UCASAL

UNIVERSIDAD CATÓLICA DE SALTA

FACULTAD DE INGENIERÍA

Proyecto de Grado

Titulo:

SEGURIDAD EN EL INTERNET DE LAS COSAS - (IoT)

Alumno: Aldo Guido Arzelán

DN: 35.194.163

Carrera: Ingeniería en Informática

Director de PFG: Ing. Ernesto Bonfiglioli

Año 2021

HOJA DE EVALUACIÓN

Proyecto de Grado

Título: **SEGURIDAD EN EL INTERNET DE LAS COSAS - (IoT)**

Director de PFG: Ing. Ernesto Bonfiglioli _____

Alumno: **ALDO GUIDO ARZELÁN** (DNI: 35.194.163) _____

EVALUACIÓN

CALIFICACIÓN: _____

TRIBUNAL

Jurado: _____

Jurado: _____

Jurado: _____

OBSERVACIONES:

_____

_____

_____

_____

Lugar y Fecha: _____

Dedicatoria

Éste trabajo está dedicado especialmente a mi mamá y a mi papá, que me brindaron la posibilidad de estudiar y darme fuerzas en todo momento, quiénes nunca me dejaron bajar los brazos y me apoyaron en todo siempre, ellos mis pilares de la vida. Totalmente agradecido por el esfuerzo que hacen día a día. Los amo

Agradecimientos

A mis hermanas: Rocío y Julieta. Gracias no solo por haberme ayudado cuando lo necesité, sino también por enseñarme a compartir y por los lindos momentos que pasamos juntos y que seguiremos viviendo siempre. Las amo.

A mi novia, que es la mejor compañera del mundo, y en este momento está sentada a mi lado dándome su incondicional apoyo. Te amo Romina Sarzur.

A mis profesores quienes me incentivaron no solo a seguir aprendiendo, sino también a tener amor por ramas de la carrera que no me despertaban interés. Y quienes me prepararon para hoy poder defender mi trabajo.

A mis compañeros, quienes me brindaron su ayuda cuando la necesite y por convertirse en amigos de la vida.

A mis amigos, que por suerte son muchos y aparecen en el momento adecuado

INDICE DE CONTENIDO

RESUMEN EJECUTIVO

Este proyecto tiene como objetivo realizar un análisis de los protocolos de seguridad de las IoT, utilizados en el sistema informático principal de una institución del Servicio de Salud, dedicada al Diagnóstico por Imágenes. Se brinda, a los interesados en el tema, la posibilidad de conocer, detectar y solucionar las vulnerabilidades de la infraestructura informática de una institución, aplicable en cualquier otro tipo de organismo o empresa.

Mediante prueba experimental, se diseñan y se ofrecen de modo exponencial, estándares y protocolos de seguridad, con el objetivo de brindar mayor seguridad ante las vulnerabilidades de los equipos IoT tomados como estudio de caso. Con dichas propuestas, se logrará evitar cualquier tipo de ataque cibernético, incluyendo tanto los de implementación como los de ingeniería social.

ABSTRACT

The objective of this Project is to carry out an analisis of the IoT security protocols used in the main computer system of a Health Service institution dedícate to Diagnostic Imagin. Those interested in the subject are given the possibility of knowing, detecting and solving the vulnerabilities of the information infrastructure o fan institution aplicable in any other type of organization or company.

Throygh expermiental testing, security standars and protocols are designed and offered exponentially, estándars and protocols of security.

Whit the aim of provifing better security against the vulnerabilities of IoT equipment taken as a case study, with these proposals, it Will be posible to avoid any type of cyberattack, including implementation and social engineering.

INTRODUCCIÓN

En el presente el mundo vive en constante cambios y avances tecnológicos, las cosas que se pueden hacer con los distintos dispositivos son cada vez más amplias. Estos avances en busca de facilitar no solo la vida cotidiana de las personas, sino también las tareas empresariales, ambientales, etc. traen con ellos un lado negativo, que es también la evolución de las amenazas y la posibilidad de los ciberdelincuentes de realizar cada vez más acciones.

Debido a la información sensible que se maneja en las instituciones de Servicio de Salud y su compromiso con los pacientes, resulta de suma importancia resguardar y proteger la información de todo tipo de ataques contra su disponibilidad, integridad y confidencialidad, disponiendo de diferentes protocolos y políticas de seguridad, que permitan brindar la protección necesaria.

Como estudiante de Ingeniería Informática y trabajador del ámbito, y mi afición por la tecnología y la seguridad lo que me llevo a elegir este proyecto como trabajo de grado, el cual combina ambas cosas. Me resulta emocionante desarrollar un proyecto en el que puedo ampliar mis conocimientos en el área, y a su vez ayudar a las personas y entidades a protegerse.

CAPITULO 1

1.A. DESCRIPCIÓN DEL PROBLEMA

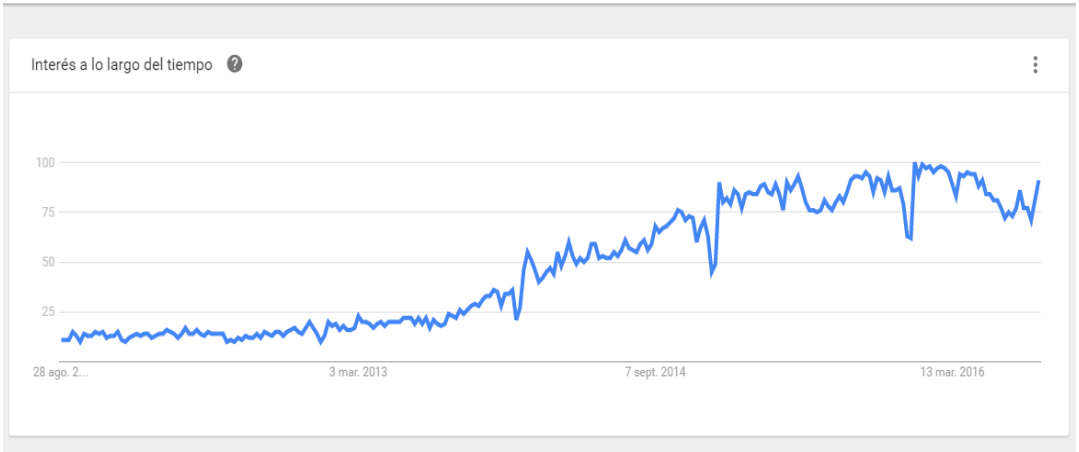
Podemos definir el **internet de las cosas**, en adelante IOT, como la consolidación a través de la red de redes de una "red" que interconecta una gran variedad de objetos o dispositivos, es decir, poder tener conectadas todas las cosas de este mundo como podrían ser vehículos, electrodomésticos, dispositivos mecánicos, o simplemente objetos sencillos como ser calzados, muebles, maletas, dispositivos de medición, biosensores, o cualquier objeto que nos podamos imaginar.

El gran objetivo de esta tecnología es hacer más práctica y cómoda la vida de las personas, así como también proporcionar una mayor seguridad en diversos ámbitos. Esta se puede tomar como un arma de doble filo ya que, al brindar seguridad, si se desea también, puede ofrecer todo lo contrario. Las consecuencias de los problemas de seguridad son cada vez más graves llegando a daños físicos a las personas.

En el siguiente gráfico (Grafico N.º 1), se puede apreciar cómo se fue incrementando el interés de las personas en el IOT, a través de los años hasta el 2016. Este es un gráfico que se puede construir con una herramienta de Google el cual muestra las tendencias de búsquedas de las personas.

El primer grafico se realizó en el año 2016 insertando como palabra clave de búsqueda "IoT". Se ve como el interés de las personas por conocer y entender que era IoT fue aumentando a lo largo del tiempo.

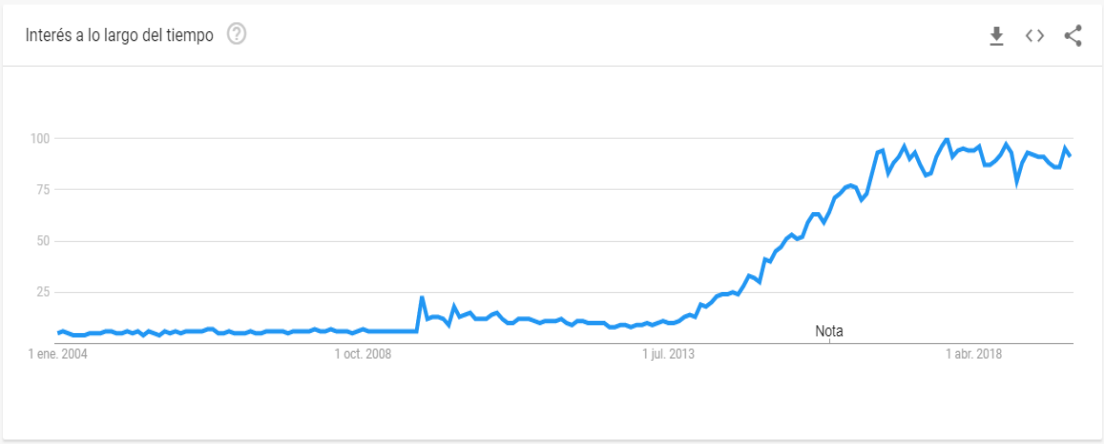
Gráfico 1: Interés por las IoT - Período 2012 – 2016



Fuente: Google Trends - https://trends.google.es/trends

El segundo grafico (Gráfico N.º 2), se realizó en octubre del 2019. Fecha de inicio en enero del 2004.

Gráfico 2: Interés por las IoT - Período 2004 - 2018



Fuente: Google Trends - https://trends.google.es/trends

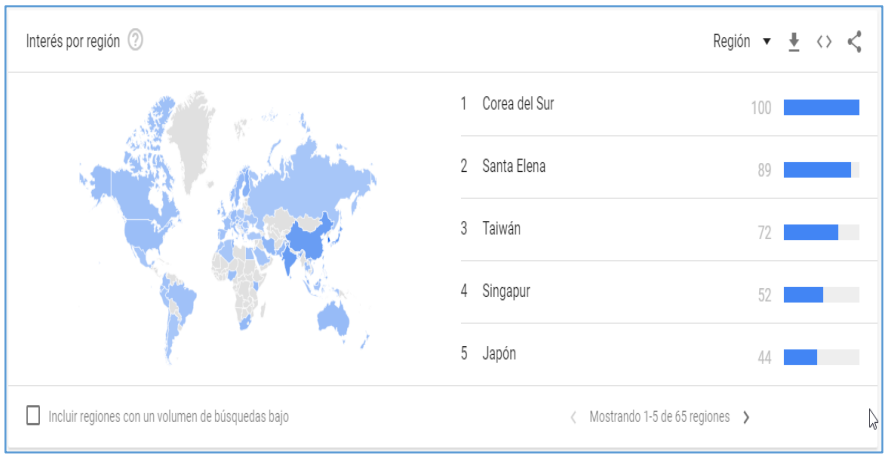
Por último, obtenemos interesantes datos a través de un gráfico divido por regiones (Gráfico N.º 3), en el cual se puede observar que la región que más búsquedas realizo sobre este tema es Corea del Sur.

El concepto de "Internet de las cosas" es un concepto que nació en el Instituto de Tecnología de Massachusetts este dice que "se trata de una revolución en las relaciones entre los objetos y las personas, incluso entre los objetos directamente, que se conectarán entre ellos y con la Red y ofrecerán datos en tiempo real."

Según un artículo de la página Web Muy Interesante, (muyinteresante.es, 2019), se plantea que gracias al IoT se podrían realizar en un futuro una serie de aplicaciones que parecieran imposibles pero que no estamos muy lejos de poderlas realizar, aplicaciones tales como un dispositivo que muestre información en tiempo real de la humedad de las plantas y flores de nuestro hogar, frigorífico con aviso al supermercado cuando se termina una comida, que el calzado que utilizamos para hacer ejercicio registren "en la nube" las estadísticas de cuanto recorre cada semana y a qué velocidad, o que los inodoros analicen su orina y detecte cualquier anomalía, o si el cepillo de dientes alertara de cualquier pequeña caries. Gracias a la tecnología de radiofrecuencia RDID (Radio Frequency Identification) solo se tendrá que integrar un microchip en cualquier objeto del hogar, del trabajo o de la ciudad para poder procesar y transmitir información a partir de él. Calculan que para el presente año (2020), cerca de entre 22 mil y 50 mil millones de dispositivos se conectaran a internet con el propósito de proporcionar a los ciudadanos una serie de servicios y aplicaciones inteligentes sin precedentes.

Extraído de: https://www.academia.edu/22066203/Ensayo_internet_de_las_cosas

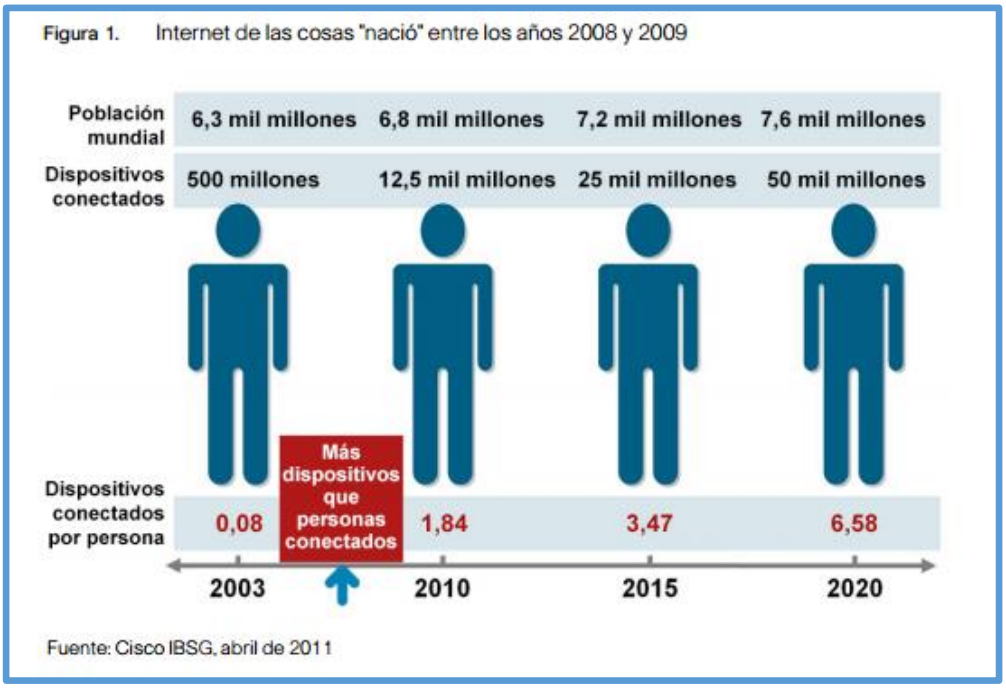
Gráfico 3: Interés por las IoT según las regiones



Fuente: Google Trends - https://trends.google.es/trends

El Informe de CISCO[1] (2011) sobre el Internet de las cosas, mencionaba cómo la evolución de Internet lo cambia todo. Ya en 2003, había aproximadamente 6,3 mil millones de personas en el planeta, y había 500 millones de dispositivos conectados a Internet. Si dividimos la cantidad de dispositivos conectados por la población mundial, el resultado indica que había menos de un dispositivo (0,08) por persona. De acuerdo con la definición de Cisco IBSG, IoT aún no existía en 2003 porque la cantidad de cosas conectadas era relativamente escasa, dado que apenas comenzada la invasión de los dispositivos omnipresentes, como los smartphones. El crecimiento explosivo de los smartphones y las tablets PC elevó a 12,5 mil millones en 2010 la cantidad de dispositivos conectados a Internet, en tanto que la población mundial aumentó a 6,8 mil millones, por lo que el número de dispositivos conectados por persona es superior a 1 (1,84 para ser exactos) por primera vez en la historia.

Gráfico 4 Proyección de IoT - 2003-2020



Fuente: Cisco IBSG, abril del 2011

[1] CISCO – 2011 - http://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf

Si se desglosan aún más estas cifras, Cisco IBSG estima que IoT "nació" en algún punto entre 2008 y 2009. Actualmente, IoT está firmemente encaminada según lo demuestra el avance de iniciativas como Planetary Skin de Cisco, la matriz inteligente y los vehículos inteligentes.

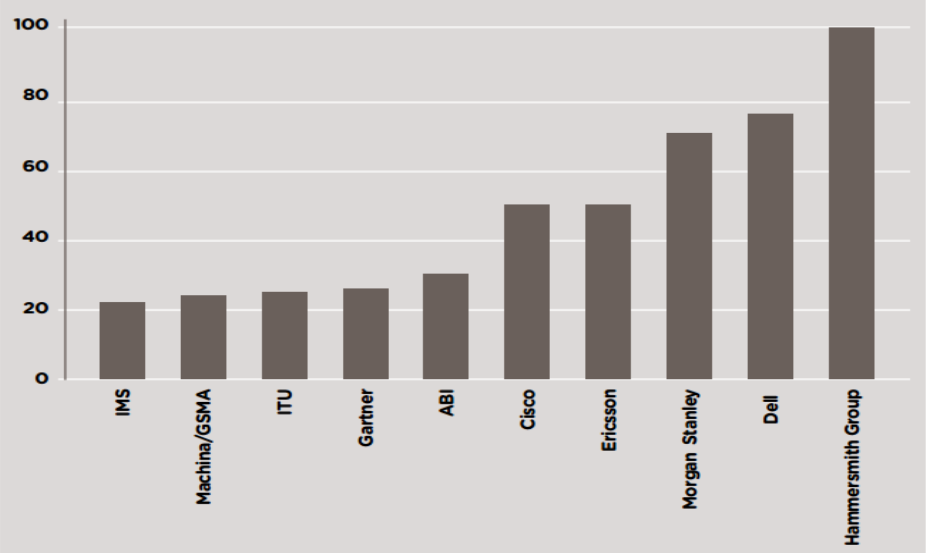
Con miras al futuro, Cisco IBSG prevé que habrá 50 mil millones de dispositivos conectados a Internet, hacia el final del año 2020. Es importante destacar que estos cálculos no tienen en cuenta los rápidos avances en la tecnología de Internet o de los dispositivos; las cifras mostradas están basadas en datos actualmente válidos."

Según afirma un artículo del sitio Web Inter Empresas[2] (2019), el Internet de las Cosas es una realidad que estamos viviendo, pero su efecto se intensificará en los próximos años. Sus posibilidades son infinitas, tanto como alcance la imaginación. Según el portal de estadísticas Statista, se prevé que en 2025 habrá más de 75.000 millones de dispositivos conectados en todo el mundo. Más de 25.000 millones en 2019, casi 31.000 millones en 2020 y más de 50.000 millones de dispositivos en 2023. En cuanto a previsiones de inversión global en despliegues IoT, IDC lo sitúa en 726.000 millones de dólares para finales de 2019."

El siguiente grafico (Gráfico N.º 5) realizado por la oficina de ciencia del gobierno del Reino Unido, muestran estimaciones de la industria de los dispositivos conectados en 2020, entre los cuales se encuentra la estimación que hemos visto recién de CISCO. (expresado en miles de millones)

2 **Inter Empresas. 2019** - https://www.interempresas.net/TIC/Articulos/252927-IoT-sacando-partido-al-mundo-hiperconectado.html

Gráfico 5 Proyección de dispositivos conectados en 2020



Fuente: Oficina de ciencia del gobierno del Reino Unido –Recuperado en junio de 2019 de: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

La consultora Gartner en un estudio estimo 26.000 millones de dispositivos para el 2020 (excluyendo a los smartphones, tablets y PC), sin embargo, en otro informe de la misma consultora, afirman que en el año 2016 un 43% de empresas adoptaron el IoT, lo cual supone un incremento del 50% del número de firmas que estarían incorporando esta nueva moda.

La cantidad de dispositivos conectados quedo en evidencia el 21 de octubre del 2016, al producirse una serie de ataques de Denegación de Servicio Distribuido (DDoS) que causo una interrupción generalizada de la actividad de internet en los Estados Unidos. Dichos ataques fueron dirigidos al Sistema de Nombres de Dominio (DNS), servicio encargado de asegurar que los pedidos de información por internet se entreguen en la dirección que corresponde, varias actividades cotidianas (Compras online, Redes sociales, escuchar música online, o simplemente realizar una búsqueda en Google) quedaron interrumpidas por periodos de tiempo variables, en algunos casos llego a durar varias horas. Lo que hicieron los atacantes fue dirigir grandes cantidades de tráfico falso a los servidores. Esto fue posible debido al gran número de dispositivos conectados con los cuales generaron grandes cantidades de tráfico falso para desbordar los servidores.

Ilustración 1 Comportamiento de conexiones de IoT

Fuente: **Welive Security – 2019 -** https://www.welivesecurity.com/la-es/2016/10/26/ataques-ddos-a-la-iot-octubre/

Como dice Guillermo Fernández, ingeniero de ventas de Soutthern Europe de **WatchGuard** Iberia, ya hay investigaciones en el mercado que indican que el 50% de las preocupaciones de los directivos con respecto a IoT tienen que ver con la ausencia de estándares específicos para toda la industria. "Esto hace que algunos países estén tomando las riendas para tratar de atajar este problema, como es el caso de la ley de seguridad de IoT de California, que establece estándares mínimos de seguridad para estos entornos" (Fernández, agosto 2019)

Coincidiendo con afirmación que hace Luis Montero de Microsoft, IoT en este momento se está extendiendo a todos los sectores a una gran velocidad y no es fácil acotarlo cuando la cantidad de dispositivos conectados es un número tan inmenso.

"Hay sectores donde el uso ya es masivo y juntos constituyen un panorama amplio y heterogéneo. Estamos hablando de ciudades inteligentes, seguridad, infraestructuras críticas, retail, sector energético y medioambiental, sanidad…La realidad es que todos los sectores pueden beneficiarse de Internet de las Cosas, más

ahora que el Edge Computing permite un procesamiento de los datos local e inteligente" (Montero, agosto 2019)

Prácticamente todas las industrias están incorporando IoT para agilizar procesos, mejorar visibilidad y crear nuevos servicios. Jordi Calvera de Intersystems aporta una serie de ejemplos del cual vamos a tomar el del interés de este proyecto, el ámbito de la salud.

"En el ámbito sanitario, una organización puede recibir datos de cientos de miles de dispositivos dedicados a la monitorización de los pacientes y de los equipos sanitarios, además de la monitorización del mantenimiento de las instalaciones. Estas aplicaciones facilitan el mantenimiento predictivo, en lugar del preventivo, que se basa en el histórico, y en la medición en tiempo real. Esto minimiza el número de incidencias, mejora la tasa de utilización de los equipos y reduce las perdidas." (Calvera, agosto 2019)

1.B. DEFINICIÓN EXACTA DEL PROBLEMA

Todos los sistemas están diseñados para prestar servicios o interactuar con personas. El punto más débil en la seguridad de la información es el ser humano. Con la utilización de ingeniería social para "engañar" o convencer a las personas ya sea cara a cara, por teléfono o por medios de telecomunicación, se logran realizar la mayoría de los ataques. Por esto es fundamental que las personas sepan reconocer cuando se encuentran ante un intento de engaño. En esta tesis lo que se busca es formar y concientizar a las personas para que puedan reaccionar adecuadamente ante un supuesto caso de ingeniería social.

Otro vector de ataque es el técnico, pero que no se aleja del error humano, ya que es el usuario el que elige como configurar los equipos. En otra época, no hace muchos años, para poder configurar un router y conectarse a internet las personas solían llamar un técnico que lo haga por ellos. Hoy en día esto cambio ya que la gran mayoría elige configurar por sus propios medios y de la manera que quieran (o puedan), ya que muchas

veces por escases de conocimientos la configuración de los usuarios deja una puerta abierta a los ciber delincuentes que se encuentran al acecho de estas fallas.

1.B.a OBJETIVOS

1.B.a.i - Objetivos generales

- Proponer una guía de buenas prácticas que todo usuario debería conocer.
- Proponer recomendaciones básicas que todo usuario debería conocer y cumplir.
- Evitar ataques de Ingeniería Social a través de una muestra de los distintos vectores de ataque para fomentar la cultura de Seguridad Informática.

1.B.b.ii - Objetivos específicos

- Desarrollar una guía de configuración para red segura.
- Analizar el impacto del hurto de información sensible.
- Desarrollar un protocolo de automatización de control de acceso a la red.

1.C. MOTIVACIÓN PARA EL ABORDAJE DEL TEMA

La motivación personal que impulsa el abordaje sobre este tema es la protección de información confidencial de las personas, pero por sobre todas las cosas preservar su salud y la vida misma de las personas sin dejar de aprovechar los múltiples beneficios del uso de las nuevas tecnologías, los dispositivos IOT que ya existen y aquellos que seguramente seguirán apareciendo para facilitar y mejorar los tratamientos de salud.

El objetivo es aportar con herramientas que brinden mayor seguridad en la conexión de los dispositivos IOT utilizados en el ámbito de la salud, seguridad que por supuesto puede trasladarse a todos los dispositivos IOT de otros ámbitos. La seguridad en la conexión genera confianza en las personas para poder utilizar tecnología con la mayor tranquilidad posible. De este modo lograr la globalización del uso de dispositivos IOT.

1.D - PASOS DEL PROYECTO

Los pasos que se desarrollan en el presente PFG son:

1º Planteamiento e identificación del problema
2º Selección y descripción de la unidad de estudio
3º Selección de los equipos a utilizar como prueba experimental
4º Identificación de las vulnerabilidades de seguridad en las IoT de la institución
5º Identificar las necesidades de red de la institución.
6º Prueba experimental de configuración de red
7º Identificar los riesgos del factor humano en la organización
8º Planteamiento de soluciones. Se establecen estándares y políticas que minimicen el riesgo humano.
9º Capacitar y entrenar al personal ante posibles ataques

1.E. CRITERIOS DE ÉXITO

Los criterios de éxito del presente PFG, se debe considerar desde diferentes puntos de vista identificando las variaciones que presentan los aspectos de análisis de factibilidad.

- **Económico:** La inversión de este proyecto no debe superar los costos de contratar una empresa de seguridad informática que brinde sus servicios. De esta manera se reducirán los costos de manera significativa.
- **Técnico:** Conocimientos necesarios para el desarrollo del proyecto.
- **Operativo:** El hospital contratista debe tener los recursos disponibles y el personal capacitado para operar satisfactoriamente.
- **Legal:** No debe infringir ninguna ley y norma legal. Los principios éticos están siempre presentes.

Aspectos técnicos:

- ✓ Identificar vulnerabilidades
- ✓ Informar sobre las vulnerabilidades encontradas

CAPITULO 2

2. EL ESTADO DE LA CUESTIÓN

2.A ANTECEDENTES

- **Antecedente 1:**

Título: "Internet de las cosas. Privacidad y Seguridad"
Tipo de investigación: Trabajo fin de grado
Autores: Miguel Castro Sola
Institución: Escuela politécnica Superior de Jaén
Año de publicación:2016
Aporte para la investigación: El objetivo de este trabajo es analizar en profundidad todos los cambios que va a suponer la implantación de esta nueva forma de entender la tecnología en general, y con ella la sociedad y la manera de hacer las cosas tanto cotidianas como laborales.

- **Antecedente 2:**

Título: "Análisis y parametrización de la seguridad en sistemas IoT.
Tipo de investigación: Trabajo de fin de grado
Autores: Perera Bartual, Oscar
Institución: Universidad politécnica de Valencia
Año de publicación:2017
Aporte para la investigación: Proponer una serie de pasos que permiten analizar, evaluar, corregir y proponer medidas y buenas prácticas concretas para abordar el estudio y mejora de la seguridad de los sistemas basados en tecnologías IoT.

- **Antecedente 3:**

  Título: "Ciberseguridad en IoT"
  Tipo de investigación: Plan de proyecto del trabajo final de carrera
  Autores: Ing. Pablo M. Almada
  Institución: Facultad de Ingeniería Universidad de Buenos Aires
  Año de publicación: 2016
  Aporte para la investigación: El trabajo comprende una investigación del estado de situación de la tecnología catalogada como Internet of Things (IoT) en lo relativo a la Ciberseguridad. En el mismo se desarrollará una introducción de qué es IoT, su impacto en Internet, a que nos exponemos con esta tecnología, cuál es su estado de madurez, análisis de la utilización de IoT para lanzar Ciberataques y su proyección a futuro. Sumado a lo anterior se analizará la estructura de implementación y despliegue de una capa de seguridad para las comunicaciones Zigbee sobre la CIAA.

2.B FUNDAMENTACIÓN TEÓRICA

En este espacio se pretende realizar un análisis del material bibliográfico que se encuentra sobre el tema del estado de seguridad en que se encuentran los dispositivos englobados en la categoría de IOT.

2.B.a Vulnerabilidad del IOT en sector salud

Al momento de crear tecnología es imposible cuidar cada aspecto de la seguridad de esta, esto se dificulta aún más, ya que personas con conocimiento en este tema dedica sus esfuerzos a encontrar nuevas formas de violar la seguridad de los equipos tecnológicos.

El internet de las cosas no está exento de este peligro, debido a que es un objetivo al que, si se llegara a alcanzar, se tendría acceso a información personal de sus usuarios y perjudicarlos de gran manera debido a la forma en que los dispositivos IoT se han instalado en los aspectos más importantes de la vida diaria de las personas.

El sector de la salud ha incorporado en gran cantidad el IOT a su infraestructura tecnológica. Estos dispositivos interconectados tienen una gran capacidad para salvar vidas. Recopilan y analizan grandes cantidades de datos y permiten a los profesionales ofrecer un tratamiento personalizado a cada paciente de forma rápida y remota. Estos dispositivos buscan mejorar el tratamiento de los pacientes brindando la información necesaria en tiempo y forma al profesional y evitando el error en formato papel (tras papeleo). El lado oscuro de estas tecnologías es que ponen en riesgo los datos sensibles de los pacientes, los cuales los ciber atacantes buscan obtener con distintos fines. En el mercado negro de Europa se venden historias clínicas por más de € 800, esta información por general es obtenida por las empresas farmacéuticas o proveedores de materiales médicos.

2.B.b. Estado actual de seguridad IOT

La seguridad de la información es un aspecto que está dando cada vez más que hablar, dado que el número de dispositivos conectados a internet es cada vez mayor, lo que supone un crecimiento en la exposición de datos en la red. Según el informe de HP FORTIFY (2014), el 80% de los dispositivos tienen fallos en la autenticación y 6 de cada 10 dispositivos con interfaz de usuario son vulnerables. Estos datos no son menores, debido a que la evolución que se está produciendo es sobre la funcionalidad y tecnología de los dispositivos, pero la seguridad es un aspecto que en principio no se está considerando con la importancia que se debería. Por el contrario, la seguridad es un aspecto que se debería tener en cuenta desde el inicio del diseño de cualquier producto.

A pesar de que los dispositivos IOT que llegan al hogar del hombre común no parecen ser productos que puedan afectar directamente a los usuarios, son elementos que pueden hacerlo si no son utilizados de forma adecuada. Podemos comenzar por imaginarnos lo que podría provocar que un tercero malicioso obtuviera acceso no autorizado al control remoto de un horno o de la caldera de una casa. Lo mismo si consiguiera acceder a una nevera, pudiendo cambiar la temperatura o apagarla. Esto podría provocar daños físicos a las personas. Si dejamos de lado por un momento el

entorno doméstico, IOT también engloba dispositivos utilizados en el entorno empresarial. Imagínense las consecuencias de perder el control del aire acondicionado de un centro de proceso de datos de una empresa, o de la heladera de un restaurante, o de las puertas de acceso a un comercio. Cualquiera de estos ejemplos podría provocar graves pérdidas a la organización.

2.B.c. Riesgos

Los riesgos varían en función de las prestaciones que brinda el dispositivo o por la dependencia que se tenga del mismo. Analizaremos algunos riesgos comunes y las áreas que pueden verse afectadas ante la presentación de una amenaza.

Ante la materialización de las amenazas a las que están expuestos estos dispositivos pueden afectar a la accesibilidad del dispositivo, a la integridad de la información que contiene y a la identidad del usuario que la posee, es decir que un intruso puede suplantar la identidad del dueño real. Quizás la disponibilidad sea uno de los aspectos que más problemas puede generar, especialmente si estamos hablando de entornos industriales donde una parada del servicio debido a un ataque que suspenda el servicio o llamado en la jerga de denegación de servicio (Dos) puede provocar grandes pérdidas. Otro factor importante y relacionado directamente con la información es la confidencialidad de los datos, que se debe garantizar ya sea a la información almacenada en el dispositivo como a la información que se transmite.

Concretaremos algunas situaciones que se pueden presentar en determinados dispositivos:

- **Posicionamiento GPS:** Los wearables son dispositivos que un usuario lleva puesto. Por lo general, estos van conectados a internet por lo que pueden ser fácilmente geo posicionados en todo momento. Esto hace que la localización del usuario quede registrada en algún sitio web y en función de la configuración de privacidad pueda estar al alcance de cualquiera. Esta situación también se puede presentar también en Smartphone si no sabemos que aplicaciones tienen acceso a la localización.

- **Hurto de información:** En los dispositivos que conectamos a internet cada vez almacenamos más información. En muchos casos, y dada la nueva mentalidad de la nube (o *cloud*), podemos acceder a esa información desde otros dispositivos a través de internet, desde aplicaciones móviles o desde entornos web donde para acceder disponemos de un usuario y una contraseña. En caso de que un tercero pudiera acceder, dispondría de información que podría vulnerar nuestra privacidad.

  El robo de información puede no producirse debido a una debilidad en el acceso, ya que como los dispositivos *wearables* son cada vez más pequeño, la facilidad de perderos también es directamente proporcional y por lo tanto facilitar a cualquier persona del acceso directo a nuestra información.

  El uso de aplicaciones en dispositivos conectados a internet puede hacer publica cierta información, como es el caso de las aplicaciones de salud y vida sana que pueden publicar posición GPS, las calorías quemadas durante la carrera, edad, altura, peso, kilómetros recorridos. En la mayoría de los casos la información es publicada por el mismo usuario, el cual no es consciente del riesgo al que se está exponiendo.
- **Control y uso malintencionado de los dispositivos:** Otro de los riesgos al que nos enfrentamos en esta nueva era son los ataques que pueden llegar a tomar el control de los dispositivos que utilizamos. Los cuales después de un ataque aprovechando una posible vulnerabilidad son controlados por terceros en forma remota. Pongamos el caso que un atacante consigue controlar nuestra heladera, horno, lavadora o incluso como ya ha ocurrido en algunos casos, nuestro automóvil. Este control remoto de estos dispositivos por parte de un tercero que quisiera podría afectar a la seguridad e integridad física de sus usuarios.

2.C. Auditoria de vulnerabilidades

Como ya se mencionó en reiteradas ocasiones, la primera barrera de seguridad son los empleados de la empresa por ello es recomendable realizar una Auditoria para conocer el nivel de capacitación de los usuarios en cuanto a ciberseguridad y también determinar si se debe realizar una capacitación y en qué puntos se debe enfatizar.

Por ejemplo, el departamento de IT o bien se puede contratar una externa para que lo realice, puede enviar correos de spam y phishing engañando al usuario para que haga clic en un enlace y se descargue un programa o lo redireccione a una página falsa en la cual solo se contabilizaría cuantos usuarios han caído en el engaño. De esta manera se puede conocer el nivel de ciberseguridad y tomar medidas al respecto.

2.D. Mecanismos de autenticación

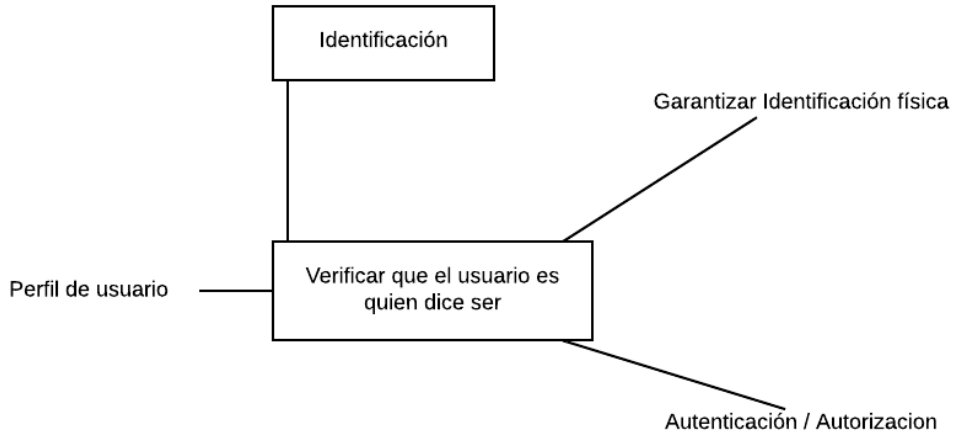
Cuando hablamos de protección de sistemas, servicios y aplicaciones, siempre se establecen 3 categorías en las que se encuentran distintas soluciones que combinadas permiten ofrecer garantías de operación, es decir disponibilidad y asegurar la integridad y confidencialidad de la información que se genere o se intercambie. Estas 3 categorías son Autenticación, Autorización, y Auditoria, conocidas también como las tres “A”.

Es importante destacar que estas 3 categorías no son independientes, la autenticación y los mecanismos que se dispongan para garantizarla permite identificar a la persona que va a interactuar con el sistema. Esta autenticación es fundamental para determinar, de acuerdo con la identidad de quien este solicitando el acceso a un recurso determinado, con que privilegio se le otorga el acceso.

Durante los procesos de autenticación y autorización, y a medida que la persona solicita un recurso, ya convertido en usuario, interactúa con el sistema es necesario definir estrategias que permitan establecer la trazabilidad de la interacción para que en caso de ser necesario auditar la actividad del usuario. Se puede decir entonces que la protección de un sistema inicia con la autenticación de quien va a solicitar un recurso e interactuar con él.

Existen distintos tipos de mecanismos que permiten la autenticación del usuario, estas alternativas están íntimamente relacionadas con las soluciones de autorización.

Ilustración 2 Identificación de usuario

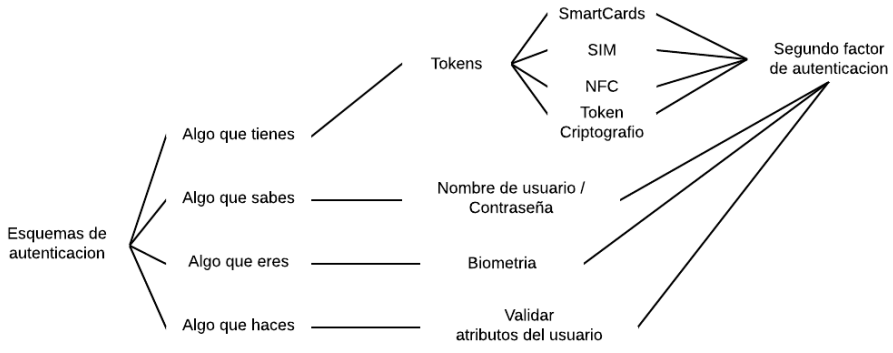


***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Al margen de las estrategias que se construyan para integrar los aspectos que permitan identificar a un individuo como usuario del sistema, es importante determinar qué información vamos a exigirle para demostrar que es quien dice ser. Para esto existen cuatro alternativas:

1- Exigir al usuario que proporcione algo que debe conocer
2- Exigir al usuario que proporcione algo que debe poseer
3- Registrar aspectos biométricos que solo este individuo posee
4- O registrar aspectos que definen su comportamiento y las cosas que hace

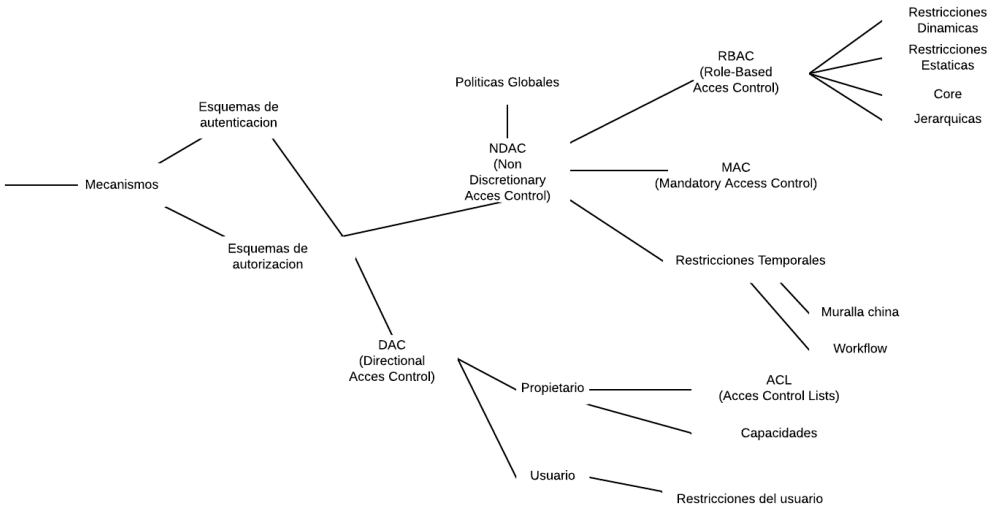
Ilustración 3 Esquemas de autenticación



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Elegir una alternativa u otra depende de ciertos factores, por un lado, el riesgo que se ha definido a partir de la criticidad que tiene el recurso al que durante la fase de autorización se va a dar acceso. Por otro lado, la complejidad de la integración de estos mecanismos, la precisión y la tasa de falsos negativos, la facilidad de uso de los mecanismos y la universalidad de las soluciones y la obligatoriedad de cumplir con la regulación específica.

Ilustración 4 Esquemas de autorización



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Se proponen muchos esquemas combinados de seguridad, que dan al usuario la sensación de que lo que está en riesgo son los sistemas de las organizaciones con las que interactúan y que ellos deben seguir complejos esquemas de autenticación y autorización para que la seguridad de estos sistemas no esté comprometida.

Todas las alternativas confían en los principios de la criptografía para garantizar la identificación de los sujetos mediante la posesión de una clave criptográfica. Esta clave puede generarse de forma sintética o a partir de los rasgos biométricos de los usuarios. A partir de esta clave es posible construir una serie de servicios criptográficos que sustentan cualquier proceso de autenticación. Además, la clave puede ser única o venir acompañada de una segunda clave complementaria que resuelve el intercambio de la primera clave.

2.E. Ciberseguridad en entornos móviles y BYOD (Bring Your Own Device)

La tecnología más avanzada ya no está solo en las empresas, sino que es propiedad de los empleados, en sus casas tienen la última tecnología en computadoras, en celulares, la conexión a internet con alto ancho de banda, más Gb de almacenamiento, correo ilimitado, videoconferencia, mensajería instantánea. Pero en la oficina en muchos casos se tiene la sensación de que se da un paso atrás y volvemos al pasado en lo que a tecnología se refiere. Este fenómeno será la tendencia más significativa que afectara a las tecnologías de información y comunicación durante los próximos 10 años y es resultado del rápido desarrollo de 4 tecnologías:

- Los denominados Smartphones.
- Internet como la plataforma ideal para la distribución de contenido multimedia
- Cloud Computing, que nos permite acceder desde cualquier lugar y cualquier dispositivo a cualquier servicio, recurso o dato que hay en la red
- Redes Sociales. La red dejo de ser un sitio donde las personas entraban solo a leer y se convirtió en un lugar donde expresarse y compartir.

Este avance se ha ido trasladando poco a poco a las empresas y organizaciones. Los empleados quieren utilizar en su entorno laboral las tecnologías como dispositivos, servicios y aplicaciones, que están utilizando en su vida personal y con las que se sienten más productivos.

Esto ha dado lugar a diferentes tendencias en el entorno empresarial que están relacionadas entre sí y que normalmente son conocidas por sus siglas en ingles. La más conocido es BYOD (Bring Your Own Device) o “trae tu propio dispositivo”, hace referencia al uso de dispositivos personales como smartphones, tablets, portátiles, discos USB en el trabajo. Generalmente la denominación BYOD se utiliza para referirse a tablets y smartphones y cuando se habla de portátiles o laptops se utiliza la denominación BYOPC (Bring Your Own PC) o BYOC (Bring Your Own Computer) o también BYOL (Bring Your Own Laptop).

Por otro lado, también tenemos BYOA (Bring Your Own App) que significa “Use su propia aplicación” y es la tendencia de los usuarios a usar también en el trabajo aplicaciones móviles que usan habitualmente en su ámbito personal.

También existe BYOC (Bring Your Own Cloud) que significa utilice su propia nube, similar al anterior pero referida a los servicios cloud, los usuarios acceden a estos servicios a través de la red corporativa y almacenan información de la empresa que puede ser sensible en estos servicios cloud de consumo que normalmente no ofrecen las mismas medidas de seguridad que los servicios orientados al uso empresarial. Esto puede originar fuga de información y aunque no se produzca ningún incidente de

seguridad la empresa deja de tener control sobre donde están replicados y almacenados los datos sensibles, lo que puede llevar a un incumplimiento de las normativas de seguridad.

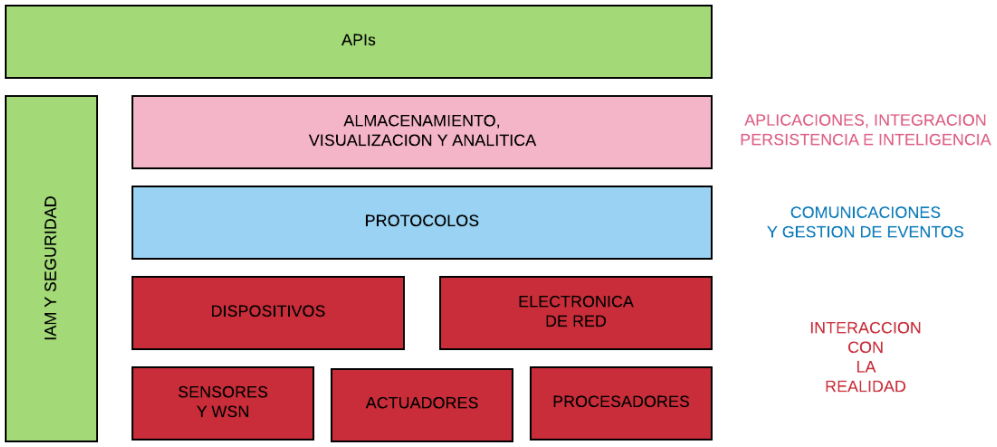
También existe BYON (Bring Your Own Network) que significas use su propia red, hace referencia a la habilidad de los usuarios de crear o acceder a redes alternativas cuando las opciones disponibles no son satisfactorias para sus propósitos. En la empresa se refiere puntualmente a la capacidad de los usuarios de crear redes de área personal, las denominadas PAN (Personal Área Networks) o redes AD-HOC como la alternativa a una red corporativa. Los usuarios crean sus propios puntos de acceso Wireless utilizando su dispositivo móvil como modem para dar acceso a internet a otros dispositivos a los que se conectan vía bluetooth. Los empleados pueden crear también puntos de acceso utilizando dispositivos MIFI, que son dispositivos portátiles de banda ancha que permiten compartir conexiones 3g o 4g a múltiples usuarios o dispositivos. En algunas organizaciones los empleados utilizan BYON para acceder a redes sociales, web de comercio electrónico o juegos online que los administradores de la red corporativo bloquearon. Los problemas surgen porque una vez que se ha creado esta red AD-HOC sin ningún tipo de seguridad ni monitorización los empleados usan esa conexión para acceder a las aplicaciones corporativas, esto puede causar la fuga de información sensible o la entrada de malware a la red corporativa.

También existe el BYOT (Bring Your Own Technology) que significa “Utilice su propia tecnología” que podría decirse que incluye todas las anteriores.

2.F. Internet of Things Segura

Se considera que la arquitectura de IoT presenta 3 capas. La primera interactúa con el mundo físico y se compone principalmente de sensores, controladores, actuadores y distintos tipos de procesadores, pero también de dispositivos de electrónica de red que permite que el mundo físico se comunique con el resto de capaz de la arquitectura. La segunda, inmediatamente por encima, proporciona las capacidades de comunicación y de gestión de eventos, es la capa de internet of things en sí misma. Y la tercera es la web of things, estrechamente relacionada con cloud computing, que proporciona almacenamiento, visualización, analítica y las API’s que permiten desarrollar todo tipo de aplicaciones para los usuarios finales.

Ilustración 5 IoT segura



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Todas estas capaz tienen sus propias necesidades en cuanto a la gestión de identidades, el control de acceso y la seguridad.

2.G. Análisis de Casos Reales ciber ataques

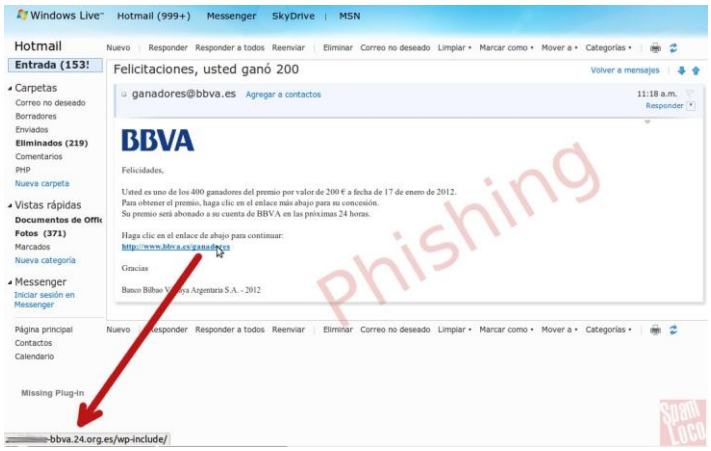
A continuación, se presentan algunas maneras de operar por medio de ejemplos. El primer caso que se analiza a continuación se trata de un caso de *scamming*. Este término hace referencia a una metodología de ataque en la cual la victima accede a una página *web* fraudulenta e idéntica a la real, por ejemplo, de alguna red social como ser *Facebook* o como en el ejemplo que veremos la página web de un banco, y de manera inconsciente ingresa sus datos brindándole información al atacante.

Caso 1 - Típico *phishing* bancario, el cual empieza a partir de un mail falso que simula ser enviado por el banco con el fin de obtener los datos de la cuenta para realizar una transferencia a su cuenta (robar dinero), realizar compras online, o bien obtener información para cometer otros delitos como secuestros virtuales, etc.

En este primer caso, se intenta engañar a los clientes de un banco con un supuesto premio de 200 *EUROS* que serían transferidos a la cuenta.

Al posar el mouse sobre el enlace, se puede ver que el destino no es la página del banco, sino una dirección ***url*** bastante particular. Las víctimas al acceder se encuentran con un diseño similar al real para que no sospechen e ingrese sus datos bancarios. Esto se puede observar en las imágenes que se presentan a continuación.

Ilustración 6 : Correo Phishing BBVA.



Fuente: Ok Diario - https://okdiario.com/tecnologia/consejos-evitar-ser-victima-phishing-2588488/2

Ilustración 7 URL falsa BBVA

Fuente: Pablo Teijeira's blog - https://pabloteijeira.wordpress.com/2012/01/18/alerta-de-phising-bbva/

Una vez que se ingresa un usuario y contraseña los estafadores también solicitan la información de la tarjeta con la excusa de que el dinero será cargo en un determinado tiempo, distraen a la persona de la realidad por medio de palabras que desvían su atención, al decirle que va a obtener dinero gratis, algo muy atractivo para ser real. Esto es parte de lo que llamamos Ingeniería Social.

Ilustración 8 : Datos de tarjeta de crédito

Fuente: Pablo Teijeira's blog - https://pabloteijeira.wordpress.com/2012/01/18/alerta-de-phising-bbva/

Una característica que cabe destacar es que en todas las capturas las URL's en el navegador no son las del banco y tampoco incluyen HTTPS. Estas son dos señales claras de que algo raro ocurre.

Como se mencionaba, es muy importante la ingeniería social que utilizan para engañar al usuario ¿a quién no le gustaría recibir 200 *EUROS* de regalo sin hacer nada más que brindar información? Pero esta información es cara y vale más de 200 *EUROS.* Muchos al recibir un correo de este tipo no durarían un segundo en ingresar sus datos, sea por la emoción de haber sido elegido entre tantas personas o por desconocer estas metodologías.

2.H. Impacto del hurto de información sensible

Es importante conocer los distintos dispositivos IOT que se utilizan en un centro médico para entender la vulnerabilidad de estos y así también el impacto que pueden tener cada uno de ellos.

En primera instancia existen dispositivos portátiles como ser una bomba de insulina o un marcapasos, un ataque contra estos dispositivos podría utilizarse para chantajear al paciente amenazándolo con hacerlo dejar de funcionar.

Existen maquinas como dispensadores de farmacia inteligentes o estaciones de quimioterapia, en estos casos el atacante puede atentar directamente contra la vida de las personas. También pueden alterarse los datos que sirven a los médicos para hacer ajustes en el funcionamiento de los dispositivos y de esta forma provocar un error en los ajustes realizados por el personal médico.

Imagínense que un atacante tiene acceso a la historia clínica de un paciente, dicha historia clínica puede alterarse y atentar en distintas formas ante la salud de esa persona. Si por ejemplo se tiene que intervenir quirúrgicamente a un paciente para extirparle un órgano como ser el apéndice y se modifica por otro órgano como por ejemplo el hígado, a dicho paciente se le extirpara otro órgano, se hará una mala praxis y por lo tanto seguirá con el apéndice en malas condiciones lo que atentaría contra la vida del paciente. En Argentina hemos tenido casos de mala praxis por negligencia médica, como el conocido caso en el que se amputo la extremidad incorrecta a un paciente, se podría alterar la historia clínica y modificar la información logrando el mismo resultado.

Es conocido el modus operandi de las empresas farmacéuticas, las cuales en muchos casos tienen el "remedio" para una determinada enfermedad y para poder vender la cura se encargan de insertar la enfermedad en la sociedad y que se esparza cubriendo la mayor población humana posible, con el fin de aumentar ventas e ingresos. Existe la posibilidad de que estas empresas ataquen centros médicos con el fin de alterar historias clínicas de pacientes insertando una enfermedad para la cual tienen el remedio. Esto tiene un impacto gigante en la sociedad ya que causaría terror y paranoia en la población. Esto a su vez se puede causar un impacto político ya que los ciudadanos exigirían al gobierno

respuestas y soluciones ante una “epidemia”, y se pueden producir manifestaciones en las calles causando disturbios en la vía pública.

CAPITULO 3

3. ESTUDIO DE CASO

3.A. Descripción de la unidad de estudio

Se tomo como caso de estudio una institución de Salta Capital dedicada al estudio de tomografías computadas y resonancias magnéticas, el cual cuenta con equipos inteligentes para realizar dichos estudios mediante computadoras con aplicativos específicos de los equipos.

La información brindada por el fabricante del equipo a sus clientes es casi nula para mantener la seguridad, la cual es una decisión acertada.

El acceso a la configuración del equipo está bloqueado por el fabricante. Solo ellos tienen acceso en caso de ocurrir algún problema.

3.B. Identificación y descripción de los equipos que se toman como estudio de caso

Equipos para técnicos

- Equipos de grado medico: tomógrafo y resonador.
- Una (1) Computadoras con sistemas operativo Windows 10

Equipos para médicos

- Dos (2) Notebooks con sistema operativo Windows 10

Equipos para personal de Tipeo/Transcripción

- Una (1) Computadoras con sistema operativo Windows 10

Equipos para personal de recepción

- Una (1) Computadoras con sistema operativo Windows 10

Equipo de sistemas

- Dos (2) Computadoras con sistema operativo Windows 10
- Un (1) Servidor con sistema operativo Windows Server 2016

Equipos tesorería y contabilidad

- Cuatro (4) Computadoras con sistema operativo Windows 10. Aplicativos de contabilidad y Tesorería.

Equipos facturación

- Tres (3) Computadoras con sistema operativo Windows 10. Aplicativos de facturación, cobros y gestión de obras sociales

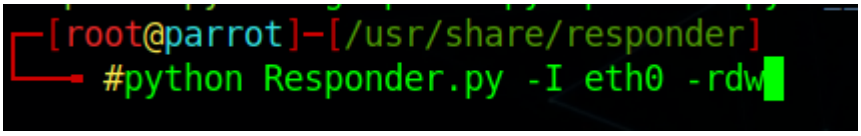
3.C. Identificación de las vulnerabilidades

Es común encontrar en entornos empresariales carpetas compartidas desde un servidor a los equipos pertenecientes al dominio y a los usuarios para de esta manera compartir archivos y múltiples usuarios poder trabajar sobre el mismo.

Hemos utilizado un envenenador de tráfico LLMNR, NBT-NS y MDNS, esta herramienta responde a solicitud del servicio de archivos. Esta es una herramienta de Linux que ya suele venir en sistemas diseñados para auditoria y seguridad informática.

Ejecutamos la herramienta

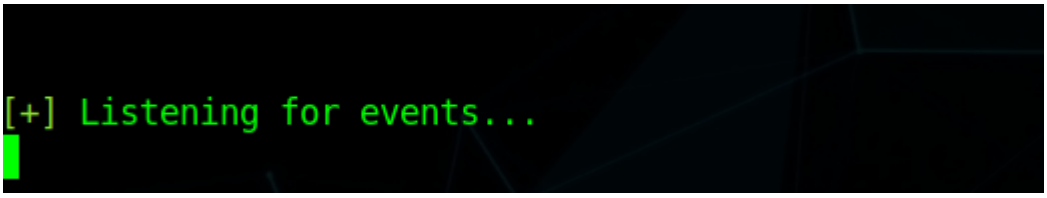
Ilustración 9 Responder .py



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Mientras esta herramienta está esperando silenciosamente que ocurran "eventos", en todo el entorno Windows no se ve absolutamente nada, es decir que los usuarios no se dan cuenta del ataque.

Ilustración 10 : Escuchando eventos



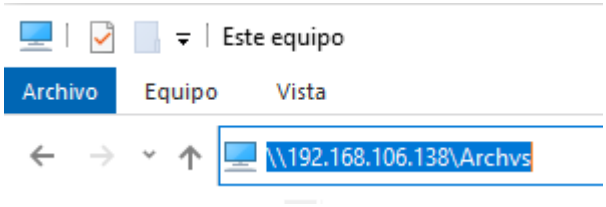
***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Es normal que a nivel de red algunos equipos accedan de forma automatizada a recursos compartidos, entre otras cosas, de otros equipos. Es común que ciertos recursos dejen de existir, es decir que se eliminen o bien que cambien de nombre, por lo tanto, las consultas hacia esos recursos no resuelven a ningún lado. Aquí entra la herramienta, por ejemplo, si un equipo intenta acceder a una carpeta compartida que cambio el nombre,

no se la encuentra, y aquí entra la herramienta. El equipo le pide el Controlador de Dominios (DC) que le pase la ruta de este recurso, el DC responde que no conoce el recurso solicitado, aquí entra la herramienta en la comunicación diciéndole que ella sabe dónde está el recurso. Pero para pasarle la información solicitada primero pide que le pase el hash NTLMv2, que luego se puede crackear o desencriptar y utilizar para comprometer el equipo.

En este caso buscamos un recurso tipiando el nombre mal a propósito a modo de ejemplo

Ilustración 11 Acceso a carpeta compartida



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

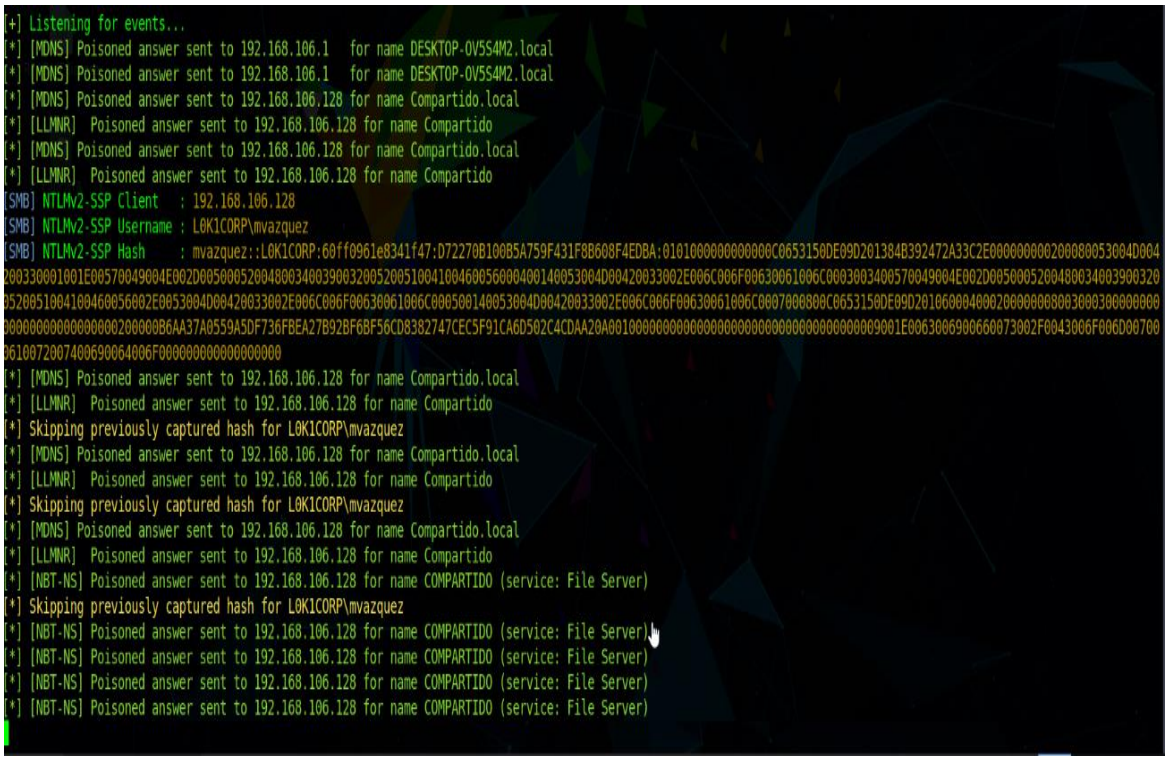
Se puede ver cómo mientras el equipo busca un recurso compartido en la red, por detrás ya fue "envenenado".

Ilustración 12 Envenenado

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Si dejamos un tiempo corto la herramienta intercepta muchísimos Hashes como se puede ver en las imágenes, de hecho, intercepta muchas veces el mismo hash y se lo saltea por el hecho de ya tenerlo guardado en un log.

Ilustración 13 Hashes interceptados



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

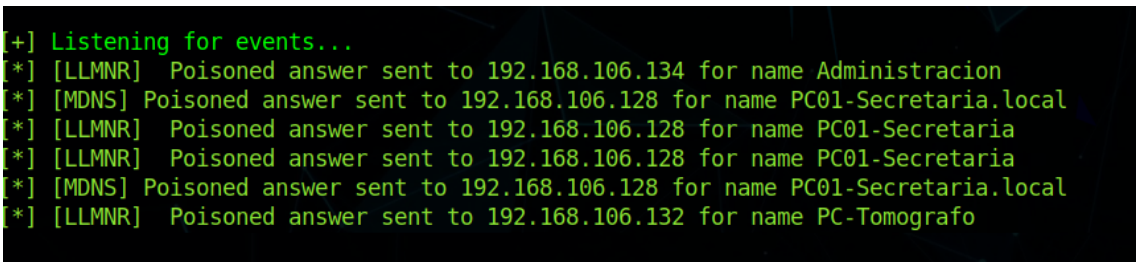
Al desplegar este ataque se intercepta una gran cantidad de hashes, en esta ocasión fue poco el tiempo desplegado del ataque, si el tiempo fuera mayor, seria una lluvia de hashes interceptados.

Ilustración 14 Muchos hashes

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Se puede observar que intercepto la comunicación de 3 equipos diferentes. Administración, PC01-Secretaria y PC-Tomógrafo, y tenemos la ip de cada equipo. Con lo cual ya tenemos mucha información ya que los nombres son descriptivos. Lo mismo pasaría si el servidor de base de datos busca conectarse con el DC y el servidor tendría un nombre como por ejemplo “DataBase”, lo cual se encuentra frecuentemente

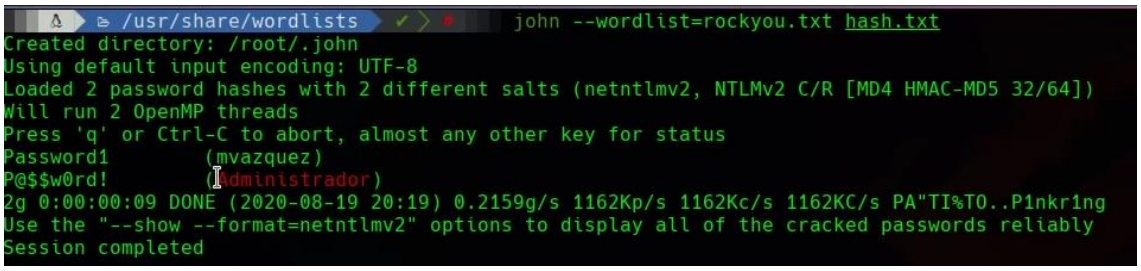
Ilustración 15 Respuestas enviadas



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Se puede observar que una vez interceptado el hash de los usuarios es posible crackear o desencriptar el hash para tener la contraseña propiamente dicha y con ella realizar múltiples variantes de ataques a la entidad. Incluso se pueden realizar ataques sin desencriptarla la contraseña, solo con el hash lo cual es mucho más crítico.

Ilustración 16 Usuarios hackeados



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

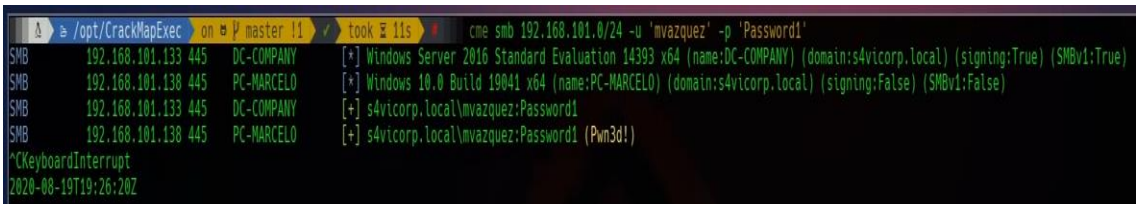
Con las credenciales obtenidas se puede hacer escanear sobre la red los equipos disponibles y sobre los cuales se tienen Permisos de administrador. Con el usuario mvazquez no tenemos permisos de administrador ya que es un usuario general del dominio, el usuario Administrador nos muestra la palabra “Pwn3d!” porque al ser usuario administrador tiene total control sobre los equipos.

Ilustración 17 Pwn3d!

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

En muchas ocasiones el usuario del dominio también es usuario local de un equipo, y este usuario local es administrador, esta es una mala práctica común que se da en muchas ocasiones en entornos empresariales. En este caso encontramos que el usuario mvazquez es también usuario local y a su vez Administrador en el equipo “PC-MARCELO”.

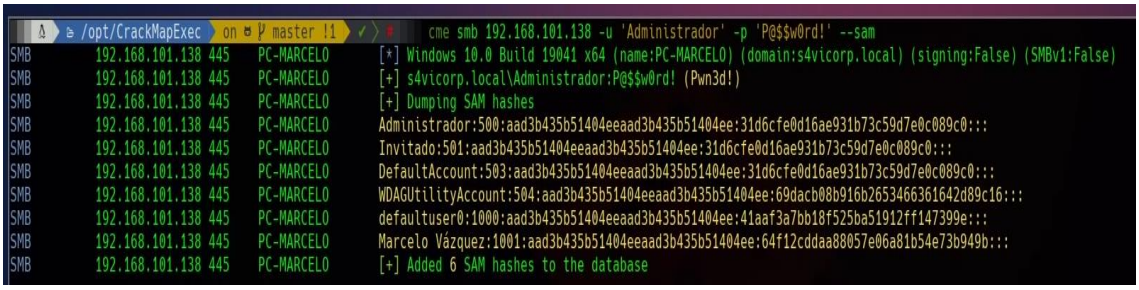
Ilustración 18 Contraseñas crackeadas



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Al tener ya credenciales de acceso de usuario administrador utilizando otra utilidad llamada “CrackMapExec”, se puede listar los hashes SAM de un determinado equipo a nivel local y utilizarlo para autenticarse en la maquina utilizando un concepto llamado ‘path the hash’ el cual permite loguearse sin necesidad de conocer la contraseña en forma explícita.

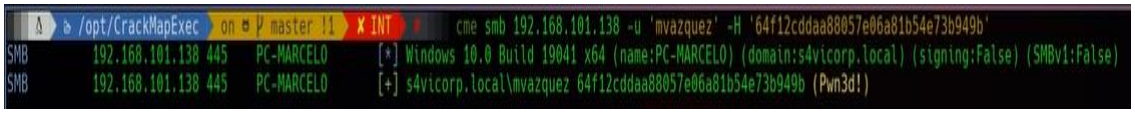
Ilustración 19 Usando el hash



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Podemos observar que si pasamos al usuario “mvazquez” el hash directamente nos muestra el mensaje “Pwn3d!”

Ilustración 20 Acceso con hash



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

De esta manera también se puede obtener el listado de hashes sam.

Ilustración 21 Lisado Hash

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

De la misma forma se puede obtener una consola interactiva del equipo que estamos atacando, lo cual es muy interesante ya que por medio de la consola tenemos el equipo a nuestra merced. Si llegamos a un equipo importante, como por ejemplo el servidor de la base de datos, se puede tener acceso a ella, realizar un backup de la base de datos y

copiarlo en una ruta a la cual podemos acceder y traerlo a nuestro equipo, editarlo y luego volverlo a cargar con datos modificados, por ejemplo. En este caso el equipo que está conectado al equipo es el que tiene la base de datos.

Todo esto se puede realizar con herramientas que ya se encuentran desarrolladas en internet, si se trabaja más en profundidad en un ataque se pueden obtener resultados asombrosos.

Se utilizo la herramienta llamada "rpcenum" la cual se encuentra disponible en internet y a la que se le modifico porción del código para poder utilizarla y recopilar información del Dominio. Se inserta el usuario y contraseña crackeados previamente, que se utilizara para recopilar la información.

Ilustración 22 Rpcenum

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

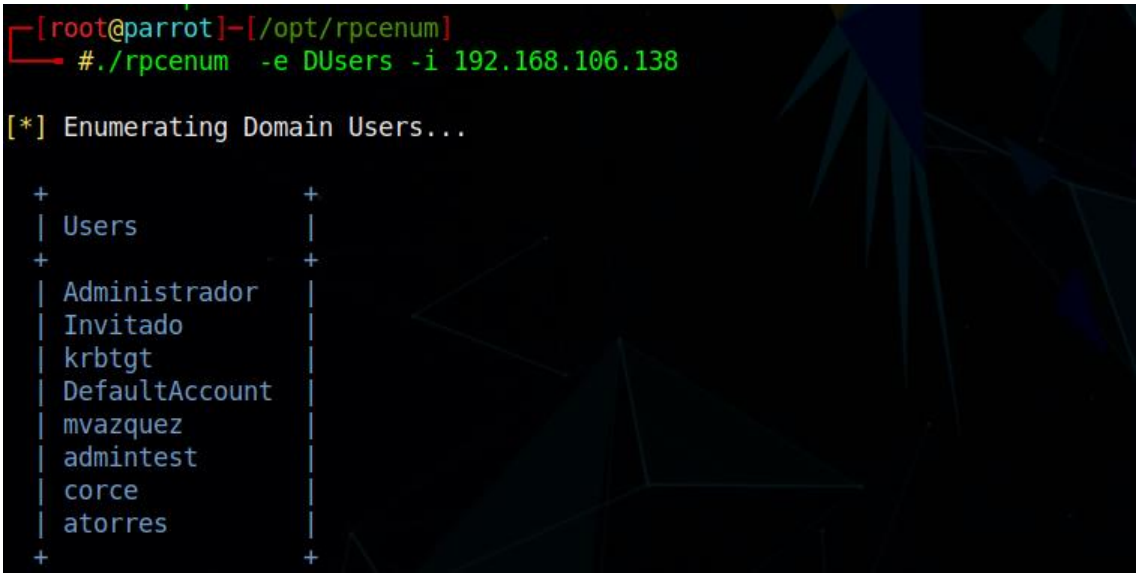
En la imagen que sigue se puede ver que el programita tiene un menú básico

Ilustración 23 Menú rpcenum

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Si corremos la herramienta con las credenciales de acceso de un usuario administrador sobre la dirección IP del servidor de dominios, obtenemos la lista de todos los usuarios del dominio como se puede ver.

Ilustración 24 usuarios del dominio



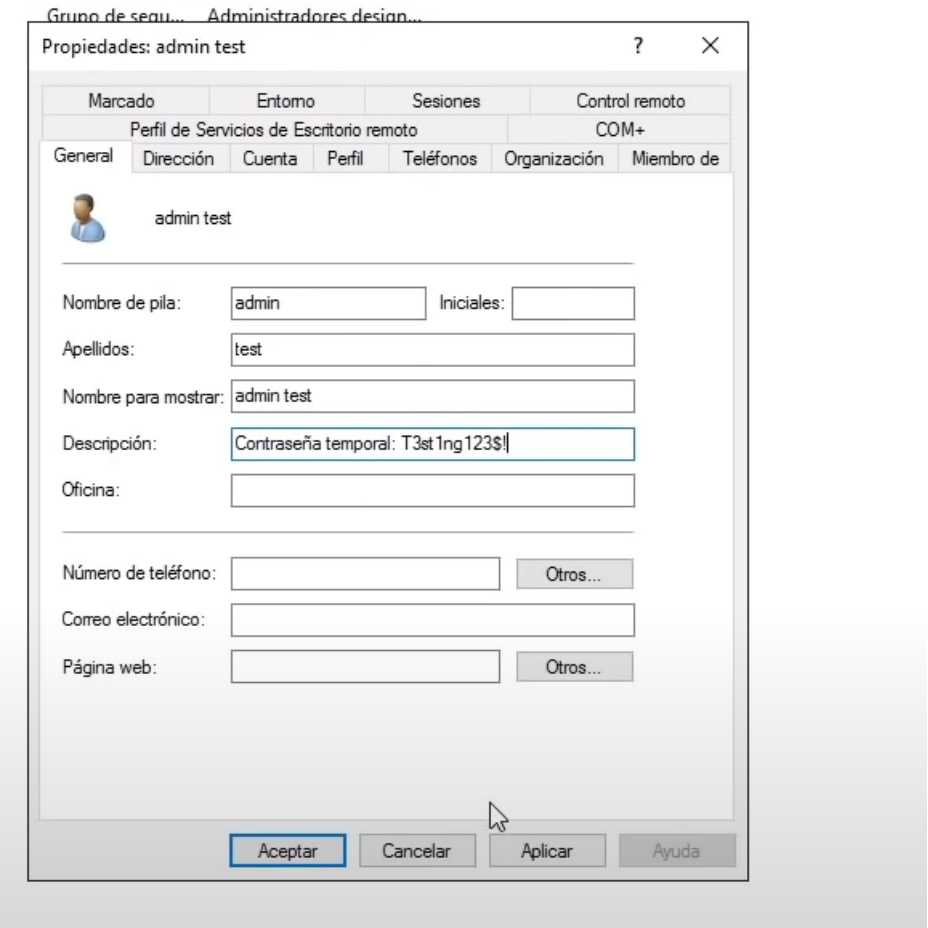
***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

También se puede leer la descripción de cada usuario en donde en muchos casos podemos encontrar información importante. Algo que podríamos encontrar y que los administradores del dominio hacen como mala práctica, es grabar en la descripción del usuario información crítica como contraseñas.

En este caso lo hicimos a propósito a modo de ejemplo, se creó el usuario “admintest” y en la descripción se grabó la contraseña temporal.

Esta también es una forma de identificar como atacante usuarios potenciales o bien que tareas realiza cada usuario.

Ilustración 25 Propiedades de usuario de dominio



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

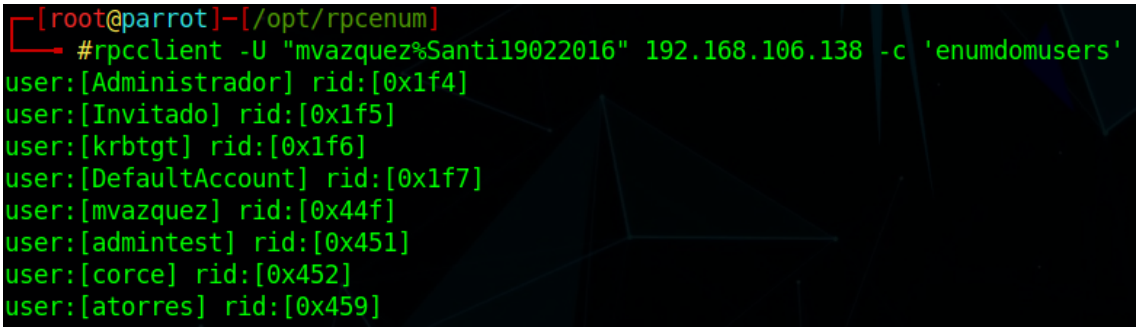
Luego ejecutamos la herramienta solicitando la información de los usuarios y se puede leer la descripción con la contraseña.

Ilustración 26 Descripción desde rpcenum.

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Se puede recopilar información de los usuarios también con una cuenta sin privilegios de administrador y como se ve a continuación listar los usuarios del dominio

Ilustración 27 Recopilación desde cuenta sin privilegios

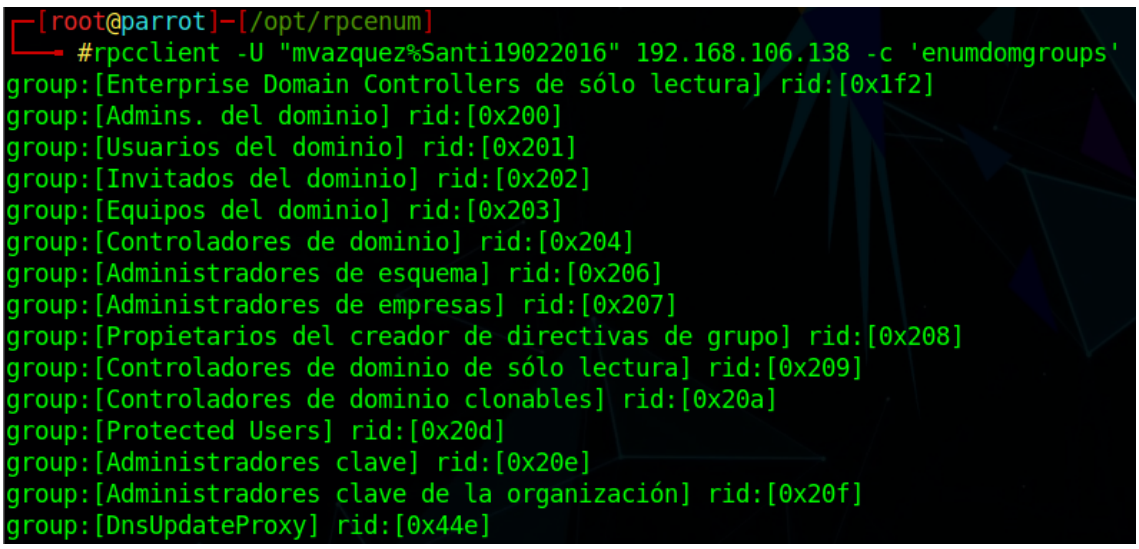


***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

A los atacantes les interesa es interceptar hashes de usuarios administradores del dominio, con esta herramienta se puede identificar rápidamente que usuarios tienen privilegios de administrador en el dominio.

Esto se realiza con el comando “enumdomgroups” el cual despliega una lista con los grupos que existen en el dominio. Cada grupo está identificado por RID, en este caso se ve que los admins del dominio es 0x200.

Ilustración 28 Grupos del dominio



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Con el RID obtenido se puede filtrar a los usuarios que son miembros de ese grupo

Ilustración 29 Usuarios miembros de grupo

```
┌─[root@parrot]─[/opt/rpcenum]
└──╼ #rpcclient -U "mvazquez%Santi19022016" 192.168.106.138 -c 'querygroupmem 0x200'
        rid:[0x1f4] attr:[0x7]
        rid:[0x451] attr:[0x7]
```

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Si se ejecuta "queryuser" con uno de los id obtenidos pertenecientes al grupo de administradores, obtenemos la información de dicho usuario, en este caso el usuario "Administrador"

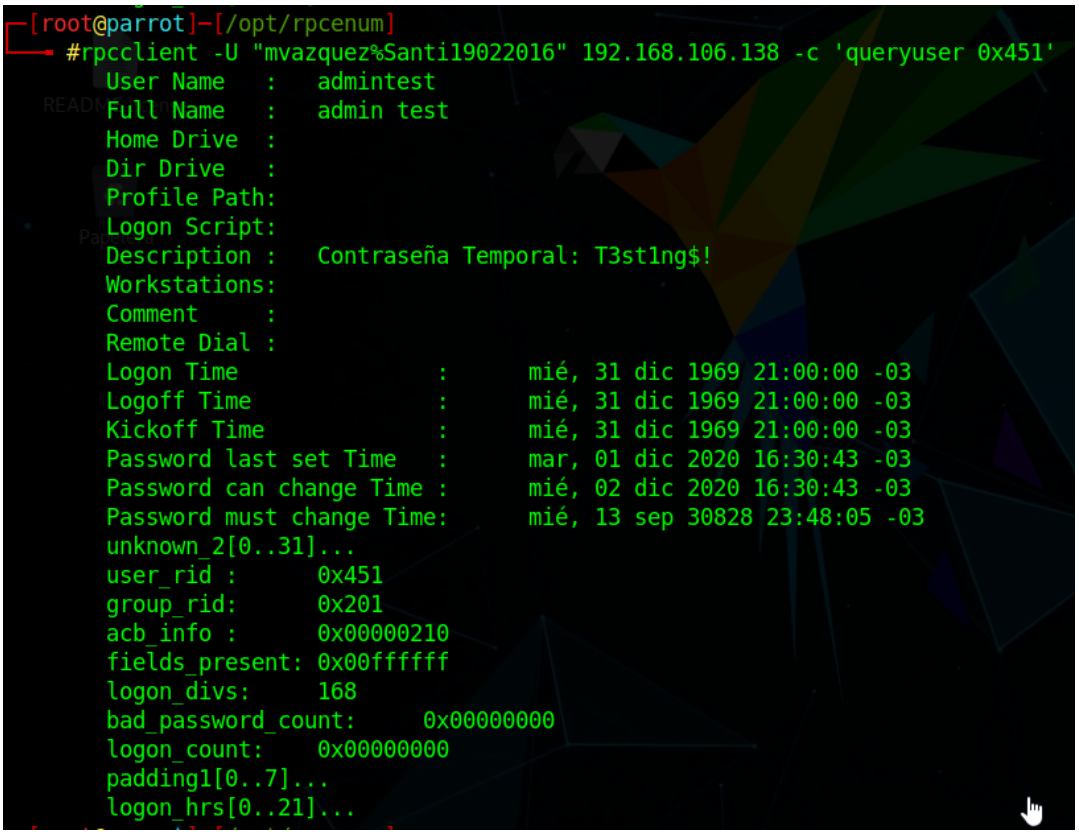
Ilustración 30 : Información de usuario

```
┌─[✗]─[root@parrot]─[/opt/rpcenum]
└──╼ #rpcclient -U "mvazquez%Santi19022016" 192.168.106.138 -c 'queryuser 0x1f4'
        User Name   :   Administrador
        Full Name   :
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :   Cuenta integrada para la administración del equipo o dominio
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time               :      jue, 25 feb 2021 21:21:01 -03
        Logoff Time              :      mié, 31 dic 1969 21:00:00 -03
        Kickoff Time             :      mié, 31 dic 1969 21:00:00 -03
        Password last set Time   :      dom, 21 feb 2021 19:58:07 -03
        Password can change Time :      lun, 22 feb 2021 19:58:07 -03
        Password must change Time:      dom, 04 abr 2021 19:58:07 -03
        unknown_2[0..31]...
        user_rid :      0x1f4
        group_rid:      0x201
        acb_info :      0x00000010
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000002
        logon_count:    0x0000004f
        padding1[0..7]...
        logon_hrs[0..21]...
```

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Si ejecutamos la misma consulta con el otro usuario miembro del grupo de administradores obtenidos, recuperamos la informacion del usuario de prueba “admintest” y tambien vemos la descripcion con la contraseña temporal.

Ilustración 31 Información completa de usuario

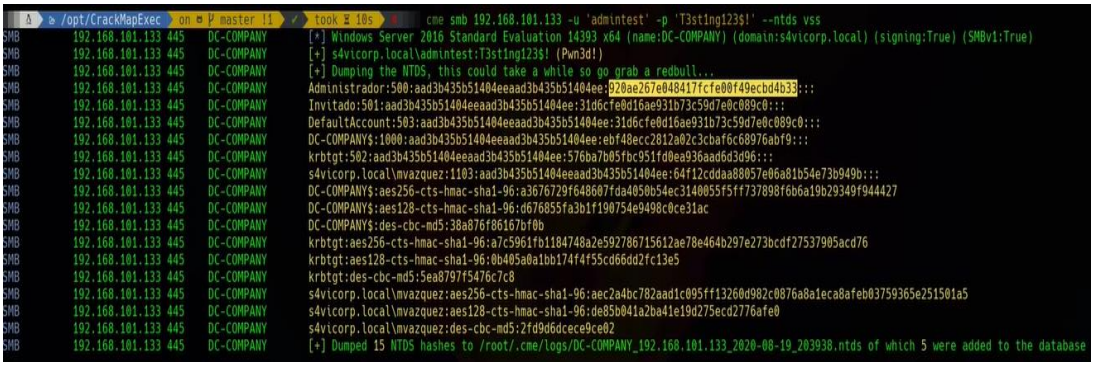


***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

El atacante al obtener la credencial de un usuario administrador del dominio puede utilizarla para listar el VSS, entre otras cosas esto va a listar los hashes NTLM de todos los usuarios a nivel de Dominio y con estos hashes se podría ejecutar una consola en cualquier equipo del dominio sin que el usuario lo detecte.

Entonces, con la cuenta “admintest” obtenemos el hash del usuario “Administrador”.

Ilustración 32 : Hash de usuario administrador



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

A continuación, con el hash obtenido ejecutamos la consola, en la que se puede ver que estamos logueados con el usuario “administrador”.

Ilustración 33 Usuario logueado

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

A modo de ejemplo, ejecutamos el comando ipconfig para mostrar que estamos realmente en la consola.

Ilustración 34 : ipconfig en consola

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

CAPITULO 4

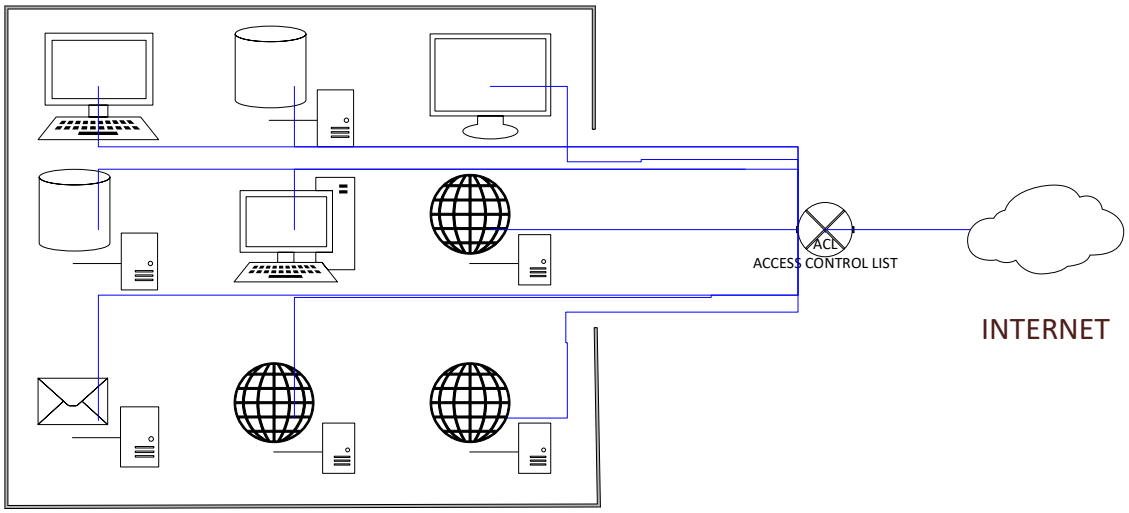
4. PROPUESTA DE SOLUCIONES

Teniendo en cuenta las vulnerabilidades detectadas en los equipos IoT, tomados como estudio de caso, en el capítulo anterior, se propone el uso de herramientas como método de seguridad en los equipos vinculados al sistema de la institución. Cabe destacar, que las propuestas que se expondrán a continuación pueden ser aplicables en cualquier empresa u organismo que tengan similares problemas de seguridad

4.A. Firewall

La defensa frente a los ataques externos inicia en el perímetro de las instalaciones, con seguridad, lo que se puede afirmar es que todos los accesos sean por una única puerta. De esta forma la red, con sus servidores, base de datos, estaciones de trabajo, etc. tendrían un único router frontera que conecten la red con el exterior (internet).

Ilustración 35 Router Frontera



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Este router de frontera será nuestra primera línea de defensa donde podremos realizar el primer filtrado de paquetes empleando el denominado ACL (Access Control List). Que son una serie de reglas que definen que tráfico se permite y que tráfico se deniega. Este trabajo de filtrado de paquetes lo realiza el Firewall, que es un hardware o software dedicado específicamente a la tarea de control de los paquetes que pasan por el para decidir si siguen o no su camino. El firewall más simple es el filtro de paquetes que sigue el esquema de lista de reglas ACL inspeccionando las cabeceras de los paquetes a nivel de red (puerto, dirección ip, etc.) para decidir si pasan o no. Por ejemplo, si quisiéramos bloquear el uso de un determinado servicio, se agregan reglas al firewall bloqueando el tráfico con origen o destino al puerto de ese servicio.

Ilustración 36 Filtro de paquetes

Regla	Acción	IP Origen	IP Destino	Puerto Origen	Puerto Destino	Protocolo
1	Aceptar	192.168.1.2	213.145.2.2	-	25 (SMTP)	TCP
2	Aceptar	192.168.1.0/24	-	-	80(HTTP)	TCP
3	Aceptar	-	192.168.7	-	80(HTTP)	TCP

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

De todos modos, la mejor opción es bloquear por defecto todo el tráfico e ir añadiendo reglas para permitir únicamente los que se necesiten o deseen.

Ilustración 37 Filtro de paquetes bloqueado

Regla	Acción	IP Origen	IP Destino	Puerto Origen	Puerto Destino	Protocolo
1	Aceptar	192.168.1.2	213.145.2.2	-	25 (SMTP)	TCP
2	Aceptar	192.168.1.0/24	-	-	80(HTTP)	TCP
3	Aceptar	-	192.168.7	-	80(HTTP)	TCP

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

A estos firewalls se les agrego la posibilidad de añadir reglas complejas a la lista de forma dinámica según el contexto de la conexión a nivel de transporte, como por ej.

comprobar si el paquete examinado pertenece o no a una sesión que este abierta en ese momento. Por lo que se denominaron Firewalls dinámicos o Stateful Packet Inspection (SPI).

Por último, tenemos los Firewall DPI (Deep Packet Inspection), que como su nombre lo indica, realiza una inspección mucho más profunda o minuciosa de los paquetes que atraviesan el firewall examinando los datos a nivel de aplicación, pudiendo así detectar troyanos, spyware, malware, etc.

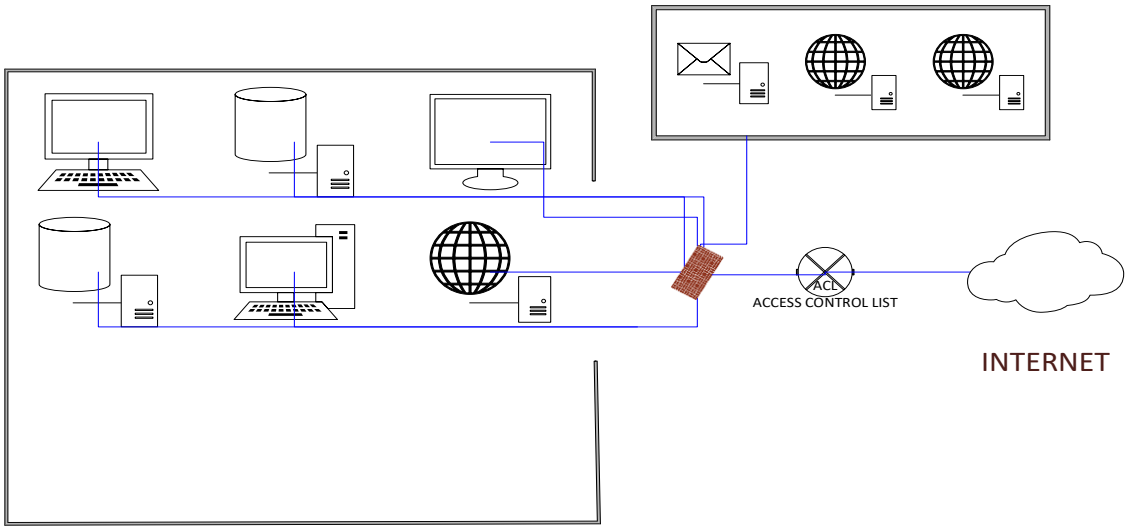
Otra opción que se suele manejar es el Firewall PROXY o aplication Gateway, que son máquinas que hacen de intermediarias entre la red interna y externa. También se denominan DUAL HOMED por estar presentes en ambas redes, de forma que examina y registra todo el tráfico de salida y entrada. Así, si un usuario de la red interna quisiera utilizar determinados servicios deberá solicitarlos al proxy, y este será el encargado de realizar las peticiones y devolverlas al usuario. Por ej. Si un usuario quisiera navegar en determinada página, tendrá que solicitarlos al proxy y este hará las peticiones de página web y se las devuelve. Esto permite el control del uso estos servicios dado que al pasar todos por el PROXY se puede llevar un registro, o bloquear usos indebidos como navegar en redes sociales o páginas de pornografía. Otra ventaja del PROXY es que se puede hacer un filtrado a nivel de aplicación evitando contenido malicioso o *respuestas mal formadas*, que de esta forma no llegaran a nuestra red interna. El principal inconveniente es el posible cuello de botella y disminución del rendimiento de estos servicios que pasan por el PROXY.

Tanto el PROXY como los demás Firewalls y router frontera son máquinas que se encuentran fuera de nuestra red y por lo tanto expuestas a ataques. A estas máquinas se las denomina NODOS BASTION y se debe tener especial cuidado en su configuración asegurándola lo mejor posible, con un sistema operativo actualizado y seguro, eliminando aplicaciones, protocolos y puertos innecesarios, y con todas las medidas de seguridad y actualizaciones posibles.

Otro servicio básico de cualquier organización que además son los que están más expuestos a ataques porque deben ser accesibles desde el exterior son el servicio web, el

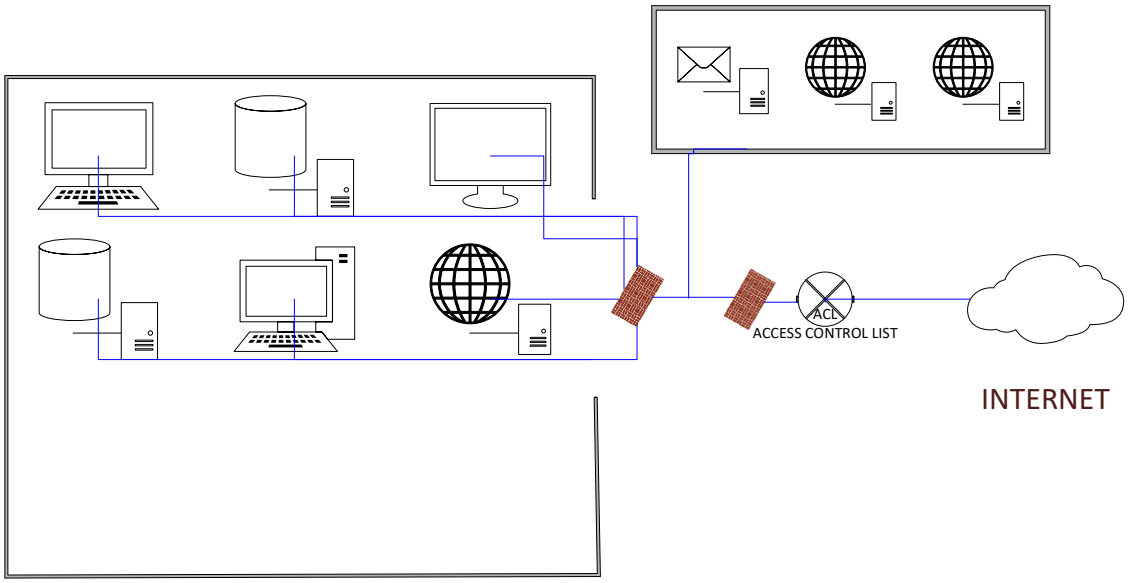
correo electrónico, DNS, etc. Estos servicios se deben proteger con un firewall pero deben seguir siendo accesibles y por lo tanto vulnerables, por lo que tampoco es óptimo que estén dentro de la red interna. Esto los sitúa en un terreno entre la red interna y la red externa, que se suele denominar zona desmilitarizada (DMZ). Según la configuración que elijamos, con un firewall seria Three-legs, con dos firewalls seria front-end. Serán estos los encargados de proteger tanto a estos equipos de las amenazas externas como a la red interna de las posibles intrusiones dentro de estos equipos tan expuestos

Ilustración 38 Zona desmilitarizada



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Ilustración 39 : Dos Firewalls



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

4.B. Segmentación de redes

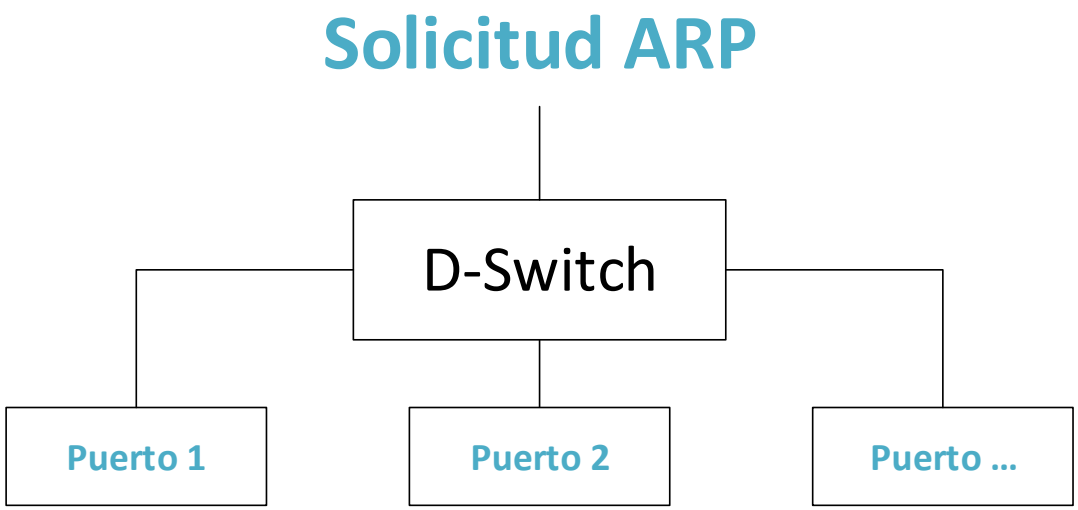
Si tenemos una red con una estructura plana, todos los dispositivos se verían entre sí, por lo que un atacante tendría acceso a todos los equipos una vez que ingreso a nuestra red, entre estos todos los servidores. La segmentación mediante redes de área local virtuales (vlan) permitirá entre otras cosas la segmentación del dominio, reduciendo el área de visibilidad de cada zona, la separación de protocolos, limitando el tráfico en cada segmento, o la movilidad de los usuarios, si se le asigna una vlan determinada a un usuario, siempre se conectará a ella independientemente de la localización física del usuario.

Para configurar las vlan se utilizan switches, que son dispositivos de conexión de red a nivel de enlace de la capa 2, que se basa en el estándar IEEE802.1Q, los denominados Q-switches para separar tráfico de una sub-lan y otra. A diferencia de utilizar los switches básicos con el estándar IEEE802.1D, denominados D-switches, todos los dispositivos conectados a ellos se verán unos a otros. Cuando un dispositivo quiere conectarse con otro necesita conocer la dirección MAC de su interfaz de red, que es un valor de 48 bits único asignado a esa interfaz por el fabricante (00:3B:55:11:4A:B9). La

forma de averiguar esta dirección es mediante el protocolo ARP que permite a un equipo enviar una solicitud conocida al IP del destino, y esa solicitud la difunde el switch a toda la red, el equipo que tenga esa dirección IP responde brindando su MAC.

Por lo tanto, cuando un D-Switch recibe una solicitud ARP la difunde por todos sus puertos a excepción del puerto que la recibió y registra en su memoria la MAC de la interfaz accesible por ese puerto.

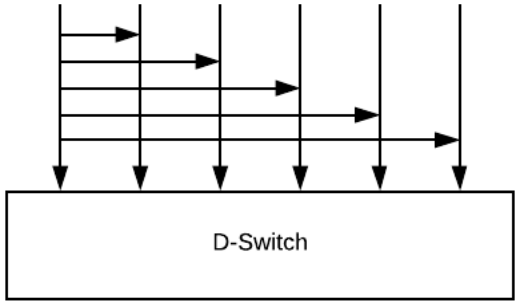
Ilustración 40 Solicitud ARP



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

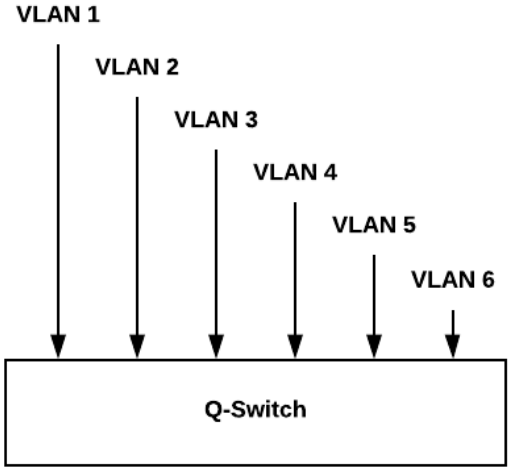
Todos los dispositivos conectados a un D-Switch están en la misma red y se pueden comunicar entre sí, en cambio sí empleamos un Q-Switch podemos segmentar la red y asignar a cada puerto del switch una vlan, de forma que se separan los dispositivos uno de otro y pueden comunicarse únicamente con los de su misma vlan.

Ilustración 41 D-Switch



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Ilustración 42 Acceso a carpeta compartida



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Las diferencias entre un D-Switch y un Q-Switch se pueden ver en la siguiente tabla

Ilustración 43 diferencias entre un D-Switch y un Q-Switch

Dirección de destino	D-switch	Q-switch
Dirección MAC conocida	1º Determinar el puerto de salida asociado con la dirección MAC destino según la tabla de del switch. 2º Si el puerto asociado de salida es diferente del de procedencia del paquete, enviar el paquete al puerto de salida. 3º Si no es así, descartar el paquete.	1º Determinar la VLAN asociada a ese paquete. 2º Si el puerto asociado de salida es diferente del de procedencia del paquete, tendrá que mirar si es miembro de la misma VLAN del paquete recibido y entonces enviar el paquete a un puerto de salida. 3º Si no es así, descartar el paquete.
Dirección MAC desconocida o broadcast	Enviar el paquete a todos los puertos excepto por el que se recibió el paquete	1° Determinar la VLAN a la que pertenece el paquete. 2° Difundir el paquete a todos los puertos de la VLAN excepto por el que se recibió el paquete

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Un D-Switch cuando le llegue un paquete con destino a una dirección MAC conocida, tendrá que:

1º Determinar el puerto de salida asociado con la dirección MAC destino según la tabla de del switch.

2º Si el puerto asociado de salida es diferente del de procedencia del paquete, enviar el paquete al puerto de salida.

3º Si no es así, descartar el paquete.

En cambio, un Q-Switch además de realizar las operaciones que hizo el D-switch:

1º Determinar la VLAN asociada a ese paquete.

2º Si el puerto asociado de salida es diferente del de procedencia del paquete, tendrá que mirar si es miembro de la misma VLAN del paquete recibido y entonces enviar el paquete a un puerto de salida.

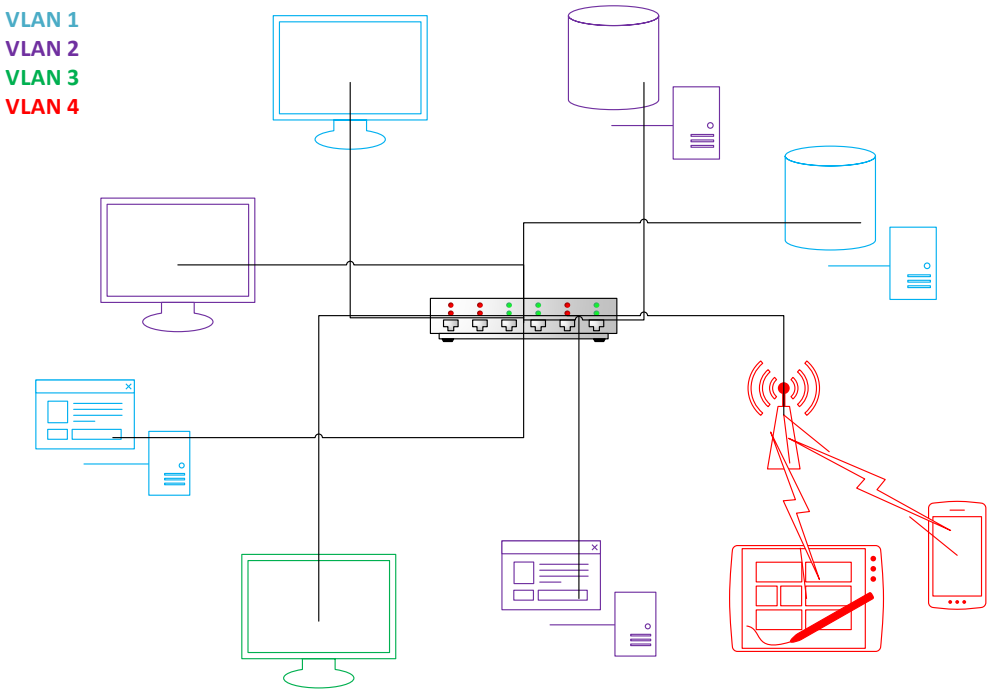
3º Si no es así, descartar el paquete.

Por otro lado, un D-Switch cuando la dirección MAC de destino sea desconocida o sea un *broadcast*, tendrá que enviar el paquete a todos los puertos excepto por el que se recibió el paquete. Mientras que un Q-Switch determinará primero la VLAN a la que pertenece el paquete y después difundirá el paquete pero solo a los puertos de la VLAN, excepto por el que se recibió el paquete.

Para configurar la sub-VLAN con un Q-Switch, se puede hacer siguiendo distintos criterios. Por ej. en la figura podemos asignar los puertos 1, 3 y 5 a la VLAN1, como por ej. sería la red del área de recursos humanos de la organización. Y los puertos 2, 4 y 5 a la VLAN2 que sería la red del área de finanzas. El puerto 7 a la VLAN 3, que sería por ejemplo la red de marketing. Y el puerto 8 a la VLAN4, que sería el acceso wifi.

De esta forma los dispositivos conectados a la VLAN1 se podrán comunicar entre ellos, pero no con los del resto de VLAN'S.

Ilustración 44 : Configuración de asignación de puertos



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Esta es la configuración más sencilla de asignación de puertos, de utilidad para segmentar una red por VLAN, pero también de las menos flexibles.

4.B.a. Diferentes métodos para la segmentación de redes

4.B.a.i- ***Segmentación por dirección MAC:*** construyendo una tabla de pares MAC-VLAN, de manera que no importe la ubicación del dispositivo, siempre se le asignara la misma VLAN. La vulnerabilidad de este enfoque radica en la posibilidad de que el atacante suplante la dirección MAC de un dispositivo, este hecho se conoce como MAC spoofing.

4.B.a.ii- ***Segmentación de las redes por subredes IP:*** En lugar de pares MAC-VLAN, registraremos en la tabla pares Rango IP-VLAN, de forma que dependiendo de la dirección IP del dispositivo, este se encontrara en una VLAN o en otra. Esta configuración es incluso menos

segura que la anterior, dado que la dirección IP de un equipo es muy sencilla de cambiar y por tanto tener acceso a determinada VLAN. Pero también es más flexible y se utiliza con mucha frecuencia en redes cableadas estables.

4.B.a.iii- ***Segmentación por asignación dinámica:*** basándonos en un servicio de autenticación, normalmente un servidor *Radius* y un directorio de usuarios, además de un conjunto de reglas que asigne a cada usuario con su VLAN correspondiente. Esta es la configuración más flexible, y al estar basada en roles funciona perfectamente con usuarios móviles con dispositivos inalámbricos o remotos.

4.B.a.iv- ***Segmentación por asignación de dispositivos:*** aunque no todas las interfaces de red lo soportan, también se podría asignar cada interfaz a una VLAN.

4.B.a.v- ***Segmentación por protocolos:*** el Q-Switch asignara las subvlan en función de los protocolos del tráfico que lleven.

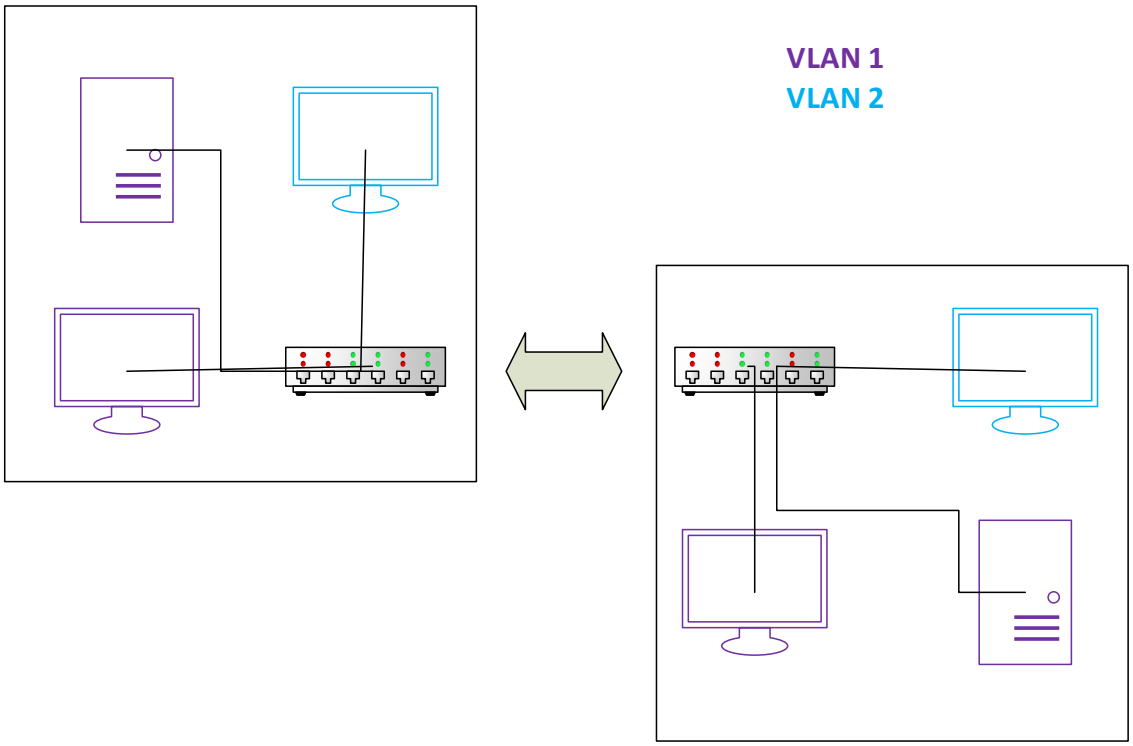
4.B.a.vi- ***Segmentación por aplicaciones:*** dependiendo del contenido de cada paquete. Lo que permite separar el tráfico según la aplicación empleada.

4.B.b. Configurar más de un SWITCH

Se deberá extender la sub-vlan al otro switch, y se deberá etiquetar de alguna forma los paquetes para que se sepa a qué VLAN pertenecen. Para conectar un switch con otro, se configura un puerto, como puerto trunk (troncal) y se conecta al puerto trunk del otro switch de forma que podemos extender la sub-vlan al resto de la red.

Además el estándar IEEE802.1Q nos permite etiquetar los paquetes para identificar a que VLAN pertenecen, así cuando viaje por la red por distintos switches no perderán esa información. Aunque no todos los dispositivos son compatibles con este estándar, y esos descartaran las etiquetas.

Ilustración 45 VLANS



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Se pueden configurar todos los switchs con la información de las sub-vlan, pero también se tiene a disposición la aplicación MVRP (Múltiple VLAN Registration Protocol) que emplea el protocolo MRP para propagar por la red desde un switch los identificadores de la subvlan.

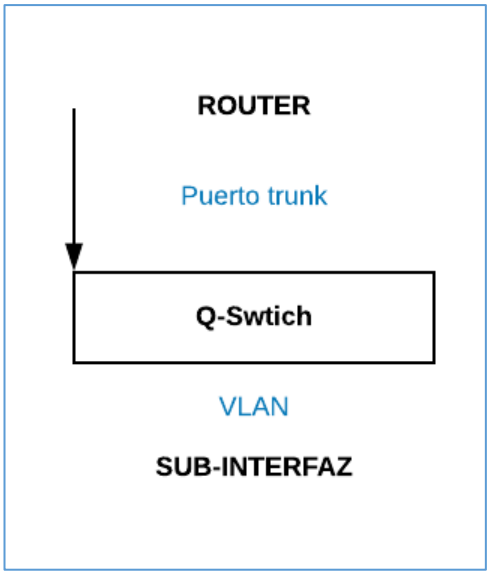
CISCO por ejemplo tiene su propio protocolo para esta tarea, el protocolo VTP (Virtual Trunking Protocol), pero recomienda desactivarlo y hacer la configuración manualmente. Recomienda esto debido al riesgo de que un atacante use este protocolo para propagar información falsa que provoque un fallo generalizado de la red, y por lo tanto una denegación de servicio.

Por defecto los puertos en un Q-Switch vienen asignados a la VLAN nativa, normalmente la VLAN1, se recomienda no enviar datos por esa VLAN. Una vez asignados todos los puertos a diferentes sub-vlan, los puertos que no se empleen se deben asignar a una VLAN especial.

Para enviar datos desde una VLAN a otra se debe enrutar el tráfico a nivel de red (la capa 3), ya que a nivel de enlace en la capa 2 las sub-vlan están separadas. Esto se puede hacer mediante un rúter que soporte puerto trunque y subinterfaces o mediante un switch de nivel 3.

Con el router simplemente se lo conecta por el Puerto Trunk al Q-switch y se le asigna a cada VLAN una subinterfaz. Sera la tabla de enrutamiento del propio router la que se encargue de dirigir el tráfico entre las subintrases o VLAN. Si utilizamos un Q-Switch de nivel 3 crearemos múltiples interfaces virtuales que asignaremos a las subredes VLAN y con esa tabla de enrutamiento de nivel 3 del switch, podemos enrutar el tráfico entre VLAN's. Por lo tanto, en el filtrado de paquetes VLAN se utilizan listas de reglas VACL que son iguales que las ya nombradas ACL pero que se aplican para el tráfico dentro de una determinada VLAN.

Ilustración 46 Puerto trunk



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

También se pueden añadir reglas ACL, pero a nivel 3 para filtrar el tráfico entre VLAN, en el router o en el switch según el equipo utilizado para conectarlas.

A pesar de estas medidas de seguridad, un atacante podría saltar de una VLAN a otra si se encuentra habilitado el DTP (Dynamic Trunking Protocol) que permite configurar los puertos como puertos de acceso o puertos trunk de forma dinámica. Se aconseja por lo tanto configurar inicialmente todos los puertos como puertos de acceso común y manualmente poner los que sean necesarios como puertos trunk, deshabilitando el uso DTP.

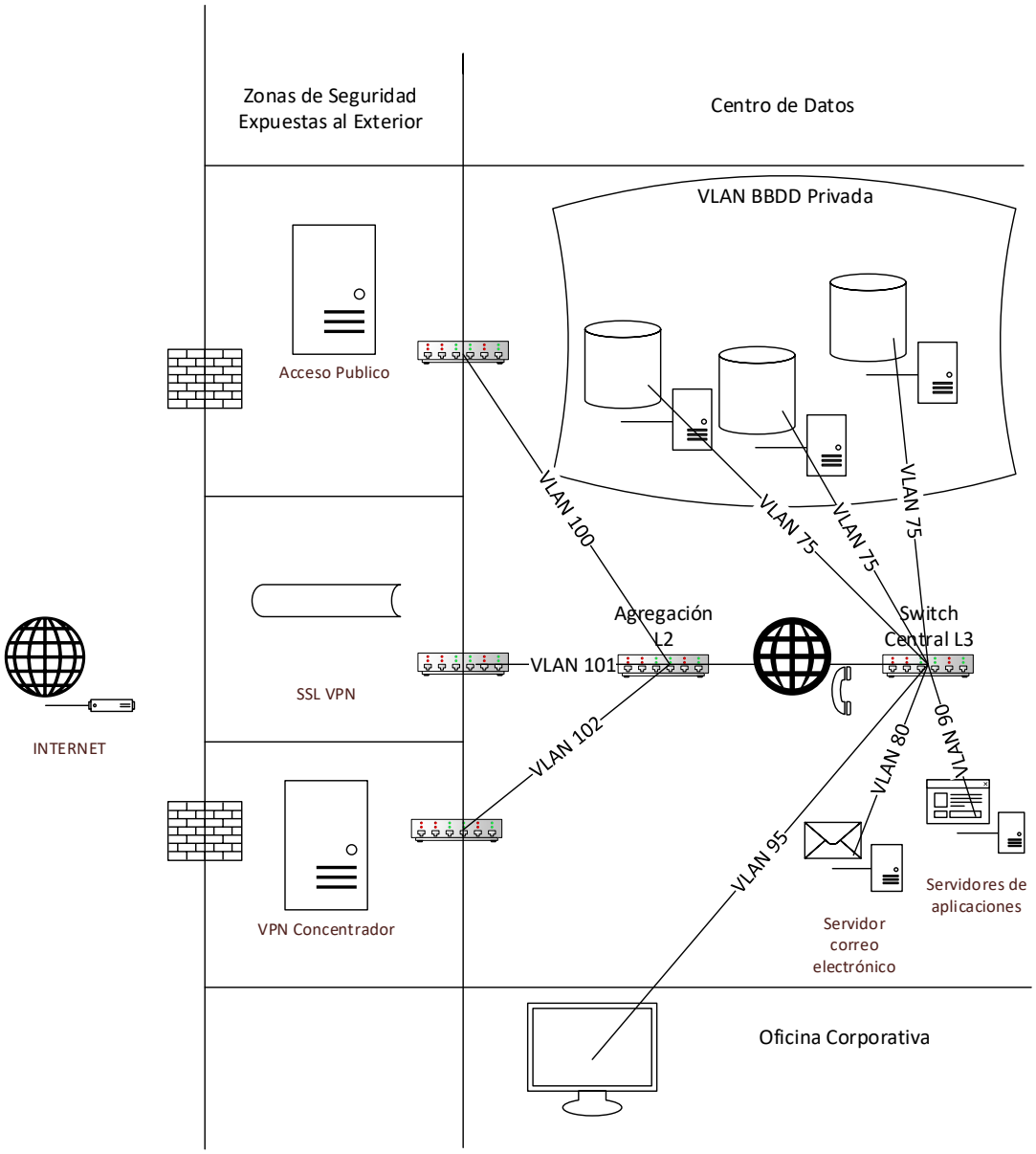
Otros de los ataques que intentan saltar la segmentación con VLAN es la inundación MAC de un switch, de forma que el atacante genera una gran cantidad de tráfico desde MAC's falsificadas, lo que va llenando la tabla del switch que tiene que ir borrando las entradas válidas para dar paso a las nuevas. El atacante aprovecha para suplantar la dirección MAC de alguno de los equipos validados. Para defenderse de este ataque alcanza con realizar la asignación de puertos a MAC's de forma manual o estática y autenticar los equipos que se conecten.

No se debe pasar por alto proteger los equipos de red frente a accesos remotos mediante contraseñas y con un control de acceso basado en roles, de forma que quede registrado en todo momento que administrador ha realizado cambios y que cambios en la configuración de un determinado equipo, por ejemplo, un Q-Switch.

Para definir las zonas en las que se va a segmentar la red se necesitan conocer muy bien los procesos de negocios y que información se intercambia. De esta forma podemos dar a los usuarios acceso a los datos que necesitan para trabajar y no otros. Siguiendo siempre la regla de mínimos privilegios, otorgando siempre el mínimo privilegio al usuario e ir dando accesos según los vaya necesitando.

Una segmentación típica, sería la propuesta en la figura siguiente

Ilustración 47 Red segmentada zonas



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Donde se dispone de una zona de seguridad expuesta al exterior con los servicios públicos básicos, principalmente la web, otra para los accesos remotos por VPN, otra para el correo electrónico, otra para la red corporativa y otra para el centro de datos, donde cada servidor de datos tendrá su propia zona.

Otra forma de segmentar redes en lugar de utilizar VLAN es directamente con firewalls, separando cada zona del resto con un firewall. Esto incrementa el número de dispositivos, lo que repercute no solamente en lo económico sino también en espacio en el CPD, aumento de temperatura y sobre todo dificulta su administración, aunque al gestionar zonas más reducidas también se simplifica en menor medida su gestión.

La alternativa consiste en emplear la virtualización de firewalls, considerando que con un único equipo se pueden implementar varios firewalls para varias zonas.

Por último, destacar las posibilidades que las SDN (Software Defined Networks) están abriendo en cuanto microsegmentación de redes, pudiendo analizar y filtrar el tráfico extremo a extremo entre dos puntos cualquiera siguiendo una política determinada. Esto permite no solo segmentar la red de una organización en una sede, sino extender esa segmentación a todas las sedes por toda la WAN de la organización, algo imposible de realizar con VLAN's.

4.B.c. PROTOCOLO SSL/TLS

Con el protocolo TLS se intenta garantizar la confidencialidad de la comunicación, su integridad y autenticar a los interlocutores. Para garantizar la confidencialidad de los datos y que otros no puedan verlos, estos se cifran con un cifrado simétrico como por ejemplo el más utilizado AES por su velocidad para cifrar grandes cantidades de datos. Para compartir la clave de este cifrado entre emisor y receptor se utiliza un cifrado asimétrico, por ejemplo, RSA.

Para garantizar la integridad de los mensajes sin que otros puedan modificarlos, se utilizan algoritmos de HASH, por ejemplo, sha256.

4.B.d. Factor humano: políticas y procedimientos de seguridad

Todas las medidas de seguridad que podemos tomar para prevenir un ataque a la integridad de nuestra red y nuestros sistemas serán en vano si no se capacita al personal humano, el cual es el factor más importante ya que usándolo de intermediario un atacante puede tener acceso a la red por medio del engaño en este ámbito llamado ingeniería social.

El valor de las empresas y organizaciones cada vez más radica en los activos de información que estas poseen, por lo que su protección es prioritaria. Para lograrlo muchos organismos han creado el cargo de *Chief Security Officer* (CSO) o *Chief Information Security Officer* (CISO), que será el encargado de supervisar la implementación del sistema de gestión de la seguridad de la información (SGSI), siguiendo normalmente algún estándar internacional como el UNE-ISO/IEC 27001, y se complementa con los objetivos de control y controles de la norma ISO/IEC 27002 y otras normas de la misma será 27000.

Según la certificación CISA (Certified Information Systems Auditor) de ISACA la implementación del SGSI se puede realizar en varias etapas.

1º Introducir el tema de la seguridad en la Visión de la empresa.
2º Definir los procesos de flujo de la información y sus riesgos en cuanto a todos los recursos participantes.
3º Capacitar a los gerentes y directivos contemplando el enfoque global.
4º Designar y capacitar supervisores de áreas.
5º Definir y trabajar sobre todo en áreas donde se pueden lograr mejoras relativamente rápidas.
6º Mejoras en las comunicaciones internas.
7º Identificar claramente las áreas de mayor riesgo corporativo y trabajar con ellas planteando soluciones de alto nivel.
8º Capacitar a todos los trabajadores en los elementos básicos de seguridad y riesgo para el manejo de *software*, *hardware* y con respecto a la seguridad física.

4.B.d.i Protocolo de Seguridad

La seguridad por oscuridad no funciona, ni tampoco las prohibiciones sin brindar ninguna razón o motivo. Deben definirse políticas de seguridad con forme a una estrategia general de seguridad de la empresa. La RFC 2196 define política de seguridad como una declaración formal de las reglas que las personas que tienen acceso a la tecnología de información de una organización deben seguir, con el principal objetivo de informar a estos usuarios y empleados de sus obligaciones para proteger los activos de la organización.

Algunos ejemplos de política de seguridad serian:

- Política de uso aceptable: Se define lo que la organización permite y no permite hacer a los usuarios con los activos que le pertenecen. Por ejemplo, puede prohibir usar los recursos de la compañía para descargar o enviar música, videos o *software* protegidos por *copyright*, o puede prohibir navegar por redes sociales, o instalar software en los equipos sin una previa autorización.
- Política de conciencia de seguridad: Se especifica cómo se asegura que el personal tiene la conciencia necesaria acerca de la seguridad de la información.
- Política de clasificación de activos: Se define como se realiza el inventario y clasificación de los activos de la organización en función de su criticidad para el funcionamiento de la organización.
- Política de seguridad física y de mesas limpias: Define la seguridad física de los activos de la compañía y también permite evitar en lo posible fugas de información por robo, o perdidas de documentos o dispositivos con información sensible.

Ilustración 48 Políticas Generales

Políticas generales	Políticas de seguridad de red	Políticas de seguridad de servidores y aplicaciones
Cifrado Aceptable	Evaluación de adquisiciones	Base de datos de credenciales
Uso aceptable	Requisitos básicos para bluetooth	Eliminación de equipamiento tecnológico
Mesas limpias	Acceso remoto	Estándar de registro de información
Plan de recuperación antes desastres	Herramientas de acceso remoto	Seguridad en laboratorios
Aceptación de firma electrónica	Seguridad de routers y switches	Seguridad en servidores
Correo electrónico	Comunicaciones inalámbricas	Instalación de software

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Se suelen utilizar documentos *standard* como base para definir las políticas de seguridad, como los que facilita www.securityforum.org en Standard of Good Practice o la ya nombrada serie 27000 de Gestión de la seguridad de ISO www.iso.org o los Control Objectives for Information Technology (COBIT) de www.isaca.org. Políticas de seguridad disponibles de forma gratuita en www.sans.org

4.B.d.ii- Estándares de seguridad

Las políticas de seguridad se pueden traducir a lo que se llama *estándare*s de seguridad, cuando se emplean detalles concretos de uso del *hardware y software*. Por ejemplo, cuando se describe como asegurar una estación de trabajo en Windows 8.1 para conectarla a la red. Teniendo en cuenta estos estándares se definirán los procedimientos de seguridad que describirán en detalle los pasos a seguir para implantar las políticas de seguridad aprobadas por la organización. Estos procedimientos suelen definir a la vez, planes de seguridad, que son un conjunto de decisiones que definen las acciones a seguir,

así como los medios que se van a utilizar. Los procedimientos de seguridad también se completan con las guías y mejores prácticas, con sugerencias que no son obligatorias pero que pueden mejorar el cumplimiento de los objetivos, facilitar el trabajo de los administradores y de los usuarios.

Ilustración 49 Políticas, estándares y procedimientos

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Es usual que las empresas definan ámbitos básicos donde implementar las políticas de seguridad, como por ejemplo la seguridad física, que va a contemplar el acceso físico, la estructura del edificio, centro de procesos de datos, etc. También la seguridad de la red corporativa, que contemplara la configuración de los sistemas operativos, acceso lógico y remoto, autenticación, internet, gestión de cambios, desarrollo de aplicaciones y muchísimos otros aspectos. También la seguridad de usuarios, que verá la composición de claves, la seguridad de las estaciones de trabajos, formación, creación de conciencia. La seguridad de datos, la cual contempla la *criptografía*, clasificación, privilegios, copias de seguridad y recuperación, antivirus, plan de contingencia.

También la auditoria de seguridad, que tendremos un análisis del riesgo, revisiones periódicas, visitas técnicas, monitorización y auditoria, sin dejar de lado los aspectos legales, que verán las practicas personales, contratos y acuerdos comerciales, leyes y reglamentación gubernamental.

Aspectos que se deben contemplar en las diferentes políticas de seguridad.

- Elección de contraseña robusta y obligar a que el usuario la cambie con frecuencia
- No dar nunca la contraseña a nadie ni anotarla en ningún lugar. Es común ver en algunos puestos de trabajos las contraseñas anotadas.
- Se debe tener cuidado con el "Shoulder surfing", que miren por encima de nuestro hombro mientras se ingresan las credenciales, o que puedan ver información sensible.
- Bloqueo de sesión y políticas de mesas limpias ya comentado. Evitando el acceso a la computadora o celular, y a información sensible que puede quedar a la vista.
- Configurar de forma correcta los privilegios de acceso a cada usuario. Emplear el usuario adecuado para cada acción
- Disponer de antivirus, firewall y todos los parches de seguridad actualizados.
- No instalar programas sin su comprobación y del debido permiso. Una buena forma de controlar esto, es que solo el personal del departamento de sistemas tengo permisos para instalar programas y realizar configuraciones.
- Comprobar siempre los dispositivos de almacenamiento, como pendrives, discos externos y demás que conectamos en el equipo
- Mantenernos alerta frente a correos electrónicos con información no solicitada para evitar el phishing.
- Eliminar documentación en papel con información sensible antes de tirarla
- No almacenar información en dispositivos no controlados o hacerlo cifrando los datos
- Mantener copias de seguridad de la información crítica para evitar perdida de información o ataques de tipo ramsonware.

- Se debe tener especial cuidado con los dispositivos móviles, smartphones, tablets, portátiles. Llevando la información cifrada y también se puede llevar un filtro de pantalla para evitar miradas indiscretas
- Cifrar la información enviada por la red es otro aspecto fundamental
- Evitar usar redes wifi-públicas, en caso de necesidad siempre cifrar la comunicación.
- Realizar un borrado seguro de la información de forma que esta no se pueda recuperar si esto es lo que se desea
- Planificar un control de acceso seguro al edificio
- Siempre pensar antes de publicar información en redes sociales

4.B.d.iii- Buenas prácticas y cultura de seguridad

Como se pudo ver en el tema anterior, es fundamental que los usuarios sepan reconocer un intento de estafa o *phishing*, de manera que no sean víctimas fáciles.

- Como primera medida se debe desconfiar de cualquier comunicación desde una fuente desconocida, sin importar el medio por el que se reciba (Correo electrónico, llamada telefónica, visita presencial, etc.). En caso de una visita personal se debe solicitar una identificación inequívoca antes de permitirle el acceso o de brindar información a la persona, o directamente se puede negar toda información a la persona y contactarse directamente con la empresa a quien supuestamente representa. Esta medida también se la puede tomar en caso de un contacto por correo electrónico o teléfono.

- En segunda instancia, nunca se debe brindar información, en especial credenciales de acceso y menos por medios como correo electrónico o acceso a formularios web sin cifrado. Un administrador de un servicio nunca pedirá al usuario esa información, se debe comprender que ellos tienen acceso al listado completo de usuarios, siendo de su dominio dar el alta o baja de usuarios, así como también

gestionarlos. Por ello cuando se recibe una solicitud de estas características se debe desconfiar y verificar la fuente.

4.B.e. Recomendaciones básicas:

A continuación, se enumerarán una serie de recomendaciones básicas que todo usuario debería conocer y cumplir.

- Elección de contraseña robusta. Al menos 8 caracteres con mayúsculas, minúsculas, números y símbolos.
- No anotar la contraseña en papel y dejarla a la vista.
- Cuidado con los papeles que se arrojan a la basura, siempre destruirlos antes.
- Cuidado con los correos de phishing, no hacer clic en enlaces desconocidos.
- Bloqueo de sesión y políticas de mesas limpias. Todos los usuarios al levantarse de su puesto de trabajo deben bloquear su sesión de usuario y dejar la mesa limpia, sin papeles.
- No dar la contraseña a nadie
- No conectar dispositivos de almacenamiento de desconocidos.
- Desconfiar de las conexiones wifi-abiertas.
- Cifrar la información y los dispositivos. Si se pierde puede que terminen en manos de alguien que no debería tener esa información, al cifrarla será imposible que la utilice.
- Realizar siempre copias de seguridad
- No aceptar nada que no entiendas, consultar siempre con soporte técnico.
- Antes de deshacerse de un dispositivo dañado, asegurarse de borrar todos sus datos.
- Implementar políticas específicas en entornos Cloud, BYOD (Bring Your Own Device), IoT.
- Implementar planes de concientización y comunicación acerca de la importancia de la seguridad en la empresa es fundamental
- Limitar la información de público acceso y destruir la información obsoleta y fuera de uso.
- Utilizar mecanismos adecuados de autenticación y control de acceso.
- Utilizar filtros antispam y antiphishing es de suma importancia.

4.C Capacitar el personal

Es de suma importancia capacitar al personal expuesto a ciberataques. Entrenar al personal para desarrollar habilidades y comportamientos que mantengan la ciberseguridad de la organización.

Esto se puede realizar de diversas maneras. La más entretenida es a través de videos, se pueden buscar algunos gratuitos, armarlos desde 0 o bien optar por pagar a una empresa dedicada a este tipo de entrenamientos.

Al final de cada video realizar una breve y sencilla encuesta ayuda afianzar los conocimientos.

Realizar "simulacros" de ciberataques, es una buena manera de poner en práctica las habilidades entrenadas del personal. Esto se puede realizar enviado periódicamente correos de phishing. El correo puede ser ignorado por el usuario o bien reportado, al caer en la trampa y hacer clic en el link malicioso, se informa al usuario que ha sido víctima de phishing.

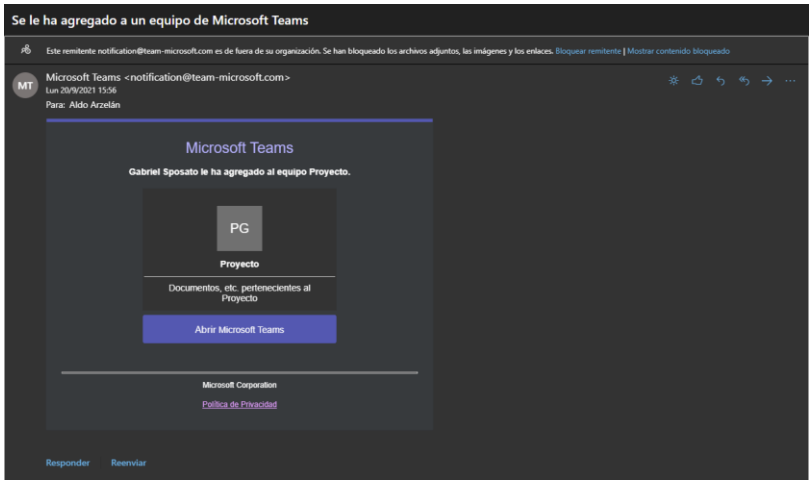
Podemos observar la verdadera dirección url al posar el cursor sobre el link.

Algunos ejemplos de correos maliciosos:

Ilustración 50 Incremento salarial

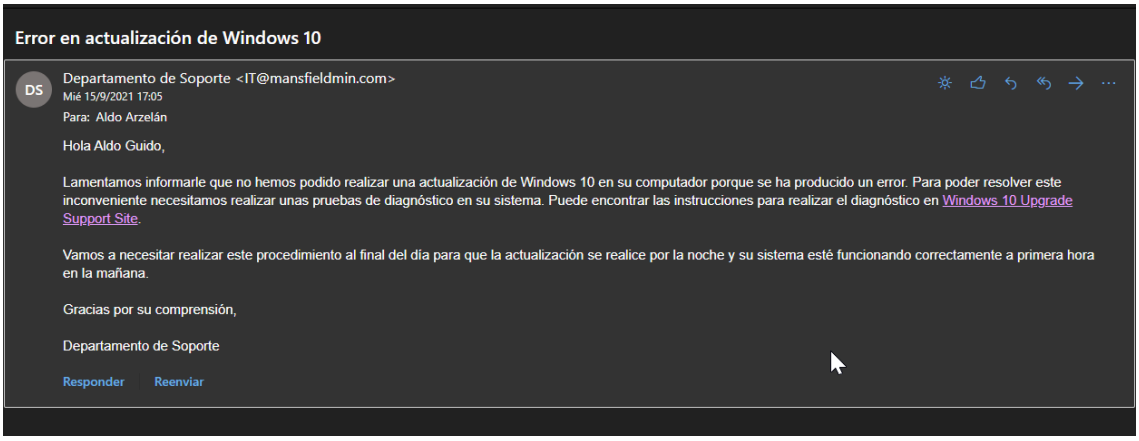
***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Ilustración 51 : Microsoft teams



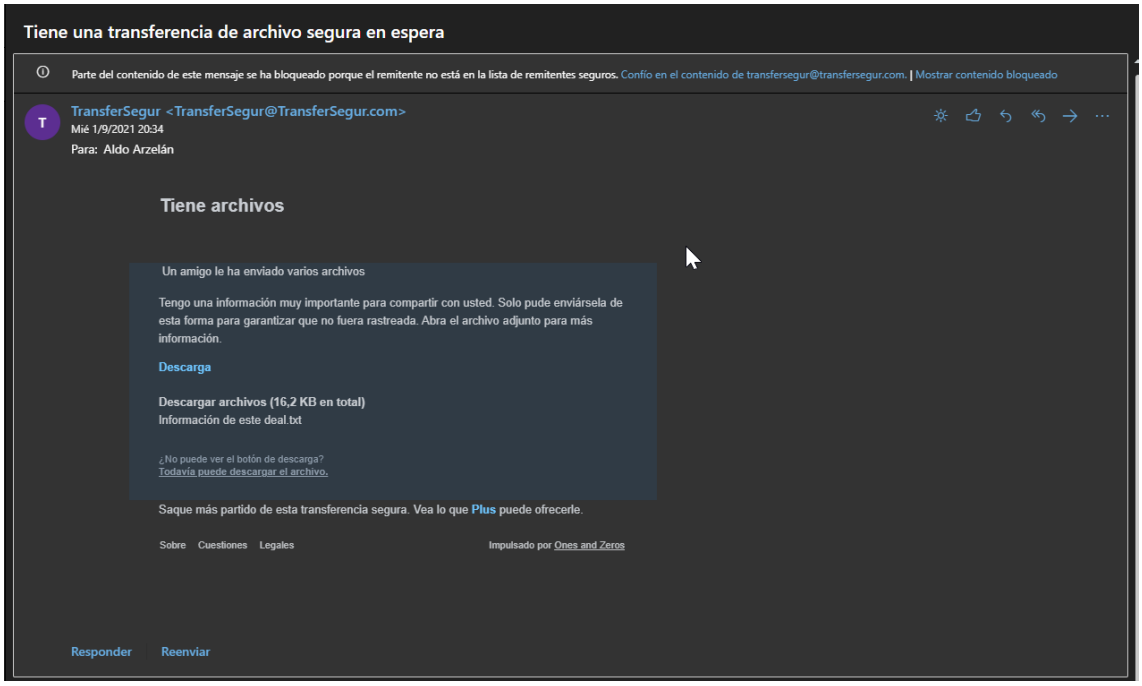
***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Ilustración 52 Actualización windows10



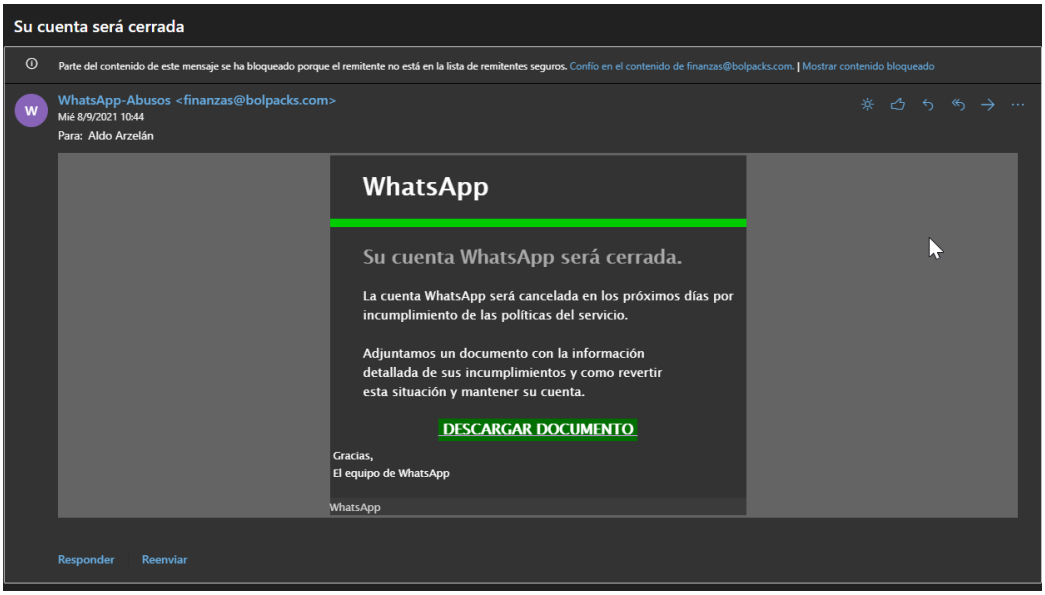
***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Ilustración 53 Transfer



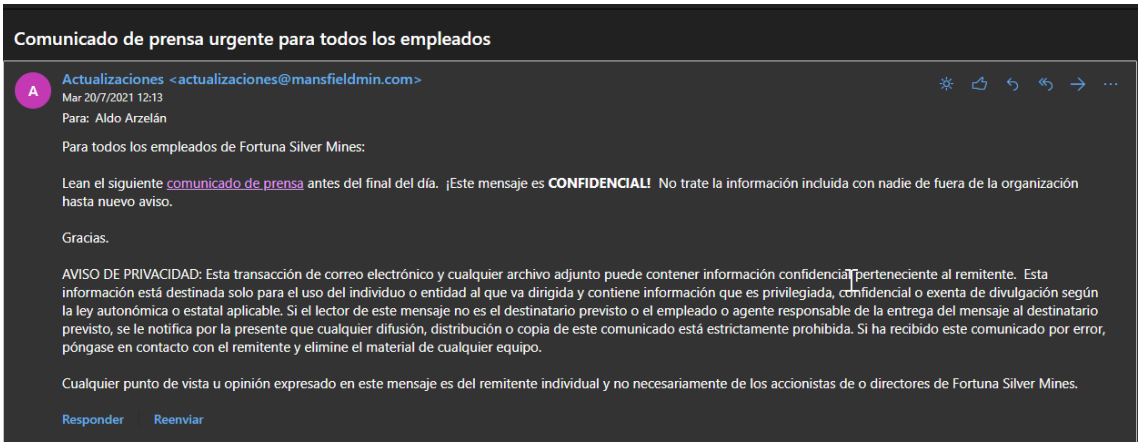
***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Ilustración 54 WhatsApp



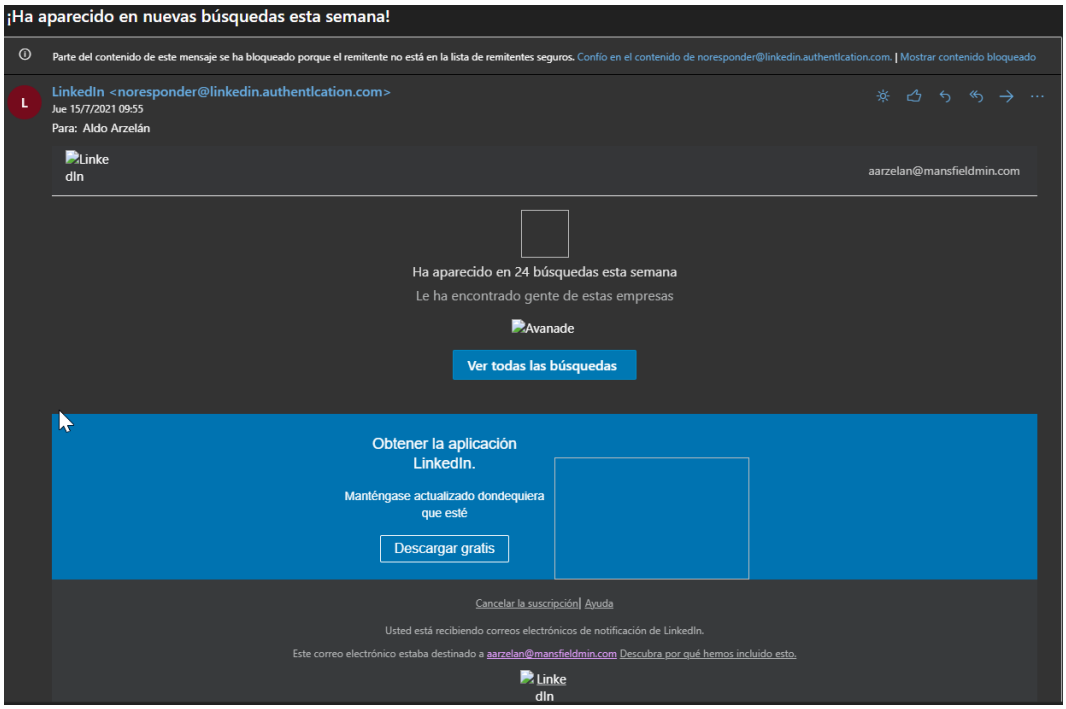
***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Ilustración 55 Comunicado de prensa



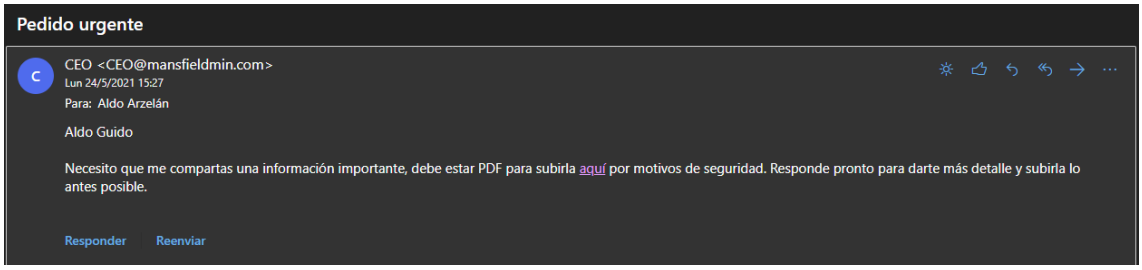
***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Ilustración 56 Linkedin



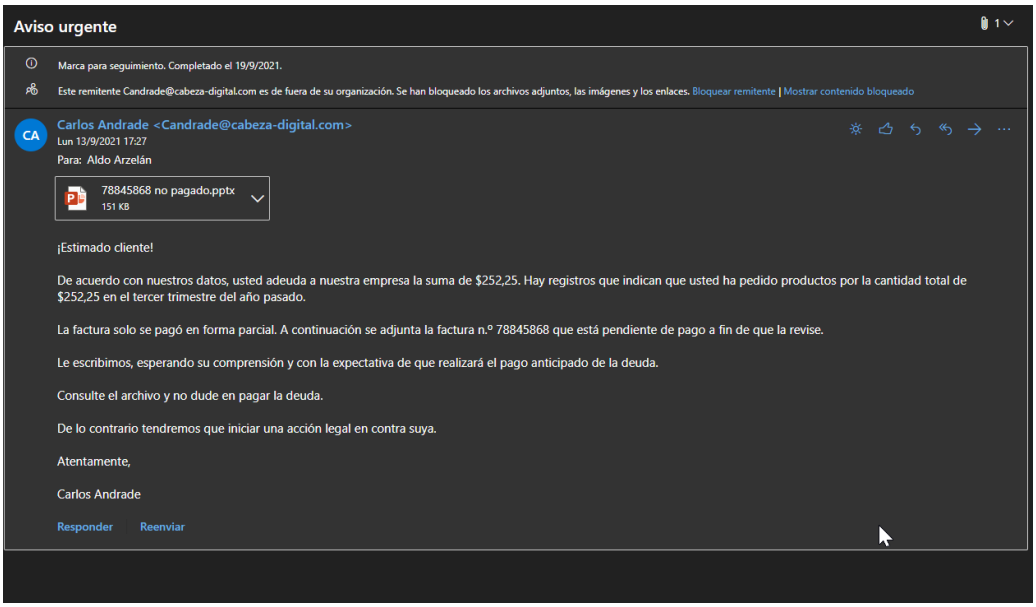
***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Ilustración 57 Pedido CEO.



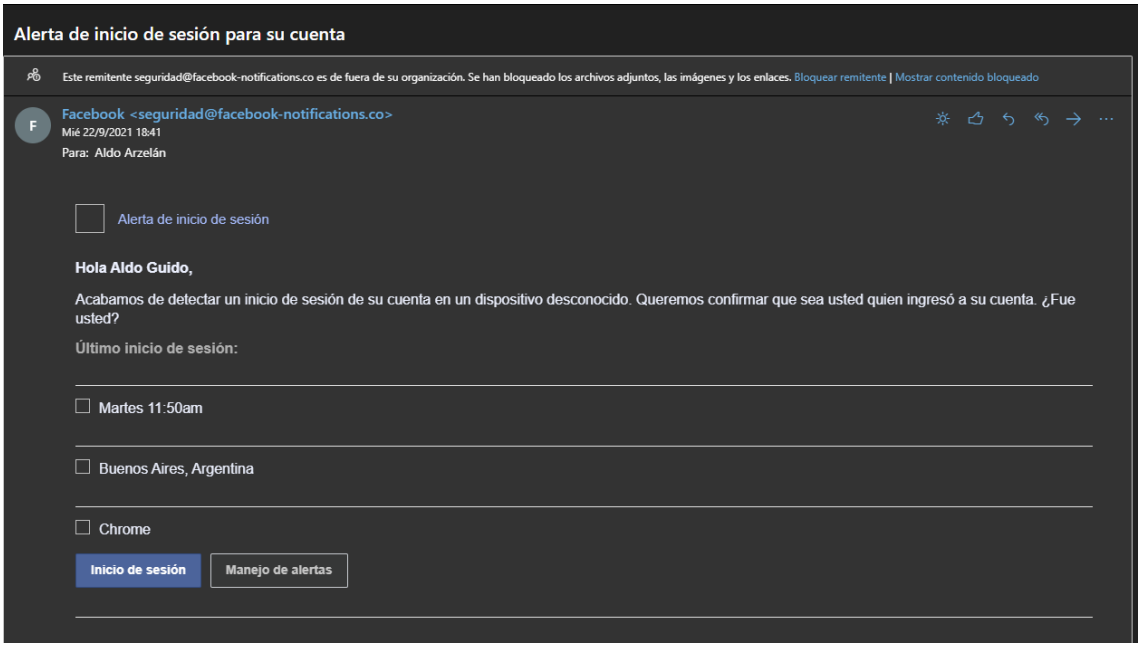
***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Ilustración 58 Aviso urgente.



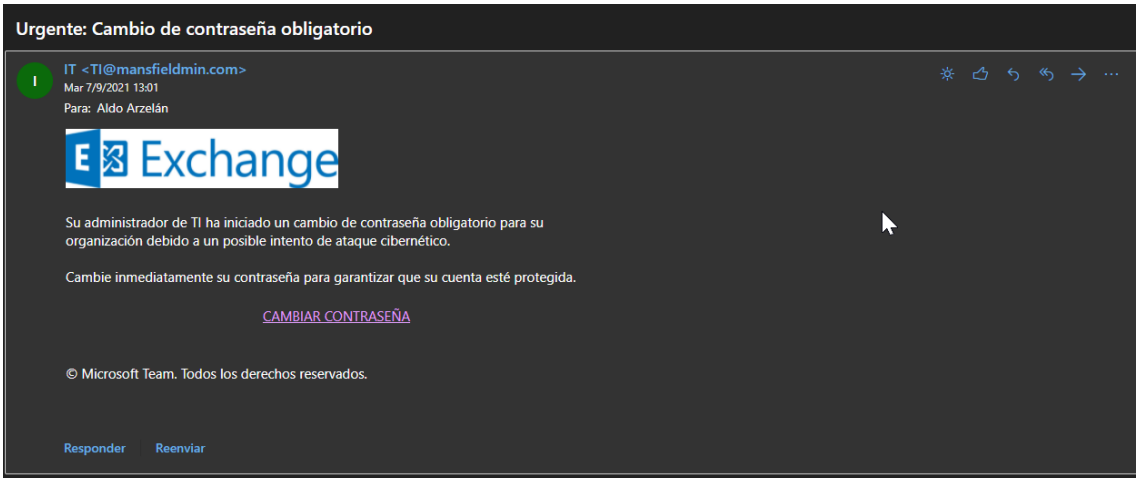
***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Ilustración 59 Alerta Facebook



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Ilustración 60 Solicitud cambio contraseña



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Ilustración 61 Mensaje Linkedin

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

De esta manera se pueden obtener estadísticas, y así saber si la capacitación al personal brinda resultados o bien si se debe continuar capacitando.

Ilustración 62 Informe seguridad.

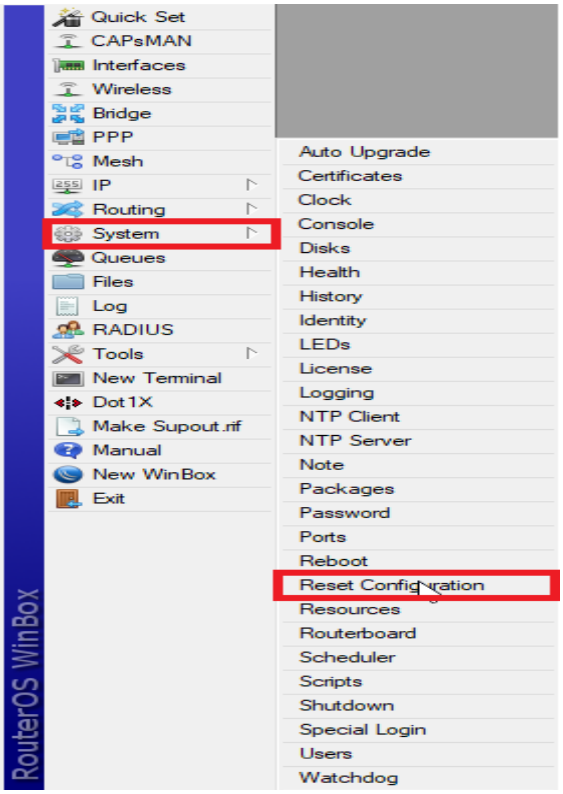
***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

4.D. Configuración Router Mikrotik

Lo primero que se debe tener en cuenta, es que basado en el kernel de Linux, nos permite utilizarlo como Router, Firewall, Switch, VPN y establecer enlaces inalámbricos.

A modo experimental, se procede a configurar un Router Mikrotik desde 0, para eso se debe utilizar la aplicación Winbox. Se recomienda borrar la configuración para que no existan reglas preestablecidas desde fabrica que puedan hacer que nuestra conjuración personalizada no se comporte de la manera esperada. Una vez iniciada la aplicación y conectada al router vamos a entrar en System y en Reset Configuration.

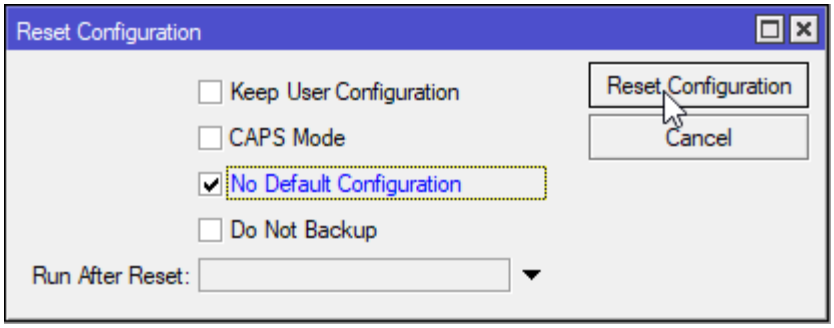
Ilustración 63 Resetear configuración



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Se debe tildar la opción "**No *Default Configuration***" y hacer clic en el botón ***reset configuration***.

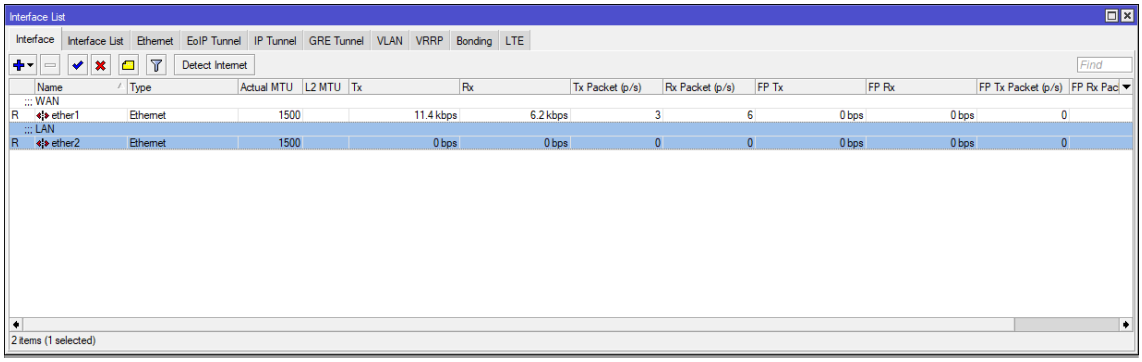
Ilustración 64 sin configuración por defecto



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Una vez *reseteada* la configuración se empieza con la configuración propiamente dicha. Para eso se ingresa en Interfaces, donde se puede ver que la existencia ya de 2 interfaces, *ether1 y ether2*. En este caso ether1 es WAN y *ether2* es LAN.

Ilustración 65 Lista de interface

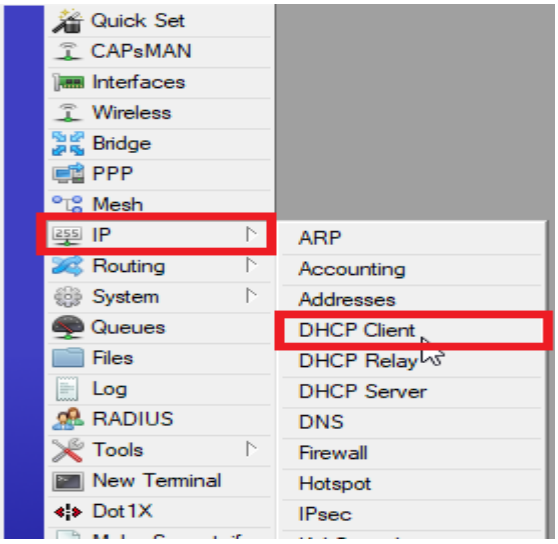


***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Se procede a hacer que el *Mikrotik* sea capaz de acceder a internet, para eso se debe añadir un cliente DHCP en la interfaz WAN. En el caso de contar con un servidor DHCP accesible desde la interfaz WAN, se pude usar el router **adsl** en el ISP. Se dejan todas las opciones por defecto, obteniéndose IP, ruta por defecto, **dns** y **ntp.**

A continuación se da clic en DHCP ***Client***

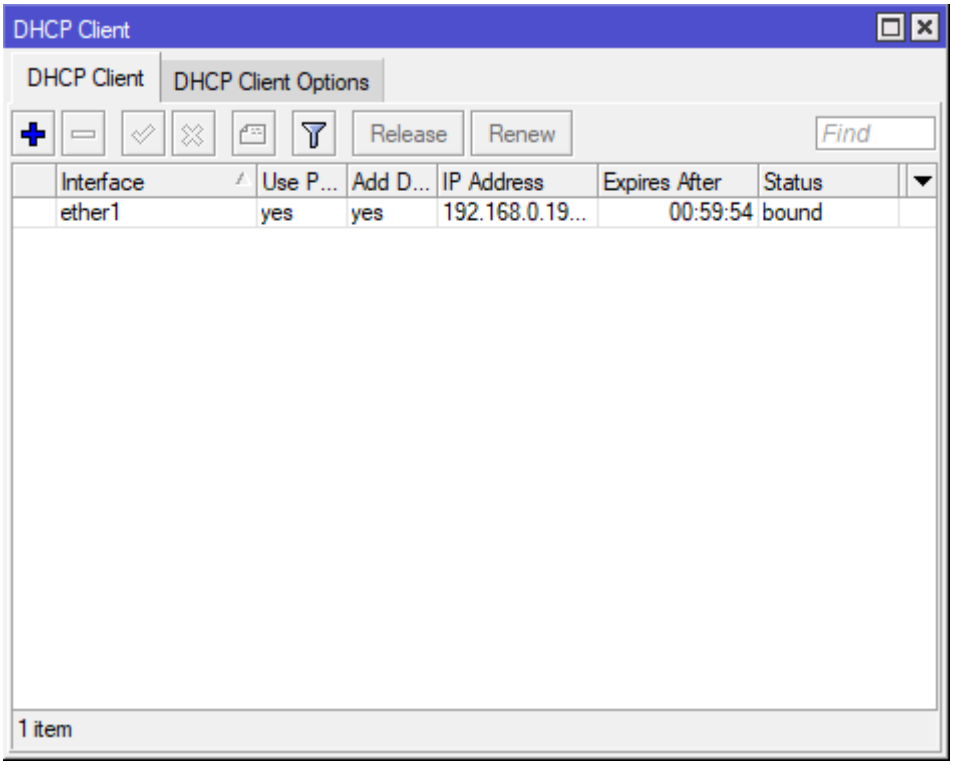
Ilustración 66 Cliente DHCP



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Aquí se visualizan los clientes y se pueden gestionar: crear, eliminar o modificarlos.

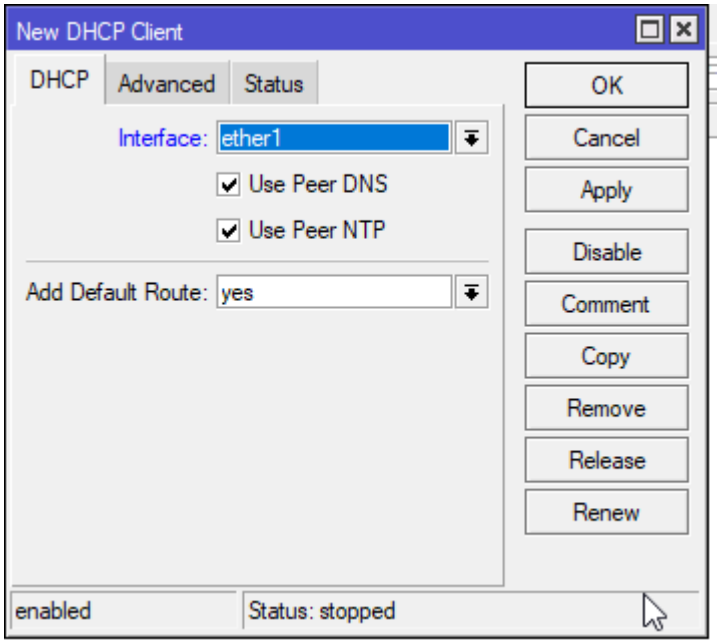
Ilustración 67 : Lista clientes DHCP



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Haciendo clic en el signo más (+) se agrega un nuevo cliente. Aquí se puede usar como interface cualquiera de los puertos disponibles, en este caso utilizaremos el puerto **ether1**.

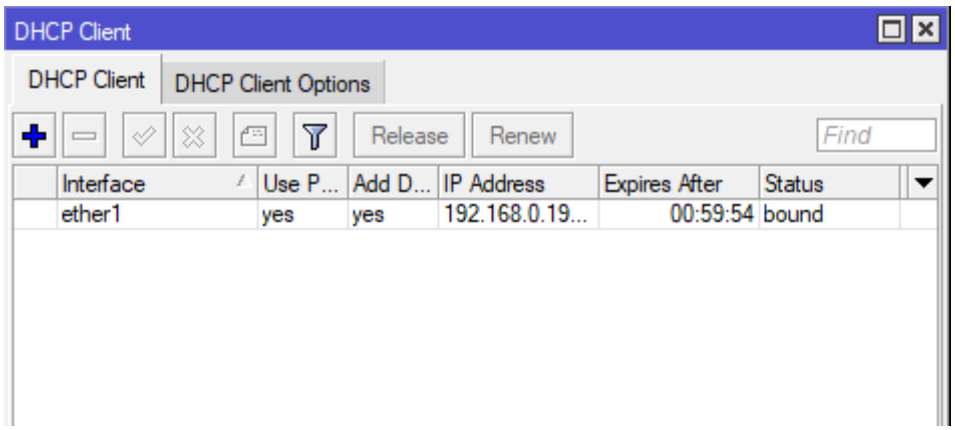
Ilustración 68 Nuevo cliente DHCP



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Se observa que en IP ***Address*** se ha generado una entrada dinámica con la IP obtenida

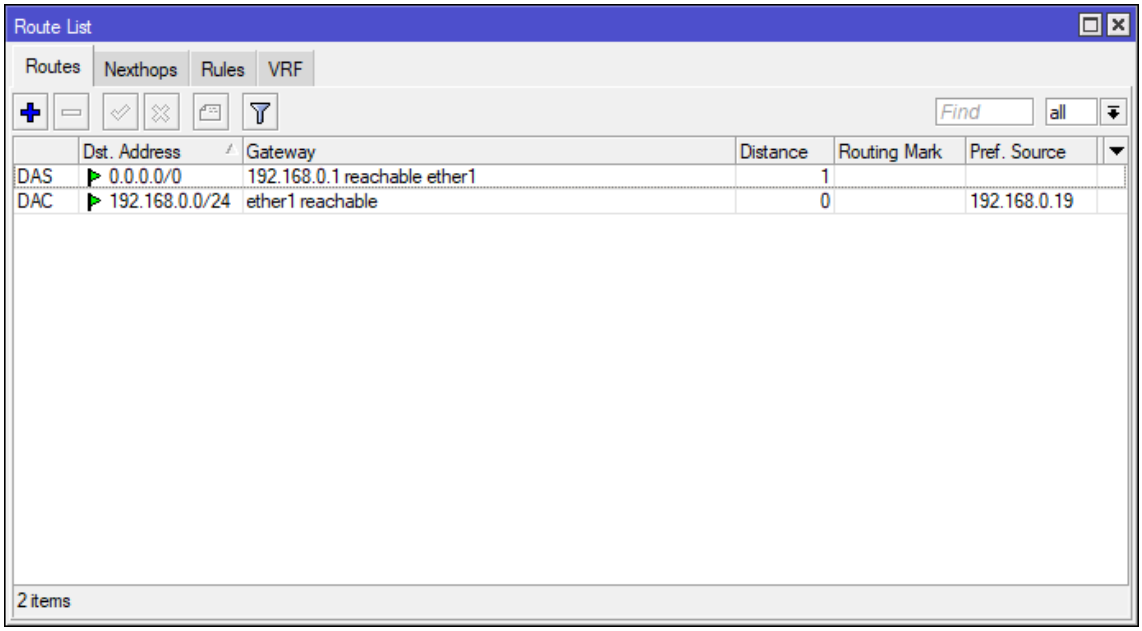
Ilustración 69 Lista nuevo cliente DHCP



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

En Router List se encuentra la entrada de la ruta por defecto y la entrada de rango de la IP obtenida. Y con esto ya tenemos salida a internet.

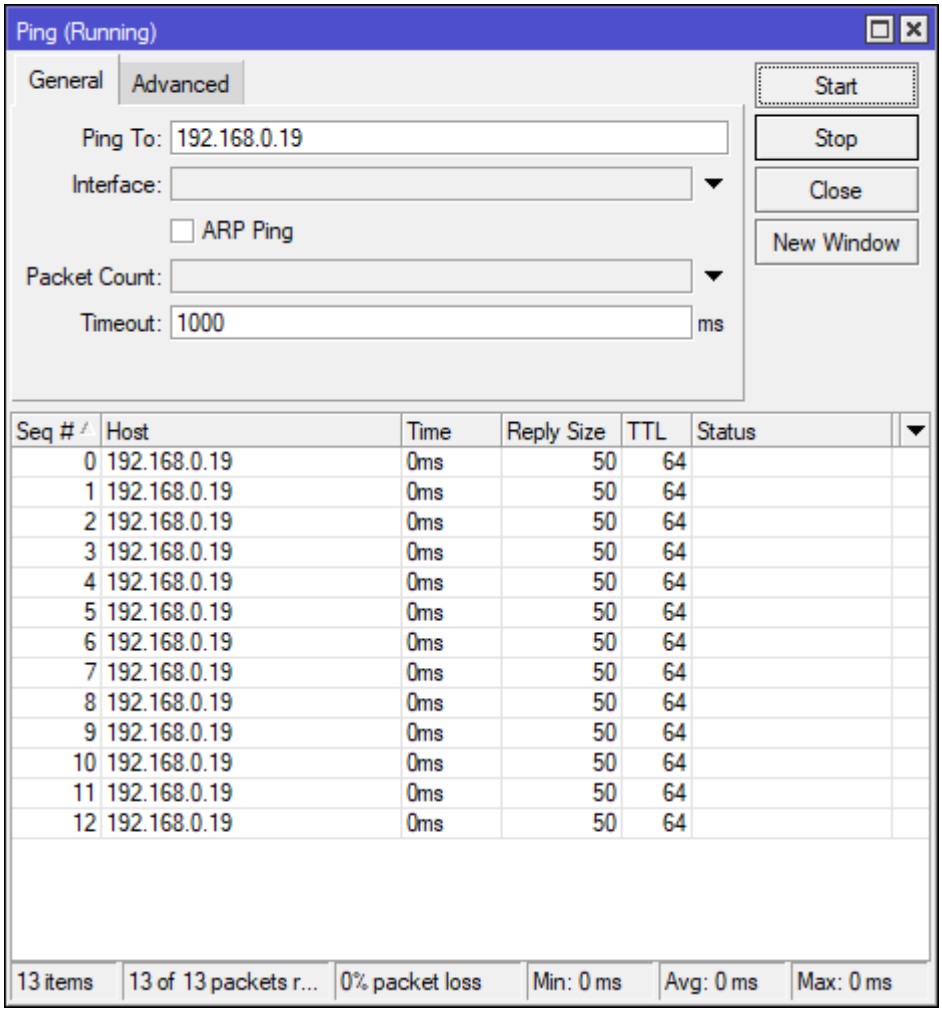
Ilustración 70 Lista de routeos



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Se puede realizar una prueba haciendo un *ping* a la IP, esto se puede encontrar en el apartado de tolos, y en la herramienta ***ping***. En este caso se coloca la dirección IP de nuestra ***mikrotik*** que es "192.168.0.19" y se le da clic a ***start***. Como se puede ver tenemos ***ping*** hacia el exterior. Lo que significa que los procedimientos anteriores se realizaron de forma correcta.

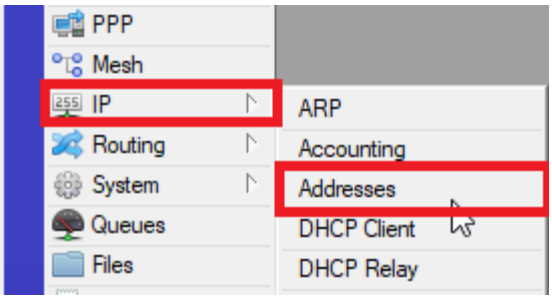
Ilustración 71 Ping



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

A continuación, se configura el propio Mikrotik para que tenga acceso a internet y pueda brindar acceso a internet a otros dispositivos. En este caso se realiza una prueba con una máquina virtual. Para esto se necesita añadir una nueva IP, para lo que se debe entrar al apartado de ***address list.***

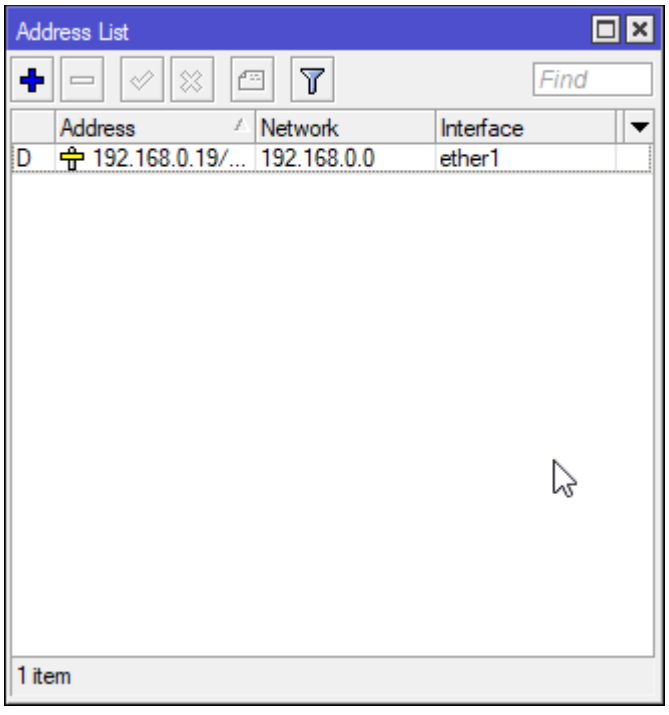
Ilustración 72 Dirección IP



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Aquí se puede observar la lista de direcciones IP y gestionarlas, se da *clic* al botón **"mas"** (+) para agregar una nueva IP.

Ilustración 73 : Lista de direcciones

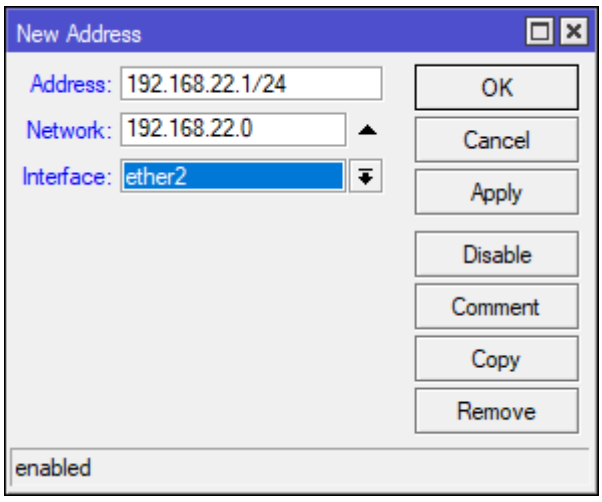


***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Aquí se añadirá una nueva dirección IP, en este caso para la interfaz del **ether2**, que es el encargado de proporcionar la salida a internet de nuestro Mikrotik. Se pone la dirección ip 192.168.22.1 y como mascara 24. Como *network* colocaremos la misma

dirección IP, teniendo en cuenta que al final se debe reemplazar el 1 por 0. En interface seleccionamos **ether2**, que tiene la configuración de salida a internet.

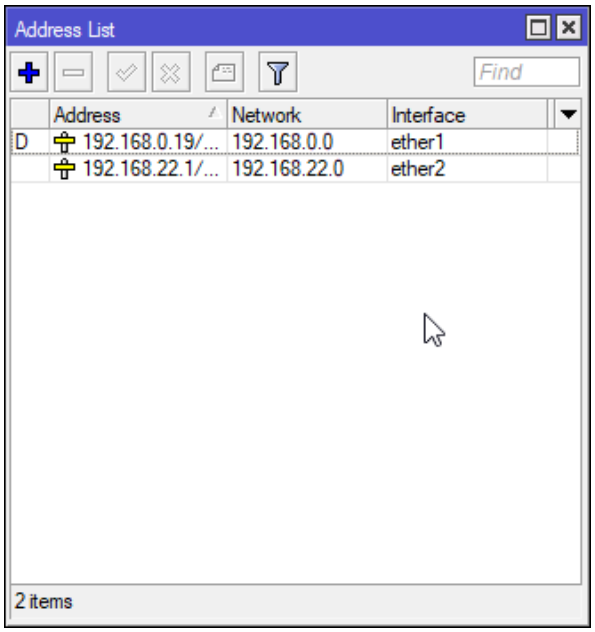
Ilustración 74 Nueva dirección IP



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

A continuación, se da *clic* en OK, y se verifica que la dirección IP en el **interfaz 2,** este creada.

Ilustración 75 Lista con nueva dirección IP

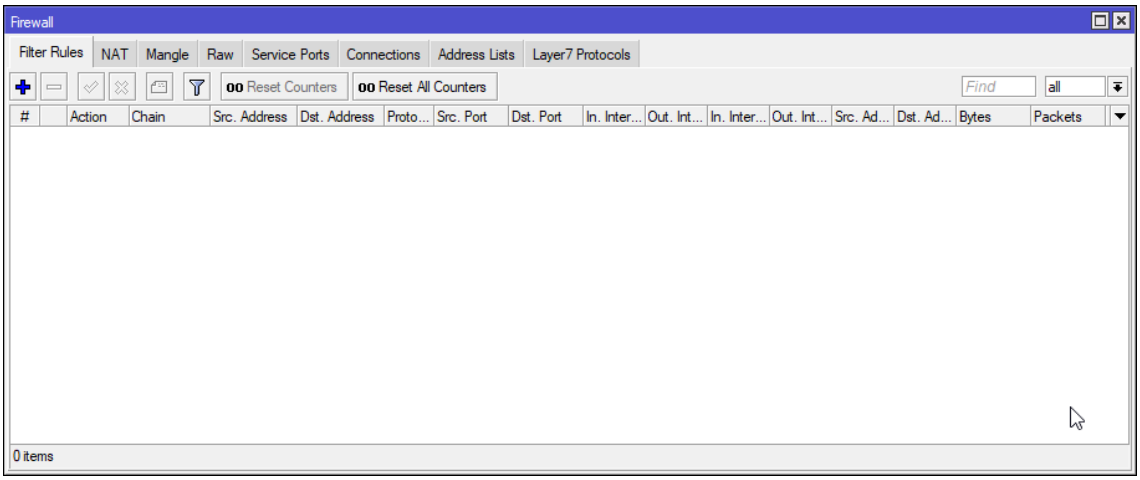


***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Una vez configurada la IP en el interfaz 2, necesitaremos crear una regla para establecer el rango de la dirección ip que acabamos de crear. Para esto tendremos que enmascarar el tráfico de ese rango, para que además el pc sea capaz de salir a internet.

Para esto se debe configurar el **firewall.**

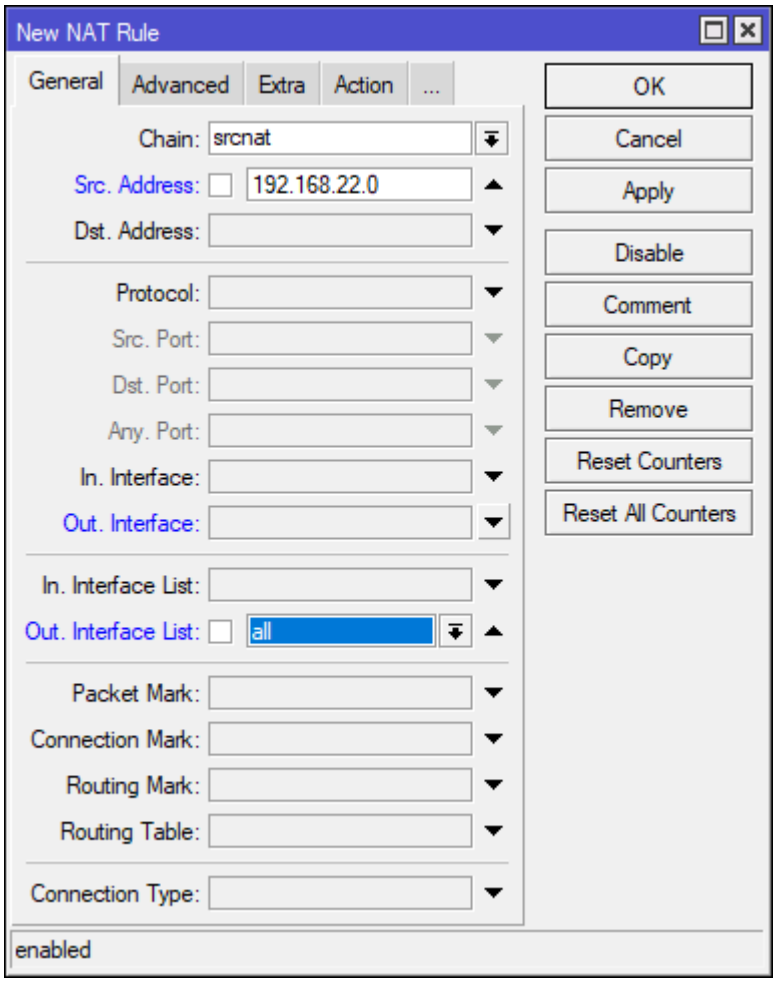
Ilustración 76 : Lista Firewalls



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Nos dirigirnos al apartado "NAT" y se crea una nueva regla. En este caso, el tipo seleccionado automáticamente que es "*srcnat"*. En el apartado **Src Address** se agrega la dirección IP que se acaba de configurar para el interfaz 2 o bien el ether2, en esta prueba **"192.168.22.0"** y en la lista de interfaces de salida se seleccionan todas con ***"all"***.

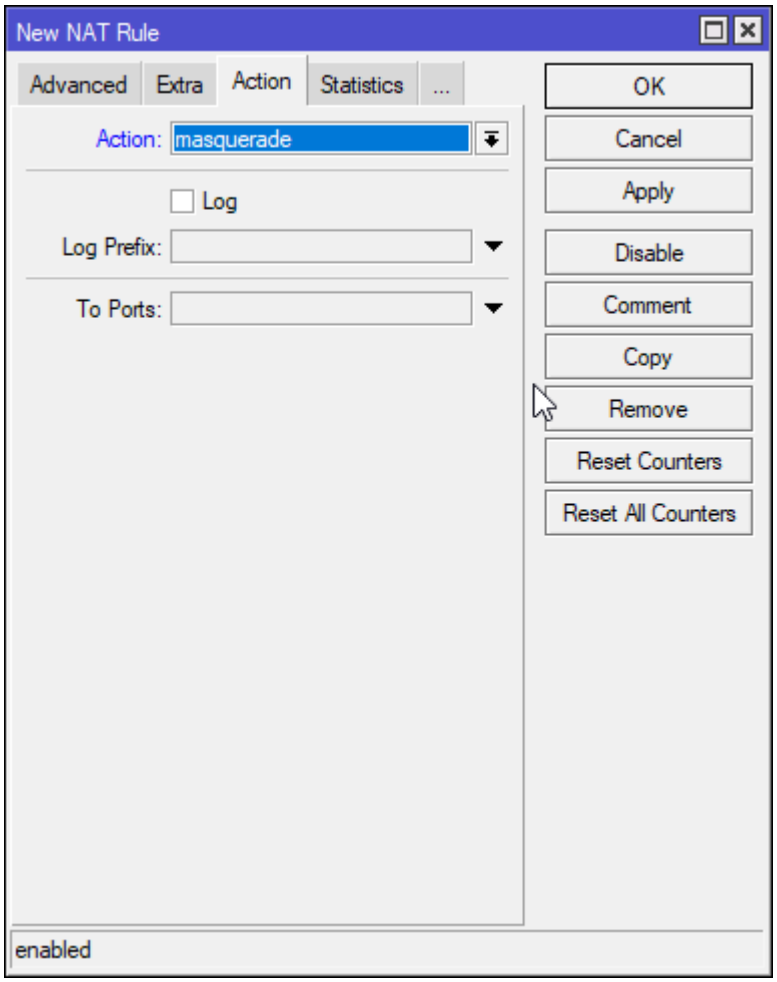
Ilustración 77 Nueva regla NAT



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Posteriormente debemos ir a la pestaña "***Action"*** y en la opción ***"Action"*** se busca la opción **"masquerade"**, dado que es la que permite justamente enmascarar el tráfico que se le está creando a esta nueva regla

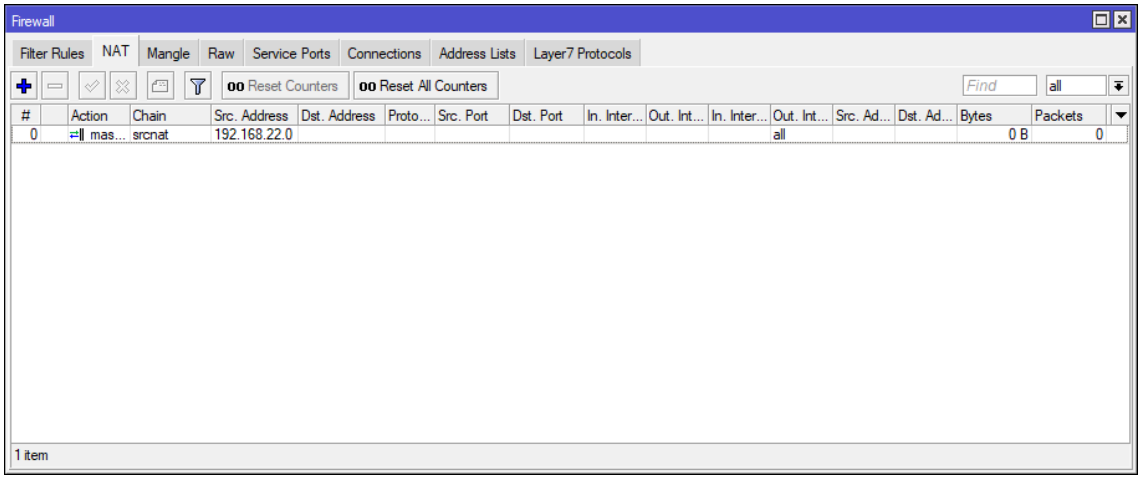
Ilustración 78 Nueva regla NAT, Action.



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

A continuación, se verifica que la regla se haya configurado correctamente como se observa en la siguiente imagen.

Ilustración 79 Lista con nuevo Firewall



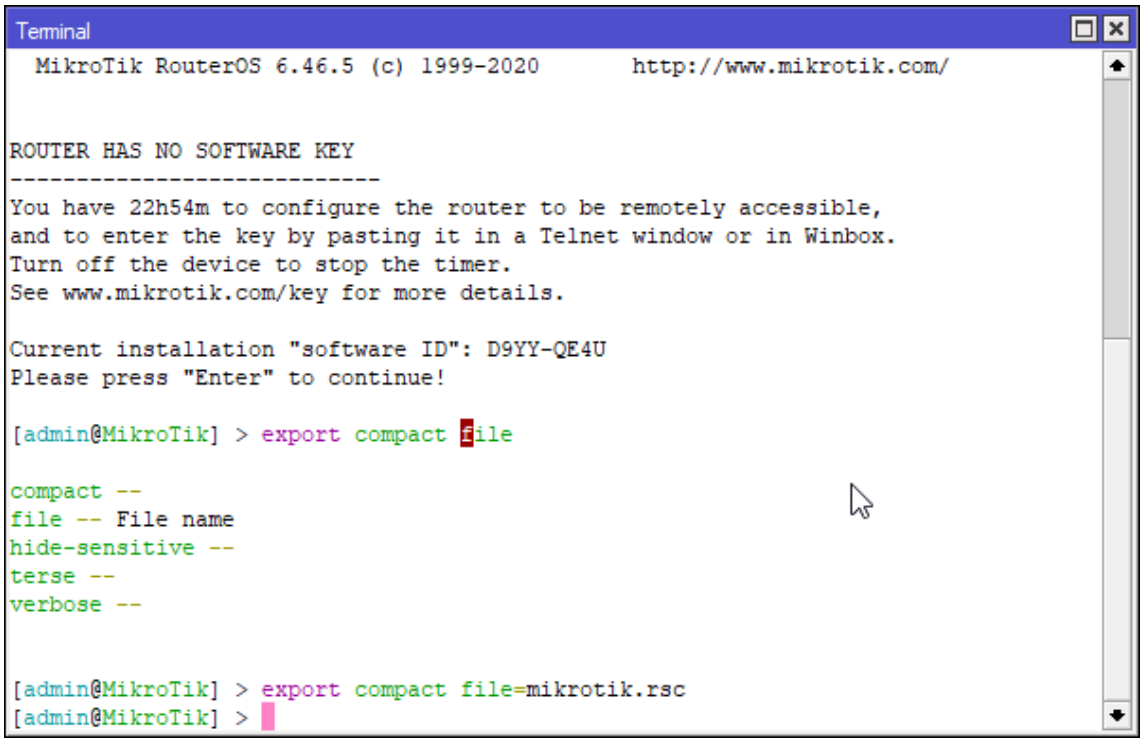
***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

En esta etapa ya se está listo para crear un *backup*. Es importante realizar el *backup* como tarea de mantenimiento preventivo, ya que, si se tiene algún problema y se pierde la configuración del Mikrotik, se puede recuperarla de manera rápida y eficaz, solo restaurando el archivo del *backup* evitando configurar todo nuevamente.

También es útil por si se llega a tener la necesidad de cambiar el equipo y configurar uno nuevo, o si contamos con otro equipo que necesitaríamos realizar la misma configuración.

Para crear el archivo *backup* se debe utilizar la terminal del Mikrotik. En la terminal se escribe la palabra reservada ***"export"*** a continuación ***"compact file"*** y seguido del signo **igual** (=) el nombre que le queremos dar al archivo, con la extensión **". rsc".**

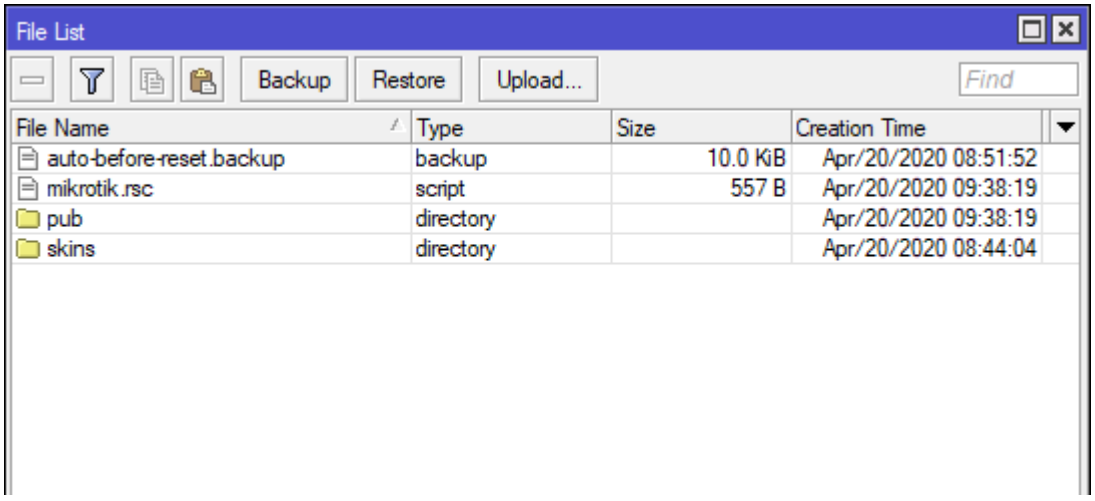
Ilustración 80 Consola Mikrotik



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Se debe verificar que el *backup* se creó correctamente ingresando al apartado ***"Files".*** Como se puede ver en la imagen el archivo se creó correctamente.

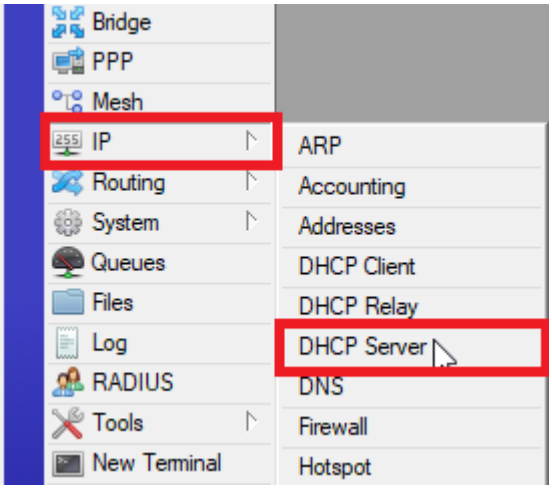
Ilustración 81 Lista de archivos



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Una vez realizado el *backup*, se procede a configurar un nuevo DHCP para que el Mikrotik no genere una IP automática a los clientes. Para esto hay que dirigirse al aparto "DHCP Server" dentro de la pestaña "IP", como se ve en la imagen.

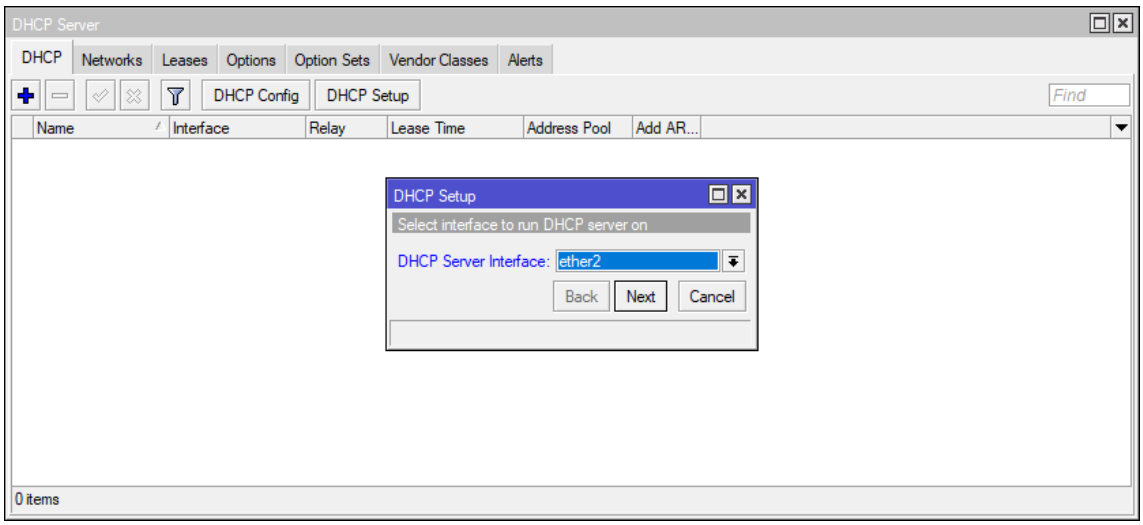
Ilustración 82 Nuevo Servidor DHCP



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

A continuación, se hace *clic* en el botón **"DHC *Setup*",** donde se elige una configuración para la interfaz 2.

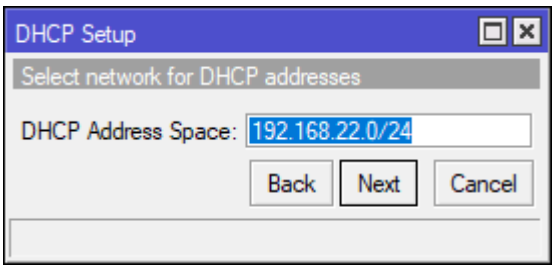
Ilustración 83 Servidor DHCP



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Posteriormente se hace *clic* en **Next** y aparece automáticamente la dirección IP de nuestra interfaz.

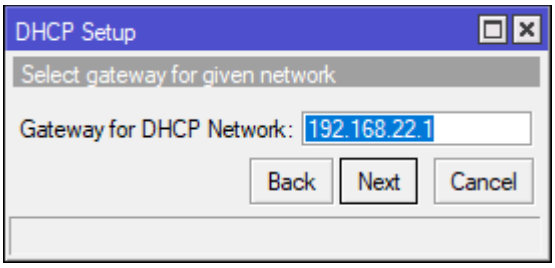
Ilustración 84 Dirección DHCP



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

También se visualiza nuestro *networ*k o *gateway* (puerta de enlace).

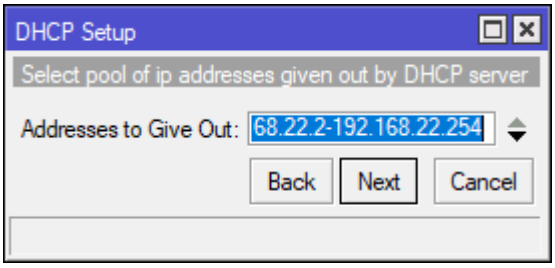
Ilustración 85 Puerto de enlace DHCP



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

También queda visible nuestra *piscina* (pool) o nuestro rango de direcciones IP. En este caso, dado que nuestra mascara es 24, nos establece desde una dirección 192.168.22.2 hasta 192.169.22.254. Si se desea modificar el rango se puede realizar en esta misma pantalla.

Ilustración 86 Rango direcciones IP



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

A continuación, aparece el DNS Server creado.

Ilustración 87 Selección de servidor DNS

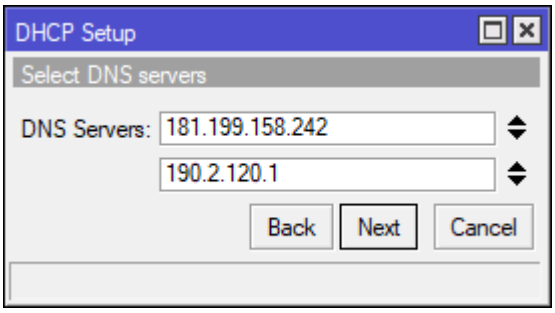


Ilustración 88 Tiempo de uso

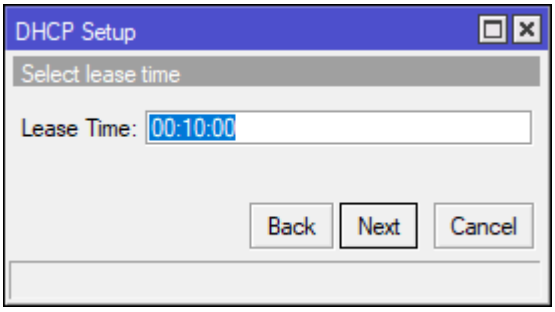
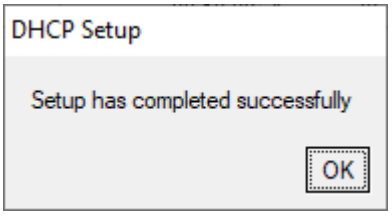


Ilustración 89 Configuración completa

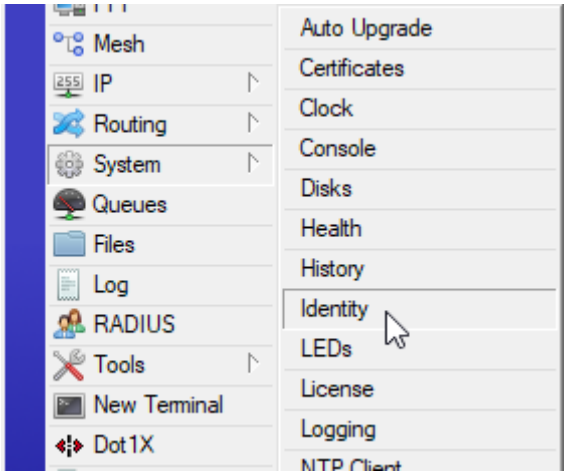


***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Habiéndose creado el DHCP Server, la Mikrotik ya está configurada para poder conectar diferentes equipos en diferentes redes locales.

Finalmente, en la configuración se debe modificar el nombre de nuestra Mikrotik y también crear una contraseña, ya que por defecto se ingresa a la Mikrotik sin clave. Para ello, en primer lugar, entra al apartado ***Identity***.

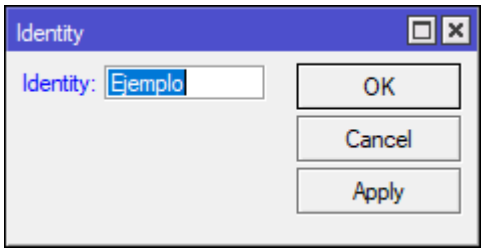
Ilustración 90 Sistema de Autenticación



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Y se completa con el nombre que se desee. En esta prueba solo pondremos **Ejemplo.**

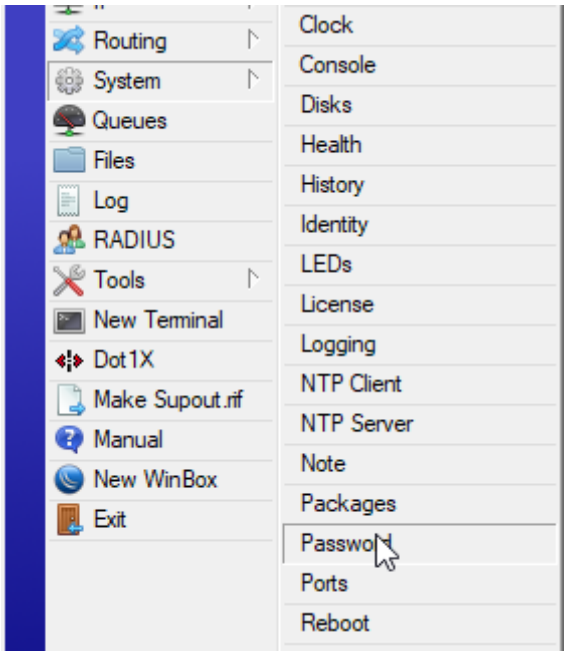
Ilustración 91 Nombre de usuario



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Luego se entra al apartado de *password* para modificar la misma.

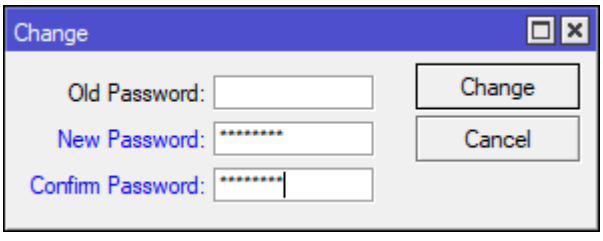
Ilustración 92 Sistema de contraseña



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

En la casilla de contraseña vieja la dejamos vacía, ya que, como se mencionó, por defecto se ingresa sin requerimiento de clave. En la casilla **nueva contraseña** se ingresa la contraseña que se desea, luego se confirma.

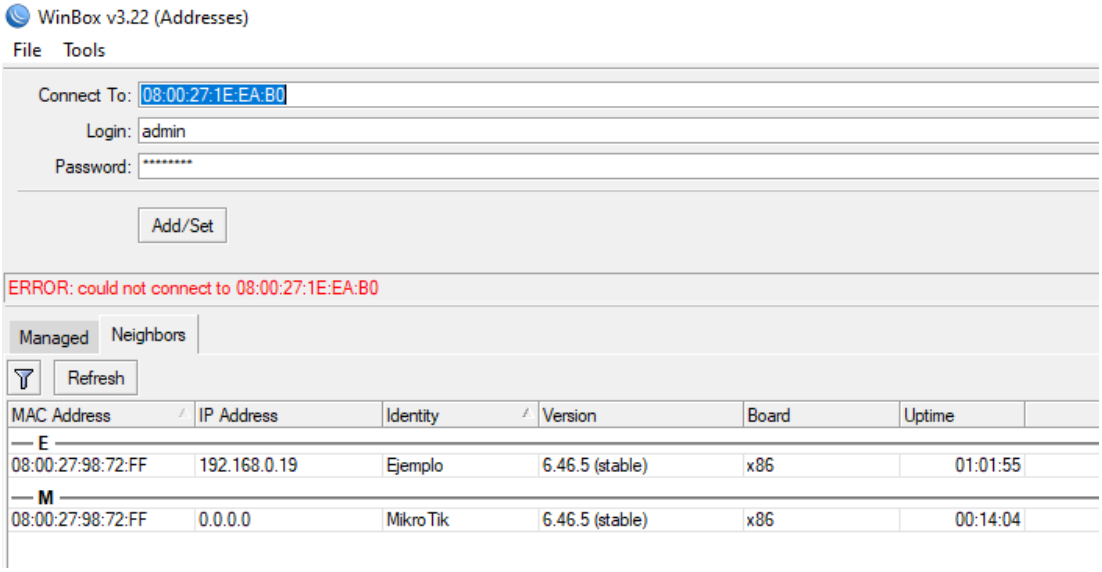
Ilustración 93 Configuración contraseña



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Para verificar, se debe desconectar el usuario en *winbox*, y en la pantalla de *logueo* se observará la modificación del nombre.

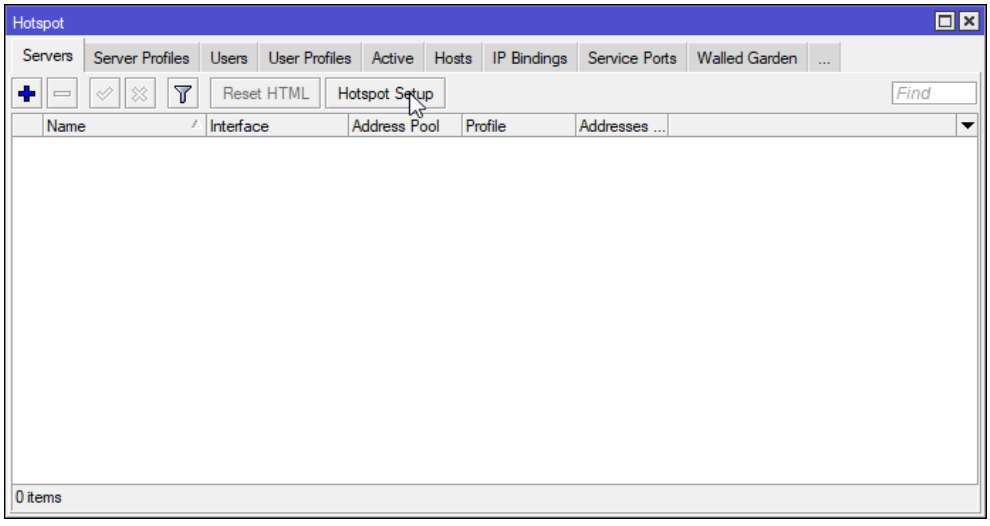
Ilustración 94 Winbox Login



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

El Mikrotik quedó ya configurado. Paso siguiente, es crear las utilidades que ofrece el dispositivo, en este caso las conexiones de tipo *hotspot*. Se trata de que se pueda acceder a internet a través de un usuario. Desde el apartado IP y adentro de ella se busca la opción *Hotspot.* Una vez que se ingresó, nos dirigimos a la pestaña por defecto, que es la de *Server* y en ella se selecciona la opción *Hotspot setup.*

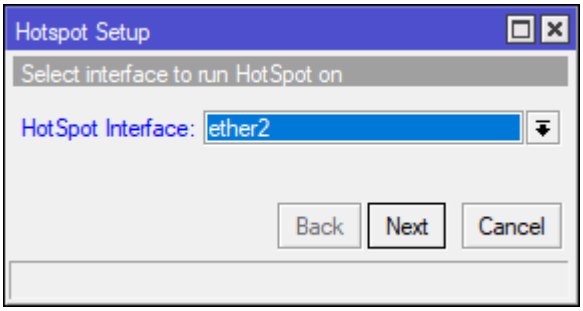
Ilustración 95 Conexiones hotspot



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Se crea un *hotspot* para la interfaz 2 o ether2

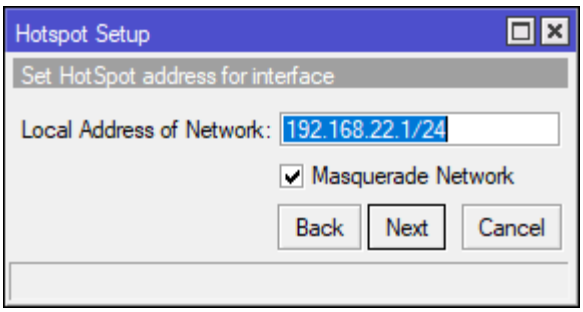
Ilustración 96 Selección interfaz para correr hotspot



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

En este caso se deja dirección IP local, la configurada anteriormente en la interfaz 2.

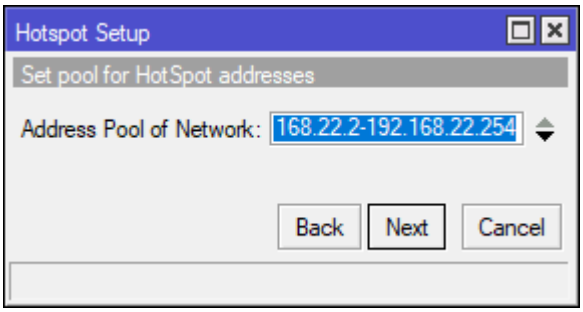
Ilustración 97 Dirección local Network



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Se mantiene el mismo *pool* o rango de direcciones IP.

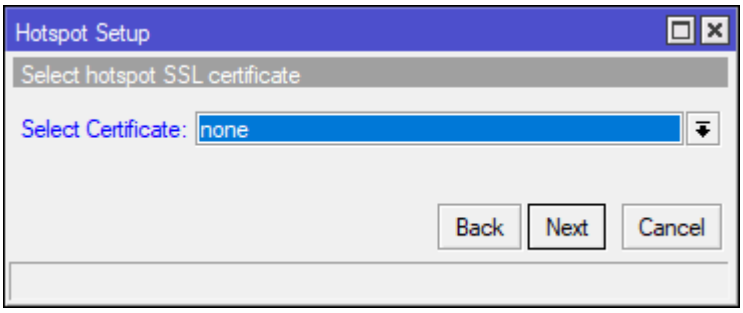
Ilustración 98 : Rango de direcciones IP Network



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

En **certificación** se selecciona la opción por defecto.

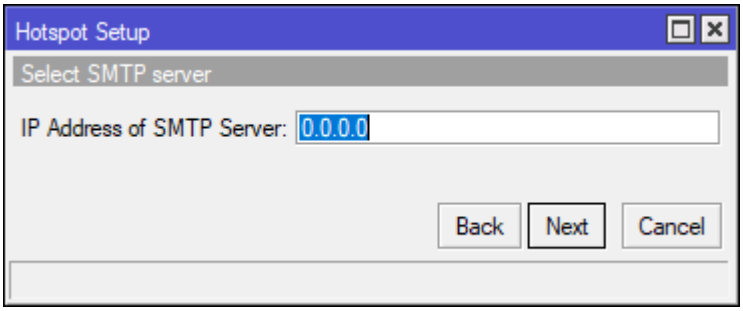
Ilustración 99 Selección de certificado



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

En el caso de la dirección IP del servidor SMTP también se la deja por defecto.

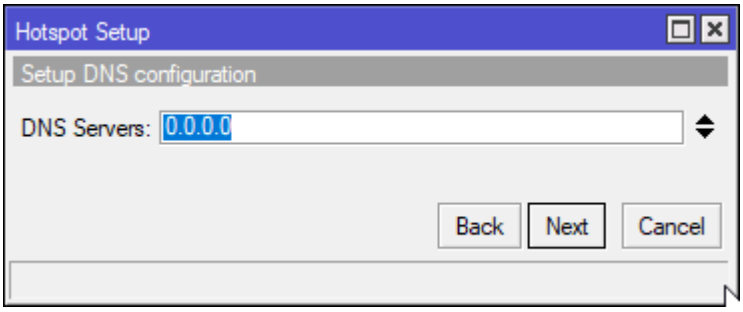
Ilustración 100 : Dirección IP de servidor SMTP



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

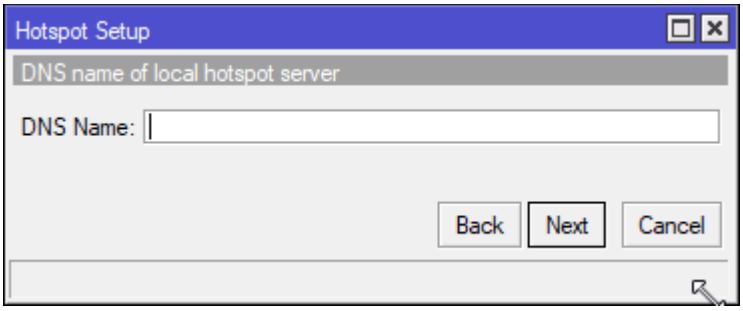
Se realiza similar procedimiento con el Servidor DNS y el nombre del mismo, tal como se puede ver en las imágenes que siguen.

Ilustración 101 Configuración Servidor DNS



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

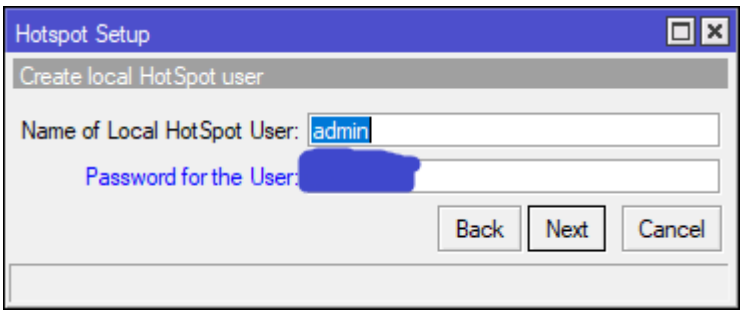
Ilustración 102 : Nombre DNS

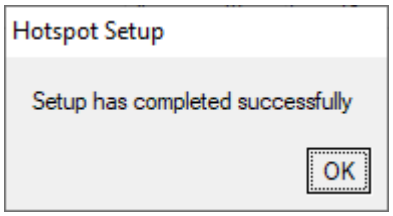


***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

A continuación, solicita el usuario y contraseña del Mikrotik, (en este caso, se completa con los que configuramos anteriormente.)

Ilustración 103 Nombre y contraseña Hotspot

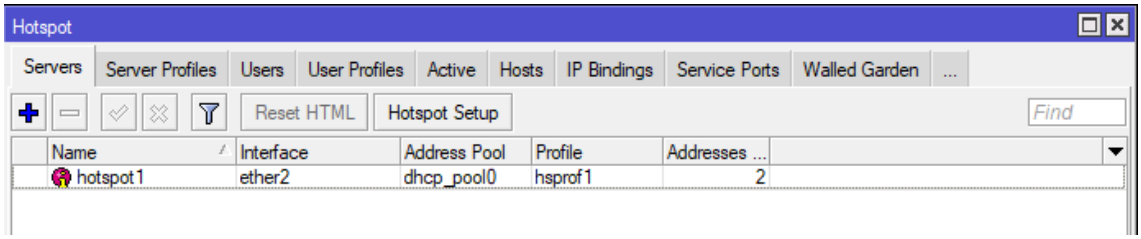




***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

En la siguiente imagen se puede observar cómo se creó el *hotspot.*

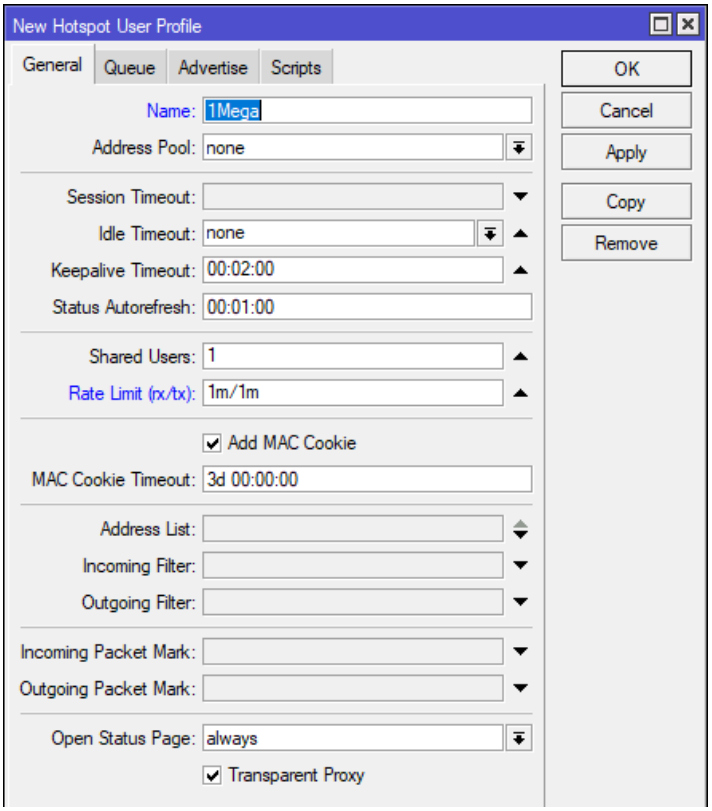
Ilustración 104 Lista hostpot



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

A continuación, en la sección de *users Profiles* se crea un perfil, donde se configurará un plan de datos. En este caso un plan de **1MB** de velocidad como límite máximo. Se le otorga un nombre al perfil, para esta prueba será "1Mega", se dejan todas las opciones tal cual están y solo modifica la opción *Rate Limit* donde se pone 1**m/1m.**

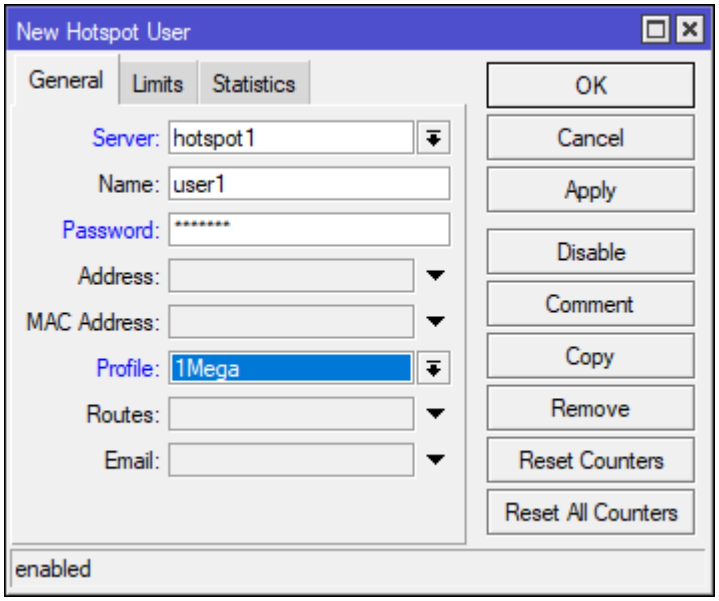
Ilustración 105 : Configuración nuevo perfil usuario hotspot



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Una vez creado el perfil, se debe crear un usuario para el *hostpot*, que tenga el perfil recién creado. Se selecciona el *hotspot*1 que se ha creado y se completar el nombre de usuario que se desee, para este ejemplo **"user1"** y también se le debe crear una contraseña. Por último, se selecciona el perfil que será el de 1Mega de navegación

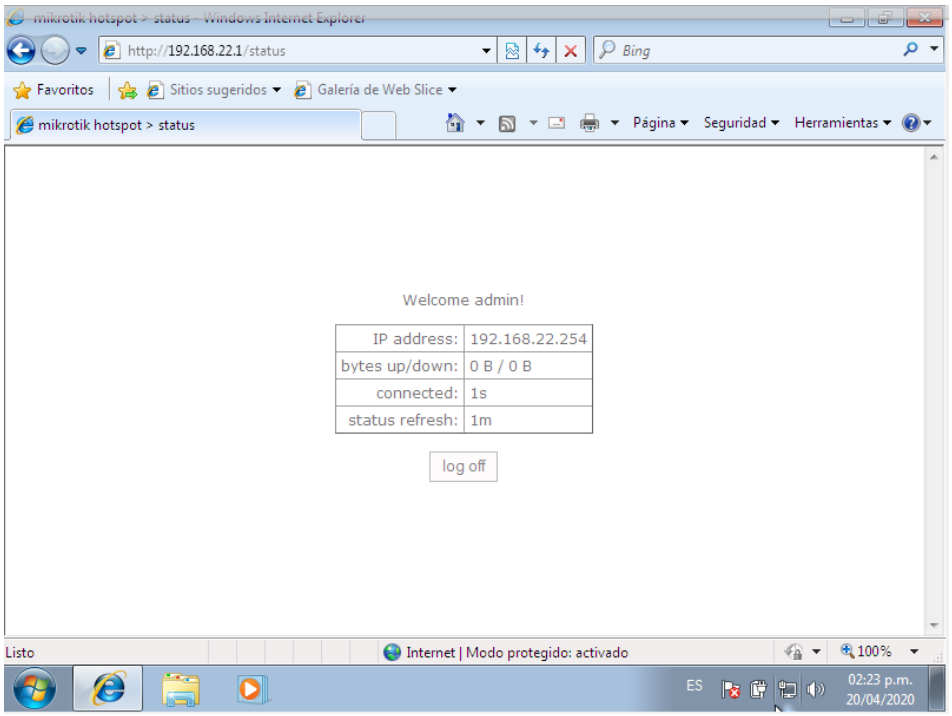
Ilustración 106 Configuración nuevo usuario hotspot



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Finalmente se procede probar la conexión *hotspot* a través del usuario. Para ello hay que conectarse en un equipo y en el explorador se debe entrar a la página de la Mikrotik y registrar la IP que se le asigno desde un principio **"192.168.22.1".** Si se tiene acceso y aparece la pantalla de *logueo*, significa que el *hotspot* fue iniciado correctamente.

Ilustración 107 Mikrotik con conexión a internet



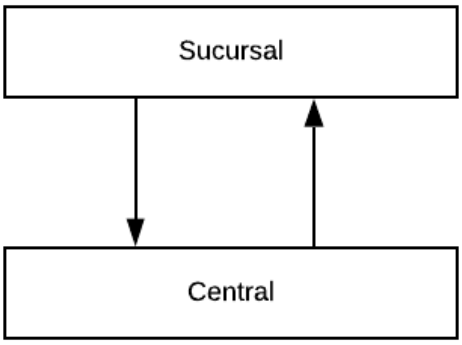
***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

4.D.a. Comunicación con sucursales

4.D.a.i- Protocolo IPSEC

Para comunicar una o más sucursales con la oficina central, se debe asegurar que el tráfico de datos, entre las oficinas, viaje seguro. Para realizar esto se construirá un túnel IPSEC entre los *routers* de los edificios y emplearemos el protocolo ESP, para garantizar la confidencialidad de los datos.

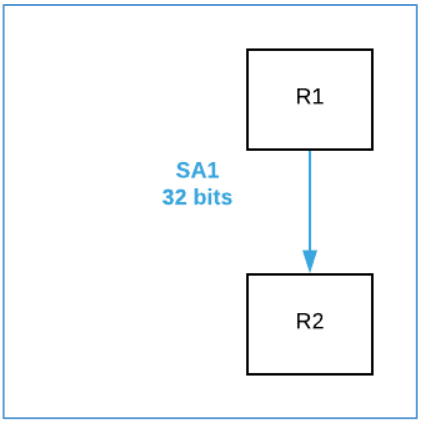
Ilustración 108 : Comunicación con sucursales



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Lo primero que se debe hacer, es crear dos asociaciones de seguridad, una por cada sentido del tráfico, que definen un conjunto de parámetros para una sesión segura. Para la asociación de seguridad 1, de R1 a R2 habrá que identificarla por un numero de 32 bits, el SPI (*Security Parameter Index*), su interfaz de origen, en este caso la R1 y su interfaz de destino, en este caso la R2

Ilustración 109 : Asociación seguridad R1 a R2



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Los parámetros de seguridad que se seleccionen para esta asociación de seguridad serán “1” (SA1), Cifrado Simétrico a usar, su clave, algoritmo de integridad, clave de autenticación, los guardaremos en R1 en su base de datos con todas las asociaciones de seguridad, esta base de datos se conoce como *Security Association Database* (SAD).

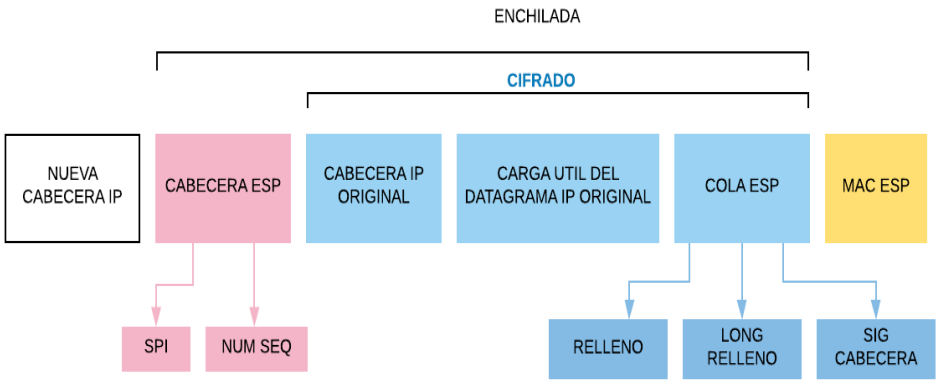
Es importante resaltar que a estos mismos parámetros se los deberá tener en el otro extremo (R2) en su base de datos SAD, para poder descifrar el contenido.

Estos parámetros se deben comunicar de forma segura a R2. En R1 se tendrá otra base de datos, la *Security Polcy Database* o SPD con todas las políticas de seguridad a aplicar. Cuando llega un datagrama al router se deben controlar ciertos valores del mismo, IP origen, IP destino, Puerto Origen, Puerto Destino, etc. Y buscaremos en la SPD que hacer con el datagrama, descartarlo, dejarlo pasar tal cual, o protegerlo con IPSEC, quien indicara la asociación de seguridad a aplicar.

Una vez que R1 conoce la asociación de seguridad que debe aplicar al datagrama le añade al final del mismo un campo, la cola ESP, para rellenar y poder aplicar el algoritmo de cifrado y clave que indique la asociación de seguridad en la base de datos SAD. Una vez que se tiene el datagrama original más la cola de cifrado, se le añade la cabecera ESP, donde se incluye el identificador SPI de la asociación de seguridad utilizada, y un numero de secuencia incremental para evitar ataques de *replay* o por reproducción. De esa forma cuando R2 reciba el nuevo datagrama, podrá con esta cabecera buscar en su SAD la asociación de seguridad que corresponda con el SPI, el índice enviado. Y comprobar también que el número de secuencia está dentro del rango de recepción esperada y que no se trata por lo tanto de un replay.

El datagrama cifrado junto con la cabecera ESP se suele llamar “Enchilada”.

Ilustración 110 Datagrama



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Paso siguiente, se debe autenticar la enchilada. Para concretarlo, R1 consulta el algoritmo de integridad y clave de autenticación especificados para esa asociación de seguridad y genera un Código de Autenticación de Mensaje (MAC) que añade al final del paquete formando así la nueva carga útil del datagrama. Crea también una cabecera IP nueva con todos los campos típicos IPV4 y la añade al principio. En la nueva cabecera IP el destino será R2 y es el equipo que esta al final del túnel, este al descifrar el datagrama original podrá leer el destinatario final en la cabecera IP de ese datagrama original que va cifrado.

4.D.a.ii- Ataque

Ante la suposición que un intruso intenta realizar un ataque “*man-in-the-middle*” entre R1 y R2 sin conocer ninguna de las claves. El intruso se verá imposibilitado con las siguientes acciones:

- ✓ No podrá ver el contenido del datagrama original porque este se encuentra cifrado. Tampoco podrá ver las direcciones IP de origen ni destino, ni el protocolo de transporte o el puerto de aplicación porque la cabecera original también está cifrada.

✓ Tampoco podrá intercambiar *bits* sin ser detectado porque el hash garantiza la integridad del paquete.

✓ Como el intruso no conoce la calve de autenticación que utiliza R1, tampoco tendrá éxito al intentar suplantarlo utilizando la dirección IP de R1.

✓ Al utilizar número de secuencia para identificar el datagrama esperado por el destino, tampoco podrá reproducir un datagrama, por lo tanto, no podría realizar un ataque de *replay*.

4.D.a.iii- Protocolo IPSEC IKE

Antes se solía establecer manualmente las asociaciones de seguridad en los terminales IPSEC pero esto no es escalable ni dinámico, en su lugar empleamos IPSEC IKE (Internet *Key Exchange*), que es un conjunto de protocolos que van a permitir el intercambio de las claves necesarias para que las SAD de ambos extremos de una asociación de seguridad tengan la misma información.

Se divide en dos fases, en la primera se crea un canal seguro bidireccional entre los dos equipos denominado *ISAKMP* (Marco de gestión de claves), y en la segunda fase se negocia los parámetros para crear las asociaciones de seguridad necesarias entre ellos. Se pueden crear varias asociaciones de seguridad utilizando el mismo canal ISAKMP de la fase 1.

4.D.a.iii.1- Fase 1

En esta fase el objetivo es crear un canal IKE seguro, para ello se debe primero definir que método se utilizara para el cifrado (DES CBC, triple DES), lo mismo con el algoritmo de autenticación (MD5, SHA) y para la autenticación (clave compartida, publica, certificados). Luego se tiene que intercambiar los parámetros públicos, para generar el secreto compartido y claves derivadas.

Por último, se autentican los nodos cifrándolos, este es el modo principal o bien no cifrándolos que sería un modo agresivo el cual es más rápido.

4.D.a.iii.2- Fase 2

Se deben negociar los parámetros de la asociación de seguridad, para lo cual se establece una asociación de seguridad en cada sentido de la comunicación especificando el protocolo ya sea AH o ESP. El modo, ya sea transporte o túnel. El cifrado y la integridad que vamos a aplicar y otros parámetros como el SPI, tiempo de vida, etc. Todos estos parámetros irán cifrados de forma segura gracias a la fase previa, la fase 1.

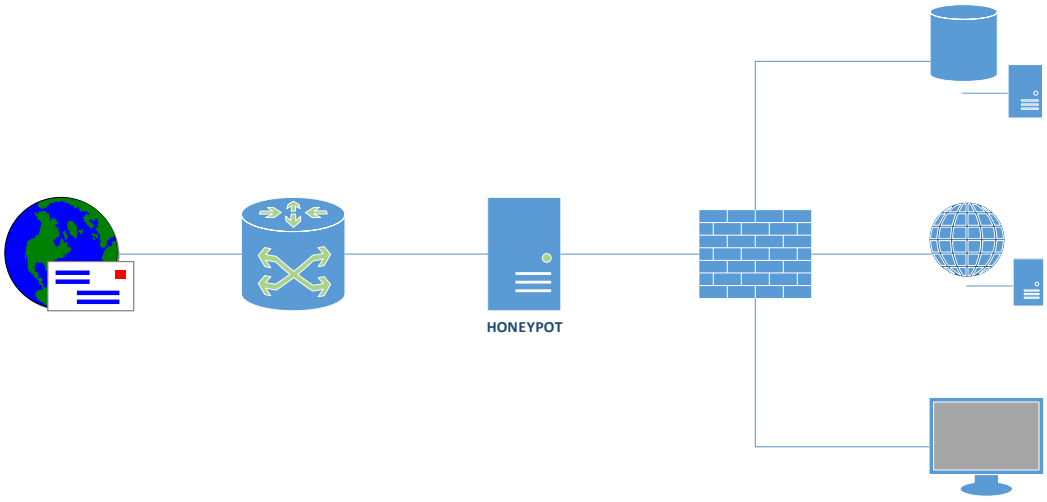
Una vez terminadas ambas fases se pasa al intercambio de datos con IPSEC ya en funcionamiento de forma completamente segura.

4.E Detección de intrusos

Otro sistema que se emplea de forma complementario a los mecanismos de defensa de nuestra red, son los "*Honeypots*", el cual es un sistema trampa para observar el comportamiento de un *ciber* ataque y analizar la intrusión y método utilizado. Estos sistemas simulan ser equipos vulnerables para atraer a los atacantes, por lo tanto permiten analizar y conocer las vulnerabilidades de nuestros sistemas, recoger información sobre nuevos métodos de ataque y herramientas hasta ahora desconocidas por nosotros, desviar la atención del atacante para salvar el sistema principal, disuadirlo, ganar tiempo para poder reaccionar y tomar las medidas necesarias para rechazar el ataque, también capturar nuevos tipos de *malware* o *zero-days* para su estudio, o también realizar la trazabilidad de los puntos de origen de los ataques obteniendo direcciones IP de atacantes para incorporarlas a la base de datos.

Para ello necesitamos que el *honeypot* sea atacado por lo que tiene que ser un sistema que este expuesto y sea lo más realista posible, conectado a nuestra red real, aunque se generan datos y procesos falsos, pero siempre convenientemente separado del resto de sistemas de la red para que estos no se vean comprometidos. Desde la organización, nadie debe llegar al *honeypot*, para que todo lo que llegue a este sistema se clasifique como un potencial ataque externo, a no ser que se diseñe el *honeypot* para detectar también amenazas internas.

Ilustración 111 Honeypot



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Si el objetivo es detectar ataques *zero-days* se debe proteger el honeypot al máximo para que solo esos ataques desconocidos lo afecten, si se quiere recolectar información de los atacantes se debe dejar al *honeypot* más expuesto. Por lo general actúan junto con los IDPS para que luego de detectar un ataque, se recompongan las trazas del atacante, toda la secuencia de paquetes registrados por el sensor del *honeypot* y se realiza un análisis por índice. De esta forma si se trata de un nuevo ataque se incorporan las nuevas reglas de detección al IDPS.

Si el Honeypot lo utilizamos para defender una red o reducir los daños de los ataques se habla de **"*Honeypot* de producción",** mientras que si lo utilizamos para recolectar información del atacante como sus estrategias, herramientas, etc. se denomina **"*Honeypot* de investigación".**

4.E.a. Tipos de HoneyPot

Los *honeypot* se pueden clasificar según la posible interacción con el atacante y lo que se le deje hacer

1º *Honeypot de baja interacción*: Emulan una parte de un sistema muy concreto, normalmente se instalan como una aplicación en un host, y solo sirven para detectar y recolectar información sobre ataques muy concretos. Es tipo *sandbox*, aislado del resto de sistemas, por lo que la información que se obtiene es muy básica. Son sencillos de instalar e implican poco riesgo, el atacante puede seguir explotando vulnerabilidades, pero siempre dentro del propio host. Los *honeypot* más sencillos y flexibles son los de monitorización de puertos, que mediante aplicaciones o servicios escuchan determinados puertos y responden simulando los servicios reales, generando las alertas y logs correspondientes.

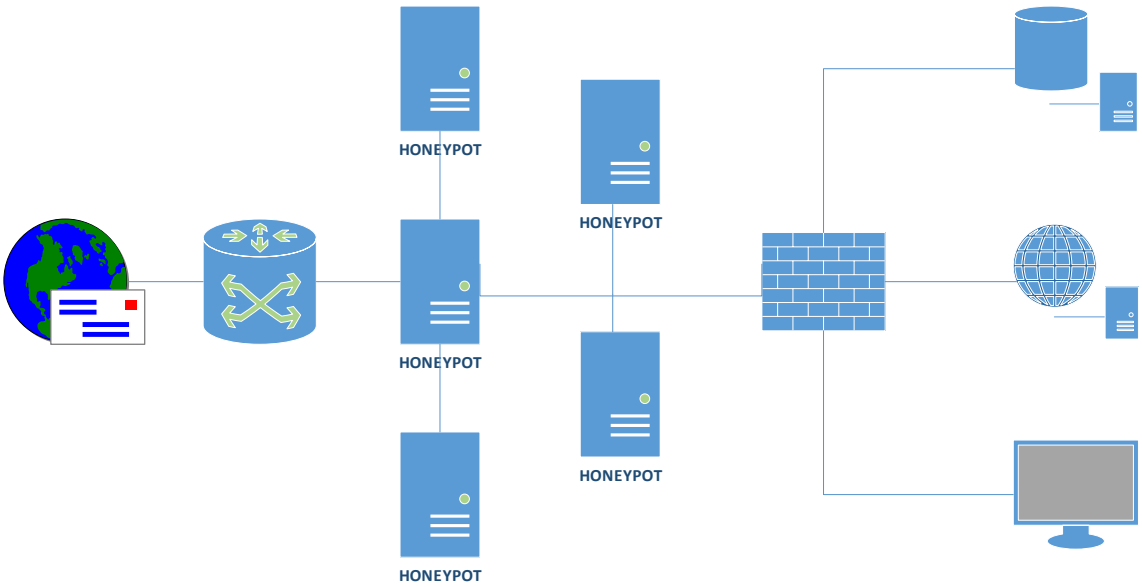
2º *Honeypot de mediana interacción:* Añaden algo más de complejidad al anterior para poder recolectar más información del ataque, por lo que hay que tener más precauciona a la hora de configurarlo y de proteger correctamente el resto de la red ya que implican mayor riesgo. Un ejemplo son los *honeypot* jaula *(jail honeypot)* que crean un entorno virtual que simula un sistema operativo real de manera que el atacante queda confinado en el consumiendo tiempo y recursos, y sin poder utilizarlo como plataforma para poder atacar otros sistemas ya que se encuentra muy limitado.

3º *Honeypot de alta interacción*: Son sistemas completos mucho más realistas que recogen toda la información necesaria, pero son muy laboriosos de configurar y analizar, además de ser más peligrosos ya que un atacante lo podría utilizar como puente para atacar nuestra red, por lo que hay que extremar las precauciones. Un ejemplo de *honeypot* comercial con media-alta interacción es *ManTrap,* que permite crear hasta 4 sistemas operativos virtuales en los que el atacante tiene completa libertad, con los riesgos que eso conlleva, pero está siendo monitoreado y sus pasos quedan registrados.

4.E.b. HoneyNet

Los *honeypot* de alta interacción por excelencia son los *HoneyNet*, el cual es un conjunto de *honeypots* de alta interacción que conforman una red completa, con los objetivos de prevención, detección y respuesta a los ataques. Realmente es como montar una red corporativa con sus ordenadores, servidores, *routers, switches*, etc. pero en la que no hay datos sensibles reales y en la que todo está siendo monitorizado y registrado.

Ilustración 112 Honeynet



***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

La gran dificultad de las *honeynets* es implementar esas medidas de control que capturan todas las actividades que suceden en los *honeypots*. Son soluciones costosas de desplegar y mantener, aunque la aparición de *honeynets* virtuales las han hecho más accesible para todo tipo de entornos.

4.F. Guía de configuración para una red wifi-segura

El primer paso de los delincuentes cibernéticos para tomar control de cualquier dispositivo IoT de un hogar o del entorno de una empresa es tener acceso al *router wifi* al cual está conectado dicho positivo, lo cual se puede lograr con distintos métodos. En este apartado vamos a ver algunos de estos métodos, y explicar una serie de configuraciones básicas para tener una red wifi más segura.

4.F.a. Cifrados

Existen distintos tipos de cifrados para una contraseña de wifi. Se exponen a continuación cuáles son estos tipos y cuáles son los más recomendables.

4.F.a.i- Sin cifrado

En esta opción, como su nombre lo indica, la red wifi está abierta a todos los usuarios. Cualquiera que desee podrá conectarse a la red sin necesidad de ingresar ninguna contraseña. Esta opción obviamente es solo recomendable para aquellos puntos de acceso públicos, en los que cualquier usuario puede conectarse de forma abierta y gratuita. Esta red solo debe usarse para brindar conexión a los usuarios, no se debe tener equipos que tengan información, ni equipos IoT a los que cualquier usuario conectado a la red pueda tener control sobre ellos.

4.F.a.ii- Cifrado WEP

Este tipo de cifrado fue de los primeros que se empezaron a aplicar hace ya varios años, utiliza calves de 63 *bits* o de 128 *bit*s. Es un cifrado débil y se pueden conseguir las claves en pocos minutos mediante programas que capturan paquetes mediante falsas solicitudes.

Este cifrado ofrece una protección insuficiente, por lo que no es recomendable su uso.

4.F.a.iii- Cifrado WPA (Wi-Fi Protected Access)

WPA nació a partir de corregir las principales debilidades del cifrado WEP. Se diferencia porque utiliza un vector de inicialización de 48 *bit*s y una clave de

cifrado de 128 *bits*. Lo importante es que utiliza lo que se denomina protocolo de integridad de clave temporal (TKIP). En el cifrado WEP se utiliza la misma clave para cifrar todos los paquetes que fluyen a través de la red, WPA con TKIP, cambia la clave de cifrado cada vez que un paquete se transmite. Esto combinado con el uso de claves más largas, impide que un router sea fácilmente accedido solo a través de la observación de un conjunto de transmisión de paquetes.

4.F.a.iv- Cifrado WPA2

Es la versión certificada del estándar de la IEEE de WPA con algunas actualizaciones como el uso de cifrado AES. Mejora tanto la seguridad como el rendimiento y dispone de calves personales PSK y autenticación RADIUS para entornos empresariales.

4.F.b. TKIP (Protocolo de Integridad de Calve Personal) y AES (Advanced Encryption Standard)

TKIP significa “protocolo de integridad de calve personal”, es un protocolo de encriptación provisional introducido con WPA para reemplazar el cifrado WEP que se veía muy afectado por la inseguridad, aunque TKIP es en realidad muy similar a WEP.

AES *(Advanced Encryption Standard*), es un protocolo de cifrado más seguro introducido con WPA2, que reemplazo el estándar WPA. AES no es una norma creada específicamente para redes *wifi*, es un estándar de cifrado usado globalmente, incluso ha sido adoptado por el gobierno de Estados Unidos. Se considera generalmente muy seguro. Su debilidad sería un ataque de fuerza bruta (probar todas las combinaciones posibles hasta encontrar aquella que permita el acceso), el cual se puede impedir usando una contraseña segura.

PSK: Significa “llave pre-compartida”, es una clave secreta compartida con anterioridad entre las dos partes usando algún canal seguro antes de que se utilice. El punto de acceso y todos los clientes comparten la misma clave. Esto lo distingue de WPA-Enterprise, que utiliza un servidor RADIUS, que crea de forma aleatoria claves únicas en redes corporativas o gubernamentales.

4.G. Cifrado recomendable

Siempre que se pueda se debe elegir la mejor protección de nuestra red *wifi* el sistema WPA2-Personal con cifrado AES (si el router no especifica TKIP o AES, la opción WPA2 probablemente utilizara AES). Se debe evitar siempre el método de conexión abierto y WEP ya que son los que más comprometen la integridad de nuestra conexión inalámbrica.

Otro aspecto importante con respecto a las contraseñas es la contraseña propiamente dicha que se elige. A la hora de configurarla hay q ser originales y evitar usar contraseñas típicas ya que si se produce un ataque sería una clave fácil de descifrar. Hay que utilizar claves largas y seguras, hoy en día en todos los sitios al crear una cuenta se recomienda una contraseña segura y hasta vemos medidores que detectan si una contraseña es fuerte o débil. Para que una contraseña sea fuerte, es decir difícil de extraer, se deben combinar letras y números, mayúsculas y minúsculas, y signos especiales. Un consejo es cambiar letras por símbolos, por ejemplo “a” por “@”, o las “o” por “0”.

4.H. Prueba Experimental

Como se dijo anteriormente, el primer paso para lograr tomar control de los dispositivos IoT o simplemente obtener información de ellos, es poder ingresar al *router* en el cual está conectado el dispositivo. En este primer experimento usaremos una herramienta, la cual ya viene incluida en el sistema operativo “Kali” de Linux, denominada “airmon-ng”, utilizada para probar la seguridad de las redes en un *router* determinado, el cual podemos observar a primera vista que cuenta con una contraseña tipo WEP, la más sencilla de atacar.

La herramienta inicia buscando un cliente activo en el router, copia su dirección MAC, y comienza a capturar y a inyectar paquetes. De esta forma *desencriptar* la contraseña. Luego de unos veinte minutos de trabajo la herramienta ha obtenido la

contraseña "*flopy"*, como podemos ver es una contraseña muy débil, que justifica el corto tiempo que costó obtenerla.

Una vez obtenida la contraseña conectamos un teléfono Samsung Galaxy A3 a la red, a este equipo se le instalo la aplicación para Android "Quien está conectado" que permite escanear los equipos conectados a la red, obteniendo su dirección IP, su dirección MAC, tipo de dispositivo e incluso la marca o el fabricante del mismo.

Ilustración 113 Dispositivos en la red

***Fuente*: Aldo G. Arzelán - TFG: Seguridad en el internet de las cosas (IoT) - Ucasal - Año 2020**

Con el escaneo terminado no solo se obtiene la información de todos los equipos con los que cuenta una red determinada, sino que también se extrae la información exacta del equipo que se quiera atacar. De esta forma se puede tener información detallada de todos los dispositivos conectados a la red y que acciones se puede realizar con ellos, así como también la información que se puede obtener de ellos

4.I. Claves por defecto

En la introducción de este documento se nombró el ataque del día 21 de octubre del 2016, como se mencionó, este ataque se pudo realizar por la gran cantidad de dispositivos IoT conectados, enviando información ficticia al servidor y de esta manera lograr saturarlo para impedir que brinde su servicio con normalidad. En este caso, los atacantes descubrieron una brecha en cámaras de seguridad, a las cuales los usuarios nunca modificaron el usuario y contraseña con el que vienen por defecto, logrando de esta manera tener acceso a una inmensa cantidad de equipos con los cuales inyectaron la información necesaria para saturar los servicios. Vemos como es de suma importancia modificar los usuarios y contraseña por defecto, ya que basta con buscar en Google el producto para tener esta información.

Se puede apreciar que mantener los datos de acceso que vienen por defecto en cualquier equipo es un grave error, el cual cometen la gran mayoría de los usuarios, sin importar de que equipo se trate. Es posible que las personas asumieron que si alguien lograba acceder a una simple cámara de seguridad, teniendo el control de ella los ciberdelincuentes no podrían tomar ninguna acción. Imagínense que se cometa el mismo error por ejemplo con un horno de microondas y el delincuente tome control sobre el equipo, podría mandarle la orden de calentar durante horas provocando una explosión o un incendio y el daño podría ser físico sobre un grupo familiar especifico. Otro ejemplo sencillo seria si toman control sobre un televisor, consola de video juegos y auriculares el cual es utilizado por niños de muy poca edad, los delincuentes podrían reproducir un video amenazante produciendo miedo en el niño para manipularlo y obligarlo a realizar alguna acción. Con la tecnología 8D y los sonidos que se pueden recrear no sería una tarea difícil para los delincuentes inducir miedo en las personas.

De la mano con las contraseñas por defecto, se debe tener presente la complejidad de las contraseñas usadas, ya que la gran mayoría utiliza como contraseña sus iniciales combinadas con fecha de nacimiento, nombre de familiares, fecha de nacimiento de familiares, por dar ejemplos, y esta información es sumamente fácil de

encontrar en la mayoría de los casos, basta solo con entrar al perfil de Facebook o Instagram y buscar un poco. Por esto es recomendable no utilizar como contraseña información personal, se recomienda utilizar palabras sin sentido, frases sin sentido, y números sin sentido, combinándolos también con signos.

4.J. Recomendaciones

- **Cambiar el nombre de usuario:** Este es el primer y más importante paso, cambiar inmediatamente el nombre de usuario y contraseña que trae por defecto el *router*. Todos los *router* tienen un sitio *web* que permite modificar la configuración, y en la mayoría el nombre de usuario que viene por defecto es *"admin*", ya conocido por los cibercriminales, de no ser este seguramente se encuentra publicado el nombre de usuario que corresponde al modelo del router.
- **Cambiar el *firmware Alrededor*** del 80% de los principales vendedores de routers "hogareños" los envía con vulnerabilidades críticas conocidas, por lo que estos son presa fácil para los atacantes. Es recomendable instalar un *firmware open source* alternativo en el dispositivo. Estas versiones que reemplazan el *firmware* oficial, por lo general son más seguras.

  Algunas alternativas disponibles:

  - Tomato firmware: http://www.polarcloud.com/tomato
  - DD-WRT: http://www.dd-wrt.com/site/index
  - Open-WRT: https://openwrt.org/
- **No divulgar el nombre de tu red**

  Las redes Wi-Fi tienen un nombre que las identifica conocido como SSID, al conectar el *router* por primera vez muestra un nombre por defecto, el cual le dice a un potencial atacante la marca y/o el modelo de router, información que puede ser muy útil, ya que como dije anteriormente algunos modelos tienen vulnerabilidades conocidas.

  Por lo tanto, una buena opción es convertir la red en una "red oculta", deshabilitando la opción de mostrar el nombre del SSID. Con esto, la red será menos visible para los atacantes. La única desventaja es que cuando quieras

conectar un dispositivo a la red deberás teclear el nombre que elegiste para buscarla.

- **Controlar quien se está conectando a tu red**

  Cada dispositivo tiene un numero único de identificación, más conocido como dirección MAC. Al acceder a la configuración de tu *router*, se puede ver los dispositivos conectados a tu red, o bien usar la aplicación que vimos anteriormente para hacerlo. De esta manera se puede identificar si algún dispositivo desconocido está conectado a tu red. En la configuración del *router* también se puede elegir que equipos pueden conectarse a la red y cuáles no (lista blanca y lista negra), con esta opción podemos o bien negar el acceso a un dispositivo, en el caso de ver alguno desconocido conectado a la red le negamos el acceso poniendo en la lista negra la dirección MAC de dicho dispositivo, o bien armando una lista blanca con todos los dispositivos del hogar que se van a conectar a la red, de esta manera solo los dispositivos que estén en la lista podrán conectarse, impidiendo que dispositivos desconocidos lo hagan.

CAPITULO 5

5. Conclusiones y futuras líneas de trabajo

En este proyecto, he tenido como propósito mejorar las condiciones en las que se trabaja con la información de las personas en especial en el rubro de la Salud. En el desarrollo de este trabajo se pudo observar que existen factores tanto internos de la institución, y principalmente el factor humano el cual debe ser evaluado y en base a esto implementar programas de capacitación para que el personal sepa cómo reaccionar ante un posible ataque cibernético.

Como futuras líneas de trabajo, se podría continuar con la implementación de medidas a nivel de Dominio de las contramedidas sobre las amenazas encontradas

Finalmente deseo destacar que, haciéndome eco de los valores éticos y morales de mi formación, como así también respondiendo a los preceptos de la Responsabilidad Social de nivel profesional que me competen, es que se desarrolló el presente proyecto, con la sola intención de concretar un servicio de seguridad informática destinada a la población con fines netamente sociales.

CAPITULO 6

6. Bibliografía

Bibliografía

Nicoletti, P. M.-S. (2017). *Ciudades inteligentes e internet de las cosas.* Barcelona, España: GSMA.

Pisano, I. A. (2018). *Tesis de Maestria en Gestion de Servicios.* Buenos Aires, Argentina: Universidad de San Andrés.

- https://www.espacioasesoria.com/Noticias/el-internet-de-las-cosas-iot-y-su-regulacion-legal-
- https://www.espacioasesoria.com/Noticias/el-internet-de-las-cosas-iot-y-su-regulacion-legal-
- https://www.welivesecurity.com/la-es/2019/05/06/legislar-seguridad-dispositivos-iot/
- https://www.google.com/url?sa=D&q=https://www.welivesecurity.com/la-es/2018/10/08/ley-obligara-dispositivos-inteligentes-vendan-sin-contrasenas-predeterminadas/&ust=1614463020000000&usg=AOvVaw3EfYFamZaVxc3ByZ8Ht0df&hl=es&source=gmail
- https://www.welivesecurity.com/la-es/2019/05/06/legislar-seguridad-dispositivos-iot/
- https://expansion.mx/tecnologia/2018/09/03/el-uso-de-iot-en-el-sector-salud-una-herramienta-de-doble-filo
- https://www.statista.com/study/27915/internet-of-things-iot-statista-dossier/
- https://www.google.com/url?sa=D&q=https://www.interempresas.net/TIC/Articulos/252927-IoT-sacando-partido-al-mundo-hiperconectado.html&ust=1614463320000000&usg=AOvVaw3okHuQj_NzUn1s9TBrKTqF&hl=es&source=gmail
- https://www.networkworld.es/archive/los-dispositivos-conectados-son-un-grave-peligro-para-la-medicina
- https://cso.computerworld.es/alertas/iot-en-hospitales-uno-de-los-grandes-objetivos-de-los-ciberdelincuentes
- http://www.automaticaeinstrumentacion.com/es/notices/2019/10/microchip-simplifica-la-seguridad-de-iot-basada-en-hardware-45801.php

- https://www.xataka.com/seguridad/silex-agresivo-malware-que-lleva-2000-dispositivos-iot-bloqueados-que-quiere-poner-jaque-al-mundo-proximos-dias
- https://cso.computerworld.es/proteccion-de-datos/muchos-hospitales-transmiten-los-datos-sin-cifrar
- https://markamagazine.com/ciudades-inteligentes-seguras-sostenibles-y-el-iot/

Tabla de ilustraciones

Tabla de gráficos

CAPITULO 7

7. Anexos

VULNERABILIDAD DEL INTERNET DE LAS COSAS DELITOS DERIVADOS Y OBTENCION DE EVIDENCIA FORENSE.

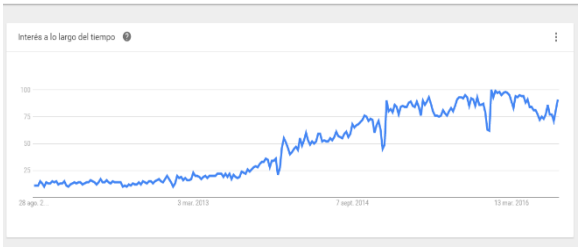
Bonfiglioli, Ernesto; Arzelan, Aldo; Gómez Castro, Fabio
UCASAL, Facultad de Ingeniería

I. Introducción:

Podríamos definir el internet de las cosas como la consolidación a través de la red de redes de una "red" que interconecta una gran variedad de objetos o dispositivos, es decir poder tener conectadas todas las cosas de este mundo como podrían ser vehículos, electrodomésticos, dispositivos mecánicos, o simplemente objetos sencillos como ser calzados, muebles, maletas, dispositivos de medición, biosensores, o cualquier objeto que nos podamos imaginar.

El gran objetivo de esta tecnología es hacer más cómoda la vida de las personas, así como también proporcionar una mayor seguridad en diversos ámbitos. Esta se puede tomar como un arma de doble filo, ya que al brindar seguridad si se desea también puede ofrecer todo lo contrario. Las consecuencias de los problemas de seguridad son cada vez más graves, ahora pueden ser daños físicos a las personas.

En el siguiente gráfico se puede apreciar cómo fue aumentando el interés de las personas en el IOT a través de los años. Se asegura que este año alrededor de 6.4 billones de "Things" (cosas) se encuentran en uso, un 30% más que el año pasado y que para el 2020 alcanzará 20.8 billones. En el presente 5.5 millones de nuevas "Cosas" (dispositivos IOT) se conectan cada día.



II. Vulnerabilidad del Internet de las Cosas:

Al momento de crear tecnología es imposible cuidar cada aspecto de la seguridad de la misma, esto se dificulta aún más, ya que personas con conocimiento en este tema dedica sus esfuerzos a encontrar nuevas formas de violar la seguridad de los equipos tecnológicos.

El internet de las cosas no está exento de este peligro, debido a que es un objetivo al que, si se llegara a alcanzar, se tendría acceso a información personal de sus usuarios y perjudicarlos de gran manera debido a la forma en que los dispositivos IoT se han instalado en los aspectos más importantes de la vida diaria de las personas.

Es por eso que el objetivo que sustentará todo el trabajo que se realizará a futuro es identificar y estudiar los puntos débiles en la seguridad del internet de las cosas. Para ello hemos iniciado una recopilación de información con el fin de encontrar documentación que nos ayude a encontrar dichas vulnerabilidades.

Nos hemos enfocado en una primera instancia en herramientas de desencriptación Wifi, ya que este es el primer paso para hacer una intrusión en los equipos de los hogares. Buscamos encontrar métodos que usen el bluetooth de ciertos equipos y medios electrónicos.

Lo que buscamos es lograr entender las formas de intrusión con el fin de ser capaces de reproducirlas en nuestros equipos para entender a fondo las vulnerabilidades de IoT.

III. Delitos Derivados:

Nuestro trabajo tiene como segundo eje el analizar los delitos no solo informáticos que pueden llegar a cometerse una vez vulnerada la seguridad de los Equipos IoT. En el mundo ya se han reportado casos de secuestro, y extorsión, pero existe un gran número de riesgos.

Por ello buscamos encontrar los tipos de delitos que pueden conocerse, nos interesa reproducirlos en ambientes controlados, Indagar en el conocimiento que lo usuarios comunes tienen de estos riesgos, que medidas toman para resguardarse de ello y como actuarían en caso de que su seguridad haya sido vulnerada,

Buscamos generar conciencia de los peligros de no contar con medidas de seguridad y así también poder sugerir formas de protección de los mismo. Como también formas de actuar en caso de sufrir un ataque de algún tipo.

IV. Evidencia Forense:

El siguiente objetivo busca conocer la información que circula por los equipos IoT, los que los controlan y las interfaces de los usuarios. Con el fin de encontrar nuevos métodos de obtener evidencia, tanto de delitos informáticos, como de cualquier otro tipo, con el fin de que puedan ser usadas para demostrar la culpabilidad de delincuentes.

V. Extorsión usando Smart TV's

En nuestros primeros pasos para entender la vulnerabilidad de las cosas nos enfocamos en un tipo de delito que ha comenzado a emerger en estos días. Se trata del envío de amenazas y extorsiones a través de los televisores inteligentes,

El acto consiste en transmitir un video previamente editado en los Smart TV's cuando estos están siendo utilizados por sus dueños. De esta forma el delincuente logra tomar por sorpresa a las personas ingresando a su hogar de forma remota. En el video se puede ver imágenes borrosas del individuo o hasta imágenes tomadas de las víctimas, sin saberlo con anterioridad. Todo esto con el fin de intimidar a las víctimas para después mostrar en pantalla un código QR, con una voz distorsionada diciendo que para asegurar su bienestar es necesario que depositen una cantidad determinada de bitcoins, una moneda digital, en la dirección que contiene el código QR. Mucha persona asustada por la perturbadora intrusión en su hogar obedece a las demandas del delincuente, con el fin de proteger a su familia.

VI. Experimentación:

El primer paso para lograr enseñar este método delictivo en nuestros propios equipos es lograr desencriptar la contraseña del equipo de ruteo wifi. De esta forma tendremos acceso a la red y luego a los equipos conectados a ella.

En este primer experimento usaremos una herramienta utilizada para probar la seguridad de las redes en un router determinado, el cual podemos observar a primera vista que cuenta con una contraseña tipo wep, la más sencilla de atacar.

La herramienta inicia buscando un cliente activo en el router, copia su dirección MAC, y comienza a capturar y a inyectar paquetes. De esta forma desencriptar la contraseña. Luego de unos veinte minutos de trabajo la herramienta ha obtenido la contraseña "flopy", como podemos ver es una contraseña muy débil, que justifica el corto tiempo que costó obtenerla.

Una vez obtenida la contraseña conectamos un teléfono Samsung Galaxy A3 a la red, este equipo tiene una aplicación que permite escanear los equipos conectados a la red, obteniendo su dirección Ir, su dirección MAC, tipo de dispositivo e incluso la marca o el fabricante del mismo.

La siguiente imagen muestra el resultado del escaneo de la aplicación. En la primera fila podemos observar los datos del router, en la segunda fila los datos de nuestro teléfono conectado a la red, en la tercera observamos los datos de un Smart TV, el cual es el objetivo de ataque en este experimento, y en la cuarta fila podemos observar un dispositivo con menos información, pero nosotros sabemos que es una consola de juegos de video Sony PlayStation 4.

Con el escaneo terminado no solo obtenemos la información de todos los equipos con los que cuenta un hogar determinado, sino que también obtenemos la información exacta del Smart Tv que queremos atacar. De esta forma sabremos si contamos con un dispositivo compatible para transmitir el video, o bien, tenemos la información necesaria para saber qué herramienta usar para hacer la transmisión.

De esta forma no quedan obstáculos que impidan la transmisión de un video extorsivo a un grupo de individuos que se encontraban disfrutando de un momento de entretenimiento sin imaginar lo que estaba ocurriendo.

VII. Conclusiones y Trabajos Futuros:

Hemos podido observar que no es complicado obtener la información de los dispositivos conectados a una red. Esto se debe primero a la facilidad de obtención de las herramientas necesarias para hacerlo y la negligencia de las personas al no gestionar la seguridad de su red, como claramente observamos en la contraseña desencriptada.

Y este trabajo es solo el comienzo para futuras experiencia ya que desde este punto se pueden analizar otro tipo de ataques y delitos. Como así también la búsqueda de información que evidencie el delito que se ha cometido.

Un aspecto importante observado fue que el uso de una computadora portátil para desencriptar contraseñas Wifi es poco discreto. Por lo que consideramos necesario estudiar la posibilidad de realizar esta operación desde un teléfono celular. Lo que permitiría a un delincuente realizar ataques sin levantar sospechas.

VIII. Referencias:

I. Nieto, R. Roman, and J. Lopez, “Testigo digital: delegaci´on vinculante de evidencias electr´onicas para escenarios IoT”, II Jornadas Nacionales de Investigaci´on en Ciberseguridad (JNIC 2016), pp. 109-116, 2016.
II. Andrés Alejandro Pazmiño Caluña, Aplicación de Hacking Etico para la determinación de vulnerabilidades de Acceso a Redes Inalámbricas WIFI, Escuela Superior politécnica de Chimborazo
III. Shancang Li , Theo Tryfonas , Honglei Li , (2016) "The Internet of Things: a security point of view", Internet Research, Vol. 26 Iss: 2, pp.337 – 359

Categoría:
Trabajos de Alumnos

UCASAL
UNIVERSIDAD CATÓLICA DE SALTA

4to Congreso Nacional de Ingeniería en Informática / Sistemas de Información
CoNaIISI 2016
17 y 18 de Noviembre
Salta | Argentina

VULNERABILIDADES DEL INTERNET DE LAS COSAS Y DELITOS DERIVADOS

Abstract

Es muy común en estos tiempos encontrar objetos inteligentes interactuando en cada ámbito de la vida cotidiana de las personas, como ser escuelas, hospitales, en el trabajo y en el hogar. La gran variedad de dispositivos que abarcan el mercado IoT y los que vendrán, cada uno con características particulares, han dejado abierta la posibilidad de que los ciberdelincuentes puedan usar sus habilidades no solo para tener acceso a la información privada que estos dispositivos manejan. En este escrito describiremos uno de los delitos más sencillos que pueden ocurrir: la extorsión a una familia tipo. Y se mostrará la preocupante facilidad con la que esto puede ser perpetrado por un tercero, con el fin de generar y poder buscar formas de proteger a los usuarios e indicar como actuar en caso de sufrir un hecho similar.

Introducción

Se han reportado múltiples casos de ciberdelitos que se han cometido usando como medio de ingreso dispositivos IoT a empresas, instalaciones gubernamentales y hogares .
En nuestros primeros pasos para entender la vulnerabilidad del internet de las cosas nos enfocamos en un tipo de delito que ha comenzado a emerger en estos días. Se trata del envío de amenazas y extorsiones a través de los televisores inteligentes como podemos observar en la representación de la **figura 1**. El acto consiste en transmitir un video previamente editado en los Smart TV's cuando estos están siendo utilizados por sus dueños. De esta forma el delincuente logra tomar por sorpresa a las personas ingresando a su hogar de forma remota. En el video se puede ver imágenes borrosas del individuo o hasta imágenes tomadas de las víctimas en momentos de su intimidad, sin saberlo con anterioridad. Todo esto con el fin de intimidar a las víctimas para después mostrar en pantalla un código QR, con una voz distorsionada exigiendo que depositen una cantidad determinada de bitcoins, una moneda digital, en la dirección que contiene el código QR para asegurar su bienestar. Muchas personas asustadas por la perturbadora intrusión en su hogar, obedecen a las demandas del delincuente, con el fin de proteger a su familia.

Instituciones Referenciadas

UCASAL

CIF

Figura 1

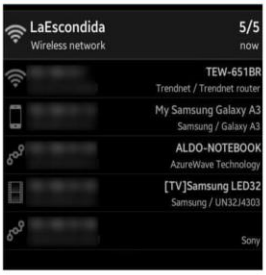
Objetivos

- **Identificación de las Vulnerabilidad del Internet de las Cosas (IoT):** identificar y estudiar los puntos débiles en la seguridad del internet de las cosas. Buscamos entender las formas de intrusión con el fin de ser capaces de reproducirlas en nuestros equipos para entender a fondo las vulnerabilidades de la IoT.
- **Estudiar los Delitos Derivados:** el analizar los delitos informáticos que pueden llegar a cometerse una vez vulnerada la seguridad de los equipos IoT. Por ello buscamos encontrar los tipos de delitos que pueden cometerse, reproducirlos en ambientes controlados, indagar en el conocimiento que los usuarios comunes tienen de estos riesgos, que medidas toman para resguardarse de ello y como actuarían en caso de que su seguridad haya sido vulnerada. Buscamos generar conciencia de los peligros de no contar con medidas de seguridad y así también poder sugerir formas de protección de los mismos, como también formas de actuar en caso de sufrir un ataque de algún tipo.
- **Evidencia Forense:** conocer la información que circula por los equipos IoT, los que los controlan y las interfaces de los usuarios, con el fin de encontrar nuevos métodos de obtener evidencia.

Elementos

- **Notebook:** 4Gb con un procesador Intel Core I5
- **Herramienta para auditoria de redes:** distribución de Linux creada para realizar auditorías de redes Wifi, Bluetooth y RFID. La misma cuenta con variadas herramientas de seguridad y auditoria Wireless. Es una herramienta gratuita fácil de conseguir y sencilla de usar para obtener la contraseña de una red Wifi.
- **Smartphone:** Utilizamos dos dispositivos móviles con sistema operativo Android.
- **Aplicación de escaneo de red:** escanearemos los dispositivos conectados a la red mediante una aplicación descargable desde cualquier store que nos permita obtener la información de los dispositivos conectados a la misma red.
- **Aplicación de transmisión multimedia:** mediante el uso de una aplicación podremos asegurar la transmisión de videos a los Smart TV's, aunque los dispositivos no sean compatibles desde fabrica para realizar esta tarea.

Figura 2



Resultados

La herramienta para auditoria de redes inicia buscando un cliente activo conectado al router, copia su dirección MAC. Luego comienza a capturar y a inyectar paquetes, y de esta forma desencriptar la contraseña. Luego de unos veinte minutos de trabajo la herramienta obtuvo la contraseña "flopy", podemos ver que es una contraseña muy débil, que justifica el corto tiempo de obtención.
Una vez obtenida la contraseña conectamos un teléfono a la red, el mismo tiene instalada una aplicación que permite escanear los equipos conectados a la red, obteniendo su dirección IP, su dirección MAC, tipo de dispositivo e incluso la marca del mismo como podemos observar en la captura de pantalla del dispositivo en la **figura 2**.
Con el escaneo terminado no solo obtuvimos la información de todos los equipos conectados a una red, sino que también obtuvimos la información exacta del Smart Tv que queremos atacar. De esta forma sabremos si contamos con un dispositivo compatible para transmitir el video, o bien, tenemos la información necesaria para saber qué herramienta usar para hacer la transmisión.
De esta forma no quedan obstáculos que impidan la transmisión de un video extorsivo desde nuestra aplicación a un grupo de individuos que se encuentran disfrutando de un momento de entretenimiento sin imaginar lo que estaba ocurriendo.

Podemos observar el resultado del escaneo de la aplicación. En la primera fila podemos observar los datos del router, en la segunda fila los datos de nuestro teléfono conectado a la red, en la tercera observamos los datos de un Smart TV, el cual es el objetivo de ataque en este experimento.

Conclusiones y Trabajos Futuros

Logramos determinar que no es complicado obtener la información de los dispositivos conectados a una red. Esto se debe primero a la facilidad de obtención de las herramientas necesarias para hacerlo y la falta de conciencia de las personas al no gestionar la seguridad de su red, como claramente observamos en las contraseñas desencriptadas.
Este trabajo es solo el comienzo para futuras experiencias, ya que desde este punto se pueden analizar otro tipo de ataques y delitos, como así también la búsqueda de información que evidencie el delito que se ha cometido y poder dar con sus perpetrador.

AUTORES
Fabio Emanuel Gómez Castro| fegomezcastro@hotmail.com
Aldo Guido Arzelán | aldoarzelan@gmail.com