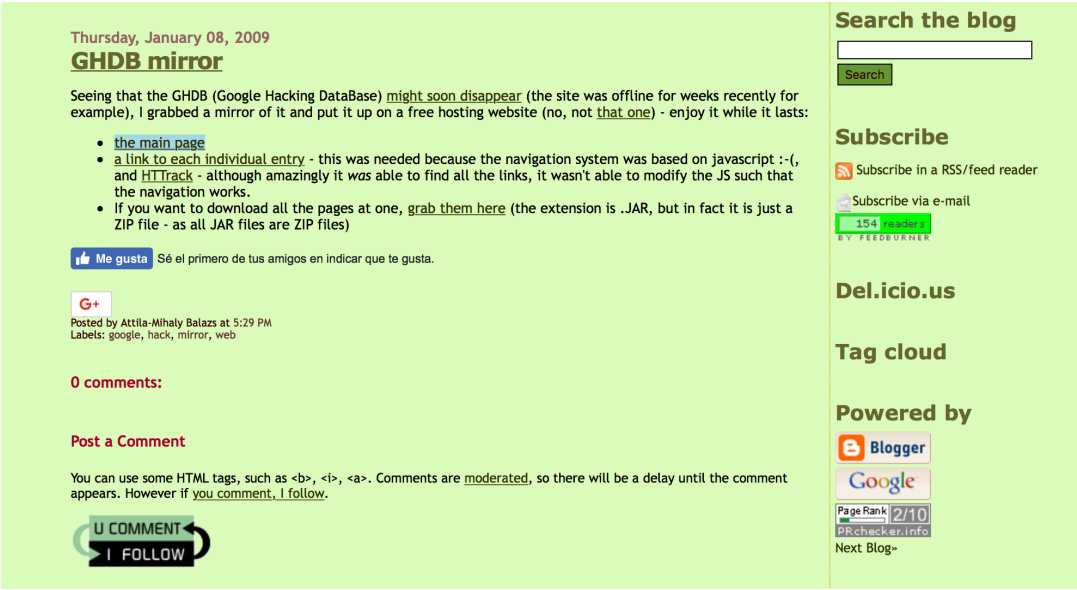

Sus principales características son:

- Almacena cientos de google dorks
- Actualizada constantemente
- Clasificada en varias categorías:
    - Vulnerabilidades
    - Mensajes de error
    - Archivos con contraseñas
    - Portales de entrada
    - Detección de servidor web
    - Archivos sensibles
    - Detección de dispositivos

## GHDB (Off-line)

En aquellas ocasiones en las que se encuentra caído el servidor web de Johnny Long (en cuyo caso la web de GHDB arroja un error 404) se puede recurrir a diferentes URLs donde dispondremos de un mirror completo de la Base de datos de GHDB.

En el caso de la Base de datos de GHDB, el mirror es el siguiente: http://ghdb-mirror.freehostia.com/index.HTM
Si se quiere acceder a todos los Google Dorks, la URL es la siguiente: http://ghdb-mirror.freehostia.com/_0toc.html
Y por último, si se necesita descargar toda la BBDD, la URL es la siguiente: http://ghdb.mirror.googlepages.com/ghdb.jar

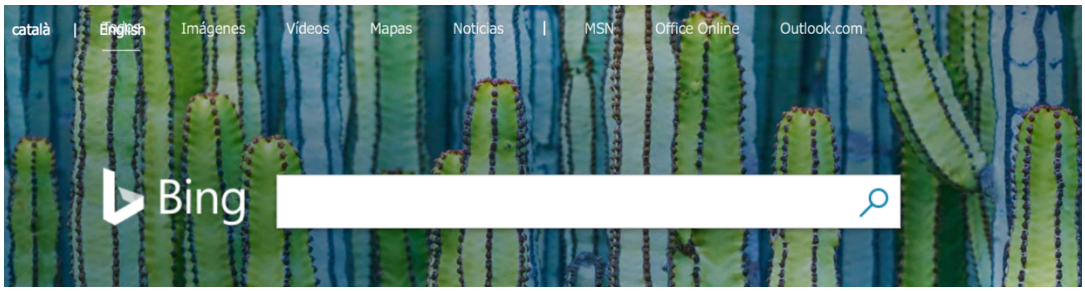



## Buscador BING

Link: https://www.bing.com

Es un buscador especialmente adecuado para realizar búsquedas de direcciones IPs y nombres de nodos y DNS.

Dispone de la posibilidad de utilizar filtro, como por ejemplo el filtro IP (ip: 123.201.023.011)




### Buscadores de paginas Web caídas o discontinuadas

Si encontramos paginas Web ofreciendo el error 404 o ya no disponibles por haber sido eliminadas podemos recurrir a herramientas como:

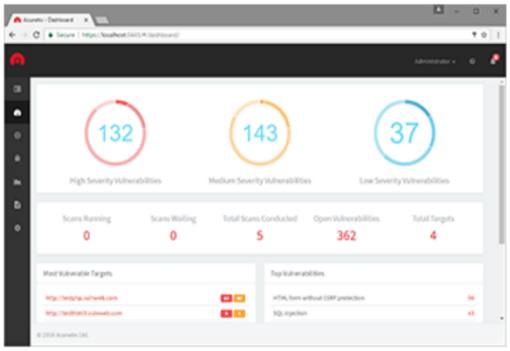
- **ACUNETIX** (Link: www.acunetix.com) que nos permiten hacer una búsqueda mas exhaustiva y poder descargar aquellas paginas web que ofrecen el error 404.
- **INTERNET ARCHIVE** (Link: www.archive.org). Internet Archive es una biblioteca sin animo de lucro de millones de libros gratis, películas, música, software y sitios web que han sido discontinuados.

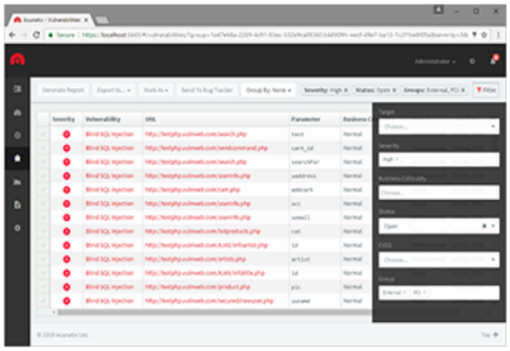
## 8.1.4. Inspección de paginas Web (ACUNETIX)

Una auditoría de sitio web utilizando herramientas web Acunetix proporciona a los expertos en seguridad web una serie de pruebas de penetración y genera de forma inmediata y a medida un informe de auditoría de la paginas web inspeccionadas.

Acunetix tiene muchas características innovadoras disponibles para el sitio web de auditoría:

- Prueba automática de XSS, SQLi y más de otras 3000 vulnerabilidades
- La reducción de falsos positivos con la exploración de caja gris que analiza el código durante la ejecución.
- Exploración automática de las áreas restringidas
- Las pruebas de más de 1200 vulnerabilidades específicas de WordPress, Drupal y Joomla!
- Analiza HTML5, JavaScript y servicios web RESTful
- Gestión de vulnerabilidades para priorización de riesgos
- Generación de informes completos para el cumplimiento legal y normativo.

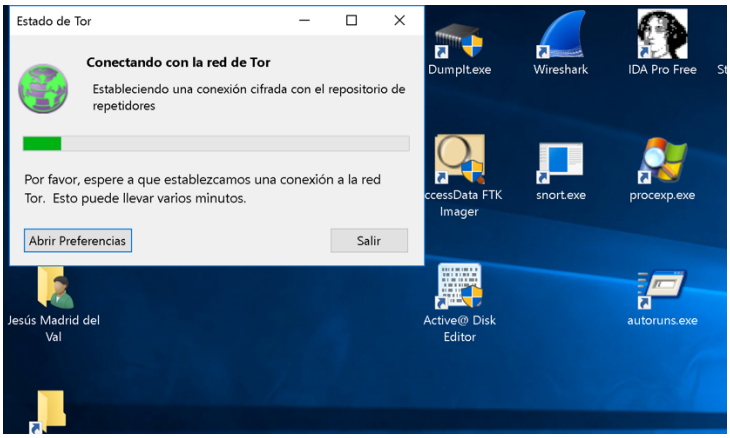


### 8.1.5. Buscadores de Información en la Deepweb

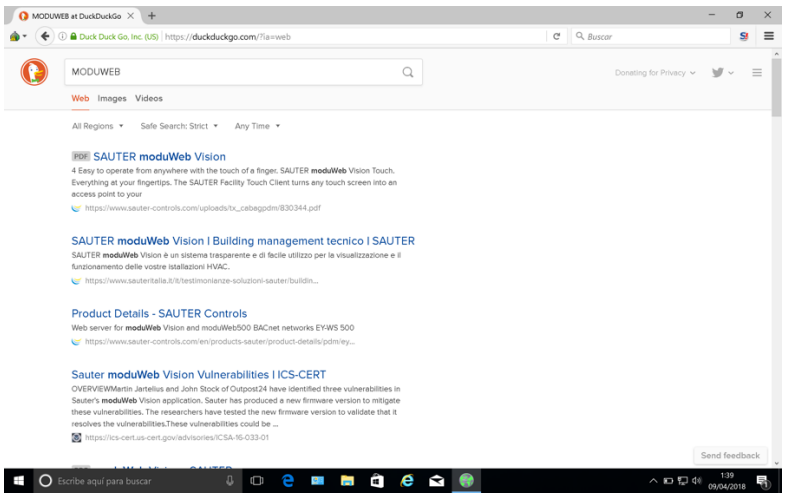
En este apartado se describen los buscadores mas empleados para búsquedas en la Deepweb,

Para ello lo primero será disponer de un explorardor compatible con la Deep Web. La aplicación mas extendida es ***TOR Browser***.

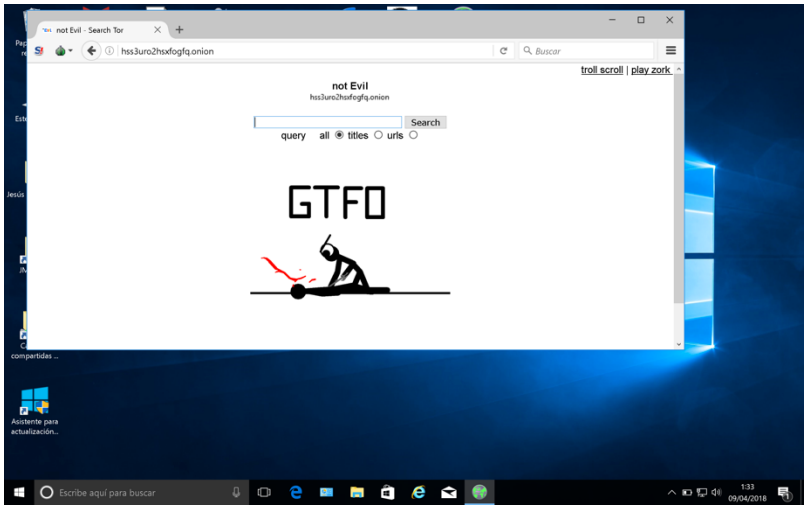



Los principales buscadores en la Deepweb son los siguientes:

Duck duck Go




Not Evil




Memex Deep Web Search Engine

Onion.City

### 8.1.6. Herramientas OSINT

a) Análisis y volcado de paginas Web

- Site Rippers.
- Wget. (Windows y Linux)
- Teleport Pro4 (Windows)

- Black Windows.
- Instant source.
- Internet Archive

b) Busqueda de información en la web

- Google dorks.
- Shodan
- Site Digger
- Acunetix
- Wikto
- Nikto

c) Busqueda e Investigación de personas. (Recopilacion)

- Maltego.
- FOCA
- Sitedigger
- Wikto
- Whois – IANA
- Netcraft
- Ping visual y Traceroute
- Nslookup (caracterización DNS)
- Anubis
- IPAdress.com

d) Obtencion de Logs

- Logstash.

e) Almacenamiento

- MongoDB
- Elasticsearch

f) Análisis y explotacion

- Robomongo
- Kibana

### 8.1.7. Automatizacion de busquedas

- TYFYP Massive TELNET Passport Tester: Automatizar consultas a protocolos TELNET (Gibhut)
- Selenium IDE 2.9.0: copia parámetros introducidos por el usuario en el Navegador.
- Java JUnit4: programación de script de búsquedas automáticas.

### 8.1.8. Aplicaciones de bases de datos

Estas son las aplicaciones relacionadas con Bases de Datos mas relevantes que pudieran emplearse para Hacking ético:

| | |
|---|---|
| **MongoDB** | https://fastdl.mongodb.org/linux/mongodb-linux-x86_64-3.0.11.tgz |
| **Robomongo** | https://download.robomongo.org/0.9.0-rc8/linux/robomongo-0.9.0-rc8- linux-x86_64-c113244.tar.gz |

### 8.1.9. Descifradores de contraseñas

Estas son las aplicaciones de desencriptado y descifrado de contraseñas mas relevantes y que pudieran emplearse para determinar credenciales de usuarios en las tareas de hacking ético:

- www.md5-hash.com
- Widows: Lophtcrack
- Fuerza bruta sobre un cjto. de hashes: John the Ripper, hashcat, 10phtcrack
- Fuerza bruta sobre proceso de logging: Brutus, Hydra

### 8.1.10. Geolocalización

Estas son las aplicaciones de Geolocalización mas relevantes:

- IPLocation.net

## 8.2. INFORMACIÓN TÉCNICA

### 8.2.1. Listado de puertos y sistemas objetivo

En la siguiente tabla se recogen los puertos mas habituales empleados en los entornos SCADA, asi como los sistemas objetivo y los protocolos mas relevantes.

| Sistemas Objetivo | | | |
|---|---|---|---|
| **Tipo** | **Descripción** | **Link** | **Puertos** |

| | | | |
|---|---|---|---|
| **WebCams** | Cámaras de seguridad | URL | |
| **Cams** | Cámara Universal Plug and Play AvTech | URL | HTTP (80)<br>Kerberos (88)<br>HTTP (8080)<br>Qconn (8000)<br>HTTP (81) |
| **Dreambox** | Decodificadores de España → Linux-powered DVB satellite, terrestrial and cable digital television receivers (set-top box) | URL | Telnet (23)<br>FTP (21)<br>HTTP (80)<br>HTTP (8080)<br>SMB (445) |
| **Default password** | Dispositivos que dentro de sus metadatos tengan relación con las palabras claves "default password" | URL | Telnet (23)<br>HTTP (8080)<br>8081<br>Automated Tank Gauge (10001)<br>HTTP (80) |
| **Netgear** | Routers inalámbricos NetGear | URL | HTTP (8080)<br>HTTPS (8443)<br>Modem Web Interface (7547)<br>HTTP (80)<br>FTP (21) |
| **Routers w/ Default Info** | Routers con información en mensaje de autenticación o en banner de admin/1234 | URL | HTTP (80)<br>HTTP (8080)<br>Kerberos (88)<br>HTTP (81)<br>Qconn (8000) |
| **Android Webcam** | Webcams Android sin clave | URL | 8081<br>HTTP (8080)<br>Webmin (10000)<br>8010<br>NAS Web Interfaces (9000) |
| **D-Link Internet Camera** | Cámaras D-link sin autenticación | URL | HTTPS (443)<br>8081<br>HTTP (8080)<br>http (80)<br>HTTP (8181) |
| | | | |

| **Protocolos convencionales SCADA** | | |
|---|---|---|
| **Tipo Protocolo** | | **Puerto** |
| **Modbus** | | 502 |
| **dnp** | | 19999 |

| | | |
|---|---|---|
| **dnp3** | | 20000 |
| **Fieldbus** | | 1089-91 |
| **Ethernet/IP** | | 2222 |
| **EtherCAT** | | 34980 |
| **Profinet** | | 34962-64 |
| **Otros varios** | | 19999, 20000, 1089-1091, 2222, 34980 y 34962-34964 |

## 8.3. NORMATIVA APLICABLE Y GUÍAS

A continuación se recogen las características de algunas de las más importantes normativas y guías de seguridad de los Sistemas OT/IT que rigen en los entornos industriales.

### 8.3.1. ISA99

La norma ISA99 engloba un conjunto de guías e informes técnicos, de los que finalmente sólo se publicaron las dos primeras guías (ANSI/ISA-99.01.01-2007 y ANSI/ISA-99.02.01-2009) y un informe técnico (SI/ISA-TR99.01.02-2007).
La primera guía publicada incluye los conceptos, términos y modelos que se han de usar en el resto de componentes de la serie. La segunda guía publicada describe los elementos necesarios para la implantación de un sistema de gestión de la ciberseguridad y cómo conocer los requerimientos de cada elemento.
El informe técnico publicado recoge una serie de herramientas de seguridad, al igual que su modo de implantación y despliegue dentro de los sistemas de control. Este informe fue actualizado para recoger nuevas herramientas.
El desarrollo de esta norma se detuvo cuando se tomó la decisión de iniciar la norma ISA IEC 62443, que recoge toda la información ya desarrollada por la ISA y define nuevos entregables.

### 8.3.2. IEC 62443

La norma IEC 62443, elaborada por el grupo TC65 de la IEC, surge como evolución de la norma ISA 99, con la intención completarla y ampliar sus capacidades de actuación.
La norma se compone de un total de 13 documentos, de los cuales algunos ya están publicados de forma oficial y el resto en estado de borrador. Los documentos se dividen en 5 informes técnicos, 1 especificación técnica y 7 guías, agrupadas en cuatro bloques según su contenido: General, Políticas y procedimientos, Sistema y Componentes.

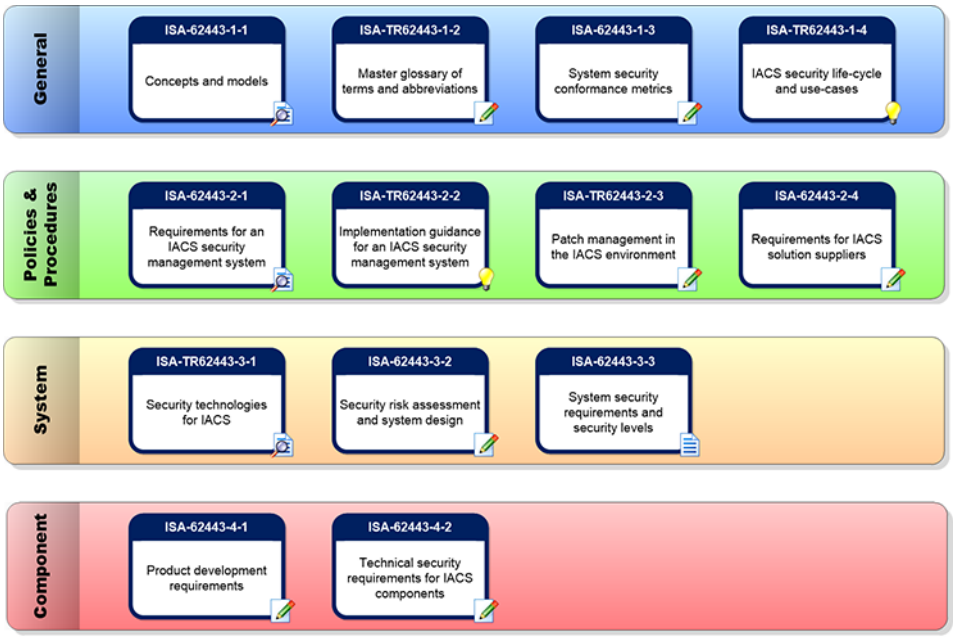



Fig. Estado de desarrollo de los documentos que componen la norma IEC 62443

Los documentos publicados son:
IEC/TS 62443-1-1:2009: Especificación técnica que define la terminología, conceptos y modelos para los sistemas de control y automatización industrial. Es la actualización del documento ANSI/ISA-99.01.01-2007 de la ISA99.
IEC 62443-2-1:2010: Este documento se corresponde con el documento ANSI/ISA-99.02.01-2009 publicado por la ISA 99, describiendo el sistema de gestión de la ciberseguridad para sistemas de control.
IEC/TR 62443-3-1:2009: Renueva el informe técnico SI/ISA-TR99.01.02-2007 con nuevas herramientas de seguridad para IACS.
IEC/PAS 62443-3-3:2008: Especificación disponible para todo el público cuyo objetivo es la creación de un marco que asegure las tecnologías de comunicación y la información referentes a los procesos industriales.

### 8.3.3. NIST SP 800-82

El propósito de esta publicación realizada por el Instituto Nacional de Estándares y Tecnología (NIST) estadounidense es proporcionar una guía para la seguridad de los sistemas de control, incluyendo sistemas SCADA (Supervisory Control And Data Acquisition), DCS (Distributed Control System) y otros sistemas que trabajan en los sistemas de control.
El documento define topologías típicas de estos sistemas, identifica amenazas y vulnerabilidades y proporciona recomendaciones y contramedidas para mitigar los riesgos asociados.
El documento fue publicado en el año 2011, actualmente se está elaborando una segunda revisión que se encuentra en fase de último borrador para ser candidato de publicación.

### 8.3.4. NIST SP 800-53

Al igual que el NIST SP 800-82, este documento también ha sido desarrollado por el NIST. El propósito de la publicación es proporcionar una guía de controles de seguridad para los sistemas de información. Aplica a todos los componentes de un sistema de información que procesa, almacena o transmite información.
El apéndice F del documento recoge una serie de controles de seguridad, diseñados para facilitar el cumplimiento con diversas leyes. El propio NIST publicó una serie de guías adicionales, ICS Supplemental Guidance, ICS Enhancements (one or more) e ICS Enhancement Supplemental Guidance, que ayudan e indican como han de aplicarse los controles publicados en NIST SP 800-53 sobre los sistemas de control industrial, así como información de cuáles aplican y cuáles no.
La guía se encuentra en este momento en la versión 4, publicada en 2013.

### 8.3.5. RG 5.71

La comisión de regulación nuclear de los Estados Unidos (NRC) publicó esta guía para establecer los controles para el cumplimiento de las regulaciones de la comisión respecto a la protección de los ordenadores, las comunicaciones y las redes frente a ciberataques.
La guía RG 5.71 (Regulatory Guide 5.71) describe una estrategia de defensa consistente en una arquitectura defensiva y un conjunto de controles basados tanto en NIST SP 800-82 como en NIST SP 800-53. Los controles están divididos en tres categorías: técnicos, operacionales, y gestión.

Las normativas que se han mencionado son las más importantes para el sector industrial y las que más se consultan e intentan cumplir, principalmente por cubrir todos los aspectos de la seguridad y no estar focalizados en un entorno específico (a excepción de RG 5.71).
Además de estas normas, existen otras normativas que también son importantes y es necesario destacar. Estas otras normativas están centradas en algún sector específico, principalmente en el sector eléctrico, que es el más avanzado; o en alguna función de seguridad concreta.

### 8.3.6. NERC CIP

El NERC es el organismo regulador de la energía de los Estados Unidos. Para poder valorar la seguridad de las instalaciones y del sector en general creó una serie de guías con controles de obligado cumplimiento. Originalmente crearon 9 guías, de las que todas menos la primera están relacionadas con la ciberseguridad, posteriormente ampliaron el número total a 11. Actualmente está en vigor la versión 3 y en desarrollo la versión 5 (excepto para CIP-010 y CIP-011 que es la versión 1).
Este estándar reconocer los diferentes roles de cada entidad en la operación del sistema eléctrico, la criticidad y las vulnerabilidades de los activos que lo componen y los riesgos a los que están expuestos.
Las demandas para la gestión y el mantenimiento de un sistema eléctrico más seguro por parte del negocio y la parte operativa hacen que los ciberactivos tengan que soportar cada vez más funciones y procesos catalogados como críticos, para comunicarse entre ellos intercambiando datos y servicios. Esto se traduce en un aumento de riesgo para estos

ciberactivos ya que al tener una mayor exposición se pueden incrementar los ciberataques a los mismos.

### 8.3.7. IEC 62351

El ámbito de actuación de la norma IEC 62351 es la seguridad en las operaciones de control del sector energético. El objetivo principal es acometer el desarrollo de estándares de seguridad para los protocolos de comunicaciones definidos por el grupo IEC TC 57, específicamente IEC 60870-5 (IEC101, IEC104, etc.), IEC 60870-6 (ICCP), IEC 61850 (MMS, GOOSE), IEC 61970 y IEC 61968.

La norma IEC 62351 se divide en 11 documentos independientes, siendo el primero la introducción a la norma, el segundo el glosario de términos y el resto el conjunto de medidas de seguridad, aplicadas por familias de protocolos. Los últimos documentos unidos a la norma definen la implementación de medidas como el control de accesos basado en roles (RBAC – Role Based Access Control), la gestión de claves, la definición de una arquitectura de seguridad o las medidas de seguridad para utilizar con ficheros XML.

### 8.3.8. IEEE 1711-2010

IEEE 1711-2010 proviene del trabajo realizado en la elaboración del documento IEEE P1689, cuyos requerimientos fueron incorporados en esta norma. A su vez, el documento IEEE P1689 proviene de la norma AGA12, desarrollado para el sector gasista americano y que recoge medidas criptográficas a aplicar en los sistemas de control para mejorar la seguridad.

IEEE 1711-2010 define un protocolo serie de seguridad para dos tipos de módulos criptográficos: el módulo criptográfico SCADA (SCM) para proteger el canal serie SCADA; y el módulo criptográfico de mantenimiento (MCM) para proteger el canal de manteamiento, habitualmente implementado sobre modem.

### 8.3.9. IEEE 1686-2007

El estándar IEEE 1686-2007 define las funciones y características que deben ser proporcionadas por los IED (Intelligent Electronic Device) para acomodarse a los programas CIP (Critical Infrastructures Protection).

El estándar expresa qué salvaguardas, mecanismos de auditoría e indicadores de alarma debe proveer el fabricante del IED (Intelligent Electronic Device) relacionadas con todas las actividades asociadas a acceso, operación, configuración, cambio de firmware y recuperación de datos e información. También permite al usuario definir un programa de seguridad alrededor de las características indicadas.

El estándar está desarrollado siguiendo los controles y medidas de seguridad publicados por el NERC en su conjunto de normas CIP, pero puede ser aplicado sobre cualquier IED, esté afectado o no por la norma, donde se requieran características de seguridad.

# 9. RESULTADOS

En el presente apartado se identifican y caracterizan un conjunto de herramientas e información que, empleadas de forma combinada con Shodan permiten hacer una explotación avanzada de dicha aplicación.
Esta suite de herramientas (Toolbox) recoge todos aquellos elementos necesarios para optimizar el proceso de Auditoria de Pentesting de sistemas SCADA, estando compuesta por:

- Aplicaciones SW: APIs, Bases de Datos, etc.
- Información técnica: Links, Filtros shodan, Puertos SCADA, etc.
- Normativa aplicable y guías: ANSI/ISA99, CCN-STIC-480, IEC, IEEE, NERC, NIST SP-800, etc.

## 9.1. LISTADO DE PUERTOS Y SISTEMAS

En la siguiente tabla se recogen los puertos mas habituales empleados en los entornos SCADA, asi como los sistemas objetivo y los protocolos mas relevantes.

| Sistemas Objetivo | | | |
|---|---|---|---|
| **Tipo** | **Descripción** | **Link** | **Puertos** |
| **WebCams** | Cámaras de seguridad | URL | |
| **Cams** | Cámara Universal Plug and Play AvTech | URL | HTTP (80)<br>Kerberos (88)<br>HTTP (8080)<br>Qconn (8000)<br>HTTP (81) |
| **Dreambox** | Decodificadores de España → Linux-powered DVB satellite, terrestrial and cable digital television receivers (set-top box) | URL | Telnet (23)<br>FTP (21)<br>HTTP (80)<br>HTTP (8080)<br>SMB (445) |
| **Default password** | Dispositivos que dentro de sus metadatos tengan relación con las palabras claves “default password” | URL | Telnet (23)<br>HTTP (8080)<br>8081<br>Automated Tank Gauge (10001)<br>HTTP (80) |
| **Netgear** | Routers inalámbricos NetGear | URL | HTTP (8080)<br>HTTPS (8443)<br>Modem Web Interface (7547)<br>HTTP (80)<br>FTP (21) |

| | | | |
|---|---|---|---|
| **Routers w/ Default Info** | Routers con información en mensaje de autenticación o en banner de admin/1234 | URL | HTTP (80)<br>HTTP (8080)<br>Kerberos (88)<br>HTTP (81)<br>Qconn (8000) |
| **Android Webcam** | Webcams Android sin clave | URL | 8081<br>HTTP (8080)<br>Webmin (10000)<br>8010<br>NAS Web Interfaces (9000) |
| **D-Link Internet Camera** | Cámaras D-link sin autenticación | URL | HTTPS (443)<br>8081<br>HTTP (8080)<br>http (80)<br>HTTP (8181) |
| | | | |

| **Protocolos convencionales SCADA** | | |
|---|---|---|
| **Tipo Protocolo** | | **Puerto** |
| **Modbus** | | 502 |
| **dnp** | | 19999 |
| **dnp3** | | 20000 |
| **Fieldbus** | | 1089-91 |
| **Ethernet/IP** | | 2222 |
| **EtherCAT** | | 34980 |
| **Profinet** | | 34962-64 |
| **Otros varios** | | 19999, 20000, 1089-1091, 2222, 34980 y 34962-34964 |

## 9.2. NORMATIVA APLICABLE

A continuación se recogen las más importantes normativas y guías de seguridad de los Sistemas OT/IT que rigen en los entornos industriales.

- ISA99
- IEC 62443
- NIST SP 800-82
- NIST SP 800-53
- RG 5.71
- NERC CIP
- IEC 62351
- IEEE 1711-2010
- IEEE 1686-2007

## 9.3. TOOLBOX HACKING DE SIST. SCADA

En el presente apartado se relaciona un conjunto de herramientas que, empleadas de forma combinada con Shodan permiten hacer una explotación avanzada de los resultados ofrecidos.

### Aplicación SHODAN

- Shoda.io
- APIs
- Plug-ins

### Buscadores de información en la web (Surface web)

- Google Dorks
- Google Hacking Data Base (GHDB)
- Bing

### Explorador y Buscadores de información en la web (Deep web)

- Explorador: TOR Browser
- Buscadores: Onion.City, Duck duck Go, Not Evil, Memex Deep Web Search Engine

### Aplicaciones de inspección de páginas

- Acunetix
- Internet Archive

### Herramientas de OSINT e Ingeniería Social

- Análisis y Volcado de paginas Web
- Busqueda de personas
- Obtencion de Logs

### Herramientas de automatización de Busquedas

- TYFYP
- Selenium IDE
- Java unit4

### Aplicaciones de Gestión de Bases de Datos

- Robo Mongo
- MongoDB
- ElasticSearch
- Kibana

### Descifradores de contraseñas

- www.md5-hash.com
- Widows: Lophtcrack

- Fuerza bruta sobre un cjto. de hashes: John the Ripper, hashcat, 10phtcrack
- Fuerza bruta sobre proceso de logging: Brutus, Hydra

## Aplicaciones de Geolocalización de IP

- IPLocation.net

# 10. CONCLUSIONES Y TRABAJO FUTURO

## 10.1. CONCLUSIONES

Del trabajo realizado se evidencia el enorme potencial que dispone la Herramienta SHODAN como un motor de búsqueda para identificar equipos conectados a la red con vulnerabilidades de seguridad por errores de configuración, como pueden ser los servidores o nodos que forman los sistemas SCADA. Este potencial que ofrece Shodan con la combinación de filtros y palabras claves se ve todavía incrementado con el empleo de una extensa librería de APIs o herramientas libres para poder hacer una explotación avanzada de los datos que obtiene de las búsquedas, permitiendo incluso la automatización del proceso de búsqueda y reporting.

La disponibilidad de una suite de herramientas compatibles con Shodan, entre sí e incluso integrables entre ellas permitirá no solo identificar fácilmente aquellos equipos SCADA vulnerables sino poder acceder posteriormente a los mismos explotando dichas vulnerabilidades.

Por lo anterior la existencia de dicha Suite podría constituir una capacidad elemental que simplificase y facilitase a los Expertos en Seguridad TI las tareas derivadas de las Auditorias de Pentesting de Instalaciones dotadas con Sistemas SCADA.

## 10.2. TRABAJO FUTURO

El presente trabajo ha servido para identificar aquellas posibles herramientas que pudieran emplearse de forma conjunta con SHODAN, mediante su previa evaluación y justificación de utilidad.

Un posible proyecto futuro podría tener como objetivo implementar las últimas versiones estables de dichas herramientas en un entorno operativo abierto diseñado para aplicaciones de seguridad (p.ej. en una licencia de Kali Linux). Dicho futuro proyecto podría contemplar la evolución de algunas de las herramientas actuales (p. ej. TYFYP Telnet) para que incorporasen la posibilidad de logarse por fuerza bruta a los dispositivos que no están configurados por defecto mediante diccionarios de palabras clave o wordlist.

# REFERENCIAS BIBLIOGRÁFICAS


- [1] "SCADA Hacking: Finding SCADA Systems using Shodan | hackers-arise" Available: https://www.hackers-arise.com/single-post/2016/06/30/Hacking-SCADA-Finding-SCADA-Systems-using-Shoda
- [2] Shodan (2015), The Search engine for Web, (https://www.shodan.io/) (12 Junio)
- [3] Daniel Miessler (2015), Account Harvesting as the Most Serious IoT Vulnerability, 06 de enero de 2015, (https://danielmiessler.com/blog/account-harvesting-serious-iot-vulnerability/) (14 de junio de 2015).
- [4] Daniel Ferreira (2014), Gracias por tu password, router, Un Informatico en el lado del Mal, 20 de enero de 2014, (http://www.elladodelmal.com/2014/01/gracias-por-tu-password-router.html) (14 de junio de 2015)
- [5] (2013), Default Passwords for Mikrotik, (https://www.google.com/fusiontables/DataSource?docid=1sjo-xQ2V6JCOIlgjm9kQUUIKQ8uQuk55CajO37w) (14 de junio)
- [6] Jhon Honovich (2012), IP Cameras Default Passwords Directory, 5 de enero de 2012, (http://ipvm.com/report/ip_cameras_default_passwords_directory) (14 de junio de 2015)
- [7] Selenium WebDriver, SeleniumHQ Browser Automation, (http://www.seleniumhq.org/projects/webdriver/) (14 de junio)
- [8] "Normativa de Seguridad en Sistemas de Control", INCIBE, (publicado el 3/07/2015): https://www.certsi.es/blog/normativas-seguridad-sistemas-control
- [9] «Google Hacking Database Offline | El diario de Juanito,» 11 Junio 2009. [En línea]. Available: https://windowstips.wordpress.com/2009/06/11/google-hacking-database- offline/ [Último acceso: 10 Mayo 2016].
- [10] IHM sistema SCADA Lookout de National Instruments. www.amcec.com
- Pablo Pérez San-José, Eduardo Álvarez Alonso, Susana de la Fuente Rodríguez, Laura García Pérez y Cristina Gutiérrez Borge. Estudio sobre la seguridad de los sistemas de monitorización y control de procesos e infraestructuras (SCADA). INTECO OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN. Año 2012. www.inteco.es.
- [11] Michael Schearer "Shodan for Penetration Testers" Available: https://www.defcon.org/images/defcon-18/dc-18-presentations/Schearer/DEFCON-18-Schearer-SHODAN.pdf (21 Febrero 2011)
- [12] Offensive Security's Exploit Database Archive https://www.exploit-db.com


# TRABAJOS CITADOS


- [1] "Análisis de Vulnerabilidad/ Seguridad con SHODAN", Cristian Fernando Timbi Sisalima, (Junio de 2015), Trabajo Fin de Master en Ingeniería del SW para la Red (UAH)

# ANEXO

AUTOMATIZACIÓN DE BUSQUEDAS DE SERVIDORES TELNET

# Automatización de busquedas de Servidores TELNET con TYFYP y SHODAN

**Autor:**

Cristian Fernando Timbi Sisalima

**Fecha:**

Junio 2015

## Consumo por exploración del DOM HTML

Se propone y valida un método para chequear el acceso de forma automática de conexiones TELNET vulnerables que han sido previamente identificadad por SHODAN. El método se basa en procesar el response de la solicitud HTTP hecha sobre el servidor Shodan, procesamiento que se podría hacer por medio de expresiones regulares o por medio de un API Java que permita procesar un documento HTML a través de su DOM, siendo una alternativa el usar JSoup (Java HTML Parser)

Para ello nos valimos de la autenticación y la navegación como tal de Selenium WebDriver, software que se ejecuta en complemento con un navegador web (Firefox) y puede ser contralado desde líneas de código es decir programadamente.

Para dicho desarrollo se instaló:

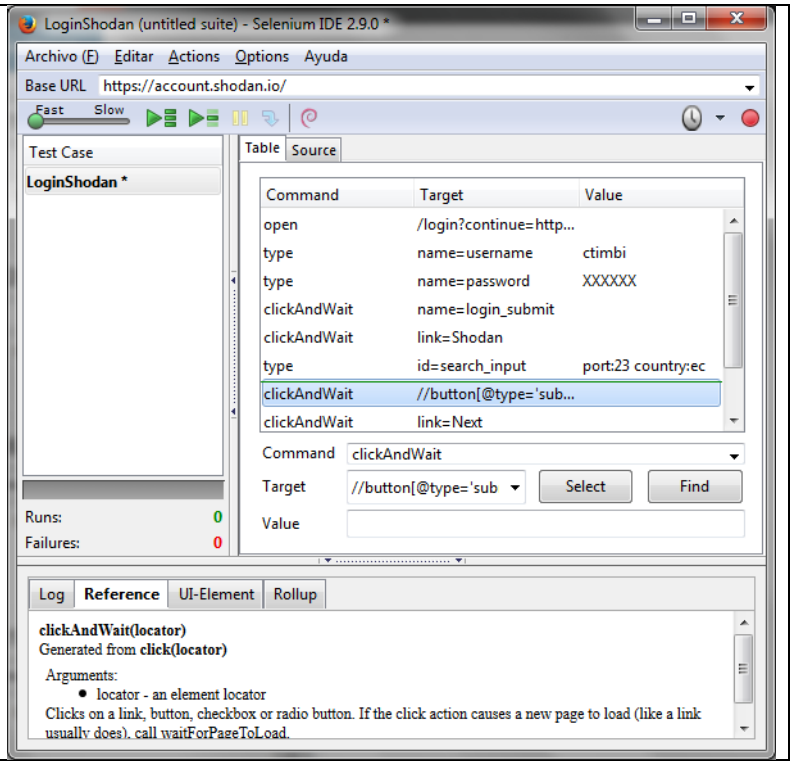
- Selenium Server Standalone
- Plugin Selenium IDE para Firefox
- Botón Selenium extensión para Firefox

Instalado estas tres herramientas, llamamos por medio de botón de extensión a Selenium IDE y grabamos un macro de la navegación que deseamos, la cual va a ir grabando cada uno de los pasos que se hacen sobre el navegador, para luego exportarlos en esta caso a código fuente Java para desde ahí hacer unas personalizaciones y desarrollar la funcionalidad deseada.

### *Paso 1. Grabar macro de navegación*

Llamando a Selenium IDE desde la extensión de Firefox, se abre la ventana de Selenium IDE, conteniendo un botón para grabar  , hacemos clic sobre el botón y posterior realizamos sobre el navegador la terea que deseamos luego repetir o emular.

La imagen muestra el macro generado para el proceso de loguearse en Shodan y luego hacer una búsqueda.

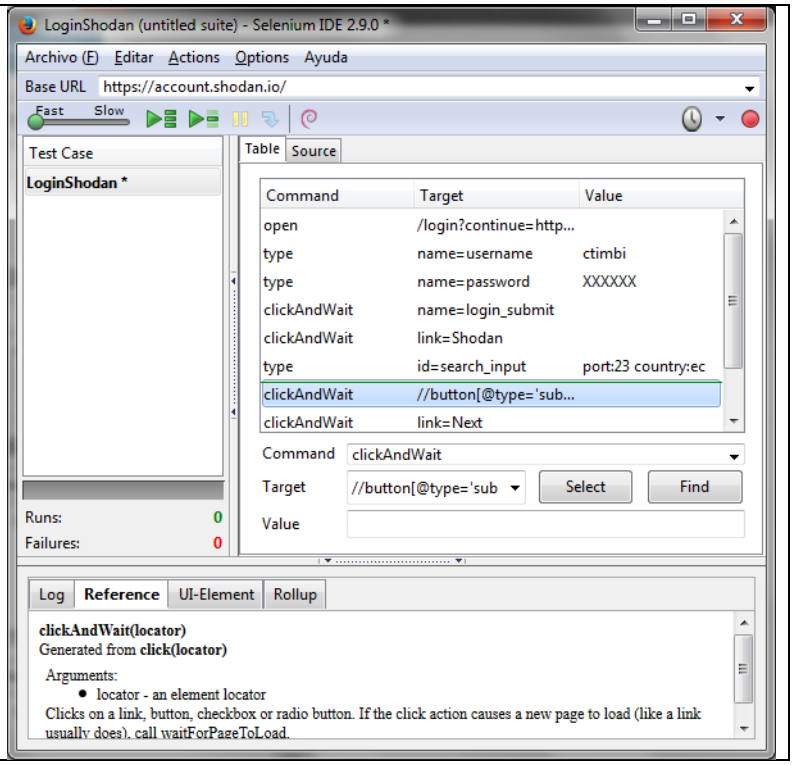


*Paso 2. Generar código fuente para lenguaje Java*

Desde el mismo Selenium IDE podemos mandar a exportar el macro a un lenguaje de programación, siendo en este caso Java.

Para esto dirigirse a: Archivo (F) > Export Test Case As > Java / JUnit 4 / Webdriver

Esto nos creara una clase Java con el código respectivo, constituido por los métodos: inicializar, emular/ejecutar y cerrar.




*Paso 3. Adaptar código fuente a necesidades para recuperar el código HTML de las páginas de resultados*

```
public List<Resultado> buscar(String params) throws Exception {
        this.params = params;

    driver.get(baseUrl + "/login");
    driver.findElement(By.name("username")).clear();
    driver.findElement(By.name("username")).sendKeys("ZZZZ");
    driver.findElement(By.name("password")).clear();
    driver.findElement(By.name("password")).sendKeys("XXXXXX");
    driver.findElement(By.name("login_submit")).click();
    driver.get("https://www.shodan.io/search?query="+params);

    String html = driver.getPageSource();
    int numeroPaginas = getNumeroResultados(html)/10;
    if(numeroPaginas>5)          //número máximo de resultados permitidos
      numeroPaginas=5;
    for(int i=0; i<numeroPaginas; i++){
        leerDOM(html);   //Análisis de DOM con Jsoup
       driver.findElement(By.linkText("Next")).click();
       html = driver.getPageSource();
    }

    return resultados;
  }
```

Las primeras líneas tienen los pasos para loguearse e iniciar la sesión para poder luego hacer consultas, luego de hacer clic en "login_submit" ya se estaría logueado, y como siguiente paso solicitamos por GET la búsqueda deseada anexando los parámetros del query "https://www.shodan.io/search?query="+parametros.

Como conocemos que Shodan da acceso a solo las 5 primeras páginas de resultados de una búsqueda, entonces recuperamos con Jsoup el número de resultados que arroja la búsqueda y estimamos el número de páginas, de ser menor a 5 leemos las que corresponden caso contrario leemos solo las 5.

### *Paso 4. Procesar DOM HTML con Jsoup*

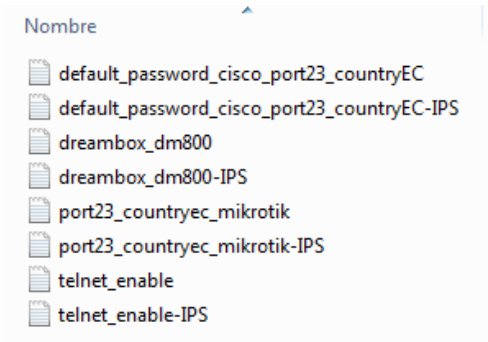
Partiendo del código HTML obtenido con Selenium ("`String html = driver.getPageSource();`"), por medio de selectores y exploración del DOM vamos creando objetos POJO que registren la IP y demás datos (host, organización, banner) y los añadimos a un arreglo para luego pasarlos a un archivo de texto.

```
public void leerDOM(String html){
	Document doc = Jsoup.parse(html);

	String numeroResultados = doc.getElementsByClass("results-
count").first().text();

	Elements resultados = doc.getElementsByClass("search-result");
	for (Element resultado : resultados) {
		Resultado server = new Resultado();
		server.setIp(resultado.getElementsByClass("ip").first().text());
		server.setTexto(resultado.getElementsByClass("search-result-
summary").first().text());
		this.resultados.add(server);
	}
  }
```

### *Paso 5. Guardar resultados en Archivo*

Desde el array de resultados creamos dos archivos, uno para todos los datos obtenidos: IP y datos, y un segundo archivo solo con las IPS, IPS que luego serán usadas para igualmente automatizar los test de conexión por clientes determinados.

El programa guarda dos archivos de texto los cuales se identifican con nombre formado por el conjunto de parámetros de la búsqueda solicitada, añadiendo al segundo archivo el texto IPS, para así identificar el uno o el otro.

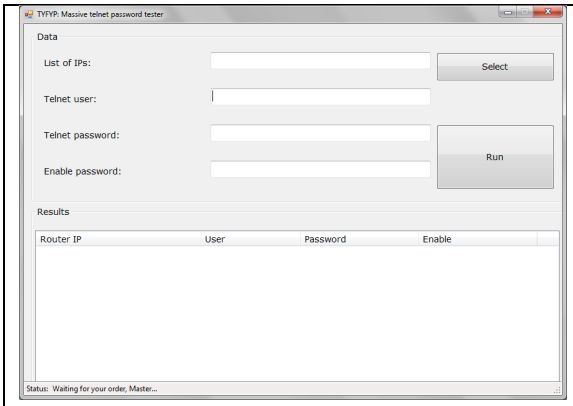



Directorio de archivos de análisis realizados con el software de consultas automáticas.

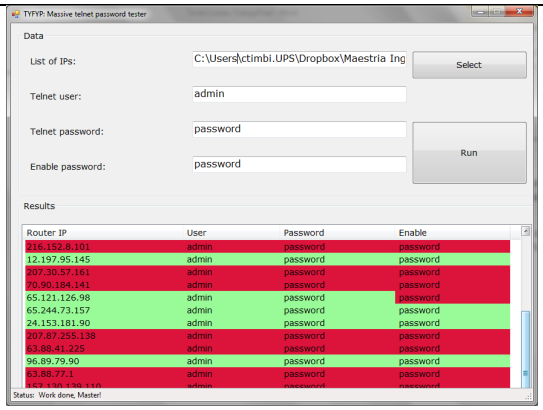
## Cliente de Test de conexiones Telnet

Con el fin de agilitar los test de conexión para un gran conjunto de equipos, se vio la necesidad de desarrollar o buscar software con este propósito, encontrando TYFYP-telnet-password-tester, el

cual parte de un archivo plano de direcciones IP de equipos a testear y el usuario y clave con el que se va a validar el acceso.




Pantalla de la aplicación que pide los datos de Archivo de lista de IPs, usuario y clave a testear, y una segunda clave usada para probar el comando enable en routers




Cargado el archivo de IPs e ingresadas las credenciales de test, se corre el programa, el cual va a testear una conexión por telnet con las credenciales indicadas, y de ser conexión satisfactoria marca el registro con color verde.