UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERÍA

CARRERA DE SISTEMAS Y COMPUTACIÓN

Proyecto de Investigación previo a la obtención del título de Ingeniero en Sistemas y Computación

TRABAJO DE TITULACIÓN

APLICACIÓN DE TÉCNICAS DE PENTESTING PARA DETERMINAR VULNERABILIDADES EN LA RED LAN DE LA EMPRESA CSEDNET DE SANTO DOMINGO

AUTOR:

Jairo Alexander Vera Correa

TUTOR:

Ing. Marlon Silva., MSc.

Riobamba - Ecuador

Año 2020

VEREDICTO DE LA INVESTIGACIÓN

Los miembros del tribunal de Graduación del proyecto de investigación de título: "**APLICACIÓN DE TÉCNICAS DE PENTESTING PARA DETERMINAR VULNERABILIDADES EN LA RED LAN DE LA EMPRESA CSEDNET DE SANTO DOMINGO**", presentado por el Sr. Jairo Alexander Vera Correa, dirigido por el MSc. Marlon Javier Silva Castañeda.

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación escrito, con fines de graduación en el cual se ha constatado el cumplimiento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la Facultad de Ingeniería de la UNACH.

Para constancia de lo expresado firman:

MSc. Marlon Silva

Tutor del Proyecto Firma

PhD. Paola Vinueza

Miembro del Tribual Firma

MSc. Danny Velzaco

Miembro del Tribual Firma

AUTORÍA DE LA INVESTIGACIÓN

La responsabilidad del contenido de este proyecto de investigación corresponde exclusivamente a: Jairo Alexander Vera Correa, autor del proyecto de investigación, bajo la dirección del MSc. Marlon Javier Silva Castañeda y al patrimonio intelectual de la Universidad Nacional de Chimborazo.

Jairo Alexander Vera Correa
1724094667
Autor

MSc. Marlon Javier Silva Castañeda
0602260598
Director del Proyecto

AGRADECIMIENTO

En primer lugar, deseo expresar mi más profundo agradecimiento a mis padres Olger y Liliana por el apoyo incondicional que me han brindado y por sus consejos ante las adversidades que surgieron en el camino cuando se empezó a realizar este trabajo y que gracias a eso pude llegar a cumplir hoy un sueño más.

Así mismo a mi tutor el MSc. Marlon Silva y a mis colaboradores: MSc. Danny Velasco y PhD Paola Vinueza por la dedicación, apoyo y dirección que han brindado a este proyecto de grado.

A mis maestros por haberme proporcionado todo el conocimiento necesario y también por su valiosa amistad ya que no solo fueron un soporte en el ámbito educativo, sino que también inculcando valores éticos y morales. Gracias por toda la confianza ofrecida desde el momento que llegue a esta carrera.

Finalmente, a mi alma Mater la Universidad Nacional de Chimborazo por permitirme formar parte de este prestigioso centro de educación superior.

Jairo Alexander Vera Correa

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El objetivo de esta investigación es identificar las vulnerabilidades que tiene la red LAN de la empresa CSEDnet de Santo Domingo, por medio de la aplicación de las pruebas de pentesting: sniffing y parameter tampering, para que, en base a los problemas encontrados, poder generar políticas de seguridad y aplicarlas en la infraestructura y los principales equipos activos de la red LAN. Con este fin, la pregunta de investigación es la siguiente: ¿Cómo la implementación de un plan de aseguramiento de la información y redes mitigará las infiltraciones no deseadas en la empresa CSEDnet? En este contexto la seguridad informática es un aspecto muy importante a tomar en cuenta para las empresas que como mínimo, usan y poseen redes LAN para desarrollar sus actividades laborales, ya que la información que se transmite por esta red es de vital importancia para quienes forman parte de la institución y de sus clientes.

Se utilizó las fases de la metodología CEH (Certified Ethical Hacker) denominada Metodología de evaluación de vulnerabilidad de red, para identificar puntos débiles en los nodos de la infraestructura LAN de la empresa CSEDnet de la ciudad de Santo Domingo. Esta metodología se encuentra dentro de la certificación CEH, que otorga el Consejo Internacional de Consulta de Comercio Electrónico (EC-Council). La evaluación de la vulnerabilidad de la red es un examen de las posibilidades de un ataque a una red.

Los resultados señalan una gran disminución de los paquetes capturados (98,62%), después de la implementación de las políticas de seguridad planteadas en esta investigación.

Palabras clave: Pentesting, sniffing, parameter tampering, CEH, LAN.

ABSTRACT

The objective of this research is to identify the vulnerabilities that the LAN network of the company CSEDnet from Santo Domingo has through the application of the pentesting tests: sniffing and parameter tampering, so that, based on the problems found, to be able to generate policies security and apply them in the infrastructure and the main active equipment of the LAN network. To this end, the research question is the following: How will the implementation of an information and network assurance plan mitigate unwanted infiltrations in the CSEDnet company?

In this context, computer security is a very important aspect to take into account for companies that, at a minimum, use and have LAN networks to develop their work activities, since the information that is transmitted through this network is of vital importance for those who form part of the institution and its clients.

The phases of the CEH (Certified Ethical Hacker) methodology called Network Vulnerability Assessment Methodology were used to identify weak points in the nodes of the LAN infrastructure of the CSEDnet company in the Santo Domingo city. This methodology is within the CEH certification granted by the International Electronic Commerce Consultation Council (EC-Council). The Network Vulnerability Assessment is an examination of the possibilities of an attack on a network.

The results indicate a great decrease in the captured packets (98.62%), after the implementation of the security policies proposed in this research.

Keywords: Pentesting, sniffing, parameter tampering, CEH, LAN.

Reviewed by:
Dra. Nelly Moreano Ojeda
ENGLISH PROFESSOR
c.c. 1801807288

INTRODUCCIÓN

La implementación de una infraestructura LAN (Local Area Network) basada en políticas, siempre ha sido un desafío para los organismos corporativos que han diversificado las situaciones de la red para manejarse con recursos limitados, especialmente en presencia de servidores con seguridad de firewall. En la era competitiva de hoy, el éxito de una organización depende únicamente de la protección de los recursos involucrados en la informática. Las intrusiones son enemigos silenciosos que pueden golpear a cualquier organización sin previo aviso. Si bien estas amenazas pueden pasar desapercibidas hasta que causen desastres operativos, no existe una cura única para las amenazas de seguridad de la organización. (Balogh, 2018)

Según el estudio de la web de Kaspersky para julio del 2020, Ecuador está en la posición número 48 de los países más atacados por ciber amenazas, es el primer país de América del Sur con más amenazas web con un 13.74%, el quinto que recibe más ataques a redes con un 8.25% siendo los principales ataques: intrusión con un 13.48% y Fuerza Bruta con 1.99%. (Kaspersky, 2018)

Aun así, la tecnología de la información y comunicación no es vista como un factor importante para el desempeño y crecimiento de las empresas. Por lo que las diferentes formas de ataques que se pueden presentar, y que afectan al correcto funcionamiento de la infraestructura de tecnología (redes inalámbricas), es conocida por los profesionales de TI, pero al no contar con herramientas adecuadas, hace que esta continúe siendo propensa a ataques y que la información sea vulnerada. (Chuquitarco, 2018)

Cuando la red se ve comprometida podría tener consecuencias muy graves, como pérdida de privacidad, robo de información o ilegibilidad. Para hacer la situación aún más compleja, los tipos de amenazas de ataques a la seguridad de la red están en constante evolución. El sniffing es el proceso de capturar comunicaciones en la red. En la LAN, los atacantes usan configuraciones de tarjetas de red especiales en modo promiscuo, lo que asegurará la recepción de toda la comunicación. Esto hace que sea más fácil capturar, guardar o utilizar cualquier comunicación de red. Los atacantes usan herramientas especiales llamadas sniffer, para capturar paquetes de datos que contienen información confidencial como: contraseñas, información de cuentas bancarias y otros. (Balogh, 2018)

Los protocolos criptográficos son protocolos de comunicación que usan la criptografía, para lograr objetivos de seguridad como la discreción, la autenticación y el acuerdo en presencia de intrusos. Ejemplos de protocolos criptográficos conocidos son: SSL (Secure Sockets Layer) / TLS (Transport Layer Security) [DR06], IKEv2 [KHNE10] y Kerberos [NHR05], que pueden usarse, respectivamente, para proteger el tráfico basado en la web, configurar redes privadas virtuales y realizar autenticación en entornos distribuidos. Para garantizar que dichos protocolos siempre logren sus objetivos, están diseñados bajo el supuesto de que la red está completamente controlada por un adversario (también llamado intruso o atacante). Esto significa que el adversario puede interceptar, redirigir y alterar datos, tener acceso a cualquier operación que esté disponible para agentes legítimos, e incluso controlar uno o más agentes legítimos y así acceder a sus claves. Dada la hostilidad del entorno previsto, no es sorprendente que los protocolos criptográficos sean difíciles de diseñar y estén sujetos a fallas sutiles, incluso cuando las seguridades, como el cifrado y las funciones sospechosas, sean seguras. (Basin et al., 2018)

También existen protocolos de autenticación como el EAP (Extensible Authentication Protocol), que se encuentra dentro del protocolo de autenticación de PPP (Point-to-Point Protocol) y ofrece un marco generalizado para distintos métodos de autenticación. Con un EAP estandarizado, interoperabilidad y compatibilidad con métodos de autenticación, es más sencillo. IEEE 802.1X es el estándar para pasar el EAP por una LAN con cable o inalámbrica. (Molina, 2004)

A pesar de todo lo antes planteado, no hay una solución estándar de seguridad para las redes de datos, por lo que es necesario identificar los requisitos de seguridad que se quieren alcanzar y sobre la base de estos emplear los protocolos, combinándolos según las necesidades. (González, 2016)

CAPÍTULO I.

1. PLANTEAMIENTO DEL PROBLEMA

1.1. Problema y Justificación

Los delitos informáticos en el Ecuador van desde el fraude hasta el espionaje, los cuales son denunciados en la fiscalía; el internet abrió el paso a estas nuevas formas de delincuencia que ponen en riesgo la información privada, la seguridad en la navegación de los usuarios y la información de las instituciones públicas y privadas. La fiscalía general del estado registró 626 denuncias por delitos informáticos en el año 2014. Desde 10 de agosto del 2014 entra en vigor el Código Orgánico Integral penal, en cual se sanciona los delitos informáticos cuyos actos se cometen con el uso de tecnología, para violentar la confidencialidad y la disponibilidad de datos personales. (Fiscalía General del Ecuador, 2015)

Para el año 2019 según el Deloitte (Deloitte Touche Tohmatsu Limited) y la Fiscalía General del Estado, los datos proyectados fueron 359 casos de acceso no consentido a un sistema informático, telemático de telecomunicaciones, 131 casos de Ataque a la integridad de sistemas informáticos, 63 casos de Interceptación ilegal de datos y 68 casos de Revelación ilegal de base de datos. (Deloitte, 2020)

En la actualidad los ataques informáticos a empresas de los sectores: financiero, energético, petrolero y manufacturero, a instituciones estatales y a medios de comunicación, se han incrementado sustancialmente, pues han evolucionado al campo de crimen organizado, siendo el robo de información confidencial de las empresas, una de las amenazas informáticas más frecuentes. En Ecuador no se toma muy en cuenta la seguridad de TI, siendo que la misma es parte de los activos más importantes de la empresa. Actualmente la infraestructura de red LAN la empresa CSEDnet cuenta con un aseguramiento en cuanto a protección de redes se refiere, pero no se ha sometido a una auditoria informática o pruebas de penetración a la red, por tanto, pueden existir vulnerabilidades que no se tomaron en cuenta al momento de implementar las medidas de seguridad, entonces es necesario protegerlo de amenazas internas y externas.

¿Cómo la implementación de un plan de aseguramiento de la información y redes mitigará las infiltraciones no deseada en la empresa CSEDnet? como ya se ha expresado

anteriormente, esta empresa de la ciudad de Santo Domingo cuenta con un aseguramiento de la información y de las redes que se han implementado, pero no se había realizado auditorias ni pruebas de penetración sobre la red LAN, entonces, en vista de que toda la información que viene de internet pasa por los nodos de la empresa, y se distribuye a los clientes en sus hogares, cualquier persona ajena a la institución inescrupulosa y con conocimientos en intrusión de redes, podría ingresar a la misma, sustraer información y hasta modificarla, por eso fue necesario realizar un análisis de la infraestructura que está siendo utilizada en la empresa, para identificar las vulnerabilidades que no se tomaron en cuenta, y tratar de eliminarlas o al menos mitigar estos riesgos que en un futuro podrían causar grandes problemas a la institución.

Se cuenta con muchas herramientas de análisis y de intrusión a redes para identificar vulnerabilidades, así como metodologías y técnicas que dan pautas para realizar dicho análisis, contando con el apoyo de los directores del departamento de tecnologías de la información la empresa CSEDnet, y las facilidades que pudieron ofrecer para desarrollar el proyecto de investigación, se contó con toda la viabilidad técnica para realizar el proyecto.

Con el estudio se consiguió tener una solución a la problemática de falta de contramedidas y salvaguardas, identificadas por medio de un pentesting en cuanto al aseguramiento de las redes LAN de la empresa CSEDnet, todo esto para evitar tener problemas de fuga de datos o infiltraciones no deseadas a la infraestructura de red, y a la información de la institución. Tomando en cuenta que la investigación presentó sus resultados mediante la información agregada y no de manera individual, gracias a esto se respetó la confidencialidad y toda cuestión ética.

1.2. Objetivos

1.2.1 Objetivo General

Aplicar técnicas de pentesting para determinar vulnerabilidades en la red LAN de la empresa CSEDnet de Santo Domingo.

1.2.2. Objetivos Específicos

- Estudiar las técnicas de pentesting denominadas sniffing y parameter tampering para identificar riesgos de seguridad informática relacionados con la red LAN.
- Ejecutar pruebas de penetración basadas en las técnicas estudiadas y la metodología de CEH para diagnosticar las vulnerabilidades que podría afectar la integridad de la red LAN.
- Evaluar la implementación de políticas de seguridad sobre la infraestructura y los principales equipos activos de la red LAN.

CAPÍTULO II.

2. MARCO TEÓRICO

2.1. Redes de Internet

Una red de computadoras, también llamada red de ordenadores o red informática es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.), servicios (acceso a internet, e-mail, chat, juegos), etc.

Las redes de área local y las redes inalámbricas se utilizan ampliamente en aeropuertos, empresas (distribuidoras de internet), escuelas, tiendas, etc. Hoy en día, las redes están creciendo muy rápido en los sectores antes mencionados. Por lo que la seguridad (especialmente la autenticación) es un problema vital debido a que el medio inalámbrico está disponible para todos en espacios abiertos. Los usuarios de la red de hoy en día aspiran a tener una seguridad estricta y un buen rendimiento (Pandey et al., 2016).

2.1.1. Tipos de Redes

Por el alcance:

- **Red de área personal (PAN)** conecta computadoras y periféricos en un área reducida, dentro de una casa u hogar.
- **Red de área local (LAN)** conecta computadoras y periféricos en un área que no supera los 200 m^2, dentro de un edificio.
    - **Redes LAN Cliente- servidor** están basadas en una computadora (generalmente la más grande) que auspicia de servidor, y las demás funcionan como clientes de éste. Los clientes comparten recursos a través del servidor. Los recursos pueden ser tanto archivos de datos como periféricos. En general hay solamente un servidor, pero puede haber más; en todo caso, cada servidor estará dedicado a un área específica.
    - **Las redes LAN Punto a punto,** o redes igualitarias, posibilitan que todas las computadoras integradas de la red actúen como clientes o como servidores no dedicados, De ese modo, todas pueden compartir los

recursos disponibles en la red. Estas redes son más económicas y flexibles que las redes cliente-servidor.

- **CAN (Red de área de campus)** conecta computadoras y periféricos en un área geográfica limitada, como in campo militar o universitario.
- **MAN (Red de área metropolitana)** conecta computadoras y periféricos en un área geográfica amplia, ciudad o provincia.
- **WAN (Red de área amplia)** conecta computadoras y periféricos en un área geográfica muy amplia, países y continentes.

Por el método de la conexión:

- **Medios guiados:** cable coaxial, cable de par trenzado, fibra óptica y otros tipos de cables.
- **Medios no guiados:** radio, infrarrojos, microondas, láser y otras redes inalámbricas.

Por el acceso de sus usuarios:

- **Red pública:** una red pública se define como una red que puede usar cualquier persona. Es una red de computadoras interconectadas, capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica.
- **Red privada:** una red privada se definiría como una red que puede usarla solo algunas personas y que están configuradas con clave de acceso personal. (Andrew et al., 2014)

2.1.2. Nodos de Red

En una red de comunicaciones, un nodo de red es un punto de conexión que puede recibir, crear, almacenar o enviar datos a lo largo de rutas de red distribuidas. Cada nodo de la red ya sea un punto final para la transmisión de datos o un punto de redistribución, tiene una capacidad programada o diseñada para reconocer, procesar y reenviar transmisiones a otros nodos de la red.

El concepto de nodos de red surgió con el uso de redes distribuidas y conmutación de paquetes. Dependiendo de su aplicación, los nodos de red realizan una variedad de funciones. (WifiMesh, 2020)

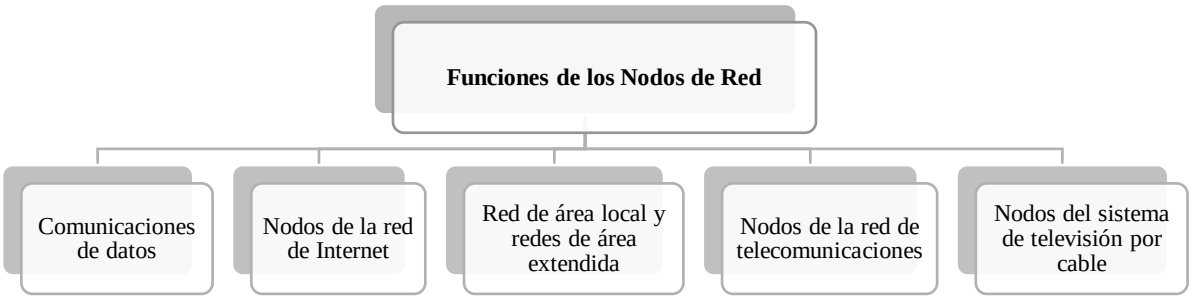


Figura 2.1. Funciones de los Nodos de Red
Elaborado por: El autor

2.2. Ataques a la red

Dado que las capas son comunes en redes cableadas e inalámbricas, la mayoría de los ataques en la red cableada también funcionan contra las inalámbricas. Sin embargo, debido a las características de los enlaces de radio, localizar un hacker o una máquina infectada siempre es difícil en una LAN. Por lo tanto, es más vulnerable al sniffing, ataque de fuerza bruta, gusanos y troyanos. (Bhatia et al., 2012)

2.3. Análisis del Riesgo del Sistema de Información

El análisis de riesgo a nivel empresarial es una excelente herramienta para generar planes de contingencia y continuidad del negocio, debido a que permite a las empresas mitigar el riesgo y garantizar el rendimiento de los sistemas informáticos. Cabe resaltar que es imposible eliminar un riesgo en su totalidad, lo que se puede hacer con la implementación de metodologías es reducirlo para que no genere ningún daño representativo al sistema informático de la organización. (Tejena, 2018)

2.4. El Riesgo Informático

Se entiende como la gestión de riesgo Informático, a la probabilidad de ocurrencia de incidentes que causen la paralización a los Sistemas Informáticos o de la red de comunicación, de forma que imposibilite el cumplimento de un objetivo o ponga en peligro a los bienes de la Organización, ocasionando de esta manera pérdidas o daños económicos irreversibles.

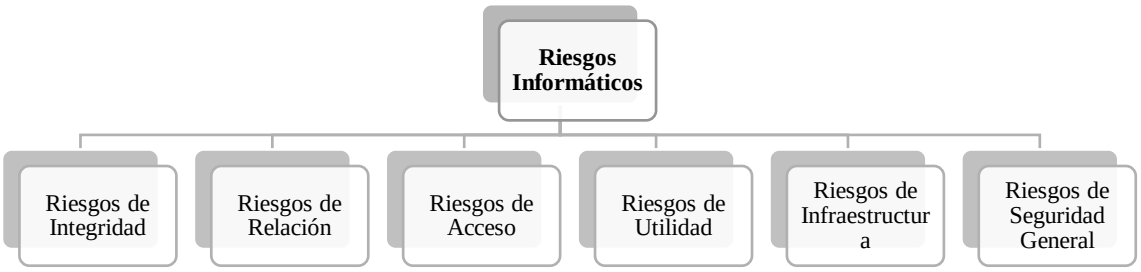


Figura 2.2. Riesgos Informáticos
Elaborado por: El autor

La Organización Internacional por la Normalización (ISO) define el riesgo tecnológico como: "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños" (ISO/IEC, 2004). Otras de las normativas con una madurez para la definición del riesgo es la de origen Australiana y Nueva Zelandia AS/NZS 4360:2004 que lo define como "Posibilidad de que un suceso tenga un impacto en los objetivos" (AS/NZS 4360:2004), normativa que ha sido incorporada y actualizada internacionalmente como ISO 31000:2009, aplicada mundialmente y que define al riesgo como: "efecto de la Incertidumbre en los objetivos" (ISO 31000:2009).

2.4.1. Características

En el análisis de riesgo es importante reconocer que cada proceso de riesgo tiene características, tales como:

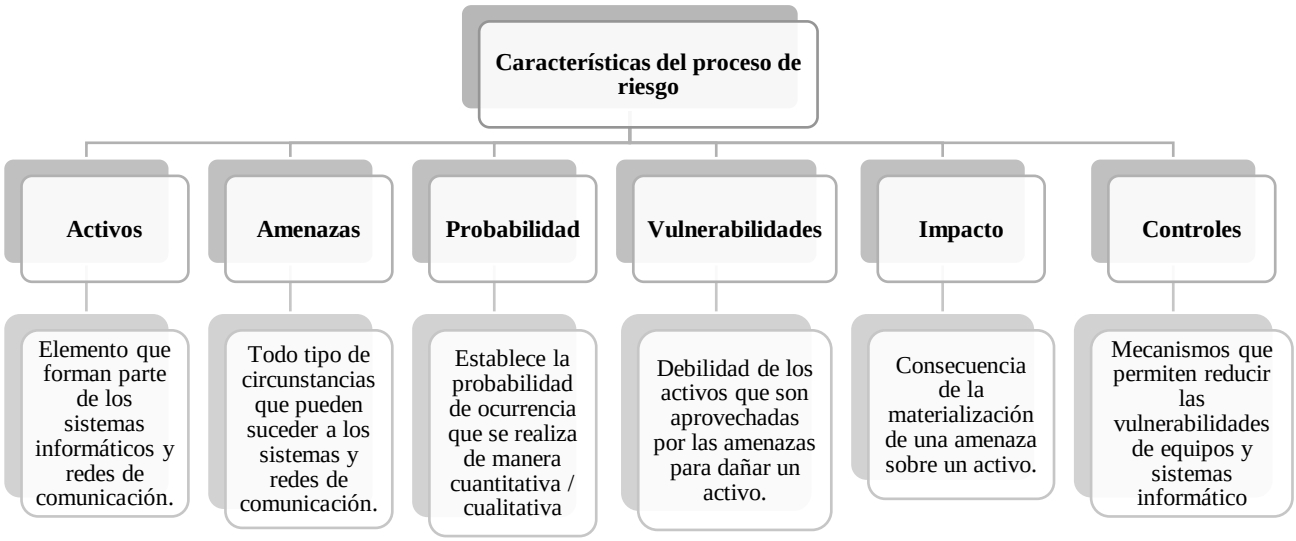


Figura 2.3. Características del proceso de riesgo
Elaborado por: El autor

2.5. Clasificación de Riesgo de TI (Tecnología de la Información)

Según el ambiente en el que se desenvuelve la empresa u organización investigada se puede identificar y relacionar los cuatro siguientes tipos de riesgo:

- **Riesgo Inherente:** Es la posibilidad de errores o irregularidades en la información financiera, administrativa u operativa, antes de considerar la efectividad de los controles internos diseñados y aplicados por la institución.
- **Riesgos Financieros:** Es todo lo relacionado a la parte financiera de la entidad, dicho riesgo se relaciona con el manejo de los recursos de la empresa.
- **Riesgo Operativo:** Comprende tanto el riesgo en sistemas como operativos provenientes de deficiencias en los sistemas de información, procesos, estructura, que conducen a ineficiencias, oportunidad de corrupción o incumplimiento de los derechos fundamentales.
- **Riesgos Tecnológico:** Riesgo que se asocia con la capacidad tecnológica disponible por la entidad, con el objetivo de satisfacer sus necesidades actuales, futuras y de soporte al cumplimiento de su misión.

2.5.1. Tipos de Ataques

En la investigación denominada Ataques en redes de datos IPv4 e IPv6 elaborado por Reyes (2017), existen varias técnicas de ataques informáticos tanto a nivel de aplicación como de red, estas son algunas de ellas:

Footprinting

El footprinting también conocido como reconocimiento, es una técnica que permite recopilar la mayor cantidad de información sobre el sistema informático o red, y sobre los dispositivos que están conectados a esta red. Algunos de los pasos para realizar esta técnica son:

- Mapeo de la Red
- Identificación de dispositivos activos
- Identificación de sistemas operativos
- Escaneo de puntos de acceso
- Escaneo de puertos abiertos
- Etc.

Toda información, por pequeña o poco relevante que sea, se debe tener en cuenta para formar la estructura del objetivo. Para esto existen herramientas como Maltego que nos da una forma muy visual de organizar la información y poder extraer los datos sensibles con técnicas de minería de datos.

Figura 2.4. Footprinting
Elaborado por: El autor

Sniffing

El concepto de sniffing se puede considerar uno de los más básicos una vez acabado el footprinting. Traducido literalmente como oler u olfatear, el sniffing es una técnica que se basa en capturar todo el tráfico de red que pasa por un equipo, siempre y cuando su tarjeta de red esté configurada en modo promiscuo.

El tráfico capturado nos permite interceptar la comunicación, pero sin intervenir en absoluto ya que ese no es el propósito de esta técnica. Los sniffers se pueden utilizar para realizar tareas lícitas dentro de una red, como pueden ser:

- Administrar y gestionar la información que pasa a través de una red LAN.
- Realizar auditoría de redes.
- Identificar estabilidad y vulnerabilidades de las redes LAN.
- Verificar el tráfico de una red y monitorear su desempeño.
- Prevenir actividades de espionaje industrial.
- Monitorear las actividades de los usuarios de una red.
- Identificar paquetes de datos.

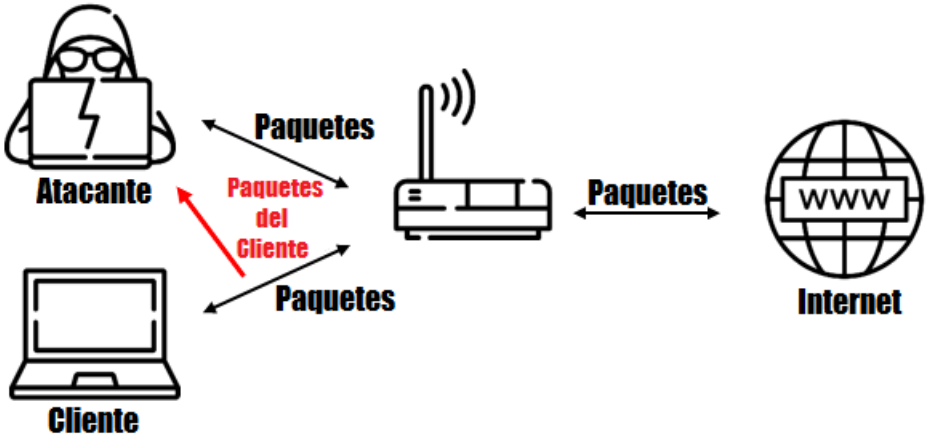


Figura 2.5. Sniffing
Elaborado por: El autor

Spoofing

Se denomina spoofing a la suplantación de identidad dentro de un sistema con el objetivo de recibir información que se intercambia entre dos sistemas distintos. En el sentido estricto spoofing identifica todas aquellas técnicas enfocadas a la suplantación, como pueden ser MAC (Media Access Control) spoofing o ARP (Address Resolution Protocol) Spoofing.

En el spoofing entran en juego tres máquinas: atacante, víctima y un sistema suplantado. Para que el atacante pueda conseguir su objetivo necesita, por un lado, establecer una comunicación falseada con su objetivo, y por otro lado evitar que el equipo suplantado interfiera en el ataque.

Dentro de los tipos de spoofing podemos encontrar los siguientes:

- IP (Internet Protocol) spoofing: suplantación de dirección IP
- ARP (Address Resolution Protocol) spoofing: suplantación de dirección MAC
- DNS (Domain Name System) spoofing: alteración de las direcciones IP en los servidores DNS para que apunten a servidores maliciosos
- E-mail spoofing: creación de mensajes de correo electrónico con una dirección de remitente falso
- Web spoofing: suplantación de una página web
- GPS (Global Positioning System) spoofing: suplantación de coordenadas geográficas

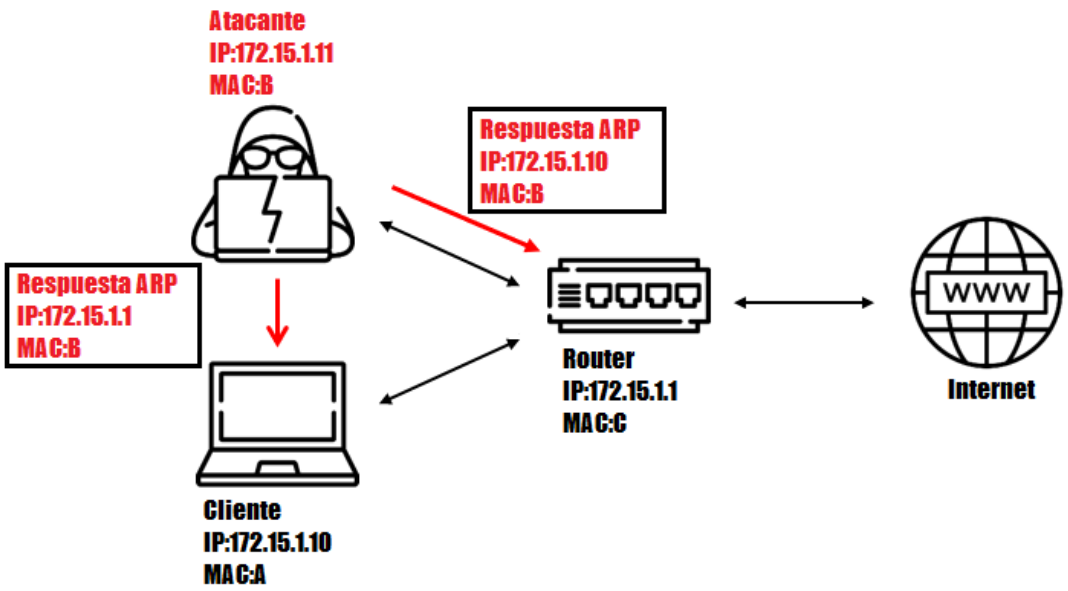


Figura 2.6. ARP Spoffing
Elaborado por: El autor

SQL Injection

Una inyección SQL consiste en la introducción de una consulta SQL a través de un punto de entrada para usuarios sin privilegios. Lo más común es pensaren una pantalla de acceso en un servidor web. Las inyecciones SQL, en el caso de ser ejecutadas correctamente, son capaces de realizar acciones CRUD sobre la base de datos que se halle detrás del servicio, ejecutar operaciones de administración e incluso llegar a ejecutar comandos del sistema operativo.

El ejemplo más sencillo es el de un formulario para acceder a un servicio:

- Suponiendo que existe un servicio tras el servidor que realiza la consulta "SELECT id FROM tabla WHERE user='usuario' and password='password'"
- La sentencia será correcta sintácticamente y será cierta si se dan las condiciones especificadas.
- No es posible impedir que el usuario escriba "'or '1'='1 ".
- La consulta "SELECT id FROM tabla WHERE user='usuario' and password=' 'or '1'='1'" sigue siendo sintácticamente correcta y lo que es más importante: también será verdadera, por lo que devolvería el atributo indicado sin problemas

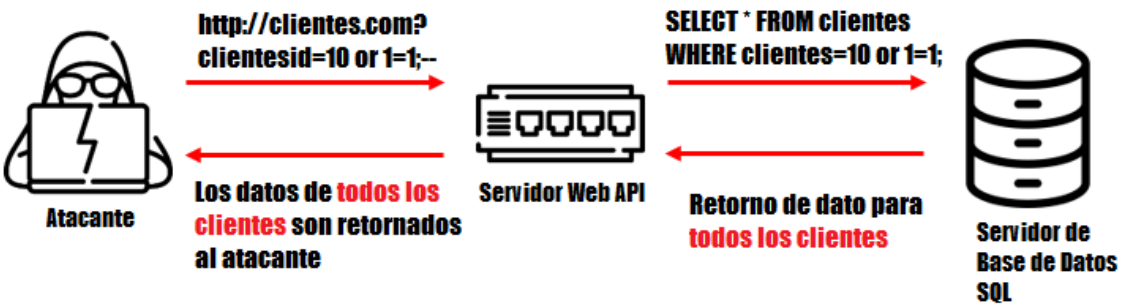


Figura 2.7. SQL Injection
Elaborado por: El autor

Parameter Tampering

Los servidores con vulnerabilidades de manipulación de parámetros están abiertos a una variedad de ataques (como permitir el acceso no autorizado, inyección de SQL, secuencias de comandos entre sitios). En la práctica, los vectores de ataque de manipulación de parámetros a veces surgen porque el desarrollador simplemente no se da cuenta de que las comprobaciones y los controles del cliente, también deben replicarse en el servidor. (Bisht et al., 2010)

Sin lugar a duda, estamos en presencia de un meta-ataque pues la manipulación de los parámetros es esencial para que los ciberdelincuentes puedan lograr sus objetivos.

El ataque consta de tres fases:

- El atacante captura una transacción HTTP normal de la aplicación web. Esta captura puede ser tan sencilla como disponer de un acceso como usuario de la aplicación web objetivo o un poco más elaborada como la realización de un ataque MitM.
- El ciber atacante modifica los parámetros de su interés en la aplicación web, ya sea en la URL, campos ocultos en formularios que son enviados como partes de peticiones POST, etc.
- Por último, realiza el envío de la petición modificada al servidor web, esperando lograr sus objetivos.

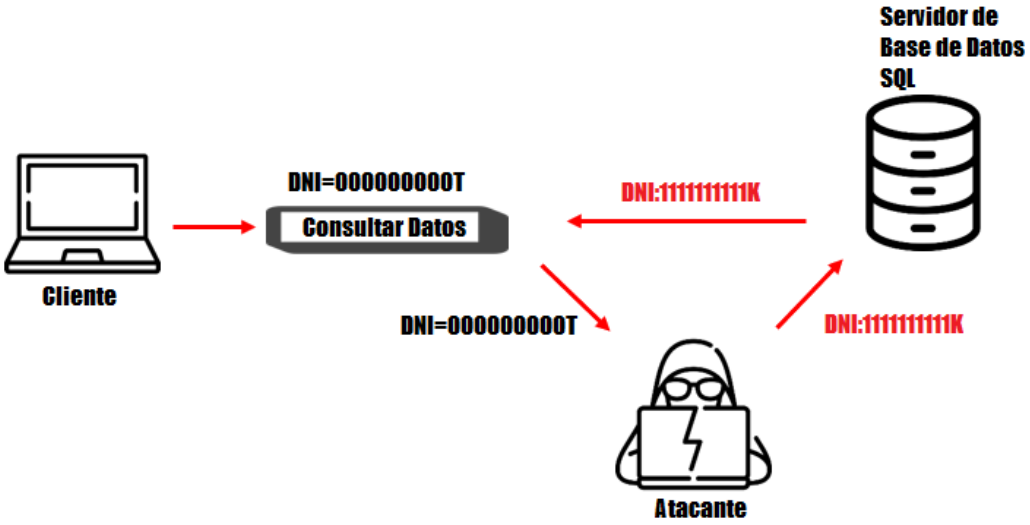


Figura 2.8. Parameter Tampering
Elaborado por: El autor

DoS/DDoS

Los ataques DoS/DDoS (Denegation of Service/Denegacion de Servicio) es un ataque dirigido por múltiples computadoras comprometidas llamadas bots o zombies que se enfocan en un solo sistema. Su motivación es hacer que el sistema objetivo o la red agote sus recursos mediante la inundación de peticiones, con el objetivo de que el servicio se vea obstaculizado o detenido, lo que lleva a la indisponibilidad del servicio.

Lo más común de interpretar es denegar el acceso a un servidor web, pero cada vez va tomando más relevancia los ataques a dispositivos móviles, sobre todo con el auge del Internet de las Cosas. (Dong et al., 2019)

El ataque DDoS se divide en siete clases notables que son:

- Ataque de inundación
- Ataque de amplificación
- Ataque de núcleo fundido
- Ataque
- Ataque TCP SYN
- Ataque de solicitud CGI
- Ataque al servidor de autenticación

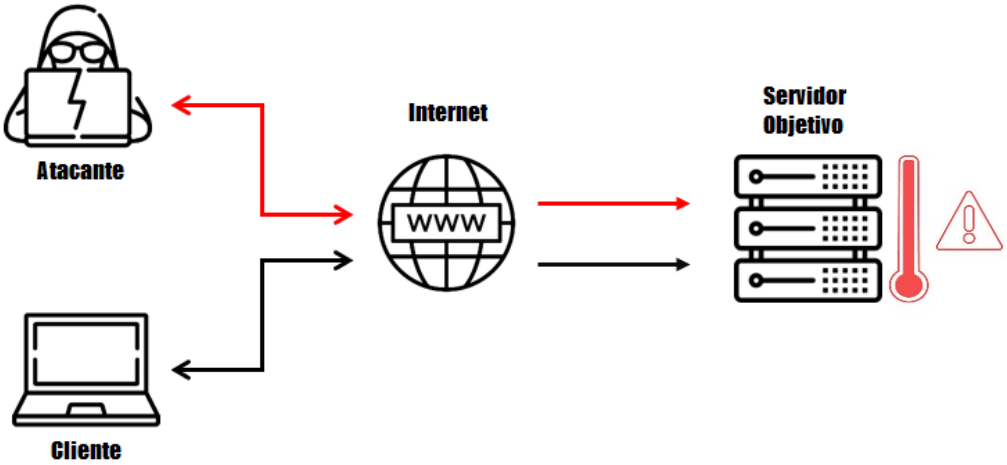


Figura 2.9. Denegation of Service
Elaborado por: El autor

2.6. Aseguramiento de las redes

Una LAN proporciona una comunicación fácil entre todas las computadoras conectadas a la red. Esta conectividad deja abierta a las computadoras, a ataques de personas malintencionadas en cualquier parte de la red. El tamaño creciente de las LAN modernas agrava las vulnerabilidades de seguridad. La capacidad de interconectar redes locales con dispositivos de enrutamiento y puente ha ampliado su conectividad, pero el desarrollo de mecanismos de seguridad para redes sigue progresando. (Krishna et al., 2019)

La seguridad informática pretende identificar las amenazas y reducir los riesgos, al detectar las vulnerabilidades, nulificando o minimizando así el impacto o efecto nocivo sobre la organización, por lo que es necesario el proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización. (Zambrano et al., 2017)

Las redes Wi-Fi, las cuales son un tipo de redes LAN, cuentan con una contraseña de seguridad, por esto, existen varias formas de asegurar una red mediante una clave. El WPA2 es el más reciente protocolo de encriptación y AES el algoritmo de cifrado más seguro. El estándar 802.11i establecido por la IEEE, está completamente implementado en el WPA2. El cambio principal que se realizó en el WPA2 sobre el WPA se relaciona con el algoritmo de cifrado de datos. El Protocolo modo contador con cifrado de mensajes de encadenamiento y Autenticación de código (CCMP) utiliza un cifrado de bloque que es el Estándar de cifrado avanzado (AES) para el cifrado de datos. Estos métodos o

técnicas de cifrado o criptografía mantienen un principio muy fuerte de seguridad de datos, pero si la clave secreta se conoce la mayoría de las veces, el sistema de cifrado se ve comprometido (Sari et al., 2015).

2.7. Hacking ético

El término Hacker ético se utiliza para referirse a profesionales que trabajan para identificar loopholes y vulnerabilidades en los sistemas, informarlo al propietario del sistema y, en ocasiones, ayudarlos a reparar el sistema. Las herramientas y técnicas utilizadas por un pirata informático ético son similares a las utilizadas por un pirata informático, pero el objetivo es diferente, ya que se utiliza de una manera más profesional. Los hackers éticos también se conocen como investigadores de seguridad.

Pero el término más profesional utilizado para describir lo que hace un hacker ético es Pentesting. La prueba de penetración es un subconjunto del hacking ético. Es una forma más ágil de identificar vulnerabilidades en los sistemas y descubrir si la vulnerabilidad es explotable o no. La prueba de penetración se rige por un contrato entre el pentester y el propietario del sistema que será puesto a prueba. Es importante definir el alcance de la prueba para identificar los sistemas que se probarán, de igual forma las Reglas de Compromiso, que determinan la forma en que se realizarán las pruebas. (Najera et al., 2018)

Aunque el pentesting no es malo, también es muy importante saber qué hacen exactamente para el interés de la sociedad. Si tratamos al hacker como la persona que impulsa la tecnología más allá de las normas percibidas, hay varios campos de la computación en los que el pentester y el hacker tienen un impacto importante. Hoy en día el internet se ha convertido en la puerta de entrada para que cualquier computadora se conecte a todo el mundo, lo que también lo hace vulnerable a los ataques de hackers desde cualquier parte. (Sánchez, 2019)

2.7.1. Fases del hacking ético

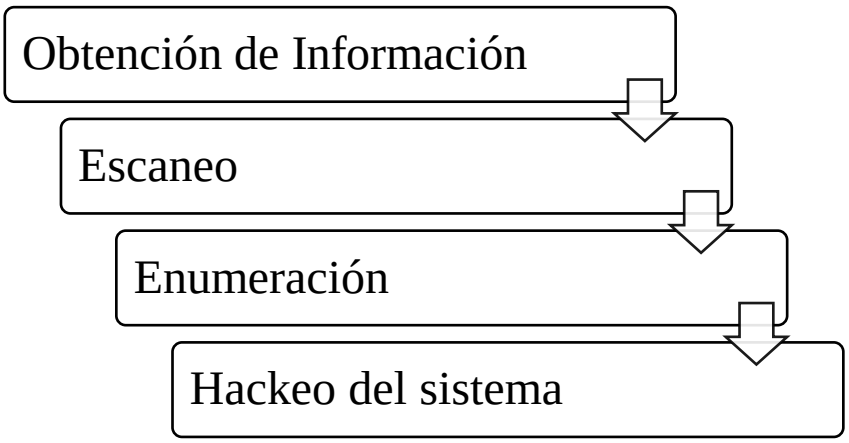


Figura 2.10. Fases del Hacking ético
Elaborado por: El autor

En la guía de estudio de Certified Ethical Hacker Version 9, existen 4 fases principales para la realización de una prueba de penetración según su creador Baloch, las cuales son las siguientes:

Fase 1: Obtención de Información (Footprinting)

Esta fase consiste en obtener información pasiva y activa sobre un objetivo. El fin es reunir tanta información como sea razonable y útil sobre un potencial objetivo, con el propósito de obtener suficiente información para que los ataques posteriores sean más precisos. El resultado final debe ser un perfil del objetivo que sea una imagen aproximada, pero que proporcione datos suficientes para planificar la próxima fase de escaneo.

La información que se puede recopilar durante esta fase incluye lo siguiente:

- Rangos de direcciones IP
- Espacios de nombres
- Información del empleado
- Números de teléfono
- Información de la instalación
- Información del trabajo

Fase 2: Escaneo

Se centra en una participación activa del objetivo, con la intención de obtener más información. El escaneo de la red de destino finalmente localizará hosts activos, que luego

pueden ser seleccionados en una fase posterior. La huella ayuda a identificar objetivos potenciales, pero no todos pueden ser anfitriones viables o activos. Una vez que la exploración determina qué hosts están activos y cómo se ve la red, puede tener lugar un proceso más refinado.

Durante esta fase se utilizan herramientas como estas:

- Pings
- Ping sweeps
- Escaneos de puertos
- Tracert

Fase 3: Enumeración

La enumeración es el sondeo sistemático de un objetivo, con el fin de obtener: listas de usuarios, tablas de enrutamiento y protocolos del sistema. Esta fase representa un cambio significativo en su proceso; es la transición inicial de estar afuera mirando hacia adentro, para moverse hacia el interior del sistema y recopilar datos. La información como recursos compartidos, usuarios, grupos, aplicaciones, protocolos y pancartas resultó útil para conocer a su objetivo, y esta información se lleva a la fase de ataque.

La información recopilada durante la fase 3 generalmente incluye, entre otros, lo siguiente:

- Nombres de usuario
- Información del grupo
- Contraseñas
- Acciones ocultas
- Información del dispositivo
- Diseño de red
- Información del protocolo
- Datos del servidor
- Servicio de información

Fase 4: Hackeo del sistema

Una vez que haya completado las primeras tres fases, puede pasar a la fase de hackeo del sistema. Hay que reconocer que las cosas se están volviendo mucho más complejas y que

la fase de hackeo del sistema no se puede completar de una sola vez. Implica un enfoque metódico que incluye descifrar contraseñas, escalar privilegios, ejecutar aplicaciones, ocultar archivos, cubrir pistas, ocultar pruebas y luego empujar a un ataque complejo.

2.7.2. Metodología de una prueba de penetración

En cada prueba de penetración, la metodología y los informes son los pasos más importantes. Existen varios tipos diferentes de metodologías de pruebas de penetración que abordan cómo se debe realizar una prueba de penetración, algunos de ellos son: OSSTMM (Open Source Security Testing Methodology Manual), CEH (Certified Ethical Hacker), NIST (National Institute of Standards and Technology), CVSS (Common Vulnerability Scoring System), PTES (Penetration Testing Execution Standard) y OWASP (Open Web Application Security Project), pero en general el existen 4 fases generales para realizar un pentesting. (Baloch, 2017)

Nombre	Características	Fases
OSSTMM (OSSTMM, 2018)	• Seguridad de la Información • Seguridad de los Procesos • Seguridad en las Tecnologías de Internet • Seguridad en las Comunicaciones • Seguridad Inalámbrica • Seguridad Física	• Fase de Inducción • Fase de Interacción • Fase de requerimientos • Fase de Intervención
CEH (CEH, 2012)	• Establecer y controlar estándares mínimos para la acreditación de especialistas profesionales en seguridad informática y ethical hacking. • Informar al público que las personas con credenciales cumplen o superan los estándares mínimos. • Reforzar el ethical hacking como una profesión única y autorregulada.	• Obtención de Información. • Obtención de acceso. • Enumeración. • Escala de privilegios. • Reporte
NIST (NIST, 2018)	• Describir la postura actual de ciberseguridad.	• Fase de Planificación • Fase de Descubrimiento • Fase de Ejecución

	• Describir el estado objetivo de ciberseguridad. • Identificar y priorizar oportunidades de mejora en el contexto de un proceso continuo y repetible. • Evaluar el progreso hacia el estado objetivo. • Comunicación entre las partes interesadas internas y externas sobre el riesgo de ciberseguridad.	• Fase de Documentación y Reporte
PTES (PTES, 2016)	• Evaluación de escaneo de servicios web • Seguridad Lighting • Mejorar la seguridad de las TI • Evaluar los riesgos de las vulnerabilidades de las TI • Seguridad en las Comunicaciones • Mayor administración de la infraestructura	• Preacuerdo • Recopilación de inteligencia • Modelado de amenazas • Análisis de vulnerabilidades • Explotación • Post explotación • Reporte
OWASP (OWASP, 2010)	• Pruebas de firma digital de aplicaciones Web. • Comprobaciones del sistema de autenticación. • Pruebas de Cross Site Scripting. • Polución de Parámetros • Cross Site Request Forgery	• Reconocimiento • Escaneo y Enumeración • Mantener Acceso • Cubrir Huellas

Tabla 2.1. Metodologías de Pentesting
Elaborado por: El autor

- **Metodología de evaluación de vulnerabilidad de red**

Esta metodología se encuentra dentro de la certificación CEH que otorga el Consejo Internacional de Consulta de Comercio Electrónico (EC-Council). La Evaluación de la vulnerabilidad de la red es un examen de las posibilidades de un ataque a una red. Las siguientes son las fases de la Evaluación de Vulnerabilidad: Adquisición, Identificación, Análisis, Evaluación y Generación de Reporte. (IPSpecialist, 2018)

- **Enfoques de evaluación de vulnerabilidad**

Las evaluaciones de vulnerabilidad tienen como objetivo, proporcionar a las organizaciones conocimientos sobre sistemas susceptibles a ataques cibernéticos. Hay cuatro pasos para realizar una evaluación de vulnerabilidad: (1) definir el alcance de la evaluación, (2) utilizar software para identificar vulnerabilidades, (3) analizar los informes generados por software y (4) intentar explotar el sistema utilizando las vulnerabilidades conocidas. (McMahon et al., 2017)

- **Evasión de vulnerabilidad**

El problema es que, aunque muchos de estos ataques son efectivos para obtener información y otros elementos de un objetivo, pueden ser detectados o frustrados. Las corporaciones ahora emplean muchas medidas defensivas, cada una con su propia forma de detener su ataque. Los sistemas de detección de intrusos (IDS), los sistemas de prevención de intrusos (IPS), los cortafuegos, los honeypots y otras defensas similares son obstáculos poderosos para sus actividades. Aunque estos dispositivos son formidables, no son insuperables. (Shimonski, 2016)

2.7.3. Tipos de pruebas de penetración

Se clasifican por el origen de las pruebas internas y externas:

- **Pruebas de penetración externas:** Se realizan desde lugares externos a las instalaciones de la organización. Se evalúan mecanismos perimetrales de seguridad informática.
- **Pruebas de penetración internas:** Se realizan dentro de las instalaciones de la organización para evaluar las políticas y mecanismos internos de seguridad de la organización.

Por el conocimiento de los objetivos este tipo de pruebas que se realizan son de caja negra, caja gris y caja blanca:

- **Pruebas de caja negra:** Las pruebas de caja negra implican la realización de una evaluación de la seguridad y pruebas sin conocimiento previo de la infraestructura o de la infraestructura de red a probar. La prueba simula un ataque de un hacker malicioso fuera del perímetro de seguridad de la organización.

- **Pruebas de caja blanca:** Las pruebas de caja blanca implican la evaluación de la seguridad y las pruebas son con conocimiento completo de la infraestructura de red, como un administrador de red podría hacer.
- **Pruebas de caja gris:** Las pruebas de caja gris implican la realización de la evaluación de la seguridad y pruebas internas. Las pruebas examinan el grado de acceso a información privilegiada dentro de la red. El propósito de esta prueba es para simular las formas más comunes de ataque, los que se inician desde dentro de la red. La idea es poner a prueba o auditar el nivel de acceso de los empleados, o contratistas y ver si esos privilegios se pueden escalar a un nivel superior. (Ruiz, 2018)

2.8. Herramientas que se usaron en las pruebas de Pentesting

Wireshark

Wireshark es el analizador de protocolos de red más importante y ampliamente utilizado en el mundo. Permite ver lo que sucede en una red a nivel microscópico y es el estándar de facto (y a menudo de iure) en muchas empresas comerciales y sin fines de lucro, agencias gubernamentales e instituciones educativas. El desarrollo de Wireshark prospera gracias a las contribuciones voluntarias de expertos en redes de todo el mundo y es la continuación de un proyecto iniciado por Gerald Combs en 1998. ("Wireshark · Go Deep.", 2020)

OWASP ZAP

OWASP Zed Attack Proxy es una herramienta integrada para realizar pruebas de penetración, la cual permite encontrar vulnerabilidades en las aplicaciones web.

Ha sido diseñada para ser utilizada por personas con diversa experiencia en seguridad, siendo también ideal para desarrolladores y personas quienes realizan pruebas funcionales, y nuevos en temas de pruebas de penetración.

ZAP proporciona escáneres automáticos como también un conjunto de herramientas para encontrar de manera manual vulnerabilidades en seguridad.

Entre sus características más importantes se tiene que; es open source, multiplataforma, fácil de instalar, completamente libre, fácil de utilizar, incluye páginas completas de ayuda, está traducido a 20 lenguajes y se basa en una comunidad con desarrollo muy activo. (Caballero, 2016)

CAPÍTULO III.

3. METODOLOGÍA

Con la investigación documental se realizó un estudio que proporcionó el conocimiento y la información necesaria para evaluar la problemática planteada en este trabajo. En este caso, con el fin de identificar amenazas potenciales que podrían afectar el correcto funcionamiento de la red LAN y de los dispositivos que se utilizan en la empresa CSEDnet.

Se debe contemplar el hecho de que, para realizar un estudio, es muy importante la utilización de metodologías, por esta razón para el desarrollo de la investigación, se optó por utilizar la Metodología CEH denominada Metodología de evaluación de vulnerabilidad de red, la cual es una metodología de pentesting o también conocido como hacking ético.

Posterior al uso de la metodología se empleó también técnicas para realizar la penetración y el análisis de la red, tomando en cuenta que el uso de las técnicas está contenido dentro de la implementación de la metodología, pero en este caso se han especificado dos, las cuales son: sniffing y paramenter tampering.

3.1. Tipo de Estudio

3.1.1. Según el objeto de estudio

Con la utilización de la Investigación Aplicada, se pudo identificar amenazas y vulnerabilidades potenciales que podrían afectar el correcto funcionamiento de la red LAN, así como la saturación del ancho de banda que ha sido asignado a los nodos que distribuyen el servicio de internet a los hogares. Se aplicaron metodologías y técnicas de pentesting, esto ayudó a tener un control de las actividades que se realizaron además de que permitió seguir ciertos pasos prestablecidos para la ejecución de las pruebas. La metodología de CEH (Certified Ethical Hacker) fue una guía importante que ayudó al proceso de puesta en marcha del proyecto, todo esto enmarcado en el uso de herramientas de software libre.

3.1.2. Según nivel de medición y análisis de la información

Por medio de la Investigación Descriptiva se efectuó un análisis de los problemas que puede sufrir la red LAN durante un ataque, en este caso un ataque simulado de sniffing y parameter tampering.

3.1.3. Según las variables

Esta investigación se considera Cuasi experimental ya que se ejecutaron pruebas de penetración a la red LAN en varios escenarios, aplicando técnicas y metodologías de pentesting con la ayuda del sistema operativo de software libre Parrot OS, en el cual se encuentran las herramientas que se utilizaron en el estudio, las cuales fueron: Wireshark y OWASP ZAP. Con los que se logró evidenciar los peligros a los que está expuesta la infraestructura de red por la falta de contramedidas y salvaguardas identificadas mediante el uso del pentesting, para que de esta forma se pueda comprobar la hipótesis de la investigación.

3.2. Operacionalización de variables

Variable	Tipo	Definición Conceptual	Dimensión	Indicadores
Técnicas de Pentesting: sniffing y parameter tampering.	Independiente	Es la práctica de atacar diversos entornos con la intención de descubrir vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques internos o externos hacia los equipos o sistemas.	Obtención de Información y Exploración Análisis y Explotación de vulnerabilidades Contramedidas	• Evaluar los nodos que se encuentran enlazados a la red LAN de acuerdo con la información obtenida. • Emplear técnicas y herramientas de pentesting para analizar y evaluar las vulnerabilidades y las políticas de seguridad. • Disminuir el número de ataques e infiltraciones no deseadas proponiendo políticas de seguridad.
Aseguramiento la red LAN de la empresa CSEDnet de la ciudad de Santo Domingo.	Dependiente	La seguridad en las redes está basada principalmente en dos aspectos: el cifrado de los datos que se transmiten a través de ella y la autenticación entre los diversos usuarios de la red.	Ataques Puntos débiles	• Nivel de vulnerabilidad del sistema a ataques de tipo parameter tampering. • Número de nodos vulnerables a ataques de tipo sniffing. • Número de vulnerabilidades encontradas.

Tabla 3.1. Variables
Elaborado por: El autor

3.3. Procedimientos de la metodología CEH

Se utilizó las fases de la metodología CEH (Certified Ethical Hacker) denominada Metodología de evaluación de vulnerabilidad de red, para identificar puntos débiles en los nodos de la red LAN de la empresa CSEDnet de la ciudad de Santo Domingo.

3.3.1. Obtención de Información (Adquisición)

Tanto el reconocimiento pasivo como activo pueden contribuir a la obtención de información. Este paso es fundamental para el éxito de las pruebas de penetración. Por esto, se debe recopilar todos los datos posibles.

3.3.2. Exploración (Identificación)

Con la información que se pretenden encontrar en la fase de observación, se examinara la red para identificar los hosts que están activos, y así poder determinar los puertos abiertos, el sistema operativo y las aplicaciones que escuchan por puertos, en otras palabras, identificar vulnerabilidades específicas.

3.3.3. Análisis de vulnerabilidades

Identificar si un sistema es susceptible a un ataque para obtener más información de la víctima, aprovechando las vulnerabilidades que han sido encontradas previamente en las fases anteriores.

3.3.4. Explotación de vulnerabilidades (Evaluación)

Aprovechar las vulnerabilidades encontradas en las fases anteriores para poder realizar una intrusión al sistema operativo, aquí también se utilizará la técnica activa denominada: parameter tampering. Tomando en cuenta que el objetivo del auditor es mantenerse dentro del sistema para recabar más vulnerabilidades, comprometer otros sistemas, aumentar el nivel de privilegios del atacante y eliminar rastros

3.3.5. Resultados del estudio (Reporte)

Reportar es el último paso para finalizar el proceso de pentesting. Aquí el analista compila un informe con los hallazgos y el trabajo realizado, como las herramientas utilizadas, la tasa de éxito, las vulnerabilidades encontradas y los procesos de explotación para finalmente generar una guía de políticas de seguridad para la red LAN.

CAPÍTULO IV

4. RESULTADOS

4.1. Topología de la red LAN

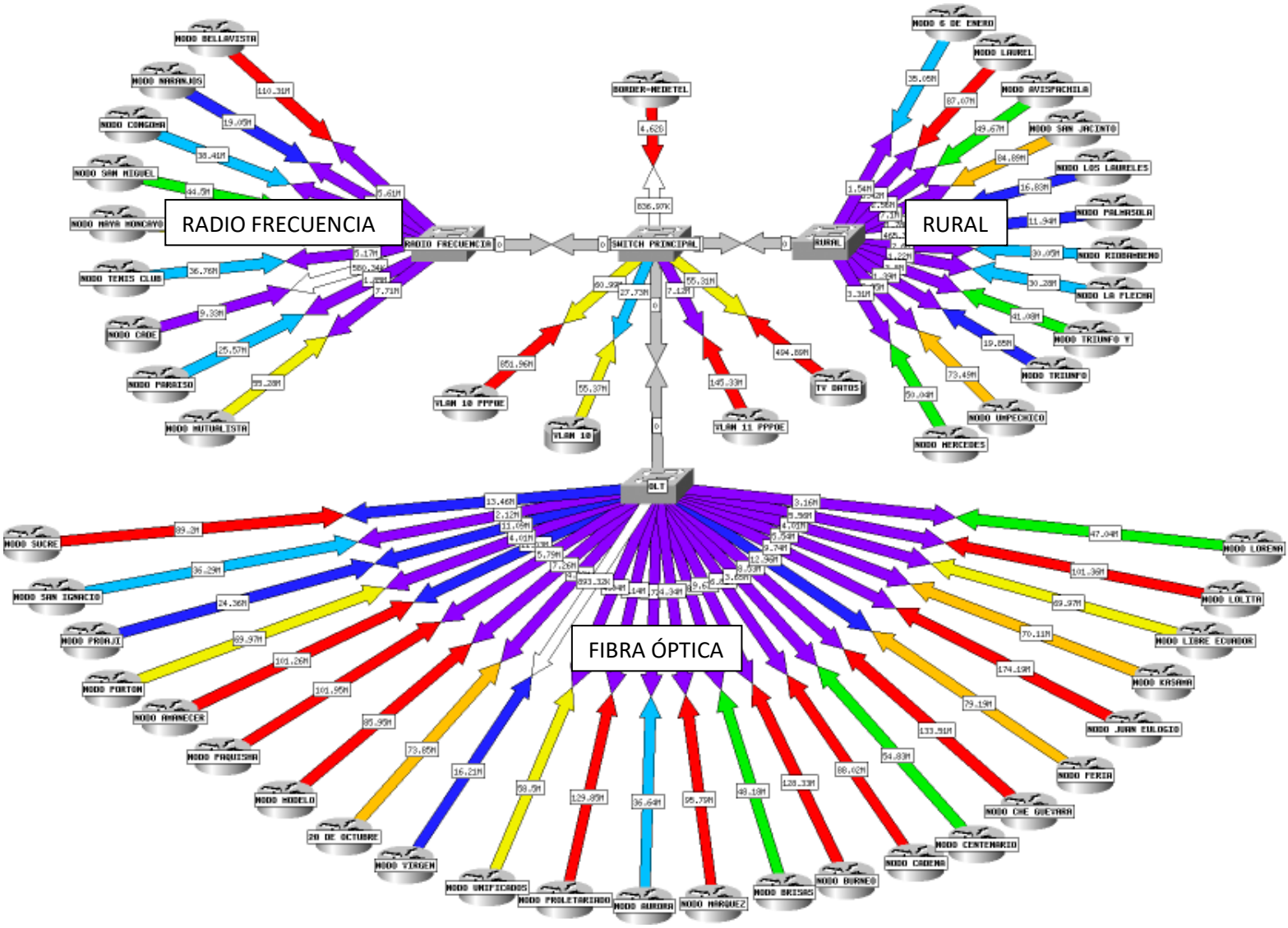


Figura 4.1. Topología de red CSEDnet.
Elaborado por: El autor

4.2. Obtención de Información (Adquisición)

Mediante el reconocimiento activo de la red, se realizó un estudio de la infraestructura para identificar la información de los principales equipos y los servicios que presta cada uno de ellos. Debido a la gran cantidad de nodos de la red, se optó por elegir el 30 por ciento de cada sección, eligiendo aquellos que poseían mayor cantidad de clientes.

N.	Nombre	Área	Número de Clientes	Servicios que presta
1	NODO BELLAVISTA	Radio Frecuencia	83 clientes	Distribuidor de Internet
2	NODO MAYAMONCAYO	Radio Frecuencia	59 clientes	Distribuidor de Internet
3	NODO SANMIGUEL	Radio Frecuencia	50 clientes	Distribuidor de Internet
4	NODO LAUREL	Rural	103 clientes	Distribuidor de Internet
5	NODO AVISPACHILA	Rural	53 clientes	Distribuidor de Internet
6	NODO MERCEDES	Rural	55 clientes	Distribuidor de Internet
7	NODO UMPECHICO	Rural	51 clientes	Distribuidor de Internet
8	NODO VLAN10	Fibra Óptica	20 clientes	Distribuidor de Internet
9	NODO SUCRE	Fibra Óptica	82 clientes	Distribuidor de Internet
10	NODO PORTON	Fibra Óptica	60 clientes	Distribuidor de Internet
11	NODO UNIFICADOS	Fibra Óptica	67 clientes	Distribuidor de Internet
12	NODO CENTENARIO	Fibra Óptica	32 clientes	Distribuidor de Internet
13	NODO MARQUEZ	Fibra Óptica	96 clientes	Distribuidor de Internet
14	NODO FERIA	Fibra Óptica	70 clientes	Distribuidor de Internet
15	NODO KASAMA	Fibra Óptica	73 clientes	Distribuidor de Internet

Tabla 4.1. Información de los nodos de la red
Elaborado por: El autor

4.3. Exploración (Identificación)

Con el fin de identificar o recabar más información, se examinó la red para identificar los hosts que están activos con el siguiente comando:

```
netdiscover -r <IP Network/Prefix>
netdiscover -r 172.20.33.0//24
```

Se determinó los puertos abiertos y el sistema operativo que usan cada uno de estos hosts con el siguiente comando:

```
nmap -sS -O <IP Network/Prefix>
nmap -sS -O -oN Desktop/NodoX_nmap.txt 192.168.1.0/24
```

Cabe recalcar que este comando es medio abierto, lo que quiere decir que no se abre una conexión TCP completa, por esta razón la actividad de escaneo es detectada por muchos

menos servidores. En las tablas se plasmó una muestra del escaneo debido a que eran demasiados hosts.

Nodo (BELLAVISTA)

N.	Dirección	Puertos abiertos	Sistema operativo
1	172.20.33.10	9011/TCP	Allworx 9211 VoIP phone
2	172.20.33.32	21,22,23,53,80,2000,8291/TCP	MikroTik RouterOS 6.35
3	172.20.33.79	21,22,23,53,80,2000,8291/TCP	MikroTik RouterOS 6.35

Tabla 4.2. Puertos abiertos y sistema operativo de 3 hosts del nodo BELLAVISTA
Elaborado por: El autor

Nodo (MAYAMONCAYO)

N.	Dirección	Puertos abiertos	Sistema operativo
1	172.20.26.10	21,22,23,53,80,2000,8291/TCP	MikroTik RouterOS 6.35
2	172.20.26.53	21,22,23,53,80,2000,8291/9011/TCP	MikroTik RouterOS 6.35
3	172.20.26.251	53,2000,8800/TCP	MikroTik RouterOS 6.35

Tabla 4.3. Puertos abiertos y sistema operativo de 3 hosts del nodo MAYAMONCAYO
Elaborado por: El autor

Nodo (SANMIGUEL)

N.	Dirección	Puertos abiertos	Sistema operativo
1	192.168.51.2	1723/2000/TCP	AXIS 210A Net Cam
2	192.168.51.30	21/22/23/53/80/2000/8291/TCP	MikroTik RouterOS 6.35
3	192.168.51.250	53/2000/880/TCP	MikroTik RouterOS 6.35

Tabla 4.4. Puertos abiertos y sistema operativo de 3 hosts del nodo SANMIGUEL
Elaborado por: El autor

Nodo (LAUREL)

N.	Dirección	Puertos abiertos	Sistema operativo
1	192.168.79.2	1723/2000/TCP	AXIS 210A Net Cam
2	192.168.79.27	21/22/23/53/80/2000/8291/TCP	MikroTik RouterOS 6.35
3	192.168.79.252	2000/8800/TCP	MikroTik RouterOS 6.35

Tabla 4.5. Puertos abiertos y sistema operativo de 3 hosts del nodo LAUREL
Elaborado por: El autor

Nodo (AVISPACHILA)

N.	Dirección	Puertos abiertos	Sistema operativo
1	192.168.177.17	21/22/23/53/80/2000/8291/TCP	AXIS 210A Net Cam
2	192.168.177.45	21/22/23/53/80/2000/5555/8291/TCP	MikroTik RouterOS 6.35
3	192.168.177.68	8080/TCP	MikroTik RouterOS 6.35

Tabla 4.6. Puertos abiertos y sistema operativo de 3 hosts del nodo AVISPACHILA
Elaborado por: El autor

Nodo (MERCEDES)

N.	Dirección	Puertos abiertos	Sistema operativo
1	192.168.84.1	1723/2000/TCP	MikroTik RouterOS 6.35
2	192.168.84.23	21/22/23/53/80/2000/8291/TCP	MikroTik RouterOS 6.35
3	192.168.84.251	2000/8291/TCP	MikroTik RouterOS 6.35

Tabla 4.7. Puertos abiertos y sistema operativo de 3 hosts del nodo MERCEDES
Elaborado por: El autor

Nodo (UMPECHICO)

N.	Dirección	Puertos abiertos	Sistema operativo
1	192.168.78.2	1723/2000/TCP	AXIS 210A Net Cam
2	192.168.78.25	21/22/23/53/80/2000/8291/TCP	MikroTik RouterOS 6.35
3	192.168.78.68	8080/TCP	Linux 2.6.22

Tabla 4.8. Puertos abiertos y sistema operativo de 3 hosts del nodo UMPECHICO
Elaborado por: El autor

Nodo (VLAN10)

N.	Dirección	Puertos abiertos	Sistema operativo
1	172.16.40.20	TODOS LOS 1000 PUERTOS ESTAN FILTRADOS	VRP V8 OS (Huawei)
2	172.16.40.39	80/TCP	VRP V8 OS (Huawei)
3	172.16.40.188	22/23/TCP	VRP V8 OS (Huawei)

Tabla 4.9. Puertos abiertos y sistema operativo de 3 hosts del nodo VLAN10
Elaborado por: El autor

Nodo (SUCRE)

N.	Nombre	Puertos abiertos	Sistema operativo
1	172.20.11.14	21/22/23/53/80/2000/8291/TCP	MikroTik RouterOS 6.35
2	172.20.11.72	21/22/23/53/80/2000/8291/TCP	Lorex NV408 Video Rec
3	172.20.11.247	53/2000/TCP	MikroTik RouterOS 6.35

Tabla 4.10. Puertos abiertos y sistema operativo de 3 hosts del nodo SUCRE
Elaborado por: El autor

Nodo (PORTON)

N.	Nombre	Puertos abiertos	Sistema operativo
1	172.20.6.17	8080/TCP	Qpcom RouterOS
2	172.20.6.34	21/22/23/53/80/2000/8291/TCP	MikroTik RouterOS 6.35
3	172.20.6.110	21/22/23/53/80/2000/8291/TCP	MikroTik RouterOS 6.35

Tabla 4.11. Puertos abiertos y sistema operativo de 3 hosts del nodo PORTON
Elaborado por: El autor

Nodo (UNIFICADOS)

N.	Nombre	Puertos abiertos	Sistema operativo
1	172.20.21.10	21/22/23/53/80/2000/8291/TCP	MikroTik RouterOS 6.35
2	172.20.21.33	21/22/23/33/53/80/89/211/544/1021/1059/1165/1524/2000/2003/2492/5000/5004/5225/5911/8087/8291/8654/15000/20221/23502/34572/42510/45100/65129/TCP	MikroTik RouterOS 6.35
3	172.20.21.246	53/2000/TCP	MikroTik RouterOS 6.35

Tabla 4.12. Puertos abiertos y sistema operativo de 3 hosts del nodo UNIFICADOS
Elaborado por: El autor

Nodo (CENTENARIO)

N.	Nombre	Puertos abiertos	Sistema operativo
1	172.20.2.1	25/53/113/135/139/143/443/445/857/TCP	Fortinet Fortigate Firewall
2	172.20.2.64	9011/TCP	Allworx 9212 VoIP Phone
3	172.20.2.251	53/2000/TCP	MikroTik RouterOS 6.35

Tabla 4.13. Puertos abiertos y sistema operativo de 3 hosts del nodo CENTENARIO
Elaborado por: El autor

Nodo (MARQUEZ)

N.	Nombre	Puertos abiertos	Sistema operativo
1	172.20.15.7	21/22/23/53/80/2000/8291/TCP	MikroTik RouterOS 6.35
2	172.20.15.34	21/22/23/53/80/1009/1032/1501/ 2000/2200/2909/3551/4129/6692/ 8291/8701/16012/TCP	MikroTik RouterOS 6.35
3	172.20.15.74	21/22/23/53/80/2000/8291/TCP	MikroTik RouterOS 6.35

Tabla 4.14. Puertos abiertos y sistema operativo de 3 hosts del nodo MARQUEZ
Elaborado por: El autor

Nodo (FERIA)

N.	Nombre	Puertos abiertos	Sistema operativo
1	172.20.23.12	9011/TCP	Qpcom RouterOS
2	172.20.23.47	21/22/23/53/80/2000/8291/TCP	MikroTik RouterOS 6.35
3	172.20.23.249	53/2000/TCP	DiskStation Manager 5 (NAS)

Tabla 4.15. Puertos abiertos y sistema operativo de 3 hosts del nodo FERIA
Elaborado por: El autor

Nodo (KASAMA)

N.	Nombre	Puertos abiertos	Sistema operativo
1	172.20.24.10	21/22/23/53/80/2000/8291/TCP	DiskStation Manager 5 (NAS)
2	172.20.24.47	21/22/23/53/80/2000/8291/TCP	MikroTik RouterOS 6.35
3	172.20.24.250	53/2000/TCP	MikroTik RouterOS 6.35

Tabla 4.16. Puertos abiertos y sistema operativo de 3 hosts del nodo KASAMA
Elaborado por: El autor

4.1. Análisis de vulnerabilidades

4.1.1. Captura de tráfico de la red durante 30 minutos

Con el fin de realizar esta fase, se utilizó la herramienta de software libre que se encuentra en el sistema operativo ParrotOS denominada WIRESHARK, mediante lo cual se puede evidenciar que de los 15 nodos elegidos: 3 de la sección de radio frecuencia, 4 de Rural y 8 de la sección de Fibra, todos eran susceptibles a ataques de sniffing.

Nodo	Fecha	Hora	Dispositivos activos	Paquetes capturados
BELLAVISTA	10/08/2020	10AM	83 / 83	211981
		4PM	83 /83	214654
MAYAMONCAYO	11/08/2020	10AM	59 / 59	549937
		4PM	59 / 59	306248
SANMIGUEL	12/08/2020	10AM	44 / 50	9094
		4PM	46 / 50	265148
LAUREL	13/08/2020	10AM	103 / 103	252572
		4PM	98 / 103	18568
AVISPACHILA	14/08/2020	10AM	53 / 53	14160
		4PM	51 / 53	9426
MERCEDES	17/08/2020	10AM	55 / 55	258771
		4PM	53 / 55	48153
UMPECHICO	18/08/2020	10AM	49 / 51	175337
		4PM	51 / 51	133409
VLAN10	19/08/2020	10AM	15 / 20	107761
		4PM	16 / 20	39134
SUCRE	20/08/2020	10AM	82 / 82	191261
		4PM	82 / 82	23392
PORTON	21/08/2020	10AM	60 / 60	153485
		4PM	60 / 60	11780
UNIFICADOS	24/08/2020	10AM	32 / 67	46026
		4PM	67 / 67	159683
CENTENARIO	25/08/2020	10AM	29 / 32	17188
		4PM	32 / 32	236648
MARQUEZ	26/08/2020	10AM	96 / 96	192547
		4PM	96 / 96	37365
FERIA	27/08/2020	10AM	70 / 70	273628
		4PM	67 / 70	6242
KASAMA	28/08/2020	10AM	73 / 73	181095
		4PM	3 / 73	9882

Tabla 4.17. Número de paquetes capturados en 30 minutos de cada nodo
Elaborado por: El autor

4.1.2. Protocolos capturados por Wireshark durante media hora (se eligió el ejemplo que capturo más paquetes)

Nodo BELLAVISTA (4PM)

Protocolo	Paquetes capturados durante 30 minutos
TCP	192351
UDP	1903
ARP	3214

Tabla 4.18. Número de paquetes por protocolo capturados en 30 minutos del Nodo BELLAVISTA
Elaborado por: El autor

Nodo MAYAMONCAYO (10AM)

Protocolo	Paquetes capturados durante 30 minutos
TCP	48250
UDP	3046
ARP	8807

Tabla 4.19. Número de paquetes por protocolo capturados en 30 minutos del Nodo MAYACONCAYO
Elaborado por: El autor

Nodo SANMIGUEL (4PM)

Protocolo	Paquetes capturados durante 30 minutos
TCP	250323
UDP	1316
ARP	610

Tabla 4.20. Número de paquetes por protocolo capturados en 30 minutos del Nodo SANMIGUEL
Elaborado por: El autor

Nodo LAUREL (10AM)

Protocolo	Paquetes capturados durante 30 minutos
TCP	226036
UDP	8378
ARP	2702

Tabla 4.21. Número de paquetes por protocolo capturados en 30 minutos del Nodo LAUREL
Elaborado por: El autor

Nodo AVISPACHILA (10AM)

Protocolo	Paquetes capturados durante 30 minutos
TCP	123850
UDP	1041
ARP	3294

Tabla 4.22. Número de paquetes por protocolo capturados en 30 minutos del Nodo AVISPACHILA
Elaborado por: El autor

Nodo MERCEDES (10AM)

Protocolo	Paquetes capturados durante 30 minutos
TCP	240724
UDP	969
ARP	3603

Tabla 4.23. Número de paquetes por protocolo capturados en 30 minutos del Nodo MERCEDES
Elaborado por: El autor

Nodo UMPECHICO (10AM)

Protocolo	Paquetes capturados durante 30 minutos
TCP	152928
UDP	768
ARP	2401

Tabla 4.24. Número de paquetes por protocolo capturados en 30 minutos del Nodo UMPECHICO
Elaborado por: El autor

Nodo VLAN10 (10AM)

Protocolo	Paquetes capturados durante 30 minutos
TCP	100077
UDP	42
ARP	860

Tabla 4.25. Número de paquetes por protocolo capturados en 30 minutos del Nodo VLAN10
Elaborado por: El autor

Nodo SUCRE (10AM)

Protocolo	Paquetes capturados durante 30 minutos
TCP	177787
UDP	548
ARP	2016

Tabla 4.26. Número de paquetes por protocolo capturados en 30 minutos del Nodo SUCRE
Elaborado por: El autor

Nodo PORTON (10AM)

Protocolo	Paquetes capturados durante 30 minutos
TCP	135288
UDP	1364
ARP	3804

Tabla 4.27. Número de paquetes por protocolo capturados en 30 minutos del Nodo PORTON
Elaborado por: El autor

Nodo UNIFICADOS (4PM)

Protocolo	Paquetes capturados durante 30 minutos
TCP	132849
UDP	3336
ARP	3041

Tabla 4.28. Número de paquetes por protocolo capturados en 30 minutos del Nodo UNIFICADOS
Elaborado por: El autor

Nodo CENTENARIO (4PM)

Protocolo	Paquetes capturados durante 30 minutos
TCP	235378
UDP	1236
ARP	2562

Tabla 4.29. Número de paquetes por protocolo capturados en 30 minutos del Nodo CENTENARIO
Elaborado por: El autor

Nodo MARQUEZ (10AM)

Protocolo	Paquetes capturados durante 30 minutos
TCP	135784
UDP	27331
ARP	19767

Tabla 4.30. Número de paquetes por protocolo capturados en 30 minutos del Nodo CENTENARIO
Elaborado por: El autor

Nodo FERIA (10AM)

Protocolo	Paquetes capturados durante 30 minutos
TCP	256216
UDP	785
ARP	4870

Tabla 4.31. Número de paquetes por protocolo capturados en 30 minutos del Nodo FERIA
Elaborado por: El autor

Nodo KASAMA (10AM)

Protocolo	Paquetes capturados durante 30 minutos
TCP	160039
UDP	2182
ARP	3488

Tabla 4.32. Número de paquetes por protocolo capturados en 30 minutos del Nodo KASAMA
Elaborado por: El autor

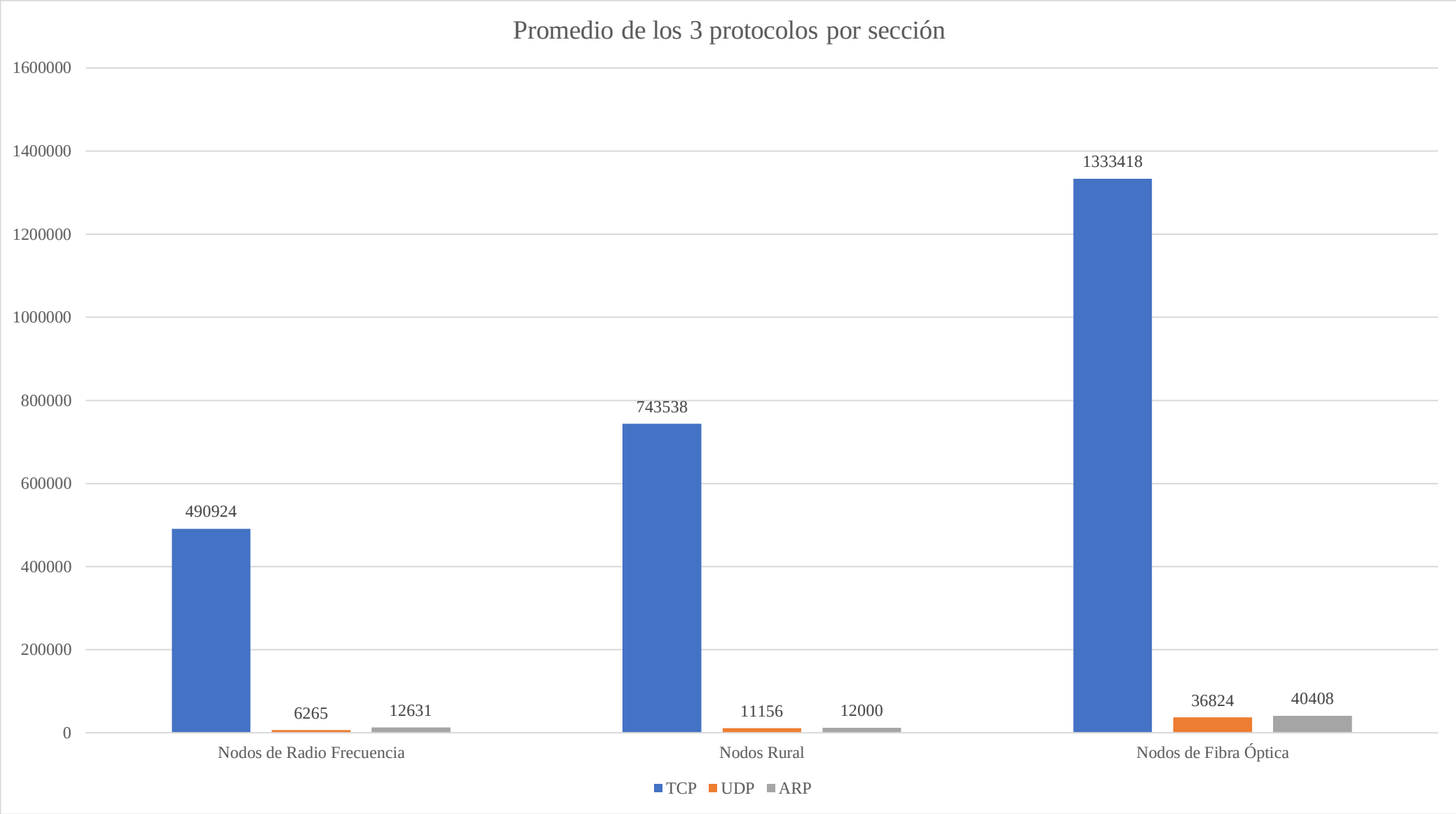


Figura 4.2. Promedio de los 3 protocolos por sección
Elaborado por: El autor

4.1.3. Explotación de vulnerabilidades (Evaluación)

En esta fase se utilizó la herramienta de software libre OWASP ZAP, para ejecutar el ataque parameter tampering al sistema que usa la empresa, para realizar sus actividades contables y la activación o suspensión del servicio de internet por falta de pago.

Fase1: Captura de los parámetros de inicio de sesión

Se inicio sesión con las credenciales del administrador para realizar las pruebas, el proceso de inicio de sesión se mantuvo en espera debido a que en segundo plano, se estaba ejecutando la herramienta para capturar los parámetros que se enviaban.

Figura 4.3. Inicio de sesión en el sistema ISP
Elaborado por: El autor

La herramienta capturó satisfactoriamente los parámetros que se estaban enviando al servidor para el inicio de sesión. Los principales parámetros capturados fueron: “data.1” y “data.2”, usuario y contraseña respectivamente.

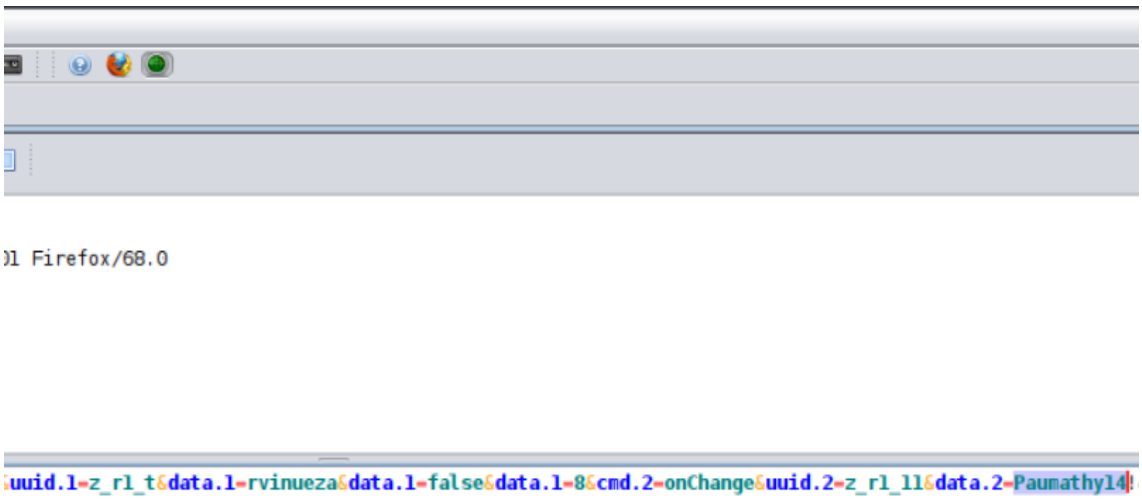


Figura 4.4. Captura de los parámetros enviados al servidor para el inicio de sesión
Elaborado por: El autor

Se modifico el parámetro que llevaba la contraseña para evitar el acceso al sistema y se dio paso a la petición que se había mantenido en pausa.

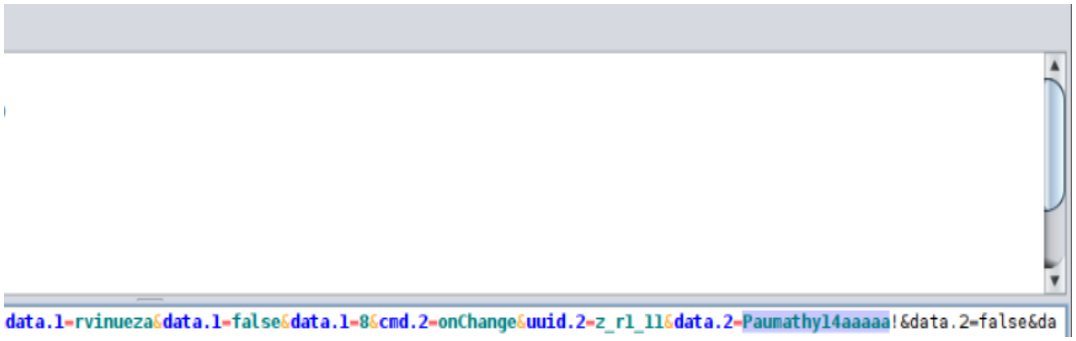


Figura 4.5. Modificación del parámetro "data.2"
Elaborado por: El autor

Cuando se ingresa una contraseña incorrecta el servidor rechaza la sesión, como se muestra en la figura 4.6.

Figura 4.6. Inicio de sesión invalidado
Elaborado por: El autor

Fase 2: Modificación de los parámetros de los usuarios (Corte de Servicio)

Para modificar los parámetros es necesario realizar una consulta de los datos del del usuario.

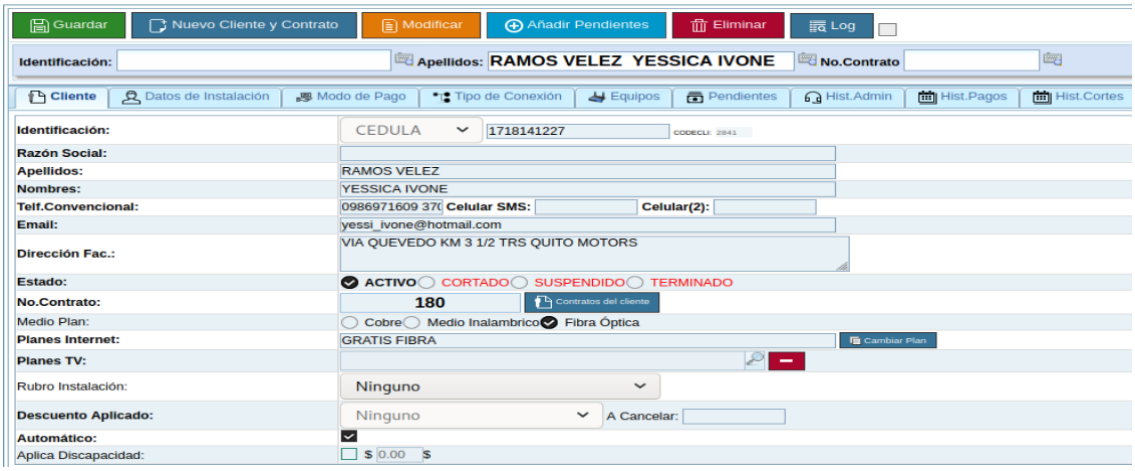


Figura 4.7. Consulta de la información del cliente en el sistema
Elaborado por: El autor

Se pueden modificar los parámetros con respecto a: información general del usuario, tipo de pago, entre otros. En este caso se modificó el estado del servicio que el cliente poseía, de **activo** a **cortado** y se guardaron los cambios, por lo que el sistema se mantuvo en pausa esperando a que la herramienta OWASP ZAP de paso a la petición.

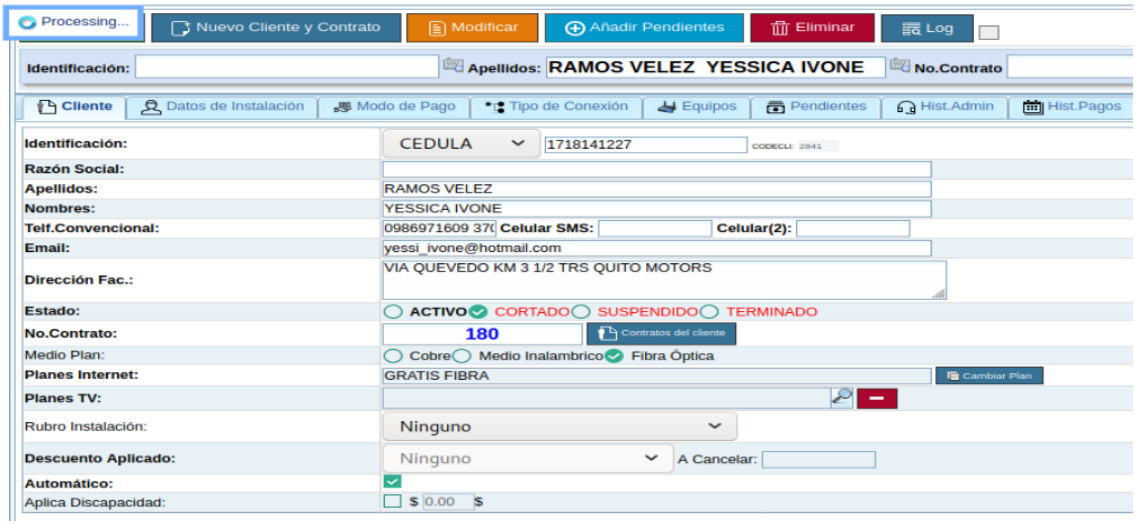


Figura 4.8. Modificación del estado de "ACTIVO" a "CORTADO"
Elaborado por: El autor

La herramienta capturó satisfactoriamente los parámetros que se estaban enviando al servidor, para modificar el estado del servicio de ACTIVO a CORTADO, las variables son: "z_n9_34" para ACTIVO, "z_n9_44" para CORTADO, "z_n9_54" para SUSPENDIDO y "z_n9_64" para TERMINADO.

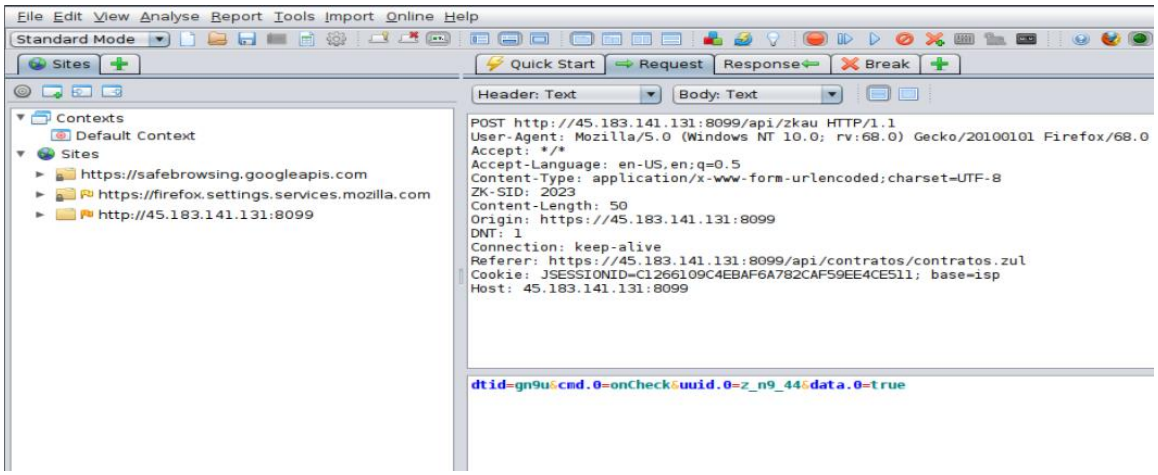


Figura 4.9. Captura de los parámetros enviados al servidor para el corte del servicio
Elaborado por: El autor

A continuación, se modificó el parámetro que contenía la variable la cual a su vez llevaba el valor de “true”, en este caso era “z_n9_44” por “z_n9_34” que era la variable perteneciente a ACTIVO y se dio paso a la petición que se había mantenido en pausa.

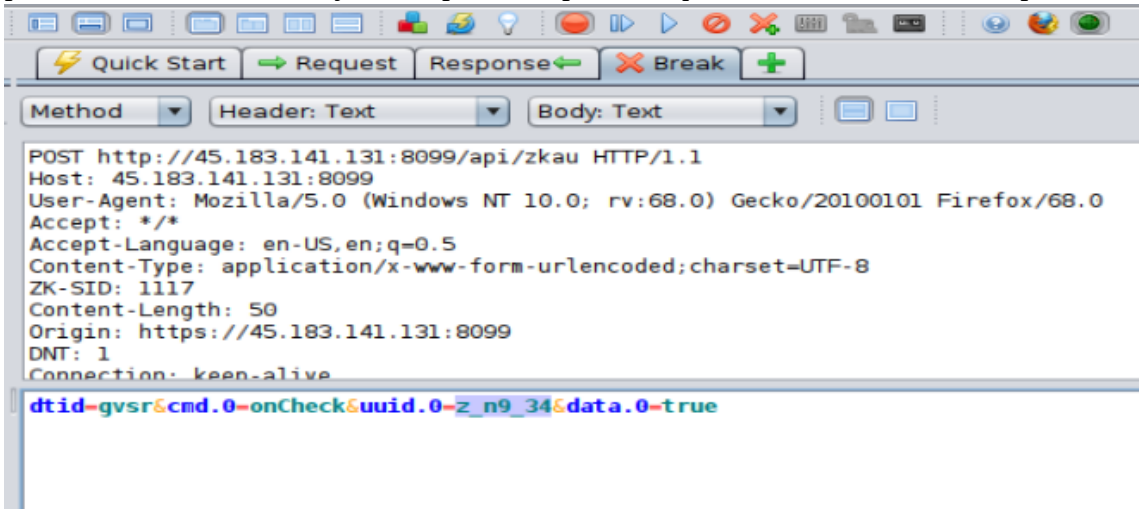


Figura 4.10. Modificación del parámetro “uuid.0”
Elaborado por: El autor

Como se puede observar en la imagen, el servicio se mantuvo en ACTIVO, debido al cambio que se hizo en el apartado anterior.

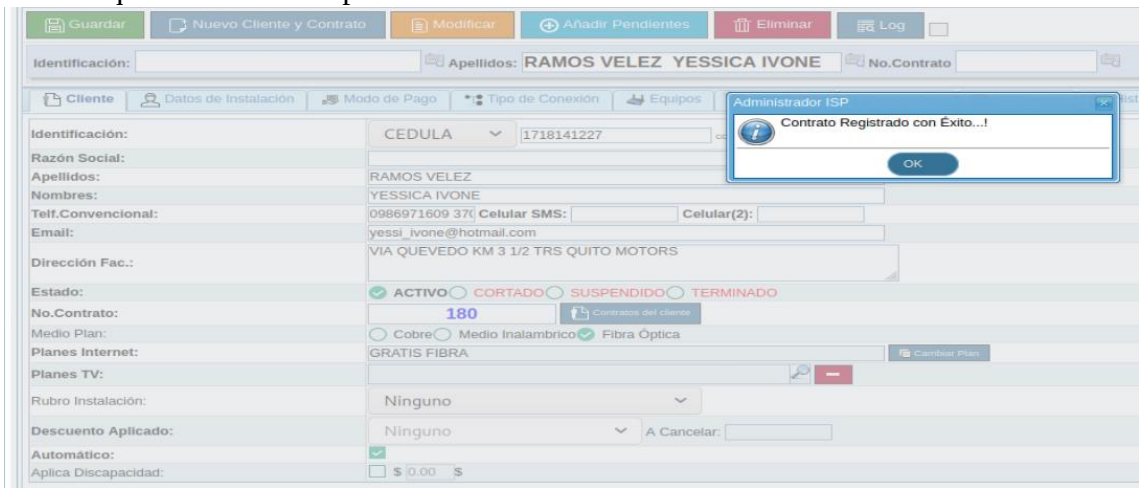


Figura 4.11. Corte del servicio invalidado
Elaborado por: El autor

4.1.4. Resultados del estudio (Reporte)

Políticas de Seguridad

Con el fin de mitigar las amenazas denominadas **sniffing** y **parameter tampering,** se implementaron políticas de seguridad y recomendaciones de la página de MIKROTIK, en los principales equipos activos de la red LAN, mismo en los que se realizaron las pruebas preliminares. En vista de que el protocolo TCP fue el que más capturas registró en todas las pruebas realizadas, se optó por priorizar las reglas en base a este protocolo.

- **Crear una Black List de IPS**

```
/ip firewall filter add chain=input protocol=tcp connection-limit=10,32 action=add-src-to-address-list address-list=blocked-addr address-list-timeout=1d
```

- **TARPIT**

Disminuye el ancho de banda del host paulatinamente hasta inhabilitarlo. Se debe realizar un TARP solo si el uso del CPU del mikrotik no excede del 25-30% de uso normal promedio.

```
/ip firewall filter add chain=input protocol=tcp connection-limit=3,32 action=add-src-to-address-list address-list="blocked_addr_tarpit_PENTEST" address-list-timeout=5h disabled=no
/ip firewall filter add chain=input protocol=tcp src-address-list="blocked_addr_tarpit_PENTEST" connection-limit=3,32 action=tarpit disabled=no
```

- **SYNFILTER (SYN FLOOD)**

Protección para Mecanismos de Exploits incluido el Sniffing, evita que la comunicación TCP sea interrumpida, y que en el servidor se acumulen paquetes incompletos.

```
/ip firewall filter add chain=forward protocol=tcp tcp-flags=syn connection-state=new action=jump jump-target=SYN-Protect comment= “SYN Flood protect” disable=yes

/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn limit=400,5 connection-state=new action=accept comment=”” disabled=no

/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn connection-state=new action=drop comment=”” disabled=no
```

- **SYN cookies (Complementa el paso anterior)**

Esta técnica se utilizada para resistir los ataques de suplantación de IP, en este caso en las pruebas de sniffing que se realizaron, se utilizó una máquina virtual con conexión bridge.

```
/ip settings set tcp-syncookies=yes
```

- **Limitar las conexiones de Mapeo**

Se debe generar un script el cual analiza automáticamente si una IP en particular está tratando de hacer un mapeo de puertos.

```
/ip firewall filter add chain=input protocol=tcp psd=21,3s,3,1 action=add-src-to-address-list address-list="blocked_port_scanners_PENTEST" address-list-timeout=5h comment="Port scanners to list PENTEST" disabled=no
/ip firewall filter add chain=input src-address-list="blocked_port_scanners" action=drop disabled=no
```

Posterior a la implementación de las reglas, se realizó una evaluación para comprobar si las medidas de seguridad antes mencionadas, funcionaron correctamente. Se utilizó como referencia los resultados que capturaron mayor cantidad de paquetes en las pruebas preliminares, estos fueron los resultados:

Comparación Nodo BELLAVISTA

Hubo una disminución del 95,47% en cuanto a los paquetes capturados.

Implementación de Reglas	Paquetes capturados durante 30 minutos
Antes	214654
Después	9725

Tabla 4.33. Antes y después de la implementación de las reglas en el Nodo BELLAVISTA
Elaborado por: El autor

Comparación Nodo MAYAMONCAYO

Hubo una disminución del 98,83% en cuanto a los paquetes capturados.

Implementación de Reglas	Paquetes capturados durante 30 minutos
Antes	549937
Después	6445

Tabla 4.34. Comparación antes y después de la implementación de las reglas en el Nodo MAYAMONCAYO
Elaborado por: El autor

Comparación Nodo SANMIGUEL

Hubo una disminución del 96,33% en cuanto a los paquetes capturados.

Implementación de Reglas	Paquetes capturados durante 30 minutos
Antes	265148
Después	9719

Tabla 4.35. Comparación antes y después de la implementación de las reglas en el Nodo SANMIGUEL
Elaborado por: El autor

Comparación Nodo LAUREL

Hubo una disminución del 94,27% en cuanto a los paquetes capturados.

Implementación de Reglas	Paquetes capturados durante 30 minutos
Antes	252572
Después	14471

Tabla 4.36. Comparación antes y después de la implementación de las reglas en el Nodo LAUREL
Elaborado por: El autor

Comparación Nodo AVISPACHILA

Hubo una disminución del 58,67% en cuanto a los paquetes capturados.

Implementación de Reglas	Paquetes capturados durante 30 minutos
Antes	14160
Después	5852

Tabla 4.37. Comparación antes y después de la implementación de las reglas en el Nodo AVISPACHILA
Elaborado por: El autor

Comparación Nodo MERCEDES

Hubo una disminución del 98,07% en cuanto a los paquetes capturados.

Implementación de Reglas	Paquetes capturados durante 30 minutos
Antes	258771
Después	4995

Tabla 4.38. Comparación antes y después de la implementación de las reglas en el Nodo MERCEDES
Elaborado por: El autor

Comparación Nodo UMPECHICO

Hubo una disminución del 98,13% en cuanto a los paquetes capturados.

Implementación de Reglas	Paquetes capturados durante 30 minutos
Antes	175337
Después	3272

Tabla 4.39. Comparación antes y después de la implementación de las reglas en el Nodo UMPECHICO
Elaborado por: El autor

Comparación Nodo VLAN10

Hubo una disminución del 98,47% en cuanto a los paquetes capturados.

Implementación de Reglas	Paquetes capturados durante 30 minutos
Antes	107761
Después	1654

Tabla 4.40. Comparación antes y después de la implementación de las reglas en el Nodo VLAN10
Elaborado por: El autor

Comparación Nodo SUCRE

Hubo una disminución del 29,65% en cuanto a los paquetes capturados.

Implementación de Reglas	Paquetes capturados durante 30 minutos
Antes	191261
Después	134547

Tabla 4.41. Comparación antes y después de la implementación de las reglas en el Nodo SUCRE
Elaborado por: El autor

Comparación Nodo PORTON

Hubo una disminución del 97,03% en cuanto a los paquetes capturados.

Implementación de Reglas	Paquetes capturados durante 30 minutos
Antes	153485
Después	4557

Tabla 4.42. Comparación antes y después de la implementación de las reglas en el Nodo PORTON
Elaborado por: El autor

Comparación Nodo UNIFICADOS

Hubo una disminución del 97,44% en cuanto a los paquetes capturados.

Implementación de Reglas	Paquetes capturados durante 30 minutos
Antes	159683
Después	4090

Tabla 4.43. Comparación antes y después de la implementación de las reglas en el Nodo UNIFICADOS
Elaborado por: El autor

Comparación Nodo CENTENARIO

Hubo una disminución del 99,01% en cuanto a los paquetes capturados.

Implementación de Reglas	Paquetes capturados durante 30 minutos
Antes	236648
Después	2336

Tabla 4.44. Comparación antes y después de la implementación de las reglas en el Nodo CENTENARIO
Elaborado por: El autor

Comparación Nodo MARQUEZ

Hubo una disminución del 91,21% en cuanto a los paquetes capturados.

Implementación de Reglas	Paquetes capturados durante 30 minutos
Antes	192547
Después	16933

Tabla 4.45. Comparación antes y después de la implementación de las reglas en el Nodo MARQUEZ
Elaborado por: El autor

Comparación Nodo FERIA

Hubo una disminución del 96,68% en cuanto a los paquetes capturados.

Implementación de Reglas	Paquetes capturados durante 30 minutos
Antes	273628
Después	9094

Tabla 4.46. Comparación antes y después de la implementación de las reglas en el Nodo FERIA
Elaborado por: El autor

Comparación Nodo KASAMA

Hubo una disminución del 97,35% en cuanto a los paquetes capturados.

Implementación de Reglas	Paquetes capturados durante 30 minutos
Antes	181095
Después	4805

Tabla 4.47. Comparación antes y después de la implementación de las reglas en el Nodo KASAMA
Elaborado por: El autor

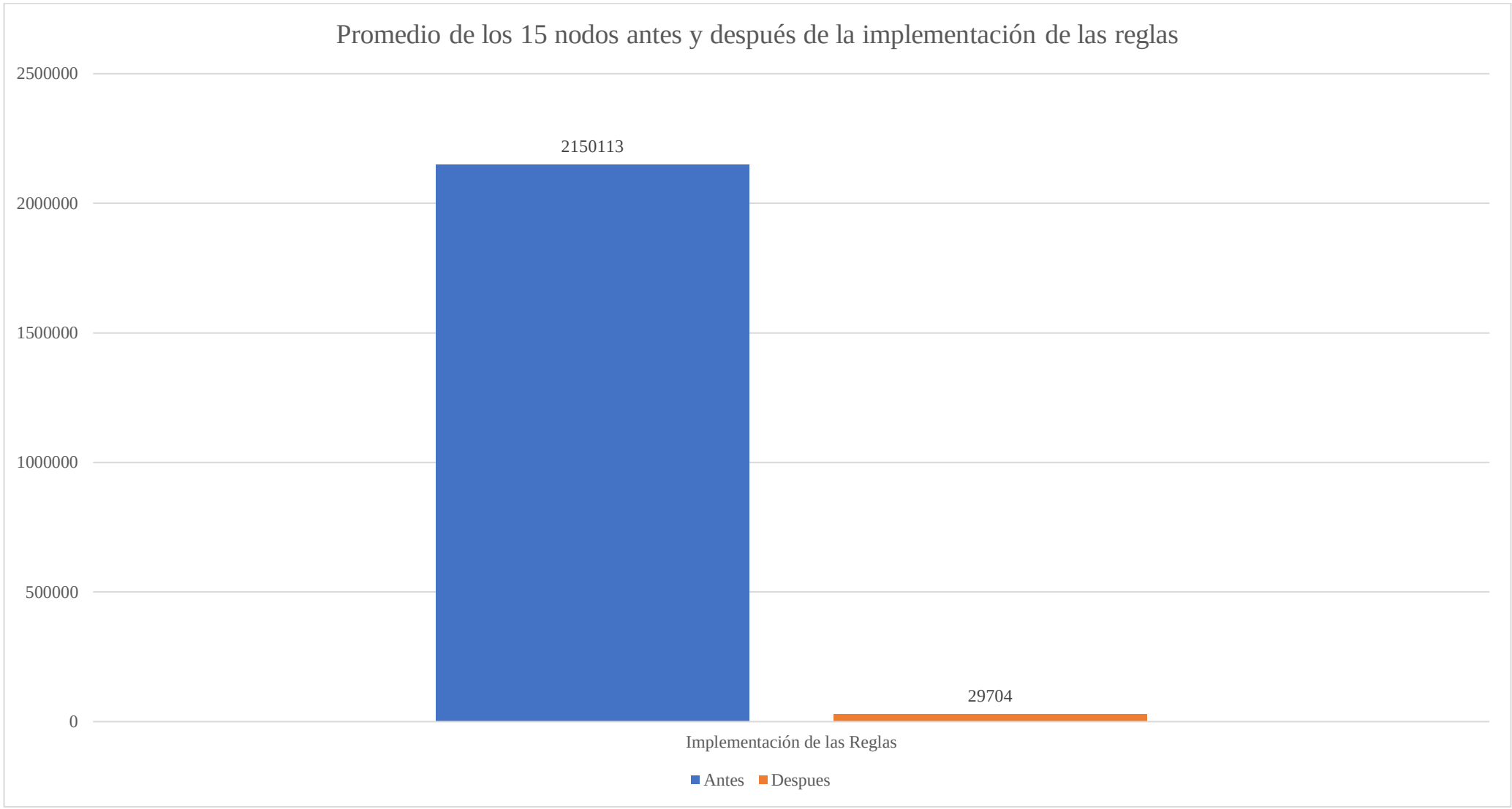


Figura 4.2. Promedio de los 15 nodos antes y después de la implementación de las reglas
Elaborado por: El autor

CONCLUSIONES

En el estudio realizado sobre las técnicas de pentesting denominadas sniffing y parameter tampering se concluye que, estas técnicas por sí solas son una amenaza para la infraestructura de red (dispositivos y sistema) de una empresa. Al combinar las técnicas mencionadas con otros métodos de hacking como: Man-In-The-Middle, Malware, SYN Flood, Ping Flood, demuestran el verdadero potencial para explotar vulnerabilidades dentro de una empresa, razón por la cual es primordial proteger la infraestructura de red de los ataques, e identificar las vulnerabilidades.

Antes de la implementar las reglas planteadas en esta investigación, se realizaron pruebas de sniffing al 30% de cada sección de los nodos, siguiendo la metodología de CEH, fue posible capturar una gran cantidad de paquetes, especialmente en la mañana, debido al gran tráfico en los nodos de red. La mayoría de los paquetes que se capturaron en la mañana fueron del protocolo TCP. Usando la técnica de sniffing se diagnosticaron vulnerabilidades tales como: Capturar contraseñas y nombres de usuario, interceptar correos electrónicos y espiar conversaciones. Mientras que para la técnica de parametter tampering se identificaron vulnerabilidades para la modificación de valores tales como: Información del cliente, tipo de pago y descuentos.

El sistema que usa la empresa CSEDnet para realizar las peticiones de cobros, activar o desactivar el servicio por falta de pago, entre otros; no envía datos innecesarios al servidor cuando se hacen estas peticiones. Sin embargo, actualiza constantemente los datos que muestra el sistema, por esta razón se pudo capturar los parámetros que se estaban enviando al servidor para iniciar sesión y para cambiar el estado del servicio (activo a cortado), pudiendo modificarlos con éxito, demostrando así que el sistema es vulnerable a ataques de parameter tampering.

Luego que se implementaron las reglas de mitigación de captura de paquetes, usando la técnica de sniffing en los equipos de la empresa, se pudo constatar que el número de paquetes capturados disminuyó drásticamente, teniendo como resultado una reducción de un 98,62% en la captura de los paquetes. Dando validez a la investigación.

RECOMENDACIONES

Se debe realizar pruebas en un entorno controlado. En primera instancia se planteó utilizar la herramienta bettercap la cual es más versátil y completa que Wireshark; por lo que para conocer el comportamiento de las herramientas se trabajó en un entorno virtualizado, en donde ninguna de las dos herramientas mostró problemas. Sin embargo, al pasarlo a un entorno real, se pudo constatar que bettercap fue más agresiva (en cuestiones de utilización de recursos: ancho de banda, memoria RAM, CPU, etc) que Wireshark, razón por la cual se optó por utilizar Wireshark en el entorno real, para realizar las pruebas y recabar la información.

Para un manejo fácil y eficaz de la detección y prevención de intrusos, se recomienda la utilización de los IPS (Intrusion Prevention System) e IDS (Intrusion Detection System) los cuales van acoplados en paralelo con el router que está conectado directamente al proveedor de internet, redireccionando el tráfico a los sistemas. Se deben implementar estos sistemas si se tiene los recursos necesarios. Para facilitar aún más el trabajo, existen distribuciones de código abierto listas para utilizarse, como es el caso de SELKS y SecurityOnion, las cuales están listas para instalarse en un servidor, por otro lado, una alternativa de paga es TrapIPS similar a SELKS, pero con características adicionales como: personalización de perfiles de seguridad, fuentes de reglas comerciales y que soporta múltiples Routers.

Para realizar el ataque de parameter tampering es necesario activar la herramienta OWASP ZAP, antes de cargar la página para que capture los parámetros, debido a que el navegador identificaba un error en el proxy. Si se activaba la herramienta después de cargar la página, la herramienta no funcionaba correctamente, provocando que se detuviera la captura de parámetros del sistema de la empresa.

REFERENCIAS BIBLIOGRÁFICA

Andrew, T., & David, W. (2014). *Redes de computadoras* (5.ª ed.). México, Naucalpan de Juárez: Pearson Educación de México, S.A. de C.V.

Balogh, Z., Koprda, Š., & Francisti, J. (2018, October). *LAN security analysis and design*. In 2018 IEEE 12th International Conference on Application of Information and Communication Technologies (AICT) (pp. 1-6). IEEE

Baloch, R. (2017). *Ethical hacking and penetration testing guide*. CRC Press.

Basin, D., Cremers, C., & Meadows, C. (2018). *Model checking security protocols. In Handbook of Model Checking* (pp. 727-762). Springer, Cham.

Bhatia, V., Gupta, D., & Sinha, H. P. (2012). *Throughput and Vulnerability Analysis of an IEEE 802. 11b Wireless LAN*. International Journal of Computer Applications, 52(3).

Bisht, P., Hinrichs, T., Skrupsky, N., Bobrowicz, R., & Venkatakrishnan, V. N. (2010, October). NoTamper: automatic blackbox detection of parameter tampering opportunities in web applications. In *Proceedings of the 17th ACM conference on Computer and communications security* (pp. 607-618).

Caballero, A. (2016). Pruebas de Penetración con Zed Attack Proxy. *OWASP ORG*. https://owasp.org/www-pdf-archive//OWASP_ZAP_Alonso_ReYDeS.pdf

Chuquitarco, M. (2018). Diagnóstico de las vulnerabilidades en redes inalámbricas en el Ecuador. *INNOVA Research Journal*, *3*(2.1), 111-122. https://doi.org/10.33890/innova.v3.n2.1.2018.692

Deloitte. (2020, 8 julio). *Informativo Gerencial*. Deloitte Ecuador. https://www2.deloitte.com/ec/es/pages/deloitte-analytics/articles/Informativo-gerencial-Deloitte-Ecuador.html

Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. *IEEE Access*, 7, 80813-80828.

Fiscalía General del Ecuador. (13 de junio de 2015). Fiscalía General del Estado. Obtenido de https://www.fiscalia.gob.ec/los-delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje/

González Paz, A., Beltrán Casanova, D., & Fuentes Gari, E. R. (2016). PROPUESTA DE PROTOCOLOS DE SEGURIDAD PARA LA RED INALÁMBRICA LOCAL DE

LA UNIVERSIDAD DE CIENFUEGOS. *Revista Universidad y Sociedad, 8*(4), 130-137.

I. P. Specialist. (2018). CEH V10 Certified Ethical Hacker Complete Training Guide with Practice Labs. IPSpecialist Ltd.

ISO/IEC. (2004). *INTERNATIONAL STANDARD ISO/IEC TR 13335-1:2004 Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*. https://www.iso.org/standard/39066.html

Kaspersky. (2018). *CYBERTHREAT REAL-TIME MAP*. Cybermap of Kaspersky. https://cybermap.kaspersky.com/es/stats

Krishna, R., & Subhasini, R. (2019) in Computing and Network Sustainability. *LAN Security Management System*.

McMahon, E., Williams, R., El, M., Samtani, S., Patton, M., & Chen, H. (2017, July). *Assessing medical device vulnerabilities on the Internet of Things. In 2017 IEEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 176-178). IEEE.

MikroTik. (s. f.). *DoS attack protection - MikroTik Wiki*. MikroTik Wiki. Recuperado 5 de septiembre de 2020, de https://wiki.mikrotik.com/wiki/DoS_attack_protection

Molina, J. M. M. (2004). Seguridad en redes inalámbricas 802.11.

Najera-Gutierrez, G., & Ansari, J. A. (2018). *Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux*. Packt Publishing Ltd.

Pandey, A., Pant, P. K., & Tripathi, R. C. (2016). *A System and Method for Authentication in Wireless Local Area Networks (WLANs)*. Proceedings of the National Academy of Sciences, India Section A: Physical Sciences, 86(2), 149-156.

Reyes, A. (2017). *Ataques en redes de datos IPv4 e IPv6*. RIUMA. https://riuma.uma.es/xmlui/bitstream/handle/10630/13305/%c3%81lvaro%20Rodrigo%20Reyes%20RosadoMemoria.pdf?sequence=1&isAllowed=y

Ruiz Gómez, J. C. (2018). *Formación de auditores internos ISO27001 y técnicas de Hacking ético.*

Sánchez Avila, M. A. (2019). *Hacking ético: impacto en la sociedad.*

Sari, A., & Karay, M. (2015). Comparative analysis of wireless security protocols: WEP vs WPA. International Journal of Communications, Network and System Sciences, 8(12), 483.

Shimonski, R. (2016). *CEH v9: Certified Ethical Hacker Version 9 Study Guide (Vol. 9)*. John Wiley & Sons.

Solarte, J., *Riesgos y Control Informático [en línea]*. http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_21_generalidades_del_estndar_cobit.html

Tejena-Macías, M. A. (2018). *Análisis de riesgos en seguridad de la información*. Polo del conocimiento, 3(4), 230-244.

Wireshark · Go Deep. (2020). Retrieved 5 August 2020, from https://www.wireshark.org/

WiFiMesh. (s. f.). *Que es un Nodo de Red*. WiFi Mesh. Recuperado 27 de marzo de 2020, de https://meshwifi.es/que-es-un-nodo-de-red/

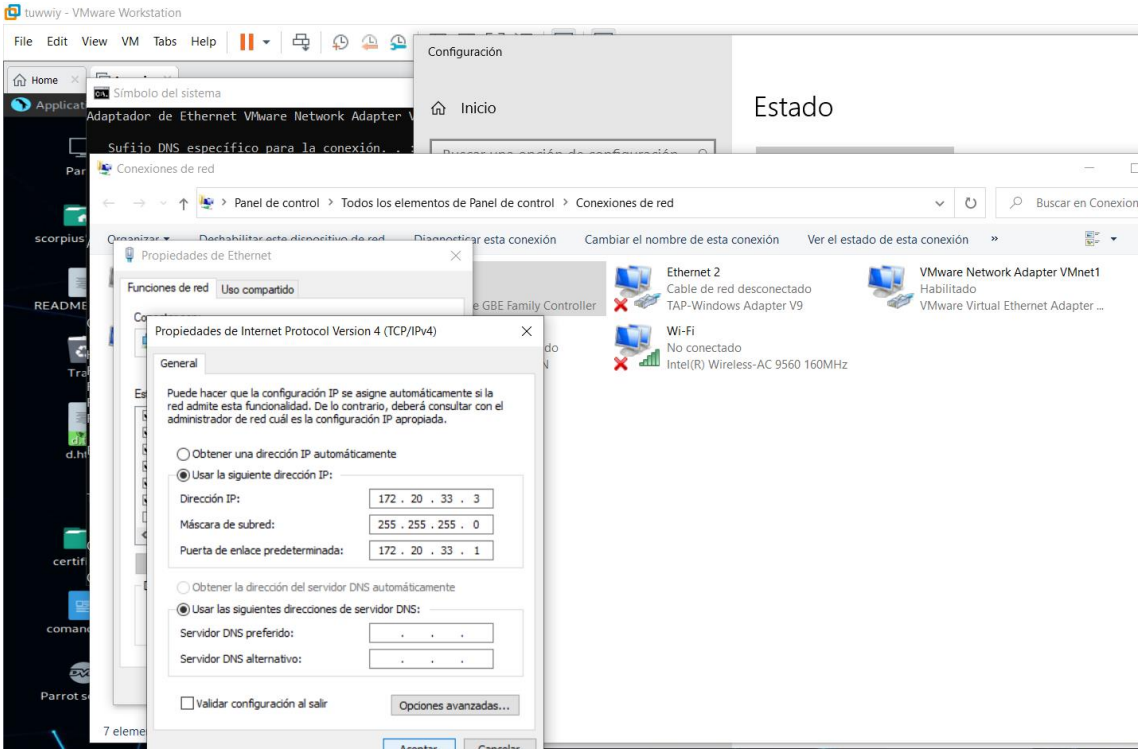
Zambrano, S. M. Q., & Valencia, D. G. M. (2017). *Seguridad en informática: consideraciones*. Dominio de las Ciencias, *3*(3), 676-688.

ANEXOS

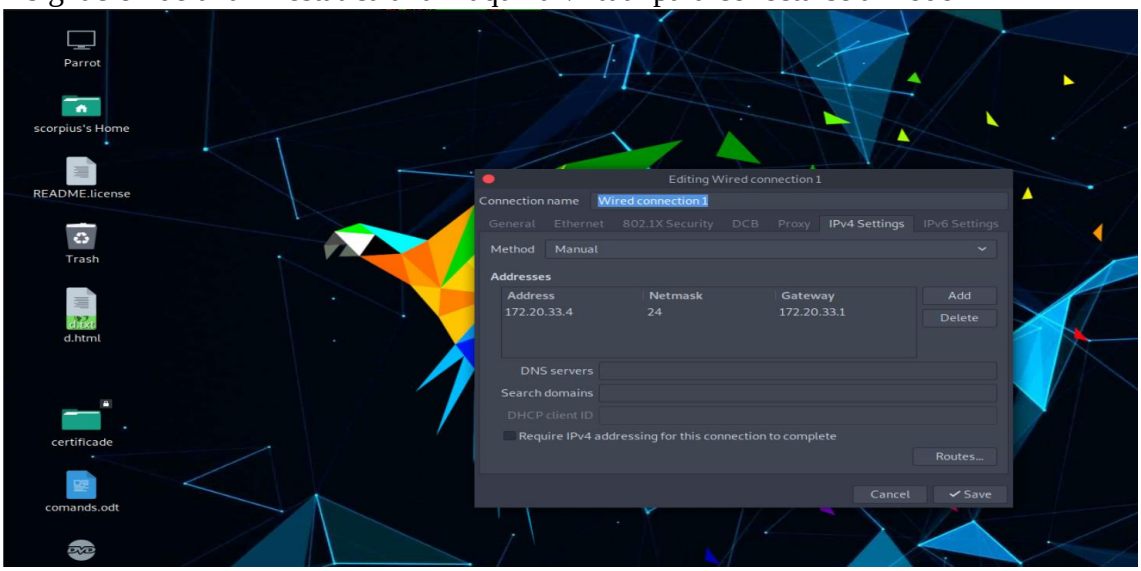
ANEXO 1: Configuración y ejecución de los ataques de sniffing a los nodos utilizando la herramienta Wireshark

Nodo MAYAMONCAYO

Asignación de una IP estática a la máquina física para conectarse al nodo

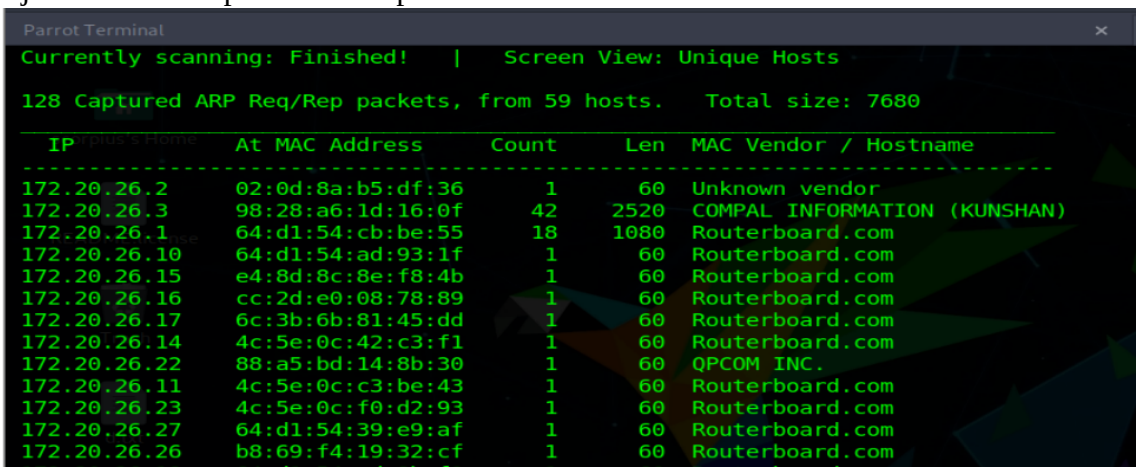


Asignación de una IP estática a la máquina virtual para conectarse al nodo

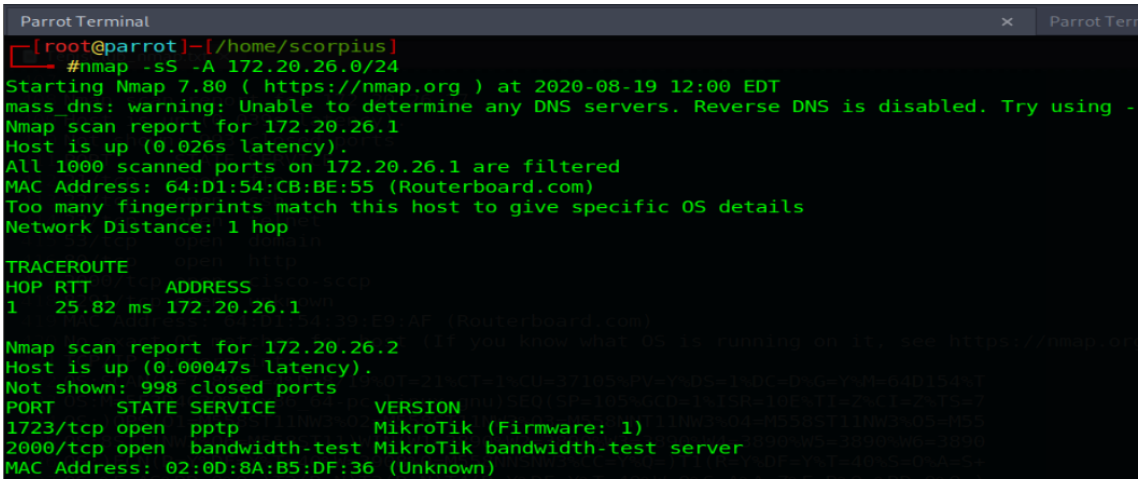


Información para conectarse al nodo MAYAMONCAYO **(IP Física:** 192.168.26.3, **IP Virtual**: 192.168.26.4, **Gateway:** 192.168.26.1**, Máscara**/24**)**

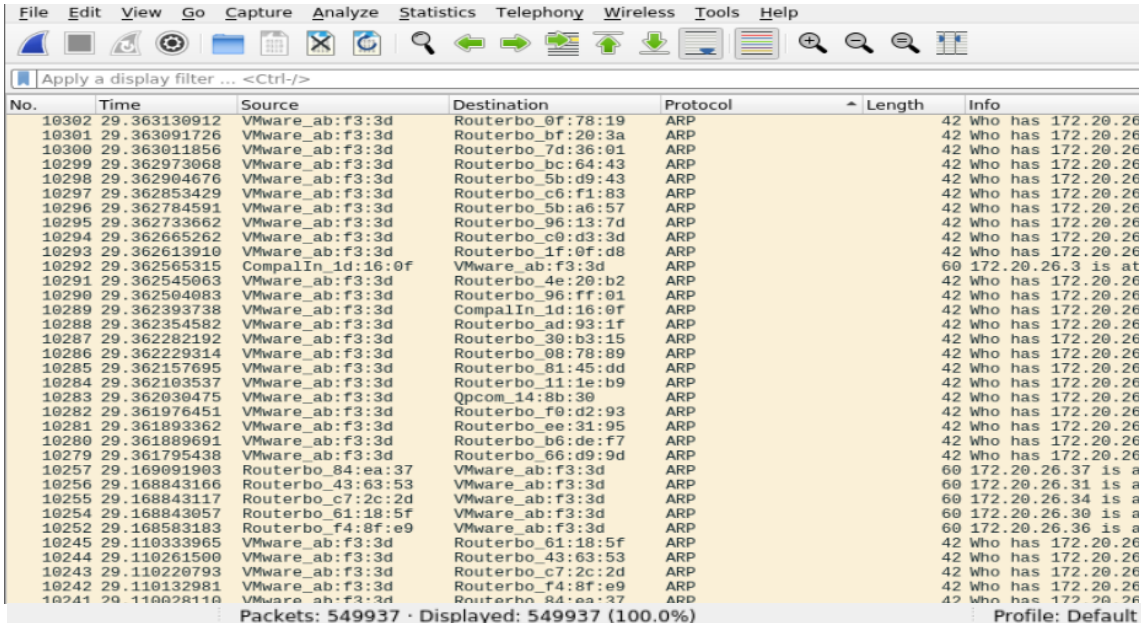
Ejecución del mapeo de la red para identificar los hosts activos.



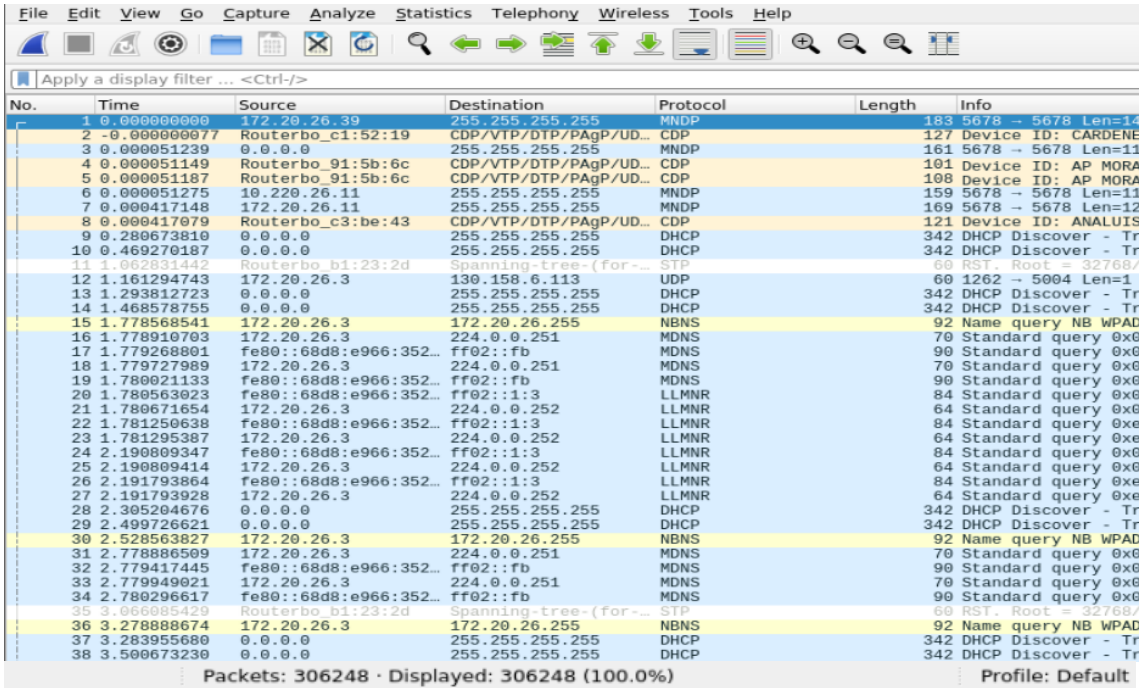
Captura y almacenamiento de la información de puertos abiertos y sistema operativo de los hosts del nodo.



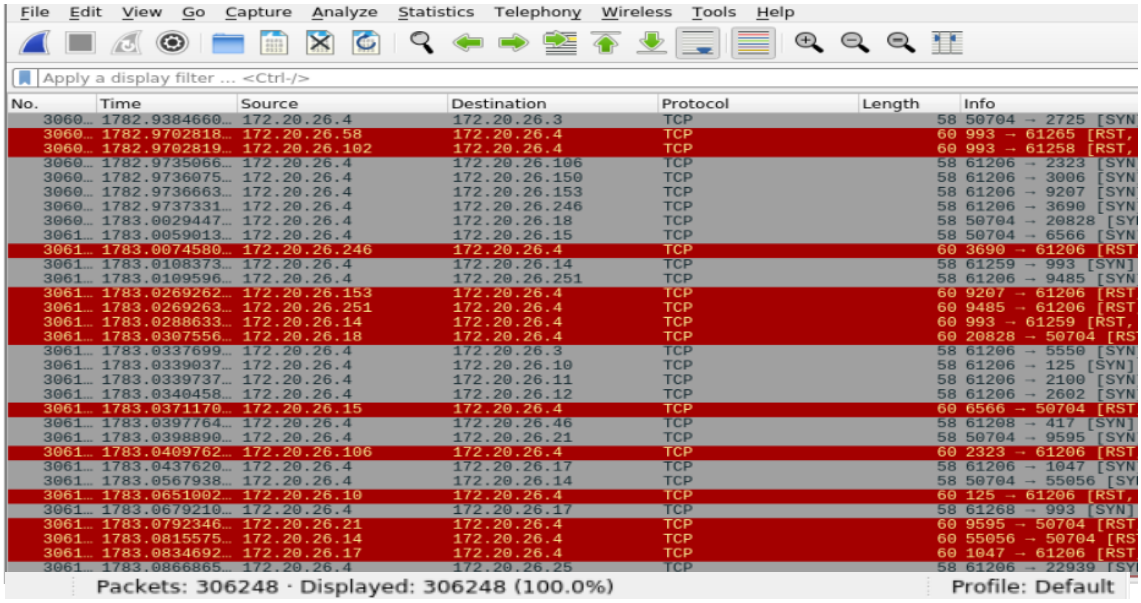
Captura de paquetes a las 10 a. m. con la herramienta Wireshark



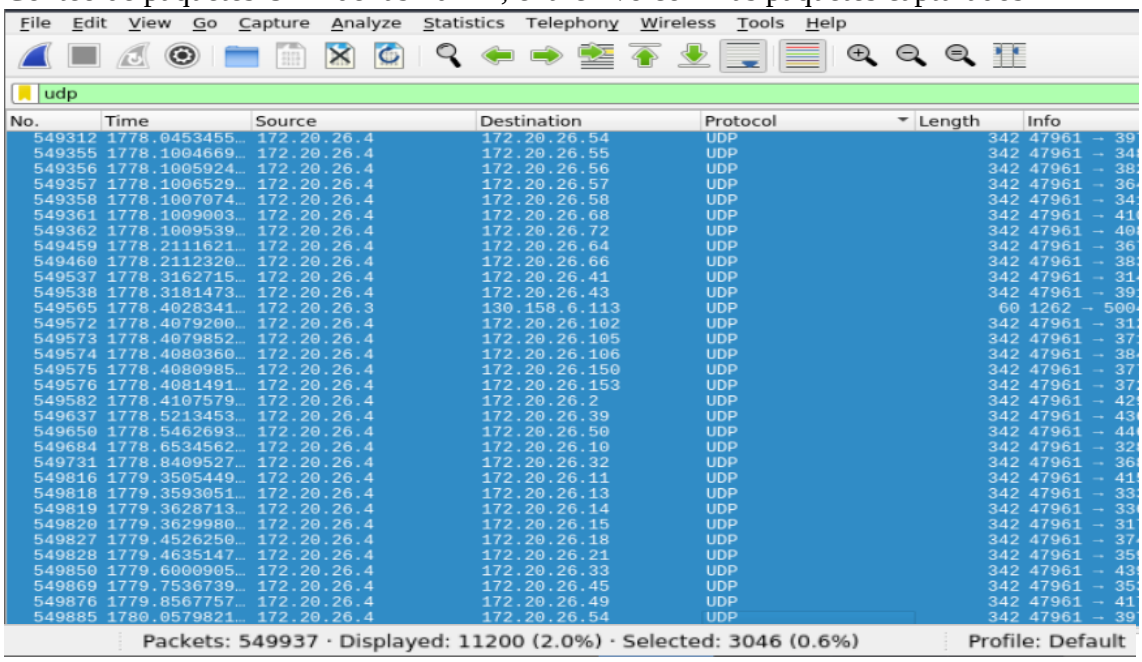
Captura de paquetes a las 4 p. m. con la herramienta Wireshark



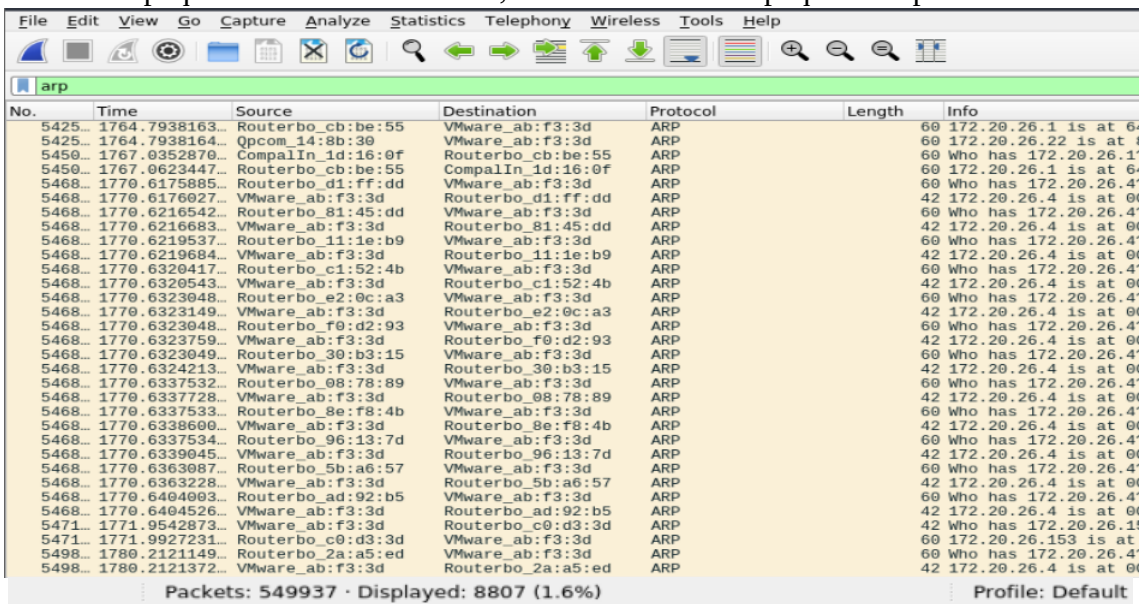
Conteo de paquetes TCP de las 10AM, el archivo con más paquetes capturados



Conteo de paquetes UDP de las 10AM, el archivo con más paquetes capturados



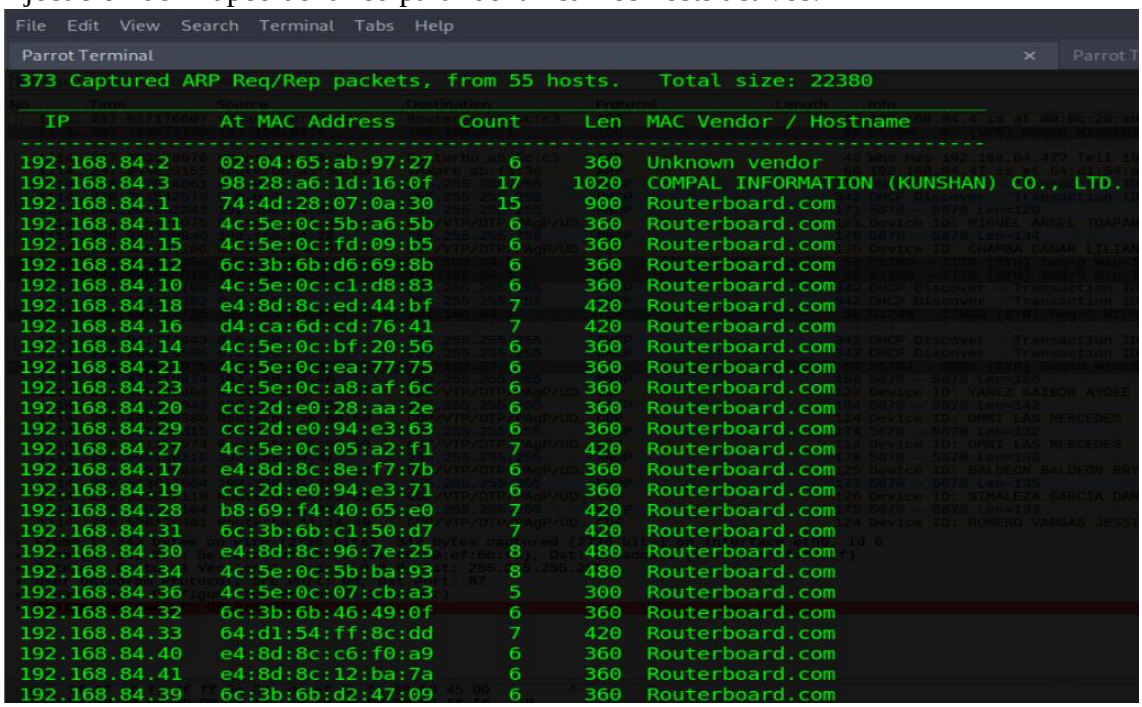
Conteo de paquetes ARP de las 10AM, el archivo con más paquetes capturados



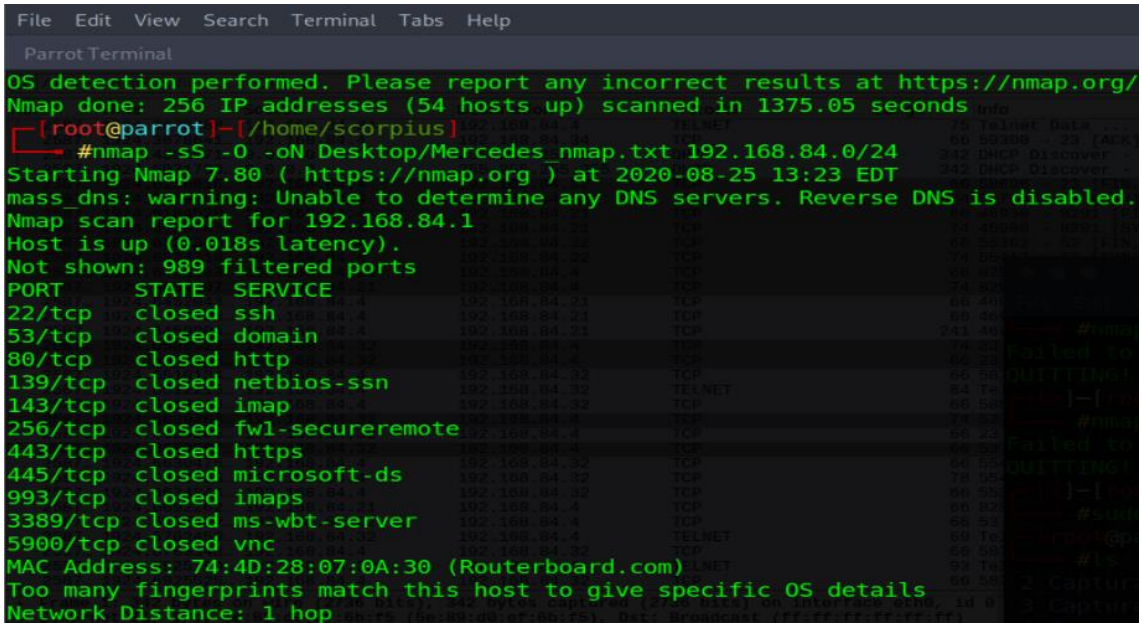
Nodo MERCEDES

Información para conectarse al nodo AVISPACHILA **(IP Física:** 192.168.84.3, **IP Virtual**: 192.168.84.4, **Gateway:** 192.168. 84.1**, Máscara**/24**)**

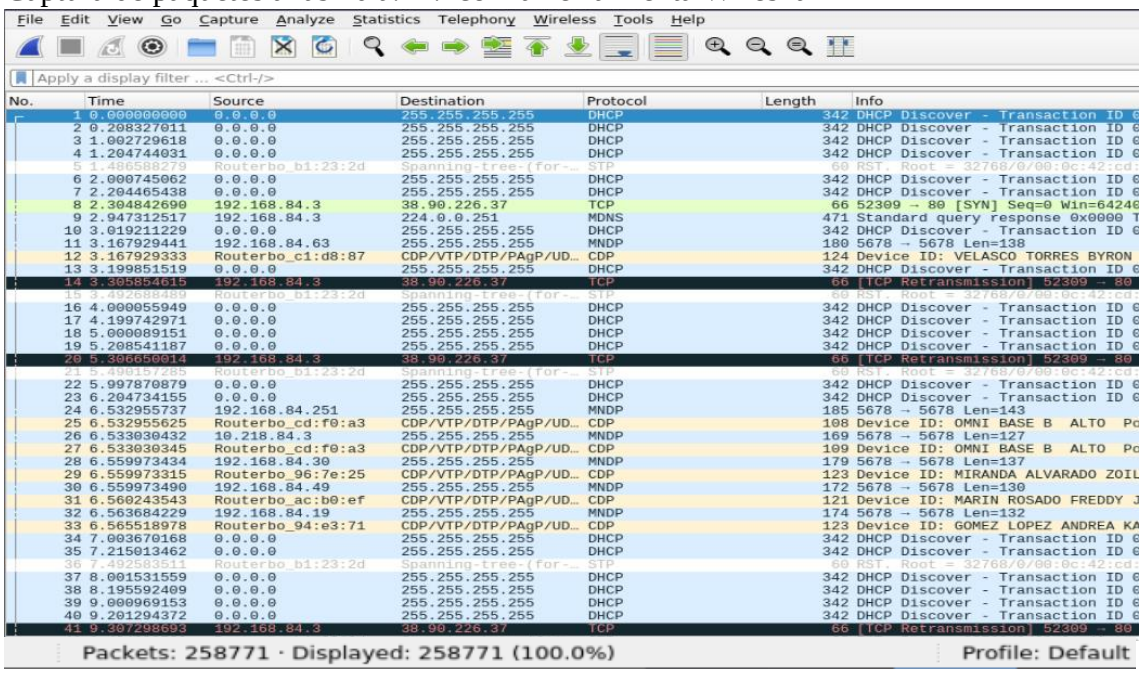
Ejecución del mapeo de la red para identificar los hosts activos.



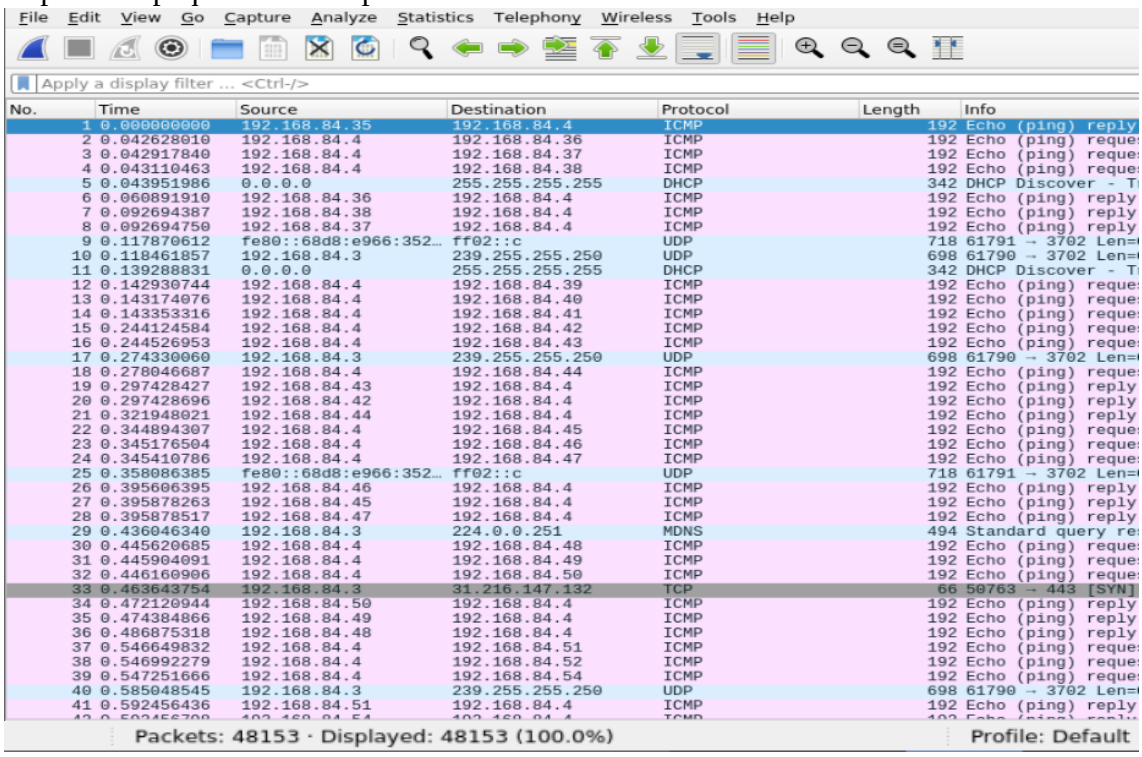
Captura y almacenamiento de la información de puertos abiertos y sistema operativo de los hosts del nodo.



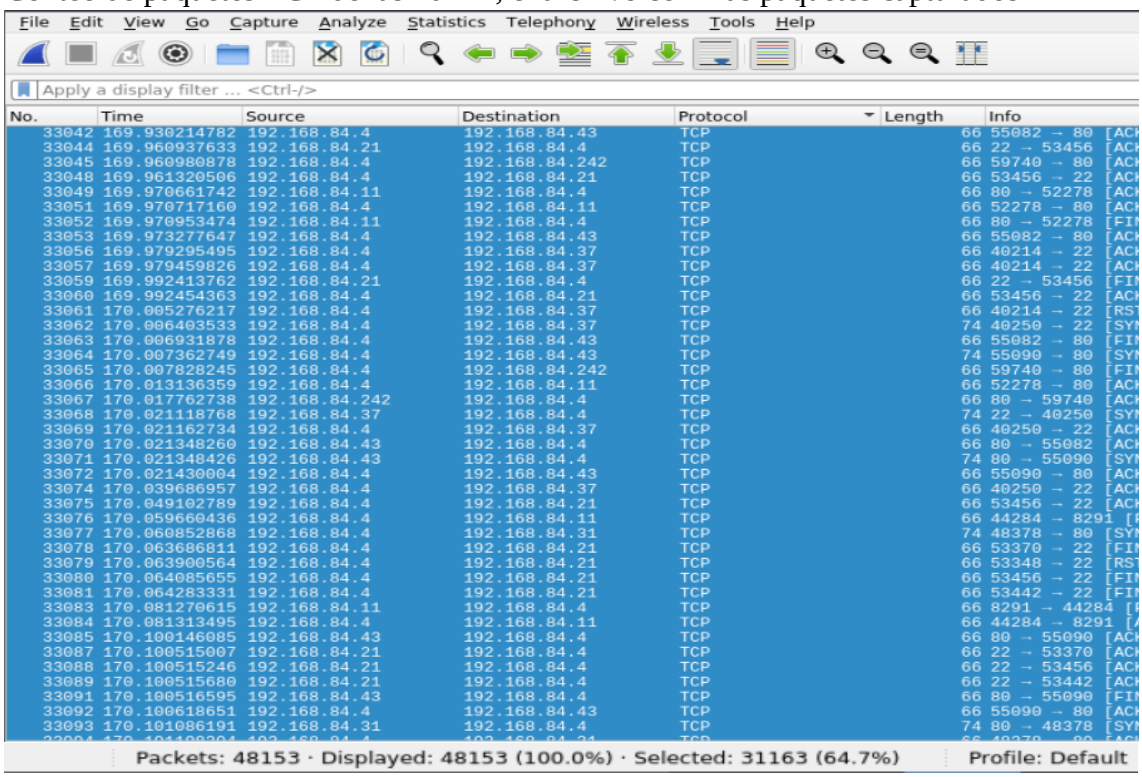
Captura de paquetes a las 10 a. m. con la herramienta Wireshark



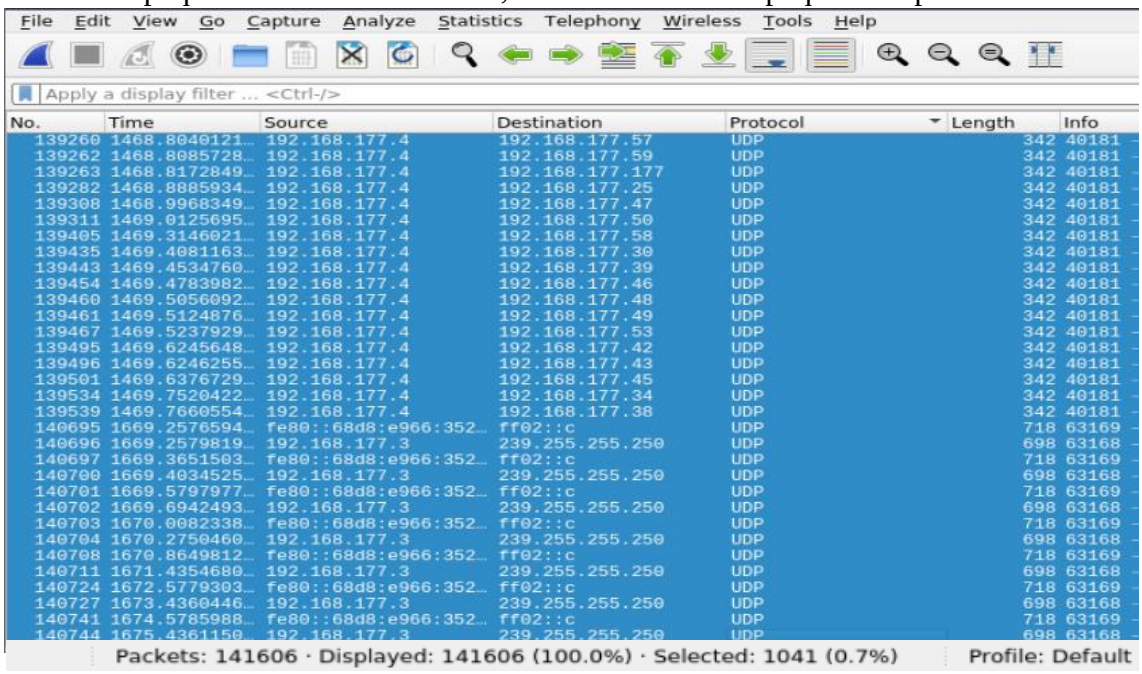
Captura de paquetes a las 4 p. m. con la herramienta Wireshark



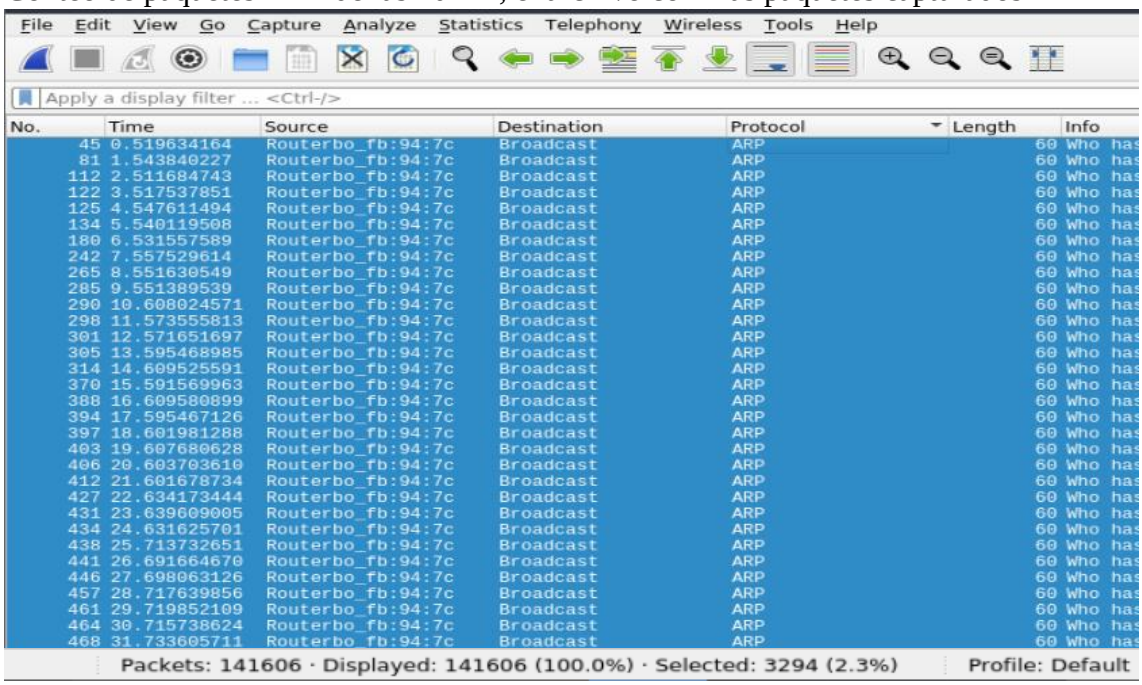
Conteo de paquetes TCP de las 10AM, el archivo con más paquetes capturados



Conteo de paquetes UDP de las 10AM, el archivo con más paquetes capturados



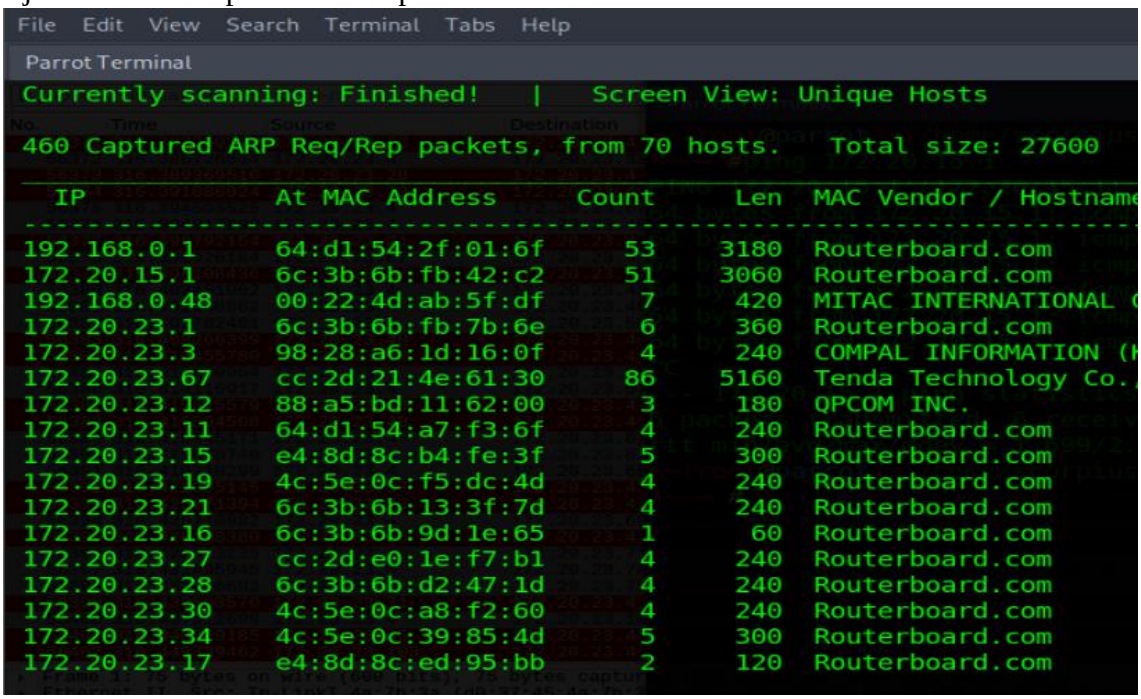
Conteo de paquetes ARP de las 10AM, el archivo con más paquetes capturados



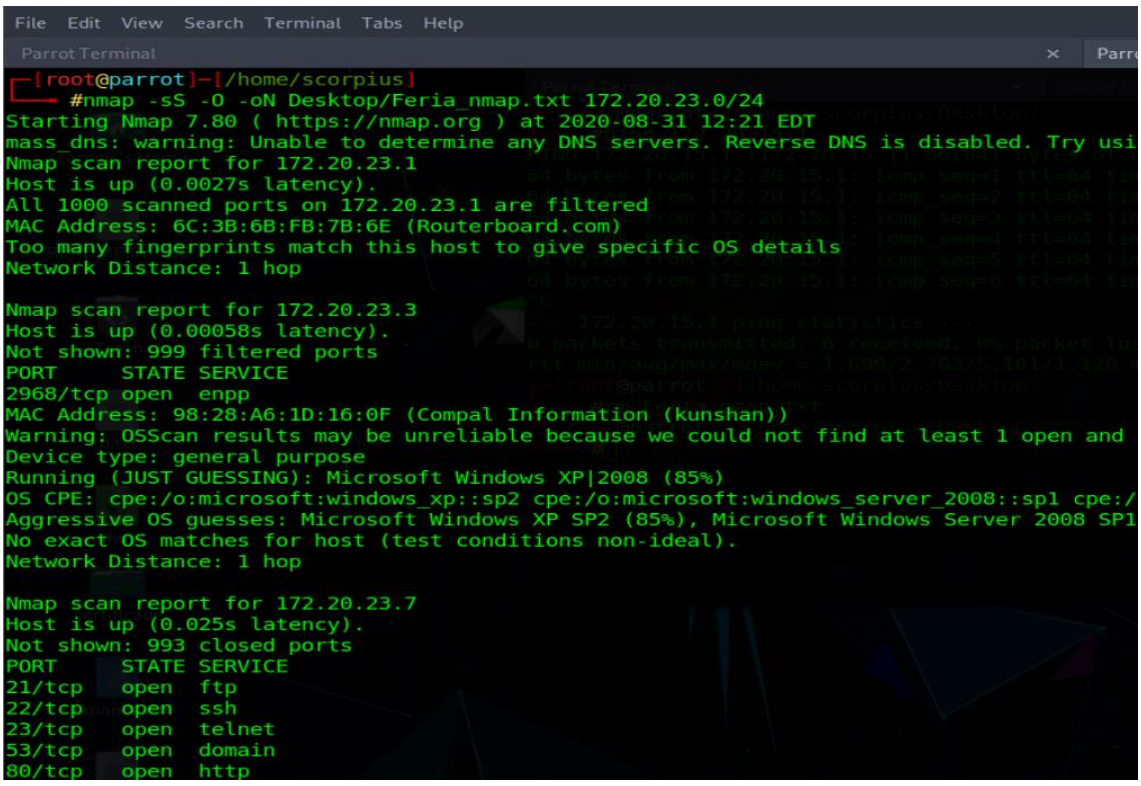
Nodo FERIA

Información para conectarse al nodo FERIA **(IP Física:** 172.20.23.3, **IP Virtual**: 172.20.23.4, **Gateway:** 172.20.23.1**, Máscara**/24**)**

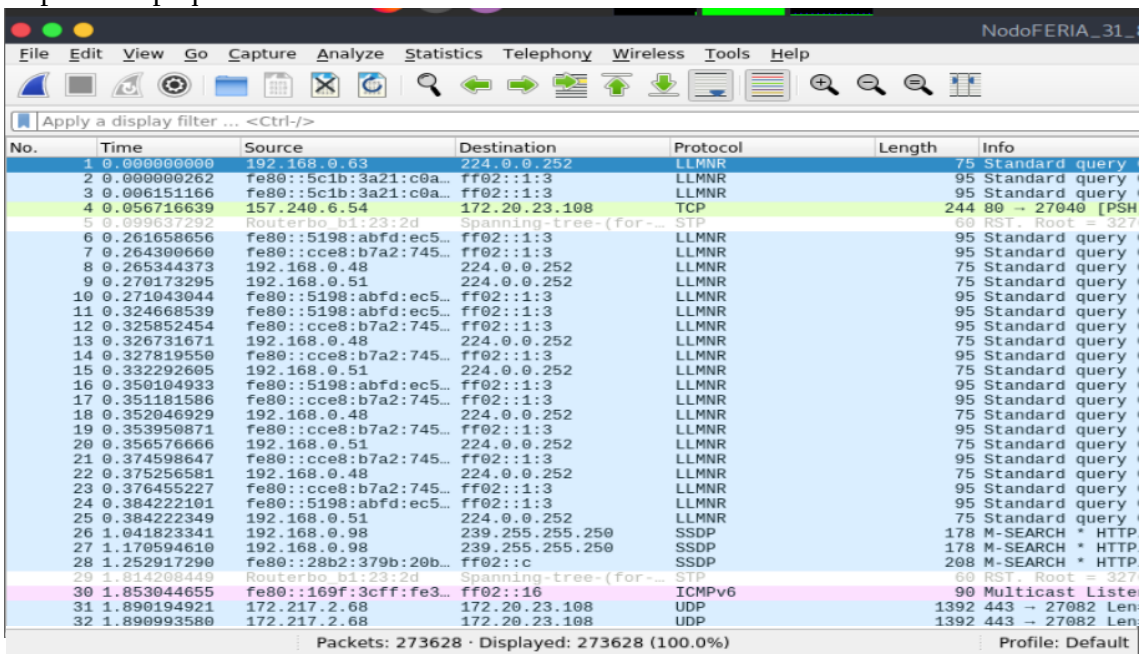
Ejecución del mapeo de la red para identificar los hosts activos.



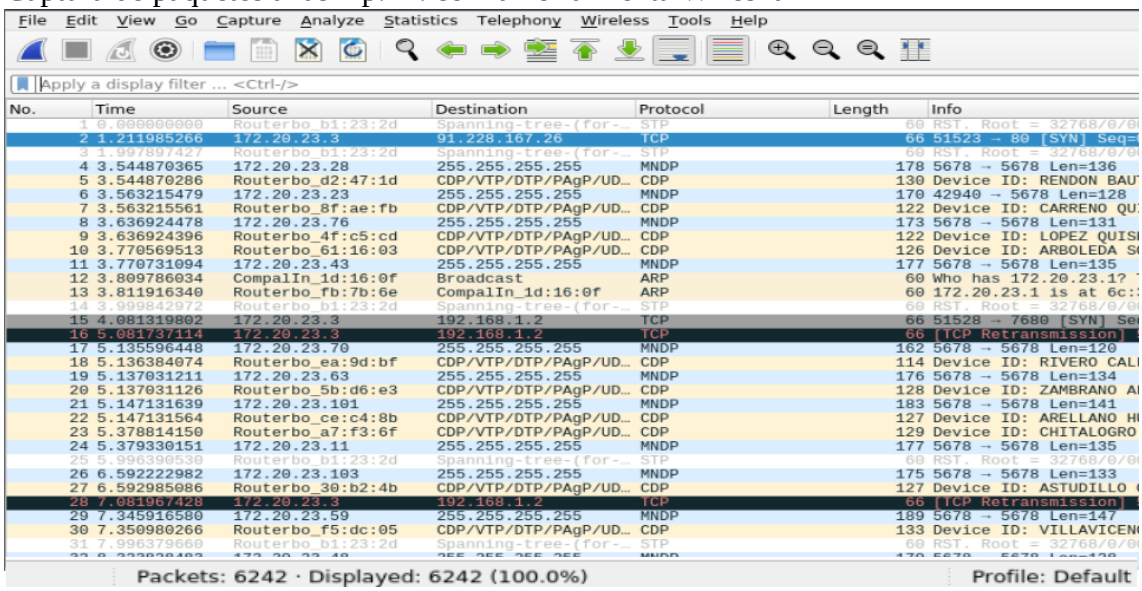
Captura y almacenamiento de la información de puertos abiertos y sistema operativo de los hosts del nodo.



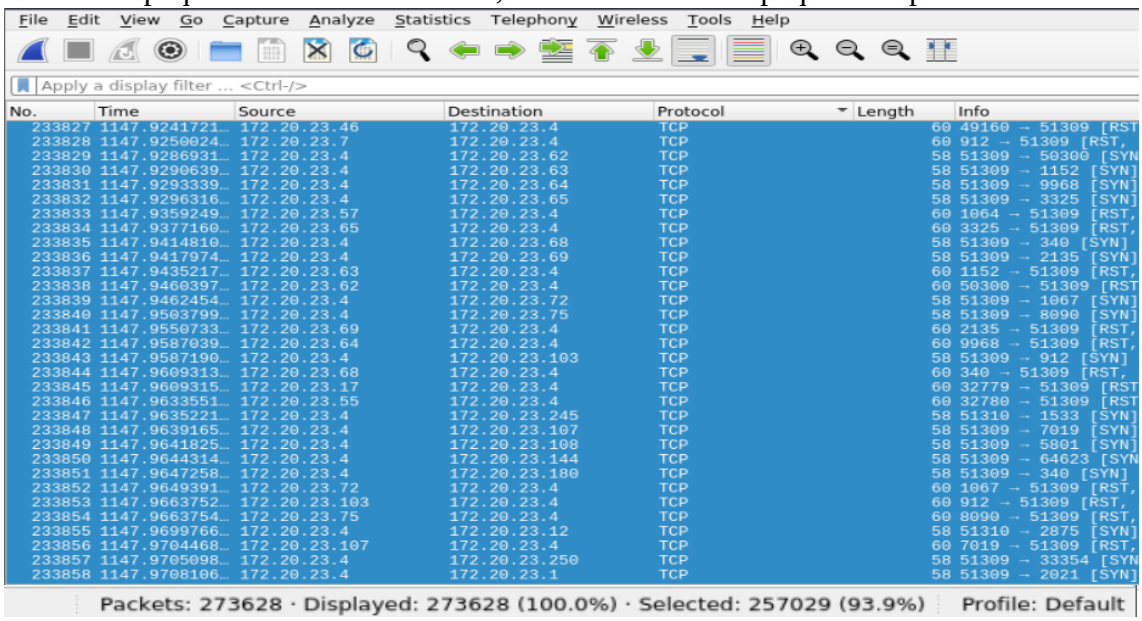
Captura de paquetes a las 10 a. m. con la herramienta Wireshark



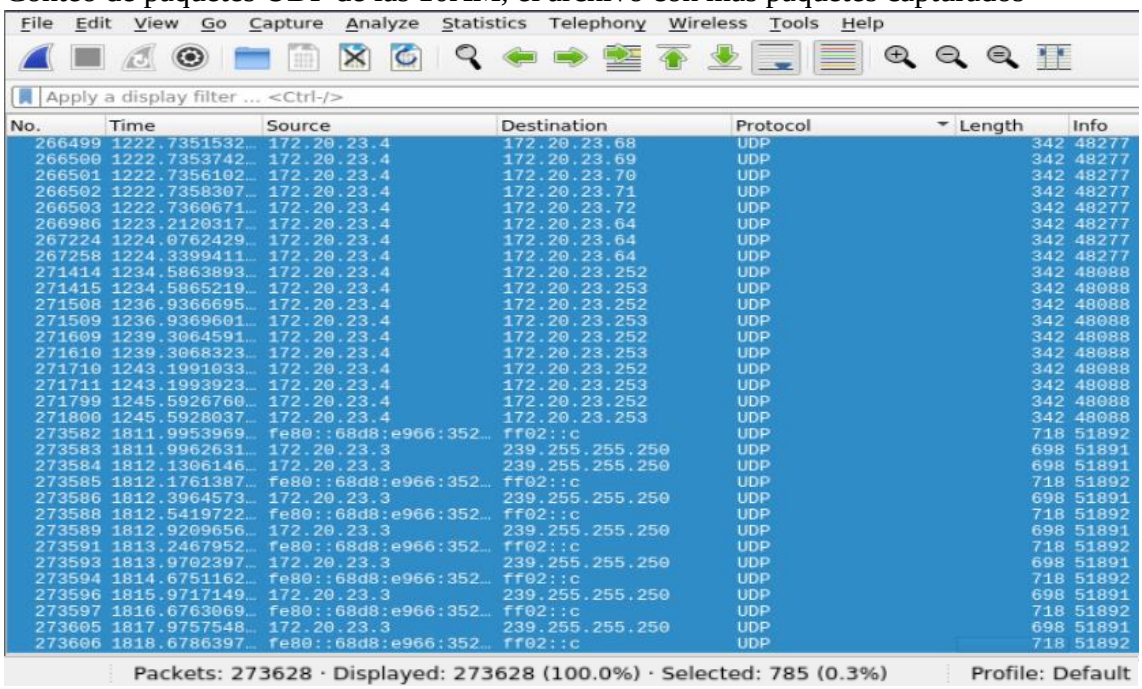
Captura de paquetes a las 4 p. m. con la herramienta Wireshark



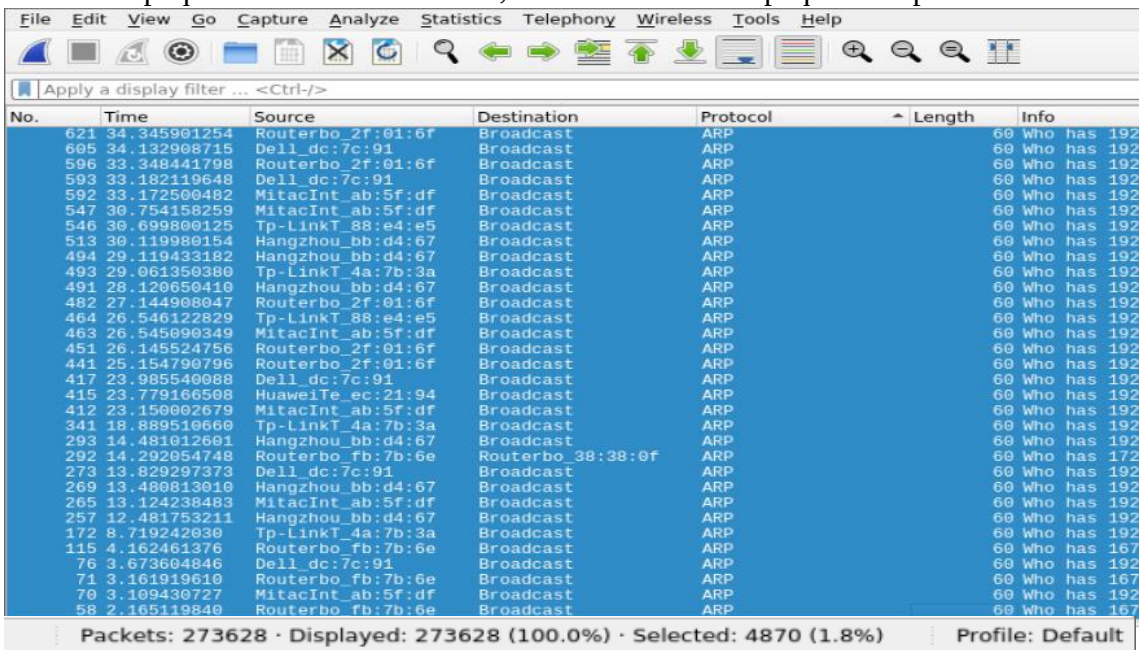
Conteo de paquetes TCP de las 10AM, el archivo con más paquetes capturados



Conteo de paquetes UDP de las 10AM, el archivo con más paquetes capturados

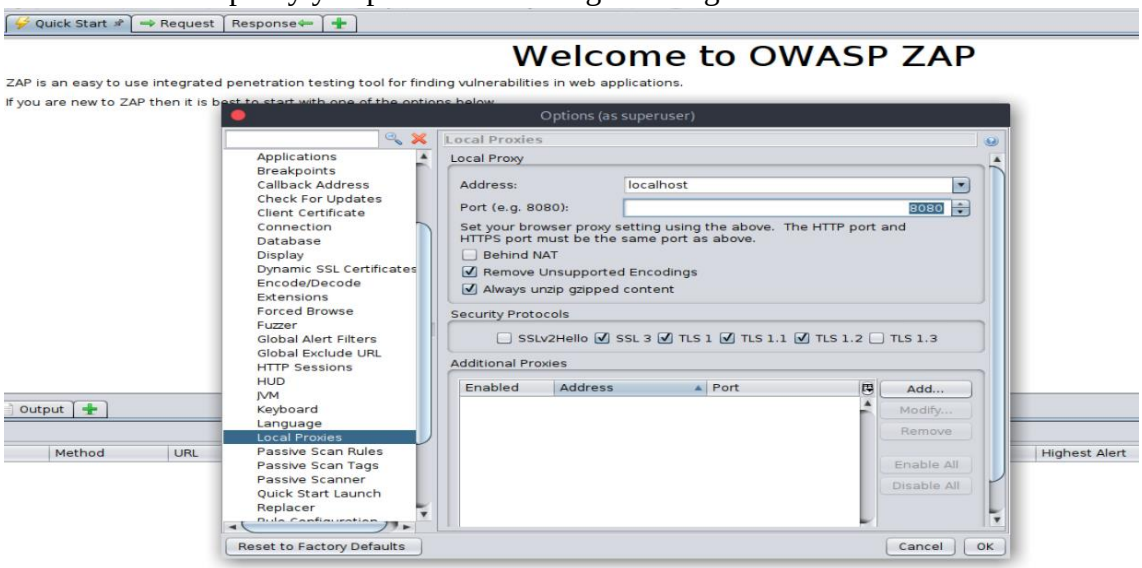


Conteo de paquetes ARP de las 10AM, el archivo con más paquetes capturados

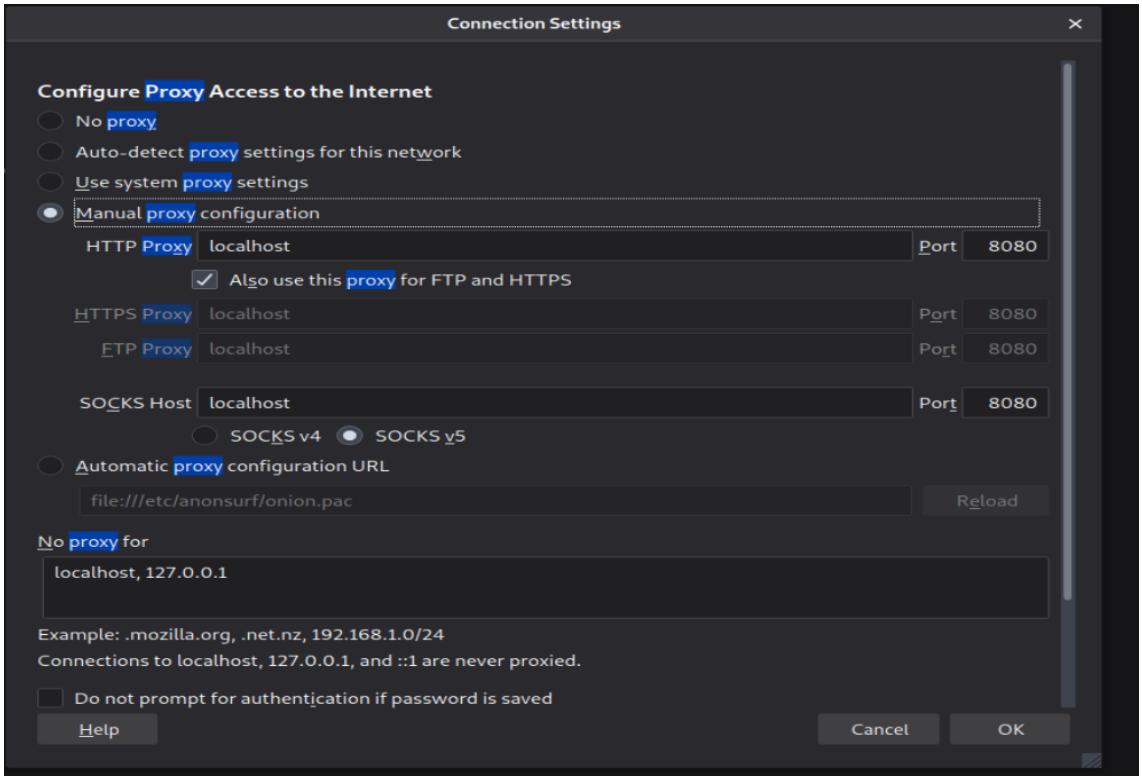


ANEXO 2: Configuración y ejecución de los ataques de parameter tampering al sistema de cobros, activación y suspensión del servicio de internet de la empresa utilizando la herramienta OWASP ZAP.

Verificar en que puerto está trabajando la herramienta para posteriormente hacer la modificación del proxy y el puerto en el navegador elegido.



Configuración del proxy local y el puerto para que todo el tráfico pase por la aplicación de OWASP ZAP.



ANEXO 3: Guía de políticas de seguridad elaborada para mitigar las infiltraciones no deseadas en la infraestructura de red de la empresa CSEDnet.

UNIVERIDAD NACIONAL DE CHIMBORAZO

Guía de Políticas de Seguridad de Red

Jairo Vera Autor

2020

Contenido

INTRODUCCIÓN

En base a las pruebas de pentesting realizadas en los nodos de la empresa SCEDnet utilizando la técnica de sniffing y la técnica de parameter tampering para identificar vulnerabilidades en el sistema que la empresa utiliza para realizar cobros, activar y desactivar el servicio de internet que prestan a sus usuarios. Se identificaron varias falencias en cuanto al aseguramiento de los dispositivos MikroTik y el sistema que usa la empresa.

Con el único fin de mitigar las amenazas producidas por las técnicas antes mencionadas se creó esta guía de políticas de seguridad en base a normas internacionales y las especificaciones y sugerencias del manual de seguridad de MikroTik

OBJETIVO

Proveer dirección y soporte a la administración de la empresa SCEDnet para mejorar la seguridad de la red que utilizan con el fin de distribuir internet a sus clientes.

GUÍA DE POLÍTICAS DE SEGURIDAD DE ACTIVOS DE INFORMACIÓN PARA LA EMPRESA SCEDNET

Protección y respaldo de la información

1. Acceso al nodo para administrarlo

1.1. Contraseña de administrador de router con alta seguridad

Usar contraseñas seguras es una de las primeras medidas para evitar que cualquier atacante acceda a los parámetros de configuración del router y obtener acceso total a la red. Para facilitar el proceso de obtener una contraseña de alta seguridad, es posible utilizar el generador de contraseñas **pwgen** o se pueden tomar en cuenta los siguientes parámetros:

- Incluir números y letras en mayúsculas y minúsculas
- Incluir un carácter especial que no sea una letra o un número
- La contraseña vence después de 90 días y la nueva contraseña debe ser diferente a las 5 contraseñas anteriores

Debido a que recordar las contraseñas de todos los nodos puede ser un problema se recomienda utilizar la herramienta de software libre **KeePassXC** para almacenar todas los nombres de usuario y las contraseñas de los diferentes nodos de la red.

1.2. Acceso por dirección IP

Además del hecho de que el firewall predeterminado protege su enrutador del acceso no autorizado desde redes externas, es posible restringir el acceso a direcciones IP concretas:

```
/user set 0 address=192.168.30.0/24
```

En donde (192.168.30.0/24) es la IP o subred que tiene permiso para acceder al enrutador.

1.3. RouterOS mac-access

Los routers por defecto tiene determinadas opciones para poder acceder a los dispositivos de red. Algunos servicios en particular deben ser deshabilitados en entornos de producción.

Mac-telnet:

Deshabilitar el acceso a través de mac-telnet:

```
/tool mac-server set allowed-interface-list=none
/tool mac-server print
```

Mac-winbox:

Deshabilitar el acceso por MAC usando Winbox:

```
/tool mac-server mac-winbox set allowed-interface-list=none
/tool mac-server mac-winbox print
```

Mac-ping:

Deshabilitar el servicio de mac-ping:

```
/tool mac-server ping set enabled=no
/tool mac-server ping print
```

1.4. Deshabilitar accesos inseguros

Mikrotik permite configurarlo vía telnet, vía SSH, por HTTP, o HTTPS. En la mayoría de los casos, se desactiva la opción de configurar por medio de HTTP, telnet, ftp, www, api, api-ssl por no ser seguras, así para una administración segura del dispositivo es recomendable utilizar SSH, HTTPS

o Winbox. En las últimas versiones, el modo seguro de Winbox está siempre activado por defecto y no puede ser desactivado.

```
/ip service disable telnet,ftp,www,api,api-ssl
/ip service print
```

1.5. Puertos de acceso al router

Al modificar los puertos de acceso al router se añade una capa de seguridad extra de acceso al router. Para acceder a la configuración del router no sólo hace falta usuario y contraseña, si no que ahora es necesario saber el puerto. Así, por ejemplo, bloquear los intentos de acceso a través de SSH o Winbox.

```
/ip service set winbox port=2200
/ip service print
```

1.6. IPs de acceso al router

Al hacer que cada servicio debe ser restringido a determinadas direcciones IP se evita que personas ajenas a los administradores generen intentos de acceso.

```
/ip service set winbox address=192.168.30.0/24
```

1.7. Acceso SSH más seguro

RouterOS usa una encriptación fuerte para el acceso por SSH. Gran parte de los programas la usan. Para activarla:

```
/ip ssh set strong-crypto=yes
```

```
/ip ssh print
```

1.8. Inicio de sesión SSH siempre con contraseña:

Para que cada vez que se acceda a través de SSH pida la contraseña de acceso es necesario habilitar esta opción mediante:

```
/ip ssh set always-allow-password-login=yes
/ip ssh print
```

2. Disuasión de Ataques

2.1. Filtrado MAC

Esta medida no deja de ser una medida disuasoria ya que las técnicas MAC Spoofing permiten a un usuario cambiar la dirección MAC de su dispositivo, y un atacante podría cambiarla por una que se encuentre en la lista de MAC´s autorizadas. No deja de ser una primera barrera para atacantes inexpertos.

2.2. Parámetros modificados

El empleo de parámetros por defecto hace la red vulnerable a ataques de diccionario. Los parámetros para modificar son: dirección IP de acceso al router, puerto de acceso SSH, SSID, contraseña (en el caso de OpenWrt, la red hay que configurarla de cero, pero routers de ISP traen la red configurada por defecto).

2.3. Interfaces del Router

Ethernet/SFP

Es una buena práctica deshabilitar las interfaces que no vas a usar de tu router, para así de alguna forma reducir el riesgo de intrusión a tu dispositivo.

```
/interface set x disabled=yes
```

x – Número del interfaz que queremos deshabilitar (ether1, ether2, etc)

3. Mecanismos de Exploración

3.1. Limitar las conexiones de Mapeo

Dentro de RouterOS, se puede generar un script el cual analiza automáticamente si una IP en particular está tratando de hacer un mapeo de puertos.

```
/ip firewall filter add chain=input protocol=tcp psd=21,3s,3,1 action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w comment="Port scanners to list " disabled=no

/add chain=input src-address-list=port-scanners action=drop
```

4. Protección contra mecanismos de explotación

4.1. Limitar las conexiones entrantes (Black List)

Se puede agregar una dirección IP a una lista negra cuando ha tenido demasiados intentos de conexión. En este ejemplo LIMIT es el número máximo de conexiones por IP. LIMIT debe tener un valor de 100 o incluso

más, ya que muchos servicios utilizan conexiones múltiples (HTTP, Torrent, otros programas P2P).

```
/ip firewall filter add chain=input protocol=tcp connection-limit=10,32 action=add-src-to-address-list address-list=blocked-addr address-list-timeout=1d
```

4.2. TARPIT

Disminuye el ancho del host paulatinamente hasta inhabilitarlo, a diferencia del DROP que corta la comunicación momentáneamente, pero después de cierto tiempo, el host se puede volver a conectar. Se debe realizar un TARP y no un DROP solo si el uso del CPU del mikrotik no excede del 25-30% de uso normal promedio.

```
/ip firewall filter add chain=input protocol=tcp src-address-list=blocked-addr connection-limit=3,32 action=tarpit
```

4.3. SYNFILTER (SYN FLOOD)

Protección para Mecanismos de Exploits incluido el Sniffing. Evita que la comunicación TCP sea interrumpida, y que en el servidor se acumulen paquetes incompletos, descartándolos cuando existe un número excesivo de conexiones.

```
/ip firewall filter add chain=forward protocol=tcp tcp-flags=syn connection-state=new action=jump jump-target=SYN-Protect comment= “SYN Flood protect” disable=yes
```

```
/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn limit=400,5 connection-state=new action=accept comment=”” disabled=no

/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn connection-state=new action=drop comment=”” disabled=no
```

4.4. SYN cookies (Complementa el paso anterior)

Esta técnica se utilizada para resistir los ataques de suplantación de IP, en mi caso para las pruebas de sniffing que realice, utilice una máquina virtual con conexión bridge.

Para version 6 RouterOS:

```
/ip settings set tcp-syncookies=yes
```

Para versions menores a 6 RouterOS:

```
/ip firewall connection tracking set tcp-syncookies=yes
```

4.5. Protección para guardar los LOGs

Los archivos de LOGs, inicialmente se guardan en la memoria del equipo, por lo que un simple reinicio los borra permanentemente. Configurar la opción “remote” en el logging de RouterOS, apuntando hacia un servidor de Syslog externo.

Fuerza Bruta

Agrega a un address list temporal la IP del host que realiza una conexión por cada intento de login, fallido o no, al completar 4 intento se agrega a un blacklist donde se hace drop por 15 dias.

```
/ip firewall filter
add chain=input protocol=tcp dst-port=8291 src-address-
list=winbox_blacklist action=drop \
comment="Drop Winbox brute forcers" disabled=no
add chain=input protocol=tcp dst-port=8291 connection-
state=new src-address-list=winbox_login3 \
action=add-src-to-address-list address-
list=winbox_blacklist address-list-timeout=15d disabled=no
add chain=input protocol=tcp dst-port=8291 connection-
state=new src-address-list=winbox_login2\
action=add-src-to-address-list address-list=winbox_login3
address-list-timeout=1m disabled=no
add chain=input protocol=tcp dst-port=8291 connection-
state=new src-address-list=winbox_login1 \
action=add-src-to-address-list address-list=winbox_login2
address-list-timeout=1m disabled=no
add chain=input protocol=tcp dst-port=8291 connection-
state=new action=add-src-to-address-list \
address-list=winbox_login1 address-list-timeout=1m
disabled=no
```