UNIVERSIDAD DEL AZUAY

UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIA Y TECNOLOGÍA

ESCUELA DE INGENIERÍA ELECTRÓNICA

"Guía de Buenas Prácticas de Seguridad en Redes para la Configuración de Dispositivos de Capa 2 y 3 del Modelo OSI y Validación en una Red de Pruebas"

Trabajo de graduación previo a la obtención del título de:

INGENIERO ELECTRÓNICO

Autor:

LUIS MIGUEL SERRANO VÁZQUEZ

Director:

DANIEL ESTEBAN ITURRALDE PIEDRA Ph.D

CUENCA, ECUADOR

2020

DEDICATORIA

Dedico esta tesis a mis padres Diana y Felipe y a mi hermano Luis Felipe por haberme apoyado siempre en mis estudios, por ser un ejemplo de valores y virtudes, por aconsejarme siempre que lo he necesitado y porque son lo más importante en mi vida.

AGRADECIMIENTOS

Mi agradecimiento va dirigido a mi director de tesis por haber sido un excelente maestro, por despertar en mí el interés por el tema de esta tesis y por haberme ayudado en el desarrollo de la misma.

A todos mis maestros por haberme instruido con sus vastos conocimientos.

A la Universidad del Azuay por haber sido mi segundo hogar durante estos últimos años y por haberme brindado facilidades para formarme como profesional.

De manera muy especial mi gratitud a Patricio Sánchez, mi maestro de matemáticas del colegio, por haberme aconsejado y motivado a seguir esta carrera.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

Guía de Buenas Prácticas de Seguridad en Redes para la Configuración de Dispositivos de Capa 2 y 3 del Modelo OSI y Validación en una Red de Pruebas

RESUMEN

Las tecnologías de la información han adquirido una gran importancia en la actualidad, por lo que los ataques a redes son cada vez más frecuentas. El presente trabajo tiene como objetivo principal elaborar una guía de configuraciones para equipos de capa 2 y capa 3, del modelo OSI, que permitan implementar seguridad en una red. Para comprobar la validez de las configuraciones, se implementaron varias redes de pruebas, compuestas por dispositivos de la marca MikroTik, a las cuales se les realizaron diferentes ataques.

Palabras Clave: Seguridad, Redes, MikroTik.

Ing. Daniel Iturralde Ph.D
Coordinador de Ingeniería Electrónica

Ing. Daniel Iturralde Ph.D
Director del trabajo de titulación

Luis Miguel Serrano Vázquez
Autor

Guide to Good Network Security Practices for the Configuration of Layer 2 and 3 Devices of the OSI Model and Validation in a Test Network

ABSTRACT

Information technologies have acquired great importance today, so network attacks are becoming more frequent. The main objective of this work is to develop a configuration guide for Layer 2 and Layer 3 devices of the OSI model, which allows to implement security in a network. To verify the validity of the configurations, several test networks were implemented, they were composed of MikroTik brand devices to which different attacks were performed.

Keywords: Security, Networks, MikroTik.

Ing. Daniel Iturralde Ph.D
Electronic Engineering Coordinator

Ing. Daniel Iturralde Ph.D
Thesis Director

Luis Miguel Serrano Vázquez
Author

UNIVERSIDAD DEL AZUAY
Dpto. Idiomas

Translated by
Ing. Paúl Arpi

1. CAPÍTULO 1: INTRODUCCIÓN

1.1. Problemática

En los últimos años el internet y las redes de computadores se han convertido en herramientas fundamentales e indispensables para el funcionamiento de empresas, industrias, negocios y la sociedad en general. Debido a la importancia que han adquirido estas herramientas, las mismas se han convertido en el foco de constantes ataques con el fin de vulnerar sistemas y obtener información valiosa para posteriormente usarla con fines malintencionados.

1.2. Motivación de la investigación

Las tecnologías de la información se han convertido en herramientas fundamentales para el funcionamiento de la sociedad. Por lo que la seguridad en redes es un área de estudio muy importante en la actualidad, ya que permite reconocer y solventar vulnerabilidades para garantizar la disponibilidad de un servicio, la confidencialidad e integridad de la información.

1.3. Objetivo general

Elaborar una guía de configuraciones, orientada a equipos de capa 2 y 3 (modelo OSI), que permita implementar seguridad en una red.

1.4. Objetivos específicos:

- Realizar una investigación sobre los trabajos previos relacionados con el tema propuesto y sobre los ataques más comunes en redes.
- Implementar una red de pruebas en la cual se puedan utilizar herramientas para generar ataques.
- Realizar configuraciones en los equipos de red que permitan contrarrestar los ataques sobre la red de pruebas.
- Analizar los resultados encontrados y obtener conclusiones en base a los mismos.

1.5. Metodología

Se utilizará la investigación bibliográfica mediante la consulta de diferentes libros, publicaciones, revistas, etc. para obtener la información de trabajos previos y de los ataques más comunes en redes.

Se realizará una investigación bibliográfica mediante la consulta de libros y páginas web para aprender a utilizar herramientas que permitan generar ataques de red y también se realizará una investigación experimental al construir la red física de pruebas.

Se utilizará la investigación bibliográfica mediante la consulta de información en la página web del fabricante de los equipos y también se realizará una investigación experimental para aplicar las configuraciones en equipos reales.

Se realizará una investigación experimental al realizar diferentes ataques en la red de pruebas para comprobar la validez de las configuraciones previamente realizadas.

Se aplicará la investigación descriptiva debido a que se detallarán los pasos a seguir para implementar una red segura.

2. CAPÍTULO 2: ESTADO DEL ARTE

2.1. Introducción

En este capítulo se expondrán trabajos realizados, por diferentes autores, sobre seguridad en redes inalámbricas, seguridad en redes cableadas, diseño de escenarios educacionales para enseñar seguridad en redes, etc.

2.2. Estado del Arte

En (Pauzhi & Coronel, 2015) se realizó el diseño e implementación de políticas de seguridad, en un WISP (Wireless Internet Service Provider), con el objetivo de invalidar ataques comunes como: ataques de diccionario, man in the middle, wardriving, puntos de acceso no autorizados, etc. El WISP utiliza dispositivos de la marca MikroTik.

En (Chiu, 2006) se presenta un trabajo en el que se exponen los riesgos de seguridad en redes inalámbricas, debido a que cualquier persona dentro del rango de cobertura puede intentar acceder a la red. Se explican las herramientas que utilizan los atacantes para detectar y marcar redes inseguras y los mecanismos y protocolos, pertenecientes al estándar IEEE (Institute of Electrical and Electronics Engineers) 802.11, como OSA (Open System Authentication), SKA (Shared Key Authentication), encriptación WEP (Wired Equivalent Privacy), etc. con el objetivo de garantizar la seguridad en una red inalámbrica

En (Zavarsky, Butakkov, & Hlyne, 2015) se realizó un trabajo en el cual se analizan los diversos componentes que conforman el protocolo SCAP (Security Content Automation Protocol) y se lo aplicó con el objetivo de automatizar las configuraciones de seguridad en un router CISCO.

En (Ternero) se exponen los ataques más comunes que son realizados en las redes y se explican las configuraciones de seguridad que se deben implementar como: ACL (Acces Control List), VLAN (Virtual Local Area Network), criptografía en redes, protocolos seguros, VPN (Virtual Private Network), cortafuegos, etc. los ejemplos expuestos son orientados a equipos de la marca CISCO.

En (Andreatos, 2017) se diseñaron escenarios educacionales para enseñar seguridad en redes. Dentro de estos escenarios se enseñó como instalar diferentes herramientas para ataque a una red, defensa de una red, monitoreo de tráfico, análisis de paquetes,

etc. También se realizaron pruebas de ataques DoS (Denial of Service) mediante herramientas instaladas en plataformas Windows y Linux.

En (Patel, Ghaghda, & Nagecha, 2014) se realizó un estudio en el que se exponen diferentes tipos de amenazas y mecanismos de seguridad en ambientes educacionales. Para abordar los problemas de seguridad, los autores proponen un modelo de seguridad para redes cableadas e inalámbricas.

En (Cueva, Pozo, & Iturralde, 2016) se desarrolló e implementó un software, denominado Easy Network Designer Software, que permite realizar la virtualización de una red y la configuración remota de parámetros de dispositivos Mikrotik. El software fue desarrollado mediante Java y Mysql. Se realizaron pruebas con redes complejas.

En (Marsá-Maestre, de la Hoz, Giménez-Guzmán, & López-Carmona, 2012) se demuestra como una herramienta, basada en tecnologías de virtualización, permite generar escenarios para ser utilizados en la educación de seguridad en redes. Se describe un ejemplo de un escenario y se establecen los beneficios del uso de esta herramienta en cursos de seguridad.

En (Roschke, Willems, & Meinel, 2010) se propone un laboratorio, para entrenamiento en seguridad, en el cual se presentan diferentes escenarios para la práctica tanto de ataque como de defensa. Los escenarios se clasifican según diferentes niveles de dificultad y se crean mediante componentes virtualizados y componentes dedicados de infraestructura de red. Al final se describen las experiencias de profesores y estudiantes en base a lo trabajado en diferentes sesiones de entrenamiento.

2.3. Conclusiones

La idea principal, de la mayoría de los trabajos citados, es exponer diferentes ataques de red que son comunes y enseñar los mecanismos de defensa que permiten contrarrestarlos.

3. CAPÍTULO 3: MARCO TEÓRICO

3.1. Introducción

En este capítulo se tratarán conceptos necesarios para el desarrollo del trabajo. Se explicarán características y protocolos de determinadas capas del modelo OSI (Open System Interconnection), conceptos sobre los servicios de la seguridad en redes, la clasificación de los ataques de red y el software que se utilizará en las pruebas.

3.2. Capa 3 (Red)

3.2.1. Protocolo IP (Internet Protocol)

"IP es un protocolo de baja sobrecarga, que provee solo las funciones necesarias para enviar un paquete de un origen a un destino en un sistema de redes. Algunas de las características de este protocolo son las siguientes: (CISCO, CCNA 1: Introduction to Networks)".

- "No establece una conexión para el envío de datos".
- "No garantiza la entrega de paquetes".
- "La operación es independiente del medio que transporta los datos".

3.2.2. Encabezado IP

"El encabezado IP contiene información importante sobre el paquete. Algunos de los campos más importantes son:" (CISCO, CCNA 1: Introduction to Networks)

- Versión: "Identifica la versión del paquete IP".
- Servicios diferenciados: "Se utiliza para determinar la prioridad de cada paquete".
- Tiempo de vida: "Se utiliza para limitar la vida útil de un paquete".
- Protocolo: "Permite que la capa de red pase los datos al protocolo de capa superior correspondiente".
- Dirección IP de origen: "Valor que representa la dirección IP de origen (de dónde proviene el paquete)".
- Dirección IP de destino: "Valor que representa la dirección IP de destino (a dónde va el paquete)".

3.2.3. ICMP (Internet Control Message Protocol)

ICMP es un protocolo, de la capa de red, utilizado para el envío de mensajes para reporte de errores o para proporcionar respuestas sobre el procesamiento de paquetes IP. El objetivo de este protocolo es brindar retroalimentación sobre problemas en la comunicación (CISCO, CCNA 1: Introduction to Networks) (Postel, 1981).

Los mensajes se envían de host a host (petición y respuesta) y utilizan la cabecera IP.

Algunos de los mensajes son los siguientes:

- Timestamp: Es un mensaje que se utiliza para la consulta del tiempo. Este valor se da en milisegundos y se cuenta desde medianoche UT (Universal Time) (Postel, 1981).
- Echo: "Este mensaje se utiliza para determinar si un host está en funcionamiento" (CISCO, CCNA 1: Introduction to Networks).
- Destino inalcanzable: "Un host o un Gateway pueden enviar un mensaje de destino inalcanzable cuando reciben un paquete que no pueden entregar" (CISCO, CCNA 1: Introduction to Networks).

3.3. Capa 4 (Transporte)

3.3.1. Protocolo TCP (Transmission Control Protocol)

"Es un protocolo de la capa de transporte, que divide los datos en segmentos y los transmite de forma confiable ya que utiliza la función de acuse de recibo. Con este protocolo se garantiza que todos los segmentos llegarán a su destino" (CISCO, CCNA 1: Introduction to Networks).

Algunas propiedades de TCP son las siguientes (CISCO, CCNA 1: Introduction to Networks):

- Establece una conexión antes de realizar la transmisión de datos.
- Realiza un acuse de recibo para confirmar la recepción de datos, y en el caso de que estos se hayan perdido hace que se retransmitan.
- Mediante números de secuencia, garantiza que el receptor rearme los segmentos en el orden correcto.
- "Administra el flujo de datos en el caso de que se produzca una sobrecarga de recursos".

3.3.2. Segmento TCP

Debido a todo el control que realiza el protocolo TCP sobre los segmentos, necesita de una sobrecarga sobre el encabezado que encapsula. En el encabezado se encuentra lo siguiente (CISCO, CCNA 1: Introduction to Networks):

- Puerto de origen: Es el número que identifica al puerto de donde salen los segmentos.
- Puerto de destino: Es el número de puerto que identifica al servicio que se quiere acceder.
- Número de secuencia: “Se utiliza para rearmar los datos”.
- Número de acuse de recibo: “Indica los datos que se recibieron”.
- Longitud del encabezado: “Indica la longitud del encabezado del segmento TCP”.
- Reservado: “Campo reservado para el futuro”.
- Bits de control o flags (banderas): “Bits que indican el propósito y la función del segmento TCP”.
- Tamaño de la ventana: “Indica la cantidad de segmentos que se pueden aceptar por vez”.
- Checksum: “Se utiliza para la verificación de errores en el encabezado y los datos del segmento”.
- Urgente: Indica si la información es urgente.

Dentro de los bits de control se encuentran los siguientes (Tanenbaum & Wetherall, 2012):

- URG: “Indica si está en uso el apuntador urgente”.
- ACK: “Indica el acuse de recibo”.
- PSH: “Indica datos que se deben transmitir de inmediato”.
- RST: “Se utiliza para reestablecer una conexión, rechazar un segmento o rechazar un intento de conexión”.
- SYN: “Se utiliza para establecer conexiones”.
- FIN: “Se usa para liberar una conexión”.

3.3.3. Establecimiento de conexión TCP

Antes de que se puedan enviar datos, se debe establecer una conexión entre las dos entidades. Para realizar esta conexión se produce el enlace de 3 vías y se utilizan los bits de control (CISCO, CCNA 1: Introduction to Networks):

- Primero, el cliente envía un paquete con el bit SYN habilitado hacia el servidor para solicitar una sesión cliente a servidor.
- El servidor envía un paquete con los bits SYN y ACK habilitados hacia el cliente para confirmar la sesión solicitada y para solicitar una sesión servidor a cliente.
- El cliente envía un paquete con el bit ACK habilitado hacia el servidor para confirmar la sesión solicitada.

3.3.4. UDP (User Datagram Protocol)

Es un protocolo de la capa de transporte poco confiable, que permite entregar segmentos con una sobrecarga reducida. El objetivo es disminuir las demoras en la transmisión (CISCO, CCNA 1: Introduction to Networks).

UDP cuenta con las siguientes características (CISCO, CCNA 1: Introduction to Networks):

- "No establece una conexión".
- "No cuenta con procesos que hagan al emisor reenviar datos que se perdieron o dañaron".
- "No dispone de un mecanismo para reordenar los datos a su secuencia original".
- "No cuenta con mecanismos para controlar la cantidad de datos que envía el dispositivo de origen".

3.3.5. Datagrama UDP

"La porción de comunicación se conoce como datagrama, y está conformado por:" (CISCO, CCNA 1: Introduction to Networks)

- Puerto de origen.
- Puerto de destino.
- Longitud.

- Checksum.

3.3.6. Puertos

Los puertos TCP/UDP se clasifican en (CISCO, CCNA 1: Introduction to Networks):

- Puertos bien conocidos (Números del 0 al 1023): “Están reservados para servicios y aplicaciones en servidores”.
- Puertos registrados (Números del 1024 al 49151): “Se asignan a procesos o aplicaciones que el usuario elige instalar en lugar de aplicaciones comunes que recibirían un número de puerto bien conocido. Si no lo utiliza un servidor, un cliente puede utilizarlo como puerto de origen”.
- Puertos dinámicos o privados (Números del 49152 al 65535): “Se asigna al cliente cuando este inicia una conexión a un servicio”.

3.3.7. Estados de un puerto

Un puerto se considera abierto si acepta conexiones TCP o datagramas UDP. Un puerto se considera cerrado cuando es accesible, pero no tiene una aplicación ejecutándose (Nmap).

3.4. Protocolos y servicios en un router

3.4.1. Telnet

“Es un protocolo que permite establecer una sesión de interfaz de línea de comandos de forma remota, mediante una interfaz virtual, a través de una red. Telnet transmite los datos sin encriptar. El dispositivo de red debe tener, por lo menos, una interfaz activa con una dirección IP asignada” (CISCO, CCNA 1: Introduction to Networks).

Telnet funciona, por defecto, en el puerto TCP 23.

3.4.2. SSH (Secure Shell)

“Proporciona un inicio de sesión remoto, similar a Telnet, excepto que utiliza servicios de red más seguros. Proporciona seguridad (encriptación) en la autenticación y en la transmisión de datos” (CISCO, CCNA 1: Introduction to Networks).

SSH funciona, por defecto, en el puerto TCP 22.

3.4.3. Winbox

Winbox es un servicio que permite administrar routers, de la marca Mikrotik, por medio de una interfaz gráfica de usuario.

Winbox funciona por defecto en el puerto TCP 8291. Para conectarse al router se utiliza la dirección IP de la interfaz *ethernet* a la cual se vaya a conectar (Mikrotik, Manual:Winbox, s.f.).

3.4.4. MAC (Media Access Control) Telnet

"Este protocolo sirve para proporcionar acceso a un router que no tiene una dirección IP asignada. Para realizar la conexión se utiliza la dirección MAC de destino. Su funcionamiento es igual al de Telnet. Solo funciona entre routers Mikrotik" (Mikrotik, MAC access, s.f.).

3.4.5. MAC Winbox

Su funcionamiento es igual al de Winbox, pero la conexión se realiza utilizando la dirección MAC de la interfaz del router (Mikrotik, MAC access, s.f.).

3.4.6. MAC Ping

"Ping es un servicio que permite verificar la conectividad, de capa 3, entre 2 dispositivos" (CISCO, CCNA 1: Introduction to Networks).

MAC ping es similar al ping convencional, pero utiliza direcciones MAC (Mikrotik, Manual:Tools/Ping, s.f.).

3.4.7. Neighbor Discovery

"Es un protocolo que se utiliza para detectar otros dispositivos, compatibles con el mismo, en una red. Con este protocolo se obtiene la dirección IP, dirección MAC, etc. de los otros dispositivos" (Mikrotik, Manual:Securing Your Router, s.f.) (Mikrotik, Neighbor discovery, s.f.).

3.4.8. Bandwidth server

"Esta herramienta se utiliza para medir el rendimiento (cantidad de datos movidos satisfactoriamente de un lugar a otro en un periodo de tiempo) entre dos routers" (Mikrotik, Manual:Securing Your Router, s.f.) (INTEL, s.f.).

3.4.9. DNS (Domain Name System)

"En redes, los dispositivos se identifican con direcciones IP para poder enviar y recibir datos. Estas direcciones numéricas son difíciles de recordar, por lo que se crearon los nombres de dominio, que son más fáciles de recordar. El protocolo DNS es un servicio encargado de realizar la traducción de un nombre de dominio a una dirección IP" (CISCO, CCNA 1: Introduction to Networks).

DNS funciona por defecto en el puerto UDP/TCP 53.

3.4.10. Cloud Update Time

Es un servicio que permite mantener actualizada la hora del reloj en un dispositivo de red. Para obtener las actualizaciones de hora, el dispositivo se conecta a la nube de Mikrotik (Mikrotik, Manual:IP/Cloud, s.f.).

3.4.11. NTP (Network Time Protocol)

"Es un protocolo que se utiliza para sincronizar la hora en los relojes de los dispositivos de red" (CISCO, CCNA 2: Routing and Switching Essentials).

NTP funciona por defecto en el puerto UDP 123.

3.5. Capa 2 (Enlace de datos)

"La capa 2 (capa de enlace de datos) es responsable del intercambio de tramas entre los nodos y a través de un medio de red físico. Los nodos son dispositivos de red conectados a un medio común. Acepta paquetes de la capa 3 y los empaqueta en tramas, controla el acceso al medio y realiza la detección de errores" (CISCO, CCNA 1: Introduction to Networks).

3.5.1. Subcapas

La capa de enlace de datos cuenta con dos subcapas que son (CISCO, CCNA 1: Introduction to Networks):

- LLC (Logical Link Control): "Coloca en la trama información para identificar el protocolo de capa de red que se utiliza para la trama".
- MAC (Media Access Control): "Proporciona el direccionamiento de la capa de enlace de datos y la delimitación de los datos".

3.5.2. Trama

Los campos que se pueden encontrar en una trama son los siguientes (CISCO, CCNA 1: Introduction to Networks):

- Indicadores de comienzo y fin de la trama: “Utilizados por la subcapa MAC para identificar el inicio y fin de la trama”.
- Direccionamiento: “Utilizado por la subcapa MAC para identificar el nodo origen y el nodo destino”.
- Tipo: “Utilizado por la subcapa LLC para identificar el protocolo de capa 3”.
- Control: “Identifica servicios para el control del flujo”.
- Datos: “Contenido de la trama”.
- Detección de errores: “Campo utilizado para la detección de errores”.

3.5.3. Ethernet

Es la tecnología más utilizada, a nivel mundial, para redes LAN (Local Area Network). Corresponde a la capa 1 (capa física) y a la capa 2 (capa de enlace de datos) del modelo OSI. Ethernet está compuesto, básicamente, por software y hardware que, en conjunto, permiten la transferencia de datos entre computadoras (Spurgeon, 2000).

3.5.4. ARP (Address Resolution Protocol)

El protocolo ARP permite obtener la dirección MAC de un dispositivo cuando se conoce la dirección IP del mismo. El dispositivo A, que desea comunicarse con el dispositivo B, envía una trama a todos los equipos de la red con la dirección IP del dispositivo B y solo este último responderá con su dirección MAC (Tanenbaum & Wetherall, 2012).

3.5.5. Switch

Permite conectar varios dispositivos dentro de una misma red. Debido a que pertenece a la capa 2, solamente utiliza direcciones MAC para la identificación de los dispositivos. Un switch utiliza la tabla de direcciones MAC en la que guarda la dirección MAC de un dispositivo y el número de puerto al que el dispositivo está conectado. Gracias a esto puede saber a dónde debe enviar los datos (CISCO, CCNA 1: Introduction to Networks).

3.5.6. Bridge

Bridge es una característica, que se puede configurar en un router, que permite conectar hosts de diferentes LANs como si estuvieran en una misma LAN (Mikrotik, Manual:Interface/Bridge, s.f.).

3.5.7. STP (Spanning Tree Protocol)

La redundancia se refiere a la existencia de varios enlaces para que los datos puedan tomar caminos alternativos en caso de que exista algún problema con el enlace principal. Si en la red existen varias rutas y no hay un servicio que administre estas rutas, se producirá un bucle de capa 2. Estos bucles pueden provocar problemas como: inestabilidad en la tabla de direcciones MAC por la recepción de una misma trama por diferentes puertos, tormentas de broadcast y la transmisión de varias copias de una misma trama (CISCO, CCNA 3: Scaling Networks).

STP es un protocolo, de capa 2, que permite controlar los enlaces redundantes en una red. Se encarga de bloquear el puerto por el que se conecta el enlace alternativo si está funcionando el enlace principal y se encarga de desbloquear el puerto por el que se conecta el enlace alternativo si el enlace principal falla (CISCO, CCNA 3: Scaling Networks).

Este protocolo utiliza un algoritmo para determinar cuál es el puerto que se debe bloquear. También establece a uno de los switches como puente raíz. Esto se refiere a que este switch se utilizará como punto de referencia para el cálculo de rutas (CISCO, CCNA 3: Scaling Networks).

Cada switch tiene un identificador de puente que está formado por un valor de prioridad, la dirección MAC del dispositivo y un identificador de sistema. Los switches se envían entre ellos unas tramas, llamadas BPDU (Bridge Protocol Data Unit), en las cuales incluyen su identificador de puente. De esta manera pueden determinar cual tiene el identificador de puente más bajo y establecerlo como puente raíz. Cuando ya se conoce el puente raíz, el algoritmo calcula la ruta más corta hacia el mismo y la establece como la ruta principal. El protocolo también identifica a los puertos de los switches de la siguiente forma (CISCO, CCNA 3: Scaling Networks):

- Puertos raíz: “Son los puertos de switch más cercanos al puente raíz”.

- Puertos designados: “Son todos los puertos que no son raíz y que aún pueden enviar tráfico a la red”.
- Puertos alternativos y de respaldo: “Están configurados en estado de bloqueo para evitar bucles”.
- Puertos deshabilitados: “Son puertos que se encuentran desactivados”.

El protocolo STP se declaró obsoleto con la aparición de RSTP (Rapid Spanning Tree Protocol), el cual es una mejora de STP. RSTP proporciona mayor velocidad de recálculo cuando cambia la topología de la red (CISCO, CCNA 3: Scaling Networks).

3.5.8. VLAN (Virtual Local Area Network)

Permite dividir una red LAN física en varias redes LAN lógicas independientes. De esta manera se pueden separar en grupos a los dispositivos que comparten una misma red física. Los dispositivos, que pertenezcan a una misma VLAN, se pueden comunicar como si estuvieran en una red física independiente, pero comparten la infraestructura con otros dispositivos de otras VLANs. Esto permite aislar a los usuarios que tengan información delicada, reducir costos en actualizaciones en la red, reducir el tráfico innecesario en la red, etc. (CISCO, CCNA 2: Routing and Switching Essentials)

Para el funcionamiento de las VLAN se utiliza un proceso de etiquetado, que consiste en añadir un campo adicional al encabezado de la trama ethernet. Este campo lo añade el switch para identificar la VLAN a la que pertenece el dispositivo que envía una trama. Este proceso se define en el estándar 802.1Q (CISCO, CCNA 2: Routing and Switching Essentials).

Cada VLAN se identifica con un valor numérico conocido como VLAN ID.

Algunos conceptos importantes, dentro de VLAN, son los siguientes (CISCO, CCNA 2: Routing and Switching Essentials):

- Puerto de acceso: Es un puerto por el que entra y sale tráfico sin etiquetar, por lo que está destinado para hosts. Pertenece a solo a una VLAN.
- Puerto troncal: “Es un puerto que acepta tráfico proveniente de diferentes VLANs o que no proviene de una VLAN. Se utiliza para la conexión con otro switch o un router”.
- VLAN nativa: Es la VLAN que se asigna a un puerto troncal. A esta VLAN se asocia el tráfico sin etiquetar.

3.5.9. SNMP (Simple Network Management Protocol)

SNMP es un protocolo utilizado para la administración de dispositivos de red. puede utilizarse para obtener información de los dispositivos y también para realizar modificaciones en la configuración de los mismos. Existen varias versiones de este protocolo, pero solo la versión 3 implementa seguridad para el intercambio de información (CISCO, Configuring SNMP, 2016).

3.5.10. Port Mirroring

Consiste en que el switch realiza una copia del tráfico que circula a través de él y la envía a un puerto determinado. El equipo que esté conectado en este puerto recibirá todo el tráfico para poder realizar un monitoreo. (Mikrotik, Manual:Switch Chip Features, s.f.).

3.6. Túnel IPsec

3.6.1. IPsec

"IPsec es un conjunto de características que se utilizan para proteger los datos IP durante la comunicación entre dos entidades" (Ariganello, 2014). Se utiliza cuando se requiere enviar información delicada a través de redes desprotegidas como internet (CISCO, Security for VPNs with IPsec Configuration Guide, Cisco IOS XE Release 3S, 2018).

Actúa en la capa de red y también puede proteger capas superiores (Ariganello, 2014) (CISCO, Security for VPNs with IPsec Configuration Guide, Cisco IOS XE Release 3S, 2018).

Los dispositivos que se comunican entre sí y utilizan IPsec para la protección se denominan peers (CISCO, Security for VPNs with IPsec Configuration Guide, Cisco IOS XE Release 3S, 2018).

IPsec garantiza lo siguiente (Ariganello, 2014) (CISCO, Security for VPNs with IPsec Configuration Guide, Cisco IOS XE Release 3S, 2018):

- Confidencialidad: El emisor puede encriptar los paquetes.
- Integridad: El receptor puede autenticar los paquetes recibidos para asegurar que no han sido alterados.

- Autenticación del origen de los datos: El receptor puede autenticar la fuente de los paquetes.
- Anti-replay: Los paquetes producidos con un ataque de este tipo pueden ser detectados y descartados por el receptor.

IPsec dispone de 2 modos, que son los siguientes (Ariganello, 2014):

- Transporte: "La cabecera IPsec se agrega después de la cabecera IP original, por lo que esta última queda expuesta. Los datos de la capa de transporte y superiores se benefician de IPsec".
- Túnel: "Los datos y la cabecera IP original se protegen al agregar una nueva cabecera IP en la que se utilizan las direcciones de los peers"

Para la autenticación, encriptación, generación de llaves, y establecimiento de asociaciones de seguridad (acuerdo de parámetros entre dos peers), IPsec se basa en los protocolos que se verán a continuación (Ariganello, 2014).

3.6.2. ESP (Encapsulating Security Payload)

Es el protocolo más utilizado en IPsec, debido a la seguridad que proporciona. Este protocolo brinda confidencialidad, integridad, autenticación del origen y Anti-replay. Es el único que encripta los datos, para lo cual utiliza los siguientes procesos (Ariganello, 2014):

- DES (Data Encryption Standard).
- 3DES (Tiple Data Encryption Standard).
- AES (Advanced Encryption Standard): Este es uno de los algoritmos más utilizados.

"Encriptar es el proceso de transformar datos mediante un algoritmo y una llave, con el fin de que sean ilegibles para todos excepto para quien pueda desencriptarlos. La llave es información que utiliza el algoritmo para encriptar o desencriptar" (Ariganello, 2014) (Criptografía, 2017).

3.6.3. AH (Authentication Header)

Este protocolo proporciona las mismas características de seguridad que ESP, excepto la confidencialidad, por lo que los datos no se encriptan para la comunicación. Para garantizar la integridad y la autenticación, AH y ESP utilizan HMAC (Hash-based

Message Authentication Code). Algunos de los algoritmos son los siguientes (Ariganello, 2014):

- MD5 (Message Digest).
- SHA-1 (Secure Hash Algorithm): Es más seguro que MD5.

Hash es una función que recibe datos de entrada y los transforma en un conjunto de caracteres de longitud finita. Cuando se utiliza HMAC, tanto el emisor como el receptor comparten una llave secreta. El emisor pasa el mensaje y la llave por una función hash y obtiene un código, el cual se envía, junto al mensaje, al receptor. Este último, al recibir el paquete, utiliza la función hash con el mensaje y la llave para obtener un código y compararlo con el que envió el emisor. De esta manera se autentica y garantiza la integridad (Ariganello, 2014).

3.6.4. IKE (Internet Key Exchange)

IKE es un método que permite el intercambio, de forma segura, de los parámetros necesarios para IPsec. Parámetros como: llaves de autenticación, llaves de encriptación, etc. (Ariganello, 2014) Utiliza el protocolo ISAKMP (Internet Security Association and Key Management Protocol) en el puerto UDP 500 (Lipták & Eren, 2012).

IKE tiene 2 fases que son las siguientes (CISCO, Configuring Internet Key Exchange for IPsec VPNs, 2018) (Molenaar, s.f.):

- Fase 1: En esta fase se realiza la negociación de llaves que servirán para la comunicación segura en la fase 2. Los peers negocian parámetros de autenticación, encriptación, grupo DH (Diffie Hellman), hashing, etc. Una vez culminada la negociación, se utiliza el grupo DH para generar llaves secretas compartidas mediante el intercambio de ciertos valores. Estas llaves se utilizarán para la encriptación. Finalmente se realiza un proceso de autenticación.
- Fase 2: En esta fase se realiza la negociación de los parámetros que se utilizarán en IPsec como: protocolo y modo IPsec, parámetros de encriptación, autenticación, etc. Esta negociación está protegida por las asociaciones de seguridad de la fase 1.

La Fase 1 tiene 2 modos de operación (Ariganello, 2014):

- Modo Main: Todo el proceso se realiza con el intercambio de 6 mensajes entre los peers. Con este modo se encriptan los parámetros que se usan en el proceso de autenticación. Es más demorado, pero seguro.
- Modo Aggressive: Todo el proceso se realiza con el intercambio de 3 mensajes entre los peers. Con este modo no se encriptan los parámetros que se usan en el proceso de autenticación. Es más rápido, pero menos seguro.

La fase 2 tiene solo un modo llamado Quick (Lipták & Eren, 2012).

3.7. Servicios de seguridad

William Stallings, en su libro (Stallings, 2004), establece que los seis servicios de seguridad en redes son:

- Autenticación: "Se refiere a la seguridad de que la entidad que se comunica es quien dice ser".
- Control de acceso: "Es la prevención del uso no autorizado de una fuente".
- Confidencialidad de los datos: "Es la protección de los datos contra una revelación no autorizada".
- Integridad de los datos: Es la seguridad de que los datos no hayan sido modificados desde que fueron enviados hasta que llegaron a su destino.
- No repudio: Es una protección de la comunicación en la cual se evita que el emisor o receptor interrumpan la comunicación.
- Disponibilidad: "Es la propiedad que tiene un sistema de estar accesible y utilizable a petición de una entidad".

3.8. Clasificación de ataques

Ernesto Ariganello propone clasificar los ataques en tres categorías principales, que son las siguientes:

3.8.1. Ataques de reconocimiento

"Los ataques de reconocimiento consisten en el descubrimiento y mapeo de sistemas, servicios o vulnerabilidades sin autorización". Este tipo de ataques se basan en el uso de software que se encuentra disponible en internet y que su descarga es gratuita. Las

herramientas más utilizadas para este tipo de ataques son las siguientes (Ariganello, 2014):

- Sniffers de paquetes: “Captura todos los paquetes de red que se transmiten en una LAN (Local Area Network)”.
- Barridos de ping: “Es una técnica que permite determinar el rango de direcciones IP (Internet Protocol) que corresponde a hosts activos”.
- Escaneo de puertos: “Escaneo de puertos TCP (Transmission Control Protocol) y UDP (User Datagram Protocol) para detectar servicios abiertos”.
- Búsqueda de información en internet: “Permite revelar información sobre el dueño de un dominio en particular”.

3.8.2. Ataques de acceso

“Los ataques de acceso explotan vulnerabilidades en servicios de autenticación, FTP (File Transfer Protocol) y web con el objetivo de obtener acceso a cuentas, bases de datos y otra información sensible” (Ariganello, 2014).

El autor expone diversos ejemplos de este tipo de ataque (Ariganello, 2014):

- Ataques de contraseña: Consiste en intentar adivinar las contraseñas para el ingreso a un sistema.
- Explotación de la confianza: Consiste en aprovechar, de forma no autorizada, los privilegios de un sistema para comprometer al objetivo.
- Redirección de puerto: Se realiza partiendo de un sistema comprometido, para redireccionar sesiones a través de él.
- Man in the Middle: Consiste en interceptar el tráfico producido entre dos entidades con el objetivo de leer y modificar los datos.
- Desbordamiento de buffer: Consiste en saturar con datos la memoria del buffer para que los datos validos se sobrescriban y se ejecute código malicioso.

3.8.3. Ataques de denegación de servicios

Los ataques de denegación de servicios consisten en enviar una gran cantidad de solicitudes a una red con el objetivo de saturar la capacidad de procesamiento provocando que el sistema no acepte solicitudes legítimas (Ariganello, 2014). Algunos de los ejemplos de este tipo de ataques son los siguientes (Ariganello, 2014):

- Ping de la muerte: “Consiste en enviar un ping con un tamaño de paquete mayor al máximo permitido para que el nodo objetivo colapse”.
- Ataque smurf: “Consiste en el envío de una gran cantidad de solicitudes ICMP (Internet Control Message Protocol) a direcciones broadcast, para que el router reenvíe el broadcast y se obtenga una respuesta de todos los hosts, generando así una gran cantidad de tráfico”.
- Inundación TCP/SYN: “Consiste en saturar un servidor con conexiones a medio abrir, que fueron generadas por la inundación de paquetes SYN TCP con direcciones de origen falsas”.

3.9. Software

3.9.1. Kali Linux

“Kali Linux es un proyecto de código abierto que provee información para el entrenamiento en seguridad informática y servicios para pruebas de penetración” (Kali, About Kali Linux, s.f.). “Es una distribución de Linux basada en Debian, que dispone de herramientas de penetración y auditoría de seguridad” (maslinux, 2018).

3.9.2. Metasploitable 2

“Metasploitable es una máquina virtual, basada en Linux, con muchas vulnerabilidades configuradas de forma intencional. Esta herramienta se utiliza para realizar pruebas de hacking en un ambiente controlado” (RAPID7, s.f.).

3.9.3. Wireshark

“Wireshark es un analizador de protocolos de red que permite analizar tráfico, a un nivel microscópico, en una red. Es utilizado en empresas, agencias gubernamentales e institutos de educación a nivel mundial” (WIRESHARK, s.f.).

3.9.4. Winbox

Es un programa por el cual se puede administrar routers Mikrotik mediante una interfaz gráfica (Mikrotik, Manual:Winbox, s.f.).

3.9.5. GNS3

“Es una herramienta gratuita, que permite diseñar, construir y probar redes en un ambiente virtual. Evita la necesidad de adquirir hardware” (GNS3, s.f.).

3.9.6. PWGen

“Es una herramienta que permite generar contraseñas seguras y de forma aleatoria. Le permite al usuario elegir la longitud de la contraseña y los tipos de caracteres que se incluirán en esta” (PWGen, s.f.).

3.10. Conclusiones

Los conceptos presentados permiten comprender las vulnerabilidades o seguridades que caracterizan a diferentes protocolos y servicios que se utilizan en las redes de computadoras.

Se conceptualiza el objetivo de la seguridad en redes y se clasifican los ataques de red en base a su objetivo para poder comprender que es lo que busca un atacante y que es lo que significa la seguridad en una red.

4. CAPÍTULO 4: DESARROLLO

4.1. Introducción

Este capítulo se enfocará en 3 temas: seguridad en un router, seguridad de capa 2 y túnel IPsec. Para cada tema se realizarán diferentes ataques en redes de prueba y se plantearán las configuraciones y las buenas prácticas de seguridad que ayuden a contrarrestar estos ataques.

4.2. Seguridad en un router

4.2.1. Topología

En la figura 4.1 se encuentra la primera topología de la red en la que se realizarán pruebas. Se utilizará el router Mikrotik hAP LITE TC (RB941-2Nd-TC).

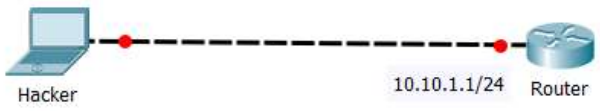


Figura 4.1: Topología N°1 de la red de pruebas.

La segunda topología, de la red de pruebas, se encuentra en la figura 4.2. El modelo del router que se utilizará es: Mikrotik hAP LITE TC (RB941-2Nd-TC).

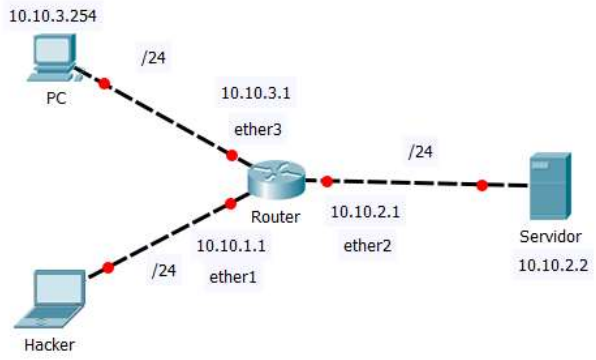


Figura 4.2: Topología N° 2 de la red de pruebas.

4.2.2. Pruebas en la red vulnerable

Se crea un usuario para administración del router, como se puede ver en la figura 4.3.

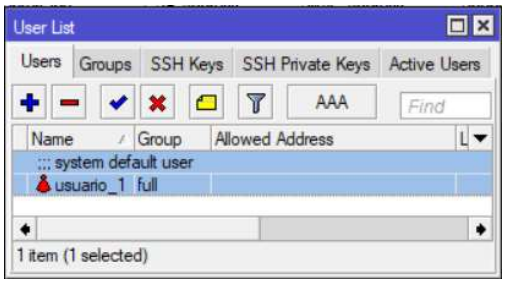


Figura 4.3: Configuración de usuario de administración.

Obtención de contraseña Telnet mediante Wireshark

Se utilizará la topología de la figura 4.1.

El servicio de Telnet está habilitado en el router.

Se inicia la captura de datos, mediante Wireshark, en la computadora.

En la figura 4.4 se pueden examinar los comandos que se deben utilizar para conectarse, mediante Telnet, a la interfaz *ethernet* con dirección IP 10.10.1.1.

En la terminal se ingresa el nombre de usuario y contraseña para acceder al router.

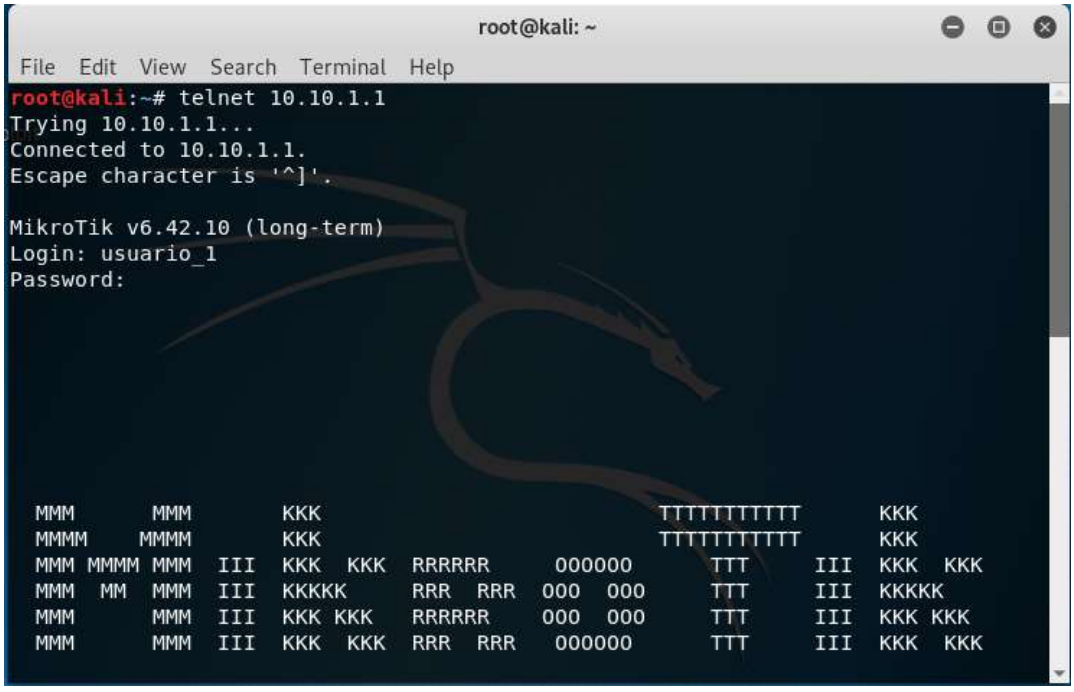


Figura 4.4: Acceso al router mediante Telnet.

En la figura 4.5, mediante Wireshark, se realiza un filtrado de los paquetes del protocolo Telnet.

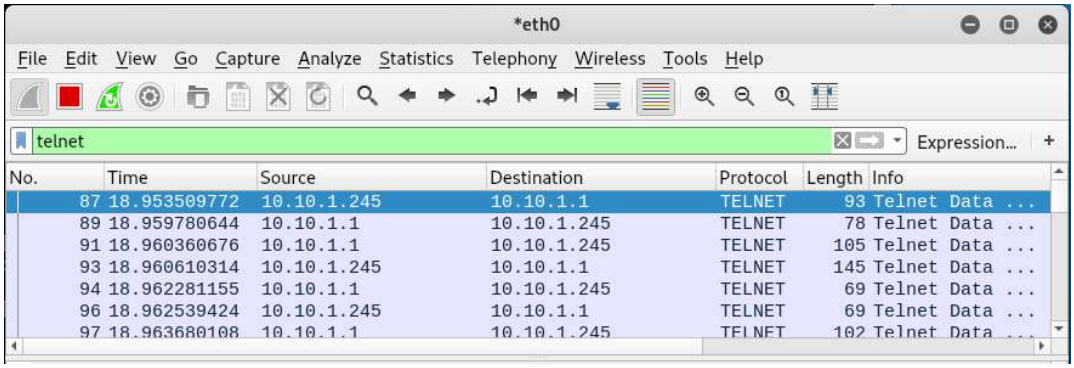


Figura 4.5: Filtrado de protocolo Telnet en Wireshark.

En cualquier paquete se hace click derecho/Follow/TCP Stream y se abre una ventana con toda la información de los paquetes Telnet, como el nombre de usuario y contraseña del administrador. La información obtenida se puede ver en la figura 4.6.

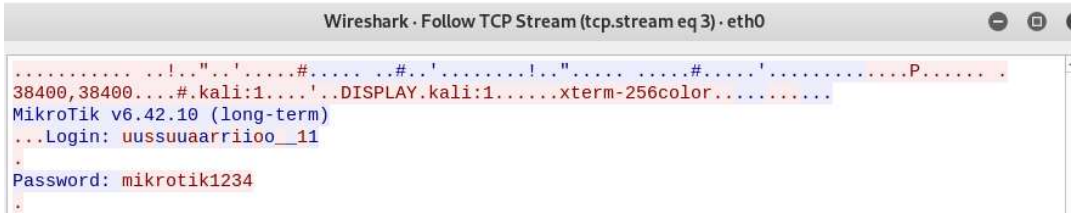


Figura 4.6: Obtención de nombre de usuario y contraseña del administrador.

Obtención de contraseña Winbox mediante Winbox Exploit

Para esta prueba se simuló el router, mediante el software GNS3, con la versión del sistema operativo RouterOS 6.42 (Stable).

Se utilizará la topología de la figura 4.1.

Algunas versiones de RouterOS cuentan con una vulnerabilidad identificada con el código universal CVE-2018-14847. Esta vulnerabilidad se basa en que, utilizando una herramienta llamada WinboxExploit, se puede obtener el archivo de base de datos de los usuarios del sistema a través del puerto Winbox. Las versiones vulnerables son: (Mikrotik, CVE-2018-14847 WINBOX VULNERABILITY, 2018).

- Desde la 6.29 a la 6.42 (Stable).
- Desde la 6.30.1 a la 6.40.7 (Longterm).
- Desde la 6.29rc1 a la 6.43rc3 (Beta).

WinboxExploit es una herramienta que se ejecuta con Python 3 y cuenta con las siguientes funciones (BasuCert, s.f.):

Winbox

- WinboxExploit: Acceso por Winbox (python3 WinboxExploit.py X donde X es la dirección IP de destino).

Mac Winbox Server

- MACServerExploit: Acceso por MAC Winbox Server (python3 MACServerExploit.py X donde X es la dirección MAC de destino).

Adicionalmente se puede agregar, junto a la dirección IP o MAC, el puerto de destino, en caso de que se haya cambiado el puerto por defecto.

En la figura 4.7 se pueden examinar los comandos ejecutados en la terminal para obtener el nombre de usuario y contraseña del router. El ataque está dirigido a la interfaz *ethernet* con dirección IP 10.10.1.1, pero también podría dirigirse a la dirección MAC, aprovechando los servicios de acceso por MAC que ofrece Mikrotik.

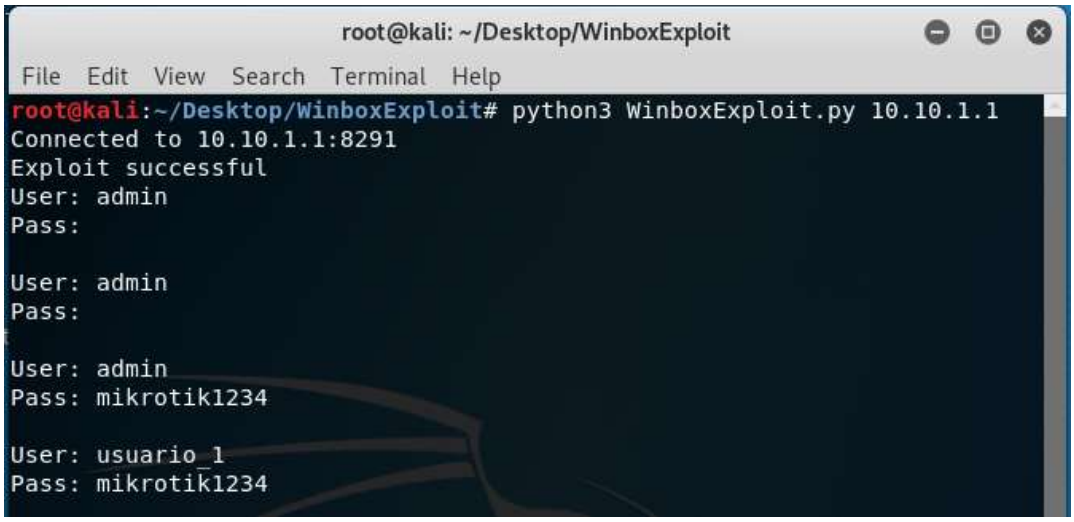


Figura 4.7: Obtención de nombre de usuario y contraseña mediante WinboxExploit.

Ataques de contraseña

En esta prueba se realizará un ataque de diccionario para obtener la contraseña de acceso, al router, por SSH.

Se utilizará la topología de la figura 4.1.

Un ataque de diccionario es una técnica para obtener acceso a un sistema protegido por una contraseña. Consiste en utilizar una lista de palabras y probar cada una de ellas como contraseña en el sistema de autenticación (Rouse, dictionary attack, s.f.). Este ataque se aprovecha del mal hábito, de los usuarios, de utilizar contraseñas cortas, con palabras comunes, sucesiones simples de números, etc.

Kali Linux dispone de hydra, la cual es una herramienta que permite realizar un ataque de diccionario (Kali, Hydra Package Description, s.f.).

Hydra soporta una gran cantidad de protocolos como: ftp, ssh, smtp, etc.

Algunas de las opciones que se pueden configurar dentro de hydra son las siguientes:

- -l: Nombre de usuario (-l X donde X es el nombre de usuario a probar).
- -L: Archivo con la lista de nombres de usuario (diccionario) (-L X donde X es la ruta al archivo).
- -P: Archivo con la lista de contraseñas (diccionario) (-P X donde X es la ruta al archivo).
- -x: Generador de contraseñas para fuerza bruta (-x MIN:MAX:CHARSET donde MIN y MAX son las cantidades mínima y máxima de caracteres y Charset es el juego de caracteres (A para letras mayúsculas, a para letras minúsculas y 1 para números)).
- -t: número de conexiones en paralelo (-t X donde X es el número de conexiones paralelas. Para ssh x=4).

Se debe indicar la dirección IP de destino y el protocolo que se desea usar.

En el router se dejó el nombre de usuario por defecto y se agregó una contraseña.

En la figura 4.8 se pueden analizar los comandos ejecutados en la terminal para obtener la contraseña del router. El ataque está dirigido a la interfaz *ethernet* con dirección IP 10.10.1.1, se utiliza ssh, se prueba con el nombre de usuario admin y se utiliza la lista de palabras rockyou.txt.

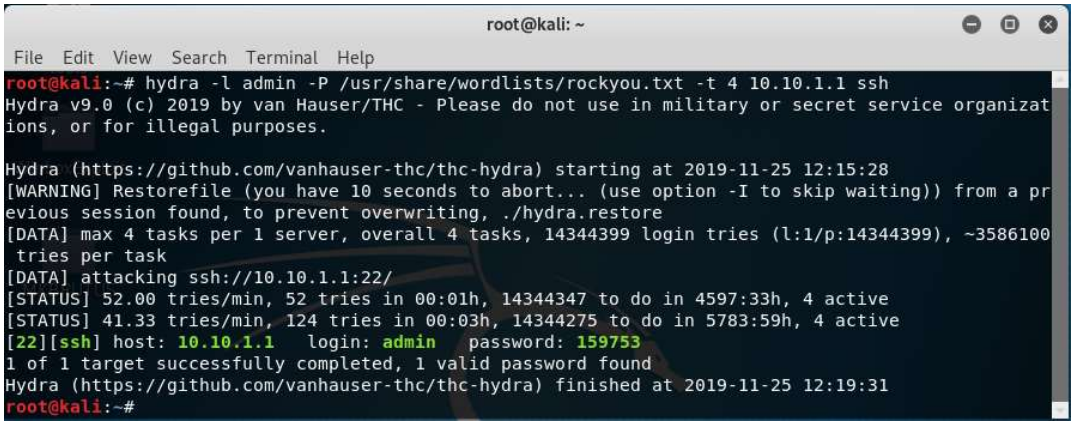


Figura 4.8: Ataque de diccionario exitoso.

En esta prueba se realizará un ataque de fuerza bruta para obtener la contraseña de acceso, al router, por SSH.

Un ataque de fuerza bruta es una técnica para obtener acceso a un sistema protegido por una contraseña. A diferencia del ataque de diccionario, en el ataque de fuerza bruta no se utiliza una lista de palabras, frases, etc. si no se utilizan todas las combinaciones posibles de caracteres permitidos para formar contraseñas y probarlas en el sistema de autenticación (Rouse, brute force attack, s.f.).

La herramienta hydra permite realizar ataques de fuerza bruta.

En el router se dejó el nombre de usuario por defecto y se agregó una contraseña.

En la figura 4.9 se pueden examinar los comandos ejecutados en la terminal para obtener la contraseña del router. El ataque está dirigido a la interfaz *ethernet* con dirección IP 10.10.1.1, se utiliza ssh, se prueba con el nombre de usuario admin y cada contraseña tiene un total de 4 caracteres numéricos.

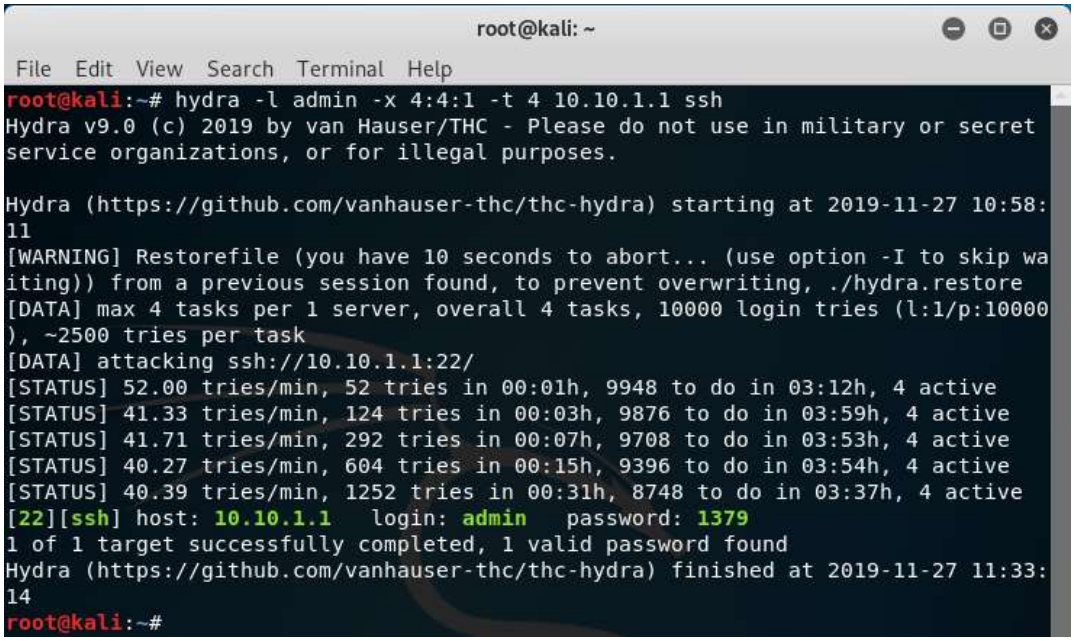


Figura 4.9: Ataque de fuerza bruta exitoso.

SYN-FLOOD

Este ataque aprovecha el enlace de 3 vías para el establecimiento de una conexión TCP. Consiste en enviar una gran cantidad de segmentos TCP con la bandera SYN habilitada y direcciones de origen falsas para abrir conexiones con un servidor. Por cada segmento SYN recibido, el servidor responderá con un segmento SYN-ACK y generará una conexión a medio abrir esperando un acuse de recibo por parte del cliente. Debido a que las direcciones de origen son falsas, el servidor nunca recibirá un acuse de recibo, por lo que llegará a saturarse el número de conexiones disponibles que el servidor puede atender (Ariganello, 2014).

Se utilizará la topología de la figura 4.2.

Kali Linux dispone de hping3, la cual es una herramienta que permite realizar un ataque SYN-FLOOD (Kali, Kali Tools, s.f.).

Algunas herramientas que se pueden utilizar dentro de hping3 son las siguientes:

Opciones para host

- -c: Cantidad de paquetes a enviar (-c X donde X es la cantidad de paquetes).
- -i: Intervalo de tiempo en el que se envía cada paquete (-i uX donde X es el tiempo en microsegundos).
- --flood: Enviar paquetes a la máxima velocidad posible.

Modo

- El modo por defecto es TCP.

IP

- --rand-source: Los paquetes se envían con direcciones IP de origen aleatorias.
- -a: Permite modificar la dirección IP de origen (-a X donde X es la dirección IP a suplantar).

UDP/TCP

- -p: Puerto de destino (-p X donde X es el número de puerto).
- -S: Establece la bandera SYN.

Se utilizará metasploitable 2, como un servidor web, para probar los efectos de un ataque SYN FLOOD y validar las configuraciones, en un router, que permitan mitigar el ataque.

Se puede acceder al servidor web por medio del puerto 80 y la dirección IP 10.10.2.2.

En la figura 4.10 se puede observar el acceso al servidor a través de un navegador web.

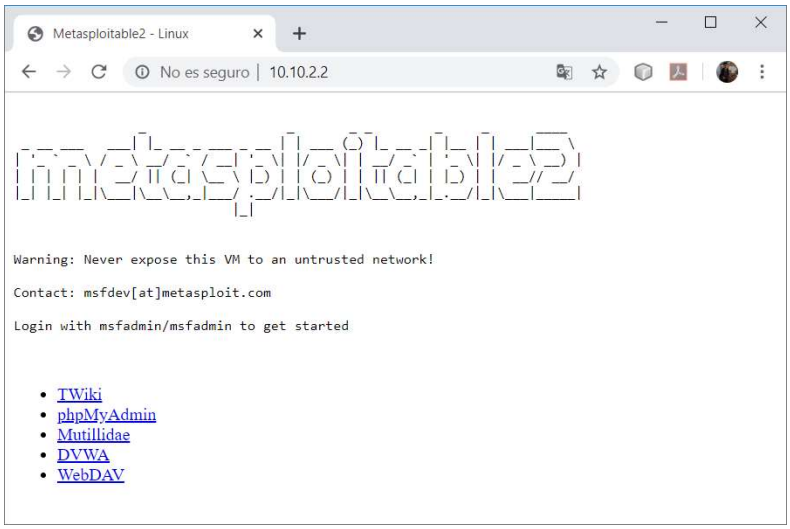


Figura 4.10: Acceso al servidor web de Metasploitable 2.

Desde la computadora, con dirección IP 10.10.3.254, se intenta acceder al servidor, a través del navegador web, y se establece la conexión de forma exitosa. En la figura 4.11, mediante Wireshark, se visualizan los paquetes que conforman el enlace de 3 vías.

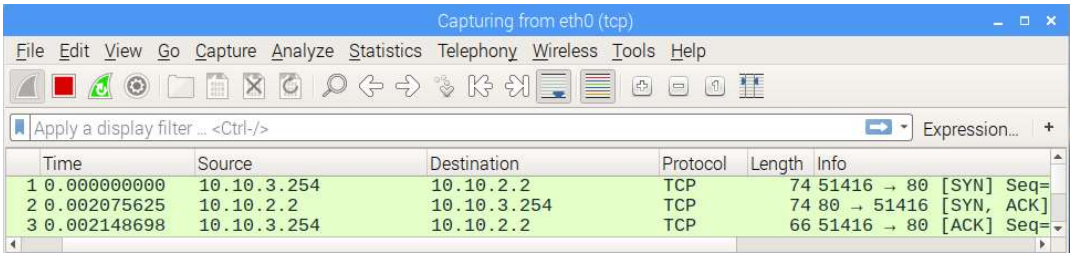


Figura 4.11: Intento de conexión, desde un cliente legítimo, al servidor web.

Desde la computadora del atacante, mediante la terminal de Kali Linux, se realiza un ataque SYN FLOOD desde la dirección IP falsa 10.10.3.3, al puerto 80 de la dirección IP 10.10.2.2 y con una velocidad de 100 p/s (intervalo de tiempo de 10000 us). Los comandos se pueden examinar en la figura 4.12.

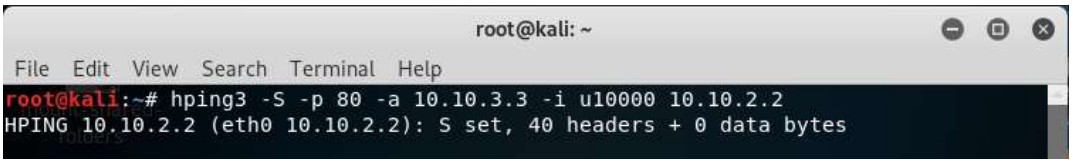


Figura 4.12: Ataque SYN FLOOD mediante hping3.

En la figura 4.13 se encuentra la ventana de monitoreo de las interfaces del router. Se puede observar que la interfaz *ethernet 1* recibe paquetes a una velocidad de 104 p/s y se transmiten por la interfaz *ethernet 2* a una velocidad de 98 p/s. Esto quiere decir que el router permite el paso de los paquetes.

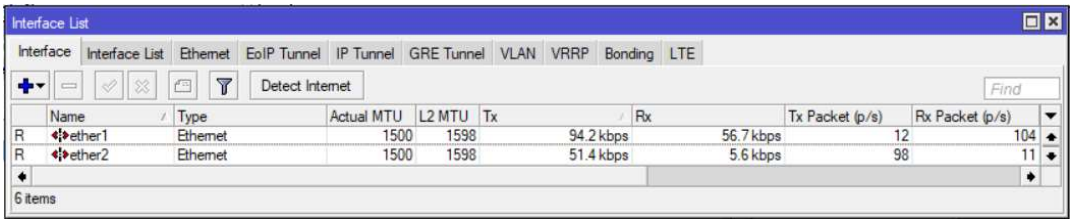


Figura 4.13: Monitoreo de tráfico en la ventana Interface List.

En la figura 4.14, mediante Wireshark, se puede notar que al servidor ingresa una gran cantidad de paquetes SYN provenientes de la dirección IP 10.10.3.3.

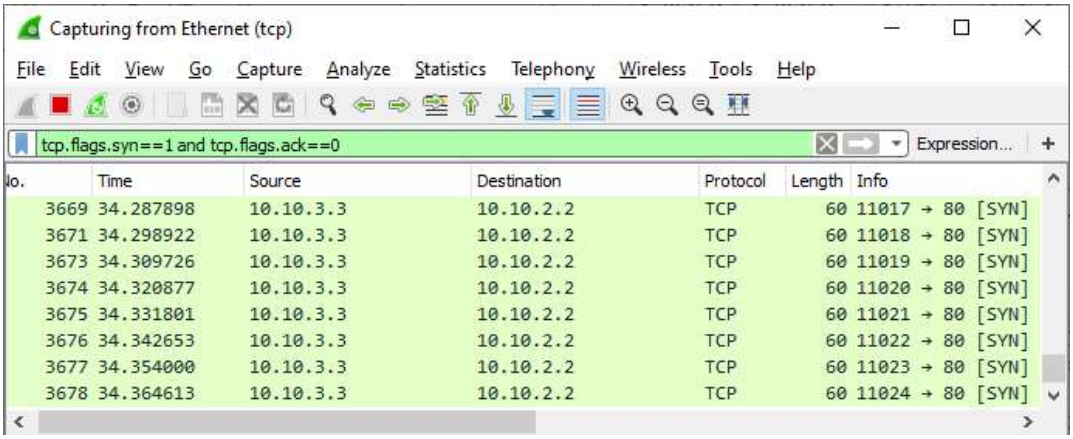


Figura 4.14: Monitoreo de tráfico, mediante Wireshark, en el servidor.

Desde la computadora con dirección IP 10.10.3.254 se intenta acceder al servidor, a través del navegador web, pero no se obtiene respuesta porque el servicio ha sido denegado. En la figura 4.15, mediante Wireshark, se comprueba que se envía el paquete SYN, pero no se recibe el paquete SYN-ACK.

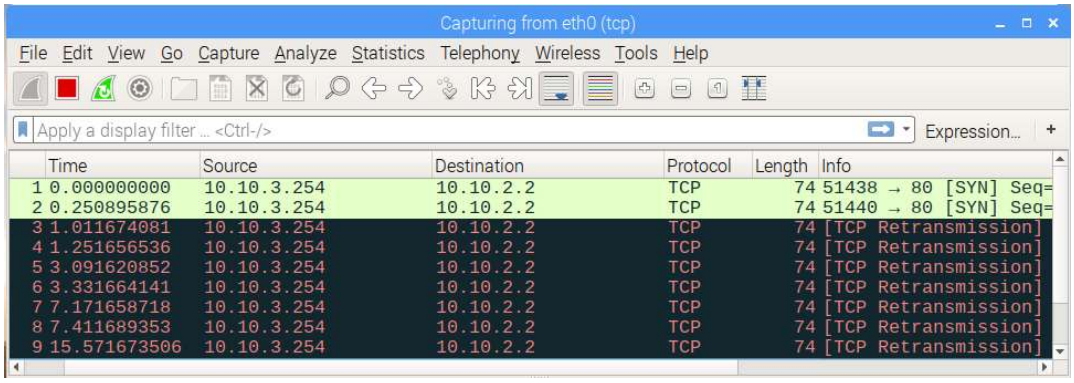


Figura 4.15: Intento de conexión, desde un cliente legítimo, al servidor web.

IP SPOOFING

El SPOOFING se conoce en español como suplantación y consiste "en que una entidad finge ser otra" (Stallings, 2004).

"El IP SPOOFING consiste en la creación de paquetes IP en los que se modifica la dirección IP de origen con el objetivo de ocultar la identidad del atacante, hacerse pasar por otra computadora o ambos. Esta técnica es muy utilizada en ataques DDOS (Distributed Denial of Service)" (CLOUDFLARE, s.f.).

Se utilizará la topología de la figura 4.2.

La técnica de SPOOFING está disponible en una gran cantidad de herramientas de ataque dentro de Kali Linux. Debido a que se requiere la creación de paquetes IP, se puede utilizar la herramienta hping 3, como se vio en la sección de SYN FLOOD.

Para realizar la suplantación de la dirección IP de origen se pueden utilizar los dos siguientes comandos:

- --rand-source: Los paquetes se envían con direcciones IP de origen aleatorias.
- -a: Permite modificar la dirección IP de origen (-a X donde X es la dirección IP a suplantar).

En esta primera prueba se utilizará la técnica de SPOOFING para vulnerar las configuraciones de seguridad realizadas en la sección SYN FLOOD y se comprobará que el servidor deja de responder.

Las reglas de firewall de protección contra SYN FLOOD están activas.

Mediante la terminal de Kali Linux se realiza un ataque SYN FLOOD generando paquetes con direcciones IP de origen aleatorias, al puerto 80 de la dirección IP 10.10.2.2 y con una velocidad de 5000 p/s (intervalo de tiempo de 200 us). La velocidad puede variar. Los comandos se pueden examinar en la figura 4.16.

Figura 4.16: Ataque SYN FLOOD mediante hping3.

Las configuraciones de seguridad, para el ataque SYN FLOOD, limitan el número de paquetes consecutivos que ingresan al router desde una misma dirección IP. Es posible vulnerar estas configuraciones al generar cada paquete con una dirección suplantada aleatoria.

En la figura 4.17 se encuentra la ventana de monitoreo de las interfaces del router. Se puede observar que la interfaz *ethernet 1* recibe paquetes a una velocidad de 2960 p/s y se transmiten por la interfaz *ethernet 2* a una velocidad de 2526 p/s. Esto quiere decir que el router no descarta los paquetes del ataque SYN FLOOD.

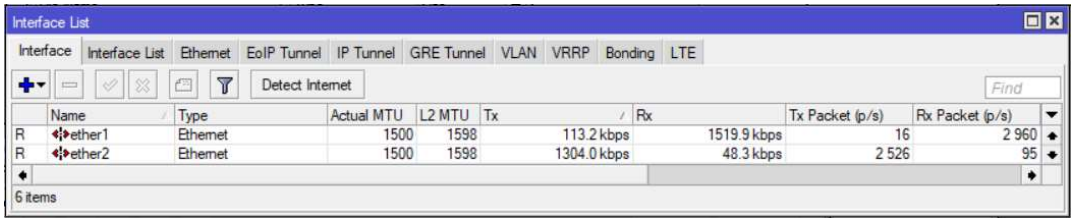


Figura 4.17: Monitoreo de tráfico en ventana Interface List.

En la figura 4.18 se verifica que no se ha agregado ninguna dirección IP a la lista de bloqueo, debido a que cada paquete, que ingresa al router, tiene una dirección IP de origen diferente.

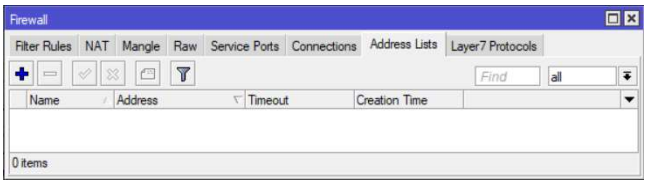


Figura 4.18: Pestaña Address Lists.

En la figura 4.19, mediante Wireshark, se comprueba que al servidor ingresa una gran cantidad de paquetes SYN provenientes de direcciones IP diferentes.

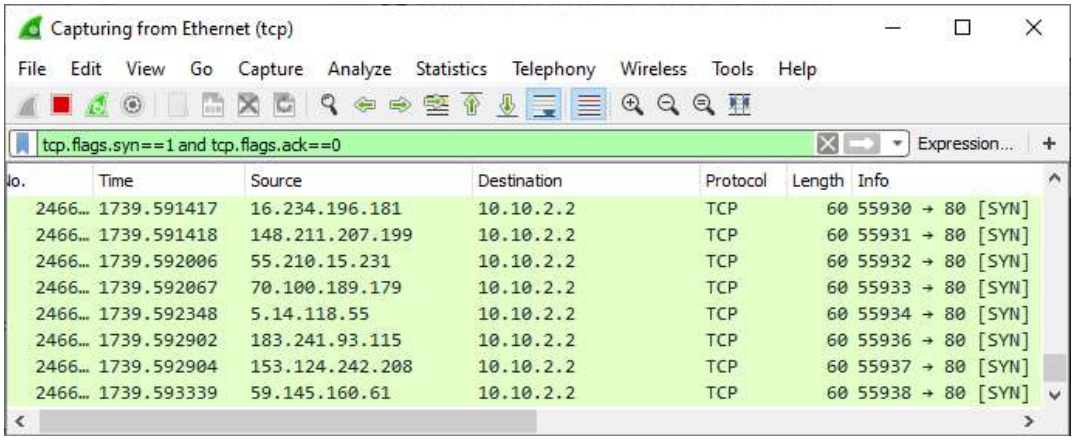


Figura 4.19: Monitoreo de tráfico, mediante Wireshark, en el servidor.

Desde la computadora, con dirección IP 10.10.3.254, se intenta acceder al servidor, a través del navegador web, pero no se obtiene respuesta porque el servicio ha sido denegado. En la figura 4.20, mediante Wireshark, se verifica que se envía el paquete SYN, pero no se recibe el paquete SYN-ACK.

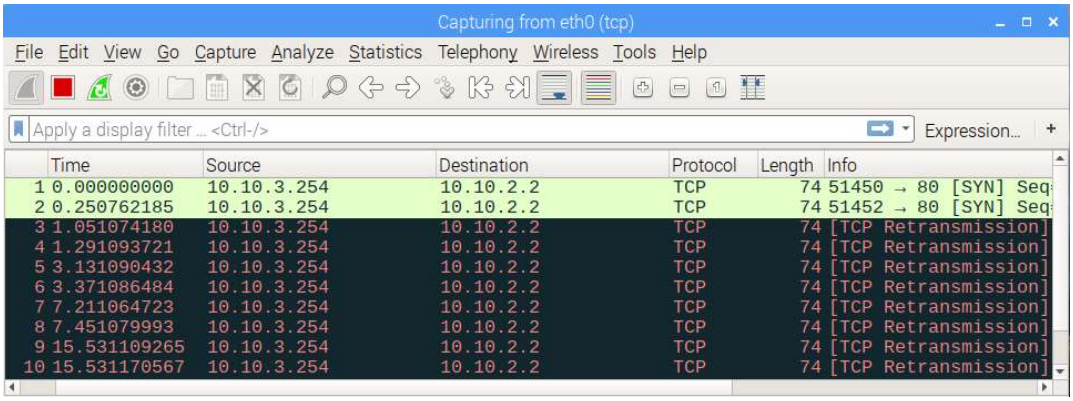


Figura 4.20: Intento de conexión, desde un cliente legítimo, al servidor web.

En esta segunda prueba se mostrará que se puede acceder al servidor usando una dirección IP de origen suplantada.

En las pruebas de la sección SYN-FLOOD ya se suplantó una dirección IP mediante el comando –a. Se generó el ataque con paquetes cuya dirección IP era 10.10.3.3, la cual no corresponde a la red de dirección 10.10.1.0/24 donde está conectado el atacante. Las configuraciones de seguridad limitaban un flujo excesivo de paquetes, pero no controlaban el origen de los mismos.

Mediante la terminal de Kali Linux se envían paquetes con la dirección IP de origen 10.10.3.3 al puerto 80 de la dirección IP 10.10.2.2. Los comandos se pueden analizar en la figura 4.21.

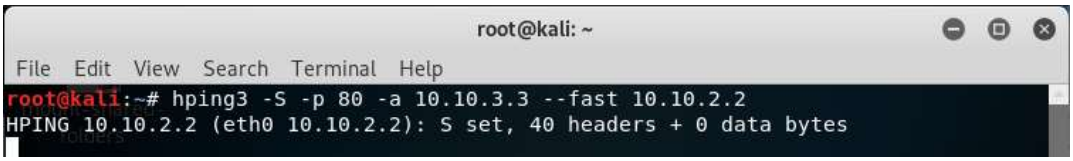


Figura 4.21: Intento de establecer una conexión, con dirección IP suplantada, al servidor.

En la figura 4.22 se encuentra la ventana de monitoreo de las interfaces del router. Se puede observar que la interfaz *ethernet 1* recibe paquetes y se transmiten por la interfaz *ethernet 2*. Esto quiere decir que el router permite el paso de los paquetes con direcciones IP suplantadas.

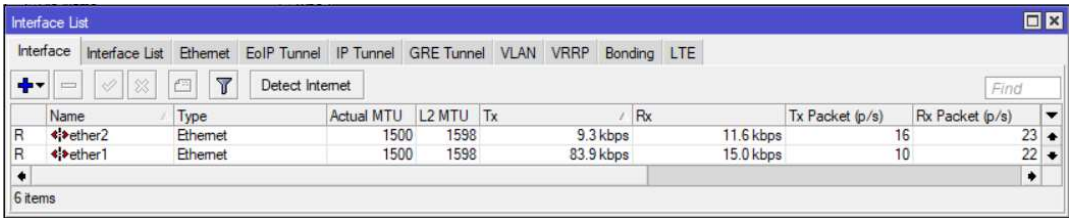


Figura 4.22: Monitoreo de tráfico en ventana Interface List.

En la figura 4.23, mediante Wireshark, se comprueba que los paquetes, con direcciones IP suplantadas, ingresan al servidor.

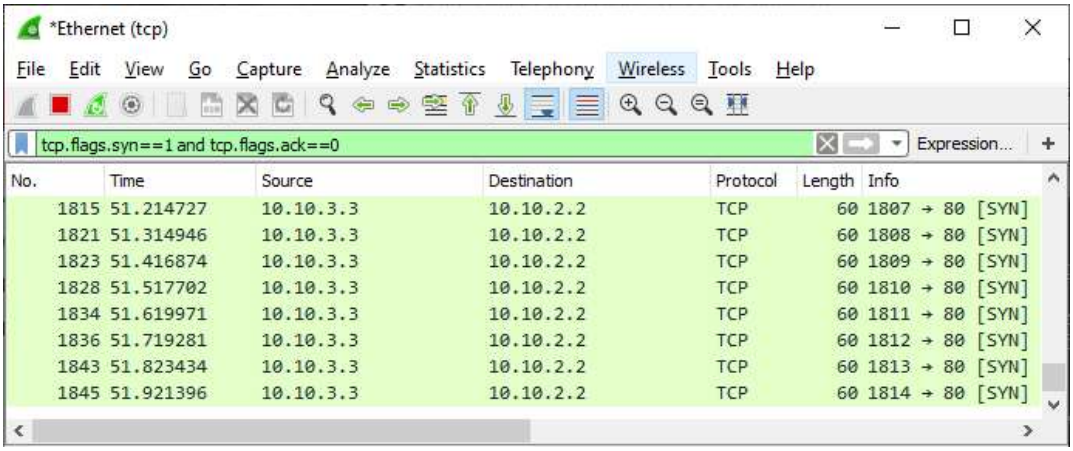


Figura 4.23: Monitoreo de tráfico, mediante Wireshark, en el servidor.

ESCANER DE RED

Un escaneo de red es un ataque en el que se realiza un descubrimiento de red con el objetivo de obtener información de la misma. Algunas de las técnicas que se utilizan son las siguientes (Ariganello, 2014) (Kali, Nmap Package Description, s.f.) (Hart, Network Scanning With Nmap, s.f.):

- Barridos de ping: “Determina qué rango de direcciones IP corresponde a los hosts activos”.
- Escaneo de puertos: “Escaneo de un rango de números de puerto TCP o UDP en un host para detectar servicios abiertos”.

- Escaneo de servicios: Determina versiones de software de los equipos analizados.

Se utilizará la topología de la figura 4.2.

Kali Linux dispone de Nmap, la cual es una herramienta que permite realizar un escaneo de red (Kali, Nmap Package Description, s.f.).

Algunas herramientas que se pueden utilizar dentro de Nmap son las siguientes (Nmap):

Descubrimiento de hosts

- -sn: Escaneo de hosts mediante mensajes ICMP echo y timestamp (-sn X donde X es una dirección IP). Adicionalmente se envía un paquete SYN al puerto 443 y un paquete ACK al puerto 80.
- -Pn: Escaneo de puertos, versión o sistema operativo asumiendo que todos los hosts están activos.

Técnicas de escaneo

- -sS: Escaneo TCP SYN (no se establece una conexión TCP completa). Se envía un paquete SYN y se espera un paquete SYN/ACK si el puerto está abierto o un paquete RST si el puerto está cerrado. Posteriormente se envía un paquete RST.
- -sT: Escaneo TCP de puertos mediante enlace de 3 vías (se establece una conexión completa). La conexión puede ser registrada por el sistema operativo de destino.
- -sA: Permite detectar si se utiliza un filtrado de paquetes o firewall mediante el envío de un paquete ACK. Si el puerto está abierto o cerrado responderá con un paquete RST. Si el puerto está filtrado, no responderá o enviará un mensaje ICMP de error.
- -sU: Escaneo UDP mediante el envío de una cabecera a un puerto. El puerto está cerrado si se recibe un mensaje de error ICMP de destino inalcanzable (puerto inalcanzable). El puerto está abierto o filtrado si no se recibe respuesta.
- -sN: Escaneo TCP Null. Se envía un paquete sin las banderas SYN, RST o ACK. Un puerto cerrado responderá con un paquete RST, un puerto abierto o

filtrado no responderá y un puerto filtrado responderá con un mensaje de error ICMP.

- -sF: Escaneo TCP FIN. Se envía un paquete con la bandera FIN. Las respuestas del destino son iguales que en el escaneo TCP Null.
- -sX: Escaneo TCP Xmas. Se envía un paquete con las banderas FIN, PSH y URG. Las respuestas del destino son iguales que en el escaneo TCP Null.

Especificación de puertos

- -p: Establece los puertos de destino (-p X donde X es el número de puerto o -p X-Y donde X-Y es un rango de puertos).

Detección de servicios

- -sV: Determina el servicio y versión disponible en un puerto.

Detección de sistema operativo

- -o: Habilita la detección del sistema operativo.

Control de tiempo y rendimiento

- --scan-delay: Establece el tiempo de demora entre cada paquete que se envía (--scan-delay X donde X es el tiempo).

En esta prueba se utilizará Nmap para obtener información sobre la red a la que está conectado el servidor.

En la figura 4.24 se puede observar que, mediante la terminal de Kali Linux, se realiza un descubrimiento de hosts en la red 10.10.2.0/24. Se descubrió que 3 hosts están activos (un host corresponde a la computadora donde se está ejecutando la máquina virtual).

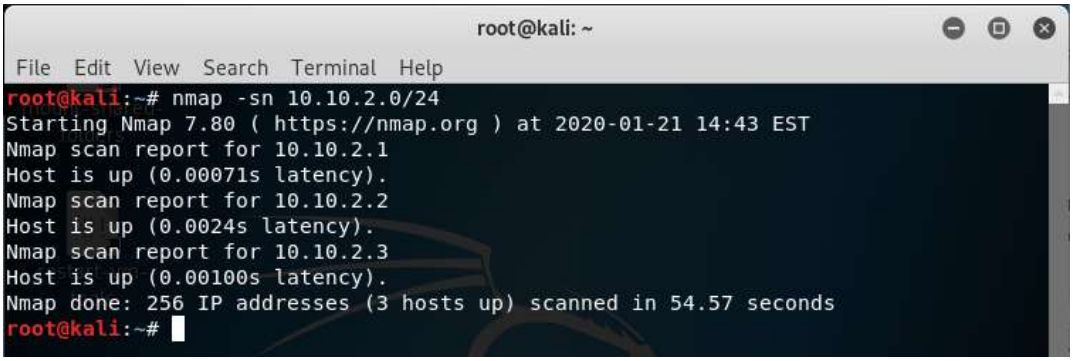


Figura 4.24: Descubrimiento de hosts exitoso.

Con los comandos de la figura 4.25 se verifica, en los hosts activos, si los puertos están protegidos por un firewall o filtrados. En este caso se analiza del puerto 21 al 80. Se descubrió que los puertos no están protegidos.

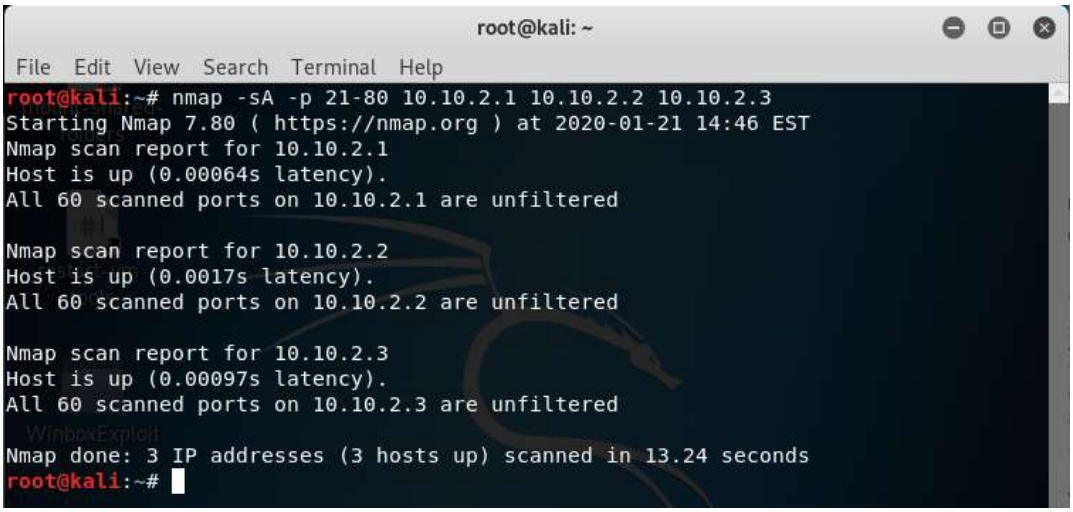


Figura 4.25: Descubrimiento exitoso de filtrado en puertos.

En la figura 4.26 se realiza un escaneo TCP SYN para identificar los puertos que están abiertos. En este caso se analiza del puerto 21 al 80.

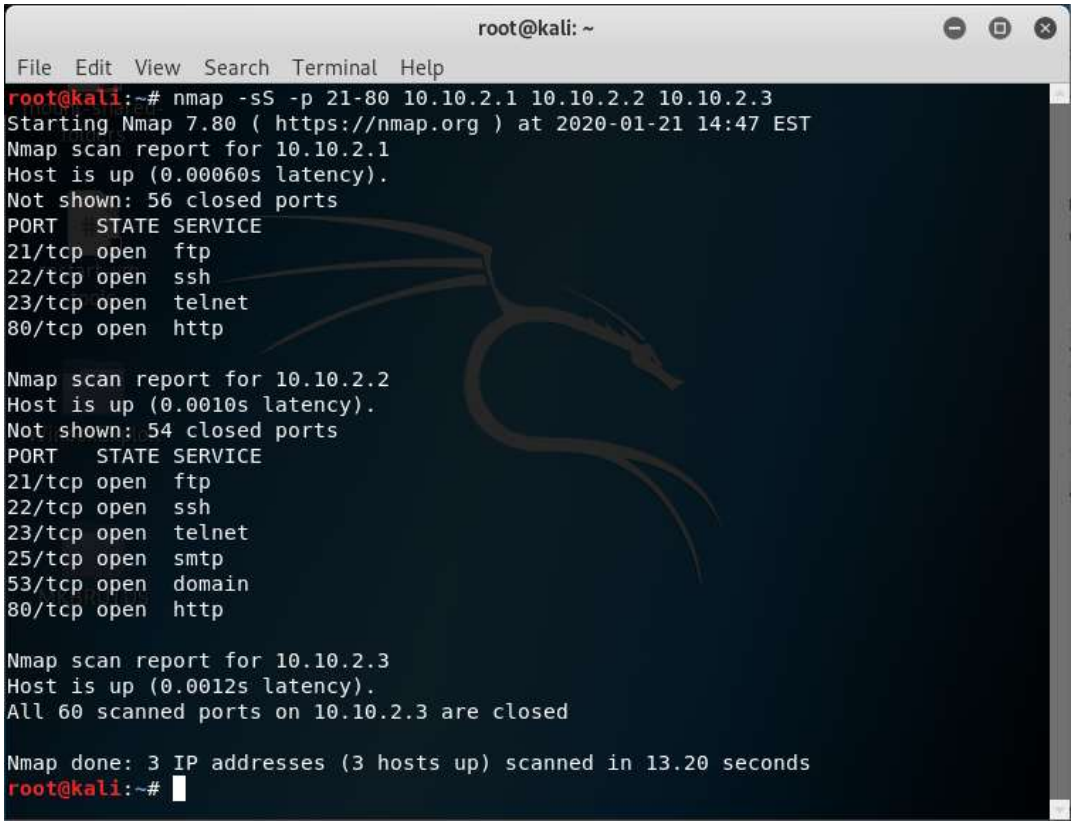


Figura 4.26: Escaneo TCP SYN exitoso.

Con los comandos de la figura 4.27 se identifican los servicios y versiones en cada puerto analizado. Se excluye del análisis la dirección IP 10.10.2.3, porque no tiene puertos abiertos. Los resultados también indican que la dirección IP 10.10.2.1 corresponde a una interfaz del router y la dirección IP 10.10.2.2 corresponde al servidor.

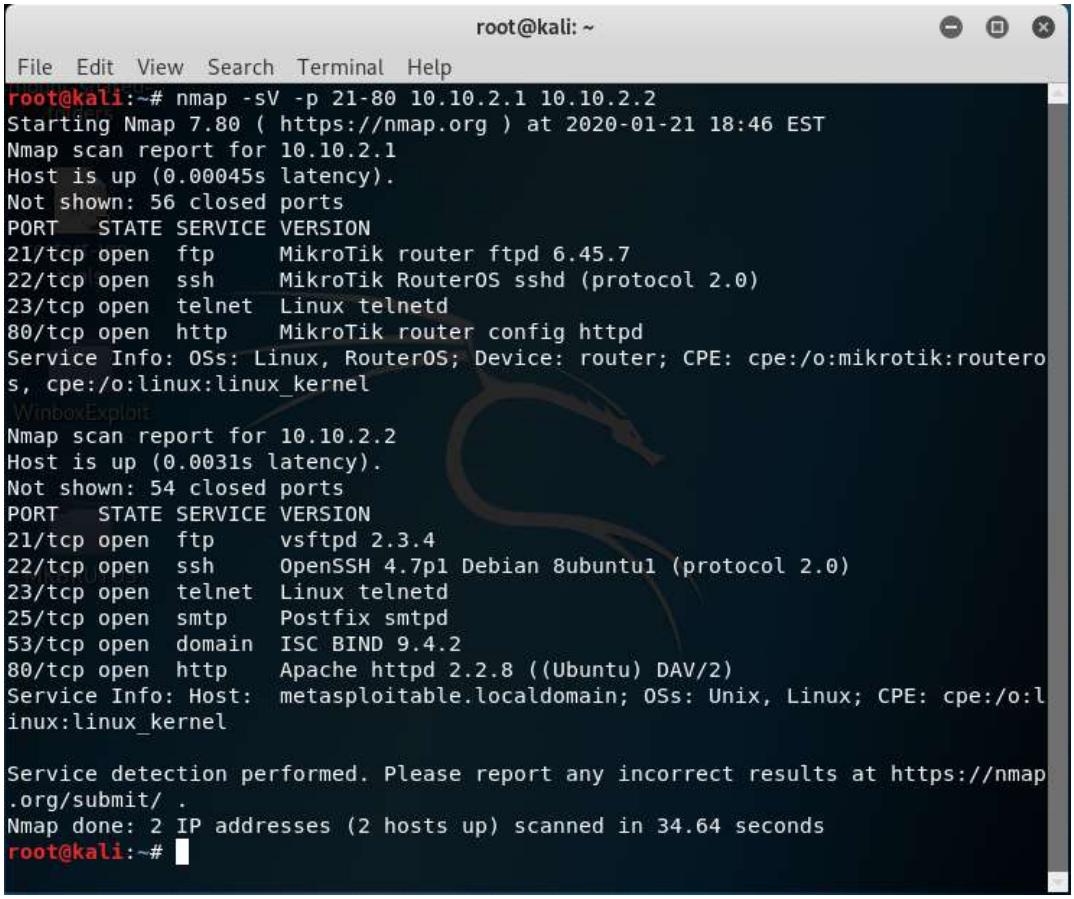


Figura 4.27: Descubrimiento exitoso de servicios y versiones en puertos.

En la figura 4.28 se realiza un escaneo UDP para identificar los puertos que están abiertos. En este caso se analiza del puerto 21 al 80.

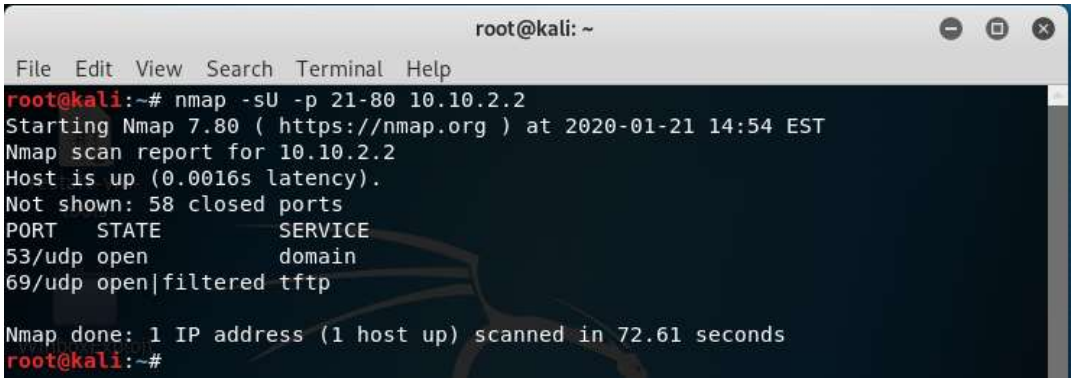


Figura 4.28: Escaneo UDP exitoso.

4.2.3. Configuraciones de seguridad

Cambiar el nombre de usuario (admin) y contraseña (vacío) por defecto.

Como se puede ver en la figura 4.29, en la ventana User List y la pestaña Users se pueden administrar los usuarios que tengan acceso al router. El usuario que tiene acceso total es el administrador y se debe cambiar su nombre de usuario y contraseña por defecto para evitar accesos no autorizados (Higgins) (Mikrotik, Manual:Securing Your Router, s.f.). Se recomienda usar una contraseña que contenga letras mayúsculas, minúsculas, números, símbolos, etc. Se pueden utilizar herramientas que generan contraseñas seguras (Mikrotik, Manual:Securing Your Router, s.f.).

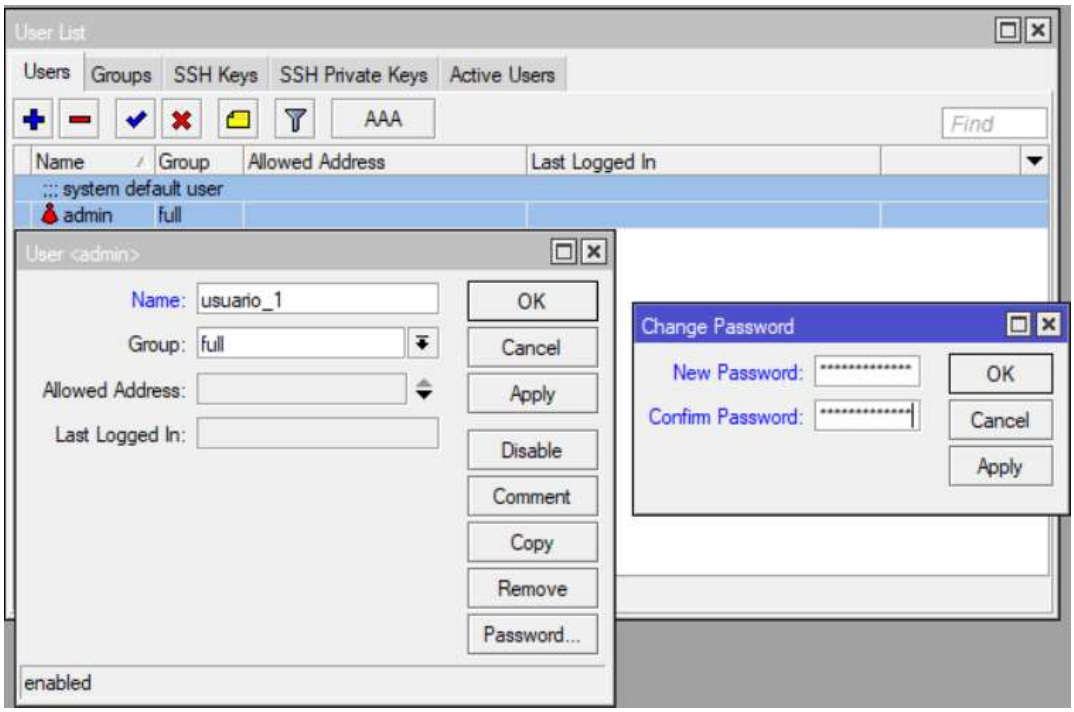


Figura 4.29: Cambio de nombre de usuario y contraseña del administrador.

Asignación de grupos

"No todos los administradores requieren los mismos roles y privilegios de acceso a los dispositivos de la infraestructura" (Ariganello, 2014). Por esto es necesario crear usuarios para todos los administradores y asignarlos a grupos de acuerdo a los niveles y privilegios que estos tengan (Takeuchi).

Por defecto existen 3 grupos (Mikrotik, Manual:Router AAA, s.f.):

- Full: Acceso total.

- Write: No tiene acceso vía ftp, no puede administrar usuarios, no tiene acceso al servidor dude.
- Read: No tiene acceso vía ftp, no puede administrar usuarios, no tiene acceso al servidor dude y no puede modificar configuraciones.

Se pueden crear grupos en los que se realice una configuración personalizada de privilegios. En la figura 4.30 se encuentran los privilegios que se pueden asignar.

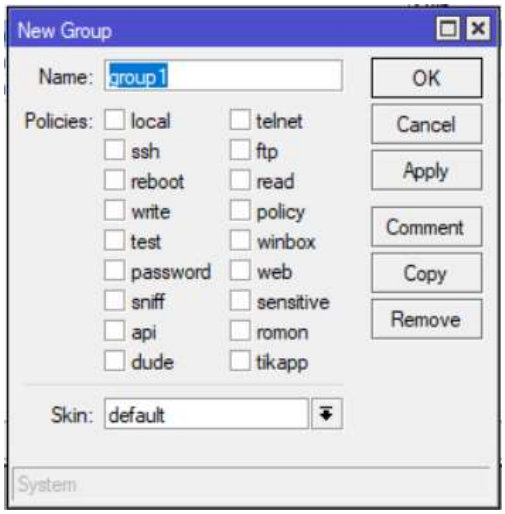


Figura 4.30: Creación de grupo con privilegios personalizados.

En la figura 4.31 se puede notar que, en la ventana User List y la pestaña Users, se puede crear un nuevo usuario y asignarlo a un grupo con privilegios limitados.

Adicionalmente se puede configurar una dirección IP permitida para cada usuario.

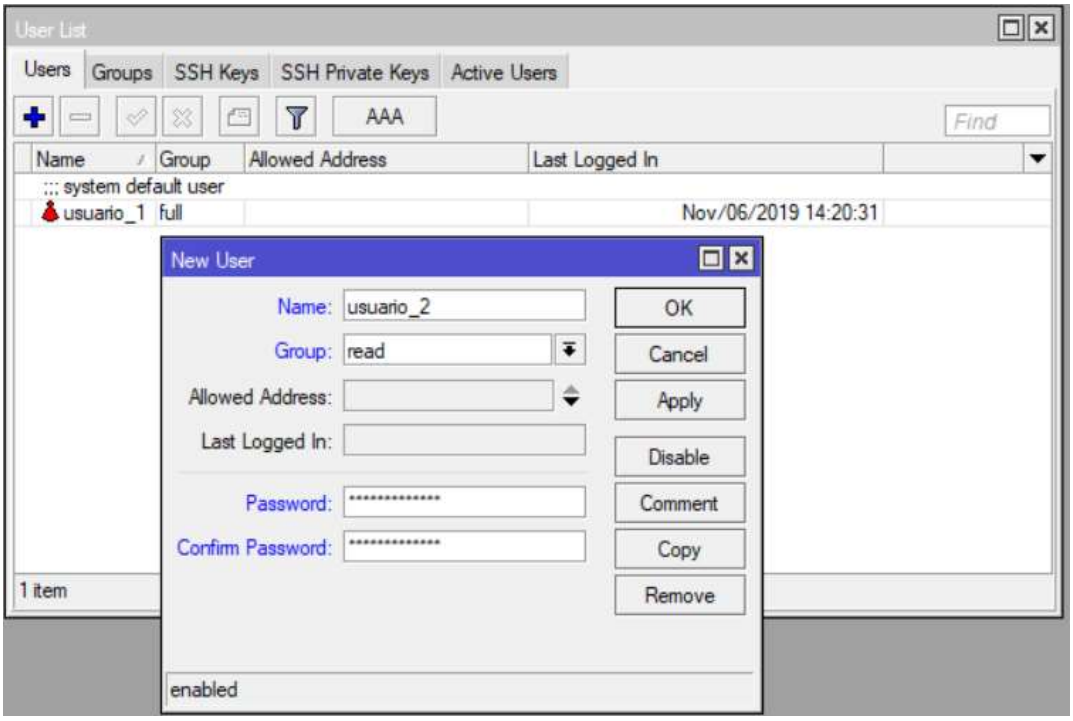


Figura 4.31: Creación de usuario y asignación a grupo.

Uso de servicios seguros

Los dispositivos deben ser administrados a través de servicios seguros como SSH o secured Winbox. Se recomienda desactivar el resto de servicios (Higgins) (Mikrotik, Manual:Securing Your Router, s.f.) (Hart, MikroTik Router Hardening).

En la figura 4.32 se puede verificar que, en la ventana IP Service List, se pueden desactivar los servicios que no son seguros.

Adicionalmente, en cada servicio, se puede cambiar el puerto por defecto y asignar una dirección IP permitida desde la cual se debería conectar (Mikrotik, Manual:Securing Your Router, s.f.).

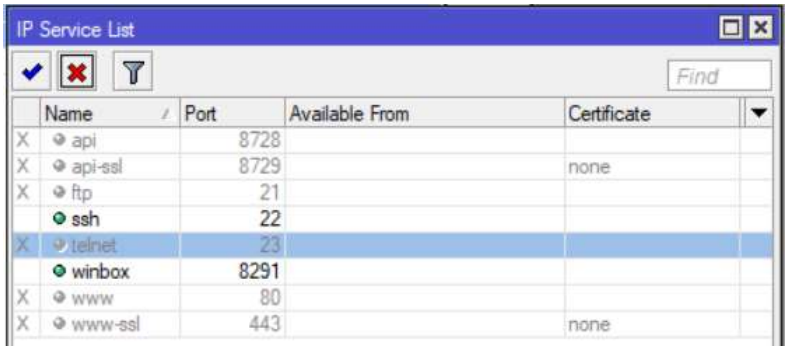


Figura 4.32: Habilitación solo de servicios seguros.

Activación solo de servicios que se van a utilizar

Acceso por MAC

Existen algunos servicios que permiten acceder a un dispositivo de red mediante direcciones MAC en lugar de direcciones IP. Se recomienda desactivarlos (Higgins) (Mikrotik, Manual:Securing Your Router, s.f.) (Takeuchi) (Hart, MikroTik Router Hardening).

Estos servicios son (Mikrotik, Manual:Securing Your Router, s.f.):

- MAC Telnet Server.
- MAC Winbox Server.
- MAC Ping Server.

En la figura 4.33 se puede observar que, en la ventana de MAC Server, se desactivan los servicios de acceso por MAC.

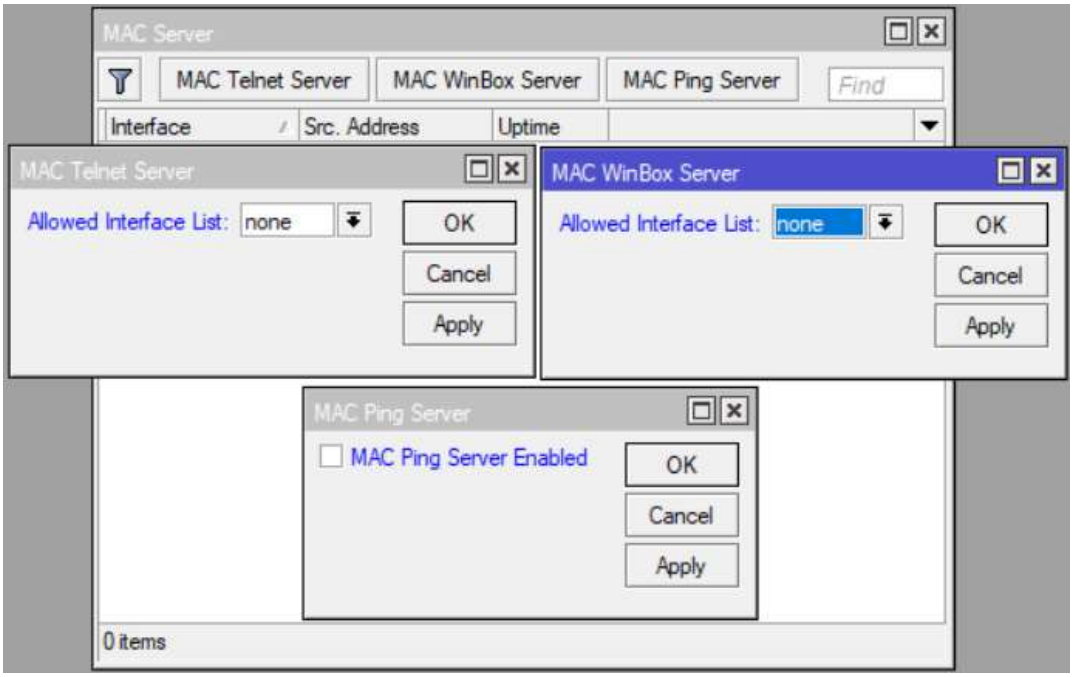


Figura 4.33: Desactivación de servicios de acceso por direcciones MAC.

Neighbor Discovery

Se recomienda desactivar el protocolo Neighbor Discovery, debido a que este permite que otros dispositivos detecten al router y obtengan información del mismo (Higgins) (Mikrotik, Manual:Securing Your Router, s.f.) (Takeuchi) (Hart, MikroTik Router Hardening).

Como se puede ver en la figura 4.34, en la ventana Neighbor List se puede desactivar este protocolo.

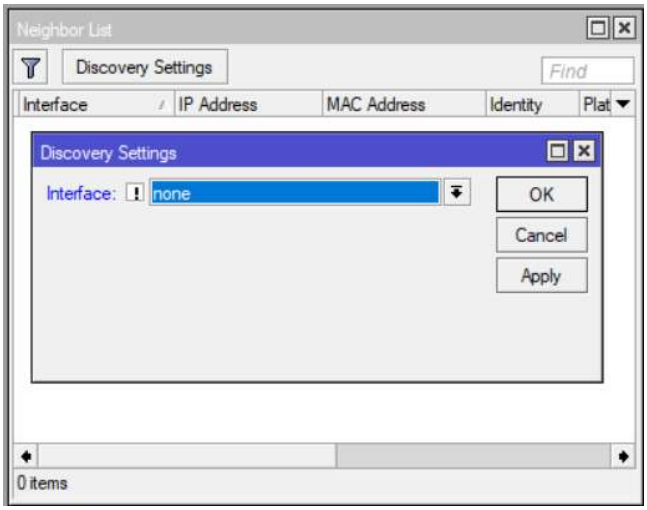


Figura 4.34: Desactivación del protocolo Neighbor Discovery.

Bandwidth server

Se recomienda desactivar Bandwidth server, porque es un servicio que no se utiliza seguido e implica un puerto abierto innecesariamente (Higgins) (Mikrotik, Manual:Securing Your Router, s.f.) (Takeuchi) (Hart, MikroTik Router Hardening).

En la ventana BTest Server Settings se puede desactivar este servicio, como se puede ver en la figura 4.35.

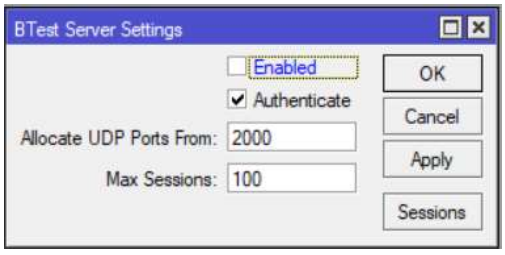


Figura 4.35: Desactivación de servicio Bandwidth Server.

Servidor DNS

Un servidor DNS puede ser un blanco de ataques, por lo que se recomienda desactivarlo si no se requiere tenerlo configurado en el router (Mikrotik, Manual:Securing Your Router, s.f.) (Takeuchi) (Hart, MikroTik Router Hardening).

En la figura 4.36 se puede notar que, en la ventana DNS Settings, se puede desactivarlo (Allow Remote Requests).

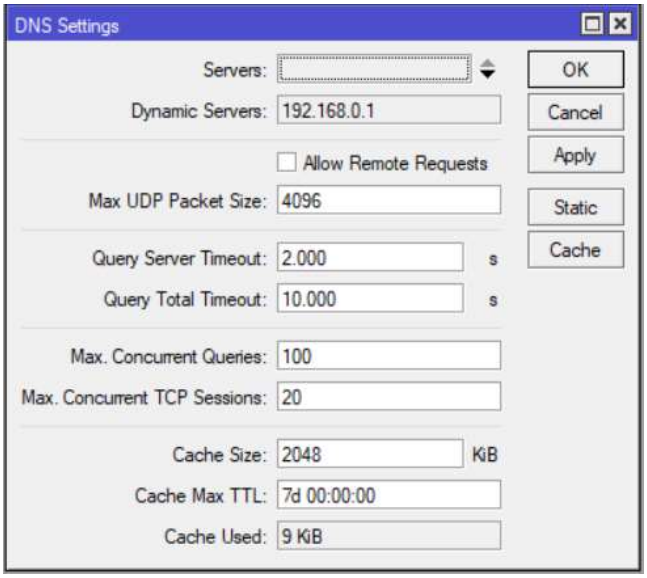


Figura 4.36: Desactivación de servidor DNS.

Desactivar Cloud Update Time

Es importante que los dispositivos de una red estén sincronizados y tengan la hora precisa y actualizada para el análisis de registros. Se recomienda utilizar servidores NTP en lugar del servicio, de sincronización de relojes, que ofrece Mikrotik (Hart, Network Scanning With Nmap, s.f.).

Como se puede observar en la figura 4.37, en la ventana Cloud se puede desactivar Update Time.

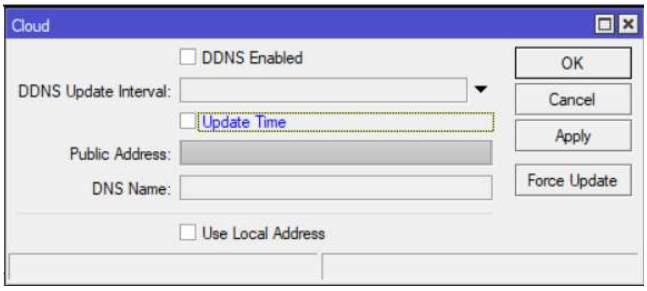


Figura 4.37: Desactivación de Cloud Update Time.

Para utilizar el protocolo NTP, en routers Mikrotik, se debe instalar el paquete ntp.

Aumentar seguridad en acceso SSH

Se recomienda habilitar la opción de encriptación fuerte (Higgins) (Mikrotik, Manual:Securing Your Router, s.f.) (Hart, MikroTik Router Hardening).

Esta opción permite utilizar algoritmos de encriptación más fuertes.

En la figura 4.38 se puede notar que se debe activar utilizando la terminal.

```
[usuario_1@MikroTik] > ip ssh set strong-crypto=yes
[usuario_1@MikroTik] >
```

Figura 4.38: Activación de encriptado fuerte.

Desactivar interfaces que no se usen

Se recomienda deshabilitar las interfaces que no se utilicen en el router para evitar accesos no autorizados (Mikrotik, Manual:Securing Your Router, s.f.).

Si un atacante tiene acceso físico a los dispositivos, deberá desconectar un cable de una interfaz que esté en uso y llamará la atención (Hart, MikroTik Router Hardening).

En la figura 4.39 se puede verificar que, en la ventana Interface List y la pestaña Interface, se pueden desactivar las interfaces.

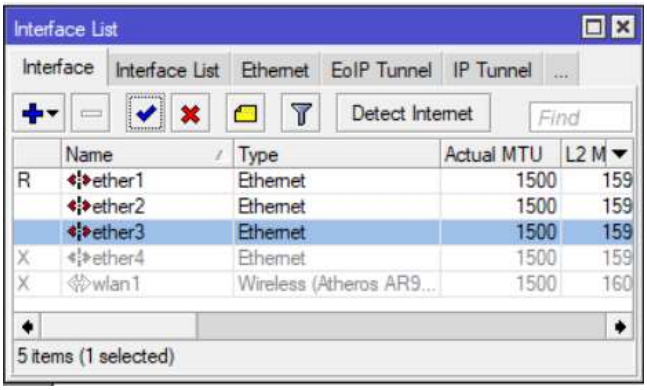


Figura 4.39: Ventana Interface List.

Desactivar LCD (Liquid Crystal Display)

Algunos routers disponen de un LCD para mostrar información. Se recomienda desactivarlo (Mikrotik, Manual:Securing Your Router, s.f.).

En la figura 4.40 se puede ver cómo se desactiva el módulo LCD mediante la terminal.

```
[usuario_1@MikroTik] > lcd set enabled=no
```

Figura 4.40: Desactivación de LCD.

Mantener actualizado el sistema operativo

Los sistemas operativos están en constante actualización con el objetivo de implementar mejoras o corregir vulnerabilidades que puedan tener versiones anteriores.

Se recomienda siempre actualizar a la última versión (Stable o Long Term) (Higgins) (Ariganello, 2014).

En la figura 4.41 se puede observar que, en la ventana Package List, se puede actualizar el sistema operativo (Mikrotik, Manual:Upgrading, s.f.).

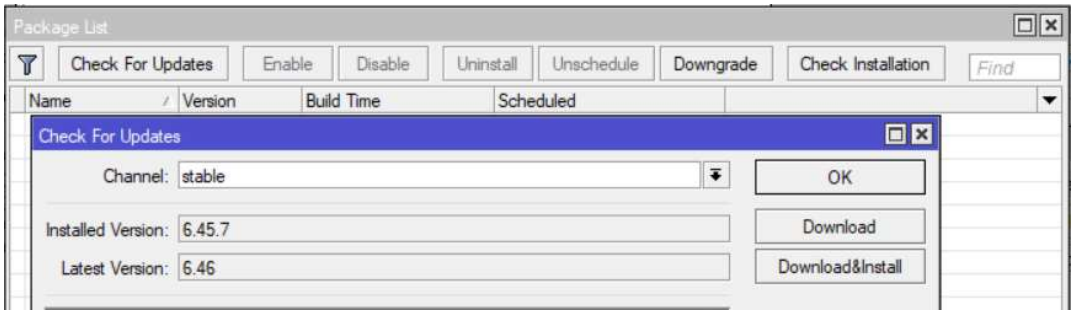


Figura 4.41: Actualización del sistema operativo.

Posterior a la actualización del sistema operativo se debe actualizar el firmware. En la figura 4.42 se puede ver que la actualización se realiza en la ventana Routerboard (Mikrotik, Manual:Upgrading, s.f.).

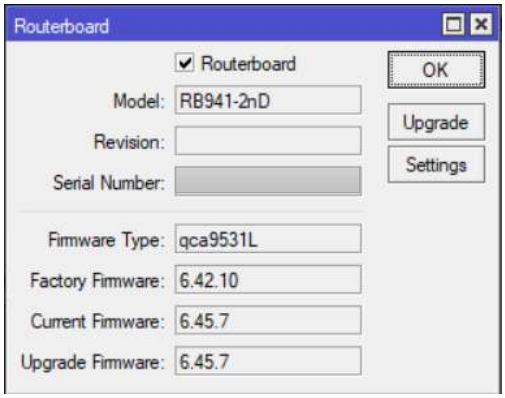


Figura 4.42: Actualización del firmware.

Respaldo de configuraciones

Se recomienda tener un archivo de respaldo de las configuraciones del router, en caso de que se necesite reconfigurar el mismo o uno nuevo (Ariganello, 2014).

En la figura 4.43 se puede notar que, en la ventana File List, se puede realizar un respaldo de la configuración actual del router y asignarle una contraseña.

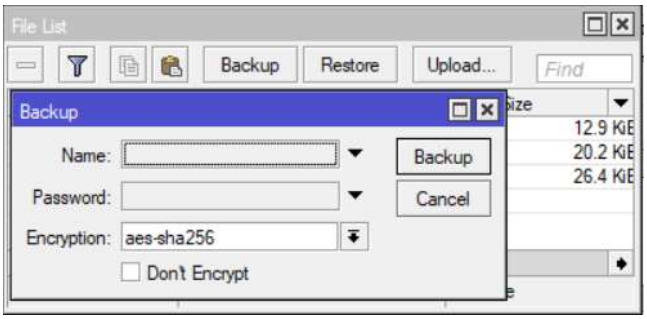


Figura 4.43: Respaldo de la configuración del router.

Limitar el número de intentos de ingreso fallidos

Una forma de protección contra ataques de contraseña es bloquear al usuario que supere un número de intentos fallidos de ingreso, pero en los parámetros de configuración del router no existe una herramienta específica que permita realizar esta detección.

En la figura 4.44, mediante Wireshark, se analizan los paquetes que se generan con un ataque de este tipo y se puede identificar un patrón en los paquetes TCP:

- Se abre una conexión.
- Se termina la conexión después de un número determinado de intentos fallidos de descifrar el nombre de usuario y contraseña.

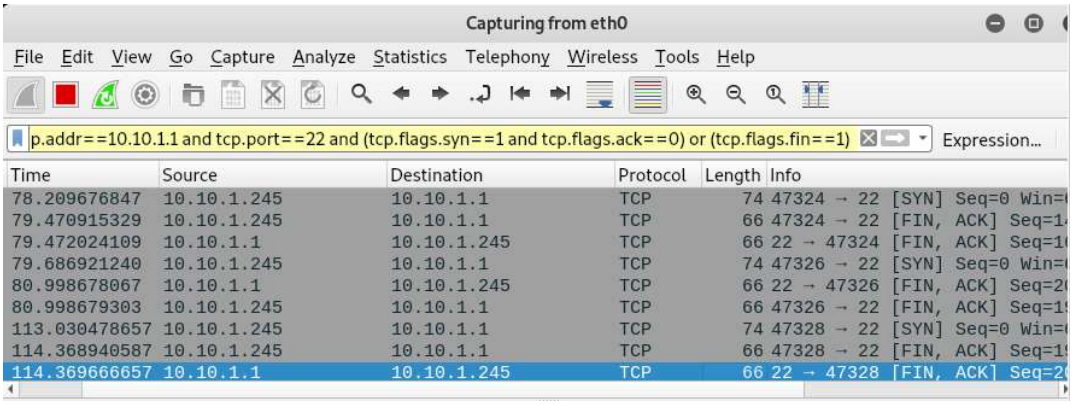


Figura 4.44: Análisis de paquetes durante un ataque de contraseña.

Firewall es una herramienta que permite realizar un filtrado de paquetes, por lo tanto, provee opciones de seguridad que permiten controlar el tráfico en el router. Sirve para prevenir accesos no autorizados y minimizar amenazas de seguridad. Su funcionamiento se basa en analizar los paquetes que ingresan al router y compararlos con unas reglas preestablecidas para posteriormente ejecutar una acción sobre esos paquetes, como descartarlos, aceptarlos, etc. (Ariganello, 2014) (Mikrotik, Manual:IP/Firewall/Filter, s.f.)

Se pueden configurar reglas de firewall que realicen lo siguiente: si se abren varias conexiones, en el puerto de SSH, desde una misma dirección IP y en un periodo de tiempo determinado, la IP de origen se agrega a una lista de bloqueo (Mikrotik, Bruteforce login prevention, s.f.).

Se necesitan 5 reglas de firewall.

La primera regla de Firewall tiene como objetivo descartar todos los paquetes provenientes de las direcciones IP de la lista de bloqueo.

En la figura 4.45 se encuentran las configuraciones realizadas en la pestaña General, las cuales establecen que los paquetes entrantes deben estar dirigidos al router (Chain: input).

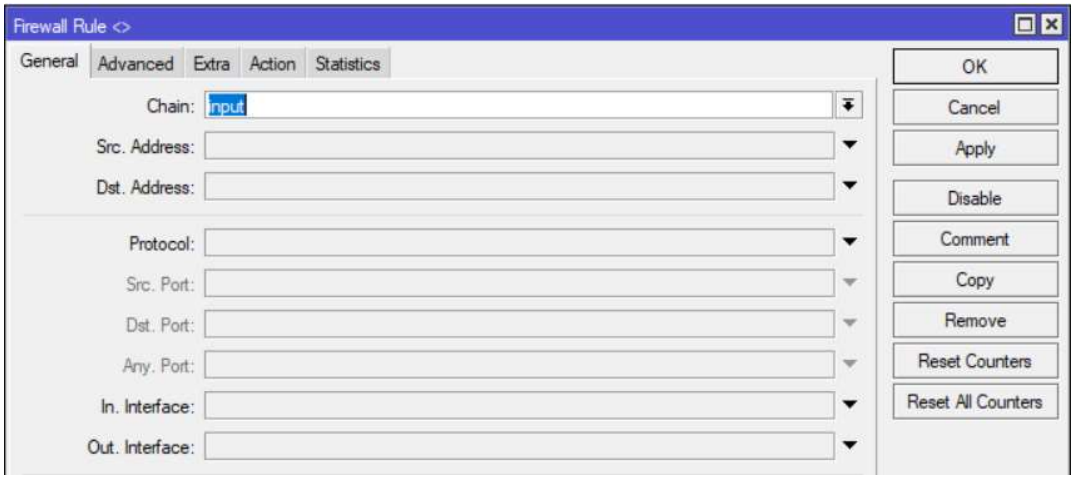


Figura 4.45: Configuraciones en la pestaña General.

Como se puede ver en la figura 4.46, las configuraciones realizadas en la pestaña Advanced establecen que las direcciones IP de origen deben pertenecer a la lista BruteForceAttacker (Src. Address List: BruteForceAttacker).

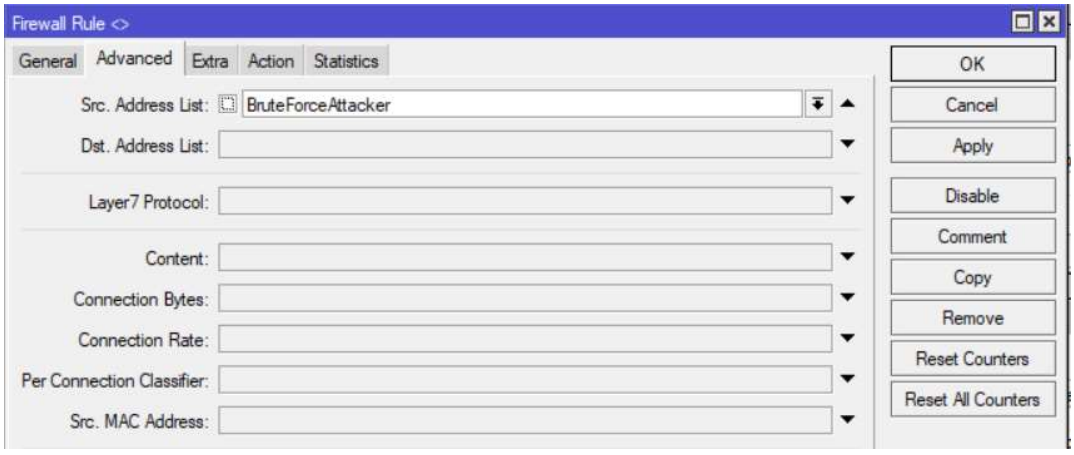


Figura 4.46: Configuraciones en la pestaña Advanced.

En la figura 4.47 se pueden observar las configuraciones realizadas en la pestaña Action, las cuales establecen que los paquetes se descarten (Action: drop).

Figura 4.47: Configuraciones en la pestaña Action.

La segunda regla de Firewall tiene como objetivo determinar si los paquetes entrantes corresponden a un intento de abrir una conexión mediante el protocolo SSH y enviarlos a las reglas de Firewall 3, 4 y 5.

Como se puede ver en la figura 4.48, las configuraciones realizadas en la pestaña General establecen que los paquetes entrantes deben estar dirigidos al router (Chain: input), el protocolo debe ser TCP (Protocol: 6(tcp)), el puerto de destino debe corresponder a SSH (Dst. Port: 22) y la conexión debe ser nueva (Connection State: new).

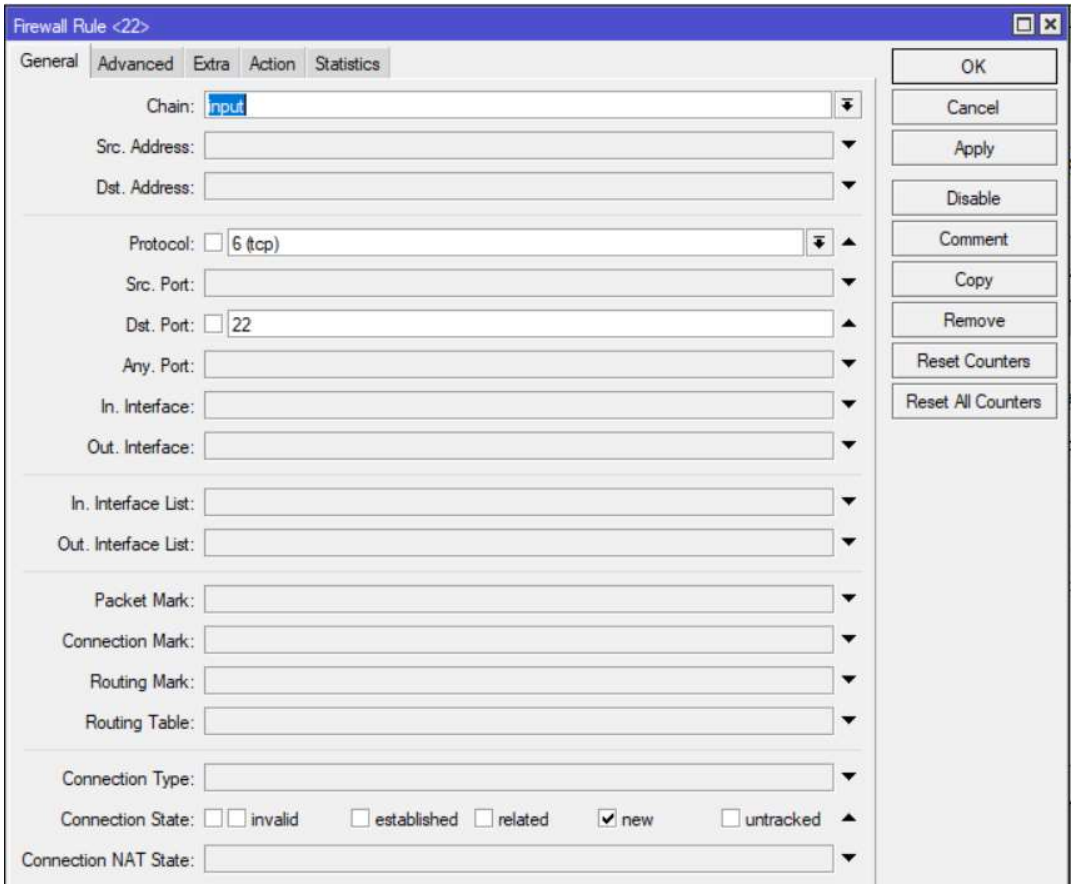


Figura 4.48: Configuraciones en la pestaña General.

En la figura 4.49 se encuentran las configuraciones realizadas en la pestaña Action, las cuales establecen que los paquetes pasen (Action: jump) a una nueva cadena llamada SSHCon (Jump Target: SSHCon).

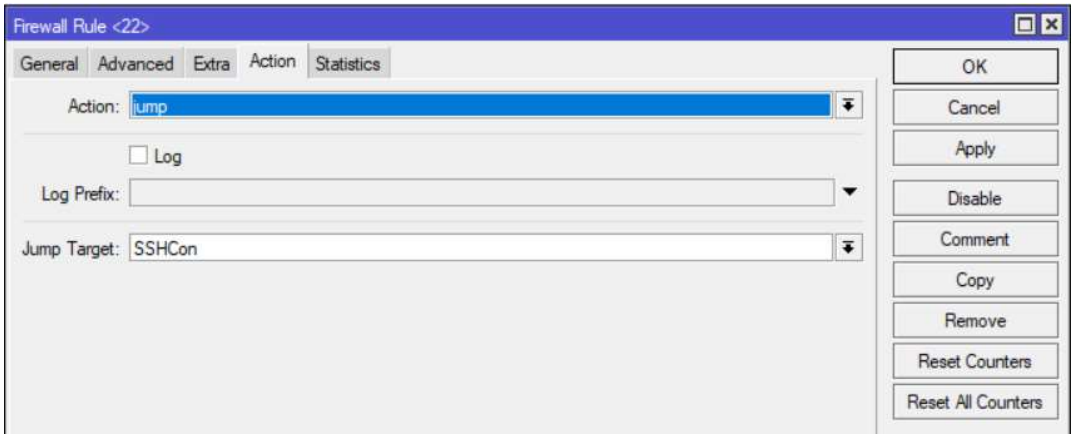


Figura 4.49: Configuraciones en la pestaña Action.

La tercera regla de Firewall tiene como objetivo agregar a la lista de bloqueo las direcciones IP de la lista auxiliar 2.

Como se puede ver en la figura 4.50, las configuraciones realizadas en la pestaña General establecen que los paquetes entrantes deben venir de la primera regla de Firewall (Chain: SSHCon).

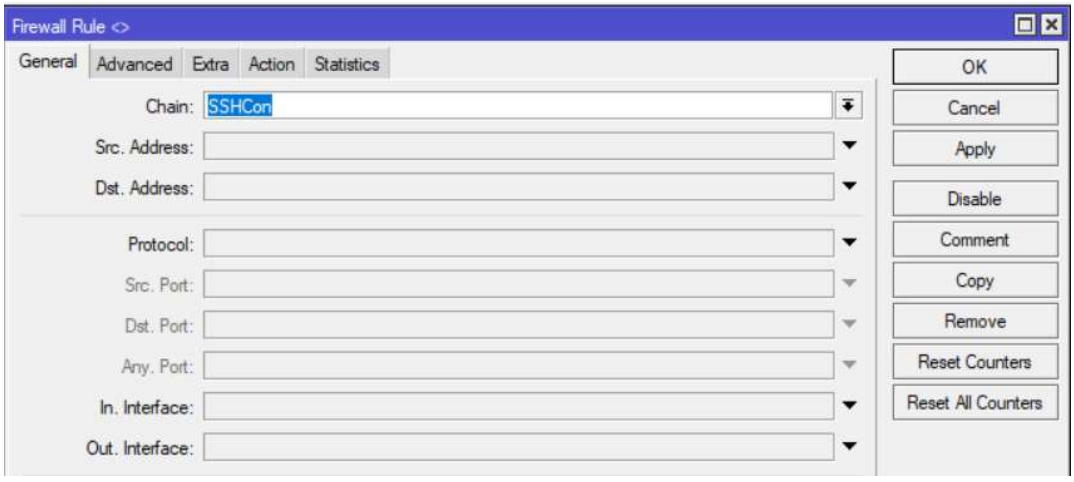


Figura 4.50: Configuraciones en la pestaña General.

Como se puede observar en la figura 4.51, las configuraciones realizadas en la pestaña Advanced establecen que las direcciones IP de origen deben pertenecer a la lista Con2SSH (Src. Address List: Con2SSH).

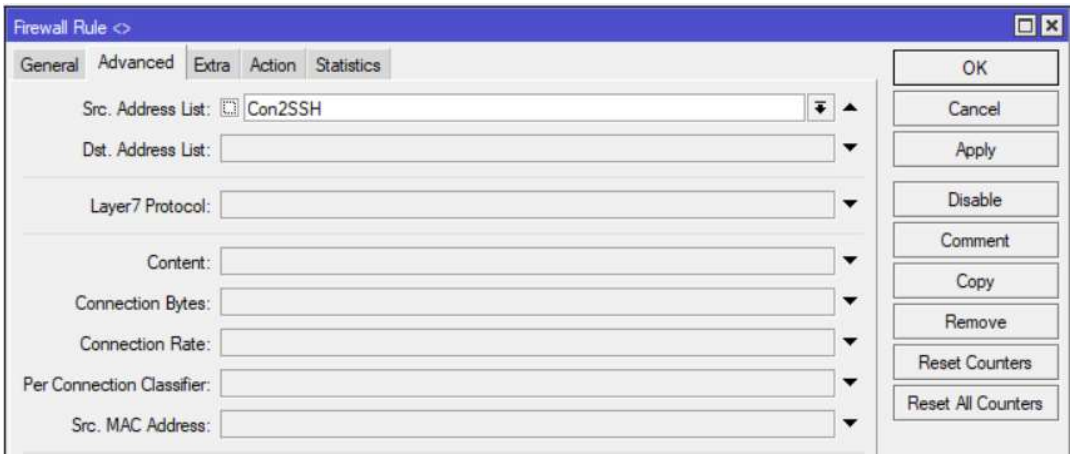


Figura 4.51: Configuraciones en la pestaña Advanced.

En la figura 4.52 se pueden examinar las configuraciones realizadas en la pestaña Action, las cuales establecen que la dirección IP de origen se agregue (Action: add src to address list) a la lista BruteForceAttacker (Address List: BruteForceAttacker) por un día (Timeout: 1d 00:00:00).

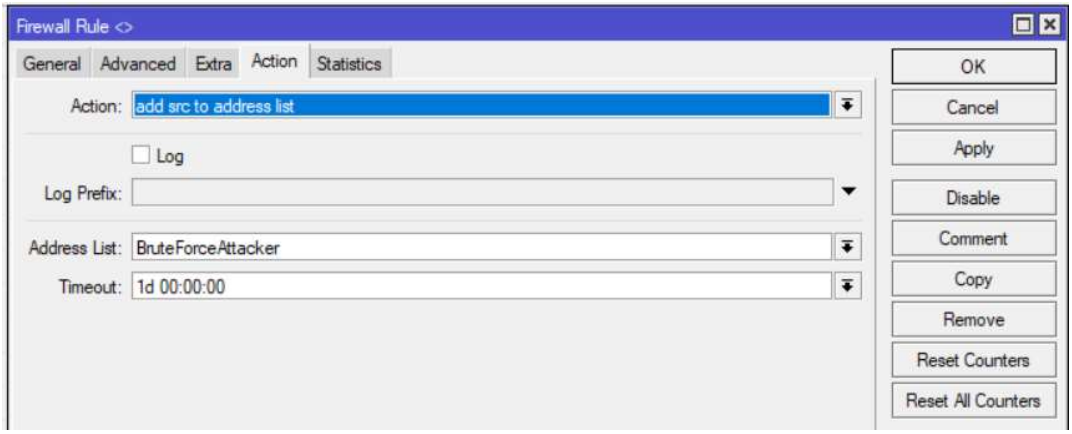


Figura 4.52: Configuraciones en la pestaña Action.

La cuarta regla de Firewall tiene como objetivo agregar, durante 1 minuto, a la lista auxiliar 2 las direcciones IP de la lista auxiliar 1.

Las configuraciones son similares a las de la tercera regla de firewall. Los parámetros que cambian son los siguientes: (Src. Address List: Con1SSH), (Address List: Con2SSH) y (Timeout: 00:01:00).

La quinta regla de Firewall tiene como objetivo agregar, durante 1 minuto, a la lista auxiliar 1 las direcciones IP de origen de los paquetes.

Las configuraciones son similares a las de la cuarta regla de firewall. Los parámetros que cambian son los siguientes: (Src. Address List: vacío), (Address List: Con1SSH).

Firewall para el router

Para la protección del router, Mikrotik recomienda agregar las siguientes reglas de Firewall:

La primera regla tiene como objetivo aceptar (Action: accept) los paquetes, dirigidos al router (Chain: input), relacionados o que pertenezcan directamente a conexiones ya establecidas (Connection State: established, related). Estos paquetes ya no pasaran por las siguientes reglas, ayudando a reducir la carga del router (Mikrotik, Manual:Securing Your Router, s.f.).

La segunda regla tiene como objetivo aceptar (Action: accept) los paquetes, dirigidos al router (Chain: input), cuyas direcciones IP de origen pertenezcan a una lista de direcciones permitidas (Src. Address List: AllowedIP). Estas direcciones IP deben corresponder a los equipos de las personas que tienen autorización para acceder al router (Mikrotik, Manual:Securing Your Router, s.f.).

En la figura 4.53 se puede verificar que, en la ventana Firewall y la pestaña Address Lists, se puede crear una lista de direcciones IP.

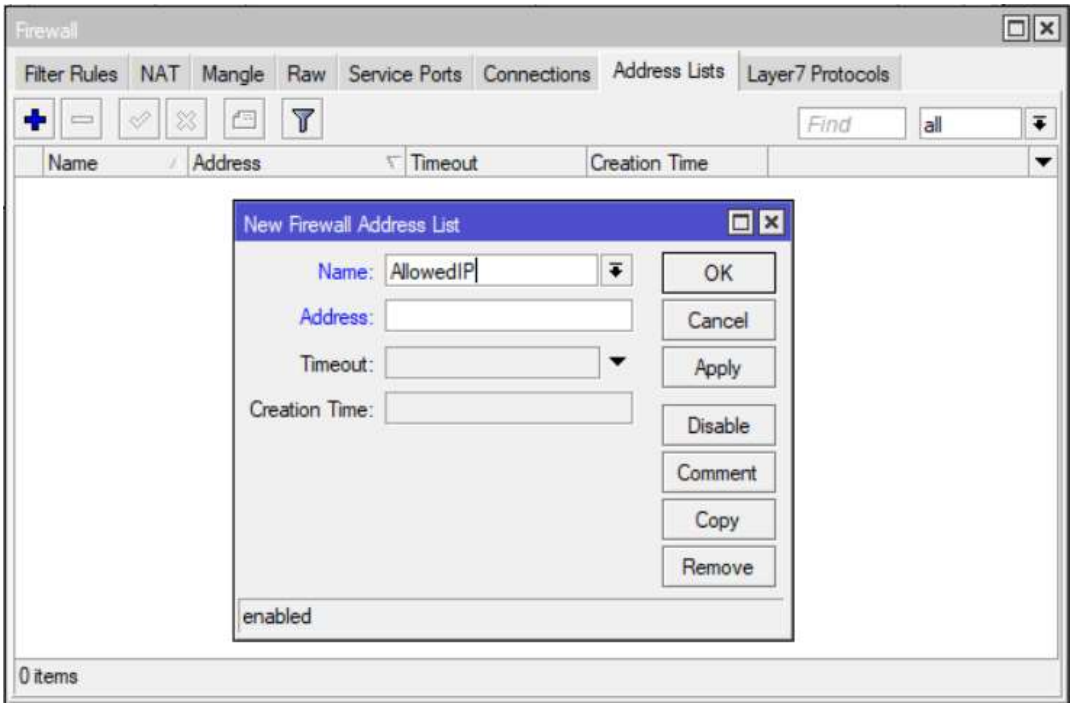


Figura 4.53: Creación de listas de direcciones IP.

La tercera regla tiene como objetivo aceptar (Action: accept) los paquetes, dirigidos al router (Chain: input), que pertenezcan al protocolo ICMP (Protocol: icmp) (Mikrotik, Manual:Securing Your Router, s.f.).

La cuarta regla tiene como objetivo descartar todo paquete (Action: drop), dirigido al router (Chain: input), que no haya cumplido con ninguna de las reglas anteriores (Mikrotik, Manual:Securing Your Router, s.f.).

Limitar el número de nuevas conexiones sucesivas en el router

Mikrotik establece que no hay solución perfecta contra ataques DoS (Denial of Service), sin embargo, existen maneras de mitigarlos. Se recomienda limitar el número de nuevas conexiones sucesivas solicitadas por una misma dirección IP (Mikrotik, DoS attack protection, s.f.).

El objetivo de esta política de seguridad es establecer un límite de solicitudes de conexión (paquete SYN) sucesivas. En el caso de que el router reciba una gran cantidad de paquetes SYN que supere el límite, la dirección IP de origen se agregará a una lista

de bloqueo. Los paquetes provenientes de direcciones IP de esta lista, serán descartados (Mikrotik, DoS attack protection, s.f.) (Mikrotik, Manual:IP/Firewall/Filter, s.f.).

Se necesitarán 2 reglas de Firewall.

La primera regla de Firewall tiene como objetivo descartar los paquetes provenientes de las direcciones IP que se han agregado a la lista de bloqueo (Mikrotik, DoS attack protection, s.f.) (Mikrotik, Manual:IP/Firewall/Filter, s.f.).

En la figura 4.54 se encuentran las configuraciones realizadas en la pestaña General, las cuales establecen que los paquetes entrantes deben estar dirigidos a un equipo conectado al router (Chain: forward).

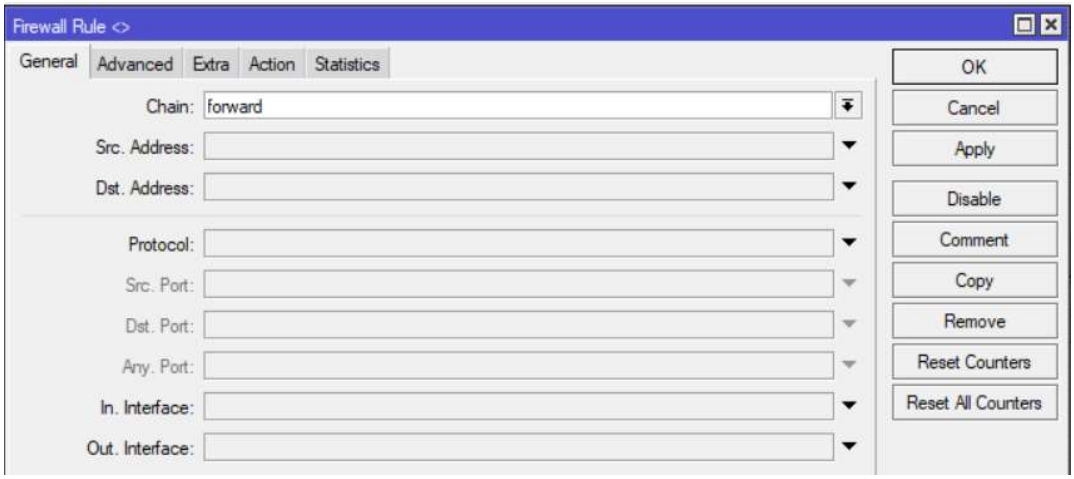


Figura 4.54: Configuraciones en la pestaña General.

Como se puede ver en la figura 4.55, las configuraciones realizadas en la pestaña Advanced establecen que las direcciones IP de origen deben estar en la lista SynFlooder (Src. Address List: SynFlooder).

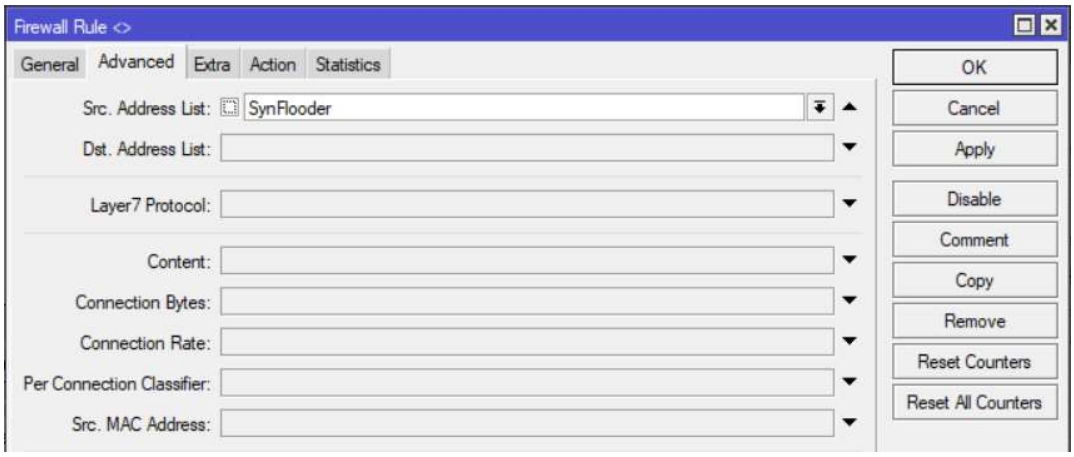


Figura 4.55: Configuraciones en la pestaña Advanced.

En la figura 4.56 se pueden observar las configuraciones realizadas en la pestaña Action, las cuales establecen que los paquetes, que cumplieron con los parámetros de las figuras anteriores, se descarten (Action: drop).

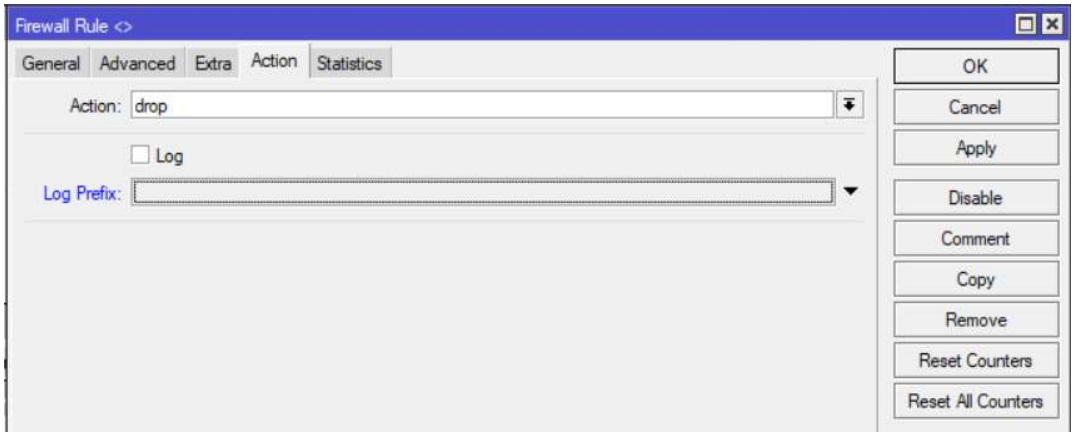


Figura 4.56: Configuraciones en la pestaña Action.

La segunda regla de Firewall tiene como objetivo realizar un filtrado para determinar si los paquetes son TCP, corresponden a una nueva conexión, si provienen de una misma dirección IP y si el número de paquetes recibidos de forma consecutiva está dentro del límite. En el caso de que se supere el límite, la dirección IP de origen se agrega a una lista de bloqueo (Mikrotik, DoS attack protection, s.f.) (Mikrotik, Manual:IP/Firewall/Filter, s.f.).

Como se puede ver en la figura 4.57, las configuraciones realizadas en la pestaña General establecen que los paquetes entrantes deben estar dirigidos a un equipo conectado al router (Chain: forward), el protocolo debe ser TCP (Protocol: 6(tcp)) y la conexión debe ser nueva (Connection State: new).

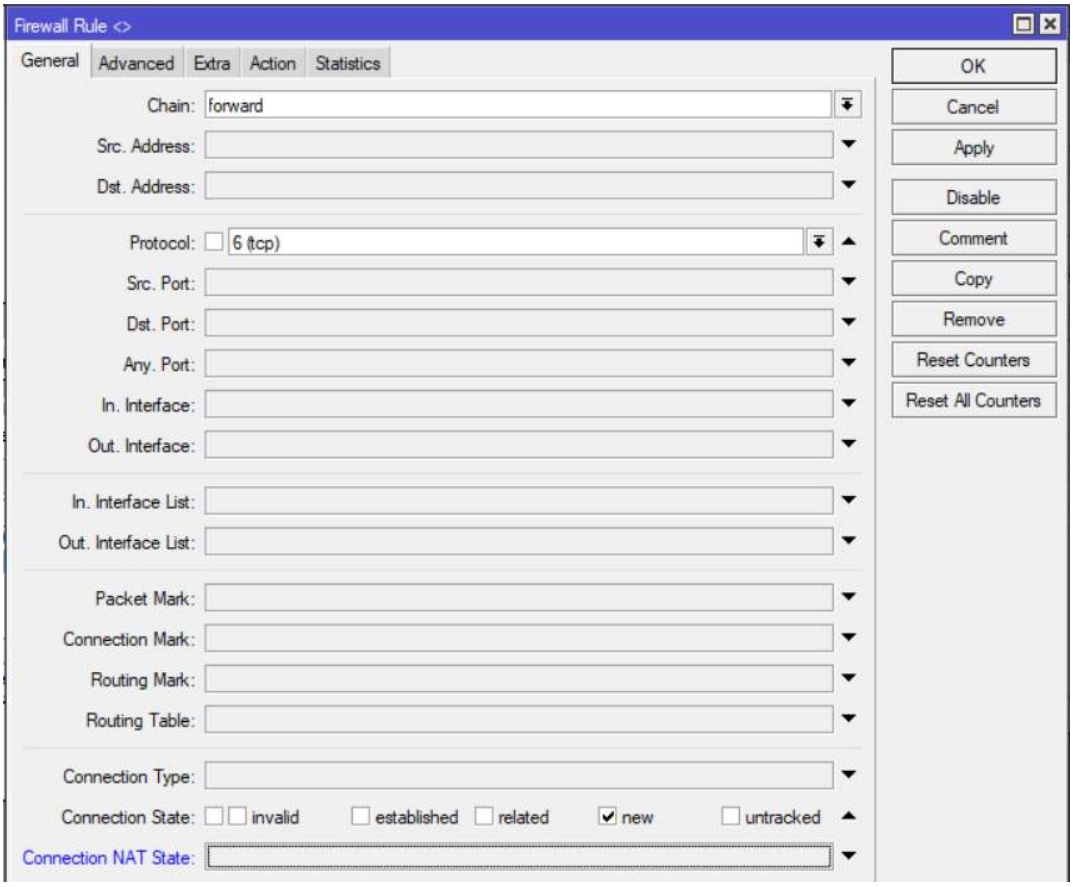


Figura 4.57: Configuraciones en la pestaña General.

En la figura 4.58 se encuentran las configuraciones realizadas en la pestaña Extra, las cuales establecen que el límite de paquetes SYN por IP es de 150 [Connection Limit (Limit: 150 Netmask: 32)].

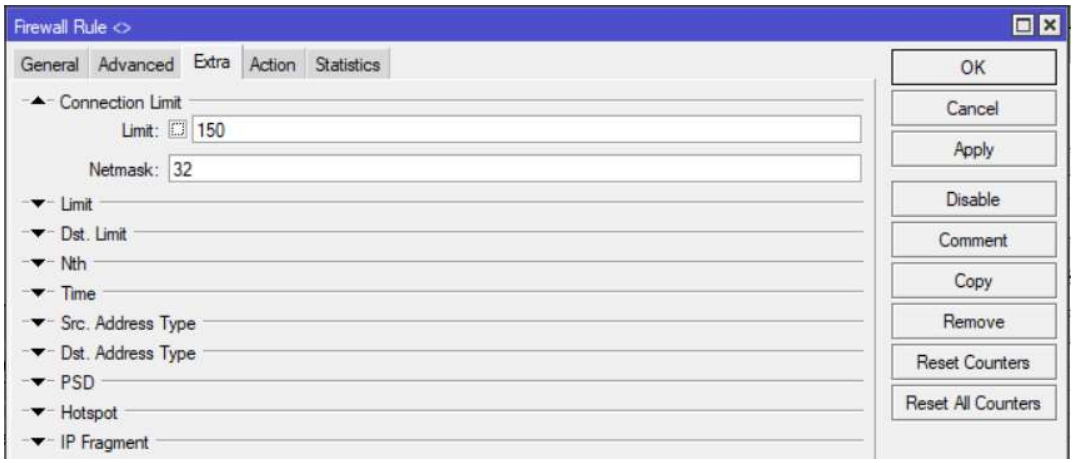


Figura 4.58: Configuraciones en la pestaña Extra.

En la figura 4.59 se pueden observar las configuraciones realizadas en la pestaña Action, estas establecen que, si se superó el límite, la dirección IP de origen se agregará (Action: add src to address list) a la lista de bloqueo SynFlooder (Address List: SynFlooder) durante 1 día (Timeout: 1d 00:00:00).

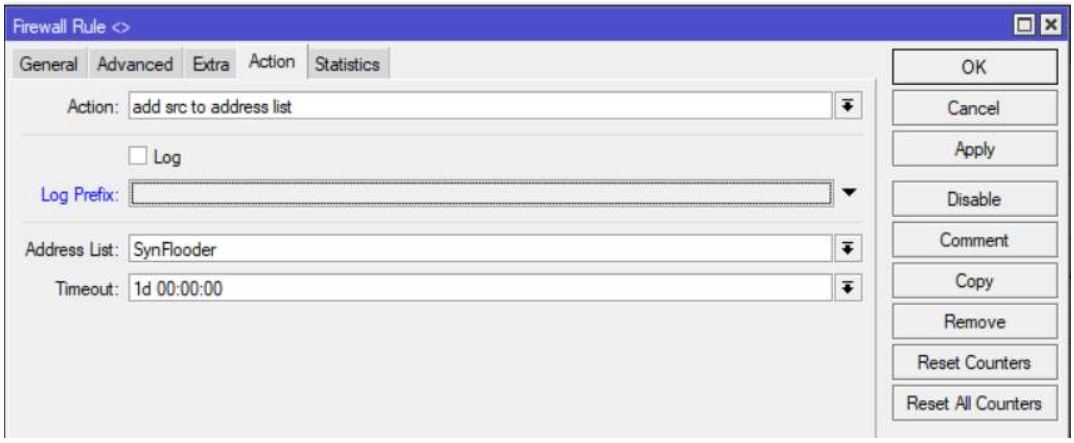


Figura 4.59: Configuraciones en la pestaña Action.

Estas configuraciones protegen a equipos conectados al router. Para protección de ataques dirigidos al router se debe cambiar únicamente (Chain: forward) por (Chain: input).

Reverse Path Forwarding

En RFC 3704 se recomienda el uso de Reverse Path Forwarding para limitar el impacto del uso de SPOOFING en ataques DDos, obtención de acceso a equipos de red, etc. (Baker, Cisco Systems, & Savola, 204)

Es una herramienta que permite evitar que el tráfico tome una ruta de salida diferente a la ruta que tomó para el ingreso. Si la entidad 1 intenta comunicarse con la entidad 2, a través de la interfaz 1, la respuesta deberá realizarse a través de la misma interfaz, caso contrario no se permitirá la conexión (Hat, s.f.).

Esta herramienta dispone de 2 modos, que son los siguientes:

- Strict: La dirección IP de origen se busca en la FIB (Forwarding Information Base), la cual es una tabla que contiene información para realizar el reenvío de paquetes, y se comprueba que el paquete ingrese por la interfaz que se utilizaría para responder a la IP en cuestión (Baker, Cisco Systems, & Savola, 204) (Trotter & Agilent Technologies, 2001).
- Loose: Se busca si existe una ruta, mas no se considera la dirección a la cual apunta la ruta. Se recomienda utilizar este modo para routing asimétrico, el cual se refiere a que el envío y respuesta de paquetes se dan por diferentes rutas. (Baker, Cisco Systems, & Savola, 204).

Para habilitar Reverse Path Forwarding, en un router Mikrotik, se debe acceder a IP/Settings y realizar la configuración (RP Filter: strict), como se puede ver en la figura 4.60.

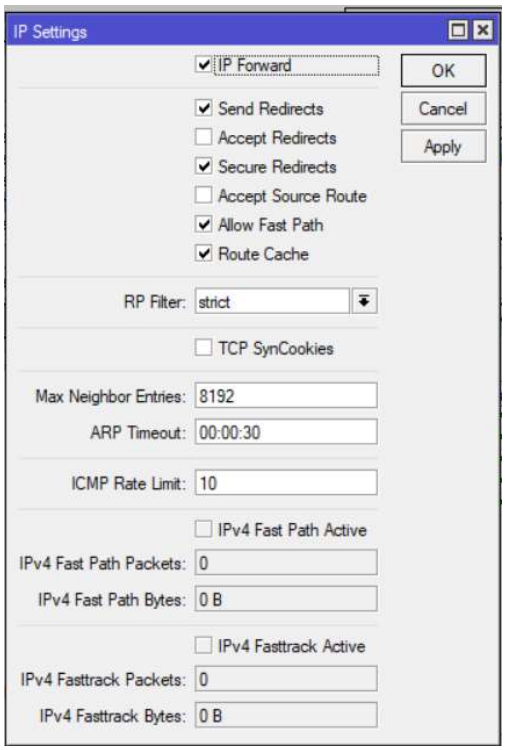


Figura 4.60: Ventana IP Settings.

PSD (Port Scan Detection)

Es una técnica que permite detectar un escaneo de puertos al descubrir anomalías en los paquetes TCP. Se analizan los números de puertos y las banderas de los paquetes (Rong-sheng, Xiao-yong, & LI, 2004).

Para utilizar esta técnica se deben configurar los siguientes parámetros (Mikrotik, Manual:IP/Firewall/Filter, s.f.):

- Weight Threshold: Máximo valor de la suma total de pesos de los paquetes TCP/UDP con diferente puerto de destino y provenientes de la misma dirección IP.
- Delay Threshold: Tiempo en el que se obtiene la suma total de pesos de los paquetes TCP/UDP con diferente puerto de destino y provenientes de la misma dirección IP.
- Low Port Weight: Peso que se le asigna al rango de puertos bien conocidos.

- High Port Weight: Peso que se asigna al rango restante de puertos.

Durante un periodo de tiempo (Delay Threshold) se van a recibir paquetes TCP. Por cada paquete que llegue al equipo, se incrementará un contador (el valor a incrementar sería de Low Port Weight para puertos de destino menores a 1024 y High Port Weight para puertos de destino desde 1024 en adelante). Al final, si el contador supera al valor de Weight Threshold, se procederá a ejecutar una acción, la cual podría ser: agregar la dirección IP de origen a una lista de bloqueo y descartar los paquetes que se originen de la misma (Mikrotik, Manual:IP/Firewall/Filter, s.f.).

Se necesitarán 4 reglas de Firewall.

En las dos primeras reglas de firewall se establece que se descartará todo paquete proveniente de una dirección IP de la lista Port Scanner (Mikrotik, Drop port scanners, s.f.). La primera regla se encargará de los escaneos dirigidos a través del router y la segunda se encargará de los dirigidos al router.

Como se puede ver en la figura 4.61, las configuraciones de la pestaña General establecen que los paquetes entrantes deben estar dirigidos a un equipo conectado al router (Chain: forward).

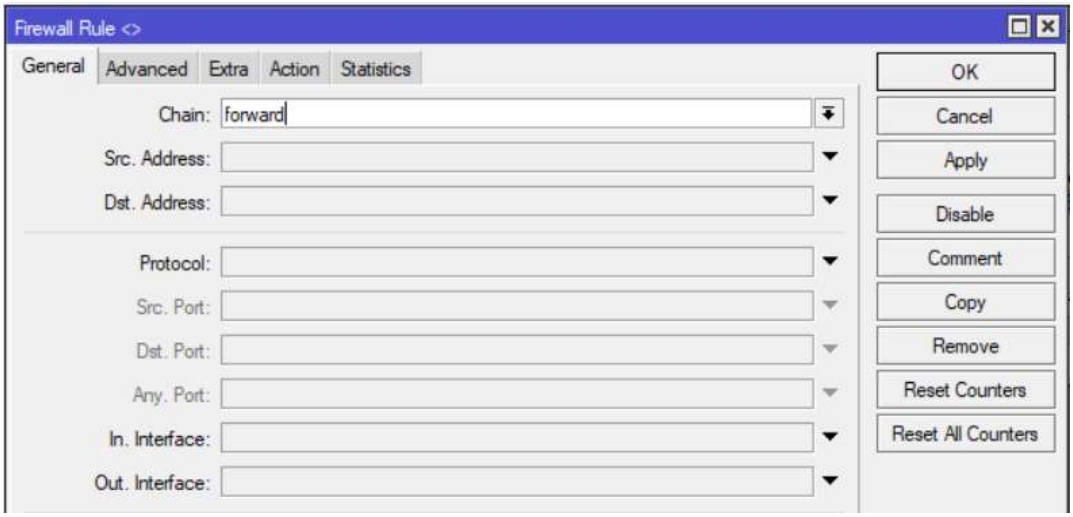


Figura 4.61: Configuraciones en la pestaña General.

En la figura 4.62 se encuentran las configuraciones de la pestaña Advanced, las cuales establecen que las direcciones IP de origen deben estar en la lista Port Scanner (Src. Address List: Port Scanner).

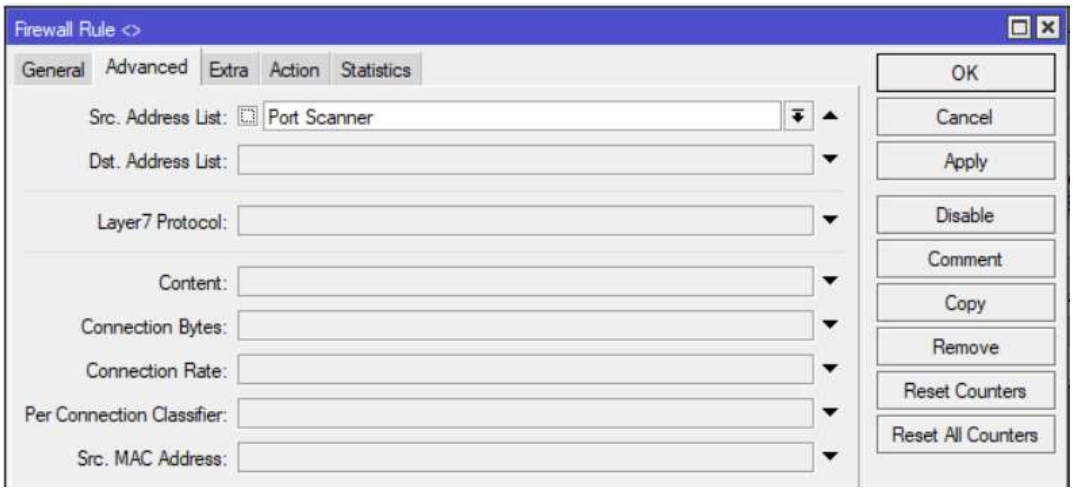


Figura 4.62: Configuraciones en la pestaña Advanced.

En la figura 4.63 se visualizan las configuraciones de la pestaña Action, las cuales establecen que los paquetes, que cumplieron con los parámetros de las figuras anteriores, se descarten (Action: drop).

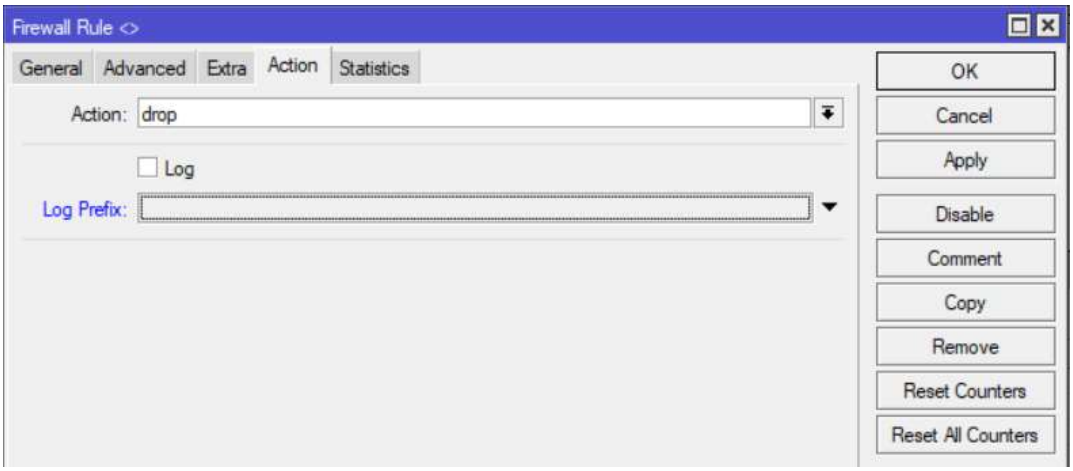


Figura 4.63: Configuraciones en la pestaña Action.

La segunda regla es similar a la primera. Solo se cambia (Chain: forward) por (Chain: input).

En la tercera y cuarta regla de Firewall se configura PSD y se agrega la dirección IP de origen a una lista de bloqueo durante 1 día (Mikrotik, Drop port scanners, s.f.). La

tercera regla se encargará de los escaneos dirigidos a través del router y la cuarta se encargará de los dirigidos al router.

Como se puede ver en la figura 4.64, las configuraciones realizadas en la pestaña General establecen que los paquetes entrantes deben estar dirigidos a un equipo conectado al router (Chain: forward) y el protocolo debe ser TCP (Protocol: 6(tcp)).

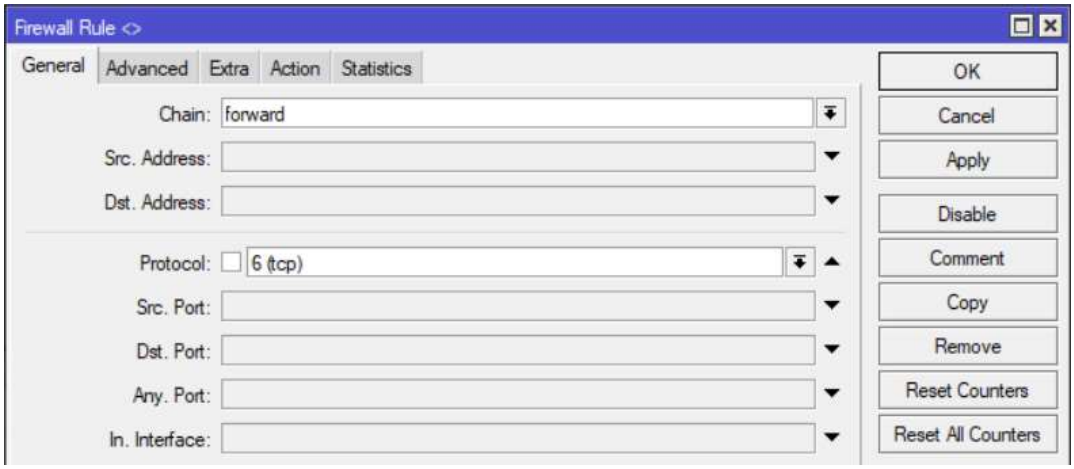


Figura 4.64: Configuraciones en la pestaña General.

En la figura 4.65 se muestran las configuraciones de PSD en la pestaña Extra. Se asignan los siguientes valores: (Weight Threshold: 12), (Delay Threshold: 00:00:03), (Low Port Weight: 4) y (High Port Weight: 1).

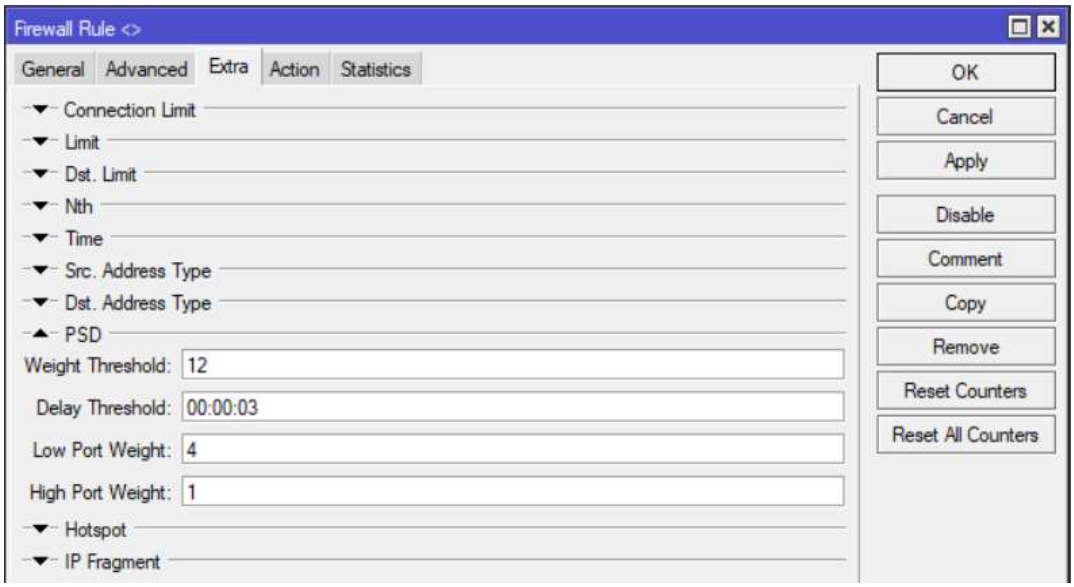


Figura 4.65: Configuraciones en la pestaña Extra.

Como se puede notar en la figura 4.66, las configuraciones de la pestaña Action establecen que la dirección IP de origen se agregará (Action: add src to address list) a la lista de bloqueo Port Scanner (Address List: Port Scanner) durante 1 día (Timeout: 1d 00:00:00).

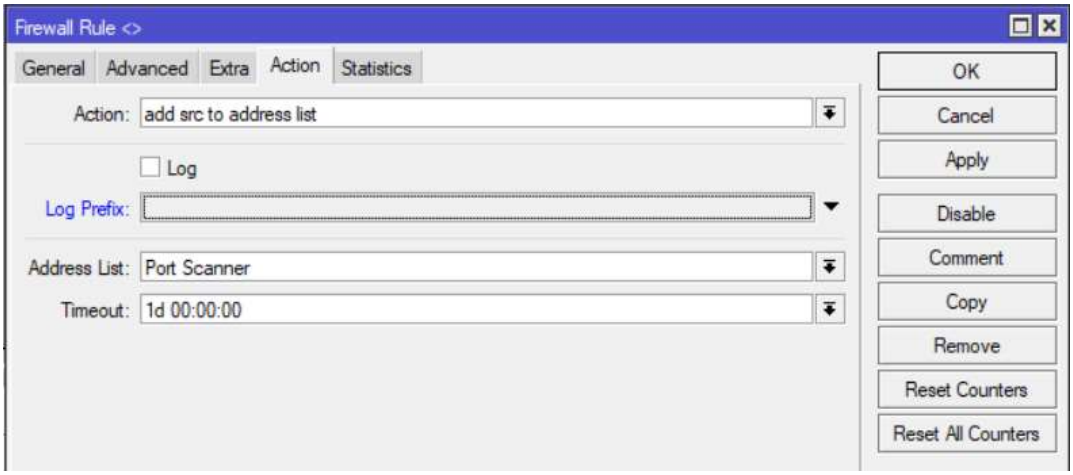


Figura 4.66: Configuraciones en la pestaña Action.

La cuarta regla es similar a la tercera. Solo se cambia (Chain: forward) por (Chain: input).

4.3. Seguridad de capa 2

4.3.1. Topología

En la figura 4.67 se encuentra la primera topología de la red en la que se realizarán pruebas. Se utilizará el switch Mikrotik RB260GSP.

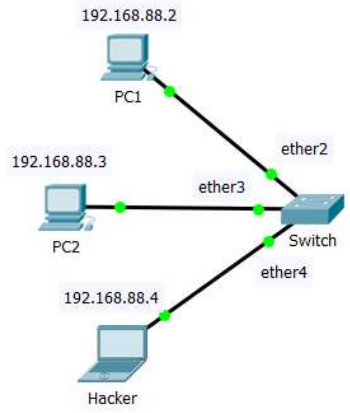


Figura 4.67: Topología N° 1 de la red de pruebas.

En la figura 4.68 se puede observar la segunda topología de la red en la que se realizarán pruebas. Para el switch 1, 2 y 3, se utilizará el router Mikrotik hAP LITE TC (RB941-2Nd-TC) configurado como bridge.

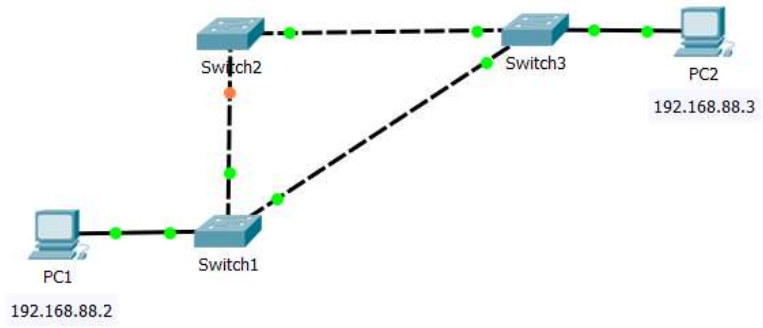


Figura 4.68: Topología N° 2 de la red de pruebas.

En la figura 4.69 se encuentra la tercera topología de la red en la que se realizarán pruebas. Para el switch 1, 2 y 3, se utilizará el router Mikrotik hAP LITE TC (RB941-2Nd-TC) configurado como bridge y para el switch 4 se utilizará el switch Mikrotik RB260GSP.

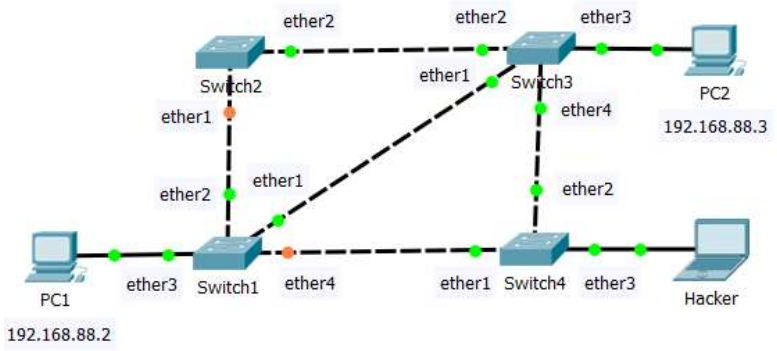


Figura 4.69: Topología N° 3 de la red de pruebas.

En la figura 4.70 se puede ver la cuarta topología de la red en la que se realizarán pruebas. Para el switch 1 y 2 se utilizará el switch Mikrotik RB260GSP.

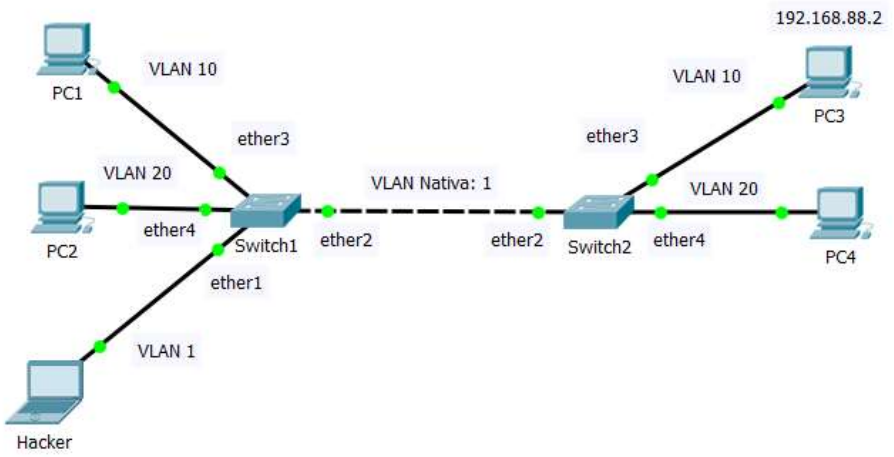


Figura 4.70: Topología N° 4 de la red de pruebas.

4.3.2. Pruebas en la red vulnerable

Falsificación de direcciones MAC

Los switches tienen un proceso de aprendizaje que utilizan para llenar la tabla de direcciones MAC. Cuando el switch recibe una trama, coloca, en la tabla, el puerto por el cual la recibió y la dirección MAC del dispositivo que la envió. Si un atacante envía una trama, en la que cambia su dirección MAC por la de un host legítimo de la red, el switch sobrescribirá la información de la tabla de direcciones MAC y ahora la información destinada al host legítimo, se enviará por el puerto al que está conectado el atacante (Ariganello, 2014).

Existe macchanger, la cual es una herramienta que permite modificar la dirección MAC de un host (Rendek, 2017).

Para las pruebas se utilizará la topología de la figura 4.67.

En la figura 4.71 se puede comprobar que, en la tabla de direcciones MAC, se han registrado los 2 hosts legítimos.

Port	MAC
Port2	f4:
Port3	d8:

Figura 4.71: Tabla de direcciones MAC.

En la figura 4.72 se pueden examinar los comandos ejecutados para cambiar la dirección MAC del host del atacante (-m) en la interfaz *ethernet* (eth0). La nueva dirección MAC pertenece a la PC1.

Se debe apagar la interfaz *ethernet* del host antes de cambiar la dirección MAC y se debe encender después del cambio.

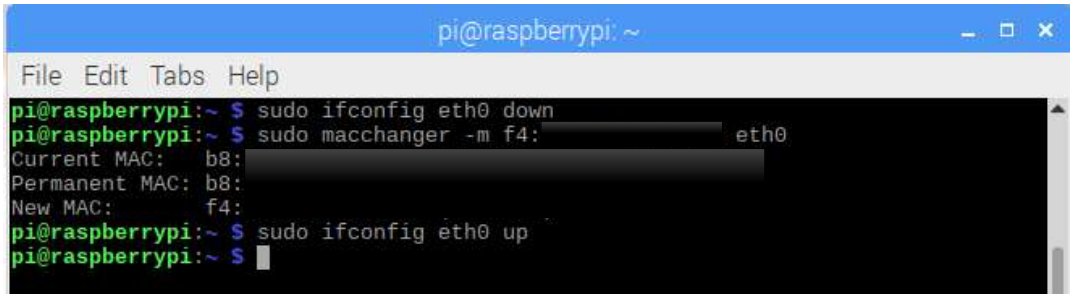


Figura 4.72: Cambio de dirección MAC en el host del atacante.

Se conecta el host del atacante al switch y se realiza ping a la PC2 para que se sobrescriba la información en la tabla de direcciones MAC.

En la figura 4.73 se puede verificar que, en la tabla de direcciones MAC, se sustituyó el puerto 2, que corresponde a la PC1, por el puerto 4 que corresponde al atacante.

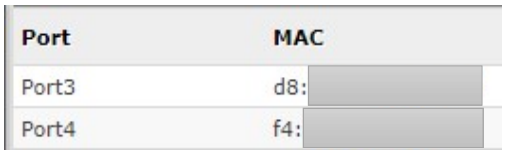


Figura 4.73: Cambio de puerto en la tabla de direcciones MAC.

Desde la PC2 se realiza ping a la PC1.

En el host del atacante se realiza la captura de paquetes mediante Wireshark y se comprueba, en la figura 4.74, que se reciben algunos paquetes correspondientes al ping que estaba dirigido hacia la PC1.

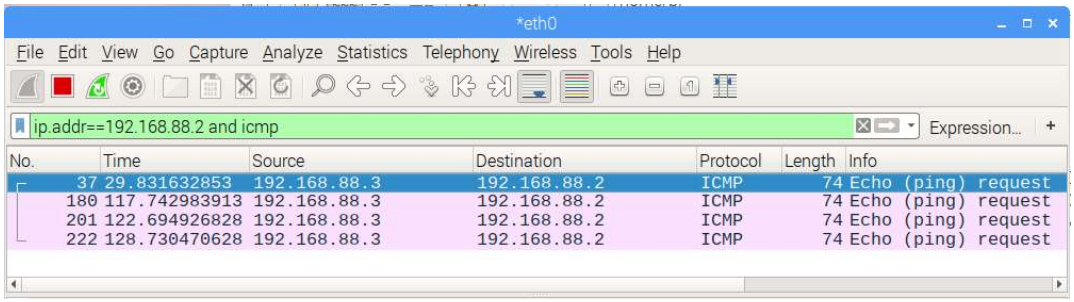


Figura 4.74: Recepción de paquetes dirigidos a la PC1.

Tormenta de LAN

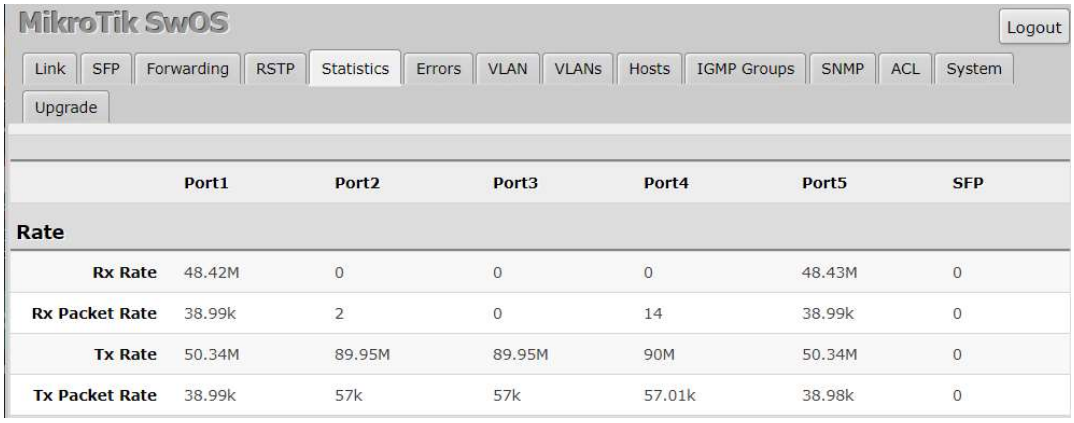
"Este tipo de ataque se da cuando se crea un exceso de tráfico en la red LAN y se degrada el desempeño de la misma. Se puede producir por errores en la configuración de la red, por tormentas de broadcast, por ataques DoS (Denial of Service), etc." (Ariganello, 2014).

"Una tormenta de broadcast se produce cuando existen tantas tramas de broadcast, atrapadas en un bucle de capa 2, que se consume todo el ancho de banda disponible" (CISCO, CCNA 3: Scaling Networks).

Para este ataque se utilizará la topología de la figura 4.67.

Para la primera prueba se realizará un bucle en el switch, conectando el puerto 1 y el puerto 5 con el mismo cable. Esto provocará una tormenta de broadcast.

En la figura 4.75 se puede notar que, en la pestaña Statistics, las tasas de transmisión y recepción de los puertos suben de forma excesiva.



	Port1	Port2	Port3	Port4	Port5	SFP
Rate						
Rx Rate	48.42M	0	0	0	48.43M	0
Rx Packet Rate	38.99k	2	0	14	38.99k	0
Tx Rate	50.34M	89.95M	89.95M	90M	50.34M	0
Tx Packet Rate	38.99k	57k	57k	57.01k	38.98k	0

Figura 4.75: Tasas de transmisión y recepción de los puertos.

En la figura 4.76 se comprueba que no puede comunicarse la PC2 con la PC1.

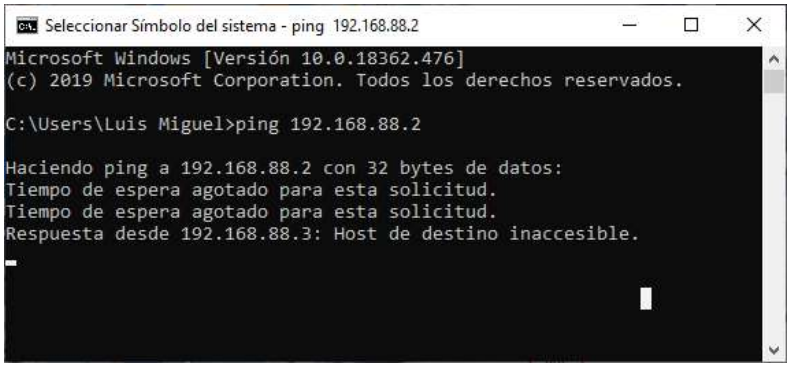


Figura 4.76: Intento de comunicación entre la PC2 y la PC1.

Manipulación STP

Cuando se analizan los identificadores de puente, para determinar el switch que será puente raíz, se le da mayor importancia al valor de prioridad. En caso de que todos los switches tengan el mismo valor de prioridad, se analiza la dirección MAC (CISCO, CCNA 3: Scaling Networks).

Este ataque se realiza en una red redundante en la que se utilice STP o RSTP. Consiste en conectar, entre 2 switches, un switch adicional que tenga configurado este protocolo y al que se le haya asignado la prioridad más baja posible. Este nuevo switch se convertirá en el nuevo puente raíz. Esto significa que todo el tráfico pasará por el nuevo switch y el atacante, conectado a una de sus interfaces, puede utilizar Port Mirroring para obtener una copia de todo el tráfico que pasa por el switch (Ariganello, 2014).

En la topología de la figura 4.68 se puede observar la red redundante sobre la cual se realizará el ataque.

El puente raíz es el switch 3.

En la topología de la figura 4.69 se puede observar la red modificada con la conexión del nuevo switch del atacante (switch 4).

En la figura 4.77 se puede observar que, en la pestaña RSTP del switch del atacante, se asigna la prioridad más baja posible (Bridge Priority (hex): 0000) para asegurar que el switch sea el puente raíz.

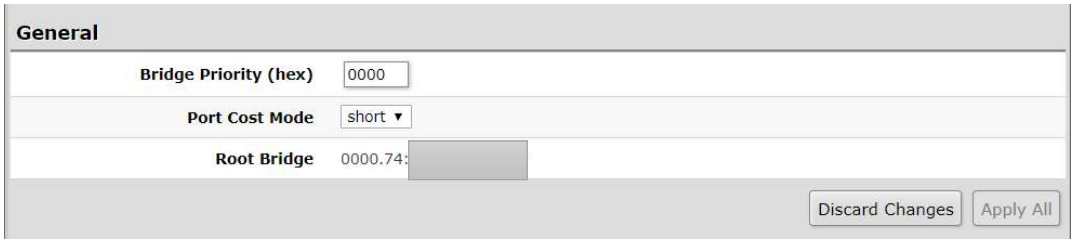


Figura 4.77: Configuración de prioridad en el switch del atacante.

En la figura 4.78 se puede ver que, en la pestaña Forwarding, se configura Port Mirroring de forma que se envíe al puerto 3 (Mirror To) una copia de todo el tráfico que ingrese al switch por los puertos 1 y 2 (Mirror Ingress:).

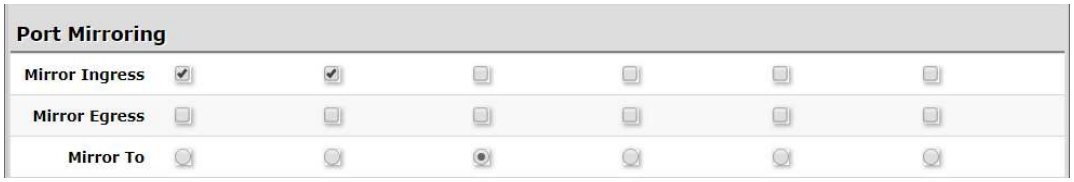


Figura 4.78: Configuración de Port Mirroring.

En la figura 4.79 se encuentra la ventana Bridge y la pestaña Bridge. En esta última se puede ingresar a las configuraciones del switch 3. En la pestaña Status se puede observar que se identifica como puente raíz al switch de prioridad 0000 (Root Bridge ID), el cual corresponde al atacante.

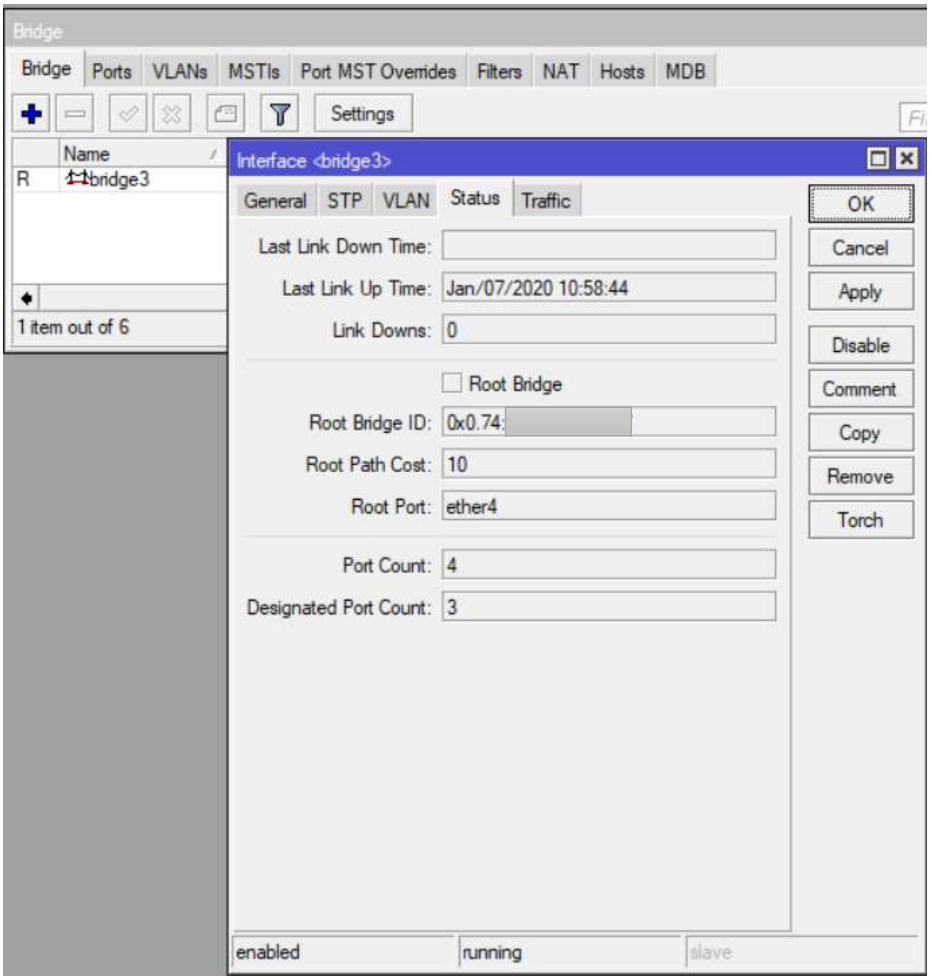


Figura 4.79: Pestaña Status del switch 3.

Se realiza ping de la PC1 a la PC2.

En la figura 4.80, utilizando Wireshark, el atacante puede ver el tráfico generado entre la PC1 y la PC2.

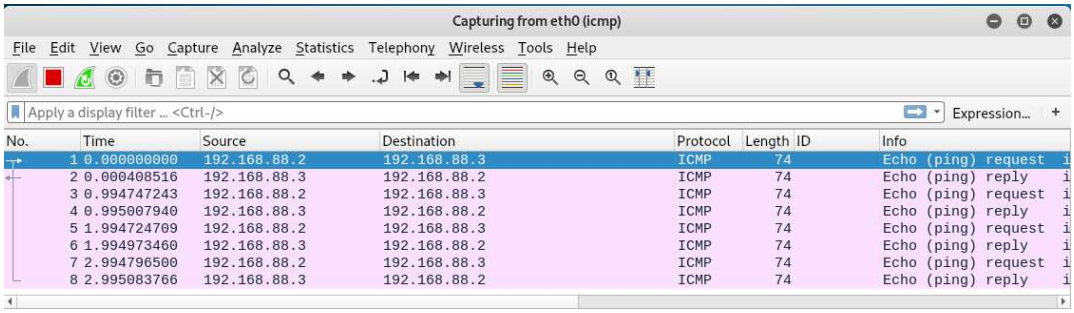


Figura 4.80: Visualización de tráfico en la computadora del atacante.

VLAN hopping

Cuando se van a utilizar VLANs en un switch, es muy común que se configuren los puertos de acceso, que se van a utilizar, con sus respectivas VLANs, los puertos troncales y se mantenga el resto de configuraciones por defecto. Los puertos de enlace troncal se mantendrán en la VLAN 1 (VLAN nativa) al igual que los puertos de acceso que no se han utilizado.

Las tramas que se envían desde la VLAN nativa no se etiquetan. Si el switch recibe una trama etiquetada, proveniente de un puerto de la VLAN nativa, retira la etiqueta para enviar la trama por el enlace troncal. Si se agregan dos etiquetas, el switch solamente quitará una de ellas y la trama pasará por el enlace troncal con la segunda etiqueta intacta. Si en el otro extremo del enlace troncal se encuentra un segundo switch, este recibirá la trama y la enviará a la VLAN especificada en la segunda etiqueta. Con este método se puede comunicar de forma unidireccional a cualquier VLAN de la red (CISCO, CCNA 2: Routing and Switching Essentials).

Las pruebas se realizarán con la topología de la figura 4.70.

Para realizar el proceso de doble etiquetado se utilizará Yersinia, la cual es una herramienta que permite realizar ataques de capa 2. Está diseñada para aprovechar las vulnerabilidades que pueden presentar algunos protocolos (Kali, Yersinia Package Description, s.f.).

El atacante está conectado en un puerto de la VLAN nativa.

Para iniciar Yersinia en Kali Linux, desde la computadora del atacante, se debe ejecutar el comando de la figura 4.81.

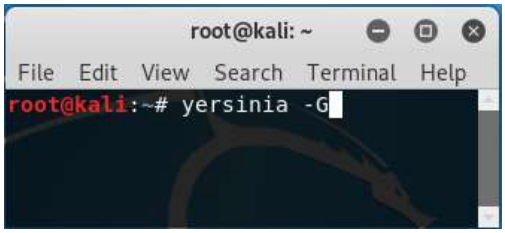


Figura 4.81: Comando para iniciar Yersinia.

En la figura 4.82 se encuentra la pestaña 802.1Q, en la cual se establecen los valores de VLAN para el doble etiquetado (VLAN: 1 y VLAN2: 10), una dirección IP de origen falsa (Src IP: 10.10.0.2) y la dirección IP de destino perteneciente a la PC3 de la VLAN 10 (Dst IP: 192.168.88.2).

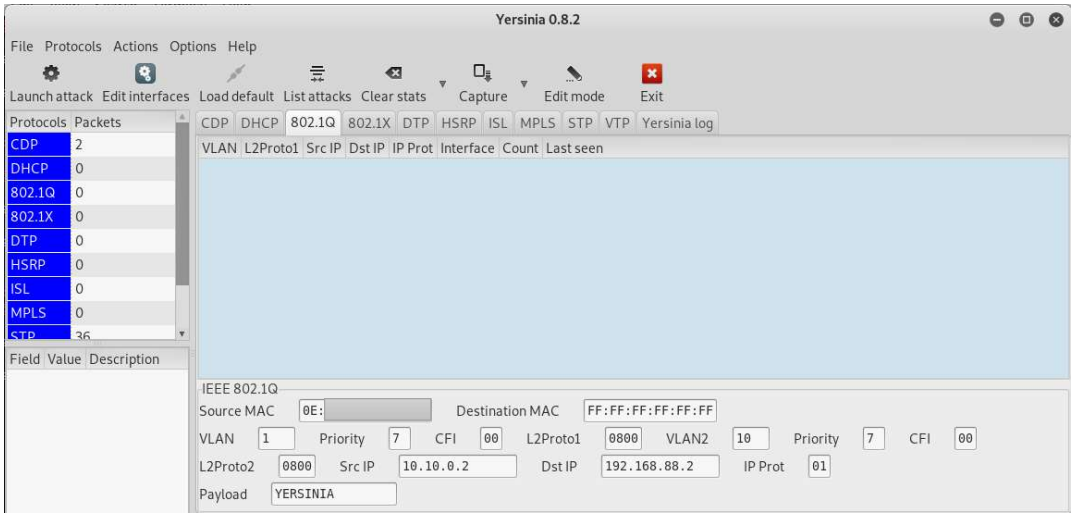


Figura 4.82: Configuración de parámetros en Yersinia.

Se presiona Launch attack, se abre la ventana de la figura 4.83 y se elige la opción sending 802.1Q double enc. packet.

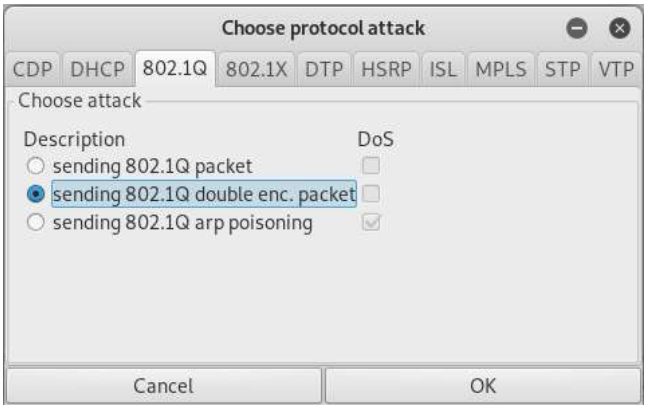


Figura 4.83: Configuración del tipo de ataque.

En la figura 4.84, utilizando Wireshark, se comprueba que la PC3, de la VLAN 10, recibió los datos enviados por el atacante.

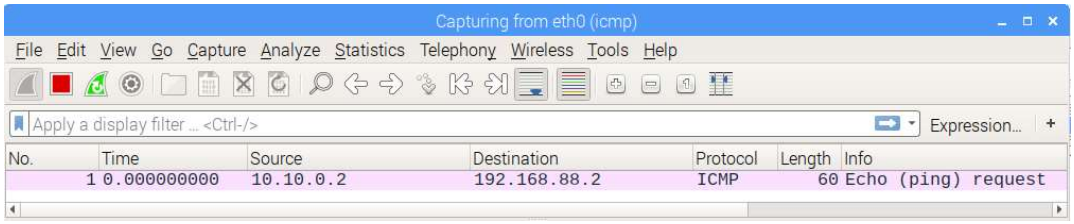


Figura 4.84: Captura de datos mediante Wireshark en la PC3.

4.3.3. Configuraciones de seguridad

Las configuraciones en el switch se deben realizar, mediante un navegador web, utilizando el servicio http.

Configuraciones básicas de seguridad en un switch

Se deben realizar ciertas configuraciones de seguridad básicas en un switch. Este tipo de configuraciones ya se trataron en la sección de seguridad en un router.

En las figuras 4.85 y 4.86 se puede observar que, en la pestaña System, se pueden realizar las siguientes configuraciones (Mikrotik, SwOS/CSS106, s.f.):

- Configurar una dirección IP al switch para el acceso al servicio de configuración (Static IP Address).

- Configurar las direcciones IP desde las cuales se puede acceder al servicio de configuración (Allow From).
- Configurar los puertos desde los cuales se puede acceder al servicio de configuración (Allow From Ports).
- Configurar la VLAN desde la cual se puede acceder al servicio de configuración (Allow From VLAN).
- Deshabilitar el servicio Mikrotik Discovery Protocol.
- Cambiar la contraseña por defecto (Usuario: admin y Contraseña: vacío).
- Respaldar la configuración del switch.

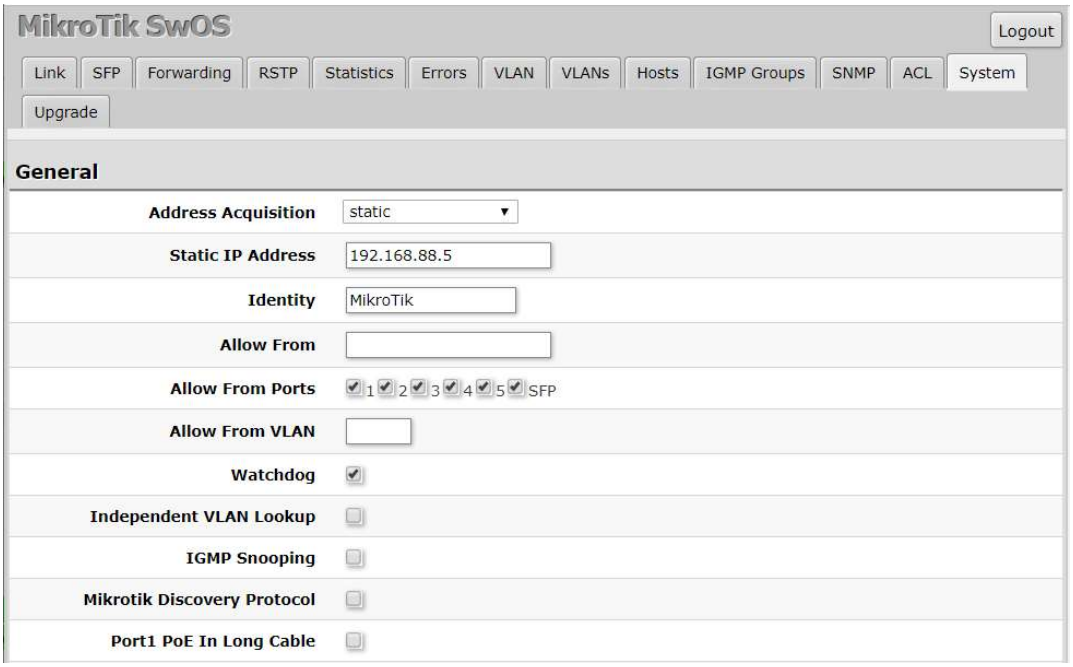


Figura 4.85: Configuraciones básicas de seguridad en el switch.

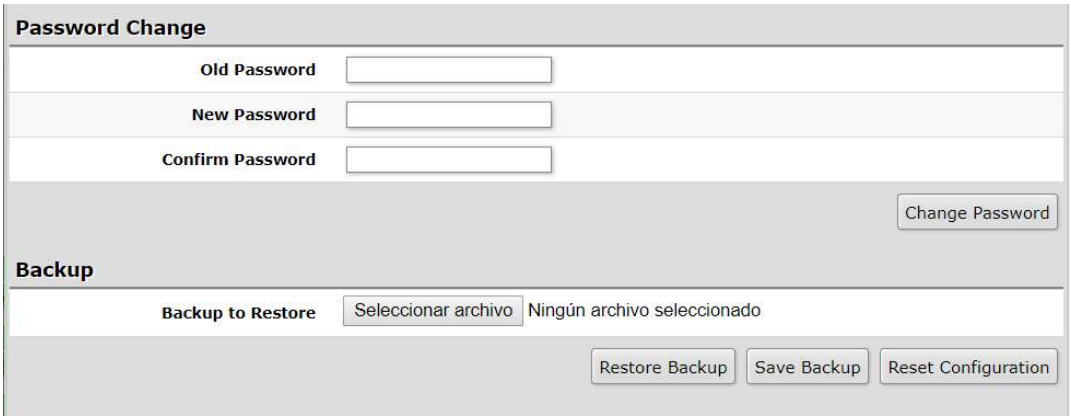


Figura 4.86: Configuraciones básicas de seguridad en el switch.

En la figura 4.87 se puede ver que, en la pestaña Link, se pueden desactivar los puertos que no se utilicen.

Figura 4.87: Configuración de puertos.

Como se puede observar en la figura 4.88, en la pestaña Upgrade se puede actualizar el firmware.

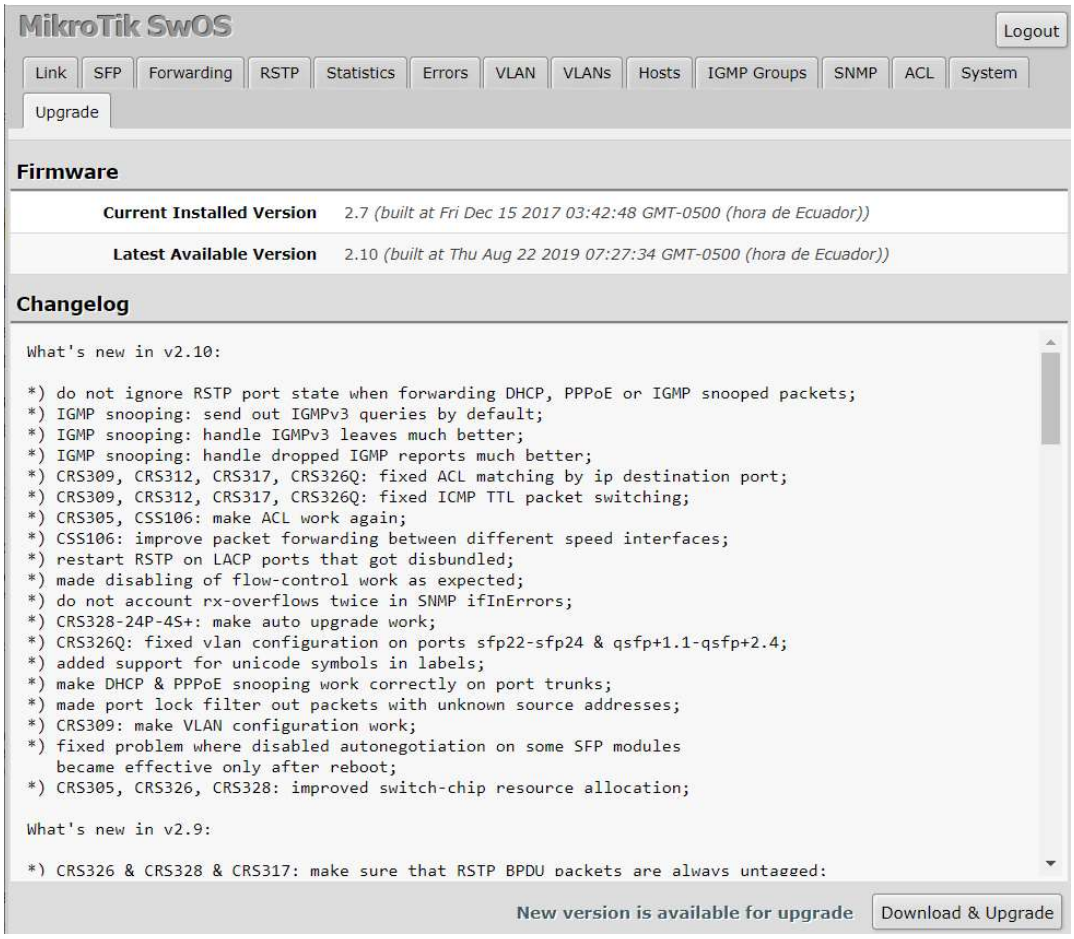


Figura 4.88: Actualización del firmware.

Se recomienda desactivar el servicio SNMP, si no se necesita utilizarlo, debido a que este modelo de switch solo soporta la versión 1, la cual no implementa seguridad (Mikrotik, SwOS/CSS106, s.f.).

En la figura 4.89 se encuentra la pestaña SNMP, desde la cual se puede desactivar este servicio.

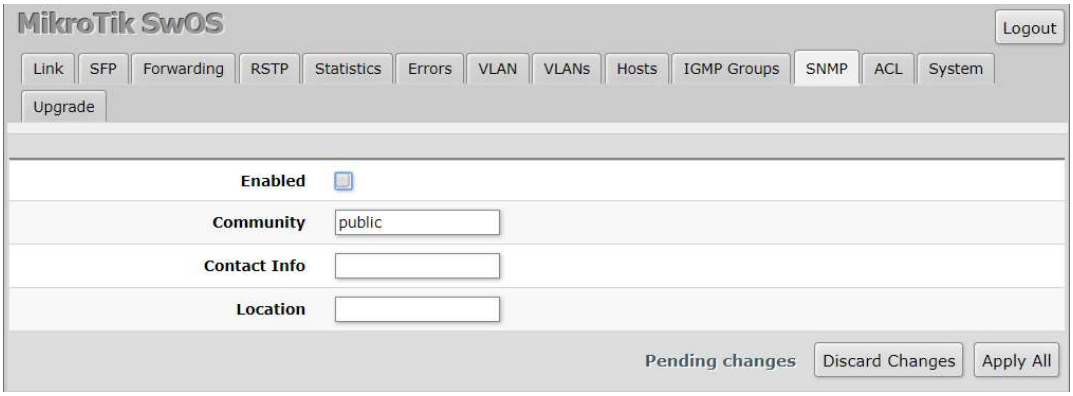


Figura 4.89: Desactivación del servicio SNMP.

Seguridad de puertos

La seguridad de puertos consiste en desactivar el proceso de aprendizaje y llenar de forma manual y estática la tabla de direcciones MAC del switch (Ariganello, 2014).

En la figura 4.90 se puede observar que, en la pestaña Forwarding, se encuentra la opción Port Lock. Se debe habilitar, en cada puerto, para desactivar el proceso de aprendizaje (Mikrotik, SwOS/CSS106, s.f.).

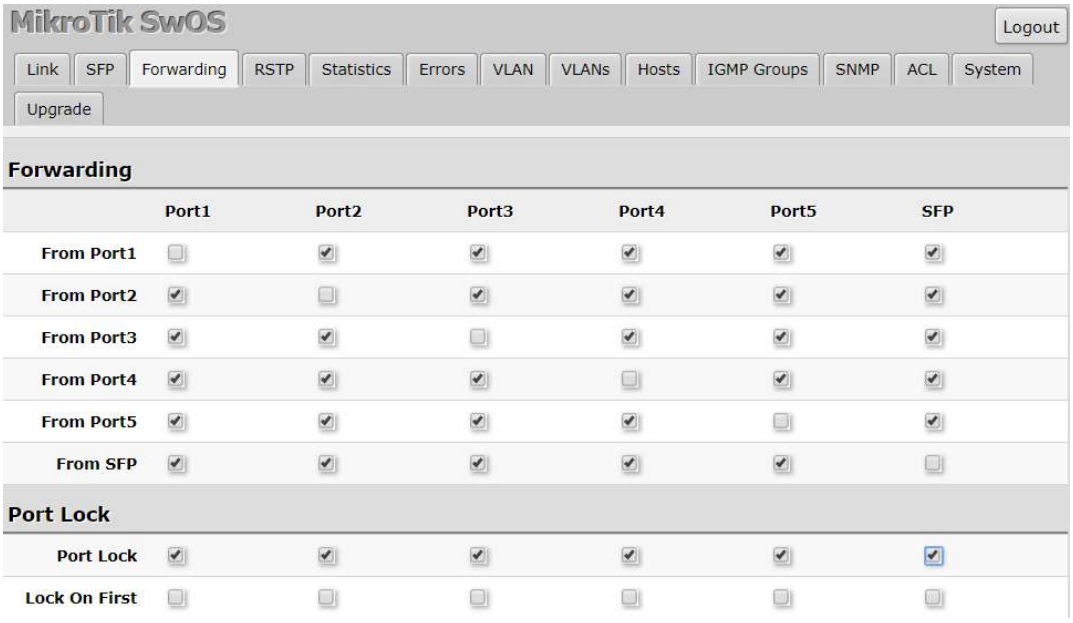


Figura 4.90: Desactivación del proceso de aprendizaje en los puertos del switch.

Como se puede ver en la figura 4.91, en la pestaña Hosts se puede asignar una dirección MAC a uno de los puertos del switch.

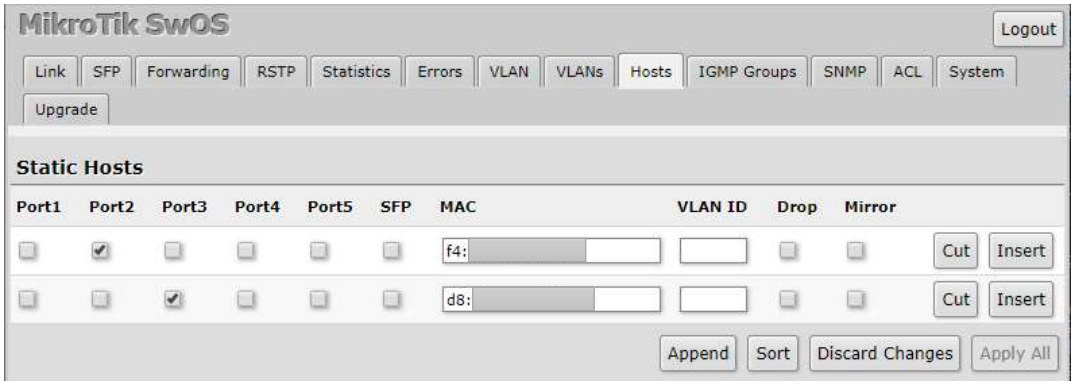


Figura 4.91: Configuración estática de la tabla de direcciones MAC.

Estas configuraciones se mantendrán incluso si el switch se reinicia.

STP o RSTP

Se debe configurar STP o RSTP en los puertos del switch para evitar que se formen bucles y que se generen tormentas de broadcast (CISCO, CCNA 3: Scaling Networks).

En la pestaña RSTP se puede habilitar este protocolo en cada puerto del switch, como se puede apreciar en la figura 4.92 (Mikrotik, SwOS/CSS106, s.f.).

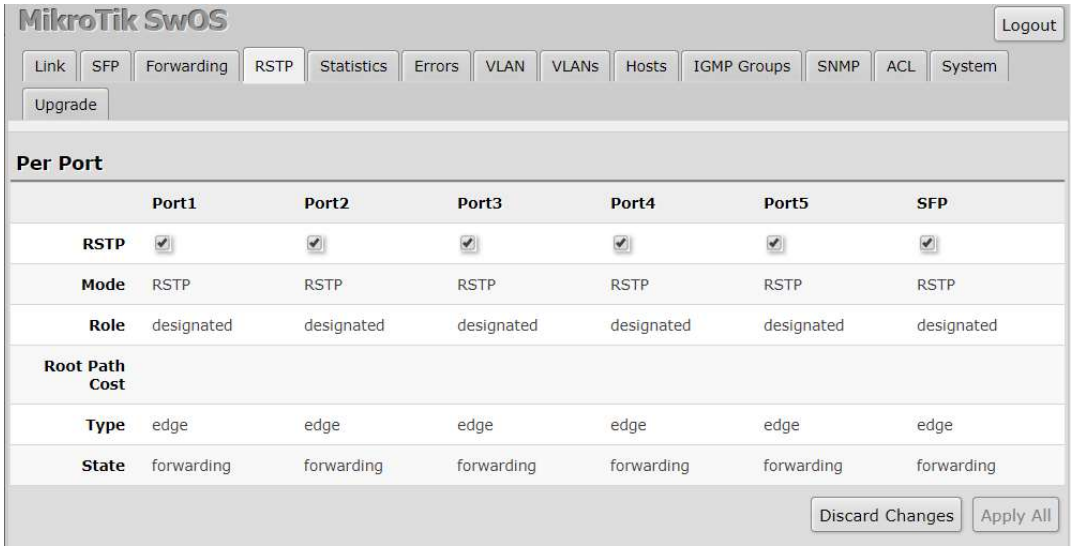


Figura 4.92: Configuración de RSTP en los puertos del switch.

Limitar el ancho de banda

Se puede limitar el ancho de banda en cada puerto para que no se puedan generar tasas de tráfico excesivas que consuman todos los recursos de la red.

ACL (Access Control List) es una herramienta que permite controlar el flujo de paquetes analizando valores como etiquetas VLAN, direcciones MAC, direcciones IP, interfaces del switch, etc. (Mikrotik, SwOS/CSS106, s.f.)

En la figura 4.93 se puede ver que, en la pestaña ACL, se limita, en el puerto 1 (From:), el ancho de banda de ingreso a 5 Mbps (Rate: 5 M).

Esta configuración también limitará el tráfico de broadcast.

Se recomienda repetir esta configuración para todos los puertos del switch de forma individual (Mikrotik, SwOS/CSS106, s.f.).

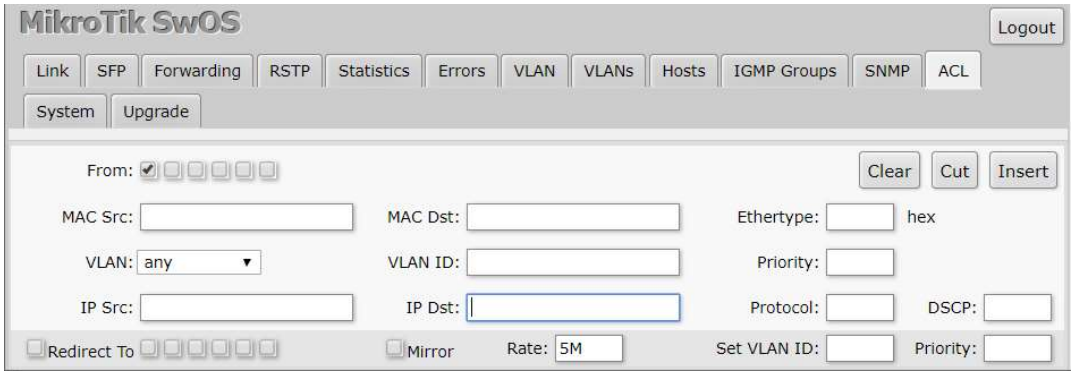


Figura 4.93: Configuración del límite de tasa de tráfico de ingreso en el puerto 1 del switch.

Seguridad en STP

El principio de funcionamiento, de este protocolo, se basa en la comunicación entre switches, por lo que los puertos que están destinados para hosts no deben recibir BPDUs.

BPDU Guard es una opción que desactiva el puerto por el cual reciba una BPDU. Se debe habilitar en los puertos destinados para hosts (Ariganello, 2014).

En la figura 4.94 se puede observar que, en la ventana Bridge y la pestaña Ports, se encuentra la lista de interfaces. Al ingresar a las configuraciones de cada interfaz, se puede configurar BPDU Guard en la pestaña STP.

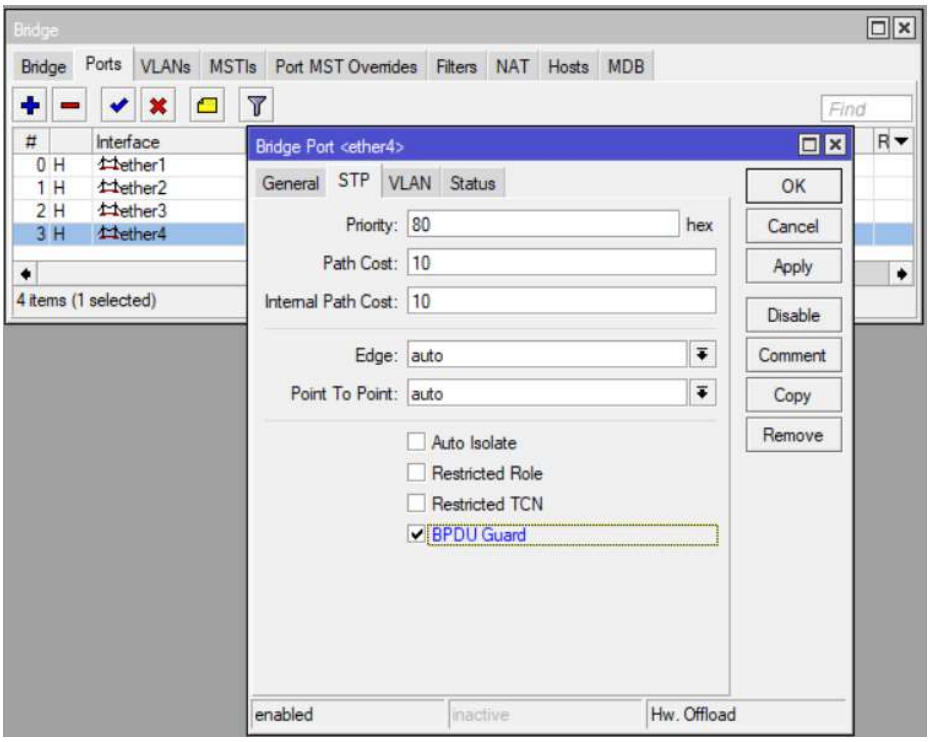


Figura 4.94: Configuración de BPDU Guard en cada puerto.

Seguridad del enlace troncal

Se recomienda cambiar los valores por defecto, utilizar la VLAN nativa solo en los puertos destinados para puertos troncales, asignar los puertos de acceso, que se vayan a utilizar, a sus respectivas VLANs y asignar los puertos restantes a una VLAN que no se vaya a utilizar (Ariganello, 2014).

Como se puede apreciar en la figura 4.95, en la pestaña VLAN y la opción Default VLAN ID se realizan las siguientes configuraciones:

- Los puertos 3 y 4 son de acceso y se asignan a las VLANs 10 y 20 respectivamente.
- El puerto 2 es troncal y se asigna a la VLAN 9 (VLAN nativa).
- El resto de puertos no serán utilizados, por lo que se los asigna a la VLAN 5, la cual no se utiliza en la red.

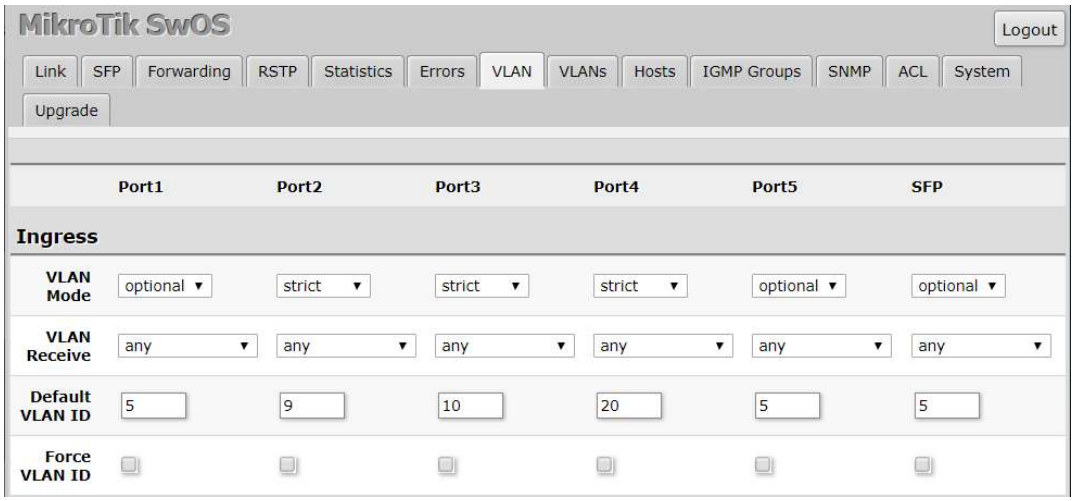


Figura 4.95: Configuración segura de VLANs.

4.4. Túnel IPsec

4.4.1. Topología

En la figura 4.96 se encuentra la primera topología de la red en la que se realizaran pruebas. Se utilizará el router Mikrotik hAP LITE TC (RB941-2Nd-TC).

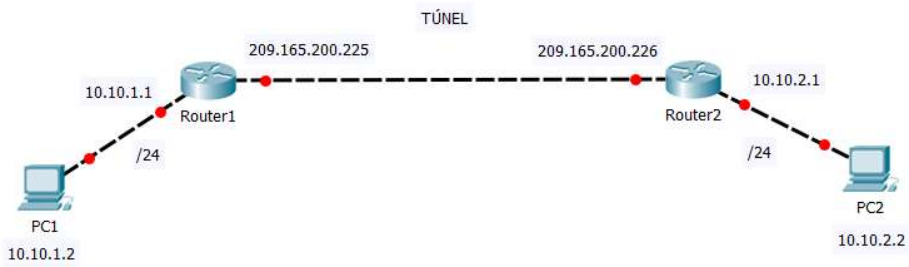


Figura 4.96: Topología N° 1 de la red de pruebas.

En la figura 4.97 se encuentra la segunda topología de la red en la que se realizarán pruebas. Se utilizará el router Mikrotik hAP LITE TC (RB941-2Nd-TC) y el switch Mikrotik RB260GSP.

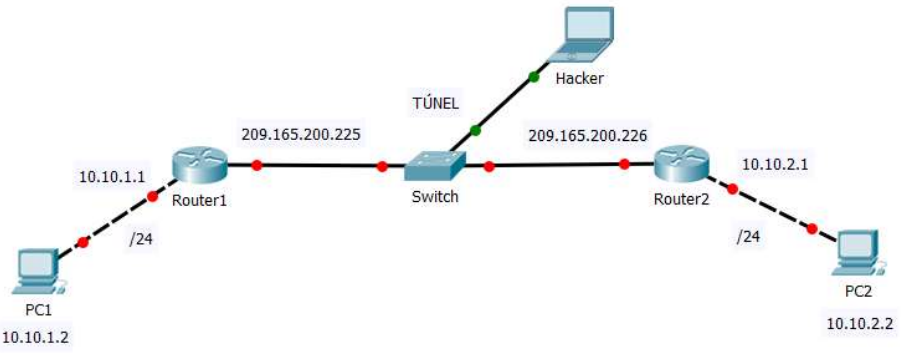


Figura 4.97: Topología N° 2 de la red de pruebas.

4.4.2. Pruebas en la red vulnerable

Se realizará la configuración de un túnel IPsec en la red de la topología de la figura 4.96.

Todas las configuraciones se deben realizar en la ventana IPsec tanto en el router 1 como en el router 2.

En la figura 4.98 se agrega un nuevo perfil en la pestaña Profiles. Aquí se especifican los parámetros de hashing (Hash Algorithms: sha1), encriptación (Encryption Algorithm: 3des) y grupo DH (DH Group: modp1024) que se utilizarán en la fase 1 de IKE (Mikrotik, Manual:IP/IPsec, s.f.).

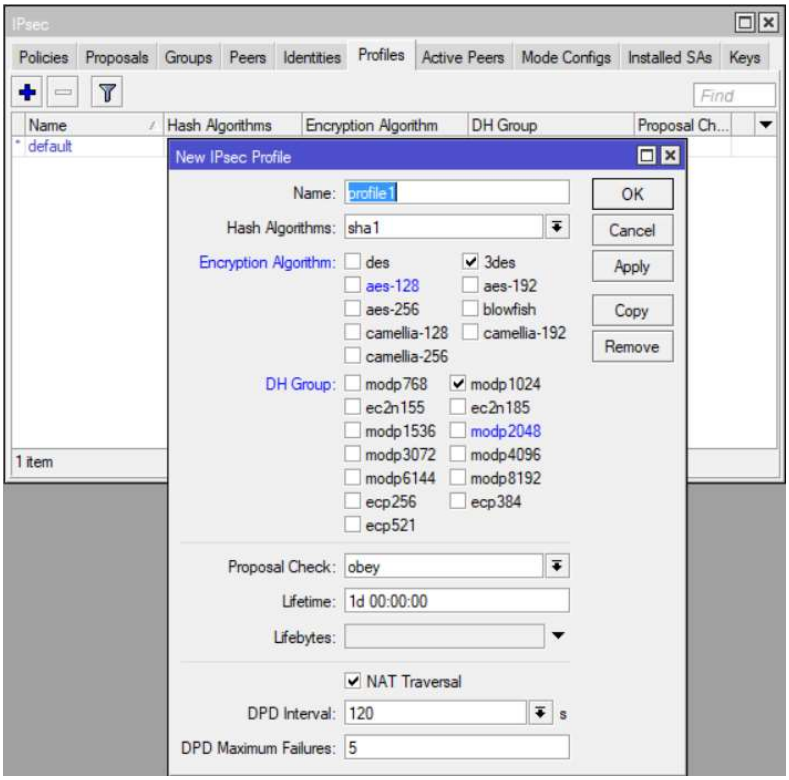


Figura 4.98: Configuraciones para la fase 1 de IKE.

En la figura 4.99 se crea una nueva propuesta en la pestaña Proposals, en la que se configuran los parámetros de hashing (Auth. Algorithms: sha1) y encriptación (Encr. Algorithms: 3des) para la fase 2 de IKE (Mikrotik, Manual:IP/IPsec, s.f.).

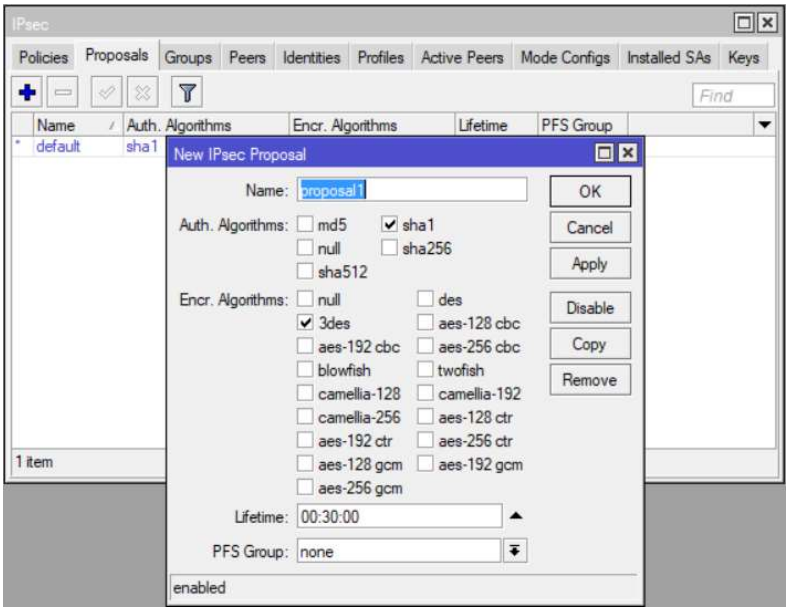


Figura 4.99: Configuraciones para la fase 2 de IKE.

En la figura 4.100, en la pestaña Peers, se configura la dirección IP del peer con el que se desea establecer el túnel (Address: 209.165.200.226/32), el perfil que se configuró anteriormente (Profile: profile1) y el modo de fase 1 (Exchange Mode: aggressive) (Mikrotik, Manual:IP/IPsec, s.f.).

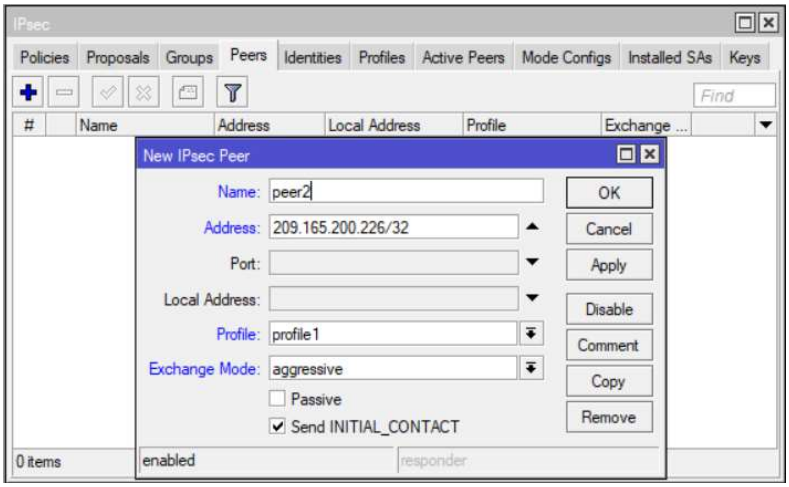


Figura 4.100: Configuraciones para la comunicación con el peer remoto.

Como se puede ver en la figura 4.101, en la pestaña Identities, se configuran los parámetros relacionados con la identificación y autenticación de los peers.

Clave precompartida o PSK (Pre Shared Key) es un método de autenticación en el que se configura un valor secreto (contraseña) en ambos extremos que participan en la comunicación (Ariganello, 2014). Se utiliza este método de autenticación de autenticación (Auth. Method: pre shared key) y se establece la contraseña (Secret: ****) (Mikrotik, Manual:IP/IPsec, s.f.).

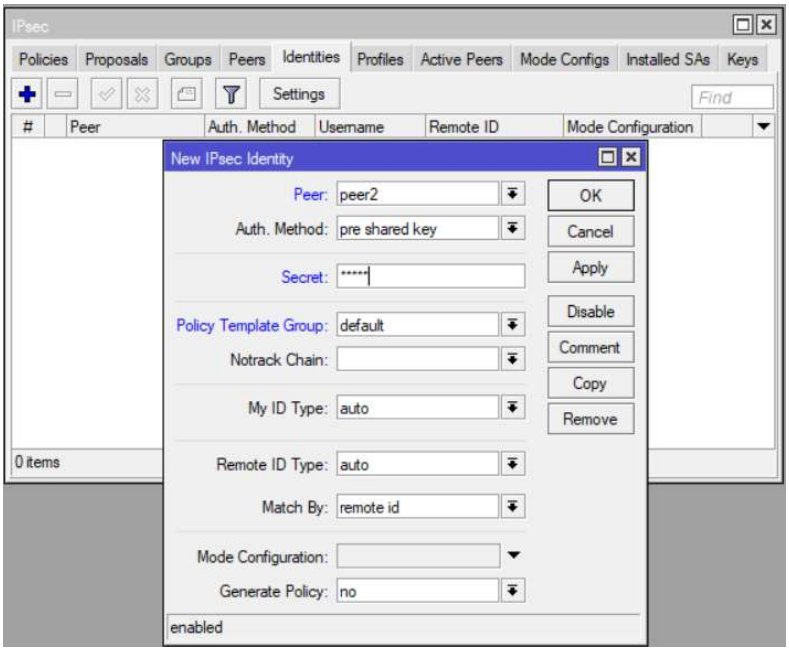


Figura 4.101: Configuración del método de autenticación y asignación de una contraseña.

Como se puede observar en las figuras 4.102 y 4.103, en la pestaña Policies, se crea una nueva política en la que se especifican las redes que se pueden comunicar por medio del túnel (Src. Address: 10.10.1.0/24) (Dst. Address: 10.10.2.0/24), el modo de IPsec (Tunnel), la acción a realizar con los datos (Action: encrypt), el protocolo IPsec a utilizar (IPsec Protocols: ah) y la propuesta configurada anteriormente (Proposal: proposal1) (Mikrotik, Manual:IP/IPsec, s.f.).

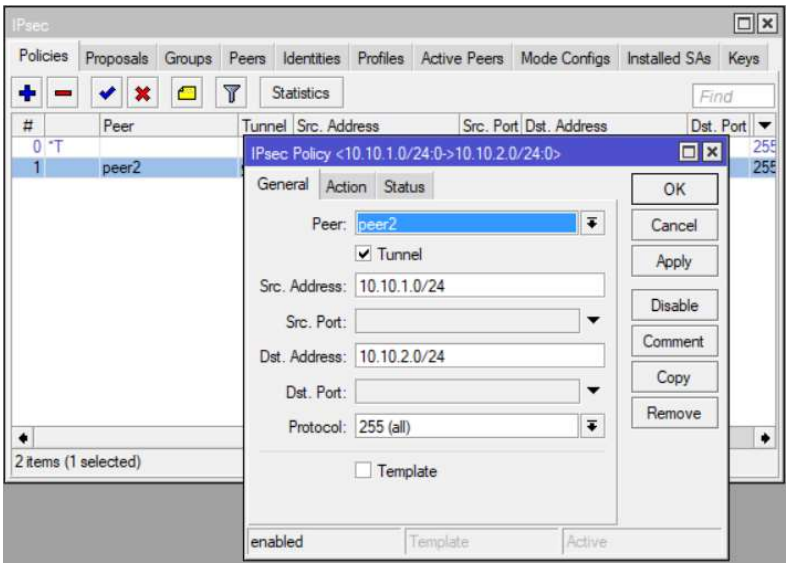


Figura 4.102: Configuración de las políticas IPsec.

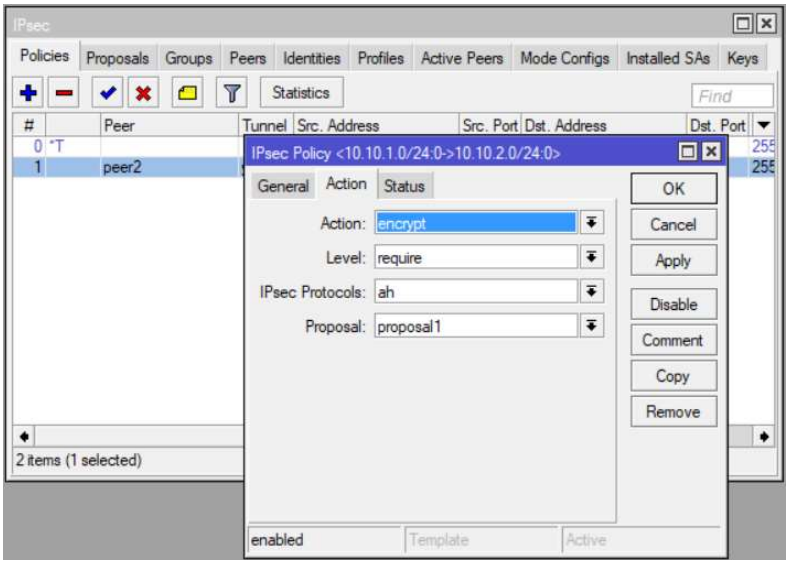


Figura 4.103: Configuración de las políticas IPsec.

Debido a que NAT (Network Address Translation) traduce las direcciones antes de que ingresen a las políticas IPsec, no se podrá establecer una comunicación a través

del túnel, por lo que se debe agregar una regla de firewall para que no se traduzcan las direcciones que se configuraron en las políticas IPsec (Mikrotik, Manual:IP/IPsec, s.f.).

Las configuraciones realizadas en la pestaña General establecen las direcciones IP de origen (Src. Address: 10.10.1.0/24) y destino (Dst. Address: 10.10.2.0/24), como se puede ver en la figura 4.104 (Mikrotik, Manual:IP/IPsec, s.f.).

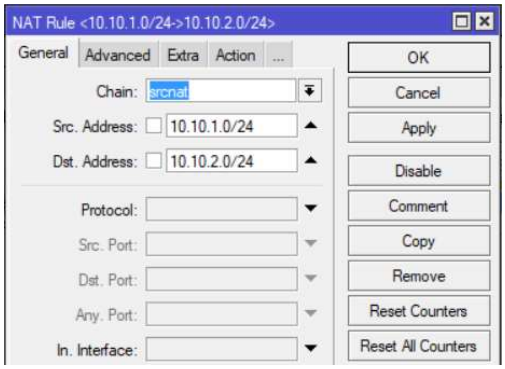


Figura 4.104: Configuraciones en la pestaña General.

En la figura 4.105 se muestran las configuraciones realizadas en la pestaña Action, las cuales establecen que se debe aceptar (Action: accept) el tráfico de las direcciones especificadas en la figura 4.104 (Mikrotik, Manual:IP/IPsec, s.f.).

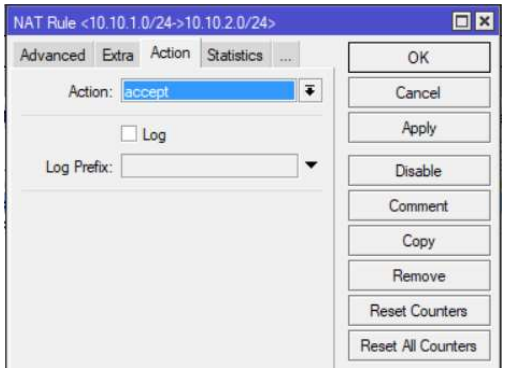


Figura 4.105: Configuraciones en la pestaña Action.

En la red de la figura 4.97 un atacante conecta un switch entre el router 1 y 2 para poder analizar el tráfico que se produce entre estos 2 equipos.

En el switch se configura Port Mirroring para que el atacante, conectado al puerto 3 (Mirror To), reciba una copia del tráfico que ingresa por el puerto 1 o 2 (Mirror Ingress:). En la figura 4.106 se pueden ver las configuraciones realizadas en la pestaña Forwarding.

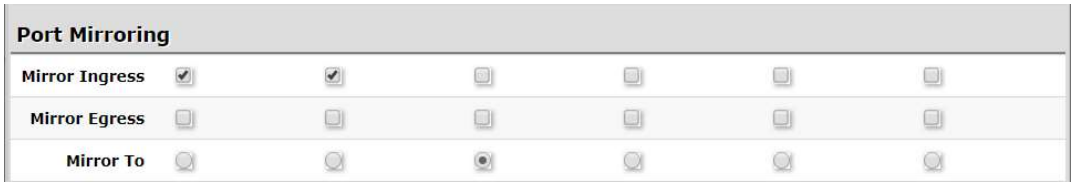


Figura 4.106: Configuración de Port Mirroring en el switch.

No confidencialidad del protocolo AH

Debido a que el protocolo AH no encripta los datos, es posible ver la información que pasa a través del túnel IPsec.

Se realiza ping desde la PC1 a la PC2.

En la figura 4.107 se analiza el tráfico, utilizando Wireshark, desde la computadora del atacante. Se comprueba que la información es visible cuando se usa el protocolo AH.

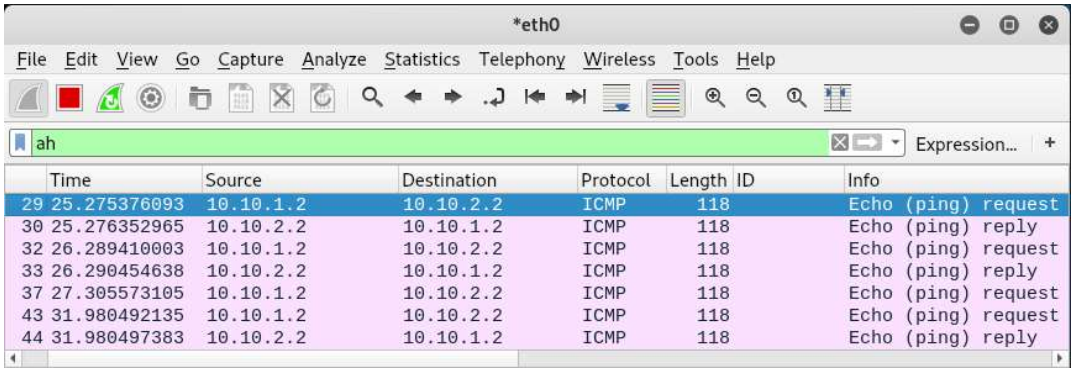


Figura 4.107: Análisis de tráfico del protocolo AH.

Ataque de contraseña fuera de línea

Este ataque está orientado a los túneles IPsec que utilizan el modo aggressive en la fase 1 de IKE y que utilizan el método de autenticación de clave precompartida (PSK).

Cuando se produce la autenticación de la fase 1 de IKE, en modo aggressive, uno de los peers envía un hash, sin encriptar, de la contraseña (PSK) y de otros valores conocidos que se utilizan dentro de la comunicación. Es posible capturar los paquetes

de la fase 1 y realizar un ataque de diccionario para intentar descubrir la contraseña de autenticación.

El ataque consiste en que se obtiene un hash de cada palabra del diccionario y se compara con el hash de los paquetes capturados. Si ambos coinciden, se descubrió la contraseña (Pitts, 2004).

Para la captura de datos y el ataque de diccionario se utilizará Cain & Abel, que es una herramienta que permite capturar tráfico y realizar ataques de contraseña. Dispone de una característica específica para la captura y análisis de tráfico de la fase 1 de IKE en modo aggressive (Pitts, 2004).

En las figuras 4.108 y 4.109 se muestra que, en la pestaña Sniffer de Cain & Abel, se pueden capturar los datos que intercambian los peers en la fase 1 de IKE.

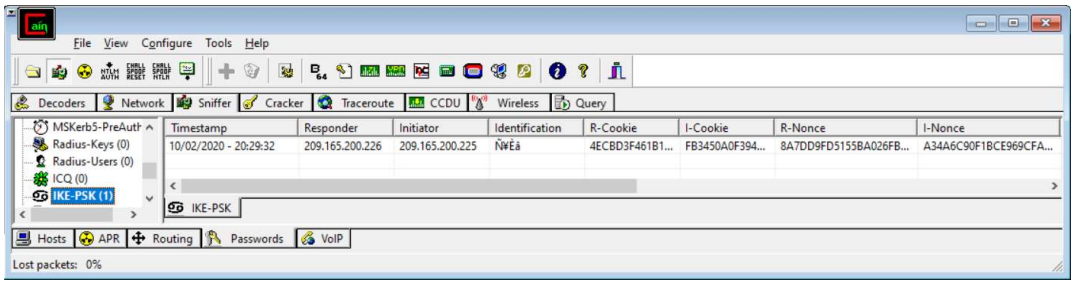


Figura 4.108: Captura de datos de la fase 1 de IKE mediante Cain & Abel.

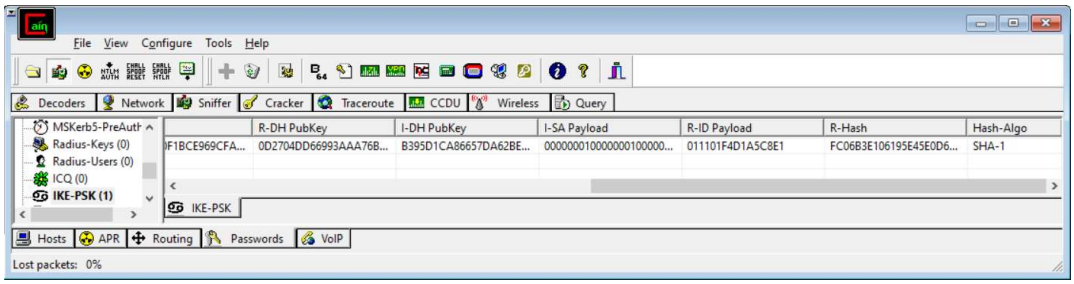


Figura 4.109: Captura de datos de la fase 1 de IKE mediante Cain & Abel.

En estos datos se realiza click derecho/Send to Cracker y esta información pasará a la pestaña Cracker que se puede ver en la figura 4.110. Aquí se puede realizar el ataque de contraseña.

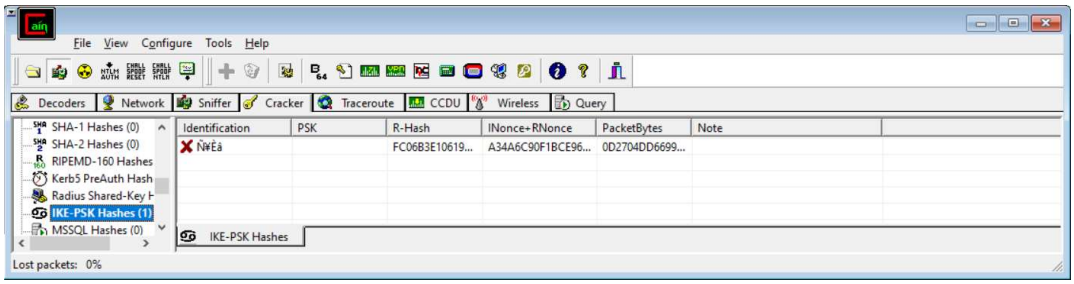


Figura 4.110: Pestaña Cracker de Cain & Abel.

En los datos se realiza click derecho/Dictionary Attack y se abre la ventana de la figura 4.111. En esta ventana se agrega una lista de palabras (diccionario) y se ejecuta el ataque.

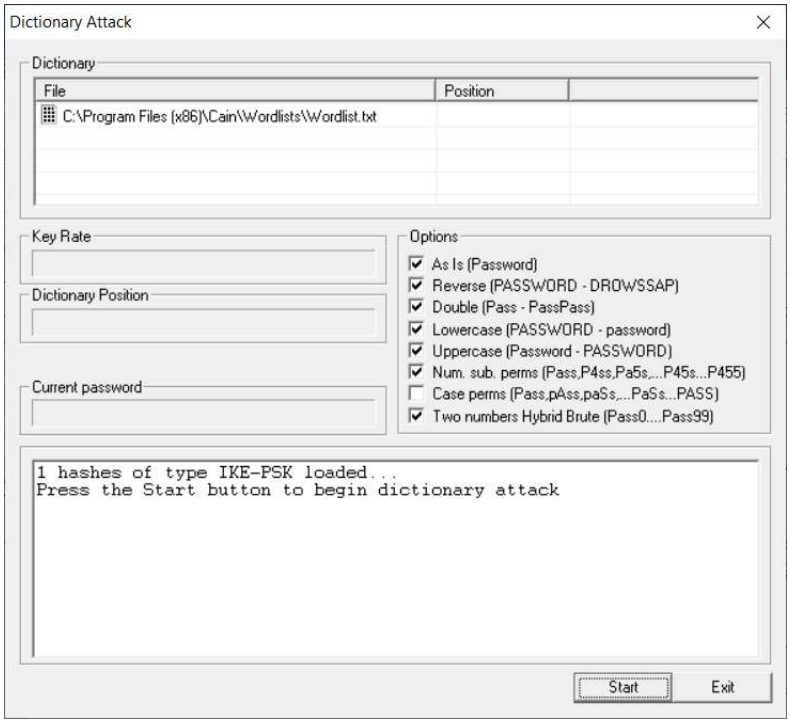


Figura 4.111: Configuraciones del ataque de diccionario.

En la figura 4.112 se muestra la contraseña (PSK) obtenida.

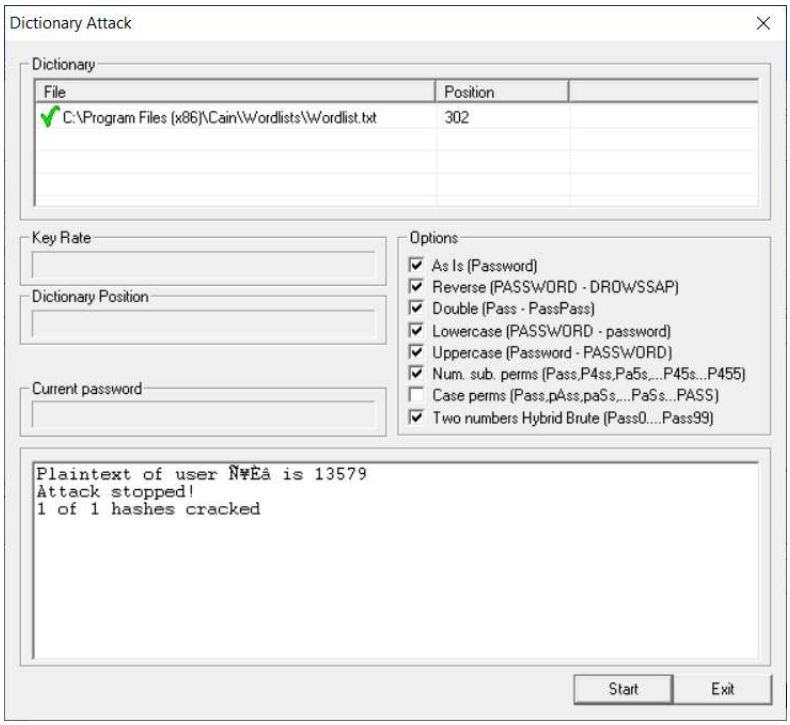


Figura 4.112: Ataque de diccionario exitoso.

4.4.3. Configuraciones de seguridad

ESP

Este protocolo ofrece las mismas características de seguridad que AH y adicionalmente encripta la información (UCF, The VPN gateway must use ESP tunnel mode for establishing secured paths to transport traffic between the organization's sites or between a gateway and remote end-stations., 2015).

En la ventana IPsec y la pestaña Policies se encuentran las configuraciones de políticas. Aquí se puede elegir el protocolo ESP (IPsec Protocols: esp), como se puede notar en la figura 4.113.

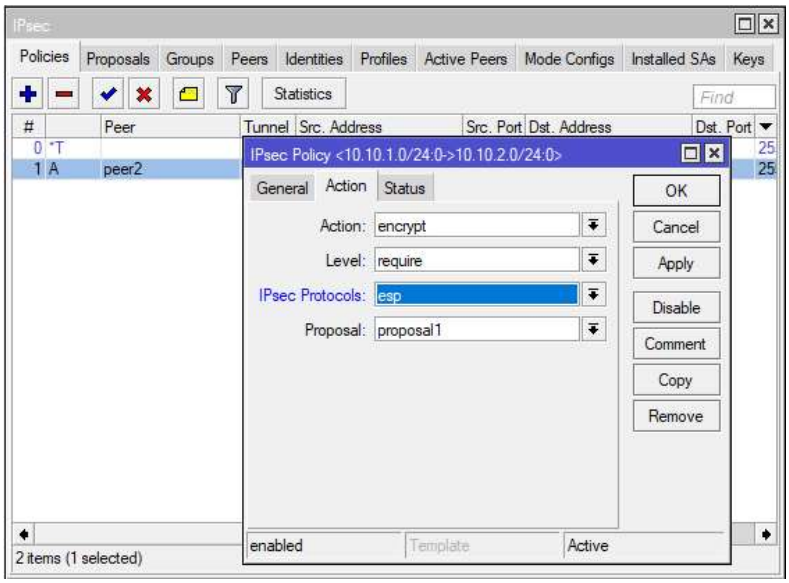


Figura 4.113: Configuración de ESP.

Modo Main

El modo main encripta la información relacionada con la autenticación, como el hash donde está incluida la contraseña (PSK) (UCF, The VPN gateway must use IKE main mode for the purpose of negotiating an IPSec security association policy when pre-shared keys are used for authentication, 2015).

En la ventana IPsec y la pestaña Peers se encuentran las configuraciones para la comunicación con el peer remoto. Aquí se puede elegir el modo main (Exchange Mode: main), como se puede notar en la figura 4.114.

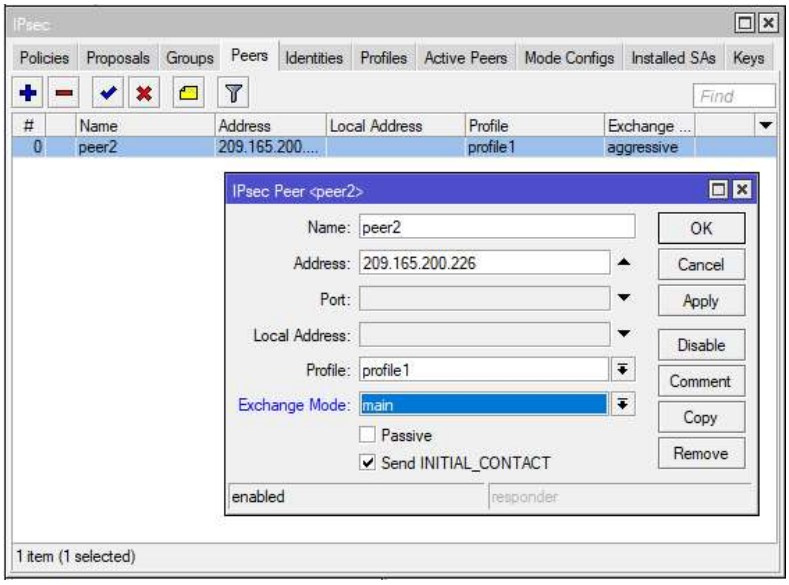


Figura 4.114: Configuración del modo main.

PFS (Perfect Forward Secrecy)

PFS es una característica que se puede configurar en la fase 2 de IKE. Su función es generar nuevas llaves de encriptación cada vez que se produzca la fase 2 en lugar de generar llaves derivadas de las que se generaron en la fase 1, por lo tanto, las llaves de cada fase son independientes entre sí. Si un atacante obtiene las llaves de encriptación de la fase 1, no podrá desencriptar los datos que se generen en la fase 2. Con PFS se generan nuevas llaves con el mismo método que en la fase 1, mediante el grupo DH (UCF, The VPN gateway must specify Perfect Forward Secrecy during IKE negotiation., 2018).

En la figura 4.115 se muestra la ventana IPsec y la pestaña Proposals. Aquí se puede configurar PFS (PFS Group: modp2048).

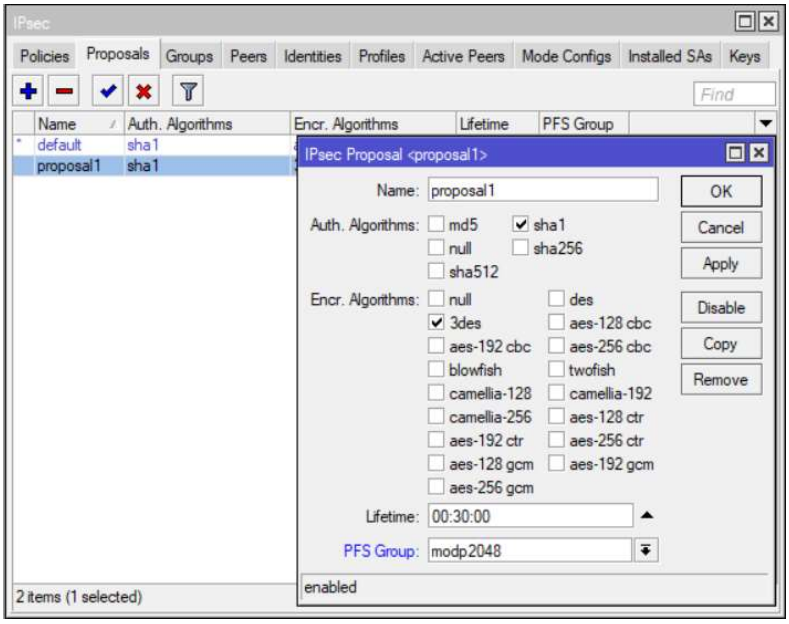


Figura 4.115: Configuración de PFS.

Algoritmos recomendados

Algunos algoritmos de hashing, encriptación y grupo DH todavía se incluyen en las configuraciones de dispositivos, pero no se consideran seguros. Se recomienda utilizar nuevas versiones.

No se recomienda utilizar algoritmos de encriptación como des o 3des. En su lugar se recomienda utilizar AES o superiores (CISCO, Configuring Internet Key Exchange for IPsec VPNs, 2018) (UCF, The VPN gateway must use AES for IPSec cryptographic encryption operations required to ensure privacy of the IPSec session., 2018).

No se recomienda utilizar algoritmos de hashing como md5 o sha1. En su lugar se recomienda utilizar sha256 o superiores (CISCO, Configuring Internet Key Exchange for IPsec VPNs, 2018) (UCF, The VPN gateway must use Secure Hash Algorithm for IPSec cryptographic hashing operations required for authentication and integrity verification., 2018) (Stevens, y otros, 2017).

No se recomienda utilizar grupos DH como modp768 o modp1024. En su lugar se recomienda utilizar modp 2048 o superiores (CISCO, Configuring Internet Key

Exchange for IPsec VPNs, 2018) (UCF, The VPN gateway must use a key size from Diffie-Hellman Group 14 or larger during IKE Phase 1., 2018) (UCF, The VPN gateway must use a key size from Diffie-Hellman Group 14 or larger during IKE Phase 2., 2020).

Para la configuración de los algoritmos recomendados, se debe acceder a la ventana IPsec, la pestaña Profiles (fase 1) y Proposals (fase 2), como se vio en las figuras 4.98 y 4.99.

4.5. Conclusiones

Se realizaron ataques para demostrar las vulnerabilidades que pueden presentarse en las redes de computadoras.

La idea principal es comprender en que consiste el ataque para saber cómo defenderse del mismo, debido a esto, se explicaron los conceptos, protocolos y servicios en los que se basan los ataques y las herramientas que se utilizan. También se plantearon las configuraciones y las buenas prácticas de seguridad que ayuden a mitigar estos ataques.

5. CAPÍTULO 5: RESULTADOS

5.1. Introducción

En este capítulo se validarán las configuraciones de seguridad, para lo cual se volverán a realizar los ataques de la sección de desarrollo, pero en esta ocasión la red estará protegida por las configuraciones de seguridad planteadas anteriormente.

5.2. Seguridad en un router

5.2.1. Validaciones

SSH en lugar de Telnet

Se desactiva el servicio de Telnet.

Se inicia la captura de datos, mediante Wireshark, en la computadora.

En la figura 5.1 se pueden analizar los comandos que se deben utilizar para conectarse, mediante SSH, a la interfaz *ethernet* con dirección IP 10.10.1.1.

En la terminal se ingresa el nombre de usuario y contraseña para acceder al router.

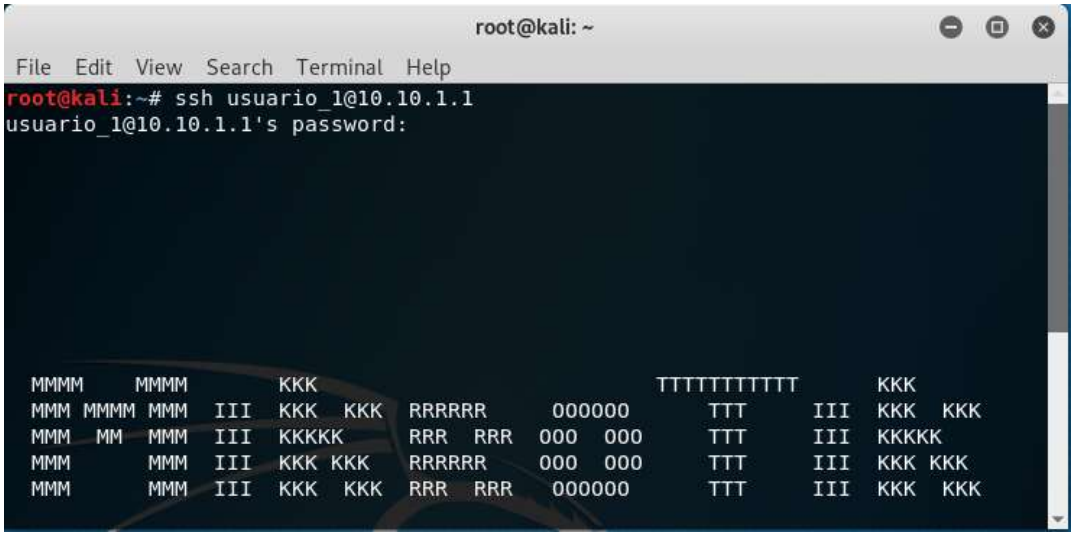


Figura 5.1: Acceso al router por SSH.

En la figura 5.2, mediante Wireshark, se realiza un filtrado de los paquetes del protocolo SSH.

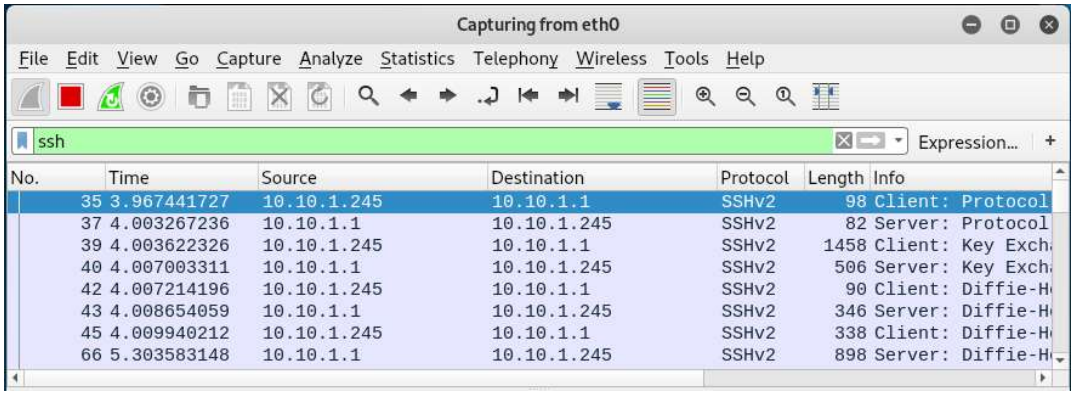


Figura 5.2: Filtrado de paquetes del protocolo SSH.

En cualquier paquete se hace click derecho/Follow/TCP Stream y se obtiene información encriptada, como se puede ver en la figura 5.3.

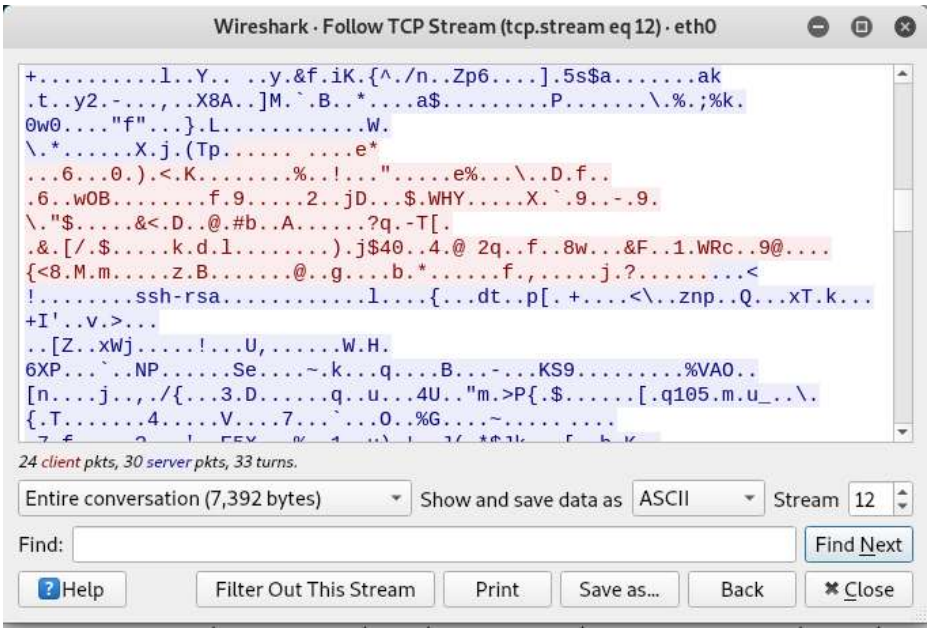


Figura 5.3: Datos encriptados por SSH.

Defensa contra Winbox exploit

La mejor defensa contra Winbox Exploit es actualizar el sistema operativo a una versión en la que se haya corregido esta vulnerabilidad.

Para esta prueba se instaló, en el router, la versión del sistema operativo RouterOS, 6.45.7 (Stable). La vulnerabilidad CVE-2018-14847 se corrigió desde la versión 4.42.1 (Stable).

En la figura 5.4 se puede comprobar que no se obtiene ni el nombre de usuario ni la contraseña al ejecutar la herramienta WinboxExploit. El ataque está dirigido a la interfaz *ethernet* con dirección IP 10.10.1.1.

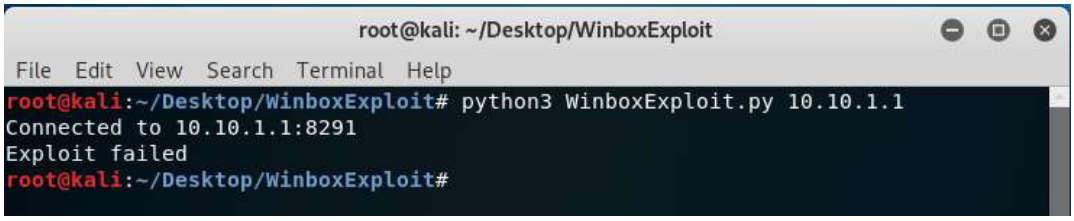


Figura 5.4: Intento fallido de obtención de nombre de usuario y contraseña mediante WinboxExploit.

Suponiendo que no existiera una actualización del sistema operativo en la que se corrija esta vulnerabilidad, se recomienda desactivar el servicio de Winbox y utilizar el servicio SSH para la configuración de dispositivos.

En el caso de que sea realmente necesario utilizar Winbox para configuración, se recomienda (BasuCert, s.f.):

- Cambiar el puerto por defecto de Winbox.
- Bloquear el acceso por MAC.
- Permitir la conexión a Winbox solo desde una dirección IP específica.
- Si el router está conectado a internet, bloquear el acceso a Winbox por esa interfaz.

En la figura 5.5 se puede verificar que no se obtiene ni el nombre de usuario ni la contraseña al ejecutar la herramienta Winbox Exploit. Este resultado se obtiene desactivando el servicio Winbox o con las 4 configuraciones explicadas anteriormente.

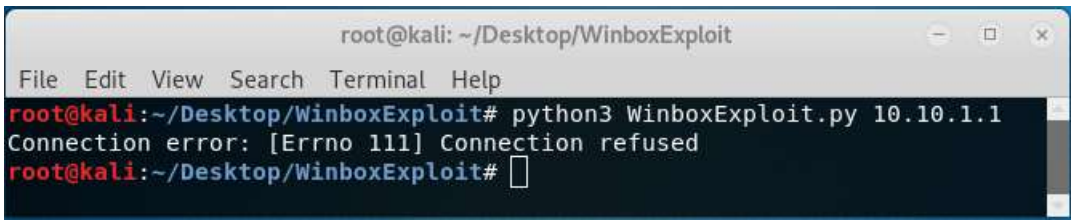


Figura 5.5: Intento fallido de obtención de nombre de usuario y contraseña mediante Winbox Exploit.

Uso de contraseñas seguras

La protección más básica contra ataques de contraseña es utilizar contraseñas seguras que no incluyan información personal, sucesiones simples de números, etc.

En la figura 5.6 se muestra que se utiliza la herramienta pwgen para generar una contraseña.

Figura 5.6: Generador de contraseñas seguras.

En el router se cambia el nombre de usuario por defecto y se le asigna la contraseña de la figura 5.6. Con estas configuraciones, el atacante tendrá dos incógnitas por descifrar.

Para el ataque de diccionario se deberá usar una lista de palabras tanto para el nombre de usuario como para la contraseña. Los comandos se pueden examinar en la figura 5.7.

El ataque no tiene éxito y se tardará demasiado tiempo en probar todos los nombres de usuario y contraseñas del diccionario.

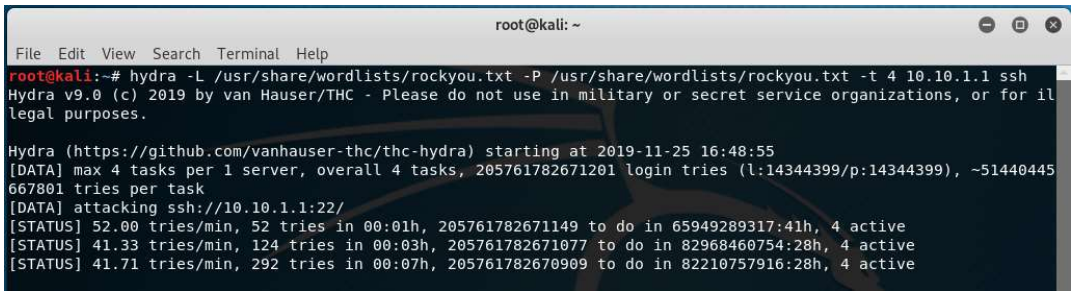


Figura 5.7: Intento fallido de descifrar el nombre de usuario y contraseña.

Para el ataque de fuerza bruta se deberá conocer el nombre de usuario y para la contraseña se tendrán que generar todas las posibles combinaciones, con 12 caracteres, que incluyan letras mayúsculas, minúsculas y números. Los comandos se pueden analizar en la figura 5.8.

No se puede generar el ataque porque existe un número demasiadamente alto de posibles contraseñas.

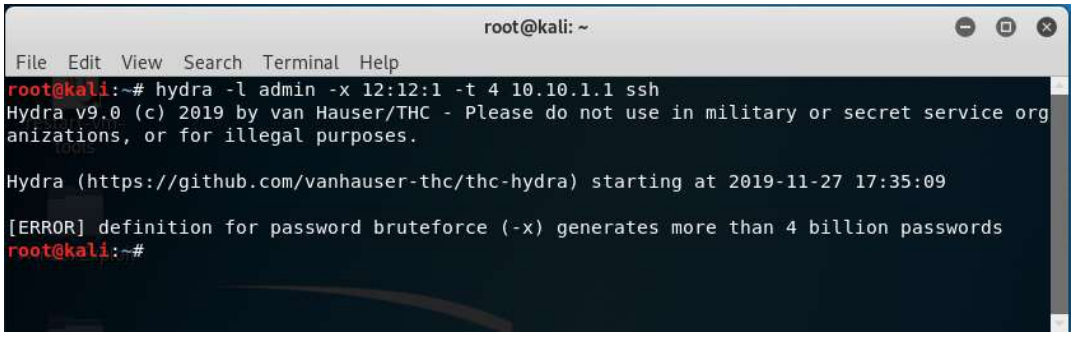


Figura 5.8:: Intento fallido de descifrar el nombre de usuario y contraseña.

Limitar el número de intentos de ingreso fallidos

Otro mecanismo de defensa contra ataques de contraseña es limitar la cantidad de ingresos fallidos en el router.

Se activan las reglas de firewall correspondientes.

Al realizar un ataque de diccionario y de fuerza bruta, como los de las figuras 4.8 y 4.9, se obtiene lo siguiente:

En la primera conexión, la dirección IP se agrega a la lista auxiliar SSHCon por 1 minuto.

En la segunda conexión, la dirección IP se agrega a la lista Auxiliar SSHCon2 por 1 min.

En la tercera conexión, la dirección IP se agrega a la lista de bloqueo BruteForceAttacker por 1 día. Se descarta todo paquete proveniente de esta dirección IP.

En la figura 5.9 se puede verificar que la dirección IP de origen se agregó a las 3 listas.

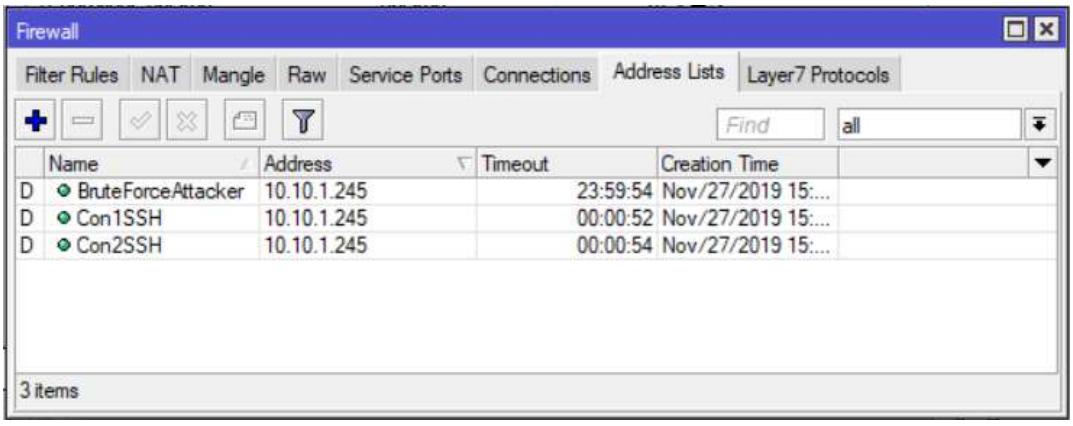


Figura 5.9: Dirección IP agregada a lista de bloqueo.

En la figura 5.10 se puede notar que la primera regla de firewall está descartando paquetes.

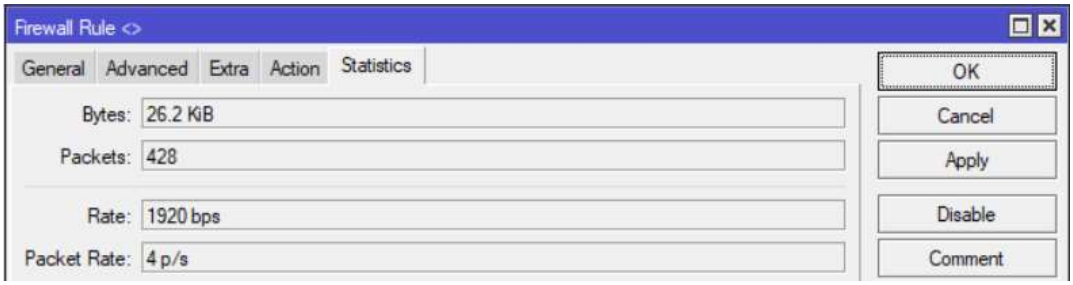


Figura 5.10: Estadísticas de la primera regla de Firewall.

Defensa contra SYN-FLOOD

Con esta prueba se comprobará que, con las configuraciones para limitar el número de nuevas conexiones sucesivas en el router, el servidor responderá a solicitudes de conexión y se mitigará el ataque SYN FLOOD.

Mediante la terminal de Kali Linux se realiza un ataque SYN FLOOD similar al de la figura 4.12, pero con la excepción de que la velocidad de los paquetes se aumenta a la máxima posible (la velocidad puede variar con el transcurso del tiempo). Los comandos se pueden examinar en la figura 5.11.

Figura 5.11: Ataque SYN FLOOD mediante hping3.

En la figura 5.12 se encuentra la ventana de monitoreo de las interfaces del router. Se puede notar que la interfaz *ethernet 1* recibe paquetes a una velocidad de 27138 p/s y no se transmiten por la interfaz *ethernet 2*. Esto quiere decir que el router no permite el paso de los paquetes.

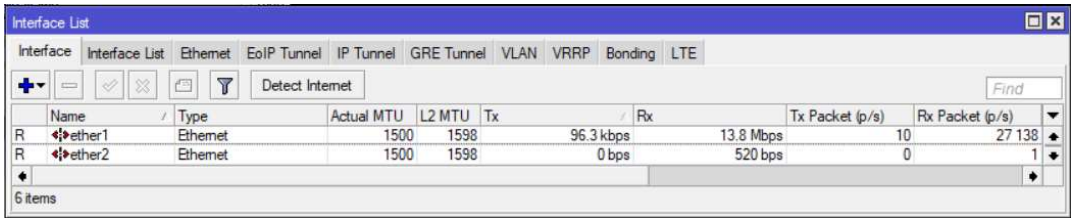


Figura 5.12: Monitoreo de tráfico en ventana Interface List.

En la figura 5.13 se verifica que la dirección IP 10.10.3.3 se añadió a la lista de bloqueo SynFlooder.

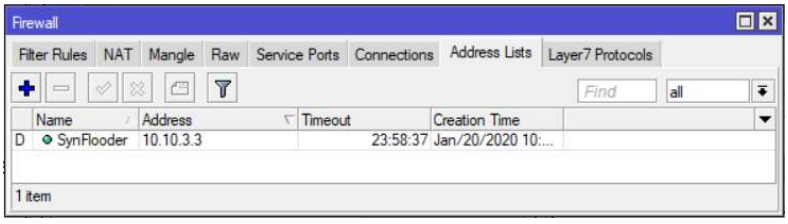


Figura 5.13: Lista de bloqueo SynFlooder.

En la figura 5.14 se encuentran las estadísticas de la primera regla de firewall y se puede ver que descarta paquetes a una velocidad de 27491 p/s.

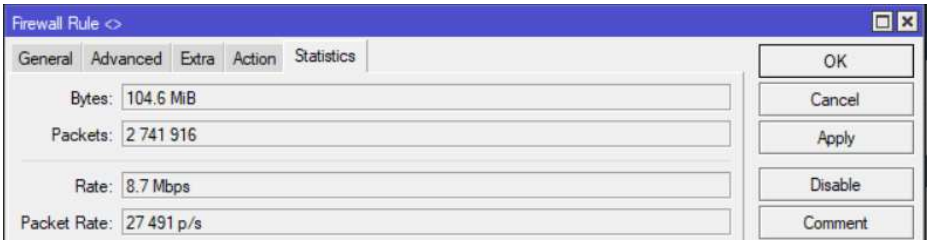


Figura 5.14: Estadísticas de la primera regla de firewall.

Desde la computadora, con dirección IP 10.10.3.254, se intenta acceder al servidor, a través del navegador web, y se establece la conexión de forma exitosa. En la figura 5.15, mediante Wireshark, se comprueban los paquetes que conforman el enlace de 3 vías.

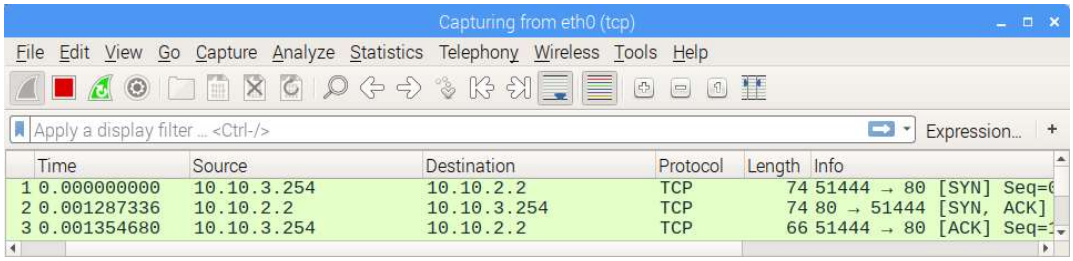


Figura 5.15: Intento de conexión, desde un cliente legítimo, al servidor web.

La defensa mediante reglas de firewall provoca que la carga del CPU sea del 75%, como se puede observar en la figura 5.16.

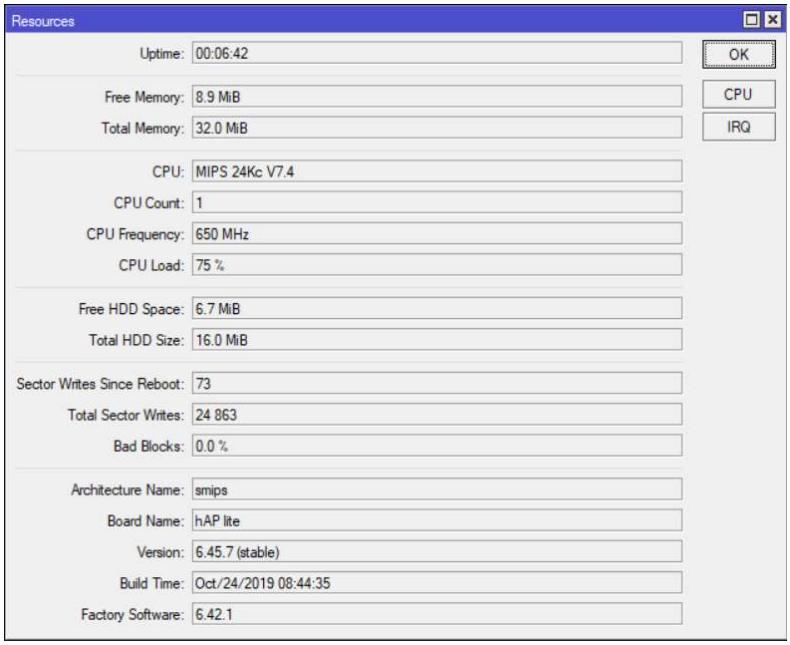


Figura 5.16: Recursos del router.

Defensa contra SPOOFING

Con esta primera prueba se comprobará que, utilizando Reverse Path Forwarding, el servidor responde a solicitudes de conexión, se contrarresta el SPOOFING y por consiguiente se mitiga el ataque SYN FLOOD.

Se activa Reverse Path Forwarding en modo strict.

Mediante la terminal de Kali Linux se realiza un ataque SYN FLOOD generando paquetes con direcciones IP de origen aleatorias, al puerto 80 de la dirección IP 10.10.2.2 y con la máxima velocidad posible (la velocidad puede variar con el transcurso del tiempo). Los comandos se pueden examinar en la figura 5.17.

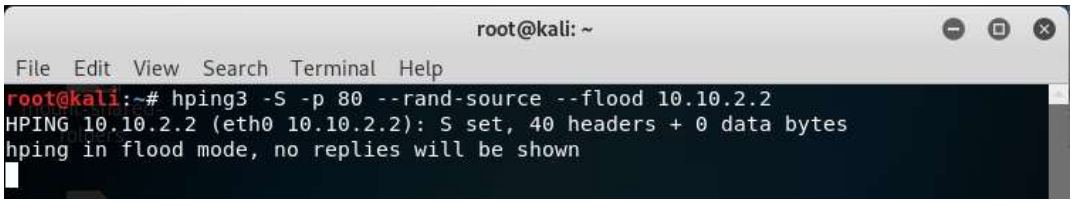


Figura 5.17: Ataque SYN FLOOD mediante hping3.

En la figura 5.18 se encuentra la ventana de monitoreo de las interfaces del router. Se puede observar que la interfaz *ethernet 1* recibe paquetes a una velocidad de 27500 p/s y no se transmiten por la interfaz *ethernet 2*. Esto quiere decir que el router descarta los paquetes provenientes de direcciones IP suplantadas.

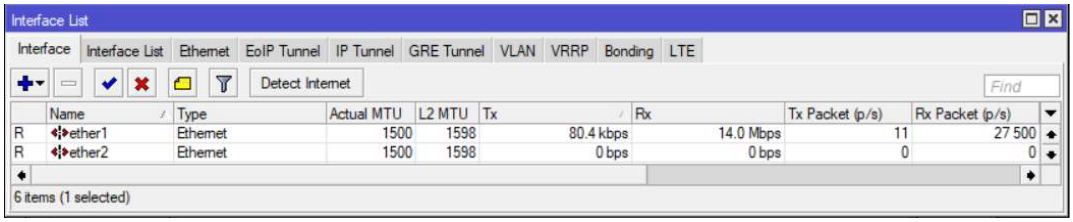


Figura 5.18: Monitoreo de tráfico en ventana Interface List.

Desde la computadora con dirección IP 10.10.3.254 se intenta acceder al servidor, a través del navegador web, y se establece la conexión de forma exitosa. En la figura 5.19, mediante Wireshark, se verifican los paquetes que conforman el enlace de 3 vías.

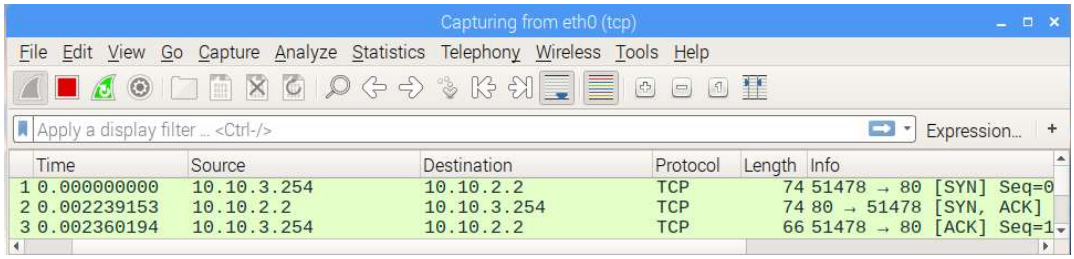


Figura 5.19: Intento de conexión, desde un cliente legítimo, al servidor web.

Con esta segunda prueba se comprobará que, utilizando Reverse Path Forwarding, el atacante no podrá conectarse al servidor con una dirección suplantada.

Mediante la terminal de Kali Linux se envían paquetes, con la dirección IP de origen 10.10.3.3, al puerto 80 de la dirección IP 10.10.2.2. Los comandos se pueden observar en la figura 5.20.

Figura 5.20: Intento de establecer una conexión, con dirección IP suplantada, al servidor.

En la figura 5.21 se encuentra la ventana de monitoreo de las interfaces del router. Se puede observar que la interfaz *ethernet 1* recibe paquetes, pero no se transmiten por la interfaz *ethernet 2*. Esto quiere decir que el router no permite el paso de paquetes con direcciones IP suplantadas.

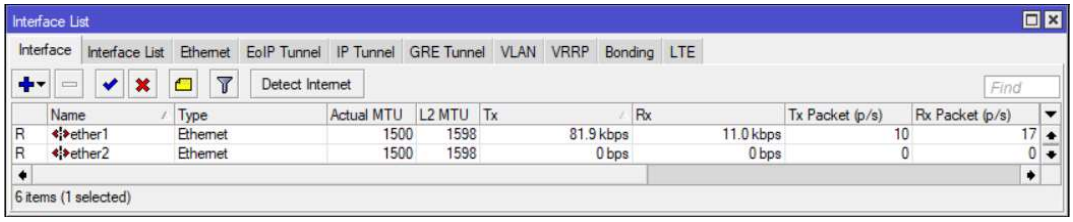


Figura 5.21: Monitoreo de tráfico en ventana Interface List.

En la figura 5.22, mediante Wireshark, se comprueba que no ingresan paquetes al servidor.

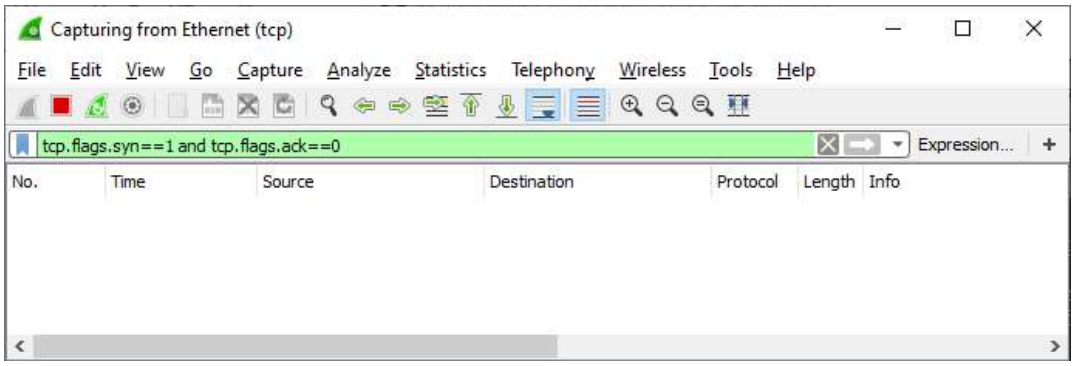


Figura 5.22: Monitoreo de tráfico, mediante Wireshark, en el servidor.

Defensa contra Escáner de red

En esta prueba se comprobará que, con Port Scan Detection, se puede detectar y mitigar el escaneo de red.

Las reglas de firewall de protección contra escáneres están activadas.

En la figura 5.23 se puede observar que se realiza un escaneo TCP SYN desde el puerto 21 hasta el 80. Solo se obtiene la información de, máximo, 3 puertos por cada host, debido a que las reglas de firewall bloquean los paquetes a partir de 4 escaneos consecutivos a puertos bien conocidos.

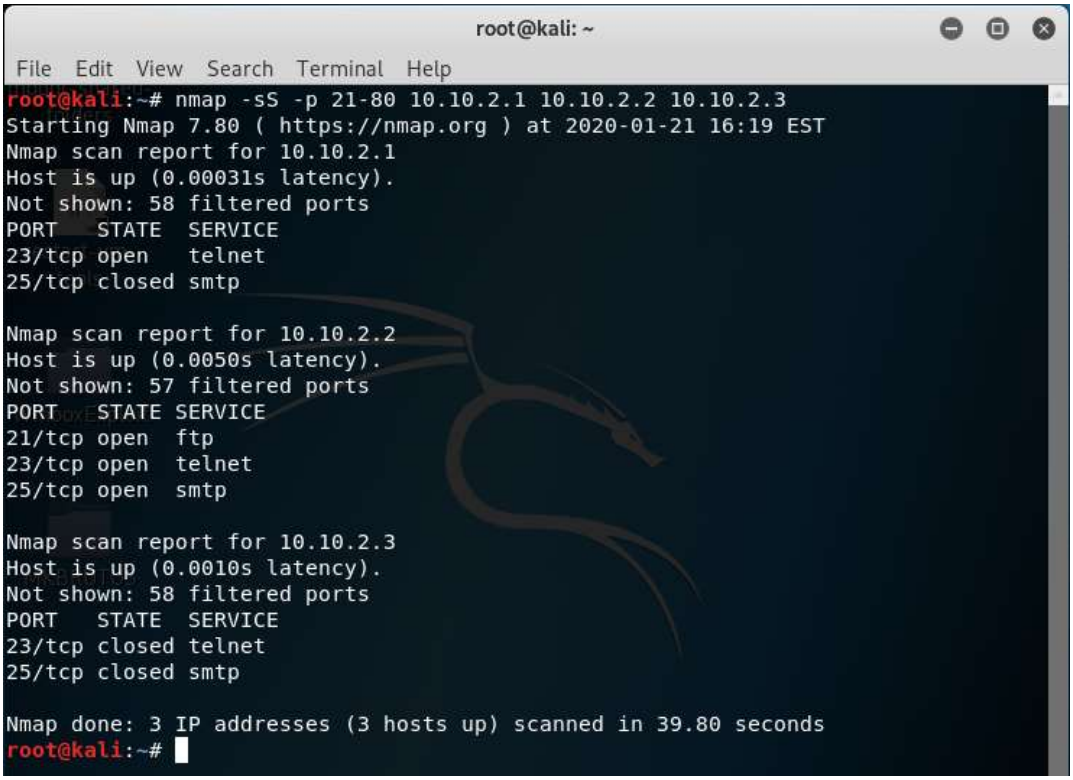


Figura 5.23: Escaneo TCP SYN fallido.

En la figura 5.24 se intenta identificar los servicios y versiones en cada puerto analizado, pero no se obtiene información.

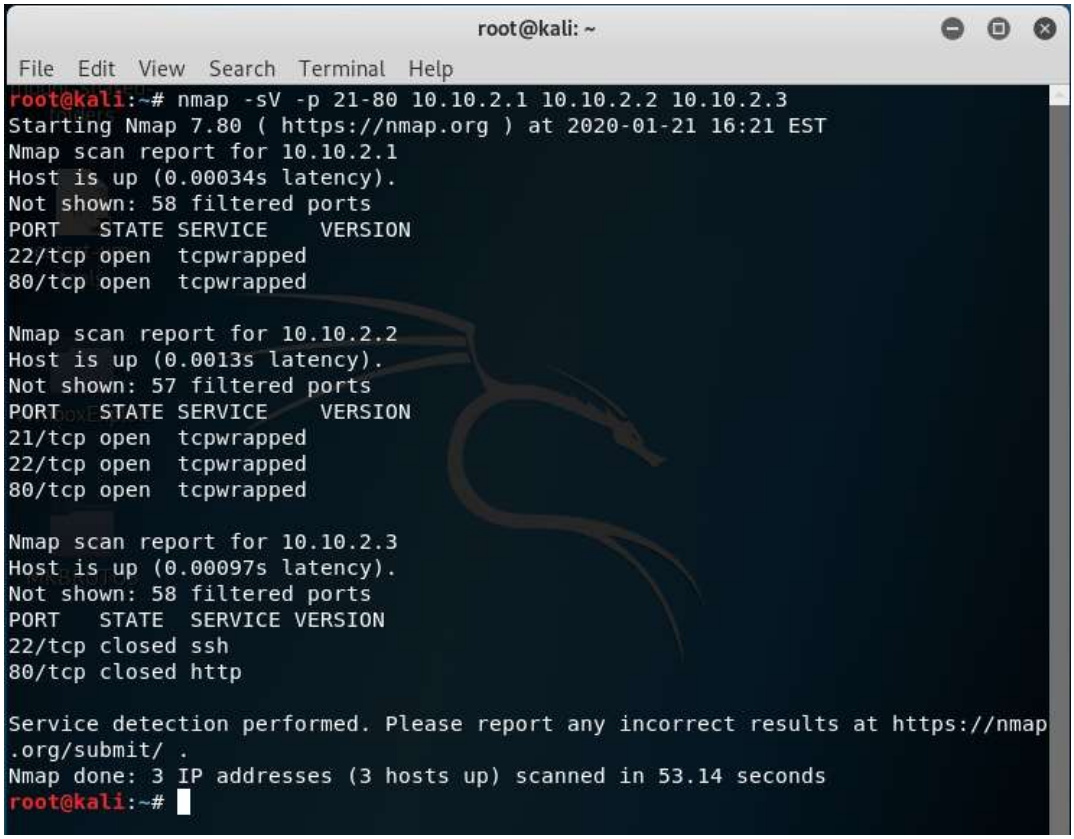


Figura 5.24: Descubrimiento fallido de servicios y versiones en puertos.

En la figura 5.25 se realiza un escaneo TCP completo desde el puerto 21 hasta el 80. Solo se obtiene la información de, máximo, 3 puertos por cada host. Debido a que las reglas de firewall bloquean los paquetes a partir de 4 escaneos consecutivos a puertos bien conocidos.

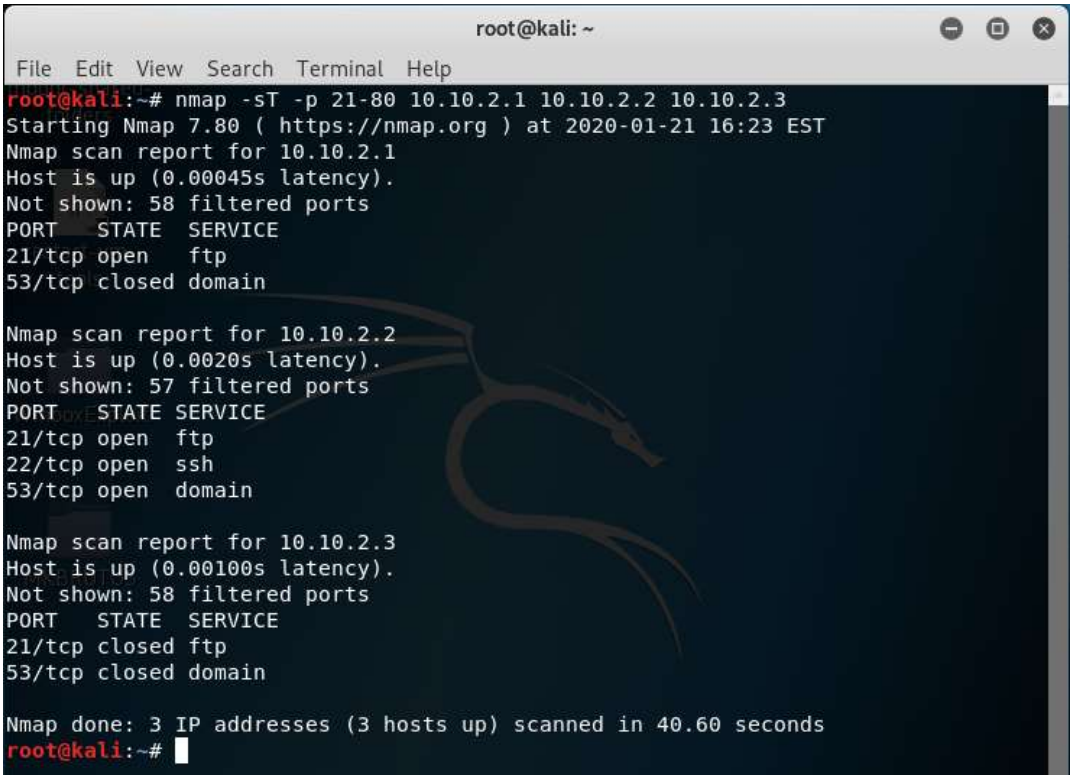


Figura 5.25: Escaneo TCP completo fallido.

En la figura 5.26 se puede ver que se realiza un escaneo TCP Null, desde el puerto 21 hasta el 80, pero no se obtiene información.

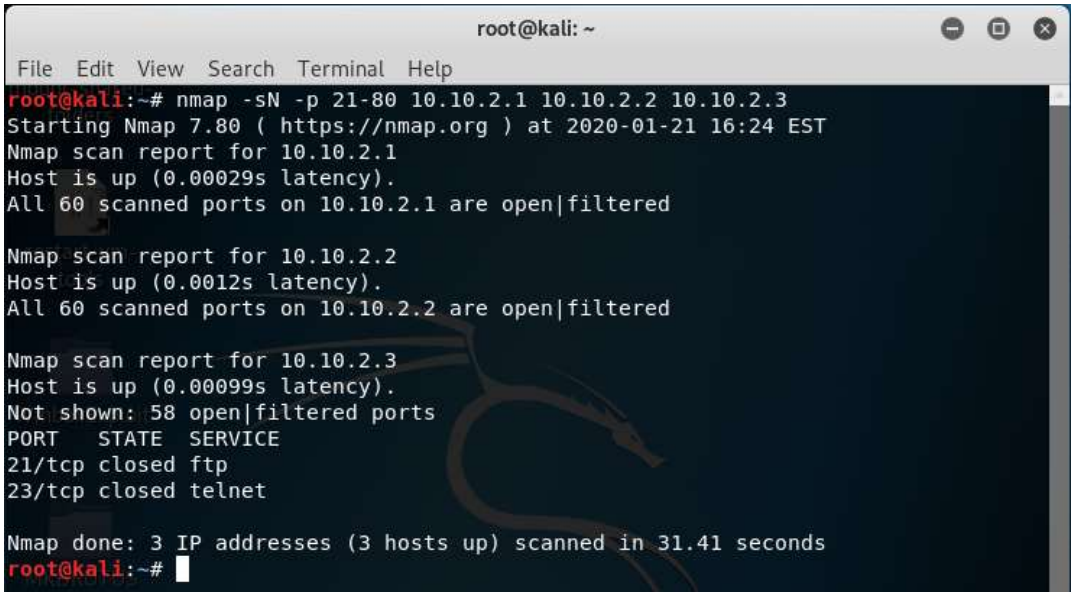


Figura 5.26: Escaneo TCP Null fallido.

Como se puede ver en la figura 5.27, se realiza un escaneo TCP FIN, desde el puerto 21 hasta el 80, pero no se obtiene información.

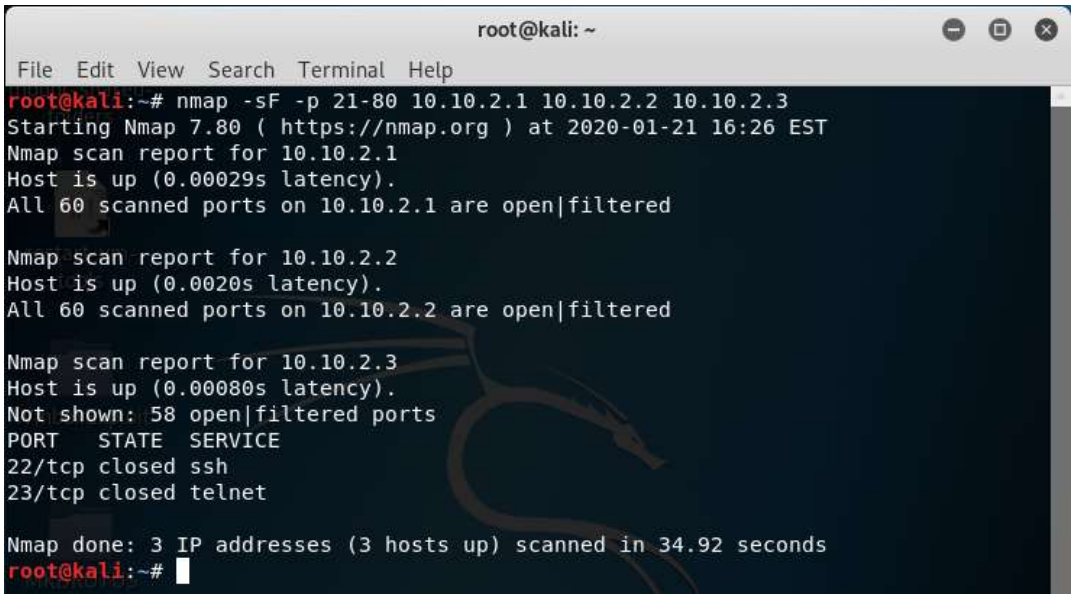


Figura 5.27: Escaneo TCP FIN fallido.

En la figura 5.28 se puede observar que se realiza un escaneo TCP Xmas, desde el puerto 21 hasta el 80, pero no se obtiene información.

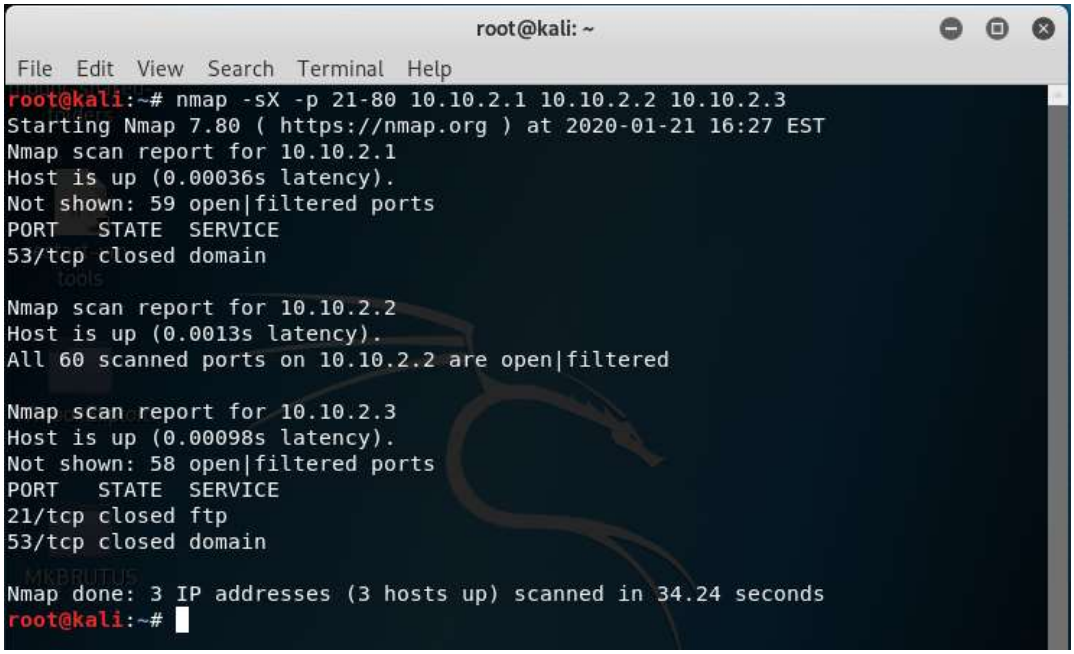


Figura 5.28: Escaneo TCP Xmas fallido.

Las reglas de firewall también bloquean escaneos UDP, pero se debe cambiar (Protocol: 6(tcp)) por (Protocol: 17(udp)).

En la figura 5.29 se realiza un escaneo UDP, desde el puerto 21 hasta el 80, pero no se obtiene información.

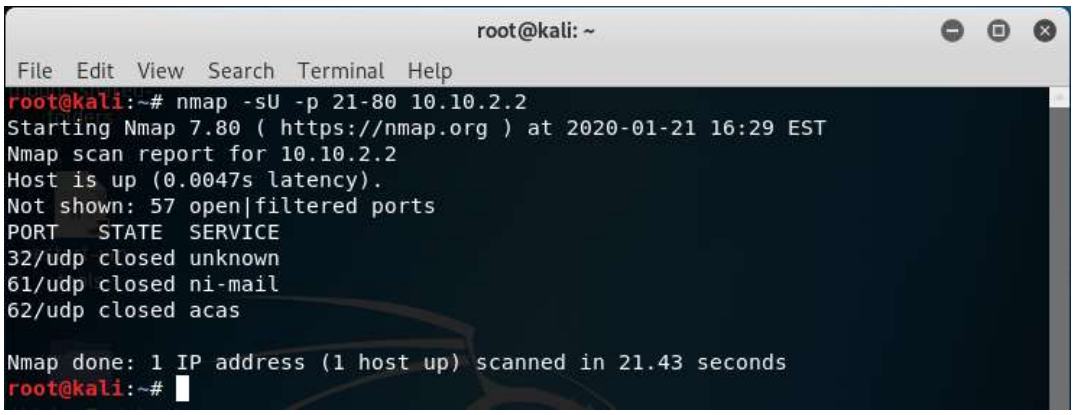


Figura 5.29: Escaneo UDP fallido.

En la figura 5.30 se verifica que, cuando se realiza cualquiera de estos escaneos, se agrega la dirección IP del atacante a la lista Port Scanner y se bloquea todo tipo de comunicación proveniente de la misma.

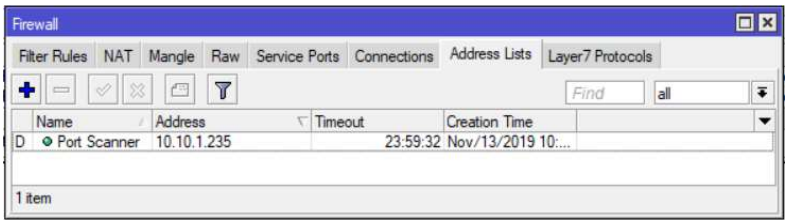


Figura 5.30: Lista de bloqueo Port Scanner.

5.3. Seguridad de capa 2

5.3.1. Validaciones

Defensa contra falsificación de direcciones MAC

Las configuraciones de seguridad de puertos están activadas en el switch y se realizó el cambio de dirección MAC en el host del atacante. La nueva dirección MAC pertenece a la PC1.

Se procede a realizar ping a la PC2 desde el host del atacante para que se sobrescriba la información en la tabla de direcciones MAC.

En la figura 5.31 se verifica que no se puede realizar ping desde el host del atacante.

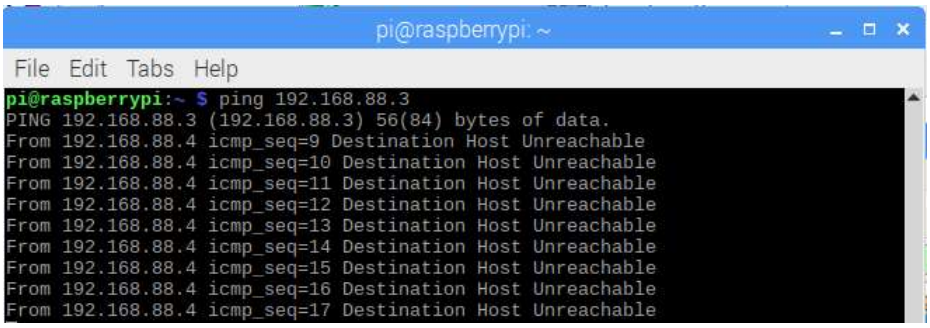


Figura 5.31: Ping fallido desde el host del atacante.

En la figura 5.32 se comprueba que, en el switch, no se registra ninguna dirección MAC para el puerto donde está conectado el atacante (Puerto 4).

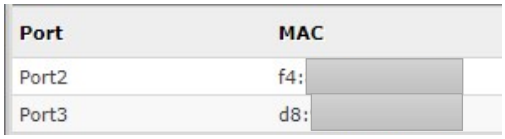


Figura 5.32: Tabla de direcciones MAC del switch.

Defensa contra tormenta de LAN

Se configuró RSTP en los puertos del switch.

Se realiza un bucle en el switch, conectando el puerto 1 y el puerto 5 con el mismo cable.

En la figura 5.33 se verifica que, en la pestaña Statistics, las tasas de transmisión y recepción de los puertos disminuyen.

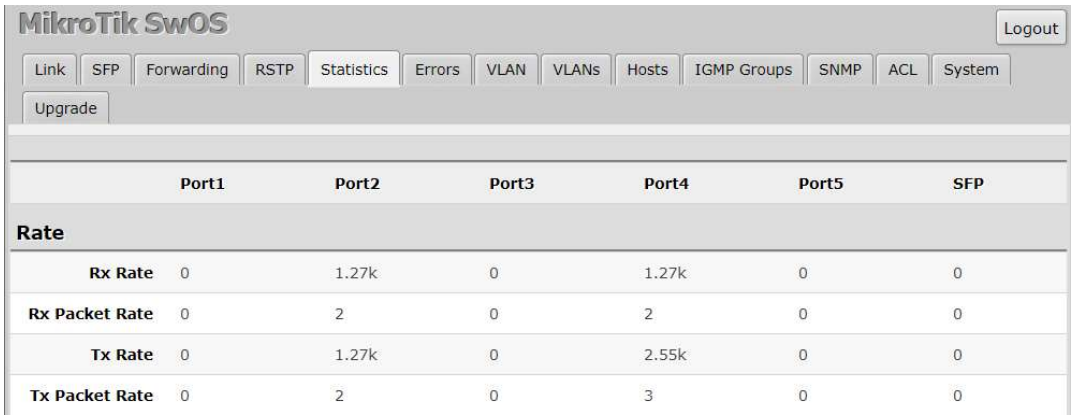


Figura 5.33: Tasas de transmisión y recepción de los puertos.

En la figura 5.34 se comprueba que puede comunicarse la PC2 con la PC1.

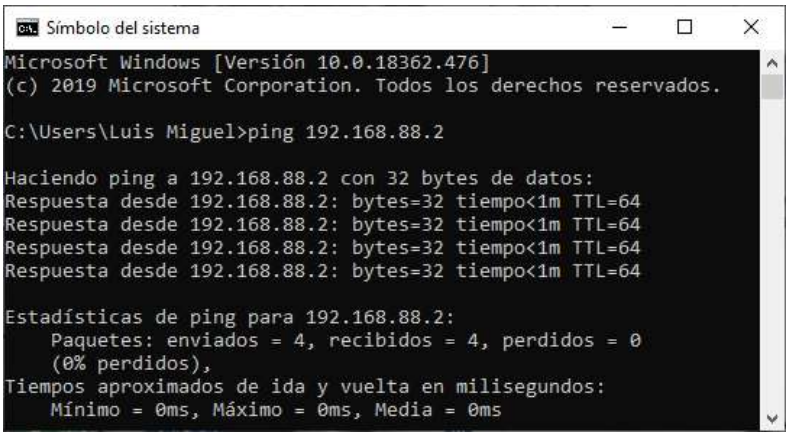
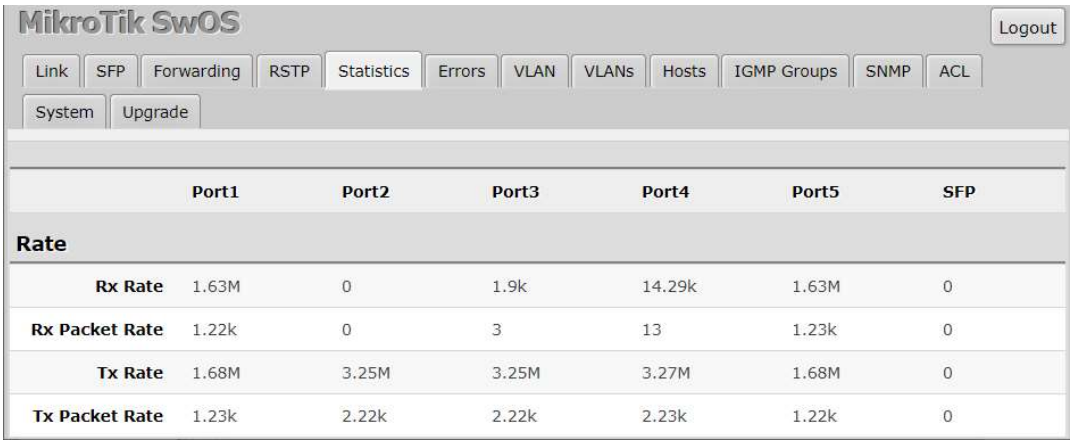


Figura 5.34: Intento de comunicación entre la PC2 y la PC1.

Se deshabilita RSTP y se activan las configuraciones para limitar el ancho de banda.

En la figura 5.35 se puede observar que, en la pestaña Statistics, las tasas de transmisión y recepción se mantienen por debajo del límite establecido (5 Mbps).



	Port1	Port2	Port3	Port4	Port5	SFP
Rate						
Rx Rate	1.63M	0	1.9k	14.29k	1.63M	0
Rx Packet Rate	1.22k	0	3	13	1.23k	0
Tx Rate	1.68M	3.25M	3.25M	3.27M	1.68M	0
Tx Packet Rate	1.23k	2.22k	2.22k	2.23k	1.22k	0

Figura 5.35: Tasas de transmisión y recepción de los puertos.

Defensa contra manipulación STP

Se configuró BPDU Guard en las interfaces destinadas para hosts.

Se conecta nuevamente el switch del atacante en la red redundante.

En la figura 5.36 se puede ver que, en la ventana Bridge y la pestaña Bridge, se puede ingresar a las configuraciones del switch 3. En la pestaña Status se puede observar que este switch se mantiene como el puente raíz.

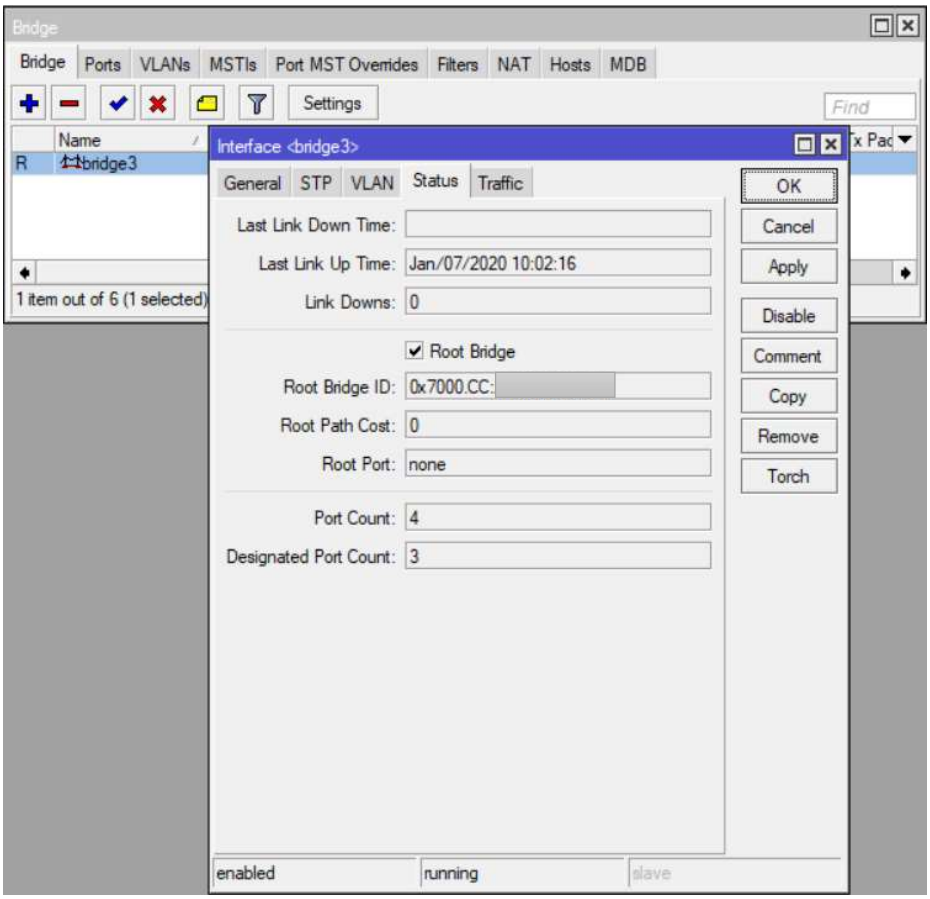


Figura 5.36: Pestaña Status del switch 3.

Como se puede notar en la figura 5.37, en la ventana Bridge y la pestaña Ports se encuentra desactivado el puerto 4 donde está conectado el switch del atacante.

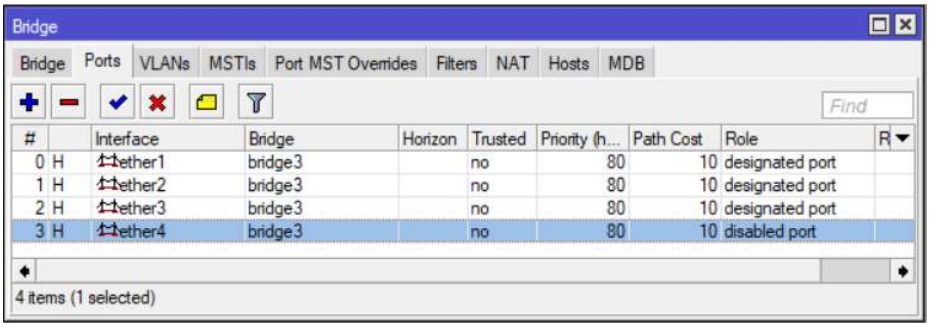


Figura 5.37: Estado de puertos.

Defensa contra VLAN hopping

Se aplicaron las configuraciones de seguridad del enlace troncal en los 2 switches y se realiza nuevamente el doble etiquetado con Yersinia.

En la figura 5.38, utilizando Wireshark, se comprueba que la PC3 no recibe los datos enviados por el atacante.

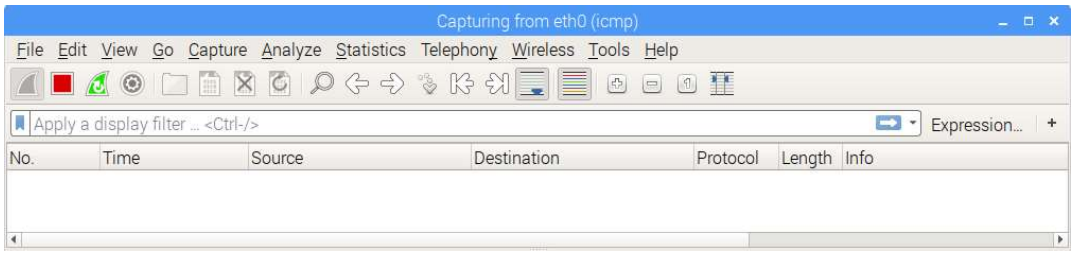


Figura 5.38: Captura de datos, mediante Wireshark, en la PC3.

5.4. Túnel IPsec

5.4.1. Validaciones

ESP en lugar de AH

Como protocolo IPsec, se configuró ESP en lugar de AH.

Se realiza ping desde la PC1 a la PC2.

En la figura 5.39 se analiza el tráfico, utilizando Wireshark, desde la computadora del atacante. Se comprueba que, con el protocolo ESP, no se puede visualizar la información de la comunicación entre las 2 computadoras.

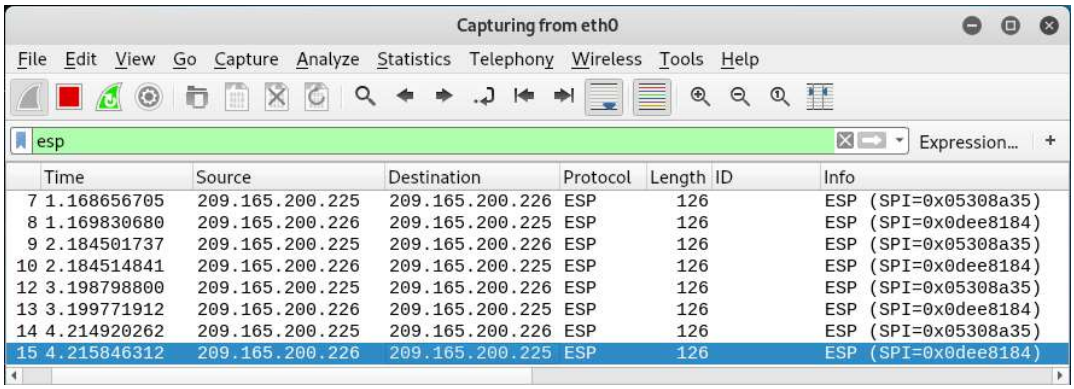


Figura 5.39: Análisis de tráfico del protocolo ESP.

Defensa contra ataque de contraseña fuera de línea

Se configuró el modo main en lugar del modo aggressive para la fase 1 de IKE.

Desde la computadora del atacante se intentan capturar los datos.

Cain & Abel no detecta los datos de la fase 1 en modo main, como se puede ver en la figura 5.40.

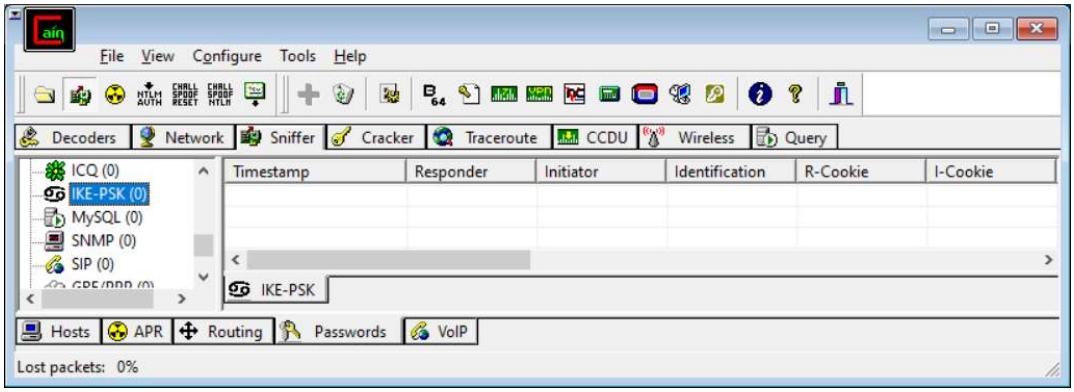


Figura 5.40: Pestaña Sniffer de Cain & Abel.

En la figura 5.41, mediante Wireshark, se capturan los paquetes generados en la fase 1.

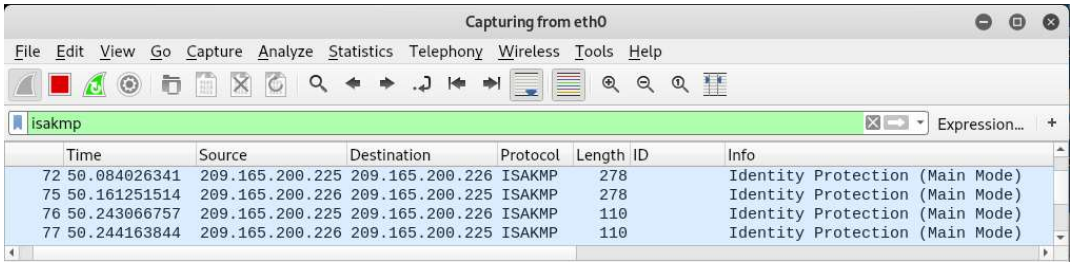


Figura 5.41: Captura de paquetes de la fase 1 mediante Wireshark.

En la figura 5.42 se comprueba que los datos, que se utilizan para la autenticación, están encriptados.

Figura 5.42: Información encriptada de la autenticación.

5.5. Conclusiones

Se comprobó que las configuraciones de seguridad permiten mitigar los ataques realizados en las redes de pruebas. En muchos casos se sacrifican recursos y velocidad en los equipos para poder brindar seguridad.

6. CONCLUSIONES

Siempre se deben utilizar servicios seguros, ya que encriptan la información.

No sirve de mucho utilizar servicios seguros si no se utilizan contraseñas seguras. Algunas recomendaciones, para la generación de contraseñas, son:

- En una contraseña nunca se deben utilizar nombres de personas, nombres de animales, sucesiones de números, frases, etc. debido a que los diccionarios contienen este tipo de palabras comunes.
- Las contraseñas deben ser largas para impedir que un ataque de fuerza bruta pueda generarlas en poco tiempo.

Bloquear las direcciones IP que tienen varios intentos fallidos de autenticación permite contrarrestar los ataques de contraseña.

Algunas buenas prácticas para la protección de servicios son:

- Permitir el acceso al router solo desde las direcciones IP de la red que tenga los privilegios para administrar los equipos.
- Cambiar los puertos por defecto.

Los fabricantes de dispositivos, constantemente, actualizan los sistemas operativos para corregir errores, vulnerabilidades, etc. por lo que es muy importante instalar la última versión.

Muchos servicios como el acceso por MAC, Neighbor Discovery, Bandwidth server, etc. son útiles al momento de las configuraciones iniciales de los dispositivos de red y deben ser desactivados cuando la red esté operando.

Se deben activar solo los servicios que se van a utilizar.

El límite del número de nuevas conexiones sucesivas en el router puede variar dependiendo del tamaño de la red, del tipo de servidor, etc. Para establecer este límite se debe realizar un análisis del tráfico normal dentro de la red. En este caso, como ejemplo, se colocó un valor de 150.

Con las reglas de firewall se mitiga el ataque SYN-FLOOD, pero la carga del CPU se mantiene en un valor alto. Vale recalcar que las pruebas se realizaron en un router que no tiene prestaciones muy altas, por lo que un router más potente podrá tolerar esta carga sin sacrificar demasiados recursos del CPU.

Se comprobó que el servidor es vulnerable a un ataque SYN FLOOD con una velocidad relativamente baja (100 p/s) y que las configuraciones de seguridad mitigaron un ataque realizado a la más alta velocidad posible (27138 p/s).

Algunas configuraciones requieren de un reinicio en el router para surtir efecto.

Comprobar en los paquetes, que las direcciones IP de origen corresponden a las interfaces por las cuales ingresan, permite mitigar el SPOOFING.

Reverse Path Forwarding obliga al atacante a utilizar direcciones IP que correspondan a la interfaz donde está conectado.

Las configuraciones de seguridad contra el SPOOFING permiten solventar una vulnerabilidad que tenían las configuraciones que mitigan el SYN FLOOD, por lo que se recomienda utilizarlas en conjunto.

Las configuraciones realizadas con PSD permiten hasta 3 conexiones con puertos bien conocidos diferentes. Estos límites se establecen como un umbral para no bloquear tráfico legítimo. Debido a esto, se obtiene información limitada de la red cuando se realizan ataques como los de las figuras 5.23, 5.24 y 5.25.

Los parámetros de PSD pueden variar dependiendo de la red donde se implemente esta seguridad.

En el caso de los ataques de las figuras 5.26, 5.27 y 5.28, no se obtuvo información debido a las configuraciones de banderas en los paquetes. PSD las detectó inmediatamente como intento de escaneo.

Está técnica es vulnerable a escaneos lentos debido al valor Delay Threshold, sin embargo, se ralentizará al atacante.

Descubrir que alguien está realizando un escaneo de puertos permitirá estar alerta ante otros posibles ataques.

Una solución más drástica sería agregar directamente a la lista Port Scanner las direcciones IP que traten de conectarse a puertos cerrados.

Para bloquear el descubrimiento de hosts se tendrían que bloquear ciertos mensajes del protocolo ICMP (como echo), sin embargo, no es recomendable en todos los casos ya

que esta es una herramienta útil para comprobación de errores y diagnósticos dentro de una red.

Debido a que el switch utilizado no se puede configurar mediante un servicio seguro como SSH o Winbox, se debe considerar desactivar los permisos de configuración en el puerto que se vaya a conectar a un router y por consiguiente a internet.

El proceso de aprendizaje del switch no es seguro, debido a que un atacante puede aprovecharlo para interceptar los datos destinados a un host legítimo de la red.

Realizar la configuración estática de direcciones MAC, en sus respectivos puertos de conexión, permite mitigar ataques de falsificación de direcciones MAC.

Si el atacante intenta reiniciar el switch, las configuraciones de seguridad en puertos no se borrarán.

Una tormenta de broadcast pueden consumir todos los recursos de una red, por lo que se puede utilizar como ataque de denegación de servicios.

Los protocolos STP y RSTP permiten que no se generen bucles de capa 2 y por consiguiente evitan que se produzcan tormentas de broadcast.

Limitar el ancho de banda en los puertos permite disminuir los efectos provocados por tráfico excesivo en la red.

Las prestaciones del switch, utilizado en las pruebas, son limitadas, por lo que en algunas pruebas se utilizó un router configurado como bridge.

Utilizando BPDU Guard se evita que ingresen BPDUs por las interfaces destinadas para hosts. Esto garantiza que no se pueda modificar el puente raíz conectándose en estas interfaces.

La VLAN nativa solo se debe utilizar en puertos troncales y no en puertos de acceso, ya que un atacante puede valerse de esto para enviar información a cualquier VLAN de la red.

Los puertos, que no se utilicen, deben asignarse a una VLAN que tampoco se utilice en la red.

Desactivar los puertos no utilizados es una de las mejores prácticas de seguridad.

IPsec permite implementar seguridad, sin embargo, pueden presentarse vulnerabilidades si no se configura correctamente.

El protocolo AH no encripta la información, por lo que no garantiza la confidencialidad. Se recomienda utilizar ESP en su lugar ya que esté si encripta la información.

El modo aggressive de la fase 1 de IKE es más rápido, pero menos seguro ya que la información, relacionada con la autenticación, se envía sin encriptar y puede ser capturada por un atacante para realizar ataques de contraseña fuera de línea. Se recomienda utilizar el modo main que, aunque sea más demorado, encripta la información relacionada con la autenticación.

Si se desea utilizar PSK como método de autenticación, la configuración de contraseñas fuertes es muy importante para que los ataques de contraseña no tengan éxito.

PFS es una característica de seguridad que obliga a la fase 2 de IKE a generar nuevas llaves de encriptación que sean totalmente independientes de las llaves de la fase 1. De esta forma si se comprometen las llaves de la fase 1, la encriptación de la fase 2 se mantendrá segura.

Muchos algoritmos de encriptación, hashing y grupo DH ya no se consideran seguros, por lo que es necesario mantenerse actualizado acerca de la información sobre los algoritmos que se recomienden en la actualidad.

Se pueden utilizar métodos más seguros de autenticación que PSK.

Existe una versión más moderna de IKE (IKEV2), que presenta algunas ventajas con respecto a la versión anterior.

Las configuraciones recomendadas permiten implementar seguridad, pero pueden tardar más en ejecutarse y consumir más procesamiento.

7. BIBLIOGRAFÍA

Andreatos, A. S. (2017). Designing educational scenarios to teach network security. *IEEE*, 1606 - 1610.

Ariganello, E. (2014). *Redes Cisco Guía de estudio para la certificación CCNA Security.* Ediciones de la U.

Baker, F., Cisco Systems, & Savola, P. (03 de 204). *RFC 3704.* Recuperado el 05 de 11 de 2019, de https://www.rfc-editor.org/rfc/pdfrfc/rfc3704.txt.pdf

BasuCert. (s.f.). *WinboxExploit*. (GitHub) Recuperado el 22 de 11 de 2019, de https://github.com/BasuCert/WinboxPoC

Chiu, S. (2006). *Seguridad en redes inalámbricas 802.11.* Recuperado el 31 de enero de 2019, de http://www. ciens. ucv. ve

CISCO. (17 de 10 de 2016). *Configuring SNMP*. (CISCO) Recuperado el 11 de 12 de 2019, de https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swsnmp.html

CISCO. (21 de 01 de 2018). *Configuring Internet Key Exchange for IPsec VPNs*. (CISCO) Recuperado el 08 de 02 de 2020, de https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ikevpn/configuration/xe-3s/sec-ike-for-ipsec-vpns-xe-3s-book/sec-key-exch-ipsec.html

CISCO. (02 de 09 de 2018). *Security for VPNs with IPsec Configuration Guide, Cisco IOS XE Release 3S*. (CISCO) Recuperado el 27 de 01 de 2020, de https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/xe-3s/sec-sec-for-vpns-w-ipsec-xe-3s-book/sec-cfg-vpn-ipsec.html

CISCO. (s.f.). *CCNA 1: Introduction to Networks.* CISCO.

CISCO. (s.f.). *CCNA 2: Routing and Switching Essentials.* CISCO. Recuperado el 27 de 11 de 2019, de https://juliorestrepo.files.wordpress.com/2015/03/pdf_ccna2_v5.pdf

CISCO. (s.f.). *CCNA 3: Scaling Networks.* CISCO.

CLOUDFLARE. (s.f.). *What is IP spoofing?* (CLOUDFLARE) Recuperado el 05 de 11 de 2019, de https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/

Criptografía. (07 de 02 de 2017). (Microsoft) Recuperado el 29 de 01 de 2020, de https://docs.microsoft.com/es-es/windows/uwp/security/cryptography

Cueva, H., Pozo, F., & Iturralde, D. (2016). Cross-platform Network Virtualization Software for MikroTik Devices. *IEEE*.

GNS3. (s.f.). *What is GNS3?* (GNS3) Recuperado el 24 de 11 de 2019, de https://gns3.com/software

Hart, T. (s.f.). *MikroTik Router Hardening.* Recuperado el 18 de 11 de 2019, de https://www.manitonetworks.com/networking/2017/7/25/mikrotik-router-hardening#neighbor-discovery

Hart, T. (s.f.). *Network Scanning With Nmap*. (Manito Networks) Recuperado el 10 de 11 de 2019, de https://www.manitonetworks.com/security/2016/11/26/network-scanning-with-nmap

Hat, R. (s.f.). *REVERSE PATH FORWARDING*. (Red Hat) Recuperado el 05 de 11 de 2019, de https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-server_security-reverse_path_forwarding

Higgins, B. (s.f.). *Routerboard Security.* Recuperado el 18 de 11 de 2019, de https://mum.mikrotik.com/presentations/UK18/presentation_6165_1539151116.pdf

INTEL. (s.f.). *Ancho de banda vs rendimiento vs velocidad vs tasa de conexión*. (INTEL) Recuperado el 19 de 11 de 2019, de https://www.intel.la/content/www/xl/es/support/articles/000026190/network-and-io/wireless-networking.html

Kali. (s.f.). *About Kali Linux*. (Kali) Recuperado el 04 de 11 de 2019, de https://www.kali.org/about-us/

Kali. (s.f.). *Hydra Package Description*. (Kali) Recuperado el 25 de 11 de 2019, de https://tools.kali.org/password-attacks/hydra

Kali. (s.f.). *Kali Tools*. (Kali) Recuperado el 20 de Octubre de 2019, de https://tools.kali.org/information-gathering/hping3

Kali. (s.f.). *Nmap Package Description*. (Kali) Recuperado el 11 de 10 de 2019, de https://tools.kali.org/information-gathering/nmap

Kali. (s.f.). *Yersinia Package Description*. (Kali) Recuperado el 02 de 01 de 2020, de https://tools.kali.org/vulnerability-analysis/yersinia

Lipták, B., & Eren, H. (2012). *Process Software and Digital Networks.* Boca Raton: CRC Press.

Marsá-Maestre, I., de la Hoz, E., Giménez-Guzmán, J. M., & López-Carmona, M. (2012). Using a scenario generation framework for education on system and internet security. *IEEE*.

maslinux. (08 de 02 de 2018). *¿Que es Kali GNU/Linux?* (maslinux) Recuperado el 04 de 11 de 2019, de https://maslinux.es/que-es-kali-gnu-linux/

Mikrotik. (25 de 03 de 2018). *CVE-2018-14847 WINBOX VULNERABILITY*. (Mikrotik) Recuperado el 11 de 21 de 2019, de https://blog.mikrotik.com/security/winbox-vulnerability.html

Mikrotik. (s.f.). *Bruteforce login prevention*. (Mikrotik) Recuperado el 26 de 11 de 2019, de https://wiki.mikrotik.com/wiki/Bruteforce_login_prevention

Mikrotik. (s.f.). *DoS attack protection*. (Mikrotik) Recuperado el 20 de 10 de 2019, de https://wiki.mikrotik.com/wiki/DoS_attack_protection

Mikrotik. (s.f.). *Drop port scanners*. (Mikrotik) Recuperado el 11 de 11 de 2019, de https://wiki.mikrotik.com/wiki/Drop_port_scanners

Mikrotik. (s.f.). *MAC access*. (Mikrotik) Recuperado el 19 de 11 de 2019, de https://wiki.mikrotik.com/wiki/MAC_access

Mikrotik. (s.f.). *Manual:Interface/Bridge*. (Mikrotik) Recuperado el 16 de 12 de 2019, de https://wiki.mikrotik.com/wiki/Manual:Interface/Bridge

Mikrotik. (s.f.). *Manual:IP/Cloud*. (Mikrotik) Recuperado el 19 de 11 de 2019, de https://wiki.mikrotik.com/wiki/Manual:IP/Cloud

Mikrotik. (s.f.). *Manual:IP/Firewall/Filter*. (Mikrotik) Recuperado el 20 de 10 de 2019, de https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter

Mikrotik. (s.f.). *Manual:IP/IPsec*. (Mikrotik) Recuperado el 09 de 02 de 2020, de https://wiki.mikrotik.com/wiki/Manual:IP/IPsec#Internet_Key_Exchange_Protocol_.28IKE.29

Mikrotik. (s.f.). *Manual:Router AAA*. (Mikrotik) Recuperado el 18 de 11 de 2019, de https://wiki.mikrotik.com/wiki/Manual:Router_AAA

Mikrotik. (s.f.). *Manual:Securing Your Router*. (Mikrotik) Recuperado el 18 de 11 de 2019, de https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router

Mikrotik. (s.f.). *Manual:Switch Chip Features*. (Mikrotik) Recuperado el 13 de 12 de 2019, de https://wiki.mikrotik.com/wiki/Manual:Switch_Chip_Features#Port_Mirroring

Mikrotik. (s.f.). *Manual:Tools/Ping*. (Mikrotik) Recuperado el 19 de 11 de 2019, de https://wiki.mikrotik.com/wiki/Manual:Tools/Ping#Mac_Ping

Mikrotik. (s.f.). *Manual:Upgrading*. (Mikrotik) Recuperado el 09 de 12 de 2019, de https://wiki.mikrotik.com/wiki/Manual:Upgrading

Mikrotik. (s.f.). *Manual:Winbox*. (Mikrotik) Recuperado el 06 de 11 de 2019, de https://wiki.mikrotik.com/wiki/Manual:Winbox

Mikrotik. (s.f.). *Neighbor discovery*. (Mikrotik) Recuperado el 19 de 11 de 2019, de https://wiki.mikrotik.com/wiki/Manual:IP/Neighbor_discovery

Mikrotik. (s.f.). *SwOS/CSS106*. (Mikrotik) Recuperado el 07 de 12 de 2019, de https://wiki.mikrotik.com/wiki/SwOS/CSS106

Molenaar, R. (s.f.). *IPsec (Internet Protocol Security)*. (NetworkLessons.com) Recuperado el 09 de 02 de 2020, de https://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security

Nmap. (s.f.). *Nmap Network Scanning.* Recuperado el 11 de 11 de 2019, de https://nmap.org/man/es/man-port-scanning-basics.html

Patel, A., Ghaghda, S., & Nagecha, P. (2014). Model for security in wired and wireless network for education. *IEEE*, 699 - 704.

Pauzhi, W., & Coronel, J. (2015). Seguridad para WISP mediante equipos MikroTik. *IEEE*, 229 - 233.

Pitts, S. (29 de 01 de 2004). *VPN Aggressive Mode Pre-shared Key Brute Force Attack.* Recuperado el 10 de 02 de 2020, de https://www.giac.org/paper/gcih/541/vpn-aggressive-mode-pre-shared-key-brute-force-attack/104625

Postel, J. (09 de 1981). *RFC792.* Recuperado el 10 de 11 de 2019, de https://www.rfc-editor.org/rfc/pdfrfc/rfc792.txt.pdf

PWGen. (s.f.). *Generator of cryptographically-strong passwords*. (PWGen) Recuperado el 26 de 11 de 2019, de http://pwgen-win.sourceforge.net/

RAPID7. (s.f.). *What is Metasploitable? How does it work?* (RAPID7) Recuperado el 27 de 10 de 2019, de https://information.rapid7.com/metasploit-framework.html

Rendek, L. (06 de 01 de 2017). *How to change MAC address using macchanger on Kali Linux*. (LINUXCONFIG) Recuperado el 05 de 12 de 2019, de https://linuxconfig.org/how-to-change-mac-address-using-macchanger-on-kali-linux

Rong-sheng, S., Xiao-yong, L., & LI, J.-h. (2004). An Adaptive Algorithm to Detect Port Scans. *Journal of Shanghai University, 8*(3), 328-332.

Roschke, S., Willems, C., & Meinel, C. (2010). A security laboratory for CTF scenarios and teaching IDS. *IEEE*.

Rouse, M. (s.f.). *brute force attack*. (SearchSecurity) Recuperado el 26 de 11 de 2019, de https://searchsecurity.techtarget.com/definition/brute-force-cracking

Rouse, M. (s.f.). *dictionary attack*. (SearchSecurity) Recuperado el 25 de 11 de 2019, de https://searchsecurity.techtarget.com/definition/dictionary-attack

Spurgeon, C. E. (2000). *Ethernet: the definitive guide.* USA: O'Reilly Media, Inc.

Stallings, W. (2004). *FUNDAMENTOS DE SEGURIDAD EN REDES. APLICACIONES Y ESTÁNDARES.* Madrid: PEARSON EDUCACIÓN.

Stevens, M., Bursztein, E., Karpman, P., Albertini, A., Markov, Y., Petit Bianco, A., & Baisse, C. (23 de 02 de 2017). *Announcing the first SHA1 collision*. (Google Security Blog) Recuperado el 11 de 02 de 2020, de https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html

Takeuchi, M. (s.f.). *MikroTik Security: The Forgotten Things.* Recuperado el 18 de 11 de 2019, de https://mum.mikrotik.com/presentations/KH19/presentation_6616_1548304246.pdf

Tanenbaum, A., & Wetherall, D. (2012). *REDES DE COMPUTADORAS.* México: PEARSON EDUCACIÓN.

Ternero, M. (s.f.). *Seguridad en redes y protocolos asociados.* Recuperado el 31 de enero de 2019, de http://www.dte.us.es/personal/mcromero/docs/ip/tema-seguridad-IP.pdf

Trotter, G., & Agilent Technologies. (12 de 2001). *RFC 3222.* Recuperado el 05 de 11 de 2019, de https://www.rfc-editor.org/rfc/pdfrfc/rfc3222.txt.pdf

UCF. (21 de 09 de 2015). *The VPN gateway must use ESP tunnel mode for establishing secured paths to transport traffic between the organization's sites or between a gateway and remote end-stations.* (UCF) Recuperado el 11 de 02 de 2020, de https://www.stigviewer.com/stig/ipsec_vpn_gateway/2015-09-21/finding/V-30964

UCF. (21 de 09 de 2015). *The VPN gateway must use IKE main mode for the purpose of negotiating an IPSec security association policy when pre-shared keys are used for authentication*. (UCF) Recuperado el 11 de 02 de 2020, de https://www.stigviewer.com/stig/ipsec_vpn_gateway/2015-09-21/finding/V-30957

UCF. (27 de 11 de 2018). *The VPN gateway must specify Perfect Forward Secrecy during IKE negotiation.* (UCF) Recuperado el 11 de 02 de 2020, de

https://www.stigviewer.com/stig/ipsec_vpn_gateway/2018-11-27/finding/V-30960

UCF. (08 de 03 de 2018). *The VPN gateway must use a key size from Diffie-Hellman Group 14 or larger during IKE Phase 1.* (UCF) Recuperado el 11 de 02 de 2020, de https://www.stigviewer.com/stig/ipsec_vpn_gateway/2018-03-08/finding/V-30959

UCF. (08 de 03 de 2018). *The VPN gateway must use AES for IPSec cryptographic encryption operations required to ensure privacy of the IPSec session.* (UCF) Recuperado el 11 de 02 de 2020, de https://www.stigviewer.com/stig/ipsec_vpn_gateway/2018-03-08/finding/V-30966

UCF. (08 de 03 de 2018). *The VPN gateway must use Secure Hash Algorithm for IPSec cryptographic hashing operations required for authentication and integrity verification.* (UCF) Recuperado el 11 de 02 de 2020, de https://www.stigviewer.com/stig/ipsec_vpn_gateway/2018-03-08/finding/V-30967

UCF. (11 de 02 de 2020). *The VPN gateway must use a key size from Diffie-Hellman Group 14 or larger during IKE Phase 2.* (UCF) Recuperado el 08 de 03 de 2018, de https://www.stigviewer.com/stig/ipsec_vpn_gateway/2018-03-08/finding/V-30963

WIRESHARK. (s.f.). *About Wireshark*. (WIRESHARK) Recuperado el 04 de 11 de 2019, de https://www.wireshark.org/

Zavarsky, P., Butakkov, S., & Hlyne, C. (2015). SCAP Benchmark for Cisco Router Security. *IEEE*, 270 - 276.