UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

DICIEMBRE 2022-ABRIL 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TITULO DE

INGENIERO(A) EN SISTEMAS DE INFORMACIÓN

TEMA:

CONTROL DE AMENAZAS E INSTRUCCIONES INFORMATICAS EN UNA RED DOMESTICA BASADAS EN OPEN SOURCE.

EGRESADA:

LEMA ALTAMIRANO DAYANNA ESTHER

TUTOR:

ING. CARLOS SOTO VALLE

AÑO 2023

RESUMEN

Control de amenazas: 1. Instalar un cortafuegos de software de código abierto: instalar un cortafuegos de software de código abierto, como pfSense, para bloquear el acceso a la red doméstica de sitios web maliciosos. 2. Establecer una política de contraseñas fuertes: establecer una política de contraseñas fuertes para todos los dispositivos conectados a la red doméstica, como mínimo 8 caracteres alfanuméricos y al menos una letra mayúscula, una letra minúscula y un número. 3. Actualizar los sistemas operativos y el software: es importante mantener actualizados los sistemas operativos y el software a su última versión, para evitar la explotación de vulnerabilidades conocidas. La seguridad de la red doméstica es una preocupación cada vez mayor para los propietarios de hogares. Debido a los constantes avances tecnológicos, los propietarios de hogares ahora tienen que prestar atención a una amplia variedad de amenazas informáticas a su red doméstica, incluyendo virus, spyware, malware, ataques de negación de servicio y, en algunos casos, incluso ataques de phishing. Para hacer frente a estas amenazas, los propietarios de hogares deben tener una buena comprensión de los principios básicos de la seguridad informática y cómo implementar estos principios en su red doméstica. Uno de los mejores enfoques para mantener la seguridad de la red doméstica es la implementación de una solución basada en open source. Estas soluciones se basan en software de código; El control de amenazas e intrusos en una red doméstica basada en open source es un desafío importante. En la mayoría de los casos, la configuración de un firewall para bloquear el tráfico malicioso es una medida básica para la seguridad de la red. Sin embargo, existen otros métodos que deben tenerse en cuenta para proteger la red de una variedad de amenazas informáticas. Estos incluyen el uso de herramientas de detección de intrusiones y la implementación de políticas de seguridad para limitar el acceso a la red y a los recursos. Además, se deben tomar medidas para asegurar que los sistemas operativos y las aplicaciones estén

actualizados para prevenir la explotación de vulnerabilidades conocidas. Finalmente, se deben tomar medidas para monitorear el tráfico de la red para detectar cual

Palabras claves: Código Abierto, Sistema Operativo, Control de Amenazas, Vulnerabilidad.

ABSTRACT

Threat control: 1. Install an open-source software firewall – Install an open-source software firewall, such as pfSense, to block malicious websites from accessing your home network. 2. Establish a strong password policy: Establish a strong password policy for all devices connected to the home network, at least 8 alphanumeric characters and at least one uppercase letter, one lowercase letter, and one number. 3. Update operating systems and software: It is important to keep operating systems and software updated to their latest version, to avoid exploiting known vulnerabilities. Home network security is a growing concern for homeowners. Due to constant technological advances, homeowners now have to pay attention to a wide variety of computer threats to their home network, including viruses, spyware, malware, denial of service attacks, and in some cases even phishing attacks. . To deal with these threats, homeowners must have a good understanding of basic computer security principles and how to implement these principles in their home network. One of the best approaches to keep your home network secure is to implement an open source-based solution. These solutions are based on code software; Threat and intrusion control in an open source-based home network is a major challenge. In most cases, configuring a firewall to block malicious traffic is a basic measure for network security. However, there are other methods that must be considered to protect the network from a variety of computer threats. These include the use of intrusion detection tools and the implementation of security policies to limit access to the network and resources. In addition, steps must be taken to ensure that operating systems and applications are up to date to prevent the exploitation of known vulnerabilities. Finally, steps should be taken to monitor network traffic to detect which

Keywords: Open Source, Operating System, Threat Control, Vulnerability.

INDICE GENERAL

PLANTEAMIENTO DEL PROBLEMA 1

JUSTIFICACIÓN 3

OBJETIVOS DE LA INVESTIGACIÓN 3

Objetivo general de la investigación 6

Objetivo específico de la investigación 6

LÍNEA DE INVESTIGACIÓN 6

MARCO CONCEPTUAL 7

1.2. Conceptos Generales 7

1.2.1. La seguridad 7

1.2.3. Seguridad de la información 9

1.2.4. Segmentación de la red 11

1.2.5. Router Dual Band 11

1.2.6. Firewalls 11

1.2.7. Sistema de Detección de Intrusos (IDS) 11

1.2.8. Sistema de Prevención de Intrusos (IPS) 12

1.2.9. Open Source 12

1.2.10. Seguridad en Open Source 13

1.2.11. Software de prevención de intrusos (IPS) Tp-Link Tether 13

1.2.12. Amenazas informáticas 14

RESULTADOS 16

DISCUSIÓN DE RESULTADO 18

CONCLUSIONES 18

ANEXOS 23

PLANTEAMIENTO DEL PROBLEMA

El control de amenazas e instrucciones informáticas en una red doméstica basada en open source es un problema complejo. Las amenazas informáticas son cada vez más sofisticadas y están diseñadas para evadir los sistemas de seguridad existentes. Esto significa que los propietarios de redes domésticas basadas en open source deben asegurarse de que sus sistemas de seguridad estén actualizados y sean capaces de detectar y responder a amenazas emergentes. Para abordar este problema, los propietarios de redes domésticas basadas en open source deben implementar una variedad de medidas de seguridad, como la instalación de cortafuegos, la configuración de seguridad de la red, el uso de software antivirus y antimalware, el filtrado de contenido y el cifrado de datos. Además, los propietarios de redes domésticas basadas en open source deben tomar medidas para asegurarse de que las instrucciones informáticas que se ejecutan en la red estén autorizadas y que los usuarios no estén expuestos a riesgos innecesarios. Esto incluye la configuración de los permisos de seguridad para aplicaciones y servicios, la restricción de la ejecución de aplicaciones sospechosas, y la implementación de una política de seguridad para el uso y almacenamiento de datos. Finalmente, los propietarios de redes domésticas basadas en open source deben implementar una rutina de monitoreo para detectar y responder a amenazas informáticas y otras actividades no autorizadas. Esto incluye la monitorización de tráfico de red, el análisis de actividades sospechosas, la identificación de vulnerabilidades y la recolección de datos para la investigación de incidentes de seguridad.

Así también, el control de amenazas e intrusiones informáticas en una red doméstica basada en open source es un desafío importante. Esto se debe a que la red basada en open source carece de una seguridad centralizada. Esto significa que no hay un sistema de seguridad centralizado que

verifique la seguridad de cada elemento de la red. Esto deja a los usuarios vulnerables a los ataques de hackers y al software malicioso. Una forma de abordar este problema es mediante el uso de herramientas de seguridad de código abierto. Estas herramientas pueden detectar amenazas y ayudar a prevenir el acceso no autorizado a la red. Estas herramientas pueden incluir firewalls, sistemas de detección de intrusiones, y otros productos de seguridad. Estas herramientas ayudarán a asegurar que los usuarios estén protegidos contra amenazas y intrusiones. Otra forma de abordar este problema es mediante el uso de soluciones de seguridad de terceros. Estas soluciones pueden incluir antivirus, cortafuegos, cortafuegos virtuales, sistemas de detección de intrusiones, y otros productos de seguridad. Estas soluciones pueden proporcionar una seguridad más robusta que los productos de código abierto, pero es importante recordar que estas soluciones también pueden ser vulnerables a ataques. Además, los usuarios deben asegurarse de que todos los dispositivos estén actualizados con las últimas versiones de los sistemas operativos y aplicaciones. Esto ayudará a prevenir vulnerabilidades y asegurará que los usuarios estén protegidos. Finalmente, los usuarios deben asegurarse de que todos los dispositivos tengan una contraseña segura y no compartan la contraseña con nadie. Esto evitará que los hackers tengan acceso a la red. Estas son algunas de las formas en que los usuarios pueden abordar el problema de control de amenazas e intrusiones informáticas en una red doméstica basada en open source.

JUSTIFICACIÓN

La justificación para el control de amenazas e intrusiones informáticas en una red doméstica basada en open source es que es una forma eficaz de proteger la red de los ataques cibernéticos. Esto es especialmente importante para los hogares, ya que tienden a ser menos seguros que las redes empresariales, debido a los dispositivos que se ejecutan en la red. Los dispositivos domésticos suelen tener menos protección que los dispositivos empresariales, lo que los hace más vulnerables a los ataques cibernéticos. Esto significa que, si un atacante cibernético puede acceder a la red doméstica, podría comprometer a los usuarios, sus datos y dispositivos conectados a la red. Por lo tanto, es importante que los usuarios instalen una solución de control de amenazas e intrusiones para protegerse a sí mismos y a sus dispositivos. Las soluciones de control de amenazas e intrusiones basadas en open source pueden proporcionar una protección adecuada para los usuarios de redes domésticas, ya que proporcionan una variedad de características de seguridad para ayudar a proteger la red. Estas características incluyen protección contra virus y malware, análisis de tráfico y registros, filtrado de contenido, detección de intrusos y mucho más. Además, algunas soluciones de control de amenazas e intrusiones basadas en open source también proporcionan herramientas para ayudar a los usuarios a monitorear y administrar sus redes. Esto les permite detectar intrusiones y amenazas potenciales, así como aplicar parches y configuraciones de seguridad para ayudar a prevenir futuros ataques. En conclusión, el control de amenazas e intrusiones informáticas en una red doméstica basada en open source es una forma eficaz de protegerse a sí mismo y a sus dispositivos. Ofrece una variedad de características y herramientas para ayudar a proteger la red y detectar cualquier amenaza potencial. Esto es especialmente importante para los hogares, ya que son más vulnerables a los ataques cibernéticos.

Por lo tanto, los usuarios de redes domésticas deberían considerar la instalación de una solución de control de amenazas e intrusiones basada en open source para ayudar a proteger su red.

Las amenazas informáticas son una amenaza real en el entorno de una red doméstica. Pueden provocar pérdida de datos, violación de la privacidad, robos de información, bloqueos de aplicaciones y sistemas, etc. Para proteger su red doméstica, es importante establecer controles de amenazas y seguir prácticas de seguridad informática. La mejor manera de mantener la seguridad informática de su red doméstica es implementar un sistema de control de amenazas basado en open source. Esto significa que los usuarios finales tienen acceso al código fuente del sistema de control de amenazas, lo que les permite comprender cómo funciona el sistema y cómo pueden usarlo para protegerse. Además de esto, el sistema de control de amenazas open source también ofrece una variedad de herramientas de seguridad informática, como firewalls, sistemas de detección de intrusiones, análisis de contenido web, etc. Estas herramientas ayudan a detectar y prevenir amenazas informáticas, lo que ayuda a garantizar la seguridad de la red. Finalmente, los sistemas de control de amenazas open source también ofrecen una variedad de instrucciones informáticas, como directivas de seguridad, procedimientos de seguridad y recomendaciones de seguridad para ayudar a los usuarios finales a mantener la seguridad de su red doméstica. Estas instrucciones le ayudarán a entender cómo usar correctamente el sistema de control de amenazas y optimizar su seguridad informática.

La seguridad informática es un tema importante para cualquier red domestica basada en open source. Controlar las amenazas e instrucciones informáticas ayuda a proteger los dispositivos conectados a la red contra el malware, la suplantación de identidad y otros problemas de seguridad.

Esto se logra configurando una variedad de medidas de seguridad, como el control de acceso, el filtrado de contenido y la protección contra ataques de denegación de servicio. Estas herramientas permiten controlar qué usuarios tienen acceso a la red, limitar qué contenido se puede acceder y prevenir el uso indebido de los recursos de la red. Estas herramientas también ayudan a proteger la red contra ataques de intrusos externos, ya que establecen reglas sobre quién puede acceder a la red y qué acciones están permitidas. Esto ayuda a reducir el riesgo de que la red sea comprometida por un hacker. El control de amenazas e instrucciones informáticas también puede ayudar a prevenir la propagación de malware, ya que los usuarios no podrán descargar archivos maliciosos o visitar sitios web que contengan malware. Esto ayuda a asegurar que los dispositivos conectados a la red no sean infectados con malware, lo que puede provocar graves problemas de seguridad.

La principal amenaza a la seguridad de una red doméstica basada en open source es el malware. Este tipo de código malicioso o programas malintencionados son creados con el objetivo de dañar el sistema o robar información confidencial de los usuarios. Estos programas se pueden propagar a través de archivos adjuntos de correo electrónico, descargas de sitios web, dispositivos externos (como una memoria USB) o incluso a través de la conexión a redes Wi-Fi públicas. Para prevenir los ataques de malware, se recomienda a los usuarios de una red doméstica basada en open source que mantengan actualizados todos sus programas y sistemas operativos. Esto evitará que los ciberdelincuentes aprovechen las vulnerabilidades conocidas para atacar la red. Además, se debe tener una solución de seguridad antivirus/antimalware instalado para detectar y bloquear cualquier intento de ataque. Otra medida de seguridad recomendada para redes domésticas basadas en open source es el uso de un cortafuegos. El cortafuegos ayuda a bloquear el tráfico entrante no deseado y a proteger la red contra ataques externos. Además, los usuarios de la red deben configurar una contraseña fuerte para el router y cambiarla con regularidad para evitar que los ciberdelincuentes

accedan a la red sin autorización. Finalmente, los usuarios también deben deshabilitar cualquier servicio innecesario que pueda estar expuesto a los ataques de ciberdelincuentes. Por ejemplo, algunas versiones de open source tienen un servicio FTP (File Transfer Protocol) habilitado de forma predeterminada. Esto debe deshabilitarse para evitar que los ciberdelincuentes descarguen archivos importantes de la red.

OBJETIVOS DE LA INVESTIGACIÓN

Objetivo general de la investigación

- Implementar un control de amenazas en una red domestica basadas en Open Source.

Objetivo específico de la investigación

- Identificar las principales amenazas en una red doméstica, empleando instrucciones informáticas y fundamentos teóricos basados en Open Source.
- Demostrar las vulnerabilidades de una red doméstica y los puertos utilizados en los dispositivos informáticos y móviles.
- Elaborar un registro atreves de un software multiplataforma ***TP-Link Tether*** en base instrucciones informáticas.

LÍNEA DE INVESTIGACIÓN

- Sistemas de información y comunicación, emprendimiento e innovación.

Sub Línea de Investigación

- Redes y tecnologías inteligentes de software y hardware

MARCO CONCEPTUAL

1.2. Conceptos Generales

1.2.1. La seguridad

La seguridad es la condición de algo o alguien que es asegura, bajo un entorno para precautelar la integridad del miso. Simboliza una instrumento, artefacto o método está bosquejado para realizar un trabajo de impedir riesgos o avalar una función específica, *"alza la propiedad de algo donde no se registran peligros, daños ni riesgos. Una cosa segura es algo firme, cierto e indubitable. La seguridad, por lo tanto, puede considerarse como una certeza"* (Pérez & Gardey, 2021). La seguridad es un instrumento que ayuda a cualquier sistema, organización, individuo y sociedad a controlar cualquier riesgo y recluir un evento o caso no deseado para establecer su correcta labor en la realización de una actividad que requiera el proceso existencial a seguir.

1.2.2. Seguridad Informática

Desde el comienzo mismo de este subtema, es necesario tener en cuenta la confusión que siempre ha existido, a saber, el hecho de que la seguridad informática y la seguridad de la información tienen características importantes que las distinguen entre sí, Según (Castro, 2018) *"manifiesta que la informática es la ciencia encargada de los procesos, técnicas y métodos que buscan procesar almacenar y transmitir la información. Entonces la seguridad informática es la disciplina que se encarga de generar, diseñar y planificar las normativas, procedimientos, reglas, técnicas y métodos que den paso a la obtención de un sistema informático confiable, veraz y seguro, donde siempre exista una correcta disponibilidad del uso del mismo"*.

La característica fundamental de la seguridad informática es reducir al mínimo los riesgos, por lo consiguiente puede ser entrada el envió o recepción de datos, atreves de un medio que transmite información.

La tarea principal es minimizar el riesgo de ataques informáticos a través de diversos medios o susceptibilidad de los dispositivos móviles, IoT, etc. Y lo principal se podría considerar la eliminación de los riesgos para lograr una excelente y mayor seguridad dentro de la infraestructura de la red.

- **Los usuarios:** Se les considera el eslabón más débil de la cadena porque la gente no puede controlarlos., Según (Castro, 2018) *"esto se debe a que los usuarios cometen errores y olvidan detalles importantes, suelen tener accidentes y estos eventos privan por completo la operación, excepto tiempo valioso e importante para realizar nuevas tareas"*, en la mayoría de los casos se emplean medidas provisorias a los usuarios en los momentos de ataque externo a través de la red.
- **La información:** Se considera la seguridad informática el medio que se desea resguardar y lo que tiene que estar a salvo. Según (Castro, 2018), *"la información determina los recursos de los usuarios entonces si esta información llega a ser vulnerada o es obtenida y usada de forma inapropiada, puede llevar a la ruina a cualquier organización o persona de la que dependa su seguridad"* por ende, la información es supone el trabajado principal de un usuario, u organización.
- **La infraestructura:** Dentro de la rama de la seguridad informática, el campo es el más protegido. Se debe considerar el acceso no autorizado, (Castro, 2018), *"la usurpación de identidad, incluso los daños más comunes, por ejemplo, robo de equipos, inundaciones, incendios o cualquier otro desastre natural que pueda tener el material físico del sistema de información".*

La importancia de la infraestructura lógica es prevenir todo tipo de ataques o detección de vulnerabilidades otorgadas a través de herramientas de prueba de los sistemas operativos.

Según (ISOTools, 2017). *"La totalidad de los especialistas en seguridad basan sus conocimientos y experticias sobre el aspecto técnico tradicional de la seguridad, esto es en las áreas IT, aunque bastantes de ellos consideran las cuestiones propias como el 9 nuevo aspecto en las comunicaciones y que hace que actualmente se hable de TIC. Además de tener un enfoque técnico prácticamente, los especialistas únicamente se manejan con las vulnerabilidades y en parte con amenazas en forma de ataques".* Con la propuesta de establecer una evaluación de riesgos en una red controlada, es necesario realizar un análisis de las vulnerabilidades de una red doméstica, en caso de ser necesario, revisar la integridad de la red y la seguridad en la red de datos.

1.2.3. Seguridad de la información

La disciplina que se encarga de brindar la evaluación de riesgos y amenazas es la disciplina. Según (Figueroa, 2017), manifiesta que *"las normativas, las buenas prácticas o el modo mediante el cual se establece un trato considerado de acuerdo a la información que se requiera resguardar con el objetivo de asegurar la confidencialidad, integridad y disponibilidad del manejo de la información".* La normativa que protege y garantiza los siguientes aspectos es la seguridad de la información.

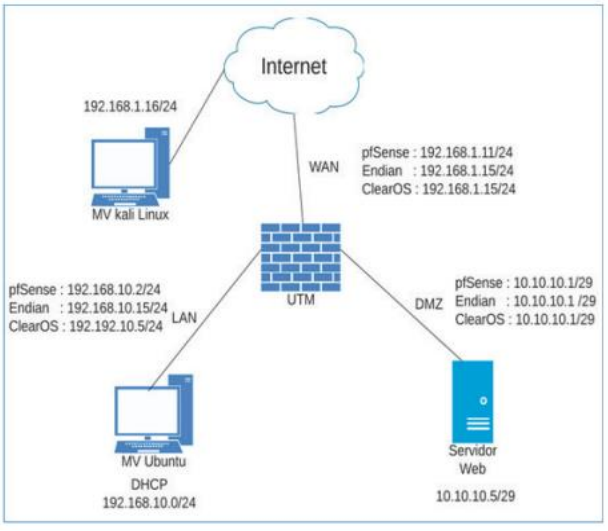

Ilustración 1. Implementación del firewall de red
Fuente: *(ISOTools, 2017)*

- **La Confidencialidad:** Poder proteger la intimidad de personas, instituciones u organizaciones, supone que un sistema informático es fiable, más aún cuando lo que se defiende es la información como prioridad de dicho sistema, concluyendo que un sistema es fiable si respeta la privacidad de su usuario sin registro. (Excellence, 2018) *"menciona que la confidencialidad, requiere que la información sea accesible de forma única a las personas que se encuentran autorizadas. Es necesario acceder a la información mediante autorización y control, entonces el objetivo de la confidencialidad es prevenir la divulgación no autorizada de la información o recursos perteneciente al usuario del sistema".*
- **La Integridad:** En caso de accidentes o intentos maliciosos, significa que la información sigue siendo la misma. Se requiere autorización para modificar la información. (Excellence, 2018). *"Por lo tanto, su objetivo es el de velar por algún cambio no permitido del recurso o información a través de cualquier medio que se use para poder lograr dicho ataque".*
- **La Disponibilidad de la información:** El acceso al sistema informático no debe degradarse. Según (Excellence, 2018) indica que *"es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. La información deberá permanecer accesible a elementos autorizados".*

Hacer que la información esté disponible para mantener activos los sistemas de información sin riesgo de ataque o manipulación, permitiendo el acceso autorizado de los usuarios asignados y al mismo tiempo protegiendo todos los demás campos se propuso como objetivo la protección de una red domestica a través de instrucciones para así evitar el acceso de personas no autorizadas.

1.2.4. Segmentación de la red

Para la ejecución de control de amenazas a través de instrucciones informáticas se debe plantear una apropiada segmentación de la red empleando VLANS con las respectivas direcciones IP, a la hora de realizar una segmentación de red se debe tener en cuenta el posible desarrollo de la red en futuro se debe construir un PULL de direcciones IP que proteja tanto la situación actual como el posible crecimiento de la infraestructura de red.

Después de segmentar la red, es necesario configurar los equipos de red activos como Switches y Routers de Capa 2, si no hay Routers, hay que configurar un Switch de Capa 3 (Fernández, 2020).

1.2.5. Router Dual Band

Como las puertas de enlace de conexión a internet tenemos los router que existen un sin número de tipos y modelos, el router dual band están provistos de doble tecnología el canal de 2.5 GHz y de 5 GHz, la característica principal del router es direccionar el enrutamiento de las IP a cada dispositivo ya sea por DHCP (***DYNAMIC HOST CONFIGURATION PROTOCOL***), o por Static IP, comparte partes de las redes públicas y privadas.

1.2.6. Firewalls

Los cortafuegos son una serie de paredes internas que sirven como filtro adicional para el tráfico entrante. Del mismo modo, otras herramientas mencionadas en este documento no pretenden ser la única defensa de la institución, ya que deben usarse junto con otro software y dispositivos.

1.2.7. Sistema de Detección de Intrusos (IDS)

El IDS es un sistema de alerta porque puede ser un solo dispositivo o un conjunto de dispositivos que monitorean la red en busca de actividad maliciosa o ataques a políticas. Se diferencia de un cortafuego ***firewall*** tiene como propósito principal bloquear accesos de ataques maliciosos y a través de intrusiones dentro de una red interna informa un ataque desde dentro de la red.

1.2.8. Sistema de Prevención de Intrusos (IPS)

A diferencia de IDS, que lo alerta sobre posibles amenazas cibernéticas, IPS las detiene automáticamente según una lista de reglas preestablecidas. Por lo tanto, un sistema de prevención de intrusiones es un "vigilante nocturno" que intercepta el tráfico entrante, lo bloquea, descarta paquetes de datos maliciosos o interviene para restaurar completamente la conectividad.

El IPS proporciona una tarifa adicional por escaneo y seguridad interna, pero sin que intervenga de forma directa un administrador; por lo que, se considera también como un cortafuegos de próxima generación, que es principalmente una versión avanzada de un firewall más clásico, pero con la técnica adicional de impedir malware y usar la inspección profunda de paquetes (DPI) en línea (Hubbard, 2022).

1.2.9. Open Source

Open Source (Código abierto) no indica que el software sea gratuito; más bien se refiere al hecho de que los usuarios pueden acceder al código fuente de forma gratuita; Por tanto, una de las ventajas es que permite fomentar la colaboración entre usuarios de diferentes programas de código abierto.

Aunque, hay más probabilidades de que los programas se vayan actualizando, no solo en relación a la usabilidad sino también en términos de seguridad y permiten a los usuarios corporativos e individuales la conveniencia de configurar todas las funciones de red fundamentales para un funcionamiento adecuado (Fernández, R. Zredeszone, 2022).

1.2.10. Seguridad en Open Source

- Detectar las Inseguridades.
- Identificar el método asequible de los puertos de red.
- Vulnerabilidad y despliegues de los DNS.
- Software detector de malware, spiderworks, etc. he identificador de vulnerabilidad.

1.2.11. Software de prevención de intrusos (IPS) *Tp-Link Tether*

Un sistema de prevención de intrusiones (IPS) es un programa de seguridad que le permite proteger de forma proactiva los sistemas contra ataques e intrusiones informáticas.

- Bloquea la dirección IP desde la que se origina la amenaza.
- Detiene el proceso, si la actividad maliciosa procede de uno específico.
- Se encarga de suspender o desactivar diversas cuentas de usuario.
- Apaga los sistemas completos para restringir los daños que puedan ocurrir.
- Manda una alerta a los que administran del sistema, registra el incidente y reportar la actividad sospechosa que detecta (Grupo Atico34, 2021).

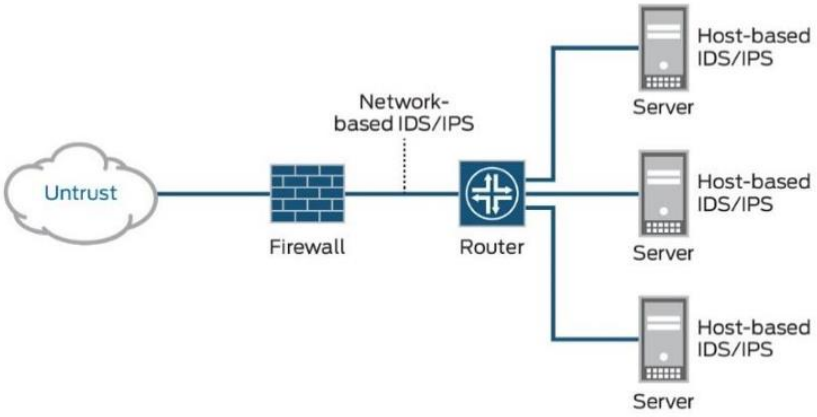

Ilustración 2 ¿Qué son IDS y SPI?
Fuente: *https://www.juniper.net/mx/es/research-topics/what-is-ids-ips.html*

1.2.12. Amenazas informáticas

Las amenazas informáticas son oportunidades donde los ciberdelincuentes informáticos logran infiltrarse en sus equipos, dispositivos y/o servidores para obtener información.

Estos ataques, según el tipo, pueden ser a través de correos electrónicos engañosos dando clic en anuncios maliciosos, entre otros. Las razones principales para que los ciberdelincuentes informáticos ejecutan amenazas cibernéticas son para conseguir información confidencial de sus víctimas colapsando su conexión a Internet a través de ataques informáticos e infectar más computadoras o dañar la Red Domestica (Arroba System, 2021).

1.2.13. ¿Qué es un IDS (Intrusion Detection System)?

Su objetivo es realizar investigaciones sobre el rendimiento de diferentes soluciones para sistemas de detección de intrusos (IDS) basados en redes definidas por software (SDN). *Dado que SDN ha ganado protagonismo en los últimos años, es importante abordar y analizar sus aspectos de ciberseguridad, ya que, si bien SDN puede brindar mejoras en esta área, también puede crear nuevas vulnerabilidades que comprometan los datos comerciales y de los usuarios. Por lo tanto, el propósito de esta investigación es: analizar el desempeño de varias soluciones IDS aplicadas en el entorno SDN* (Arroba System, 2021), compararlas de acuerdo con los objetivos de evaluación y los resultados de cada solución propuesta y, finalmente, determinar qué soluciones son las más prometedoras. La investigación muestra que hay una gran cantidad de soluciones relacionadas con el tema de la seguridad de la red y SDN; se dirigen a diferentes tipos de ataques como DoS, escaneo de puertos, botnets; así como recomendar nuevas funciones, como eludir ciertos firewalls o reducir la carga de tráfico de IDS para mejorar el rendimiento de la red. Para llevar a cabo este trabajo se realizó un levantamiento bibliográfico sobre temas relacionados con las aplicaciones IDS, enfocándonos en entornos SDN.

MARCO METODOLÓGICO

En esta etapa de la propuesta tecnológica se establecen criterios clave a través de los cuales se obtiene información relevante para el diseño de un modelo de sistema de seguridad informática, para ello se debe explicar el entorno en el que se encuentra instalado el sistema. ayuda al investigador a recopilar suficiente información que le permita hacer un análisis estratégico del contenido.

1.3.1. Enfoque de la investigación

Porque los objetivos del estudio introducen diferentes tipos de análisis que es necesario cuestionar, tanto cualitativamente por el uso de descripciones de vulnerabilidades y amenazas a partir de las cuales se aborda la conceptualización propiamente dicha del problema, se abordan las amenazas a la seguridad informática y la conceptualización de las LAN corporativas. y cuantificada a través del uso de parámetros que permiten establecer el nivel de seguridad de la red local donde se presentan las anomalías y el acoso, por lo que el objetivo de investigar esta propuesta tecnológica es la forma mixta en que se manifiestan tanto el uso cuantitativo como las cualidades cualitativas.

1.3.2. Enfoque Mixto:

Naturalmente es una composición en la cual las tipologías individuales de cada enfoque se borran o se vuelven relativas. *La riqueza de la investigación mixta consiste en aprovechar las bondades y fortalezas de cada enfoque* (Salas, 2019).

Por ello, se propone una relación entre las características en función de la utilidad de los dos componentes, para recoger mejor la información a la hora de diseñar un modelo de seguridad informática utilizando criterios que puedan ser utilizados para descubrir y generar un concepto sólido y fiable que tenga un rango estimado. y así será utilizado en el futuro por muchas empresas

y organizaciones que cuenten con este plan, de cara a futuras amenazas digitales, que será el elemento definitorio de una sociedad tecnológicamente avanzada y de progreso en las próximas generaciones.

1.3.3. Tipo de Investigación

Los tipos de investigación son un medio para saber qué tipo de adaptaciones debo realizar para establecer el conjunto de variables en un tema de investigación, están motivados por un enfoque investigativo en el que el modelo sirve a la investigación. tema de investigación. Proponer tecnología para desarrollar un plan para diseñar y mejorar el modelo de seguridad en LAN en una organización.

1.3.4. Investigación descriptiva

La investigación descriptiva analiza los fenómenos sin conocer las relaciones. Así, la investigación de tipo descriptivo tiene como tarea evaluar las áreas necesarias para poder lograr el objetivo, plantean sin cuestionar por qué o de dónde viene el problema antes de que suceda. o averiguar cómo las variables se relacionan.

- **Método de observación:** El más eficaz para llevar a cabo la investigación descriptiva. Se utilizan tanto la observación cuantitativa (*recopilación objetiva de datos que se centran principalmente en números y va lores*) como la observación cualitativa (*mide características de los elementos a investigar*) (Arias, 2021). *En este caso se utilizó NMAP como herramienta de observación, ya que con este implemento se podrá escanear el equipo target deseado y de este modo poder observar cuáles son sus vulnerabilidades a nivel lógico, para esto bastaría utilizar el comando NMAP más la dirección IP del equipo que se quiera auditar.*

```
nmap [ip]
```

Ilustración 3 Escaneo rápido de puertos en un host.
Fuente: *(DeLuz, 2021)*

- **Investigación Explicativa. -** Según (Mejía, 2020) *la investigación explicativa es un tipo de investigación cuya finalidad es hallar las razones o motivos por los cuales ocurren los hechos del fenómeno estudiado, observando las causas y los efectos que existen, e identificando las circunstancias.* Por lo tanto, con este tipo de investigación es posible dar explicaciones detalladas de los riesgos que se pueden presentar cuando existen amenazas y vulnerabilidades que se están aprovechando en la empresa, por lo que esta investigación debe seguir adelante, algunas encuestas como las descritas brindan datos importantes y de esta manera se puede hacer un proceso claro y preciso de la situación dentro de un cierto período de tiempo.

En este apartado en particular se llevó a cabo el proceso de investigación explicativa a través del resultado de mapeo de puertos, ya que con esta incidencia se podrá determinar las vulnerabilidades dentro del servidor que se desee auditar.

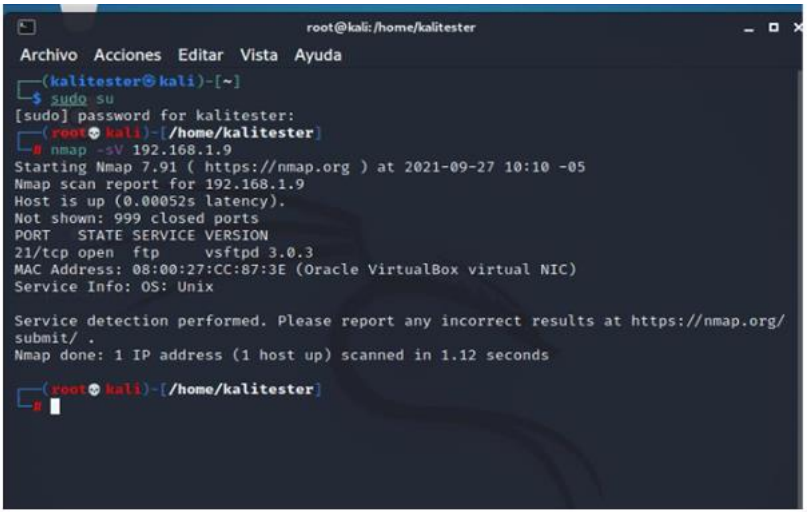

Ilustración 4 lista de estados de los puertos.
Fuente: *(DeLuz, 2021)*

RESULTADOS

Un equipo que tenga Kali Linux como sistema operativo y adicionalmente se hizo uso de un escaneado de puertos, en este caso se optó por NMAP, el cual dio como resultado que ciertos puertos críticos se encontraban habilitados, por ende se dedujo que el sistema de seguridad perimetral que presentaba la compañía era sumamente ineficiente; y para validar este a argumento se procedió a realizar un exploit de tipo de denegación de servicios al servidor FTP y así mostrar que a pesar de que el servicio se encontraba habilitado el ingreso a sus recursos no era posible.

Debido a todas estas problemáticas se diseñó un p lan de mejoras destinado para fortalecer la seguridad informática de la compañía. En rasgos generales esta planeación está sustentada bajo la estructura y para validar este argumento se procedió a realizar un tipo de denegación de servicios al servidor FTP y así mostrar que a pesar de que el servicio se encontraba habilitado el ingreso a sus recursos no era posible. Debido a todas estas problemáticas se diseñó un p lan de mejoras destinado para fortalecer la seguridad informática de la compañía. En rasgos generales esta planeación está sustentada bajo la estructura.

DISCUSIÓN DE RESULTADO

En cuanto a determinar los fundamentos teóricos relacionados con la seguridad en redes de datos, se determinó como resultante la factibilidad de la implementación de un control de amenazas en una red domestica basadas en Open Source a través del software multiplataforma TP-Link Tether, e instrucciones informáticas actualizar conocimientos en base a futuros ataques. Al evaluar la seguridad de la red con el uso de herramientas para la detección de vulnerabilidades, escaneo y

diagnóstico se recomienda no solo utilizar herramientas Open Source, sino también implementar mecanismos o software privado o licenciado, ya que estos presentan protección al no ser un mayor nivel que ser fácilmente adquirido y también dejar.

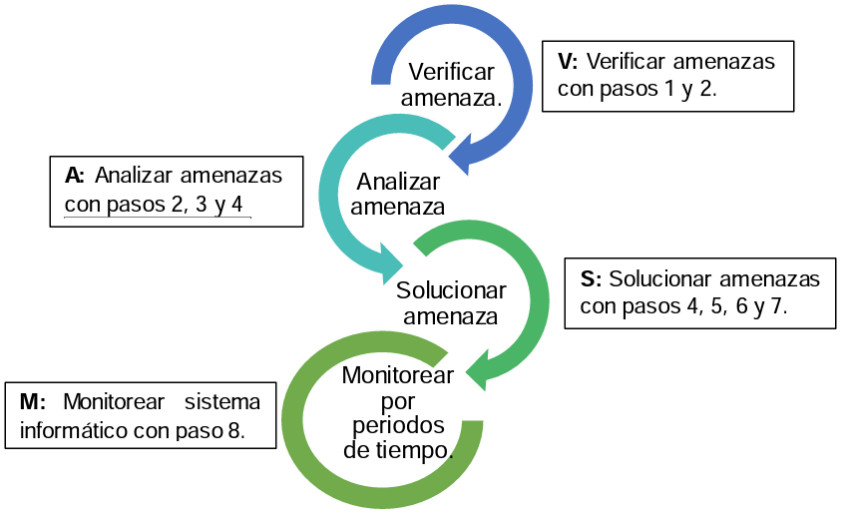

Ilustración 5 Pasos para determinar el ataque a la red.
Fuente: *(Autora, 2023)*

CONCLUSIONES

Al final de la presente investigación mediante el respectivo método de investigación se ha definido las técnicas de recolección de información que permitan el despliegue de una red domestica segura a través de código abierto para mejorar la seguridad y esto ayude a evitar ataques internos y externos que tengan el alcance a los dispositivos más vulnerables que son los dispositivos de domótica o más conocidos como IoT por lo tanto se exclaman las siguientes conclusiones:

- Todas las redes domesticas se encuentran en constante amenazas por ataques informáticos en la que en algún momento pueden derivar en fuga de información delicada, por lo que es necesario proteger la información a través de políticas de seguridad aplicadas a la red y aunque no se cuenta con los recursos necesarios disponible, se logró diseñar una red de segura a través de una serie de instrucciones informáticas empleando un software

multiplataforma ***TP-Link Tether*** de código abierto que permite al administrador detectar y reportar amenazas informáticas, garantizando así la seguridad de la información.

- El uso de un firewall protege la red a una red vulnerable; a pesar de ello se propuso implementar políticas de seguridad para determinar la vulnerabilidad en tres redes domesticas de diversos proveedores de internet, garantizando la seguridad de todas las redes, por ello es necesario combinar diferentes elementos de seguridad que ayuden a proteger la información de posibles ataques informáticos.
- Después de completar este documento, hemos llegado a la conclusión de que el tremendo crecimiento de las comunicaciones globales hace que la seguridad de la información sea esencial en las redes de datos actuales integrando diversas funcionalidades como el Firewall, IDS e IPS.

RECOMENDACIONES

En el presente caso de estudio está determinado a la investigación de las amenazas o ataques en una red domestica a través de instrucciones que proveen servicio de internet domestico en el cual está orientado bajo ataques informáticos empleando un software multiplataforma ***Tp-Link Tether***, en el cual es un Open Source, se determinaron las siguientes recomendaciones:

- Respecto sobre los fundamentos teóricos relacionados con la integridad, seguridad de las redes de datos, las actualizaciones de conocimientos son las principales bases para futuros ataques, foros de tecnología, videos tutoriales, noticias de tecnología son los medios indispensables para determinar la integridad y poner en práctica la seguridad de las redes domesticas bajo un entorno controlado, se recomienda poseer un constante desarrollo y crecimiento en el estudio de las redes ya que cada día evolucionan, por el cual se determinó

analizar un software de control para así determinar las vulnerabilidades que requieren una red doméstica y solventar los problemas actuales de la tecnología en redes.

- Al evaluar la seguridad de la red utilizando herramientas de detección, escaneo y diagnóstico de vulnerabilidades, recomendamos implementar mecanismos o software privado o con licencia además de utilizar herramientas de código abierto. Es un nivel superior al que puedes conseguir fácilmente, lleva un registro de cada compra o licencia de uso e inicia una búsqueda si detecta un atacante.
- Para interpretar los resultados en base a la medición de cada indicador de red, es necesario emplear indicadores que ayuden a medir las fluctuaciones de la red y el comportamiento físicas y lógicas de las mismas, por lo que es recomendable establecer un índice en la cual permita ayudar a segmentar la red empleando ***subneting*** para así distinguir y dar solución del problema, para no alterar el servicio está disponible de la red.

REFERENCIAS

AAAPN. (23 de Agosto de 2021). AAAPN. Obtenido de Asociación de Agentes Aduanales de Piedras Negras: http://www.aaapn.mx/aniv50/blog/tecno/7-00007.php

Aguilera , P. (2010). Seguridad Informática. Editex.

Aguilera López, P. (s.f.). Seguridad Informática. 2021.

Ambit Team. (10 de Noviembre de 2020). ambit-bst. Obtenido de ambit-bst.: https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazasinform%C3%A1ticas

Anonymous. (29 de Enero de 2013). Historia de la web. Obtenido de Historia de la web: http://charliedaw2236.blogspot.com/

Areitio, G., & Areitio, A. (2009). Información. Informática e Internet: del ordenador personal a la Empresa 2.0. Visión Libros.

BAHILLO, L. (18 de Mayo de 2021). marketing4ecommerce. Obtenido de marketing4ecommerce.net: https://marketing4ecommerce.net/historia-de-internet/

Borghello, C. (23 de Ago de 2021). Noticias sobre seguridad de la información. Obtenido de Segu.Info: https://www.segu-info.com.ar/virus/tipos_virus

Calvo , L. (3 de Noviembre de 2020). Go Daddy. Obtenido de https://es.godaddy.com/blog/lean-startup/ Cámara Valencia. (2019). camaravlencia. Obtenido de https://www.mastermarketingvalencia.com: https://www.mastermarketing-valencia.com/marketingdigital/blog/internet-historia-evolucion/

Carazo, J. (30 de Mayo de 2017). economipedia. Obtenido de economipedia.: https://economipedia.com/definiciones/metodo-lean-startup.html

Calderon, F (28 de Junio de 2018) Siclos y vulnerabilidades de la red. Obtenido de redes informaticas: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992021000300055

Cabrera, F (12 de Octubre de 2022) Obtenido de Diseño de una red de seguridad perimetral basada en OPEN SOURCE para aplicación de IDS E IPS para el control de amenazas informáticas en la Universidad Técnica de Babahoyo: http://dspace.utb.edu.ec/handle/49000/13035

HACKWISE (12 de Abril de 2022) Obtenido de Los 8 puertos más vulnerables que debes verificar al realizar un pentesting: http://dspace.utb.edu.ec/bitstream/handle/49000/13035/E-UTB-FAFI-SIST-000377.pdf?sequence=1&isAllowed=y

Zambrano, J (12 de Febrero de 2022) Obtenido de Diseño de modelo de seguridad y plan de mejoras para la seguridad de la red, en función de las vulnerabilidades y amenazas detectadas en la empresa cenforsp. cia ltda. https://repositorio.ecotec.edu.ec/bitstream/123456789/273/1/ZAMBRANO%20JOAN.pdf

TICPYMES. (13 de Febrero de 2020). computing. Obtenido de computing: https://www.computing.es/seguridad/noticias/1116703002501/10-ciberataques-masgrandes-de-decada.1.html un fantasma en el sistema . (06 de Mayo de 2020). un fantasma en el sistema. Obtenido de https://www.unfantasmaenelsistema.com/2020/05/analisis-de-vulnerabilidades-connessus/

V., A. C. (s.f.). archivo.ucr.ac.cr. Obtenido de archivo.ucr.ac.cr: http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf

Vargas, A. (2013). archivo.ucr.ac. Obtenido de archivo.ucr.ac: http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf

Vargas, A. C., & Castro Mattei, A. (2020). Sistemas de Gestión de Seguridad de la Información. ISOTools Excellence. (2017) ¿Seguridad informática o seguridad de la información? Recuperado el 05 de marzo de 2017, de http://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Vieites, Á. G. (2013). Auditoría de seguridad informática. Bogotá, Colombia: Ediciones de la U.

ANEXOS

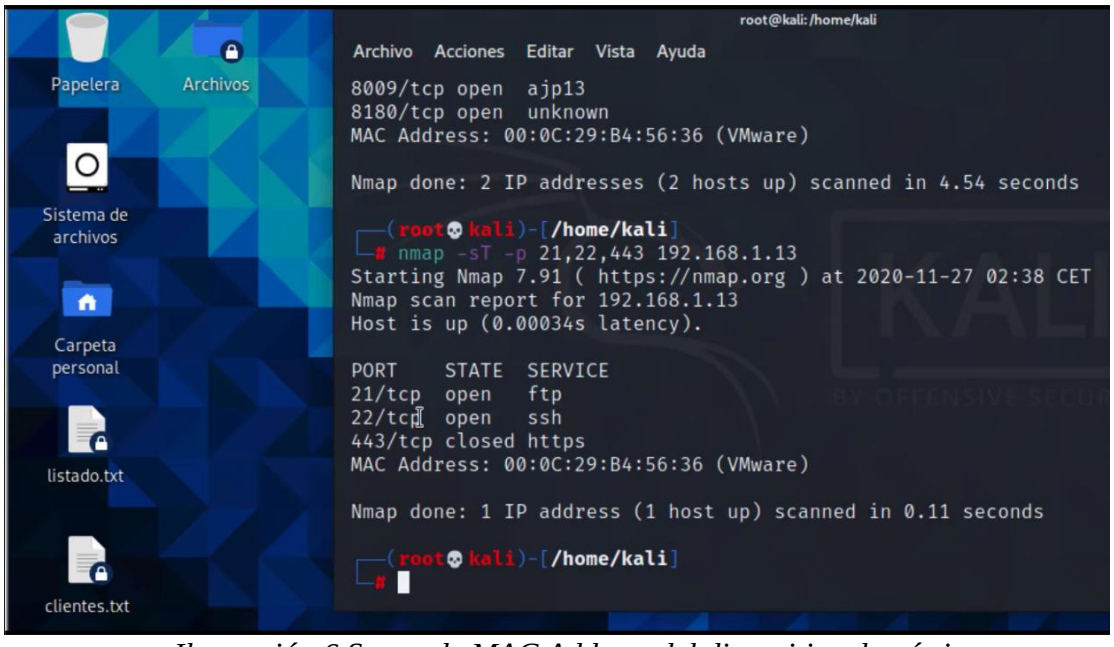

Ilustración 6 Status de MAC Address del dispositivo doméstico.
Fuente: *(Autora, 2023)*

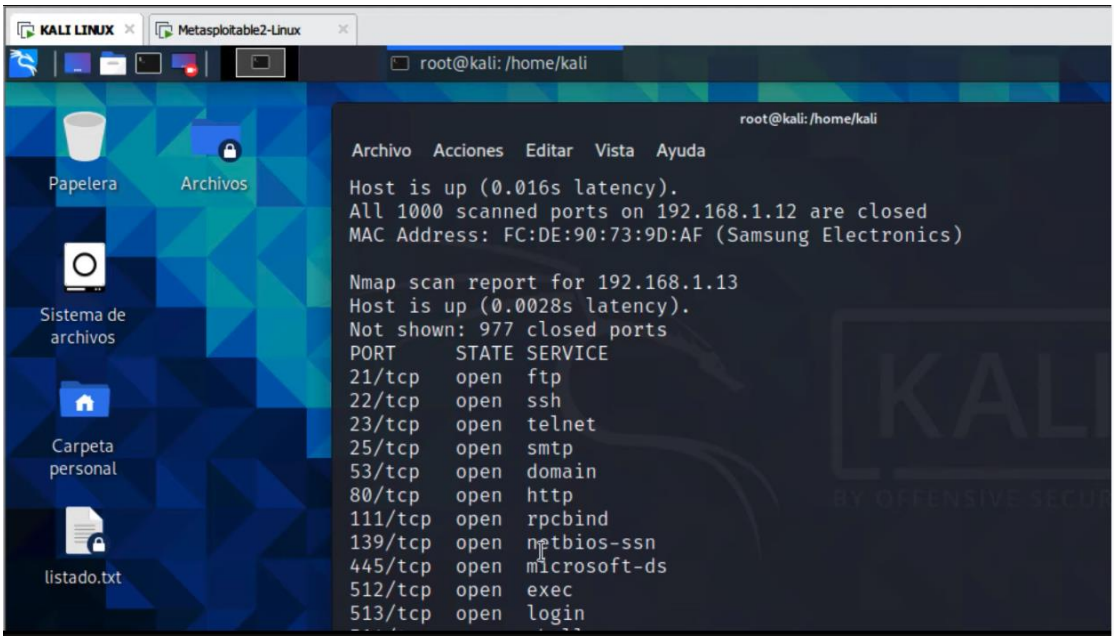

Ilustración 7 Estados de puertos vulnerables.
Fuente: *(Autora, 2023)*

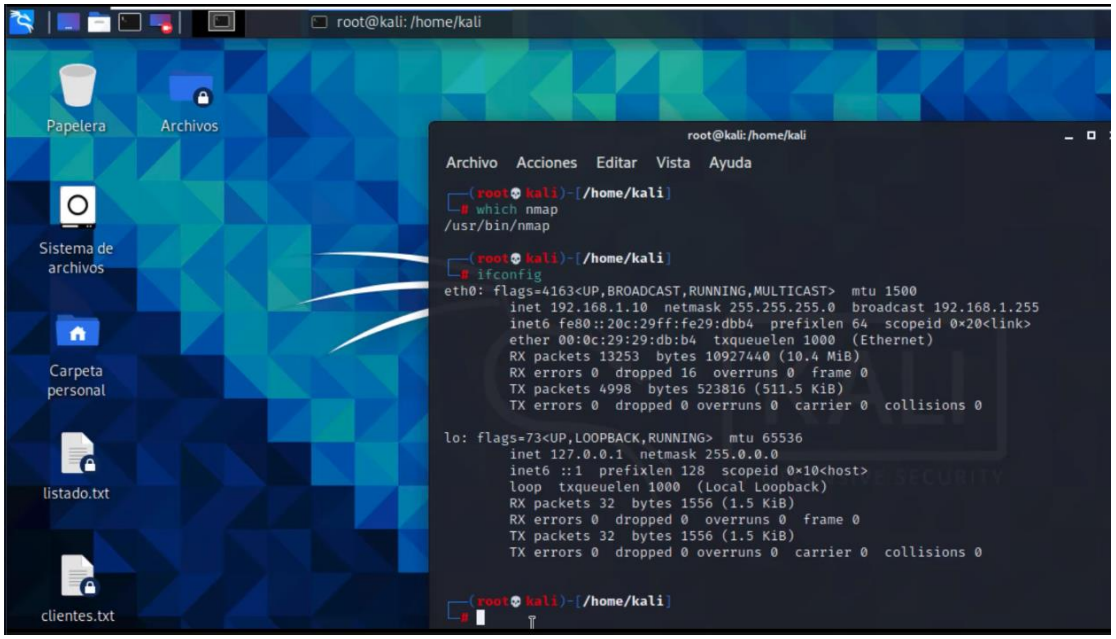

Ilustración 8 Acceso al Broadcast para el acceso a la red.
Fuente: *(Autora, 2023)*

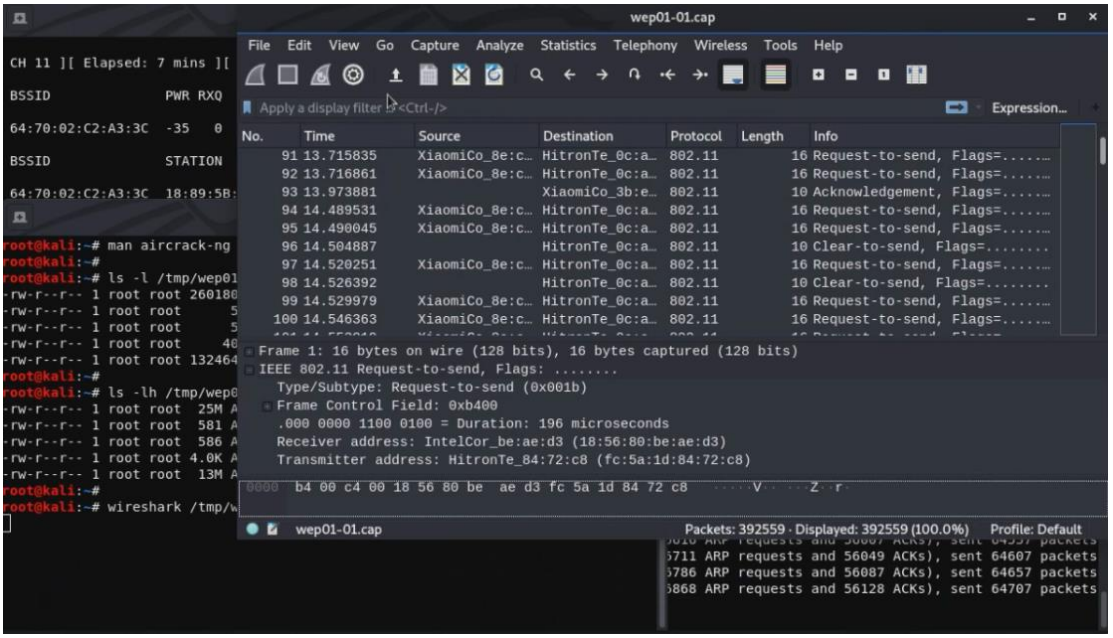

Ilustración 9 Visualización del tráfico de la red.
Fuente: *(Autora, 2023)*

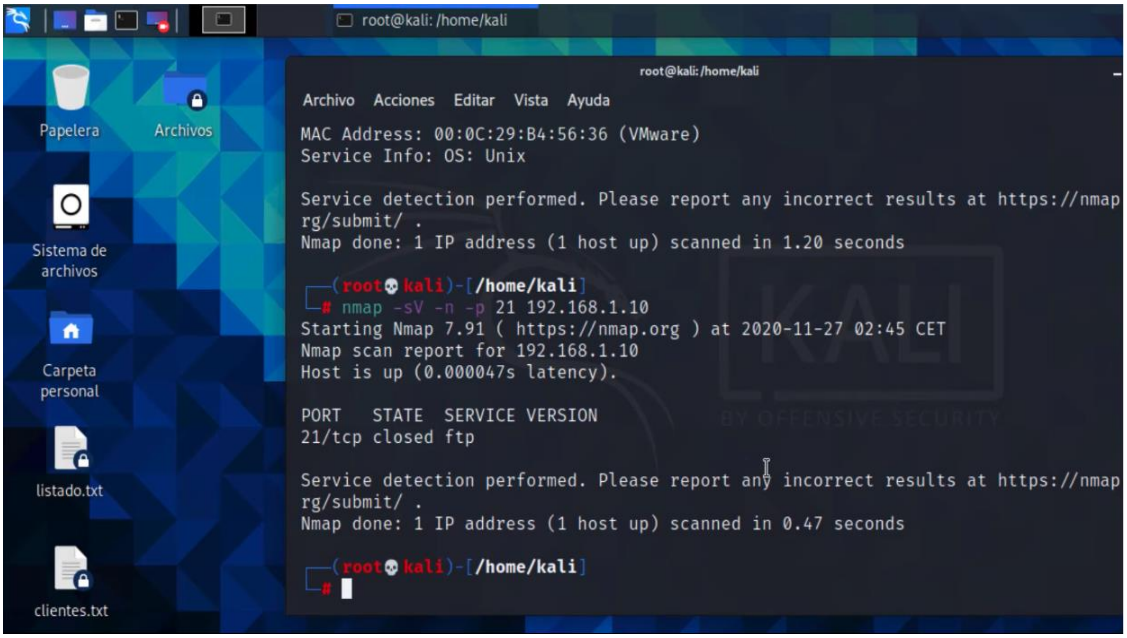

Ilustración 10 Bloqueo de accesos no deseados a la red.
Fuente: *(Autora, 2023)*