Detección de ataques en una red WiFi mediante la implementación de un software IDS

Jonny Alejandro Díaz
Rodríguez Brayan David
Sastoque Piza

Universitaria Agustiniana
Facultad de Ingeniería
Programa de Ingeniería en
Telecomunicaciones Bogotá, D.C
2019

Detección de ataques en una red WiFi mediante la implementación de un software IDS

Jonny Alejandro Díaz

Rodríguez Brayan David

Sastoque Piza

Director

Francisco Clemente Valle Díaz

Trabajo de grado para optar al título de Ingeniero en Telecomunicaciones

Universitaria Agustiniana

Facultad de Ingeniería

Programa de Ingeniería en

Telecomunicaciones Bogotá, D.C

2019

Dedicatoria

Dedico el resultado de este proyecto primeramente a Dios que me presto el tiempo, la salud, la sabiduría y el entendimiento para desarrollarlo, además puso en mi camino las personas correctas para guiarme apoyarme y alentarme cuando fue necesario. Seguido a mi familia quienes fueron un pilar fundamental en la búsqueda de mis objetivos, motivándome, apoyándome y celebrando cada uno de los triunfos que aparecían en el camino. Agradezco los valores, los consejos, la motivación, la perseverancia y el amor que han inculcado cada uno de ellos en mi vida para que con ello pudiese superar los obstáculos que pretendían privarme de mis objetivos.

Brayan David Sastoque Piza

Dedicatoria

Dedico el presente proyecto a Dios que me ha guiado a lo largo de la vida, me ha brindado la salud, la sabiduría y siempre ha estado presente; y a mi familia, ya que gracias al apoyo de ellos me encuentro finalizando una carrera profesional, buscando cumplir uno de mis sueños, y son ellos los que han estado en cada paso que doy brindándome su apoyo, sus consejos, su ayuda.

Jonny Alejandro Díaz Rodríguez

Agradecimientos

Agradecemos primero que todo a Dios, luego a cada uno de nuestros docentes por su dedicación, por guiarnos a lo largo de todo nuestro proceso educativo y profesional, en cada uno de ellos siempre encontramos esfuerzo, dedicación y amor por su profesión, lo que nos llevó a crecer no solo como profesionales sino como personas, interiorizando cada uno de los conocimientos impartidos.

Un especial agradecimiento al ingeniero Jorge Hernandez quien con su paciencia, perseverancia y fe compartió cada uno de sus conocimientos con nosotros con el fin de dar solución a cada uno de los obstáculos que se presentaban a lo largo del proyecto.

A nuestro guía y tutor el ingeniero Francisco Clemente Valle Díaz quien con su paciencia y entusiasmo siempre nos dio la motivación necesaria para persistir, además de guiar nuestro proyecto de manera profesional con el fin de obtener los resultados esperados.

Agradecemos también a la Universitaria Agustiniana quien nos dio la oportunidad de cursar una carrera profesional con todos los recursos necesarios para lograrlo de manera eficiente, llevándonos a ser una gran competencia para el campo laboral.

Resumen

En el desarrollo del presente proyecto se ha buscado implementar un software IDS conocido como Snort en una red Wifi para de esta manera determinar si algún host o dispositivo conectado a la red Wifi es atacado o vigilado por algún intruso de la red. Para lograr realizar el proyecto mencionado se llevó a cabo la implementación y configuración del software IDS Snort en un dispositivo conocido como Raspberry en la cual fue instalado anteriormente el sistema operativo Raspbian el cual tiene como base el Debian de Linux, también fue necesario configurar un router MikroTik como espejo, ya que el router establece la red pero todo el tráfico que se va a dar por la red pasa primero por el segmento de red dado a la Raspberry en la cual se encuentra el software IDS para analizar el tráfico y mirar si hay intrusos o ataques en la red, posterior a eso se llevó a cabo la realización de pruebas en una red Wifi corporativa para determinar si se realizan ataques.

Tabla de contenido

Lista de figuras

Lista de tablas

Introducción

Las redes WiFi cada vez se vuelven más importantes en la vida de cada ser humano, desde la aparición de los dispositivos móviles y las redes inalámbricas, el acceso a Internet por medio de redes WiFi las cuales permiten que los celulares, pc o cualquier otro tipo de dispositivo se conecten a internet inalámbricamente, en otras palabras (Valle, 2018, pág. 73) cuenta "El estar conectados todo el tiempo desde diversos dispositivos se ha convertido en algo habitual, sin embargo, los riesgos asociados a esta creciente conectividad también aumentan y al parecer dichos riesgos son ignorados por la ciudadana en general", esto quiere decir que la seguridad de las redes WiFi se pasa por alto, aun sabiendo que es un tema al que hay que tenerle mucho cuidado ya que la información de todas las personas conectadas a la red están expuestas, y debido al gran impacto de las redes WiFi en la humanidad, hay hackers que buscan robar dicha información para cometer cibercrímenes y que se han convertido en un gran problema para todo usuario, organización y hasta países, como cuenta (Valle, 2018, pág. 75)

> "El ciber espionaje, las preocupaciones en materia de privacidad y la proliferación de nuevas vulnerabilidades, han sido en parte responsable de los altos costos asociados a los delitos cibernéticos. Solo en el año 2013 según cifras reveladas por la OEA [12] se estima que ascendieron a por lo menos USD 113.000 millones. En Brasil los costos asociados a los delitos cibernéticos alcanzaron los USD 8.000 millones, seguidos por México con USD 3.000 millones y Colombia con USD 464 millones"

Debido a lo mencionado anteriormente es necesario tomar medidas que busquen disminuir este tipo de ataques, una de esas medidas es la implementación de software IDS como Snort, que se encarga principalmente de monitorear una red deseada para detectar si hay intrusos que estén buscando realizar un ataque a alguno de los hosts conectados a la mencionada. En el presente proyecto se hará la implementación de Snort en un dispositivo conocido como Raspberry previamente configurada, posterior a la instalación y configuración del software IDS en el dispositivo se realizará la configuración de un router MikroTik para que actúe de manera que todo el tráfico de la red pase primero por el segmento de red al cual está conectado la Raspberry dándole una dirección IP estática, donde se podrá analizar el tráfico que pasa por toda la red para de esta manera determinar si hay intrusos en la red y poder tomar medidas contra esto.

Justificación

El presente trabajo de grado se enfocará en el análisis y estudio de los diferentes tipos de intrusos que se presentan en una red Wifi, ya que según (Symantec, 2019) el gran problema del Wi-Fi es que es muy probable que su seguridad sea inexistente, una de las amenazas más conocidas se le conoce como Man-in-the-Middle (MitM) que consiste básicamente en el espionaje, permitiendo que el atacante tenga acceso a la información pues al navegar no está cifrada como en una red privada, también es probable introducir malware en los equipos mediante las vulnerabilidades del software, esto por mencionar algunos ataques. Es importante conocer los diferentes ataques de intrusos que se pueden generar en una red Wifi para de esta manera saber cómo enfrentarlos o tomar medida contra ellos.

A partir de la realización de este proyecto se tendrá la obligación de investigar y aprender en temas como montaje y configuración de Snort, al igual que de los ataques a los que puede estar expuesta la red donde sea implementado, nos encontraremos con pruebas funcionales e implementación de conocimientos adquiridos a lo largo de la carrera profesional, como lo son: IP privada, IP publica, Routers, segmentos de red, configuración de red, programación, sistemas inalámbricos, entre otros, con el fin de obtener un informe de los posibles ataques a los que se encuentra expuesta una red inalámbrica. Ampliando así los conocimientos profesionales y adquiriendo experiencia en la configuración e implementación de sistemas de seguridad en diferentes tipologías de red.

Problema de investigación

La cantidad de personas que acceden a una red para ingresar a la internet ronda por los cuatro mil millones de personas conectadas (Live Stats, 2019), por tal motivo es casi imposible imaginarse la vida sin una conexión a la red de redes, de acuerdo con (it Reseller, 2016) durante la temporada de vacaciones son casi el 80% de los turistas que siguen conectados a la internet y el 70% de ellos lo hace desde redes públicas Wi-Fi, de hecho estas redes se han convertido en un lujo en las cafeterías, aeropuertos y universidades, el problema es que estas redes no están bien protegidas y su tráfico de datos es fácilmente interceptarle por los cibercriminales, a esto se le sume el 21% de estos turistas suelen utilizar ordenadores en cibercafés que tampoco tienen algún tipo de seguridad, por esta razón para las fechas de temporada vacacional se convierten en objetivos para ciberataques, interceptando fácilmente el tráfico que circula a través de ellos, desde contraseñas a tarjetas de crédito y todo tipo de información personal, afirma Tim Berghoff, experto en ciberseguridad de G DATA Software .

Un ejemplo es el caso del gran robo bancario cibernético que se realizó en febrero de 2016, donde se extrajeron 81 millones de dólares de los fondos del banco central de Bangladés y que se mantenían en el banco de la reserva federal de Nueva York. Lo anterior se realizó mediante un malware que simuló realizar transferencias legítimas de dinero a través de una aplicación llamada SWIFT, que utilizan todos los bancos para realizar operaciones entre ellos, por tal motivo se puede evidenciar que una red privada con diferentes tipos de seguridad como lo es la de un banco sigue siendo vulnerable.

Las redes WiFi siempre están expuestas a ataques, a espionaje, en otras palabras, a que estén circulando intrusos en la red buscando algún host o dispositivo para poder robar información importante como en el caso del banco.

Objetivos

Objetivo general

Implementar un software IDS en la red de un router MikroTik con el fin de realizar un estudio de los diferentes ataques a los que está expuesta la red WiFi propagada por dicho router.

Objetivos específicos

- Realizar la instalación y configuración del IDS Snort en una Raspberry basada en Raspbian lite.
- Implementar el IDS en una red WiFi corporativa bajo la cobertura de un router MikroTik.
- Programar las reglas de seguridad del software IDS para la detección de ataques deseados.
- Realizar pruebas y análisis de las reglas configuradas en el Snort para los ataques realizados a la red WiFi que es el objeto de protección.

Marco de referencia

En la actualidad el avance tecnológico ha llegado bastante lejos, como por ejemplo el internet de las cosas (IoT) en el que podemos encontrar bombillas inteligentes, asistentes controlados por voz, entre otros y a pesar de que según (Symantec, 2019) los routers y las cámaras representan el 90% de los dispositivos infectados este avance tecnológico representa mayor cantidad de ciberataques pues aumenta los puntos de acceso fácil, los **ciberataques** consisten en el robo de información como credenciales y datos, borrar datos de dispositivos, espionaje, interceptar comunicaciones como por ejemplo de tipo SCADA entre otros, con amenazas como Thrip y Triton poniendo en riesgo diferentes tipos de redes. Así mismo los sectores de alta dependencia de la informática son un blanco potencial para los ciberataques.

La idea de estos ataques informáticos es que se implantan archivos maliciosos en páginas web, USB, o también hay intrusos que se infiltran en una **red WiFi** a la cual se conectan varios usuarios por medio de host o servidores, que a la vez son los blancos para los mencionados intrusos, sea cual sea el dispositivo que el usuario utilizó para acceder a dicha red tuvo que utilizar una dirección **IP privada**, la cual es la que se le dio al dispositivo para poder acceder a la red o en otras palabras es el segmento de red que se le otorga al dispositivo para que éste pueda acceder a ella, y es la que utiliza **intruso o hacker** que es la persona con conocimiento informático para realizar los mencionados ciberataques, tendrá entonces acceso a todos los datos suministrados o almacenados en esa base de datos, por lo tanto mucha información personal estará comprometida y afectará de gran manera a cada uno de los usuarios hackeados.

Existen una que otra manera para prevenir los ataques mencionados anteriormente, una de ellas es la utilización de **software IDS** (Sistema de detección de intrusos), que se implementa en un dispositivo o una red para de esta manera estar atentos a los diferentes tipos de intrusos que intenten infiltrarse a la red.

Antecedentes investigativos

Para la realización de este proyecto en primera medida se tiene que realizar un estudio de los diferentes ataques a los que está expuesta una red WI-FI, debido a esto se tomara provecho de las diferentes menciones en ataques de inyección inalámbrica a los que está expuesta una red WI-FI que se encuentran en el artículo (Ibrahim Ghafir, 2018), ataques ya sean de autenticación, en la capa física, y ataques de punto de acceso no autorizado, para la solución de este problema presenta una metodología empleada en un software IDS que se encarga de monitorearlas redes WI-FI de los diferentes tipos de ataques de inyección, en particular los MitM y los de autenticación, mediante el uso de datos que pasa por el tráfico de una red WI-FI, en el presente artículo explican cómo debe ser configurada la metodología ya que ésta se debe adaptar dependiendo del ataque que se desea detectar, tomándose en cuenta que sigue sin ser suficiente abarcar todos los ataques a los que puede estar expuesta una red WI-FI se tomaran referencias de Tao Y et al (2011) donde se da a entender que, con el rápido desarrollo del Internet, la red se ha convertido en un lugar para cometer ataques o delitos informáticos. Se habla de la protección de la información de la red teniendo en cuenta los ataques a las que la ya mencionada está expuesta. El artículo nos menciona que el sistema de red es complejo y vulnerable, por esto mismo se debe hacer un estudio de los ataques que más afectan la red y así tomar medias, dicho estudio se va a realizar con una simulación de ataques de red. La simulación de ataques de red está diseñada con los modelos de parámetros de inmunidad de los ataques y las tácticas de evaluación de ataques de inmunidad. Se hace uso de una plataforma práctica para de esta manera hacer una investigación del entorno y obtener los ataques y una descripción de estos para afectan la plataforma, estos ataques simulados ahorran costos, daños, entre otras cosas y basados en todo esto se tomarán dichos ataques para una red WI-FI. A partir de aquí el objetivo ya habiendo abarcado algunos ataques, la implementación del Software es paso a seguir y para ello será de provecho la presentación que muestra (Reina, 2019) donde se encuentra la sexta parte de un tutorial para la implementación del IDS Snort con pasos simples e información detallada como de donde viene el Snort, los usos, la arquitectura, hace un especial énfasis en las reglas para la respectiva configuración de alertas, es decir la implementación del código para algunos ejemplos de los diferentes tipos de virus en el Snort, debido a que es la prioridad de la

presentación toca temas como la activación, modos de activación, instalación, protocolos entre otros, sin embargo el manejo y presentación del software IDS seguirá siendo un reto, es por ello que basados en (Xiaojin Hong, 2012) donde trabajan en la implementación de una herramienta de visualización llamada VisSRA, incorporada al IDS Snort con el fin de observar más fácilmente y rápidamente las reglas y las alertas y poder diferenciarlas, se tomaran ventajas para la representación y manipulación de dicho software pues habla detalladamente de las formas de visualización ya implementadas en el IDS Snort conocidas como los mapas de árboles con el fin de especificar detalladamente las ventajas y/o diferencias con el viso VisSRA, como por ejemplo una visión general del estado de la red para principiantes, en conclusión el experimento presenta una propuesta con cierta conveniencia para analizar las anomalías de la red para los administradores. Por ultimo Gan J et al (2015) donde dice que Internet es de libre acceso para cualquier persona y esto implica un problema en la seguridad de nuestra información o nuestros datos personales, pues usualmente todos nuestros archivos navegan por la nube, diferentes estudios de diferentes entidades comprueban la filtración de información de usuarios, afectando no solo la propiedad de los usuarios sino creando vulnerabilidad en el caso de que dicha información termine en manos de delincuentes, cualquier divulgación nos hace pensar en la seguridad de nuestra red. Por esta razón se implementa un módulo de detención en tiempo real de ataques de red que es lo más importante para la seguridad de nuestra información, el objetivo es realizar varias capas de defensa para que el atacante no pueda dar con nuestra información, haciendo backup, realizando mantenimientos, leyes y conciencia de la seguridad de nuestra información y basados en esto se realizaran las presentaciones y muestras del presente proyecto.

Metodología

El presente proyecto dará inicio con un estudio de los diferentes ataques informáticos a los que es vulnerable una red WI-FI, para de esta manera hacer una recolección de datos lo más detallada posible; para la realización de este proyecto es necesario aprender a programar el software de detección de intrusos, conocido como Snort, como bien se sabe para poder implementar el software mencionado se deben conocer los ataques que se desean detectar ya que para cada ataque Snort debe ser programado de diferente manera, es en este momento cuando se hace uso de la recolección de datos mencionada al principio, después de que se haga la implementación del software en el entorno y tiempo deseado, se realizará un análisis estadístico de los datos obtenidos para poder dar conclusiones sobre los ataques a los que la red WI-FI es más vulnerable. La investigación cuantitativa es la que permite obtener conclusiones mediante recolección de datos que son analizados con métodos estadísticos, relacionando el proceso del proyecto y la definición del enfoque investigativo se sabe que es la adecuada y la que mejor encaja con los objetivos deseados. Otro aspecto importante a tener en cuenta es que en el proyecto no se podrán saltar pasos, un paso debe llevar al otro, "El enfoque cuantitativo es secuencial y probatorio. Cada etapa precede a la siguiente y no podemos eludir pasos. El orden es riguroso." (Sampieri, 2014). Cabe destacar que la investigación cuantitativa a realizar tiene un alcance descriptivo debido a que es el que pretende y se limita a recoger y medir la información, en caso del presente proyecto, de los ataques a identificar mediante un estudio de los diferentes conceptos y variables que interfieren en lo ya mencionado.

Cronograma

		MES 1				MES 2				MES 3				MES 4			
ACTIVIDAD	SEMANA	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Investigación sobre los diferentes ataques que afectan a una red WI-FI	x	x														
2	Estudio de cada uno de los ataques yla forma de detectarlos con el software			x	x	x	x										
3	Instalar y configurar sistema operativo Raspbian en la Raspberry	x	x														
4	Instalar y configurar software IDS en la Raspberry					x	x	x	x	x							
5	Configurar router MikroTik para que todo el tráfico de la red pase primero por la Raspberry										x	x	x	x			
6	Realizar pruebas de funcionamiento del software IDS														x	x	x
7	Instalar KaliLinux en un pc en máquina virtual			x	x												
8	Aprender a realizar ataques desde KaliLinux					x	x										

9	Realizar ataques en la red para comprobar funcionamiento														x	x	x

Desarrollo

Instalación del IDS

La instalación del software IDS se realizó en un dispositivo conocido como Raspberry Pi que según el blog historia de la informática “es una placa computadora (SBC) de bajo coste, se podría decir que es un ordenador de tamaño reducido, del orden de una tarjeta de crédito… el concepto es el de un ordenador desnudo de todos los accesorios que se pueden eliminar sin que afecte al funcionamiento básico. Está formada por una placa que soporta varios componentes necesarios en un ordenador común y es capaz de comportarse como tal” (PI, 2013). Aprovechando la distribución Raspbian lite que es un sistema operativo gratuito basado en Debian, optimizado para el hardware Raspberry Pi, que viene con más de 35,000 paquetes (Raspberrypi, 2019). La versión lite no cuenta con interfaces gráficas o entorno de escritorio, se adapta a las necesidades de un sistema operativo muy ligero con un conjunto mínimo de paquetes, esta versión requiere una cantidad muy baja de RAM y uso de CPU, por esta razón es la distribución ideal para el aprovechamiento de los recursos de la Raspberry y el óptimo funcionamiento del IDS. (peppe8o, 2019)

En el primer contacto que se tiene con una Raspberry en base Raspbian lite requiere el uso de algunos recursos para su manipulación y configuración, para este caso fuera de las Raspberry se necesitó un teclado, un monitor con interface HDMI, un adaptador de 5V y un cable HDMI, los cuales en conjunto permitieron los primeros pasos de configuración del sistema operativo Raspbian.

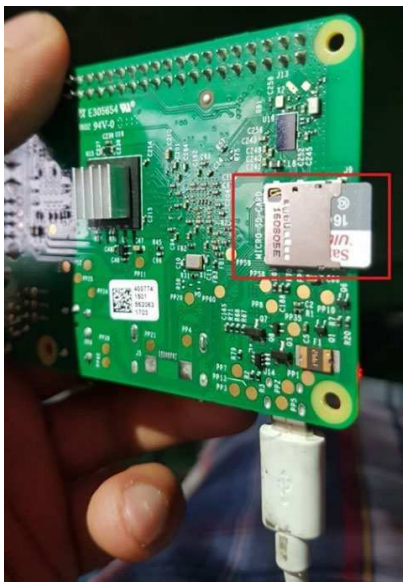


Figura 1. Raspbian3 con su respectiva microSD. (Autoridad propia)

Figura 2. Raspberry pi 3 con alimentación HDMI y corriente. (Autoridad propia)

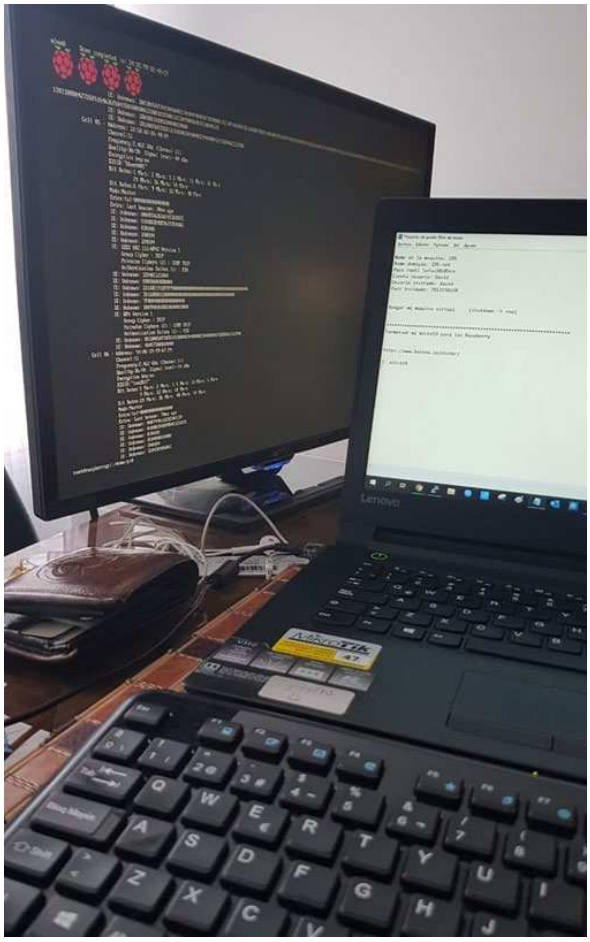


Figura 3. Primer contacto con Raspbian lite. (Autoridad propia)

Para la inserción del sistema operativo que no es más que un archivo de formato iso, en la microSD de manera correcta para una iniciación limpia de Raspbian en la Raspberry se requiere de un proceso y un software adecuado, proceso en el cual se utilizó el aplicativo conocido como balenaEtcher que según su sitio oficial:

> "Nace con la necesidad de facilitar mediante una aplicación el flasheo, escritura y sobreescritura de una tarjeta SD de manera simple para sus usuarios finales, extensible para los desarrolladores, otorgando seguridad en los procesos y con la disponibilidad en cualquier plataforma (Windows/MAC/Linux)" (balenaEtcher, 2019).

Gracias a las funciones que presta la aplicación en cuestión se puede realizar la escritura del sistema operativo raspbian lite sobre la microSD de la Raspberry o en su defecto la sobreescritura de la imagen creada como respaldo de la información y configuración ya realizada (Backup).

BalenaEtcher tiene una interfaz gráfica que permite cargar la imagen que se desea escribir en la microSD seleccionada, con el fin de lograr una escritura o sobreescritura de manera simple.

Figura 4. Interfaz gráfica balenaEtcher. (Autoridad propia)

1. Selección de imagen (.iso)
2. Selección de microSD
3. Inicio del proceso de escritura

En el primer contacto que se tiene con el sistema operativo se encuentran líneas de comando informando sobre cada una de las inicializaciones de servicios de Raspbian con el fin de tener un seguimiento del encendido de este, se puede evidenciar un “OK” en cada uno de los procesos que al final llevan a la autenticación de usuario para administración, por defecto el usuario administrativo y su respectiva contraseña son:

Usuario: pi

Contraseña: raspberry

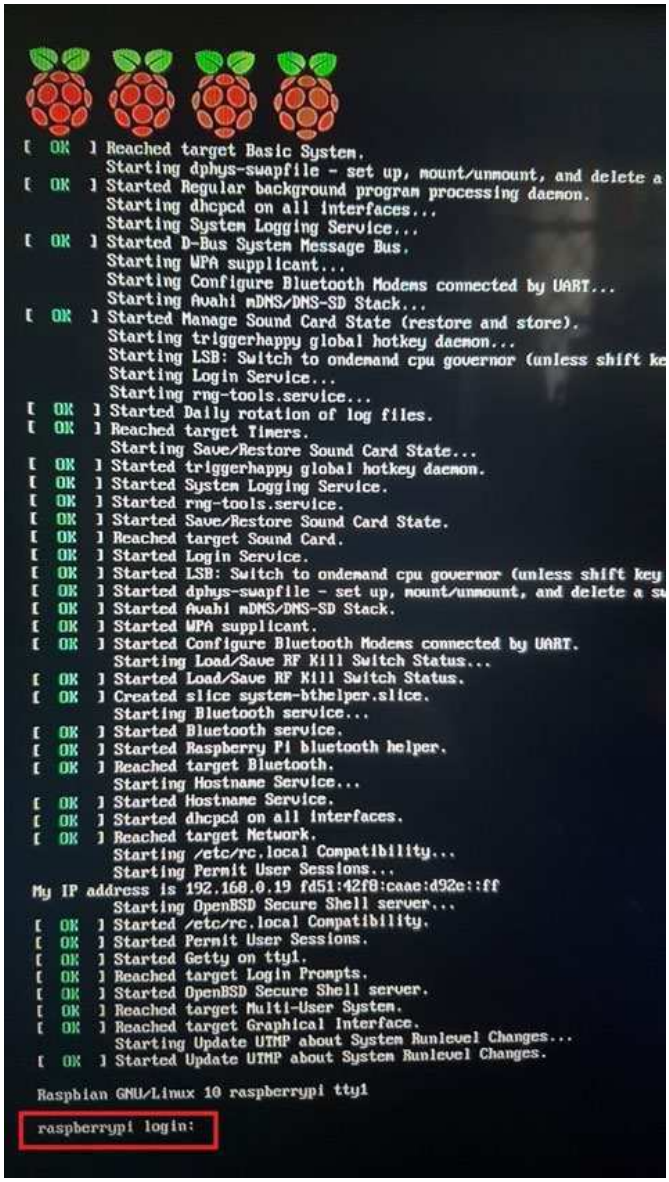


Figura 5. Estado de inicialización de Raspbian. (Autoridad propia)

Para la configuración del sistema operativo e instalación del IDS se requiere el uso de un usuario conocido como “Superusuario” el cuál en Raspbian se crea automáticamente con el nombre “root” y que cuenta con acceso a la raíz del sistema, es decir a /root. Para este caso se le asignará la contraseña (Safas10i05ce) al usuario root con el comando que se aprecia en la figura 6 donde solicitará introducir la contraseña y confirmarla.

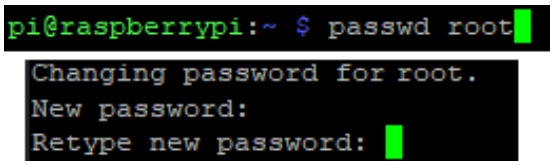


Figura 6. Cambio de contraseña. (Autoridad propia)

Autenticados como usuario “root” se procede a la configuración del sistema operativo donde como primer paso se requiere el acceso a internet mediante una red Wi-Fi y para ello se gestiona la validación de usuarios y contraseña de la red Wi-Fi deseada que se configura editando el fichero (wpa_supplicant.conf) ubicado en el directorio “/etc/wpa_supplicant” aprovechando el editor de texto nano que viene instalado por defecto en el sistema operativo raspbian utilizando así el comando expuesto en la figura 7.

```
nano /etc/wpa_supplicant/wpa_supplicant.conf
```

Figura 7. Comando editor del fichero wpa_supplicant. conf. (Autoridad propia)

Según un blog:

> “Nano es un editor de texto minimalista y amigable que no solo nos permite editar texto, sino que además tiene otras características muy interesantes que lo hacen especialmente útil para modificar archivos de configuración en la terminal… Entre otras características, nano nos ofrece las siguientes: Operaciones de búsqueda y reemplazo interactivas, permite las hacer y deshacer acciones, permite ir directamente a un número de línea o autoguardado de archivos” (atareao, 2017).

Al ingresar en el fichero (wpa_supplicant.conf) se encontrará una ventana editable con sus respectivas funciones en la parte inferior como se aprecia en la figura 8, donde se digitará las líneas de código que se evidencian en la figura 9 remplazando “nombre-de-tu-wifi” y “password-de-tu-wifi” por los datos solicitados conservando las comillas.

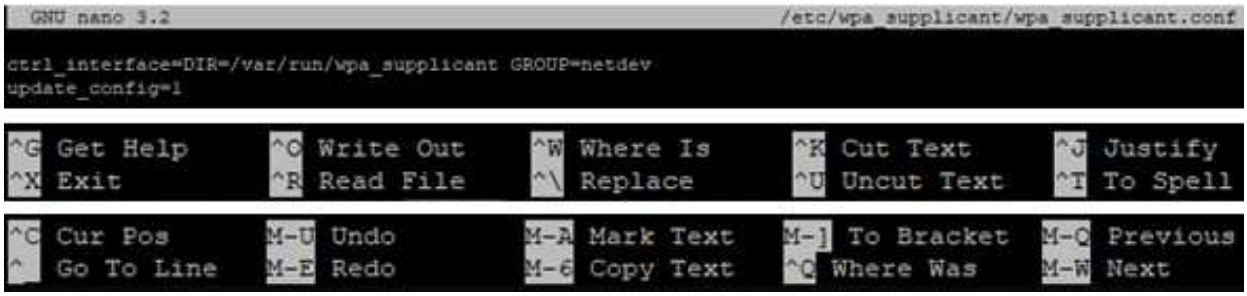


Figura 8. Ventana de configuración del fichero wpa_supplicant. conf en nano. (Autoridad propia)

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
update_config=1
country=ES

network={
        ssid="nombre-de-tu-wifi"
        psk="password-de-tu-wifi"
        key_mgmt=WPA-PSK
}
```

Figura 9. Línea de código para autenticación. (Llamas, 2018)

La configuración de autenticación para la red Wi-Fi quedo como se encuentra en la figura 10 y las pruebas realizadas para validar servicios de navegación se evidencian en la figura 11, donde básicamente se realiza un ping a los DNS de Google donde se obtiene respuesta de estos. Adicionalmente se realiza una validación de los valores de configuración de red TCP/IP actuales mediante el comando expuesto en la figura 12 donde se evidencia el direccionamiento asignado a la interfaz wlan0.

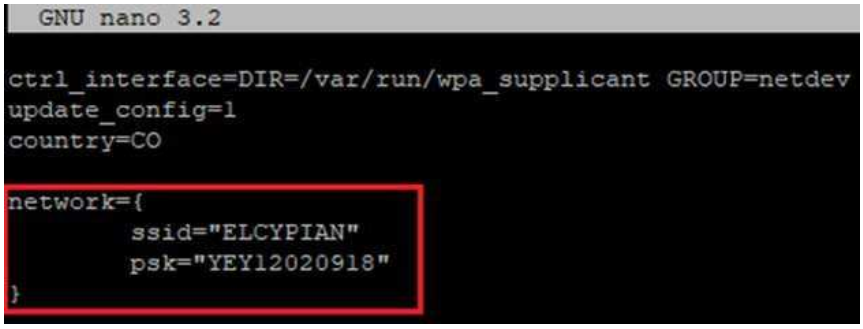


Figura 10. Líneas de código para autenticación de red Wi- Fi. (Autoridad propia)

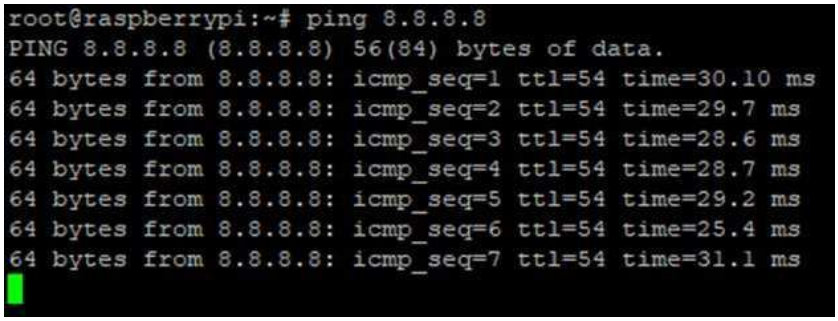


Figura 11. Ping a los DNS de Google. (Autoridad propia)

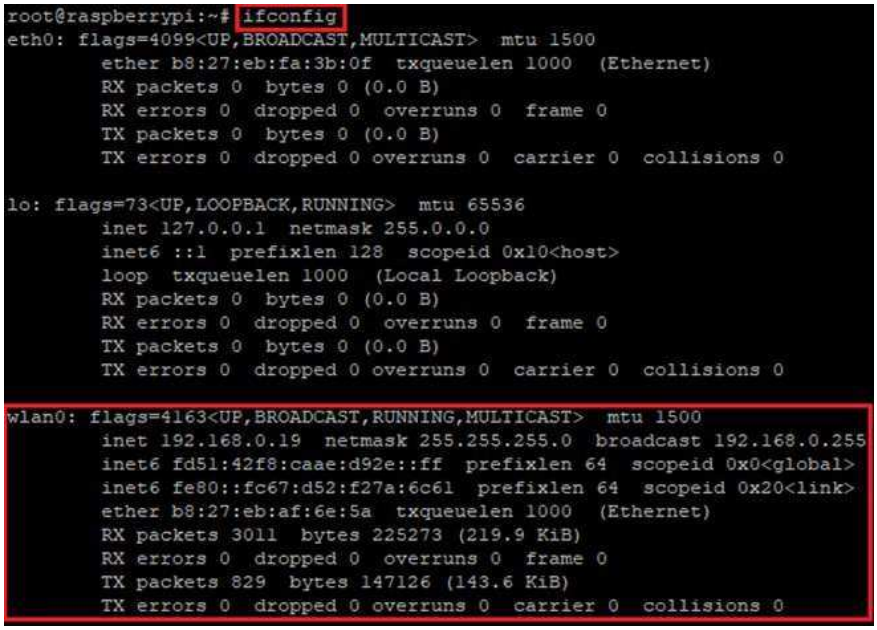


Figura 12. Direccionamiento de la interface wlan. (Autoridad propia)

Aprovechando la conexión a internet se procede a la instalación y actualización de aplicativos y servicios previos requeridos para la instalación y configuración del IDS como por ejemplo el cambio de editor de texto “nano” a “vim” puesto que según Ciberaula.

> “Vim además de ser un editor muy potente y suplir las opciones de nano, permite hacer complicadas operaciones en grandes ficheros con muy pocos comandos, por lo que su aprendizaje puede ahorrarnos mucho tiempo… Vim, es un clon mejorado del “vi”, incluye coloreado de sintaxis para casi todos los lenguajes de programación existentes y ficheros de configuración de Linux/Unix” (Ciberaula, 2019).

Esta instalación se realizó bajo el comando que se evidencia en la figura 13.

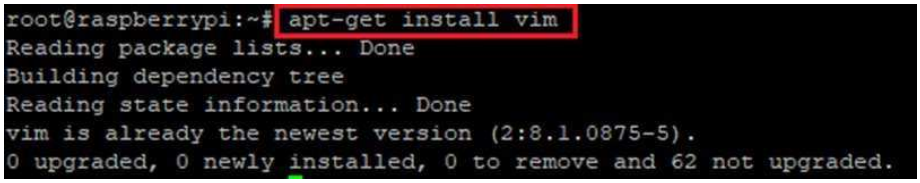


Figura 13. Instalación del editor de texto vim. (Autoridad propia)

Teniendo la Raspberry conectada a una red Wi-Fi y parámetros iniciales configurados como lo es la instalación del editor de texto "vim" se puede considerar la implementación de un túnel de administración del dispositivo con el fin de omitir periféricos innecesarios como los son, el monitor y el teclado, llegando así a la configuración del sistema operativo raspbian en línea de comandos desde un equipo de cómputo ubicado en el mismo segmento de red, para esto se considera el uso del aplicativo PuTTY.

"PuTTY es un emulador gratuito de terminal que soporta cliente SSH y Telnet entre muchos otros protocolos, con el podemos conectarnos a servidores remotos iniciando una sesión en ellos que nos permite ejecutar comandos" (Zeokat, 2014). Es una herramienta muy útil a la hora de conectar a un servidor Unix o Linux a través de SSH pues permite administrar un servidor remoto mediante línea de comandos de manera gratuita y portable en múltiples plataformas, además de contar con un constante desarrollo y una gran comunidad que brinda amplias oportunidades de soporte. Estas cualidades hacen de PuTTY una herramienta fundamental para la instalación y configuración del IDS en Raspbian.

Para establecer el túnel de comunicación con PuTTY entre un equipo de cómputo y la Raspberry ubicados en el mismo segmento de red es necesario utilizar el protocolo de comunicación SSH que según el blog de Tutorial H Hostinger

> "SSH o Secure Shell, es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet, a través de un mecanismo de autenticación. Proporciona un mecanismo para autenticar un usuario remoto, transferir entradas desde el cliente al host y retransmitir la salida de vuelta al cliente. El servicio se creó como un reemplazo seguro para el Telnet sin cifrar y utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sucedan de manera encriptada" (C., 2019).

La interface gráfica de PuTTY tiene diferentes prestaciones con las cuales se puede llegar a establecer un túnel SSH para la administración de la Raspberry de manera sencilla. En la figura 14 se encuentran los parámetros establecidos a lo largo de toda la configuración e instalación del IDS, dentro de los cuales se encuentra la IP con la que se entabla el túnel, el puerto y el protocolo de comunicación, también se encuentra un apartador para guardar el túnel con el fin de poder realizarlo en cualquier momento de manera simple.

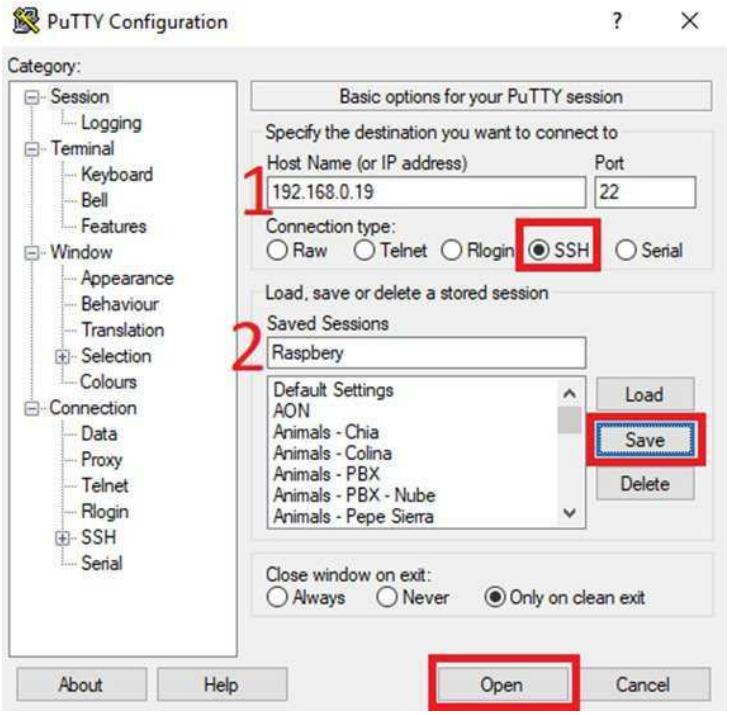


Figura 14. Interface grafica de PuTTY. (Autoridad propia)

Los respectivos apartados evidenciados en la figura 14 hacen referencia a la selección de protocolo, guardado e inicio de comunicación, también se encuentra:

1. Dirección IP adoptada por la Raspberry
2. Nombre del túnel SSH guardado en PuTTY

Cabe resaltar que para la implementación del túnel es necesario habilitar los permisos para la conexión por el protocolo de comunicación SSH de la Raspberry, esto se realiza modificando el fichero (sshd_config) ubicado en el directorio "/erc/ssh" con el comando que se aprecia en la figura 15, donde básicamente se reemplaza las líneas de código como se evidencian en la figura 16. Adicionalmente es necesario correr el comando de habilitación ssh como se puede ver en la figura 17.

```
root@raspberrypi:~# vim /etc/ssh/sshd_config
```

Figura 15. Comando para edición del fichero sshd_config. (Autoridad propia)

Antes

```
# Authentication:

#LoginGraceTime 2m
#PermitRootLogin without-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Despues

```
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Figura 16. Cambios de líneas de código para habilitación SSH. (Autoridad propia)

```
root@raspberrypi:~# systemctl enable ssh
```

Figura 17. Comando para habilitación de servicios SSH. (Autoridad propia)

Establecido el túnel se encuentra una ventana del aplicativo PuTTY como en la figura 18 donde se puede administrar, gestionar y configurar el raspbian y el IDS de manera remota desde un computador ubicado en el mismo segmento de red.

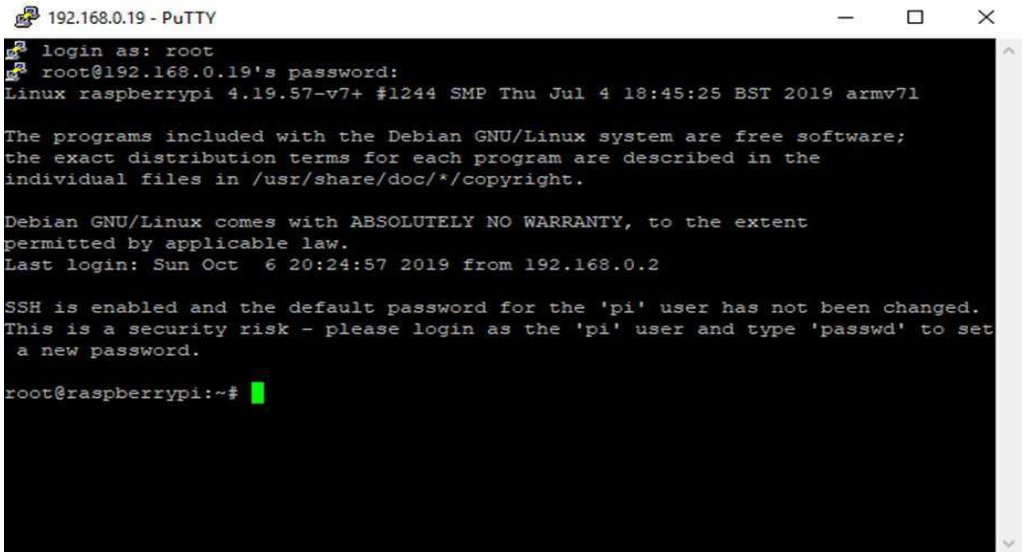


Figura 18. Ventana del aplicativo PuTTY con túnel establecido. (Autoridad propia)

No obstante, aparece un percance en esta etapa de configuración de la Raspberry pues en cada reinicio que requiere el dispositivo, el direccionamiento IP que adopta es alterado puesto que la configuración de red está asignada mediante un DHCP Client que según el blog de Adslzone “Se trata de un protocolo de configuración dinámica de host… de tipo cliente / servidor que se encarga de asignar direcciones IP de forma dinámica… Esto es lo que permite que puedan comunicarse con otras redes IP” (Gonzáles, 2019). Este percance provoca la reconexión de los periféricos, teclado y monitor con el fin de conocer el nuevo direccionamiento adoptado para volver a establecer el túnel con el aplicativo PuTTY.

Para dar solución a este inconveniente se requiere la configuración de un direccionamiento estático, el cual se puede asignar configurando el fichero (dhcpcd.conf) ubicado en el directorio “etc” con el comando que se evidencia en la figura 19. En este fichero se encontrará comentadas algunas líneas de código ofreciendo un ejemplo de configuración de direccionamiento estático como se evidencia en la figura 20, aprovechando este ejemplo se aplica una nueva línea de código asignado el direccionamiento deseado y a la interface de red que se desee, en este caso la interface Wireless como se puede ven en la figura 21. Con esto se da solución definitiva pues cada reinicio que requiera el dispositivo llevará a una asignación estática de direccionamiento IP que permitirá establecer un túnel SSH sin problema alguno.

```
root@raspberrypi:~# vim /etc/dhcpcd.conf
```

Figura 19. Comando para edición de fichero dhcpcd.cong. (Autoridad propia)

```
# Example static IP configuration:
#interface eth0
#static ip_address=192.168.0.10/24
#static ip6_address=fd51:42f8:caae:d92e::ff/64
#static routers=192.168.0.1
#static domain_name_servers=192.168.0.1 8.8.8.8 fd51:42f8:caae:d92e::1
```

Figura 20. Ejemplo de direccionamiento estático. (Autoridad propia)

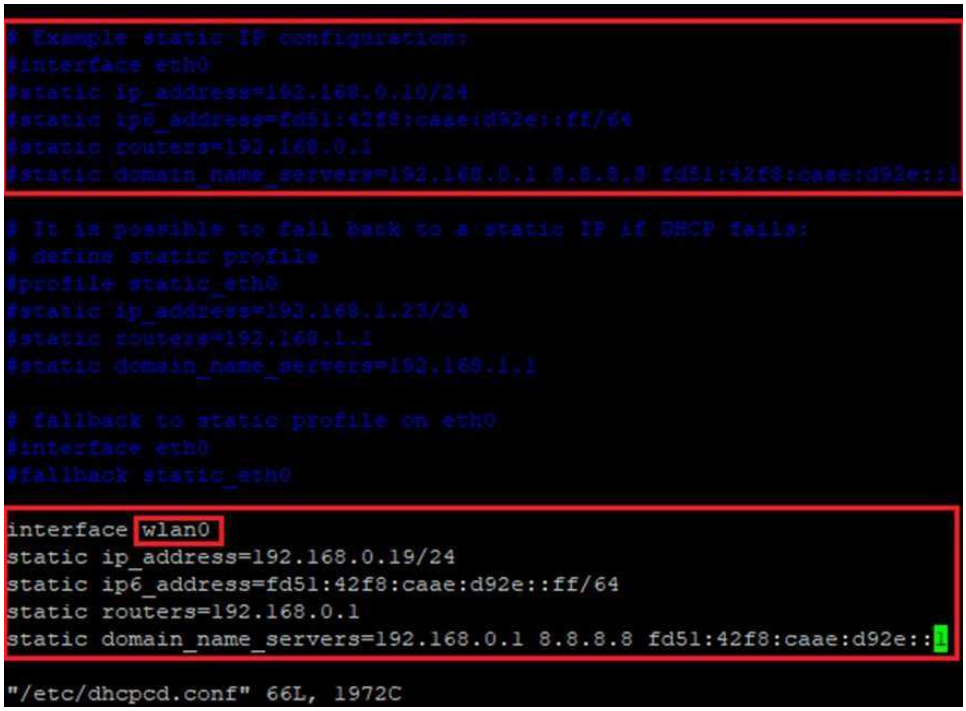


Figura 21. Configuración de direccionamiento estático. (Autoridad propia)

A partir de este momento teniendo la Raspberry preconfigurada se puede proceder con la instalación del IDS "Snort" el cual según su página oficial.

> "Snort es un sistema de prevención de intrusiones de red de código abierto, capaz de realizar análisis de tráfico en tiempo real y registro de paquetes en redes IP. Puede realizar análisis de protocolo, búsqueda / coincidencia de contenido, y puede usarse para detectar una variedad de ataques y sondas, como desbordamientos de búfer, escaneos de puertos furtivos, ataques CGI, sondas SMB, intentos de huellas dactilares del sistema operativo y mucho más" (Snort, Snort, 2019)

Lo que llevo a su selección debido a sus grandes disponibilidades como lo menciona el blog de Reporte Digital.

> "La gran escalabilidad que ha tenido snort, y flexibilidad para ejecutarse en varios sistemas operativos y la capacidad que tiene de realizar acciones para alertar a usuarios de actividades sospechosas en la red a través del uso de firmas, los usuarios pueden personalizar su propio conjunto de reglas. Para lograrlo se recibe la ayuda tecnológica de la vasta comunidad snort. De igual manera se puede monitorear el tráfico entrante y saliente e identificar el tráfico sospechoso o malicioso.

La ventaja de snort es que la tecnología goza de una tasa de adopción bastante amplia. Esto representa remedios rápidos para las amenazas emergentes. Por ejemplo, Equifax, una compañía de tecnología, pudo solucionar un problema de vulnerabilidad gracias a una Snort Rule. Este parche estuvo disponible un día después de que se anunciara esta amenaza" (Editorial, 2019)

Para la instalación de Snort como primer paso se hace uso del comando de la figura 22, el cuál según el cofundador de Codection "Actualiza la lista de paquetes disponibles y sus versiones, pero no instala ningún paquete. Esta lista la coge de los servidores con repositorios que tenemos definidos en Raspbian" (Gil, 2013)

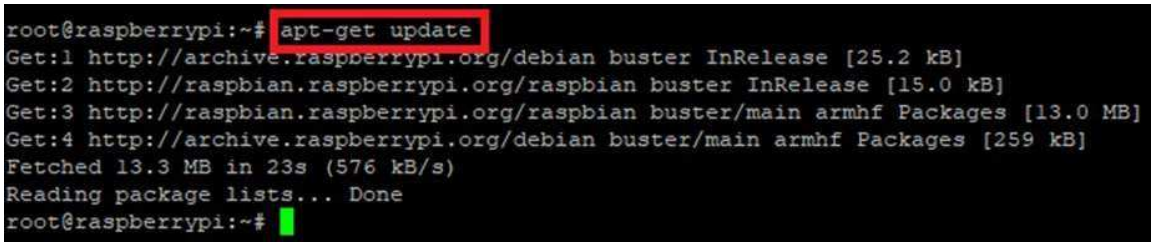


Figura 22. Comando apt- get update para actualización de paquetes. (Autoridad propia)

Posterior a esto es necesario preparar el servidor haciendo la instalación de todas las bibliotecas que son requisitos previos para el correcto funcionamiento de Snort, este proceso se realiza con los comandos que aparecen en la figura 23, en caso de requerir confirmación de la instalación es necesario digitar "Y" y pulsar enter.

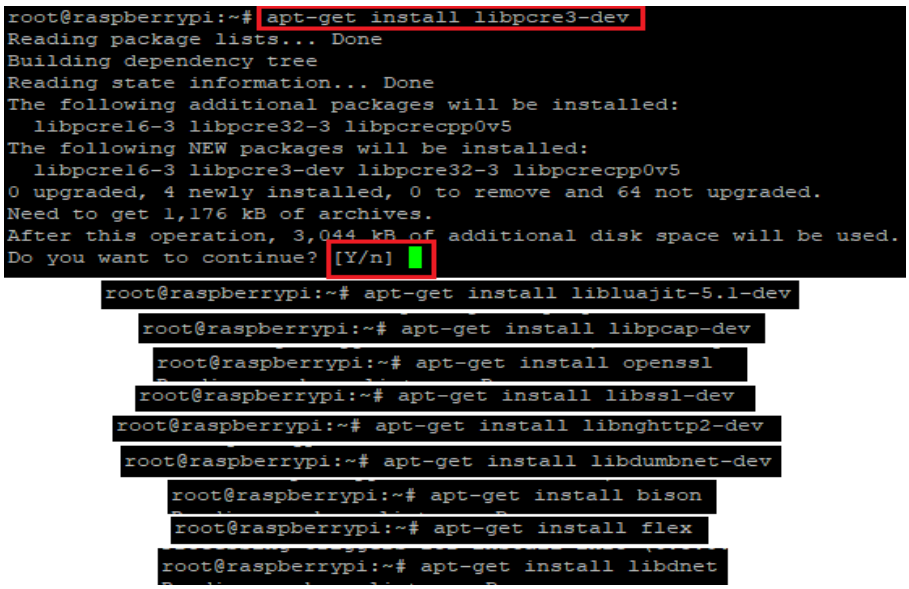


Figura 23. Comandos para la instalación de bibliotecas para el uso correcto de Snort. (Autoridad propia)

Aunque para la instalación de la biblioteca libnghttp2 se debe utilizar el comando de la figura 24 ya que no se encontraban los paquetes compatibles para la descarga e instalación de la librería puesto que la arquitectura de Raspberry es en "arm" y la arquitectura "–dev" no siempre funciona a pesar de que Raspbian sea en base Debian.

```
root@raspberrypi:~# apt-get install libnghttp2-14:armhf
```

Figura 24. Comando de instalación biblioteca l ibnghttp2- 14:armhf. (Autoridad propia)

Después de la instalación de los requisitos previos se procede a crear una carpeta o directorio llamada "snort_src" con el comando presentado en la figura 25, posterior a esto (Ruostemma, 2019) cuenta que "Snort utiliza algo llamado Biblioteca de adquisición de datos (DAQ) para hacer llamadas abstractas a las bibliotecas de captura de paquetes"

Para descargar la biblioteca de adquisición de datos (DAQ) se hace uso del comando de la figura 26, luego se hace la extracción del código fuente con el comando presentado en la figura 27.

```
root@raspberrypi:~# cd snort_src
```

Figura 25. Creación de directorio snort_src. (Autoridad propia)

```
root@raspberrypi:~/snort_src# wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
```

Figura 26. Descarga de la biblioteca de adquisición de datos de Snort. (Autoridad propia)

```
root@raspberrypi:~/snort_src# tar -xvzf daq-2.0.6.tar.gz
```

Figura 27. Extracción código fuente. (Autoridad propia)

Luego de la descarga del DAQ se procede a su instalación la cual requiere el siguiente proceso, primero que todo es necesario dirigirse al directorio daq-2.0.6, para de esta manera ejecutar el script de configuración utilizando sus valores predeterminados, y así mismo compilar el programa para finalmente instalar la biblioteca de adquisición de datos, este proceso de instalación se lleva a cabo con los comandos presentados en la figura 28 en su respectivo orden.

```
root@raspberrypi:~/snort_src# cd daq-2.0.6
root@raspberrypi:~/snort_src/daq-2.0.6# ./configure
root@raspberrypi:~/snort_src/daq-2.0.6# make
root@raspberrypi:~/snort_src/daq-2.0.6# make install
```

Figura 28. Instalación de la biblioteca de adquisición de datos. (Autoridad propia)

Por medio del comando de la figura 29 se hace la descarga del Snort en su versión actual, ya que al no utilizar su última versión va a generar un error.

Figura 29. Comando para la descarga del Snort. (Autoridad propia)

Al haber realizado los procesos anteriores de manera exitosa ya se tiene descargado el software Snort, por lo tanto se procede a su instalación, para esto se deben ejecutar una serie de comandos que se ven en la figura 30, los cuales sirven primero para extraer los archivos, después dirigirse al directorio llamado "cd-snort-2.9.15", y así configurar la instalación del archivo fuente o el sourcefile habilitado para poder compilar, cabe resaltar que es un proceso demorado pero gracias a estos pasos previos se podrá instalar el Snort con el comando de la figura 31.

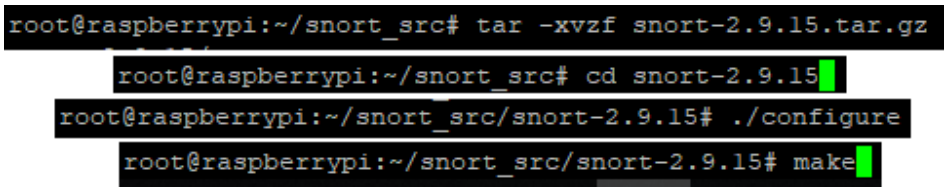


Figura 30. Configuración del archivo fuente para instalación Snort. (Autoridad propia)

Figura 31. Instalación del Software IDS Snort. (Autoridad propia)

Configuración de IDS

En este momento teniendo instalado el software Snort se procede con la configuración donde se editarán algunos archivos de configuración comenzando por la actualización de bibliotecas compartidas utilizando el comando de la figura 32 donde según del blog de Linux 10 Hacks "ldconfig se usa para crear, actualizar y eliminar enlaces simbólicos para las bibliotecas compartidas actuales basadas en los directorios lib" (Ramesh, 2019)

Figura 32. Comando para actualización de bibliotecas. (Autoridad propia)

Snort queda instalado en el directorio (/usr/local/bin/snort) y se sabrá con el comando de la figura 33, se procederá con crear un enlace simbólico del Snort con el comando de la figura 34.

Figura 33. Comando para conocer la ubicación de Snort. (Autoridad propia)

```
root@raspberrypi:~# ln -s /usr/local/bin/snort /usr/sbin/snort
```

Figura 34. Comando para crear un enlace simbólico de Snort. (Autoridad propia)

Adicionalmente se requiere un modo seguro para la inicialización del Snort en Raspbian lo cual se realizará creando un grupo de usuarios el cual se llamará "snort" con el fin de que los usuarios dentro de este grupo se ejecuten bajo el dominio, esto se realizará con el comando que se evidencia en la figura 35. Posterior a esto se requiere crear un usuario para el sistema operativo sin privilegios administrativos al que se le asignara el nombre "snort" y a su vez asignándolo al grupo "snort" previamente creado, esto se realizara con el comando evidenciado en la figura 36.

```
root@raspberrypi:~# groupadd snort
```

Figura 35. Comando para crear grupo snort. (Autoridad propia)

```
root@raspberrypi:~# useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort
```

Figura 36. Comando para crear el usuario snort y asignarlo al grupo snort. (Autoridad propia)

Culminadas las creaciones de usuarios y grupos de usuarios se procede con la creación de algunos directorios donde se albergará la configuración de Snort estos directorios se llamarán respectivamente "rules – snort - snort_dynamicrules" y se crearán con el comando que se ve en la figura 37. Luego de eso se le asignan los permisos a cada uno de esos directorios con los comandos que se evidencian en la figura 38.

```
root@raspberrypi:~# mkdir -p /etc/snort/rules
root@raspberrypi:~# mkdir /var/log/snort
root@raspberrypi:~# mkdir /usr/local/lib/snort_dynamicrules
```

Figura 37. Comando creación de directorios de snort. (Autoridad propia)

```
root@raspberrypi:~# chmod -R 5775 /etc/snort
root@raspberrypi:~# chmod -R 5775 /var/log/snort
root@raspberrypi:~# chmod -R 5775 /usr/local/lib/snort_dynamicrules
root@raspberrypi:~# chown -R snort:snort /etc/snort
root@raspberrypi:~# chown -R snort:snort /var/log/snort
root@raspberrypi:~# chown -R snort:snort /usr/local/lib/snort_dynamicrules
```

Figura 38. Comando para asignar permisos a directorios de snort. (Autoridad propia)

Seguido se configurará el preprocesador de reputación del snort con el fin de crear nuevos archivos para las blacklist/whitelist que según el sitio web oficial de Snort.

> "El preprocesador de reputación proporciona capacidades básicas de lista negra / lista blanca de IP, para bloquear / descartar / pasar tráfico de las direcciones IP enumeradas. En el pasado, usamos reglas estándar de Snort para implementar el bloqueo de IP basado en reputación. Este

preprocesador abordará el problema de rendimiento y facilitará la gestión de la reputación de IP. El preprocesador de reputación se ejecuta antes que otros preprocesadores" (Snort, Snort, 2019)

Este proceso se realiza con los comandos de la figura 39, seguido a esto se deben copiar los ficheros de configuración que quedaron en el directorio de descargas a los directorios previamente creados con el comando de la figura 37, este proceso se realizara con el comando de la figura 40.

```
root@raspberrypi:~# touch /etc/snort/rules/white_list.rules
root@raspberrypi:~# touch /etc/snort/rules/black_list.rules
root@raspberrypi:~# touch /etc/snort/rules/local.rules
```

Figura 39. Comando para crear archivos para las blacklist/ whitelist. (Autoridad propia)

```
root@raspberrypi:/etc# cp ~/snort_src/snort-2.9.15/etc/*.conf* /etc/snort
root@raspberrypi:/etc# cp ~/snort_src/snort-2.9.15/etc/*.map /etc/snort
```

Figura 40. Comando para copiar los archivos de descargas. (Autoridad propia)

Lo siguiente será realizar la descarga de reglas de detección que Snort seguirá para la identificación de posibles amenazas y esto se puede realizar obteniendo un código el cual al registrarse de forma gratuita en el sitio web de Snort tendrá el privilegio de obtenerlo, a este código en la comunidad de Snort se le conoce como "Oink" y básicamente permite descargar los conjuntos de reglas de usuarios registrados, para este proyecto el Oinkcode asignado por Snort es (47b2a6db35497010b55c6d314154578bd59b6e68) el cual se obtiene siguiendo los pasos del anexo "1. Obtener Oinkcode". Una vez obtenido el Oinkcode se procede a la descarga de las reglas con el comando de la figura 41 donde se puede apreciar el Oinkcode asignado por Snort, luego de culminar la descarga lo siguiente es extraer estas reglas en el directorio de configuración "snort" con el comando que se evidencia en la figura 42, donde al final se obtendrá los ficheros y directorios que se pueden apreciar en la figura 43.

```
wget https://www.snort.org/rules/snortrules-snapshot-29120.tar.gz?oinkcode=
oinkcode=47b2a6db35497010b55c6d314154578bd59b6e68 -O registered.tar.gz
```

Figura 41. Comando para descargar reglas de Snort. (Autoridad propia)

```
root@raspberrypi:/etc/snort# tar -xvf registered.tar.gz -C /etc/snort
```

Figura 42. Comando para extraer las reglas de Snort. (Autoridad propia)

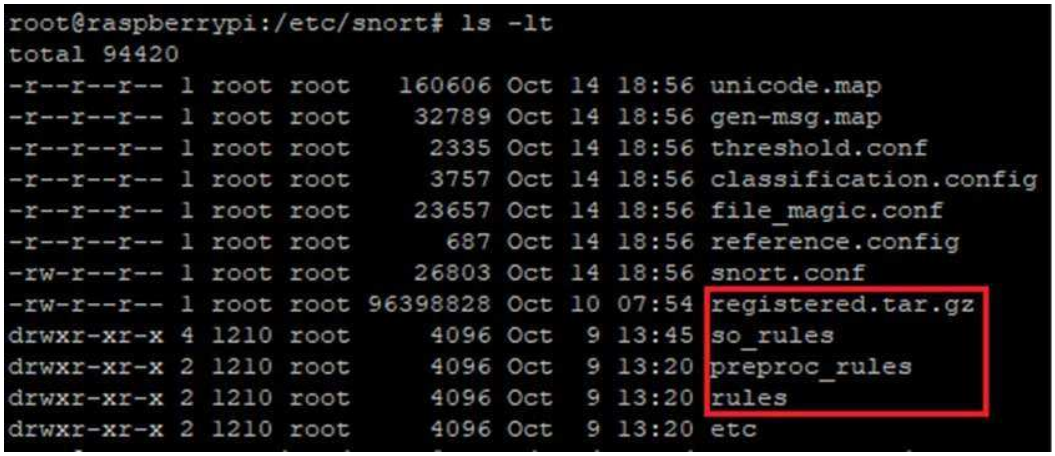


Figura 43. Ficheros y directorios obtenidos por la descarga del Oinkcode. (Autoridad propia)

Dentro de las reglas extraídas y descargadas se incluye una gran variedad de reglas útiles para detección y preconfiguración que se irán viendo a lo largo del proyecto. Antes de esto se requieren configuraciones previas para modificar parámetros como la variable que se utilizara en las reglas de detección a la que en este caso se le asignará el nombre de "HOME_NET" o también el segmento de red el cual será objetivo claro de análisis y protección, estos parámetros se modificaran en el fichero "snort.config" ubicado en el directorio de configuración "snort" al que se accederá con el comando de la figura 44. El cambio de variable se ve en la figura 45, mientras que el cambio de segmento se aprecia en la figura 46. Además de esto en este mismo fichero se asignarán las carpetas previamente creadas en la figura 37, para ser objeto de configuración y de análisis esto debería verse como en la figura 47.

Figura 44. Comando para acceder al fichero "snort. conf". (Autoridad propia)

Figura 45. Cambio de variable en el fichero "snort. conf". (Autoridad propia)

Figura 46. Cambio de segmento en el fichero "snort.conf". (Autoridad propia)

Figura 47. Asignación de carpetas a las configuraciones de Snort. (Autoridad propia)

Seguido de estas preconfiguraciones en el mismo fichero "snort.conf" en la sección identificada como "Step 6" la cual se ve resaltada en la figura 48 se configura la salida unified2 que según la página oficial de Snort funciona de la siguiente manera.

> "Unified2 puede funcionar en uno de los tres modos, registro de paquetes, registro de alertas o registro unificado verdadero. El registro de paquetes incluye una captura de todo el paquete y se especifica con log_unified2. Del mismo modo, el registro de alertas solo registrará eventos y se especifica con la alerta unificada2. Para incluir ambos estilos de registro en un único archivo unificado, simplemente especifique unificado2" (Snort, Snort, 2019)

Esta configuración tiene como fin un registro del Unified2 con el nombre del fichero "snort.log" donde básicamente se apreciará el log de análisis en un espacio de tiempo requerido para así llevar una base de datos de los registros del IDS y acudir a ellos en el momento que se les necesite, esta configuración debería quedar como en la figura 48.

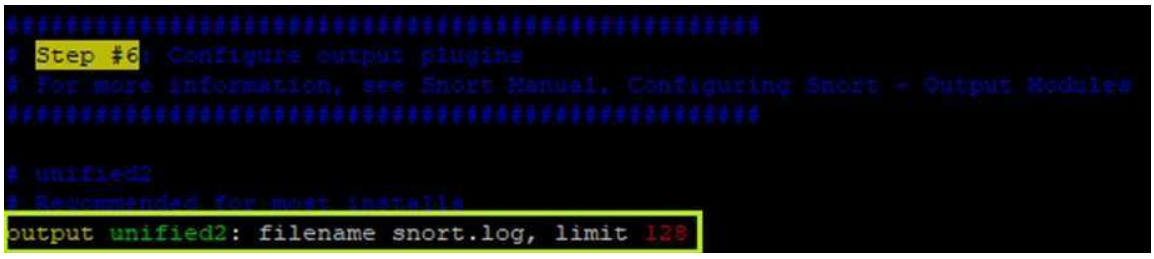


Figura 48. Configuración del Unified2 del Snort. (Autoridad propia)

En el mismo fichero "snort.conf" al final de este, se encontrará una lista de conjuntos de reglas incluidas como se evidencia en la figura 49, donde básicamente se suprimirá el carácter "#" en cada una de las reglas locales, el cual tiene como función comentar las líneas de código introducidas en

un fichero para que a su vez quede como una línea informativa y no una función, esto con el objetivo de que Snort trabaje con cualquier regla personalizada dejando las líneas de código como instrucciones como en la figura 49.

```
# site specific rules
include $RULE_PATH/local.rules

include $RULE_PATH/app-detect.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/blacklist.rules
include $RULE_PATH/botnet-cnc.rules
include $RULE_PATH/browser-chrome.rules
include $RULE_PATH/browser-firefox.rules
include $RULE_PATH/browser-ie.rules
include $RULE_PATH/browser-other.rules
include $RULE_PATH/browser-plugins.rules
include $RULE_PATH/browser-webkit.rules
include $RULE_PATH/chat.rules
include $RULE_PATH/content-replace.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/experimental.rules
include $RULE_PATH/exploit-kit.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/file-executable.rules
include $RULE_PATH/file-flash.rules
include $RULE_PATH/file-identify.rules
include $RULE_PATH/file-image.rules
include $RULE_PATH/file-multimedia.rules
include $RULE_PATH/file-office.rules
include $RULE_PATH/file-other.rules
include $RULE_PATH/file-pdf.rules
```

Figura 49. Lista de conjuntos de reglas incluidas sin comentar. (Autoridad propia)

Ejecución de Snort

A partir de aquí Snort ya está configurado y listo para ejecutarse y para validar dicha configuración y la correcta instalación se utilizará el parámetro "-T" que básicamente habilita el modo de pruebas en la ejecución de Snort, esto se realizará con el comando que se evidencia en la figura 50, donde como resultados se enviará un reporte a la ventana de comandos donde se podrá apreciar la inicialización del software IDS Snort como se puede ver en la figura 51, una vez culminado su proceso reportará la satisfactoria validación de configuración del Snort y saldrá automáticamente del proceso como se puede evidenciar en la figura 52.

```
root@raspberrypi:/etc/snort# snort -T -c /etc/snort/snort.conf
```

Figura 50. Comando para ejecución en modo de prueba de Snort. (Autoridad propia)

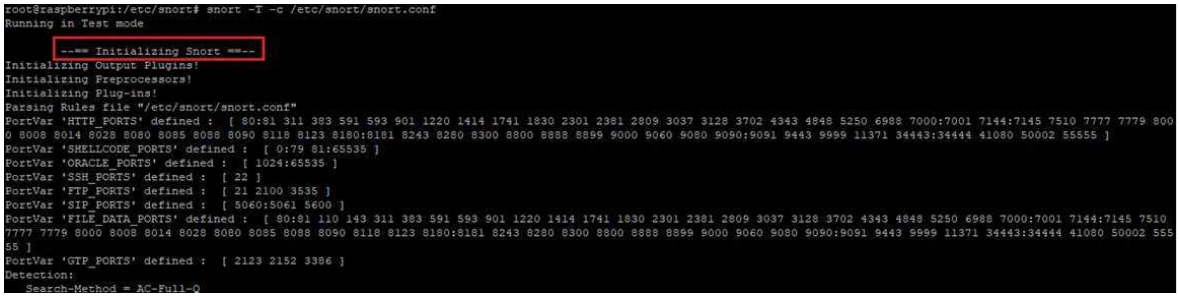


Figura 51. Inicialización de pruebas de Snort. (Autoridad propia)

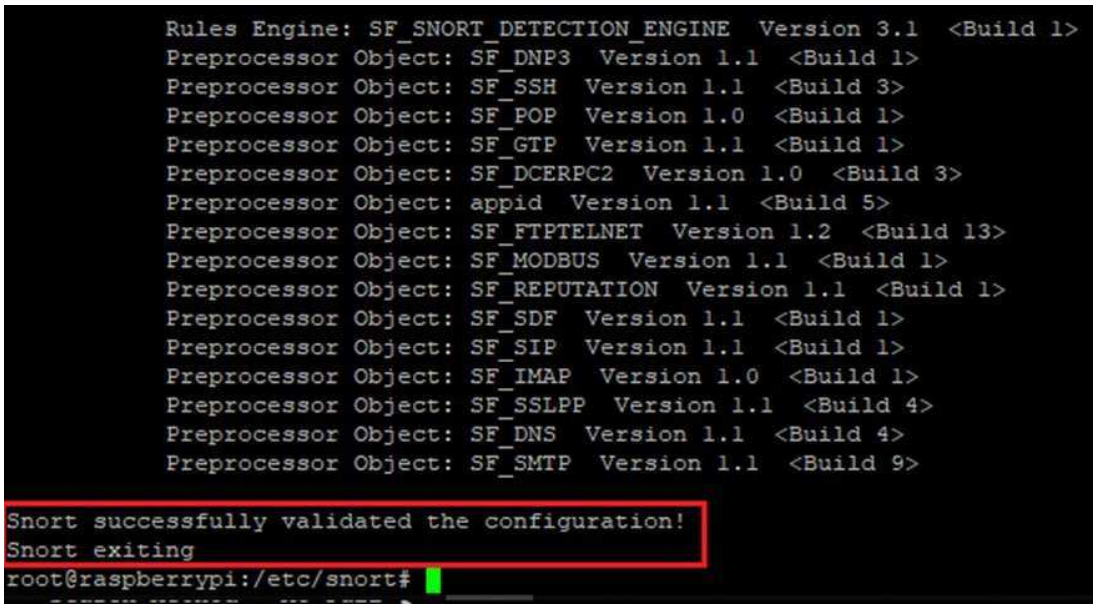


Figura 52. Finalización de pruebas Snort. (Autoridad propia)

Para iniciar Snort se requiere la asignación de al menos una regla personalizada, para esta validación se configuraron un par de reglas como se evidencia en la figura 53, las cuales se detallarán a profundidad más adelante, sin embargo, es importante aclarar que estas reglas se configuran en el fichero "local.rules" ubicado en el directorio "/etc/snort/rules/" y se ingresara a este fichero con el comando de la figura 54.

Figura 53. Reglas para validación del funcionamiento de Snort. (Autoridad propia)

```
root@raspberrypi:/etc/snort# vim /etc/snort/rules/local.rules
```

Figura 54. Comando para ingresar al fichero local. rules. (Autoridad propia)

Configuradas un par de reglas y validada la configuración del Snort ya se puede proceder con la ejecución del IDS la cual se realizará con el comando de la figura 55 donde básicamente se está dando la instrucción "-A console" (ejecutar la acción consola), "-i wlan0" (en la interface Wireless), "-u snort" (con el usuario snort), -g snort (con el grupo snort), "-c /etc/snort/snort.conf (con el fichero de configuración "snort.conf"). A lo que se obtendría una inicialización como se puede ver en la figura 56.

```
root@raspberrypi:~# snort -A console -i wlan0 -u snort -g snort -c /etc/snort/snort.conf
```

Figura 55. Comando para ejecución de Snort. (Autoridad propia)

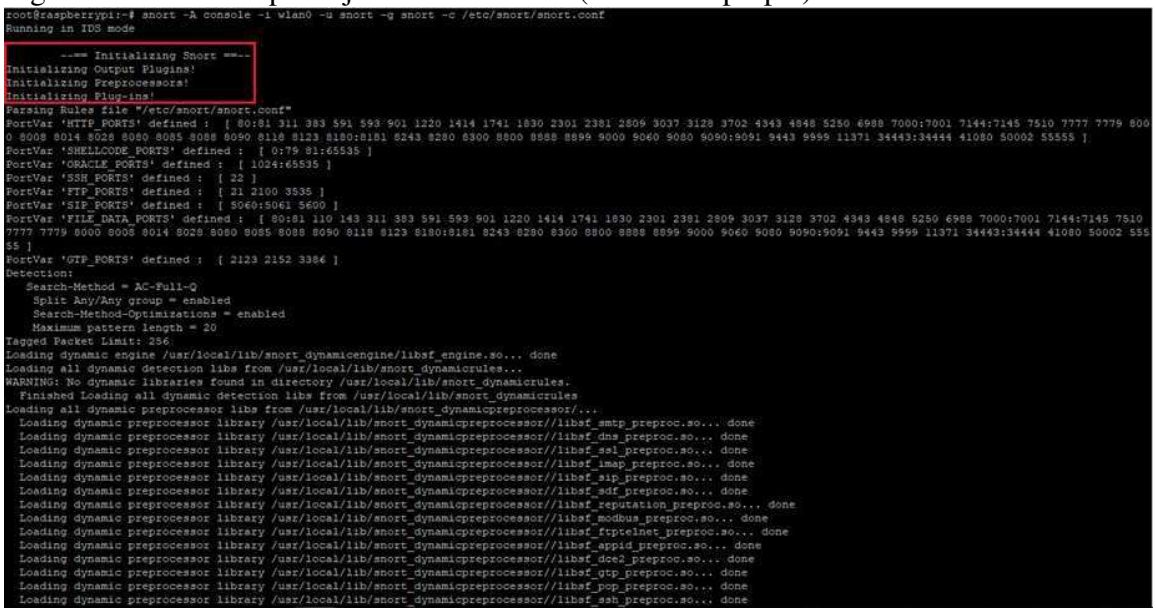


Figura 56. Ejecución del Snort. (Autoridad propia)

Una vez iniciado se podrán ver los reportes de ataques que como en la figura 57 se muestra detalladamente. Donde se encuentra información como el tag del ataque, el protocolo de comunicación, la IP de origen, la IP de destino la fecha con su respectiva hora y su prioridad. El ataque que se encuentra en la figura 57 se está presentando debido al túnel SSH generado por el aplicativo PuTTY con el que se administra la Raspberry de manera remota pues detecta un intento de conexión por TCP/IP. Para salir del análisis se puede presionar "Control + C" y expulsará la ejecución del Snort.

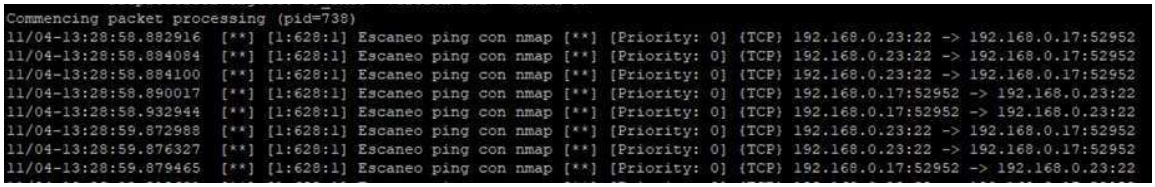


Figura 57. Reporte de ataques en Snort. (Autoridad propia)

Configuración del MikroTik

Fue necesario el enrutamiento y configuración de la red WLAN por medio de los dispositivos MikroTik gracias a las enormes prestaciones que tienen y los conocimientos previos con los que se contaban, según la página oficial de MikroTik.

> "MikroTik es una empresa letona que se fundó en 1996 para desarrollar enrutadores y sistemas ISP inalámbricos. MikroTik ahora proporciona hardware y software para conectividad a Internet en la mayoría de los países del mundo. Nuestra experiencia en el uso de hardware de PC estándar de la industria y sistemas de enrutamiento completos nos permitió en 1997 crear el sistema de software RouterOS que proporciona una amplia estabilidad, controles y flexibilidad para todo tipo de interfaces de datos y enrutamiento. En 2002 decidimos hacer nuestro propio hardware, y nació la marca RouterBOARD. Tenemos revendedores en la mayor parte del mundo y clientes en probablemente todos los países del planeta. Nuestra empresa está ubicada en Riga, la capital de Letonia, y cuenta con más de 280 empleados" (MiroTik, 2019)

Dentro de sus prestaciones y ventajas las cuales favorecían la configuración de una red WLAN a la cual se le pudiese aplicar un IDS dentro de sus interfaces para el correcto análisis del tráfico que es el principal objetivo se encontró la simplicidad en su manipulación y configuración la cual se puede realizar de manera simple en un aplicativo conocido como Winbox proporcionado por MikroTik el cual según Rodrigo Anrrango.

> "Winbox es una pequeña aplicación que nos permite la administración de Mikrotik RouterOS usando una interfaz gráfica. Incluye una sofisticada tecnología para realizar estas conexiones basada en el sistema operativo RouterOS. Este software permite a sus usuarios realizar conexiones vía FTP, telnet y SSH. Incluye también una API que permite crear aplicaciones personalizadas para monitorizar y administrar." (Anrrango, 2014)

Además de eso MikroTik permite de manera simple la adopción de un canal de servicios de internet y segmentación de red puesto que ofrece la configuración mediante Winbox de un

direccionamiento dedicado a la interface que asume los servicios de internet, otro para la Raspberry la cual porta el IDS y otro direccionamiento dedicado a la WLAN a la cual se le debe asignar un DHCP Server para la entrega del pool de IP a los dispositivos autenticados en la red WiFi. El dispositivo MikroTik RB951Ui-2HnD el cual fue asignado como router del proyecto cuenta con las opciones de configuración requeridas como la segmentación de red la cual se realizó con el apartado "Addresses" donde básicamente se asigna la dirección IP que el dispositivo adoptara dentro de la red, la interface a la que se le otorgara dicha red y la dirección IP de red, en la figura 58 se puede apreciar esta configuración donde además de eso se le asigno un tag para el reconocimiento de la interface. Culminada esta configuración el router crea automáticamente el enrutamiento en el apartado de "Routes" como se ve en la figura 59 donde básicamente hace la entrega o asigna la dirección que tendrá la interface y la dirección IP, se puede ver como las interfaces 1, 2 y 3 son entregadas respectivamente a sus IP de red las cuales se configuraron previamente en el apartado "Addresses" no obstante se requiere crear una ruta la cual se puede apreciar resaltada en la figura 59, esta ruta está enviando la puerta de enlace o Gateway de los servicios de internet hacia 0.0.0.0/0 que no es una IP asignable, generalmente es interpretada como "toda la internet" o cualquier dirección IP, se utiliza con más frecuencia como la ruta predeterminada para el host o enrutador, de modo que la puerta de enlace asignada por el ISP apuntara hacia esta ruta predeterminada como se aprecia en la figura 59.

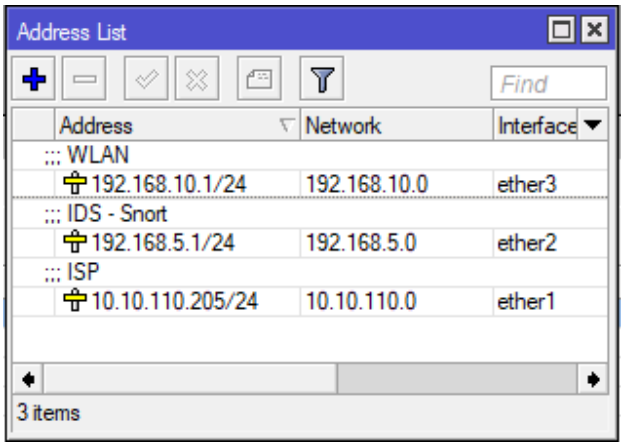


Figura 58. Address List. (Autoridad propia)

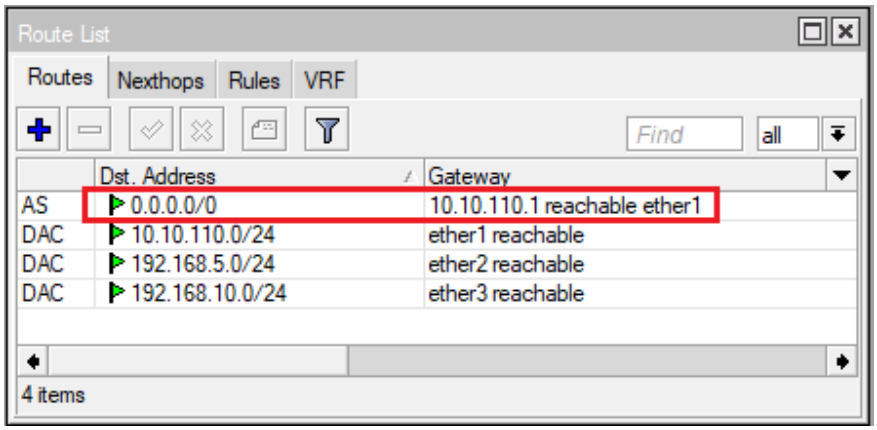


Figura 59. Route List. (Autoridad propia)

En esta posición de la configuración el router MikroTik ya está recibiendo un canal de internet y está segmentando la red para dos interfaces, la del IDS la cual adopto el direccionamiento 192.168.5.0/24 y la de la red WLAN la cual adopto el direccionamiento 192.168.10.0/24 como se puede ver en la figura 58, no obstante la propagación de internet sobre estas sub redes requiere un NAT en la interface 1, la cual fue asignada para el ISP, este NAT según el sitio web de SPEEDCHECK funciona de la siguiente manera.

> "A través de un sistema NAT, estas direcciones privadas se traducen en una dirección IP pública cuando las peticiones salientes de los dispositivos de red se envían a Internet. Un proceso inverso ocurre cuando los datos entrantes, normalmente como respuesta a peticiones específicas, se envían a una red local. En este caso, el NAT cambia la dirección IP pública por la dirección IP privada del dispositivo específico al que se dirige el paquete de datos. La dirección IP pública es utilizada repetidamente por el enrutador que conecta los ordenadores a Internet" (speedcheck, 2019)

Es decir que en vista de que en esta interface está llegando un direccionamiento público el cual entrega el ISP para la salida a la WAN se requiere una traducción de este enmascaramiento de IP Publica a IP Privada y esta configuración se puede realizar de manera simple gracias al MikroTik en el apartado "Firewall" en la casilla "NAT" como se puede ver en la figura 60, donde es importante cambiar los parámetros de (Chain, Out. Interface y Action) que respectivamente están diciendo que todo lo que se origina del ether1 sea enmascarado como se evidencia en la figura 61.

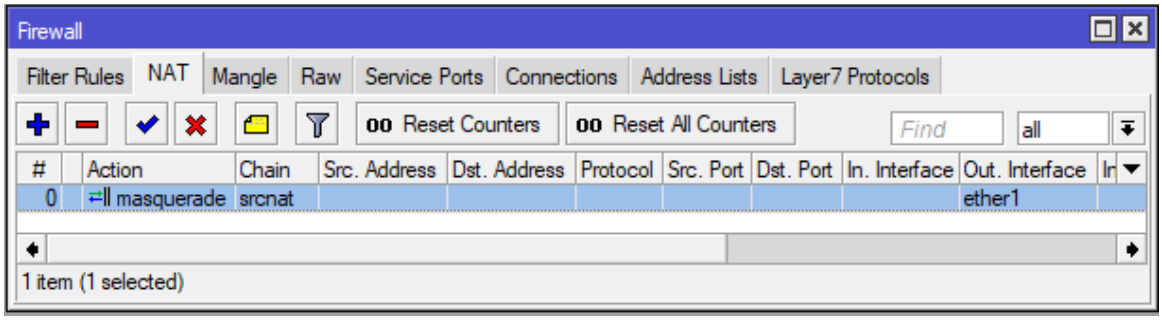


Figura 60. Apartado Firewall – NAT. (Autoridad propia)

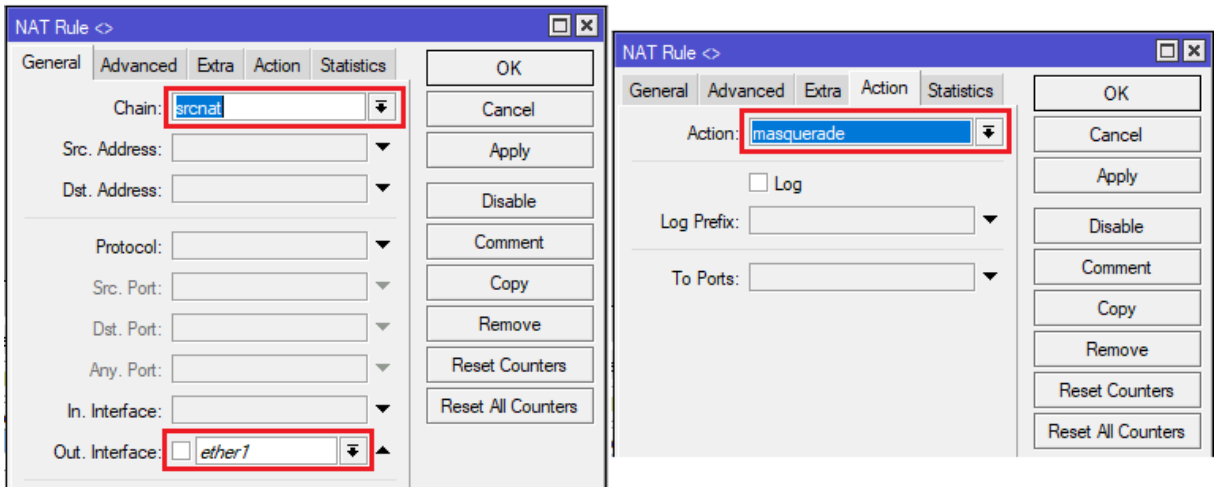


Figura 61. Configuración del NAT. (Autoridad propia)

En este punto el router ya tiene servicios de internet, y está entregando internet en cada una de las subredes creadas, sin embargo, los dispositivos conectados a estas interfaces requerirían de un direccionamiento estático configurado en sus respectivas interfaces de red, ya que el router aún no tiene configurado un servidor DHCP, pero aquí aparece otra de las grandes prestaciones de un router MikroTik, pues permite de manera simple asignar un DHCP Server a la interface que se requiera, para este caso la interface 3 o también conocida como ether 3 ya que esta interface es la que entregara la WLAN y los dispositivos que requieran autenticarse a la red WiFi corporativa necesitaran adoptar una IP de manera dinámica, mientras que la interface 2 o ether 2 estará asignada para la Raspberry o IDS, la cual ya tiene y requiere un direccionamiento estático para su administración. Para la asignación y configuración del DHCP Server se requiere seguir los pasos que se pueden apreciar en la figura 62, estos pasos se pueden trabajar en el apartado "DHCP Server" del MikroTik, al final de dicha configuración se tendrá un DHCP Server asignado a la interface 3 con un pool de IP y una apartado de red donde se podrá ver la IP de la red, la puerta de enlace y los DNS entregados a los host, debería verse como en la figura 63.

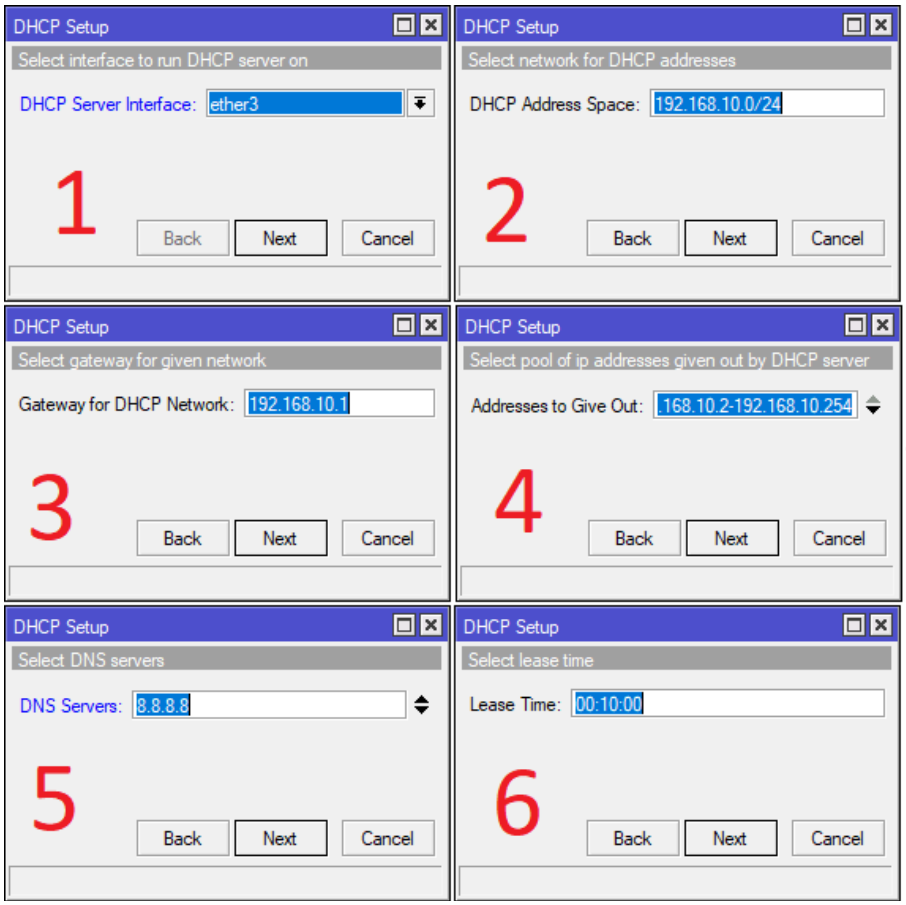


Figura 62. Configuración del DHCP Server. (Autoridad propia)

1. Asignación de interface para el DHCP Server en cuestión
2. Dirección IP de red
3. Puerta de enlace para los hosts autenticados en la WLAN del ether 3
4. Pool de IPs o rango para la asignación de IPs a los hosts.
5. Servidores DNS que resolverán los hosts autenticados en la WLAN del ether 3
6. Tiempo de arrendamiento de IPs

La puerta de enlace funcionara para los hosts como la dirección IP por la cual saldrán a la red y a su vez a internet, mientras que el pool de IPs será el rango de IPs el cual el DHCP podrá entregar a los hosts que están en su red. El DNS Servers es “El proceso de traducción de los nombres de dominio en direcciones numéricas que las máquinas puedan entender es lo que se conoce como resolución de nombres” (Guide, 2019) es decir resolver o traducir las URL a los servidores donde se encuentran alojados los sitios web, para este caso “8.8.8.8” que son los DNS de Google y tienen

un gran campo de cobertura. Por último, el tiempo de arrendamiento que es el tiempo donde el DHCP ser cerciora de sus actuales conexiones e IPs establecidas y operativas.

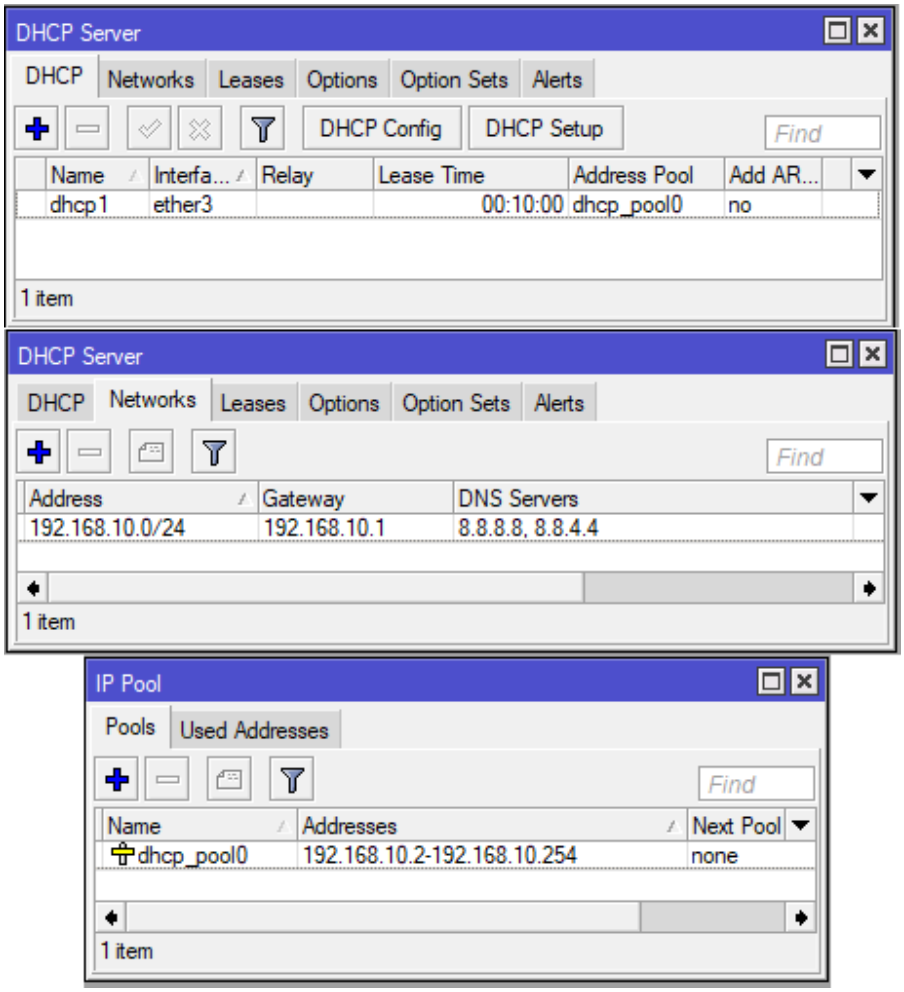


Figura 63. DHCP Server configurado. (Autoridad propia)

Configurada correctamente la salida a internet y la entrega de servicios a cada una de las interfaces lo que procedería seria configurar la WLAN o Wireless, para la cual también se tomó provecho de un dispositivo MikroTik en este caso un RouterBOARD 941-2nD el cual básicamente adoptó el papel de Access Point (AP) pues tiene la gran ventaja de comportarse como Switch, haciendo un bridge o puente en cada una de sus interfaces incluida la interface wlan y es esta la configuración realizada en este MikroTik como se puede apreciar en la figura 64, donde se evidencia la asignación de las interfaces wlan1, ether2 y ether1 al bridge propagando así sobre ellas el mismo tráfico, comportándose como un HUB. La interface 1 es asignada al bridge pues recibirá el DHCP Server propagado por el router desde la interface 3 del mismo, mientras que la interface

2 es simplemente un puerto de validación de servicios ethernet pues la interface que realmente tiene relevancia es la wlan1 que es el núcleo del proyecto, el análisis de una red WiFi.

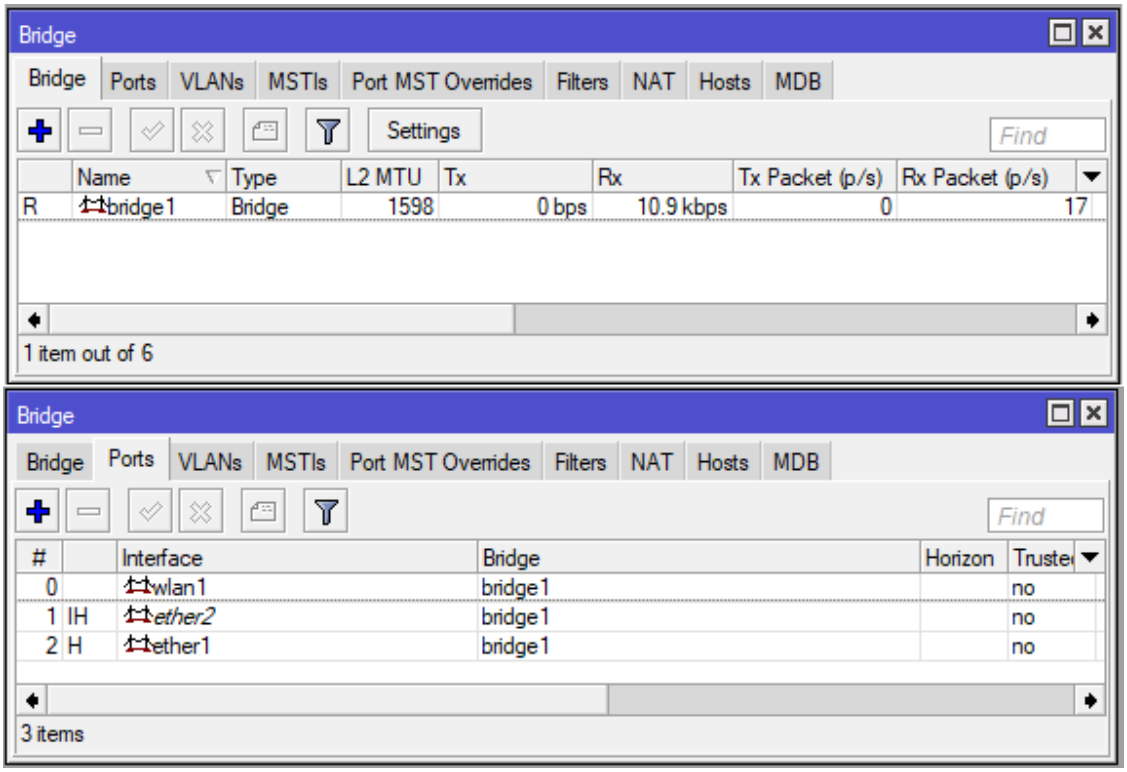


Figura 64. Configuración del bridge. (Autoridad propia)

Una vez configurado el bridge lo siguiente será configurar la red WiFi o la interface wlan1, la cual gracias al aplicativo Winbox en el apartado "Wireless" permite una configuración simple, la interface ya se encuentra creada solo requiere el cambio de las secciones resaltadas en la figura 65, como el "Mode" que es el modo en el que se comportara la interface en este caso como ya se ha mencionado varias veces es simplemente un AP que está dentro de un bridge, además de eso la frecuencia que se dejara automática para que se comporte según los dispositivos autenticados en la red WiFi, luego el SSID que es el nombre de la red WiFi como tal, seguido el protocolo que para este caso es el protocolo 802.11 y según el artículo del noticiero Network World.

> "El estándar 802.11 es una estándar establecido por IEEE para la certificación de productos WiFi este estándar codifica las mejoras que aumentan el rendimiento y el alcance inalámbrico, así como la disponibilidad de nuevas frecuencias. También abordan las nuevas tecnologías que reducen el consumo de energía" (networkworld, 2018)

Y por último se configura el perfil de seguridad el cual se crea en la casilla de “Security Profiles” del apartado “Wireless” en el Winbox como se evidencia en la figura 66, donde se le asignara un nombre al perfil, en este caso “profile 1” y un key o contraseña para cada uno de los tipos de autenticación que respectivamente son WPA PSK y WPA2 PSK y que según el artículo de Acrylic.

> “Una red WiFi WPA-PSK dispone de una contraseña conocida por todos y cada uno de los clientes que se conectan a la red WiFi. Es la configuración de red más utilizada en los routers WiFi que los ISPs facilitan con sus conexiones de ADSL/Cable/Fibra óptica” (Acrylic, 2014)

> “WPA2-PSK. WPA2 es el nuevo estándar de seguridad WiFi que incorpora algunas mejoras para hacerlo más resistente a algunos ataques conocidos. con WPA2 las contraseñas se pueden seguir intercambiando cómo un secreto compartido (PSK) en las redes domésticas” (Acrylic, 2014)

Las demás configuraciones las adopta de manera automática, cabe aclarar que cada una de las opciones seleccionadas son ofrecida por MikroTik y las que son modificadas se cambian con el fin de dar un correcto funcionamiento de la red WiFi para el proyecto en cuestión.

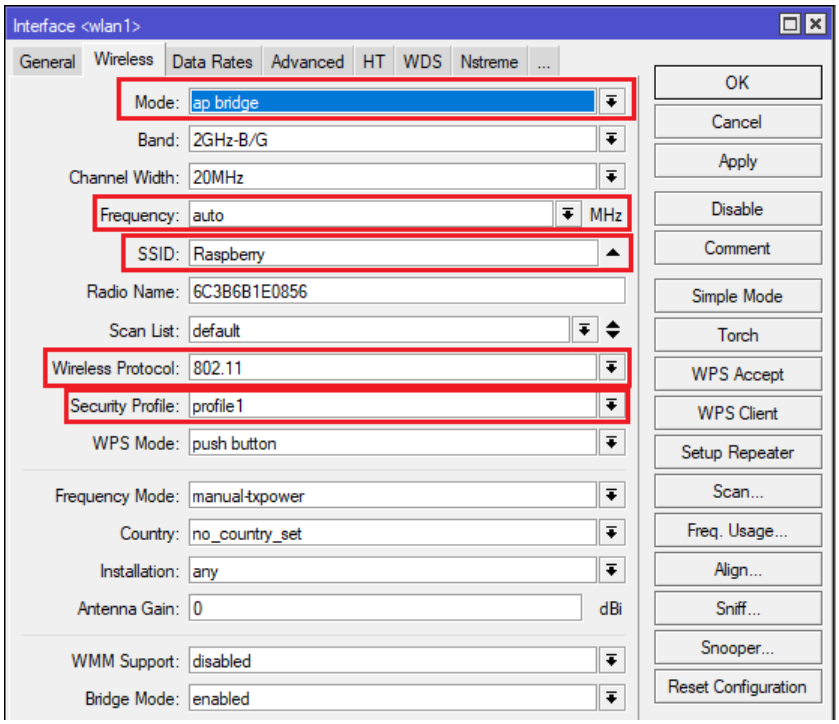


Figura 65- Configuración de red Wi Fi. (Autoridad propia)

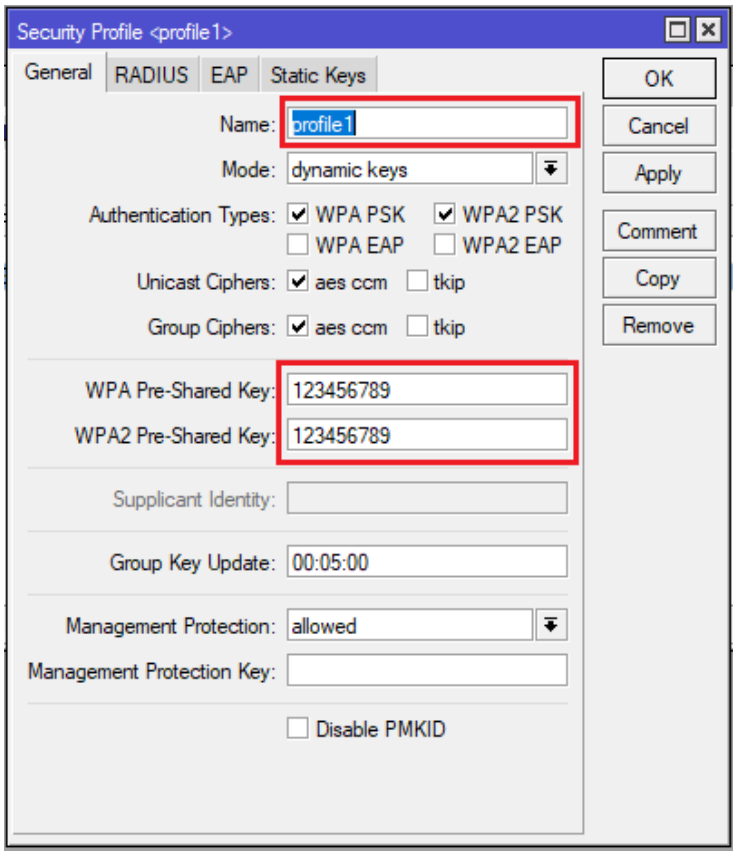


Figura 66. Configuración de Security Profile. (Autoridad propia)

Aquí los dispositivos MikroTik tanto el router como el denominado “AP” ya están entregando una red WLAN con su respectivo DHCP la cual otorga servicios de navegación bajo la autenticación en la red WiFi con el SSID: Raspberry y su respectivo Key: 123456789 la cual se puede ver en la figura 67.

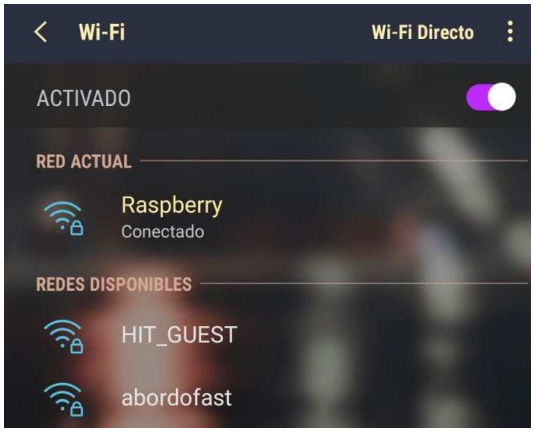


Figura 67. Red Wi Fi. (Autoridad propia)

No obstante, no solo por esto se acudió a MikroTik pues estos router cuentan con un servicio bastante importante para el proyecto, el cual permite el óptimo funcionamiento del IDS y cumbre la gran necesidad del proyecto que es analizar mediante el IDS el tráfico de la red WiFi propagada por el MikroTik denominado "AP". A este servicio se le conoce como "Port Mirroring" o "Puerto Espejo" y según el blog del sitio web Enredado con redes.

> "Port Mirroring o Puerto Espejo es la capacidad de un switch para poder replicar el tráfico que pasa por dos o más puertos y enviarlo por un tercero… con esta funcionalidad lo que conseguimos es que el switch haga una copia de dicho tráfico y lo envíe por un tercer puerto. ¿Con qué finalidad? Por ejemplo, si en este último conectamos un analizador de tráfico, podremos estudiar todo aquello que suceda entre "HMI" y "PLC" y detectar posibles anomalías sin interferir entre el flujo de comunicaciones" (redes, 2017)

Este servicio lo presta el MikroTik RB951Ui-2HnD en el apartado "Switch" del Winbox y su configuración es muy simple, al acceder ya se encuentra creado el puerto espejo como se puede apreciar en la figura 68 al que le es asignado por defecto el nombre "switch1" lo único que requiere es asignar los puertos que adoptaran la función de espejo como se puede ver en la figura 69, donde básicamente esta asignando el "Mirror Source" o el puerto que será replicado o reflejado, para este caso la interface 3, la cual propaga le red WLAN y luego se le asigna el "Mirror Target" o la interface que vera el tráfico, para este caso la interface 2 la cual tiene consigo el IDS el cual tiene como objetivo el análisis de la red WiFi es decir la interface 3.

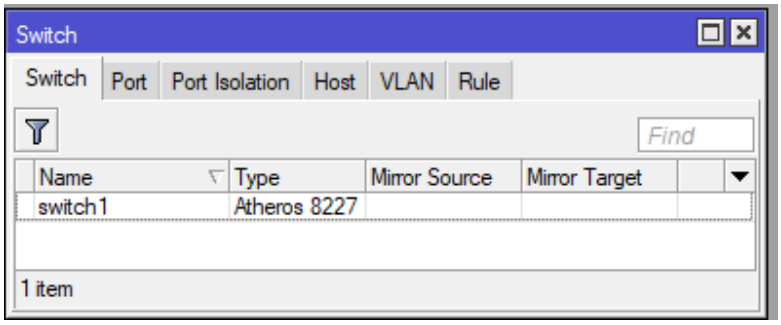


Figura 68. Port Mirroring. (Autoridad propia)

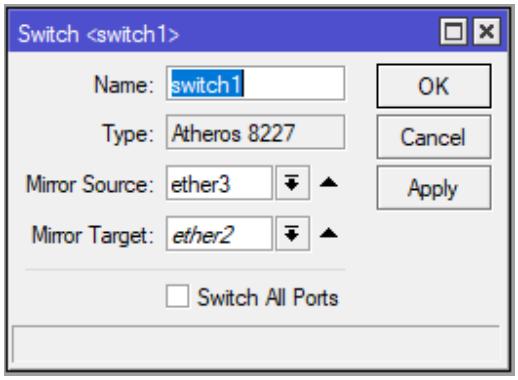


Figura 69. Configuración de Port Mirroring. (Autoridad propia)

La instalación en general y los equipos en cuestión se pueden apreciar en la figura 70, además de eso en la figura 71 se puede apreciar la topología de la red para el proyecto. En las dos figuras se encuentra el Router MikroTik 951Ui-2HnD, el AP MikroTik RouterBOARD 941-2nD, El IDS Raspberry Pi 3 Model b v1.2 y un host que para este caso es una laptop Lenovo V310- 14iSK la cual esta autenticada en la red WiFi.

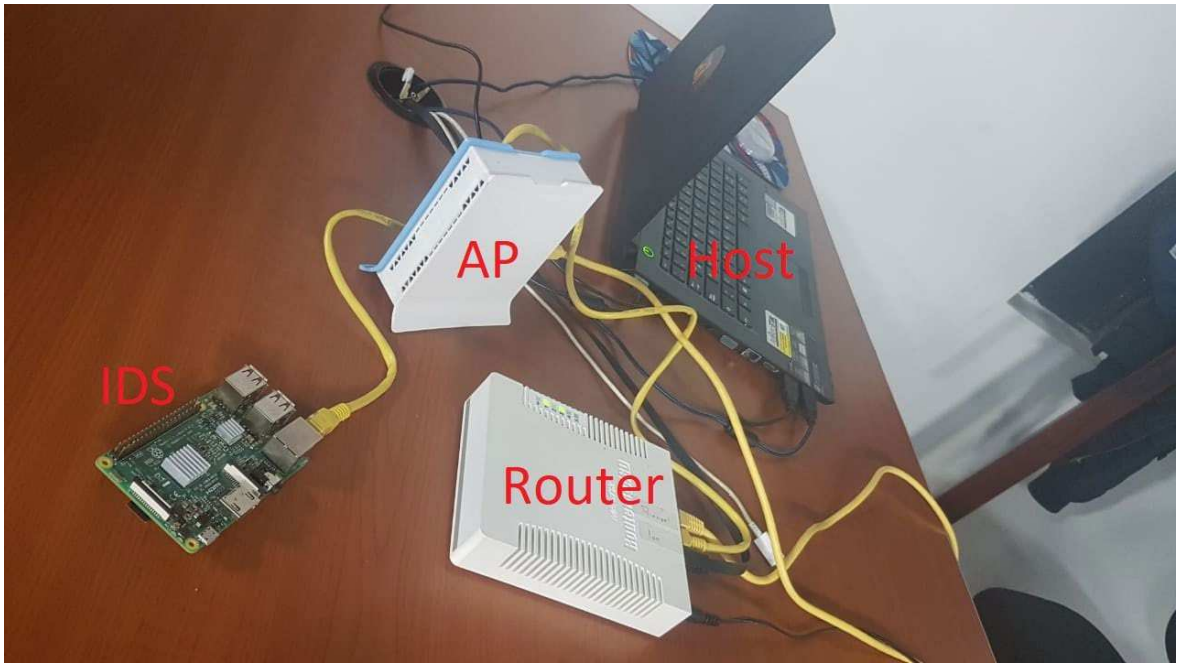
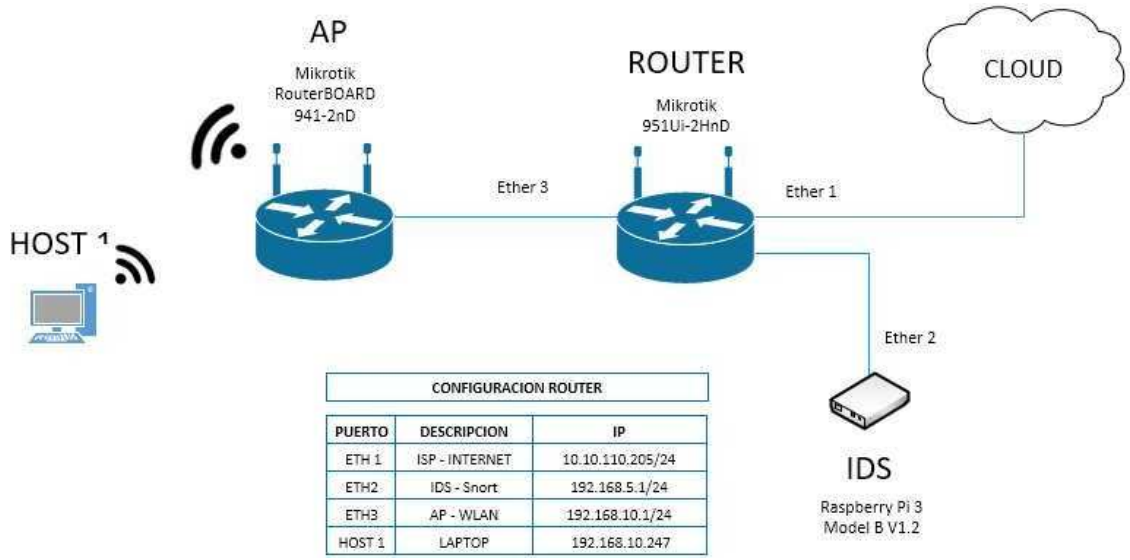


Figura 70. Instalación general. (Autoridad propia)



CONFIGURACION ROUTER		
PUERTO	DESCRIPCION	IP
ETH 1	ISP - INTERNET	10.10.110.205/24
ETH2	IDS - Snort	192.168.5.1/24
ETH3	AP - WLAN	192.168.10.1/24
HOST 1	LAPTOP	192.168.10.247

Figura 71. Topología de Red. (Autoridad propia)

Configuración de reglas al Snort

Para el funcionamiento adecuado del Snort es necesaria la configuración de las reglas que sirvan para realizar acciones contra los diferentes ataques detectados, aunque hay reglas estándar que se pueden descargar para el Snort es mejor crear reglas específicas para el software y así mismo minimizar los falsos positivos que pueden aparecer.

Las reglas personalizadas de Snort se ubican en el directorio previamente configurado y asignado con el nombre “rules” en este está ubicado un fichero el cual adopta el nombre de “local.rules” que es donde se digitan estas reglas personalizadas como se aprecia en la figura 53, para acceder a este fichero se utiliza el comando que se encuentra en la figura 54.

Ya ubicados en el fichero se procede a estructurar las reglas según la necesidad u objetivo que se le tiene al IDS dentro de la red LAN.

Las reglas de Snort se pueden dividir en 2 partes: la cabecera que establece la acción, de la regla, el protocolo IP, máscaras de red, puertos de origen y destino del paquete o dirección de la operación; por otro lado se tiene la sección de opciones que no es más que los mensajes de información necesaria para tomar una decisión en cuanto se detecte el ataque para el cuál fue establecida la regla, la estructura de la cabecera de una regla de Snort se puede evidenciar en la Tabla 1.

Tabla 1.
Estructura de la cabecera de una regla Snort. (Autoridad propia)

Estructura de una regla Snort						
Acción	Protocolo	Red de Origen	Puerto de origen	Dirección	Red Destino	Puerto Destino
alert	tcp	$HOME_NET	any	->	any	22

Nota. En esta tabla se muestra la estructura de la cabecera de una regla Snort.

Cuando se habla de la acción se refiere a indicar la acción que se va a realizar sobre dicha regla y la cual tiene las opciones contempladas en la Tabla 2.

Tabla 2.
Opciones de la acción de una regla Snort. (Autoridad propia)

Acción	Función
alert	Genera una alerta y registra el paquete posteriormente
log	Registra el paquete
pass	Ignora el paquete
activate	Activa la alerta y llaman a una regla dinámica
dynamic	Se pone en funcionamiento cuando se activa una regla anterior
drop	Se utiliza en modo inline y le indica a iptables que elimine el paquete
reject	Se utiliza en modo inline y le indica a iptables que rechace el paquete
sdrop	Se utiliza en modo inline y le indica a iptables que elimine el paquete, pero no lo registre

Nota. En esta tabla se muestran las opciones de las diferentes acciones que se pueden utilizar en una regla Snort.

Por otra parte, se encuentra el protocolo que para el caso de la tabla 1 es el protocolo de transporte TCP, sin embargo, además de este se puede utilizar el protocolo ICMP y UDP que según Franklin Matango en su blog para Server VoIP.

> "TCP es un protocolo de transporte que se transmite sobre IP, descrito en la RFC 793. TCP ayuda controlando que los datos transmitidos se encuentren libre de errores y sean recibidos por las aplicaciones en el mismo orden en que fueron enviados. Si se pierden datos en el camino introduce mecanismos para que estos datos sean reenviados por el emisor.
>
> "UDP Es un protocolo simple, sin conexión descrito en la RFC 768. Se diferencia con TCP en que a este protocolo no comprueba si los datos llegan con errores o no y tampoco si llegan en secuencia. Cuenta con la ventaja de proveer la entrega de datos sin utilizar muchos recursos. Aplicaciones que utilizan UDP" (Matango, 2016)

Mientras que el protocolo ICMP a pesar de no aplicar a los protocolos de transporte de datos es relevante en estas reglas para el control de transmisión y recepción de dato, según el informe de Speedcheck.

> "ICMP una red de protocolo que es responsable de reportar errores a través de la generación y envío de mensajes a la dirección IP de origen cuando hay problemas de red que son encontrados por el sistema.[1] Los mensajes que genera la ICMP indican que no se puede acceder a un determinado gateway, router, servicio o incluso host que deba conectarse a Internet. Básicamente, el destinatario no puede recibir paquetes durante la transmisión. Cualquier dispositivo de red IP puede enviar, generar, recibir y procesar mensajes de error ICMP" (Speedcheck, 2019)

Lo seguido es la red de origen la cual corresponde a la IP desde donde se origina el ataque, para el caso de la tabla 1 hay una variable "$HOME_NET" la cual se asignó en la figura 52, donde básicamente se le entrego el segmento de la red WLAN a dicha variable, en la regla simplemente se trae la variable que en teoría es la IP que se le asigno.

Seguido se encuentra el puerto de origen, en ocasiones los ataques provienen de diferentes protocolos y/o servidores los cuales tienen un puerto asignado, por ejemplo, el puerto por defecto del protocolo FTP es el puerto 21, si se requiriera filtrar por el protocolo FTP solo se le asignaría el puerto 21 a la regla. Para la regla de la tabla 1 se le tiene asignada la palabra "any" la cual hace referencia a todos los puertos, estos puertos también pueden ser asignados bajo una variable preconfigurada, como la variable $FTP_PORTS que cuenta por defecto en el Snort con la configuración de los puertos utilizados comúnmente por FTP.

Después está el apartado de dirección que básicamente direcciona la regla de la IP de origen a la IP de destino o viceversa. Por último, la red y puerto de destino que cumplen la misma función que la IP y puerto de origen solo que estas abarcan el área de protección del IDS, es decir el destino del ataque.

Finalizando con la parte de la cabecera de una regla, en su estructura también hay una sección llamada Opciones, la cual contiene la información necesaria para tomar la decisión sobre qué hacer cuando se detecta dicho ataque. En esta parte hay 4 diferentes tipos los

cuales son metadata, payload, non-payload y post-detection.

Tabla 3.
Opciones de las reglas de Snort. (Gómez, 2020)

Categoría	Opciones
Metadatos	Msg, reference, sid, rev, classtype y priority
Payload	Content, nocase, rawbytes, Depth, Offset, distance, within, uricontent, isdataat, pcre, byte_test, byte_jump, ftpbounce, regex y content-list
Non-payload	Fragoffset, ttl, tos, id, idpopts, fragbits, dsize, flags, Flow, flowbits, seq, ack, Windows, iffype, icode, icmp_id, icmp_seq, rpc, ip_proto y sameip
Post-Detection	Logto, session, resp, react y tag

Nota. En esta tabla se muestran las opciones que tienen las reglas Snort con sus diferentes protocolos.

Tabla 4.
Opciones Metadata. (Gómez, 2020)

Tag	URL Prefix	Ejemplo
Reference		reference:”mi referencia”;
url	http://	reference:url,www3.ca.com/securityadvisor/pest/pest.aspx?id=3648;
Bugtrag	http://www.securityfocus.com/bid	reference:bugtrag,1656;
Cve	http://cve.mitre.org/cgi-bin/cvename.cgi?name=	reference:cve,2000-0869;
Nessus	http://cgi.nessus.org/plugins/dump.php3?id=	reference:Nexus, 11110;
mcafee	http://vi.nai.com/vil/dispVirus.asp?virus_k=	mcafee, reference:10450;

Nota. En esta tabla se muestran las opciones de la regla Metadata.

Tabla 5.
Opciones non-payload. (Gómez, 2020)

Nombre	Descripción
fragoffset	En los paquetes fragmentados indica la posición que ocupa el paquete actual dentro del datagrama original de forma que el destino pueda reconstruirlo. En el primer o un único fragmento el valor es siempre 0.
ttl	Hace referencia al time to live (tiempo de vida) de un paquete IP
tos	Comprueba el valor del campo TOS de la cabecera IP que corresponde al tipo de servicio respecto a la fiabilidad, velocidad, retardo, seguridad, etc.
id	Se utiliza para comprobar el valor del datagrama IP. Este campo es muy útil ya que algunas herramientas (p.e. exploits, ecaneadores) ponen este campo a un valor determinado.
ipopts	Se utiliza para comprobar el campo opción de la cabecera del datagrama IP.
fragbits	Permite comprobar el bit de fragmentación del datagrama IP.
dsize	Se utiliza para comprobar el tamaño del payload.
frag	Se utiliza para comprobar si se encuentra activa alguna opción del frag TCP.

low	Permite indicar la dirección del flujo del tráfico.
flowbits	Se utilizan en conjunción con el procesador flow y se utiliza para seguir los estados de las sesiones del protocolo de transporte.
seq	Se utiliza para identificar el número de secuencia TCP.
ack	Se utiliza para identificar el valor ACK de un paquete TCP.
window	Se utiliza para identificar un determinado tamaño de la ventana TCP.
ltype	Se utiliza para identificar el tipo de mensaje ICMP.
lcode	Se utiliza para identificar el valor del código ICMP.
lcmp_id	Se utiliza para identificar el identificador ICMP.
lcmp_seq	Se utiliza para identificar una determinada secuencia de paquetes ICMP.
rpc	Se utiliza para identificar una determinada aplicación RPC.
lp_proto	Permite identificar el protocolo de la cabecera del mensaje IP.
same_ip	Permite indicar que utiliza la misma dirección de origen y de destino.

Nota. En esta tabla se muestran las diferentes opciones de la regla non-payload.

Tabla 6.
Opciones post-detection. (Gómez, 2020)

Nombre	Descripción
Logto	Permite guardar el paquete en un determinado archivo.
Session	Permite extraer datos de usuario de las sesiones TCP.
Resp	Permite realizar una respuesta activa a un paquete. Por ejemplo, se puede enviar un determinado paquete TCP o ICMP.
React	Permite reaccionar ante un determinado paquete. Por ejemplo, puede bloquear un paquete o generar un aviso.
Tag	Permite registrar un determinado número de paquetes después de que se active una regla

Nota. En esta tabla se muestran las diferentes opciones de la regla post-detection.

Por último, la opción Payload en la cual se encuentra según (Gómez, Administración de Sistemas Operativos, 2020)

> "Content que es la opción que permite especificarle a Snort el string que debe buscar dentro de la parte útil de un paquete (data)…, por otro lado, está pcre que al igual que content permite indicar el contenido que se debe buscar dentro de un paquete. La diferencia entre pcre y content es que pcre busca los datos en una línea y content afecta a todo el paquete."

Teniendo clara la estructura de las reglas personalizadas se crean las reglas evidenciadas en la figura 71 para el proyecto en cuestión, donde además de los parámetros ya explicados previamente se evidencian algunos otros que hace referencia

respectivamente a la identificación de la regla, por ejemplo, el parámetro “msg” hace referencia al tag del reporte del ataque, es decir cuando se genere la alerta enviara el mensaje deseado para identificar el ataque realizado. Además de eso está el parámetro “content” que identifica un contenido especificado como una alerta cuando se evidencie conciencia con este contenido. Por otra parte, está el “sid” que es básicamente una identificación de la regla para el snort, cada regla debe tener una identificación diferente, de lo contrario el snort no podrá ejecutarse, este identificados debe ser igual o superior a 1000001 para reglas locales, pues los números previos están asignados a las reglas descargadas con el Oinkcode. Por último, se tiene el parámetro “rev” que es un parámetro para darle una versión a la regla, este difiere pues en caso de existir una regla con el mismo objetivo se ejecutara por versiones.

```
#------------
# LOCAL RULES
#------------

alert tcp any any -> any any (msg:"Ataque DoS"; \
    flow:established,to_server,no_stream; content:"X-a:"; dsize:<15; \
    detection_filter:track by_dst, count 3, seconds 30; \
    classtype:denial-of-service; sid:1; rev:1; )

#alert tcp any any -> any any (msg:"Ataque FTP fuerza bruta"; \
#       content:"530"; classtype: unsuccessful-user; \
#       threshold: type threshold, track by_dst, count 5, seconds 30; sid:30; rev: 1;)

alert tcp any any -> any 21 (msg:"Potencial Ataque FTP fuerza bruta"; \
        flags:S; threshold: type threshold, track by_src, count 6,seconds 120; \
        flowbits: set, ssh.brute.attempt; classtype:attempted-admin; sid:2001219; rev:8;)

#alert icmp any any -> $HOME_NET any (msg:"Ataque ICMP"; sid:10000001; rev:001;)
#alert tcp any any -> $HOME_NET any (msg:"Escaneo ping con nmap"; sid:10000002; rev:1;)
alert tcp any any -> $HOME_NET any (content:"www.youtube.com";msg:"Acceso a Youtube"; sid:10000007; rev:005;)
alert tcp any any -> $HOME_NET any (content:"www.facebook.com";msg:"Acceso a Facebook"; sid:10000003; rev:002;)
alert tcp $HOME_NET any -> 192.168.10.1 22 (msg:"Conexion SSH desde la LAN hacia el Router"; sid:10000004; rev:003;)
alert tcp $HOME_NET any -> 192.168.10.1 $FTP_PORTS (msg:"Conexion FTP desde la LAN hacia el Router"; sid:10000005; rev:004;)
alert tcp $HOME_NET any -> 192.168.10.2 $FTP_PORTS (msg:"Conexion FTP desde la LAN hacia el IDS"; sid:10000006; rev:006;)
#alert tcp 192.168.10.251 any -> any 80 (msg:"Ataque Dos tcp"; sid:10000010; rev:006;)
#alert icmp 192.168.10.251 any -> any 80 (msg:"Ataque Dos icmp"; sid:10000011; rev:001;)
#alert udp 192.168.10.251 any -> any 80 (msg:"Ataque Dos udp"; sid:10000012; rev:002;)
```

Figura 71. Reglas configuradas para el snort. (Autoridad propia)

Las reglas que requieren especial atención son la de “Ataque DoS” y la de “Potencial Ataque FTP fuerza bruta” pues son el objetivo principal de estudio del proyecto y a su vez de análisis para el IDS Snort en la WLAN, estas reglas respectivamente se pueden apreciar en más detalle en las figuras 72 y 73, es importante resaltar que cada uno de los parámetros, opciones e instrucciones asignas en estas reglas tienen como finalidad filtrar el ataque evitando falsos positivos y cada una de estas se encuentra especificada previamente en la construcción de reglas.

```
alert tcp any any -> any any (msg:"Ataque DoS"; \
    flow:established,to_server,no_stream; content:"X-a:"; dsize:<15; \
    detection_filter:track by_dst, count 3, seconds 30; \
    classtype:denial-of-service; sid:1; rev:1; )
```

Figura 72. Regla detección de ataque DoS. (Autoridad propia)

```
alert tcp any any -> any 21 (msg:"Potencial Ataque FTP fuerza bruta"; \
       flags:S; threshold: type threshold, track by_src, count 6,seconds 120; \
       flowbits: set, ssh.brute.attempt; classtype:attempted-admin; sid:2001219; rev:8;)
```

Figura 73. Regla detección de ataque fuerza bruta a FTP. (Autoridad propia)

Ataques generados con Kali Linux

Dentro de las reglas de Snort configuradas para el análisis mediante el IDS se encuentran reglas de tipo ICMP las cuales reportan él envió de un ping a cualquiera de los hosts autenticados en la WLAN, además de eso también se evidencian reglas para el acceso a URLS especificados, para este caso "www.facebook.com" y "www.youtube.com" con el fin de que en el caso de que alguno de los host autenticados en la WLAN intenten acceder a estos aplicativos generaría una alarma reportando el acceso o intento de acceso a los mismo, también se tienen configuradas reglas de tipo TCP, las cuales generarían una reporte en el caso de que algún host intente generar algún acceso mediante SSH o FTP a los servidores, en este caso el Router o el IDS. No obstante, el fuerte el proyecto se enfoca en dos tipos de ataques especiales conocidos como "Dos" y "Ataque de fuerza bruta a FTP".

Ataques Dos

> "Un ataque de denegación de servicio (DoS) ocurre cuando un atacante bombardea continuamente un AP designado o red con solicitudes falsas. Estos causan que los usuarios legítimos no pueden conectarse a la red e incluso pueden hacer que la red falle. Estos ataques se basan en el abuso de protocolos como la autenticación extensible" (Valle, 2018, pág. 75)

Es decir, es un tipo de ataque que envía repetidas solicitudes de autenticación a un servidor o una página web especificada, con el único fin de saturar dicho servidor o página web, provocando así su indisponibilidad de servicios, son ataques comunes en el mundo de las telecomunicaciones, es por esto por lo cual se le dio gran prioridad a la identificación de estos ataques mediante el IDS. Para generarlos se utilizó el sistema

operativo Kali Linux, el cual cuenta con grandes prestaciones para generar ataques, dentro de los que encontramos ataques de denegación de servicios “DoS”. El objetivo es simple, tener una máquina virtual con el montaje del sistema operativo Kali Linux autenticado a la red Wi-Fi generada por el “AP” MikroTik, del tal forma que esté dentro del segmento de red analizado por el IDS, y de esta forma generar el ataque DoS con el Kali Linux a algún servidor o host de la red LAN o en su defecto a alguna página de preferencia, de esta forma el IDS debería arrojar reportes de ataques informando el tipo de ataque, el tipo de protocolo, la IP de origen y la IP de destino, que para este caso la IP de origen correspondería a la IP adoptada por la interface Wireless de la máquina virtual.

Lo primero que se debe realizar es la descarga del directorio “slowloris.pl” con el comando de la figura 74, el cual cuenta con los ficheros necesarios para generar el ataque DoS que es según Edwing Gabriel Calizaya Ventura en su blog para “blog.calivent”.

> “Slowloris es un script que está diseñado para que desde una PC puede atar fácilmente un servidor web típico o un servidor proxy al bloquear todos sus hilos mientras esperan pacientemente por más datos.
>
> Algunos servidores pueden tener una tolerancia más pequeña para los tiempos de espera que otros, pero el Script Slowloris puede compensar eso personalizando los tiempos de espera. Hay una Función agregada para ayudarlo a comenzar a encontrar el tamaño correcto, tiempos de espera también” (blog.calivent, 2019)

Una vez descargado este directorio se procede a acceder al mismo con el comando de la figura 75, desde donde podremos generar el ataque al servidor o dirección URL que se prefiera, este proceso se realiza con el comando de ejecución de ataques DoS que se aprecia en la figura 76. En este comando básicamente se está dando la instrucción con la palabra “perl” al llamado de lenguaje de programación para el directorio slowloris.pl sobre DNS de Facebook por el puerto 80 es decir el puerto HTTP, con la instrucción “timeout” se asigna el tiempo de enviado del paquete, y finalmente la instrucción “num” hace referencia al número de paquetes que se enviaran.

Figura 74. Descargar directorio “slowloris. pl”. (Autoridad propia)

Figura 75. Cambiar el directorio “slowloris. pl”. (Autoridad propia)

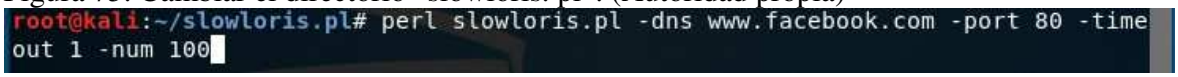


Figura 76. Comando de ejecución de ataque Dos. (Autoridad propia)

Una vez generado el ataque la consola de comandos de Kali empezara a imprimir reportes de autenticación, para cada uno de los “num” especificados en el comando como se puede ver en la figura 77, esto con el fin de provocar una saturación en el servidor o URL en cuestión, para este caso la saturación apunta a la página web “www.facebook.com”.

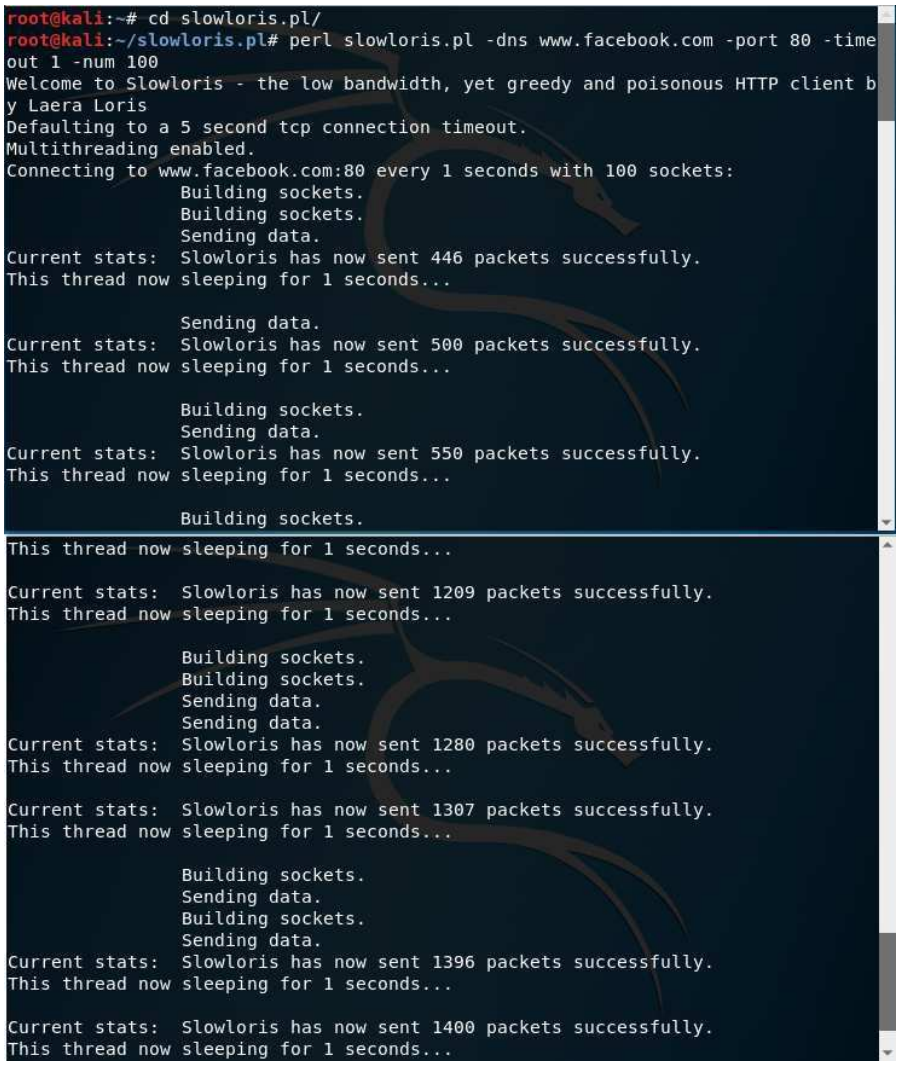


Figura 77. Reportes de ataque Dos. (Autoridad propia)

Ataque de Fuerza bruta a FTP

> "Un ataque de fuerza bruta es un método de prueba y error utilizado para obtener información como contraseñas u otros códigos de acceso. El atacante prueba una variedad de posibles combinaciones de caracteres con la ayuda del software apropiado, con el objetivo de encontrar la secuencia de caracteres deseada para obtener acceso ilegal a datos sensibles, parcialmente encriptados" (Spamina, 2019)

Dicho de otra forma, es el repetido intento de autenticación en un servidor o host validando todas las combinaciones posibles en cuanto a usuario y contraseña con el fin de superar la seguridad proporcionada por un password haciéndole honor a su nombre con un acceso por fuerza bruta. Para este tipo de ataque también se tomará provecho de Kali Linux

el cual cuenta con el programa Hydra incluido en su sistema pues este es indispensable para generar dicho ataque, según Rubén Velasco.

> "Hydra es una de las aplicaciones más conocidas y utilizadas en hacking ético (y por piratas informáticos) para crackear contraseñas y conseguir acceder de forma no autorizada a redes y sistemas. Esta aplicación es totalmente gratuita y de código abierto y cuenta de base con más de 30 protocolos compatibles (sistemas operativos, webs, bases de datos, etc) donde intentar conseguir el acceso no autorizado crackeando y rompiendo contraseñas" (Velasco, 2019)

Hydra permite realizar ataques a diferentes protocolos como lo son FTP, SSH, TELNET o IMAP, para este caso se realizará el ataque mediante el protocolo FTP, por tal motivo se requiere la apertura de este protocolo en el servidor que se quiera atacar. El Router MikroTik es un objetivo claro para este tipo de ataques y aún más teniendo en cuenta que no cuenta con un Firewall configurado provocando así si vulnerabilidad a cualquier tipo de ataque, este router cuenta con el puerto FTP o puerto 21 abierto, y para cerciorarse de ello, se ejecuta el comando de la figura 78 el cual realiza un escaneo de la dirección IP especificada la cual según la figura hace referencia a la IP del router, este escaneo mostrara los puertos abiertos de dicho router donde se evidencia claramente la apertura del puerto FTP.

Figura 78. Escaneo de la dirección IP del Router MikroTik. (Autoridad propia)

Sin embargo, no es todo lo que se requiere para generar este ataque, pues aún se deben generar las posibles combinaciones de usuarios y de contraseña para el acceso mediante fuerza bruta, para ello se requieren dos ficheros que contengan millones de palabras con

las cuales se puedan realizar las posibles combinaciones hasta dar con la acertada, uno para usuarios y otro para contraseñas, estos ficheros se realizarán con el software conocido como "Crunch" el cual ya viene incorporado en Kali Linux. Crunch básicamente toma provecho de letras, números, símbolos y un rango de estos para generar todas las combinaciones de palabras posibles, los parámetros son asignados previamente por el usuario, en el comando de la figura 79 se puede apreciar claramente el uso, donde inicialmente se hace el llamado del software, seguido se le asigna el rango que se cree tiene la contraseña, para este caso es entre 7 y 8 letras en una palabra, luego se le especifica los caracteres que podría tener la contraseña, para este caso los numero comprendidos entre 0 y 9, finalmente se trae la opción "-o" la cual hace alusión a la ruta donde se guardara el fichero generado, como se aprecia en la figura el fichero adoptará el nombre de "Contraseñas" y quedaría guardado en el directorio "Documentos". Por otra parte, en la figura 80 se puede ver la creación del fichero "Usuarios" con Crunch donde se le asigno un rango de 5 a 6 letras por cada palabra con los caracteres comprendidos por cada una de las letras del abecedario.

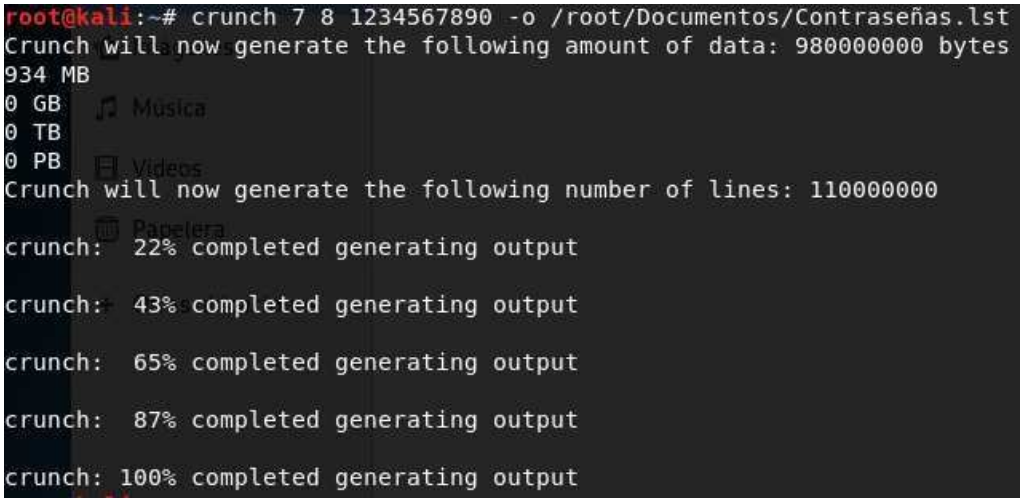


Figura 79. Creación del fichero Contraseñas con Crunch. (Autoridad propia)

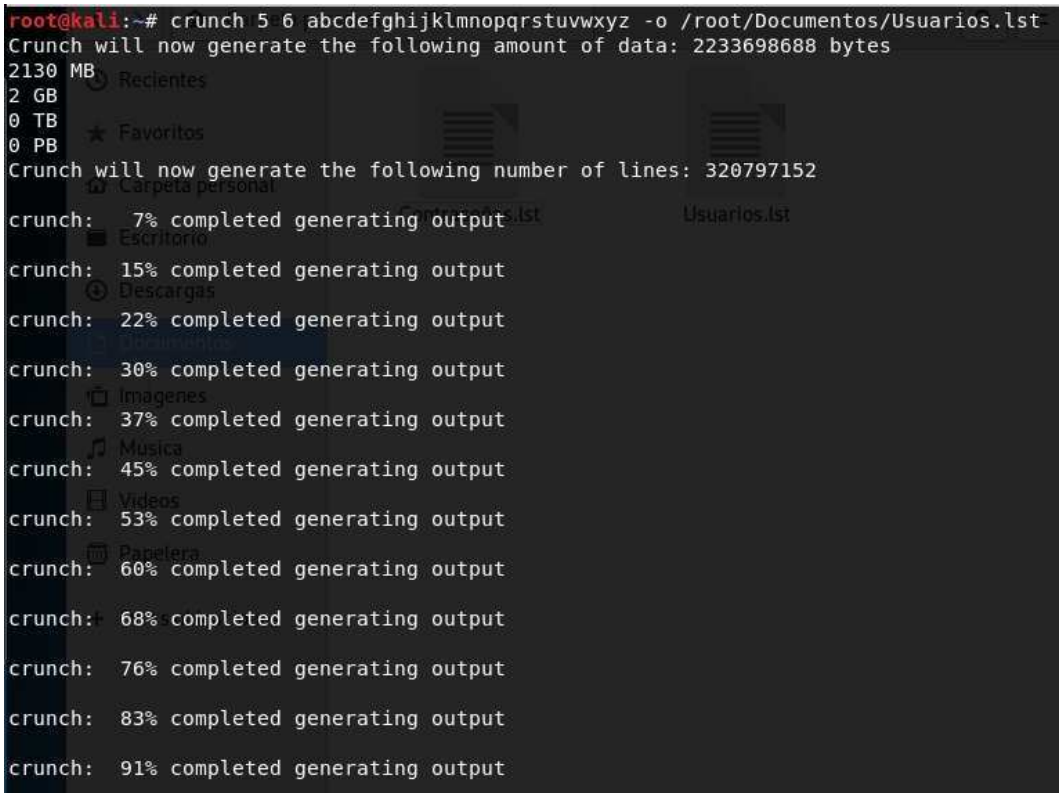


Figura 80. Creación del fichero "Usuarios" con Crunch. (Autoridad propia)

Finalmente creados los ficheros necesarios para el ataque de fuerza bruta y con la certeza del puerto FTP abierto en el objetivo del ataque se procede a realizar el ataque de fuerza bruta a FTP mediante el comando de la figura 81, donde primeramente se hace el llamado de la herramienta Hydra, seguida la instrucción "-L" la cual especifica de un fichero los usuarios posibles, seguido la ruta del fichero asignado para usuarios, luego la opción "-P" que especifica de un fichero las contraseñas posibles, seguido la ruta para el fichero de contraseñas y finalmente la dirección IP del objetivo con el protocolo que se utilizará en el ataque en este caso FTP. Un ataque de fuerza bruta puede tardar bastante dependiendo de la cantidad de combinaciones, ira imprimiendo los intentos realizados y el tiempo aproximado para concluir el ataque, pero una vez haya encontrado la combinación correcta la imprimirá en verde como se aprecia en la figura 81, donde mostrara claramente el usuario y contraseña pertenecientes al host, en este caso el router MikroTik concluyendo así un ataque de fuerza bruta a FTP exitoso.

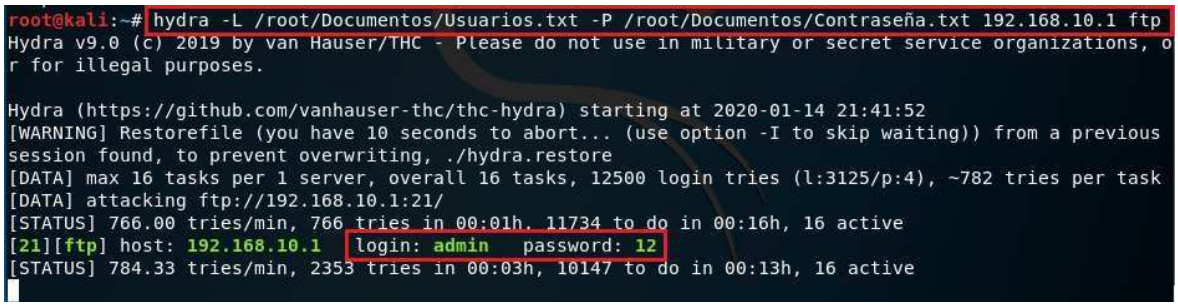


Figura 81. Comando para generar ataque de fuerza bruta a FTP. (Autoridad propia)

Para confirmar, en la misma consola de Linux se puede acceder al router MikroTik con el comando de la figura 82, donde una vez ejecutado intentara realizar un acceso al Router MikroTik mediante FTP solicitando usuario y contraseña de acceso, y como se puede apreciar en la misma figura con los datos proporcionados por Hydra se consigue un acceso exitoso.

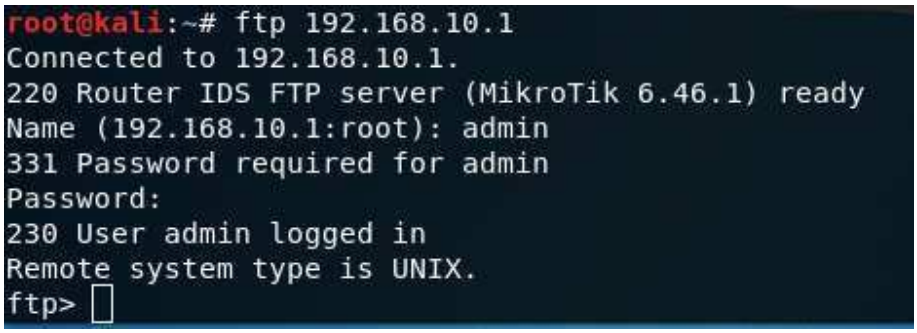


Figura 82. Acceso FTP a Router MikroTik. (Autoridad propia)

Fase de análisis

Configurados los equipos necesarios, autenticados los dispositivos en la red Wi-Fi, asignas las reglas necesarias para el Snort y ejecutados los ataques pertinentes, el IDS Snort empezaría a cumplir su función, identificar los ataques según las necesidades del usuario y las reglas previamente configuradas. En el experimento realizado con ataques DoS se pudo evidenciar en el reporte de Snort una saturación de ataques en la red, pues como ya se mencionó los ataques DoS son repetidos intentos de autenticación o ingreso a un servidor o sitio web al mismo tiempo con el único fin de saturarlo, en este caso Facebook, debido a esto Snort presenta varios reportes. En la figura 83 se puede apreciar como el IDS reporta ataques de denegación de servicios (Ataque DoS) bajo el protocolo TCP, estos ataques son originados desde la dirección IP adoptada por la máquina virtual según dichos reportes, en la figura 84 se pude confirmar la dirección IP del servidor Kali

Linux bajo el comando “ifconfig” la cual concuerda con los reportes de Snort, además de esto se puede ver como el destino del ataque son DNS públicos donde se alojan los servidores de Facebook y en este caso concuerda con el ataque generado por Kali el cual pretende saturar la página web de Facebook, también se puede ver la fecha y hora en la que se generó el ataque con su respectiva identificación de reporte, esta es utilizada para filtrar el reporte en el log de Snort en caso de requerirlo, finalmente se encuentra la clasificación del ataque que para esta ocasión es “Denegación de servicios”.

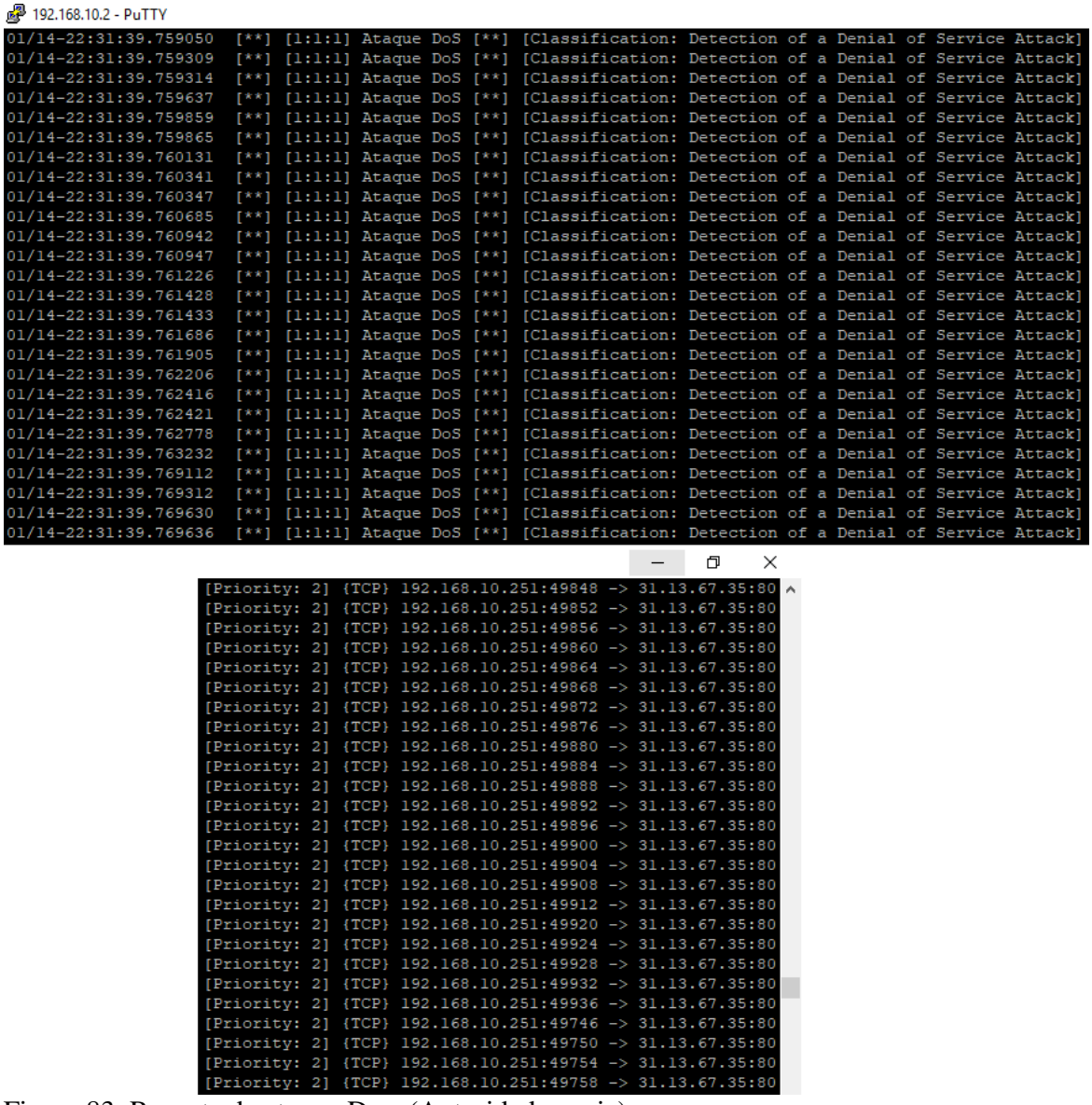


Figura 83. Reporte de ataque Dos. (Autoridad propia)

Figura 84. IP de la máquina virtual. (Autoridad propia)

Por otra parte, para el experimento realizando en el ataque de fuerza bruta a FTP se puede apreciar en la figura 85 al igual que en el ataque DoS varios reportes por parte de Snort, pues el ataque conocido por fuerza bruta también genera repetidos acceso al host o servidor que está siendo atacado a diferencia de que en el ataque de fuerza bruta los genera uno a uno con el fin de validar diferentes combinaciones de usuario y contraseña hasta dar con la correcta y es aquí donde actúa IDS Snort identificando un uso inusual de accesos al servidor con repetidas combinaciones erróneas, provocando el reporte (Potencial Ataque FTP fuerza bruta) en el cual se puede apreciar la IP de origen la cual corresponde a servidor Kali Linux como se puede evidenciar en la figura 84 y la IP de destino, la cual corresponde al router MikroTik como se evidencia en la figura 58, pues es la IP configurada para red WLAN donde se encuentran todos los host autenticados, es decir la puerta de enlace para estos, además de eso se encuentra la clasificación del ataque que para este caso corresponde a “Intento de obtener el privilegio de administrador” por ultimo su fecha, hora e identificación del reporte.

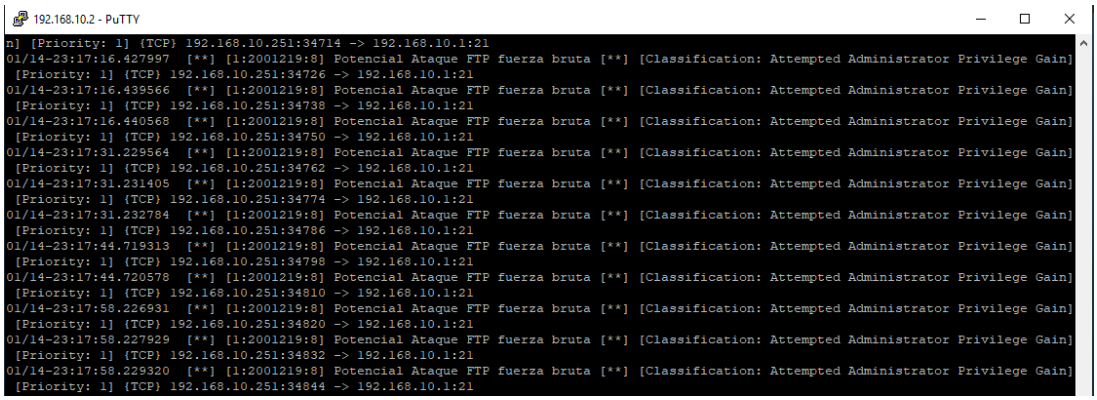


Figura 85. Reporte de ataque fuerza bruta a FTP. (Autoridad propia)

Los ataques DoS y los ataques de fuerza bruta son dos tipos de ataques comunes en el mundo de las telecomunicaciones y el estudio de estos en el IDS Snort es una fuerte validación de sus prestaciones a nivel de una red WLAN, la vulnerabilidad de los servidores y los crackers o hackers a la espera de dichas vulnerabilidades son situaciones que se presentan todos los días en redes corporativas, un IDS para el análisis y prevención de fraudes o perdidas de servicios o información es una pieza clave y el IDS Snort con su reporte detallado al instante de ser generado el ataque, con la información necesaria para identificar el atacante e identificar con exactitud el host que está siendo víctima presta la tranquilidad de una red LAN o para esta caso WLAN segura, el log de Snort permite llevar un estudio detallado de los ataques y respectivos reportes gracias a la identificación que le asigna a cada uno de ellos además de la identificación de fecha y hora del ataque, esto puede favorecer a la implementación de un IPS o Firewall en la red pues al tener un reporte de los posibles ataques a los que esta o ha estado expuesta la red se puede llegar a generar reglas de prohibición por parte del administrador de la red en dicho Firewall o IPS.

Además de esto dentro de las reglas configuradas en el Snort se encuentran reglas para control de tráfico y prevención de acceso a los servidores de la red mediante SSH y FTP estas reglas se pueden apreciar en la figura 71, donde se exponen conexiones al Router MikroTik desde la red LAN y accesos a páginas web como Facebook y YouTube, con esto se puede apreciar que Snort también presta funcionalidades de control de tráfico de la red, donde podemos controlar el acceso a sitios web o servidores desde host que no lo tienen permitido y host que si lo tienen, llevando a una toma de decisiones por parte del administrador de la red para permitir o bloquear dichos accesos, en la figura 86 se encuentran evidencias de acceso a estas páginas web desde un dispositivo móvil con su respectiva dirección IP, también se pueden apreciar dos host también con sus direcciones IP, uno accediendo a las páginas web controladas y también accediendo al Router MikroTik mediante el protocolo FTP y otro host realizando un intento de acceso al Router MikroTik mediante el protocolo SSH, estos accesos a los cuales el IDS Snort le tiene un control generarían un alarma en el momento de ser aplicada su acción, estas alarmas se pueden apreciar en la figura 87, donde en comparación con la figura 86 se encontrarían evidentes las direcciones IP de origen y destino o en su defecto los DNS donde se encuentran alojados los sitios web a los que se les está dando control, YouTube y Facebook.

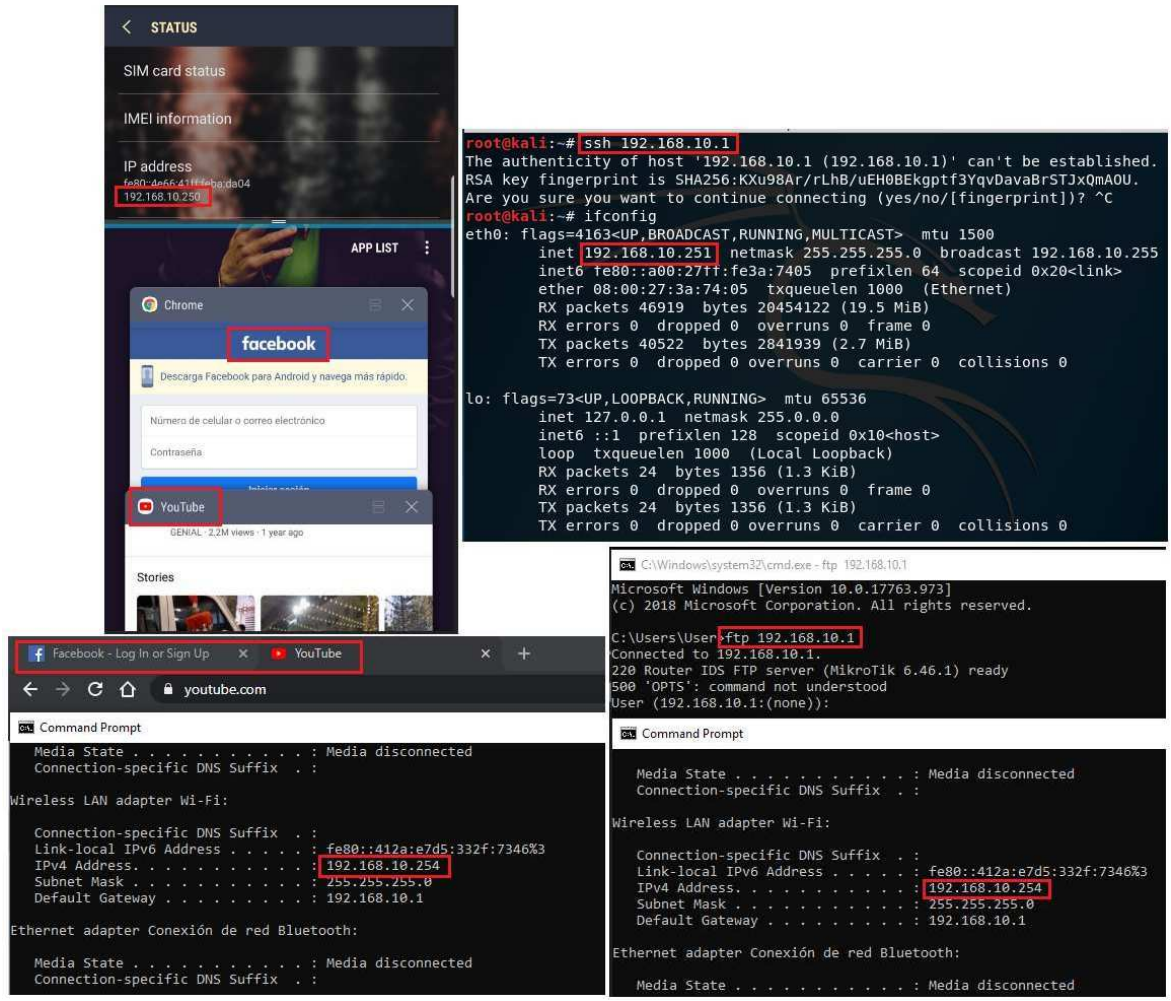


Figura 86. Infracciones de los diferentes hosts. (Autoridad propia)

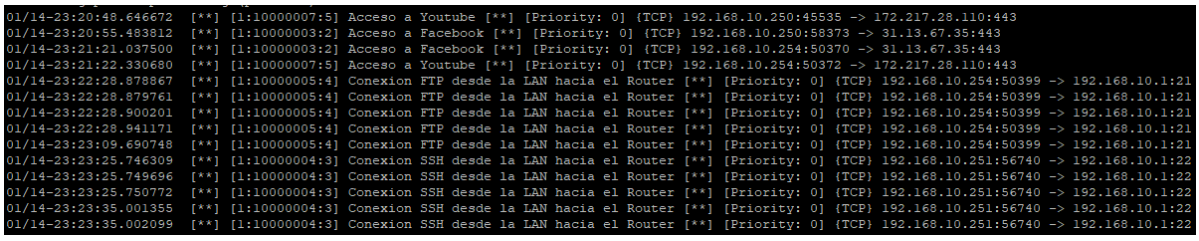


Figura 87. Reporte de Snort. (Autoridad propia)

Conclusiones

En ocasiones las redes corporativas cuentan con DNS privados es decir con aplicativos funcionales únicamente dentro de la red LAN, hay casos en los que las redes corporativas cuentan con servidores para la entrega de aplicativos a cada una de sus tiendas de manera local, con el fin de que estos aplicativos no sean alcanzados fuera de sus Firewall, promoviendo la disponibilidad de estos dependiendo únicamente de su administración, si un atacante cuenta con la posibilidad de acceder a esta red LAN podría generar una indisponibilidad de los aplicativos y así mismo de las sucursales y de manera anónima, provocando un caos para la compañía, es aquí donde el IDS cumple un papel fundamental pues de manera simple informara a los administradores de la red de donde proviene el ataque y que tipo de ataque es, para que con esto se tomen medidas sobre el asunto, y pueda darse seguridad en la red, que a fin de cuentas es el principal objetivo.

Hay corporaciones en las que sus redes no solo cuentan con DNS privados, sino que también los routers que administran cada una de sus sedes son router MikroTik, el proyecto propone implementar un IDS sobre la red LAN de estos mismos dispositivos, lo que permite un óptimo funcionamiento a la hora de analizar el tráfico de la red con solo permitirle una interface en el router al IDS, como se presentó a lo largo del proyecto, entidades que tienen de por medio administración de grandes cantidades de dinero cuentan también con grandes posibilidades de ser atacados. Controlar la seguridad de una entidad tan importante no solo con el firewall del MikroTik sino también con un IDS, que ni siquiera se haría notar en la red sería un avance importante para la seguridad de su de sus servicios, asignando las reglas según las necesidades.

Pero aquí no terminan las grandes prestaciones de un IDS, pues como se pudo evidenciar, si se quisiera llevar un control de acceso a aplicativos en una oficina, aplicativos como lo son las redes sociales el IDS informaría de manera inmediata el acceso a estas y la IP de origen, provocando así un control total de los equipos administrados por un ingeniero, además de eso la seguridad de servidores como los son PBX, aplicativos, bases de datos, routers, entre otros es prioridad para los administradores de una red, poder controlar con un IDS el acceso mediante FTP o SSH que son protocolos comunes de acceso a estos tipos de servidores, monitoreando bajo alarmas generadas por el IDS simplificaría el trabajo ampliamente y aumentaría la seguridad de la red de manera importante.

Además de esto, como ya se mencionó este IDS no solo no se haría notar físicamente sino que tampoco a nivel de RED, pues su consumo a nivel de tráfico en la red ni siquiera se haría notar, el software de Snort esta implementado en un sistema operativo en base debían, diseñado para el máximo aprovechamiento de los recursos de la Raspberry al que decidieron llamar Raspbian, el cual no se aprovechó solo con ser diseñado para el máximo rendimiento sino que también se tomó provecho de la versión lite, la cual al no contar con interface grafica lo recurso de la Raspberry son aún más aprovechados.

Un IDS es una herramienta importante para cualquiera área corporativa y debería ser fundamental al igual que un firewall, las prestaciones que ofrece cumplen y superan las necesidades de seguridad de un área corporativa o de cualquier proyecto de negocio. Aún más en una red WiFi a la cual se le dio especial prioridad con el proyecto, pues la contraseña de una red WiFi no se suele manejar con la discreción y seguridad que se requiere, se comparte el acceso a internet como si fuera una taza de café y no se sabe con certeza las verdaderas intereses del acceso, pues al formar parte de la red WLAN se abre un mundo de posibilidades dentro de la misma.

Por último, la gran posibilidad de generar reglas personalizadas conforme a lo que se requiere identificar como un ataque es una gran prestación del IDS Snort pues en ocasiones se requiere filtrar ciertos tipos de ataques o de alertas para la red, o también re requiere filtrar ciertos dispositivos ya sea a nivel de destino o a niel de origen, con esto se puede identificar los ataque que deseen sobre los equipos que se deseen y con el reporte como se desee, todo esto como se pudo apreciar a lo largo del proyecto, generando las reglas conforme a la necesidad y generando los reportes que se preferían, con cada una de sus respectivas pruebas realizadas y con resultados satisfactorios.

Referencias

Acrylic. (2014, Diciembre 14). *Acrylic*. Retrieved from Acrylic: https://www.acrylicwifi.com/blog/que-es-wpa-psk-tkip-ccmp/

AibiTech. (2019, 11 21). *AibiTech*. Retrieved from AibiTech: https://www.aibitech.com/router-routerboard-mikrotik-rb951ui-2hnd-wireless-1000mw-24ghz-80211bgn-5-ethernet-1usb-l4-mikrotik-3481.html

Andrés, R. (2016, 04 03). *ComputerHoy*. Retrieved from ComputerHoy: https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671

Anrrango, R. (2014, Septiembre 30). *configurarmikrotikwireless*. Retrieved from configurarmikrotikwireless: https://configurarmikrotikwireless.com/blog/conceptos-winbox-configurar-mikrotik.html

atareao. (2017, Agosto 28). *El atareao*. Retrieved from El atareao: https://www.atareao.es/software/programacion/nano-un-editor-de-texto-para-la-terminal/

Australian Cyber Security Centre. (2015). *2015 cyber security survey: Major Australian businesses.* Retrieved from https://www.acsc.gov.au/publications/ACSC_CERT_Cyber_Security_Survey_2015.pdf

balenaEtcher. (2019). *balenaEtcher*. Retrieved from balenaEtcher: https://www.balena.io/etcher/

blog.calivent. (2019, Febrero 15). *blog.calivent*. Retrieved from blog.calivent: http://blog.calivent.com.pe/ataque-dos-slowloris-desde-linux/

C., D. (2019, Octubre 17). *Tutorial H Hostinger*. Retrieved from Tutorial H Hostinger: https://www.hostinger.co/tutoriales/que-es-ssh

Ciberaula. (2019). *Ciberaula*. Retrieved from Ciberaula: https://linux.ciberaula.com/articulo/Curso_comandos_en_Linux_III

Editorial, E. (2019, Mayo 3). *Reporte digital*. Retrieved from Reporte digital: https://reportedigital.com/iot/snort/

Gan J et al. (2015) Design and implementation of network attacks detection module, Tercera Conferencia Internacional sobre Tecnología del Ciberespacio

Gil, J. C. (2013, Mayo 3). *Linux Hispano*. Retrieved from Linux Hispano: http://www.linuxhispano.net/2013/05/03/diferencia-entre-apt-get-update-y-apt-get-upgrade/

Gómez, J. (2020, Enero 15). *Administración de Sistemas Operativos*. Retrieved from http://www.adminso.es/index.php/Snort-PAYLOAD

Gomez, J. (2020, Enero 15). *Administración de Sistemas Operativos*. Retrieved from http://www.adminso.es/index.php/Snort-OPCIONES_DE_UNA_REGLA

Gómez, J. (2020, Enero 15). *Administración de Sistemas Operativos*. Retrieved from http://www.adminso.es/index.php/Snort-METADATA

Gonzáles, C. (2019, Junio 6). *Adslzone*. Retrieved from Adslzone: https://www.adslzone.net/como-se-hace/wifi/activar-dhcp/

Guide, D. (2019, Julio 30). *Digital Guide*. Retrieved from Digital Guide: https://www.ionos.es/digitalguide/servidores/know-how/que-es-el-servidor-dns-y-como-funciona/

Ibrahim Ghafir, K. G.-N. (2018). A Basic Probability Assignment Methodology for Unsupervised Wireless Intrusion Detection. *IEEE Access (volume 6)*, 40008-40023.

it Reseller. (2016, Julio 14). *Uso de las redes públicas en vacaciones facilitan los ciberataques*. Retrieved from it Reseller: https://www.itreseller.es/seguridad/2016/07/el-uso-de-las-redes-wifi-publicas-en-vacaciones-facilita-los-ciberataques

kaspersky. (2019). *kaspersky*. Retrieved from kaspersky: https://latam.kaspersky.com/resource-center/threats/ddos-attacks

Linux, K. (2019, 11 18). *Kali Docs*. Retrieved from Kali Docs: https://docs.kali.org/introduction/what-is-kali-linux

Live Stats. (2019, 04 01). *Internet Live Stats*. Retrieved from http://www.internetlivestats.com/

Llamas, L. (2018, Mayo 16). *Configurar wifi en raspberry pi por gui o terminal*. Retrieved from Configurar wifi en raspberry pi por gui o terminal: https://www.luisllamas.es/raspberry-pi-wifi/

Macas M et al. (2017) Data Mining model in the discovery of trends and patterns of intruder attacks on the data network as a public-sector innovation. Cuarta Conferencia Internacional sobre eDemocracia y Administración Electrónica

Matango, F. (2016, Agosto 18). *Server VoIP*. Retrieved from Server VoIP: http://www.servervoip.com/blog/tag/protocolos-de-transporte/

MikroTik. (2019). *MikroTik*. Retrieved from MikroTik: https://mikrotik.com/product/RB941-2nD-TC

MikroTik. (2019). *MirkoTik*. Retrieved from MirkoTik: https://mikrotik.com/product/RB951Ui-2HnD

MiKroTik. (2019). *MikroTik*. Retrieved from MiKroTik: https://mikrotik.com/aboutus

networkworld. (2018, Febreo 30). *networkworld*. Retrieved from networkworld: https://www.networkworld.es/wifi/80211-estandares-de-wifi-y-velocidades

Oracle. (2019, 11 19). *VirtualBox*. Retrieved from VirtualBox: https://www.virtualbox.org/

peppe8o. (2019, Septiembre 17). *peppe8o*. Retrieved from peppe8o: https://peppe8o.com/2019/09/raspbian-lite-vs-desktop/

PI, R. (2013, Diciembre 18). *Blog Historia de la Informatica*. Retrieved from Blog Historia de la Informatica: https://histinf.blogs.upv.es/2013/12/18/raspberry-pi/

PricewaterhouseCoopers. (2015, 07). *Pricewaterhouse.* Retrieved from https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf

Ramesh. (2019). *Linux 101 Hacks*. Retrieved from Linux 101 Hacks: https://linux.101hacks.com/unix/ldconfig/

Raspberrypi. (2019). *Raspbian*. Retrieved from Raspbian: https://www.raspberrypi.org/documentation/raspbian/

redes, E. c. (2017, Septiembre 04). *Enredando con redes*. Retrieved from Enredando con redes: https://enredandoconredes.com/2017/09/04/puerto-espejo-un-aliado-a-veces-olvidado/

Reina, J. (2019). *Intrusion Detection Systems IDS.* Bogotá: Universidad Pontificia Bolivariana.

Ruostemma, J. (2019). *UpCloud*. Retrieved from UpCloud: https://upcloud.com/community/tutorials/installing-snort-on-debian/

Sampieri, R. H. (2014). *Metodología de la investigación.* Mexico: Mc Graw Hill Education.

Sincables. (2019, 11 21). *Sincables*. Retrieved from Sincables: https://sincables.com.ec/product/rb941-2nd-tc-hap-lite-2-4ghz/

Snort. (2019). *Snort*. Retrieved from Snort: https://www.snort.org/faq/what-is-snort

Snort. (2019). Snort. Retrieved from Snort: https://www.snort.org/faq/readme-reputation

Snort. (2019). Snort. Retrieved from Snort: https://www.snort.org/faq/readme-unified2

Snort. (2019). Snort. Retrieved from Snort: https://www.snort.org/oinkcodes

Softpedia. (20 de Marzo de 2018). Win32 Disk Imager. Obtenido de Softpedia: https://www.softpedia.com/get/CD-DVD-Tools/Data-CD-DVD-Burning/Win32-Disk-Imager.shtml

Spamina. (2019). *Spamina part of hornetsecurity group*. Retrieved from Spamina part of hornetsecurity group: https://spamina.com/knowledge- base/brute-force-attacks

speedcheck. (2019). *speedcheck*. Retrieved from speedcheck: https://www.speedcheck.org/es/wiki/nat/

Speedcheck. (2019). *Speedcheck*. Retrieved from Speedcheck: https://www.speedcheck.org/es/wiki/icmp/

Symantec. (2019). *Informe sobre las amenazas para la seguridad en internet 2019*. Retrieved from Symantec: https://www.symantec.com/es/es/security-center/threat-report

Symantec. (2019). *Los riesgos del wifi público*. Retrieved from Symantec: https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html?otm_medium=onespot&otm_source=onsite&otm_content=category-landing:top-of-feed-unit&otm_click_id=98f56acd-270e-4605-b1c9-5d84080b481e

Tao Y et al. (2011) Research on the simulation model of network attacks, Conferencia Internacional sobre Informática y Sistema de Servicios.

Tapan P et al. (2013) Intrusion detection system on MAC layer for attack prevention in MANET, Cuarta Conferencia Internacional sobre Computación, Comunicaciones y Tecnologías de Redes (ICCCNT)

Valle, F. (2018). Estudio de usos y riesgos asociados a las redes abiertas bajo el protocolo IEEE 802.11 en la ciudad de Bogotá. In E. Serna, *Desarrollo e innovación en ingeniería 3ra edición* (p. 73). Medellín: IAI.

Valle, F. (2018). Estudio de usos y riesgos asociados a las redes abiertas bajo el protocolo IEEE 802.11 en la ciudad de Bogotá. In E. Serna, *Desarrollo e Innovación en Ingeniería 3ra Edición* (p. 75). Medellín: IAI.

Valle, F. (2018). Estudio de usos y riesgos asociados a las redes abiertas bajo el protocolo IEEE 802.11 en la ciudad de Bogotá. In E. Serna, *Desarrollo e innovación en Ingeniería 3ra edición* (p. 75). Medellín: IAI.

Velasco, R. (2019, Junio 8). *RZ Redes Zone*. Retrieved from RZ Redes Zone: https://www.redeszone.net/2019/06/08/hydra-9-0-herramienta-romper-contrasenas/

Xiaojin Hong, C. H. (2012). VisSRA: Visualizing Snort Rules and Alerts. *2012 Fourth International Conference on Computational Intelligence and Communication Networks.* Mathura.

ZEOKAT. (2014, Mazro 28). *VoziDEA*. Retrieved from VoziDEA: https://www.vozidea.com/que-es-putty-y-para-que-sirve

Anexos

Programas Utilizados

Win32 Disk Imager.

A lo largo de la configuración del IDS e implementación de este en la microSD por seguridad se requería realizar un backup de dicha microSD pues cualquier error o configuración mal realizada podría provocar una pérdida total del proceso realizado, en vista de que dicho backup debía quedar en formato iso para obtener este backup se requirió el uso de la herramienta Win32 Disk Imager que según el sitio web de (Softpedia, 2018).

> "Win32 Disk Imager es una aplicación compacta que le permite crear un archivo de imagen desde un dispositivo de almacenamiento extraíble, como una unidad USB o una tarjeta de memoria SD. Se puede utilizar para hacer una copia de seguridad de la información almacenada en el dispositivo para restaurarla más tarde"

Es decir, con este aplicativo se puede generar un archivo iso del estado actual de la microSD, con el fin de que en caso de requerirlo se pueda regresar a el estado guardado por Win32 Disk Imager, el aplicativo tiene un apartado grafico como el que se aprecia en la figura 88.

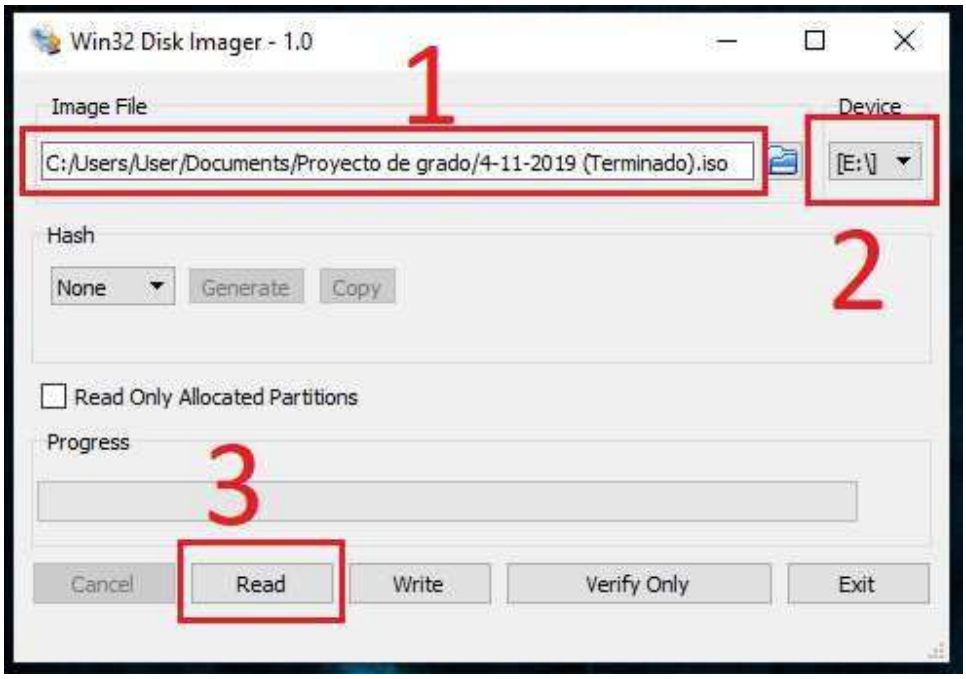


Figura 88. Interface grafica de Win32 Disk Imager. (Autoridad propia)

Respectivamente cada una de las secciones corresponden a:

1. Ruta de ubicación donde se desea almacenar él backup y nombre para el archivo iso.
2. La unidad asignada por el sistema operativo para la microSD de donde se requiere obtener un backup
3. Aparatado para ejecutar el proceso de respaldo de la información.

En caso de necesitar restaurar el backup "iso" se tomaría provecho del aplicativo balenaEtcher ejecutando el mismo proceso que se realizó para la escritura de Raspbian, esta tarea se puede ejecutar sobre la microSD si necesidad de formatearla gracias a las prestaciones de sobre escritura de balenaEtcher.

Obtener Oinkcode.

Los Oinkcode según la página oficial de Snort "son claves únicas asociadas a su cuenta de usuario. El oinkcode actúa como una clave de API para descargar paquetes de reglas con las URL que se enumeran a continuación" (Snort, Snort, 2019)

Para obtener los Oinkcode asignado por Snort para los usuarios registrados lo que se requiere es inicialmente el registro en la página oficial de Snort, es un paso simple donde solo se requiere de un correo electrónico y una contraseña como se puede evidenciar en la figura 89. Una vez registrados se accede al usuario pulsando sobre el correo electrónico correo como se aprecia en la figura 90.

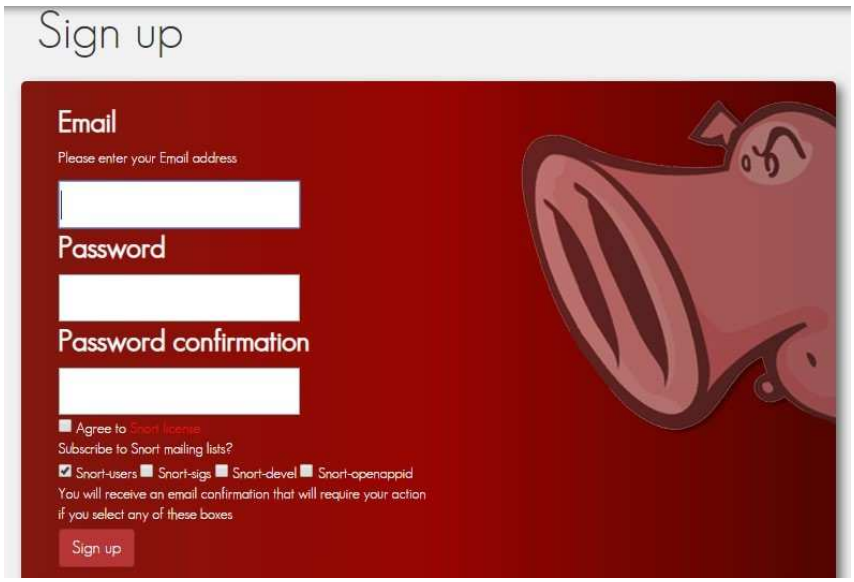


Figura 89. Registro de Snort. (Autoridad propia)

Figura 90. Acceso al usuario de registro Snort. (Autoridad propia)

Ubicados en el usuario se accede al apartado “Oinkcode” donde desplegaría un código el cual en la figura X está señalado de color rojo y es el que se utilizara para la descarga de las reglas de Snort en el raspbian bajo el comando de la figura 91.

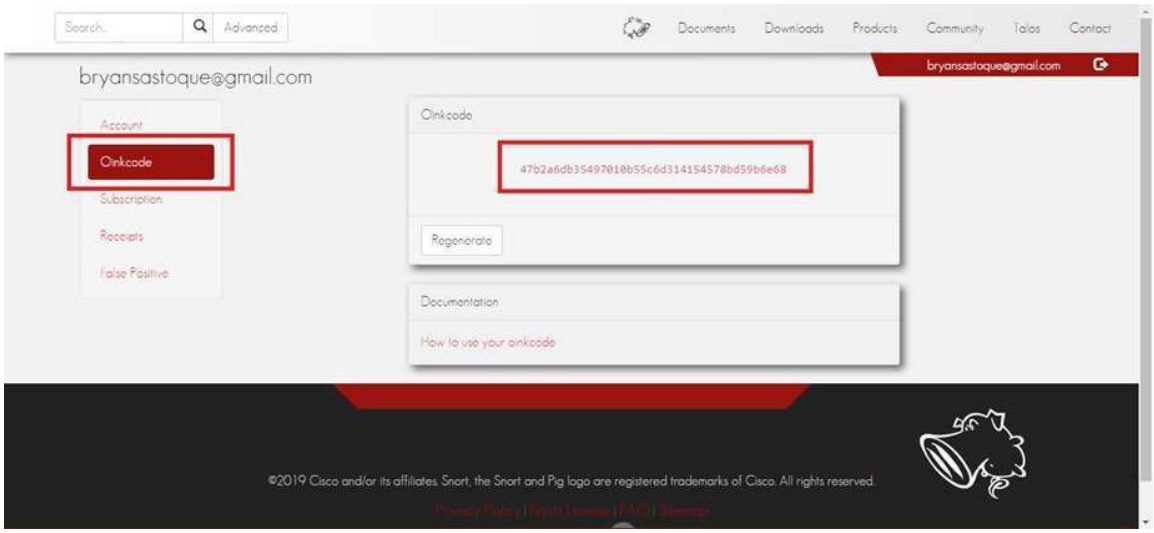


Figura 91. Oinkcode (Autoridad propia)

Dispositivos MikroTik Utilizados.

Dentro de los dispositivos utilizados encontramos inicialmente El MikroTik RouterBOARD 951Ui-2HnD que se puede apreciar en la figura 92 y que es según el sitio web oficial de MikroTik.

“El RB951Ui-2HnD es un SOHO AP inalámbrico con una nueva generación de CPU Atheros y

más potencia de procesamiento. Tiene cinco puertos Ethernet, un puerto USB 2.0 y un AP inalámbrico de alta potencia de 2.4GHz 802.11b / g / n con antenas incorporadas" (MirkoTik, 2019)

"Tiene una CPU de 600MHz, 128MB de RAM y función de salida PoE para el puerto # 5 - puede alimentar otros dispositivos con capacidad PoE con el mismo voltaje que el aplicado a la unidad. La carga máxima en el puerto es de 500 mA" (MirkoTik, 2019)

Figura 92. MikroTik RouterBOARD 951Ui- 2HnD. (Aibi Tech, 2019)

Adicionalmente se utilizó el MikroTik RouterBOARD 941-2nD, el fua fue denominado "AP", este se puede apreciar en la figura 93. Este MikroTik es según el sitio Web de MikroTik.

"Home Access Point lite (hAP lite) es un pequeño dispositivo ideal para su apartamento, casa u oficina.

Admite WPS activado por botón, para la conveniencia de no escribir una contraseña complicada cuando alguien quiere tener acceso inalámbrico a Internet, y también se le puede pedir que cambie al modo cAP y se una a una red administrada centralmente CAPsMAN con solo presionar un botón.

Por supuesto, el dispositivo ejecuta RouterOS con todas las características, configuración de ancho de banda, firewall, control de acceso de usuario y muchos otros.

El hAP lite está equipado con una potente CPU de 650 MHz, 32 MB de RAM, conexión inalámbrica integrada de 2,4 GHz de doble cadena, cuatro puertos Fast Ethernet y una licencia RouterOS L4. Se incluye fuente de alimentación USB" (MikroTik, 2019)

Figura 93. MikroTik RouterBOARD 941- 2nD (Sincables, 2019)

Instalación de Kali Linux

Se escoge el sistema operativo Kali Linux debido a las características y herramientas que posee y es que según su página oficial:

"Kali Linux es una distribución de Linux basada en Debian destinada a pruebas avanzadas de penetración y auditoría de seguridad. Kali contiene varios cientos de herramientas que están orientadas a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa." (Linux, 2019)

Debido a lo anterior y a las ventajas que posee, como cuenta un blog de tecnología:

> “Efectivamente, Kali Linux es la herramienta perfecta para hackers, que buscan (y encuentran) los límites y fisuras en la seguridad de las redes y sistemas informáticos. Pero eso no tiene por qué estar orientado a cometer actos ilegales, ya que ser hacker no está vinculado a la ciberdelincuencia, aunque algunos puedan dedicarse a utilizar sus conocimientos para cometer delitos.” (Andrés, 2016)

La instalación del sistema operativo Kali Linux se hará por medio de una máquina virtual y se ha escogido Oracle VM VirtualBox ya que según su página oficial:

> “VirtualBox es un potente producto de virtualización x86 y AMD64 / Intel64 para uso empresarial y doméstico. VirtualBox no solo es un producto extremadamente rico en funciones y de alto rendimiento para clientes empresariales, sino que también es la única solución profesional que está disponible gratuitamente como software de código abierto bajo los términos de la versión 2 de la Licencia Pública General (GPL) de GNU.” (Oracle, 2019)

Como primer paso para la instalación del sistema operativo mencionado anteriormente en la máquina virtual es necesario llevar a cabo unas configuraciones y realizar el proceso de instalación de una manera exitosa.

Configuración máquina virtual

Oracle VM VirtualBox maneja una interfaz gráfica que se puede ver en la figura 94, esta facilita el proceso de configuración de una máquina virtual, como primer paso se debe hacer clic en la opción que dice “nueva” como se muestra en la figura 94, donde aparecerá una ventana donde se podrá digitar el nombre de la máquina virtual y el sistema operativo a instalar como se evidencia en la figura 95 y a continuación se dará clic a “Next”.

Figura 94. Interfaz gráfica Oracle Vm VirtualBox. (Autoridad propia)

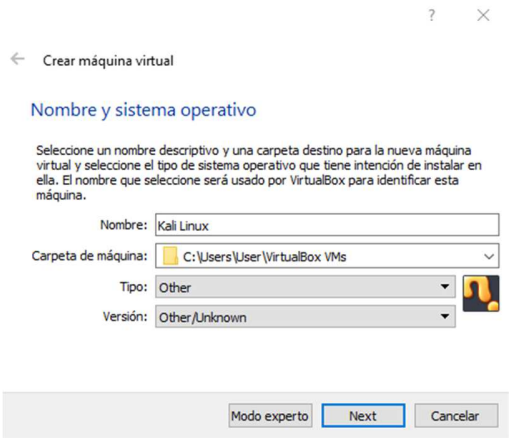


Figura 95. Nombre y sistema operativo máquina virtual. (Autoridad propia)

Posterior a esto se deberá digitar el tamaño de memoria RAM para la máquina virtual, la cual se dejó en 2GB equivalentes a 2048MB como se ve en la figura 96, es entonces cuando se procede a seleccionar la opción de "Crear un disco virtual ahora", a lo que se le dará "Next" como en la figura 97, en cuanto al tipo de archivo de disco duro se escoge VDI (VirtualBox Disk Image) tal como se evidencia en la figura 98 y después se selecciona "Reservado dinámicamente" hablando del almacenamiento en unidad de disco duro física como se ve en la figura 99, por último se escribe la ubicación del archivo la cual se deja por defecto y se selecciona el tamaño del disco duro virtual que se dejó en 20GB como en la figura 100 ya que debe ser mayor a 15GB.

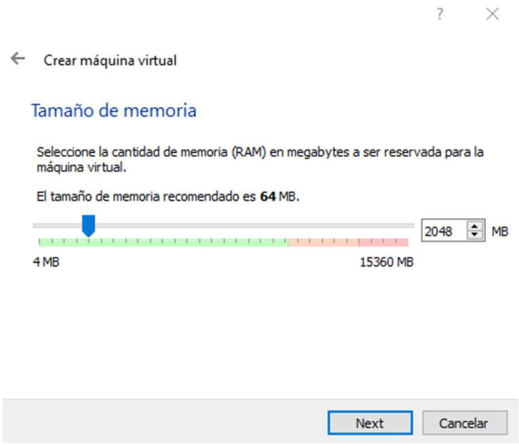


Figura 96. Tamaño de memoria RAM máquina virtual. (Autoridad propia)

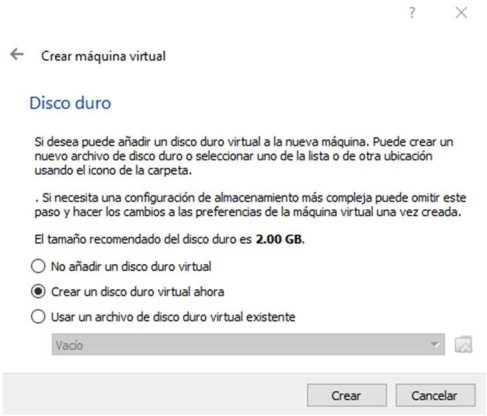


Figura 97. Crear disco duro virtual. (Autoridad propia)

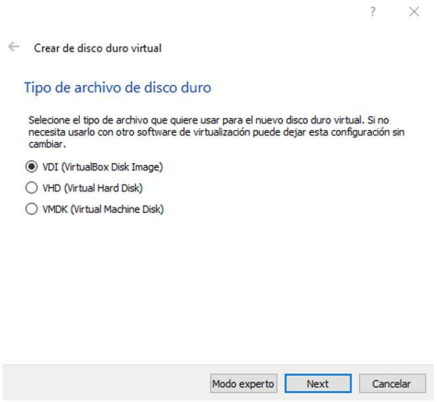


Figura 98. Tipo de archivo de disco duro virtual. (Autoridad propia)

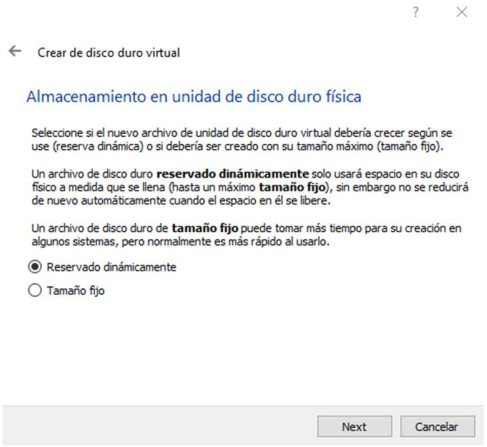


Figura 99. Almacenamiento en unidad de disco duro física. (Autoridad propia)

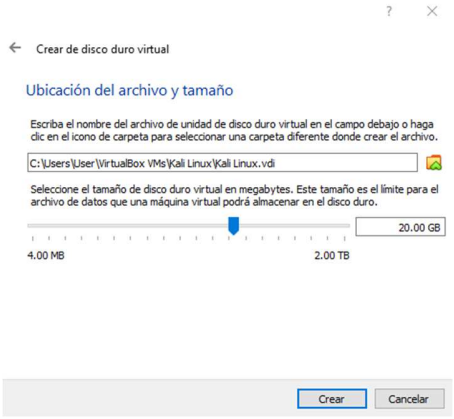


Figura 100. Ubicación del archivo y tamaño. (Autoridad propia)

Después de haber realizado los pasos anteriores ya se tiene creada la máquina virtual, por lo tanto, se procede a hacer unas configuraciones adicionales para el funcionamiento efectivo; se empieza entonces por dar en la opción configuración la cuál desplegará una ventana donde se procederá a dar clic en el apartado "Sistema" como se muestra en la figura 101, donde hay que ubicarse en la pestaña "Procesador", para poder seleccionar 2 núcleos, posterior a esto dar clic en la pestaña "Aceleración", y en la parte de "Interfaz de paravirtualización" se dejará la opción Hyper-V como en la figura 102.

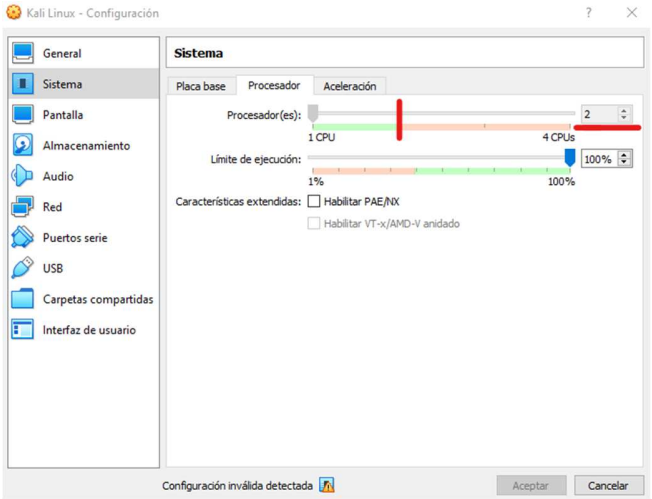


Figura 101. Modificación número de núcleos para el procesador máquina virtual. (Autoridad propia)

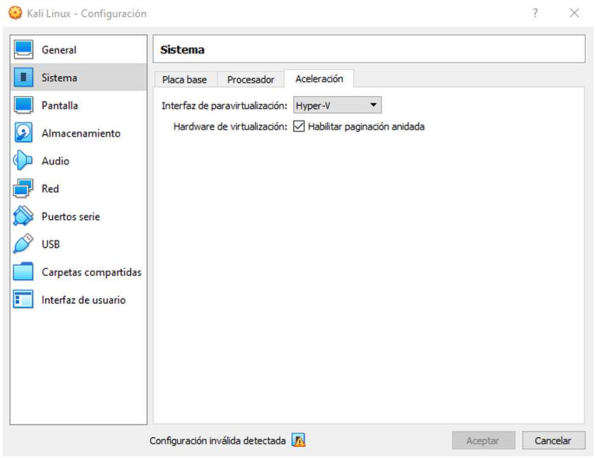


Figura 102. Cambio interfaz de para virtualización en máquina virtual. (Autoridad propia)

Posterior a esto se procede a configurar la pantalla en la cual se dejará al máximo la memoria de vídeo y en cuánto al controlador gráfico se seleccionará VBoxSVGA como en la figura 103, por otro lado, en la configuración de la red en la parte de Conectado se dejará "Adaptador puente" como en la figura 104 ya que esta opción puentea la conexión a red de la pc y de lo contrario asignara un NAT que lo que hará es natear la red y tener un segmento completamente distinto de la red.

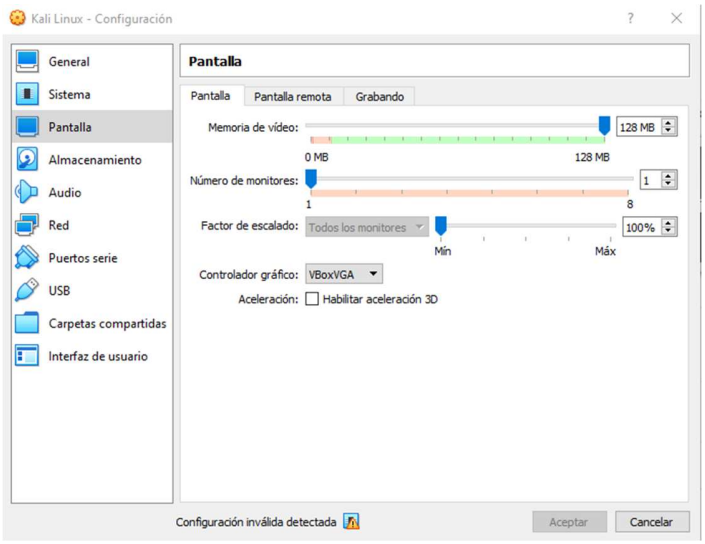


Figura 103. Configuración pantalla máquina virtual. (Autoridad propia)

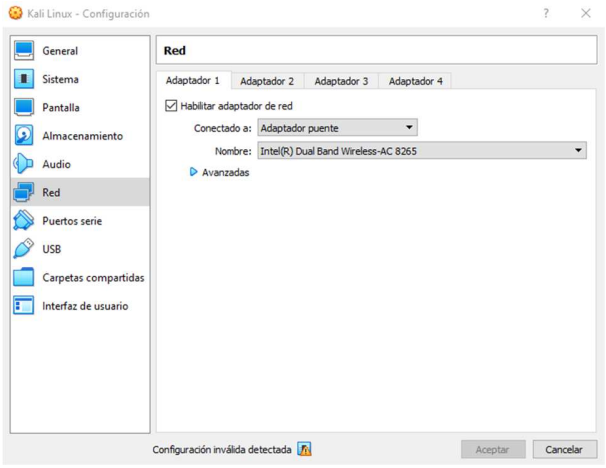


Figura 104. Configuración red máquina virtual. (Autoridad propia)

Por último, se podrá dar iniciar, en esta parte pedirá que se seleccione el archivo .iso o la imagen del sistema operativo a instalar, en este caso en el Kali Linux como se ve en la figura 105.

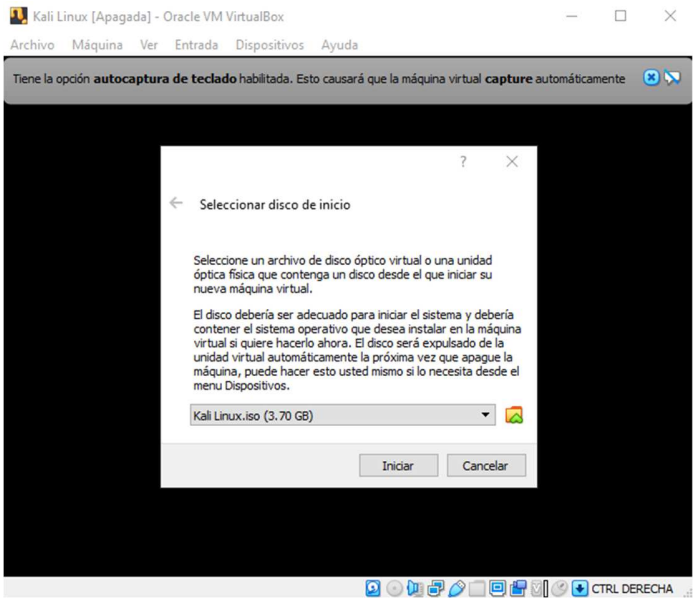


Figura 105. Selección archivo .iso para instalación Kali Linux. (Autoridad propia)

Pasos para instalación Kali Linux

Después de la configuración e iniciación de la máquina virtual se procede a hacer la instalación de Kali Linux, en la cual como primer paso se le da Instalación Gráfica, tal como se evidencia en la figura 106.

Figura 106. Instalación gráfica Kali Linux. (Autoridad propia)

Se procede a escoger idioma (figura 107), ubicación (figura 108) y configuración del teclado (figura 109).

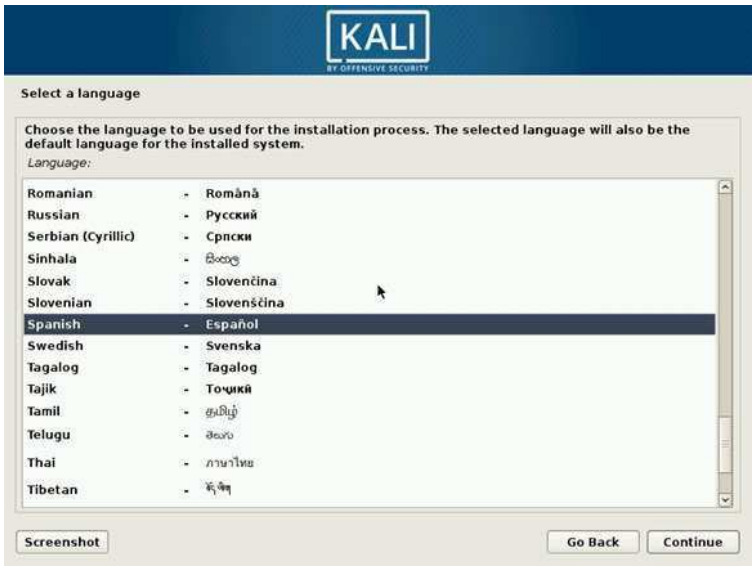


Figura 107. Seleccionar lenguaje instalación. (Autoridad propia)

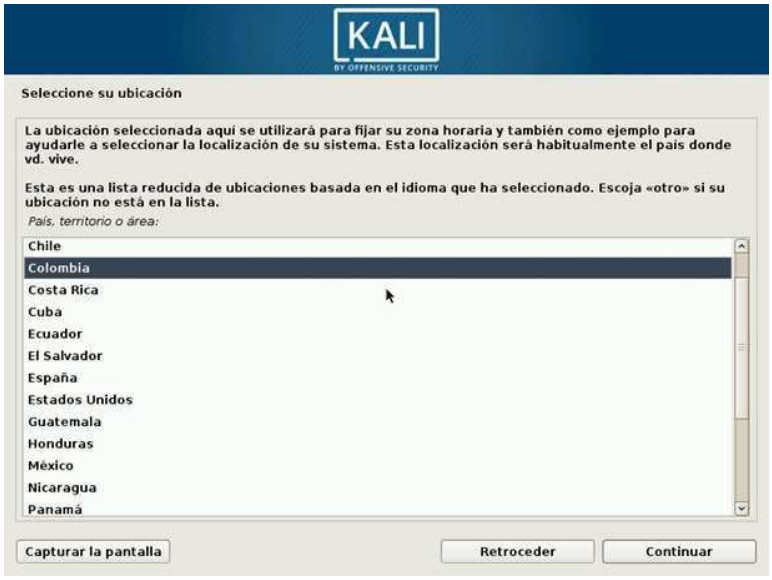


Figura 108. Seleccionar ubicación instalación. (Autoridad propia)

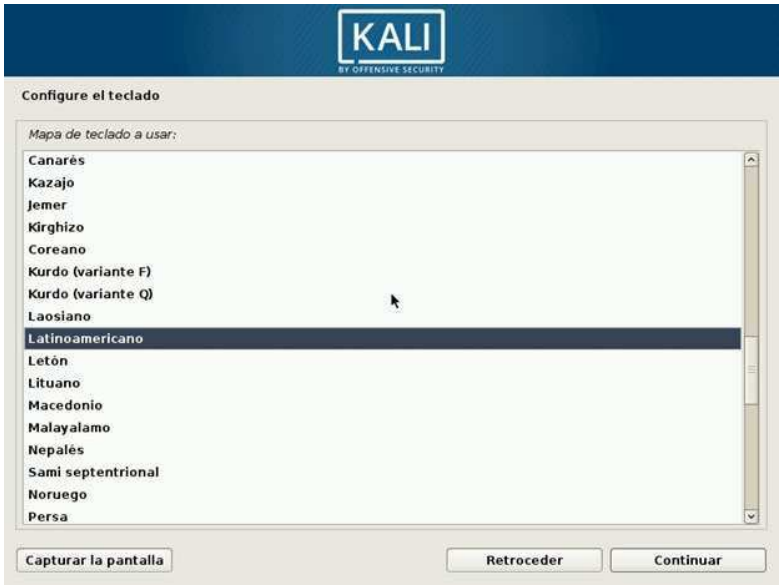


Figura 109. Configuración teclado instalación Kali. (Autoridad propia)

Posterior a esto se debe introducir el nombre de la máquina, se dejó por defecto que es Kali tal como en la figura 110, se llega entonces al paso donde hay que digitar la contraseña para el Superusuario o también llamado Root que es la cuenta o usuario que se encarga de la administración del sistema, este paso se puede evidenciar en la figura 111.

Figura 110. Introducir nombre máquina Kali. (Autoridad propia)

Figura 111. Digitar contraseña superusuario Kali. (Autoridad propia)

Es cuando se llega entonces al paso de particionar los discos, que como se está instalando en una máquina virtual y no hay ningún otro sistema operativo dentro de la máquina virtual se escoge la opción “Guiado – utilizar todo el disco”(Figura 112), posterior a eso se escoge el disco duro que se va a particionar(Figura 113), se selecciona la opción de “Todos los ficheros en una partición”, la cual es recomendada para novatos(Figura 114), después de dar continuar se escoge la opción de “Finalizar el particionado y escribir los cambios en el disco” (figura 115), para de esta manera confirmar el particionado como en la figura 116, cabe resaltar que si el sistema operativo no se va

a instalar en una máquina virtual hay que tener más cuidado con estos pasos, ya que podría dañar el sistema operativo existente en el pc.

Figura 112. Opción particionado Kali. (Autoridad propia)

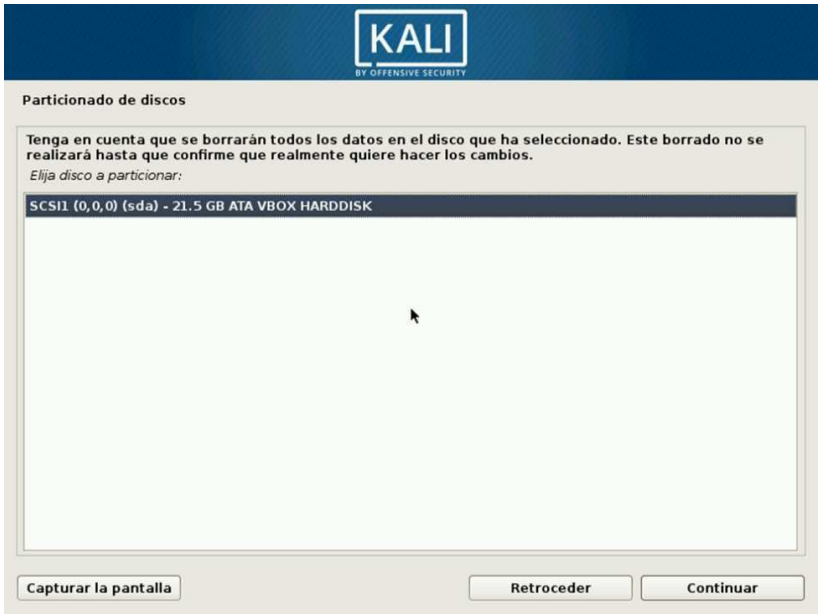


Figura 113. Selección disco duro a particionar. (Autoridad propia)

Figura 114. Seleccionar forma para particionar disco. (Autoridad propia)

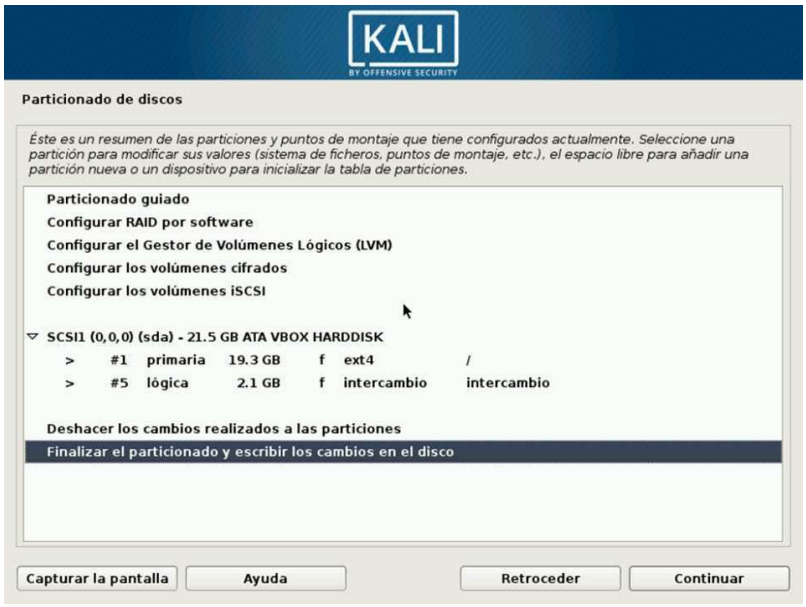


Figura 115. Finalizar particionado para escribir cambios en disco. (Autoridad propia)

Figura 116. Confirmar particionado de disco. (Autoridad propia)

Debido a que se va a manejar el sistema operativo a bajo nivel no es necesario utilizar una réplica en red para poder instalar o complementar los programas que vienen dentro del archivo .iso del Kali Linux, por lo tanto, a la opción de utilizar una réplica en red se le da “No”, como en la figura 117.

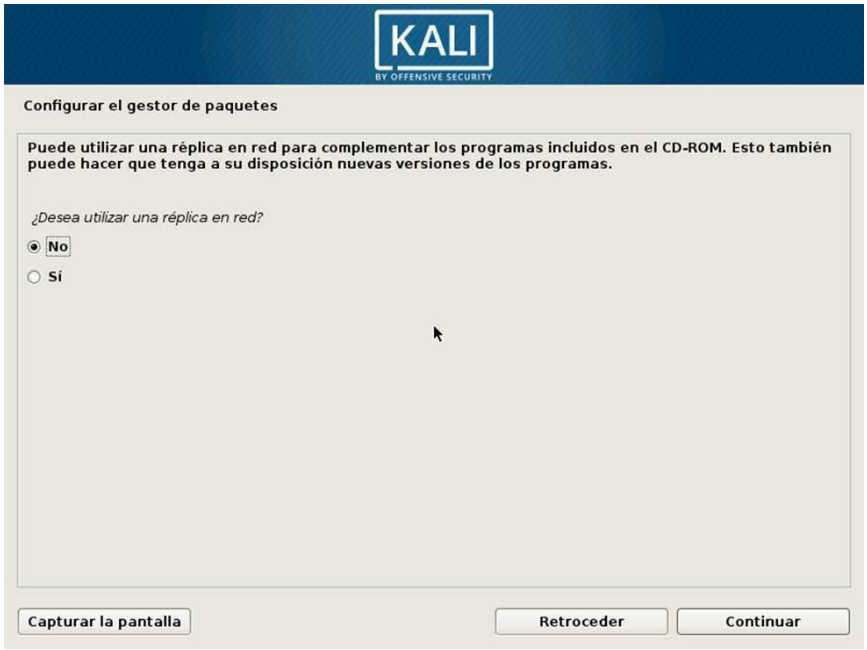


Figura 117. Utilizar una réplica en red. (Autoridad propia)

Como últimos pasos para la instalación del Kali Linux se debe instalar el cargador de arranque GRUB que se debe instalar en el registro principal de arranque como en la figura 118 ya que se está hablando de una máquina virtual y posterior a eso indicar donde se va a instalar el cargador de arranque GRUB tal como se evidencia en la figura 119, al haber realizado estos pasos y después de un tiempo de espera se habrá finalizado la instalación del sistema operativo y deberá aparecer un mensaje como el de la figura 120.

Figura 118. Instalar cargador arranque GRUB. (Autoridad propia)

Figura 119. Indicar donde se va a instalar cargador de arranque GRUB. (Autoridad propia)

Figura 120. Mensaje de finalización de instalación Kali. (Autoridad propia)

Completada la instalación la máquina virtual se reiniciará y aparecerá las opciones para iniciar Kali o las opciones avanzadas, como en la figura 121, dando enter en Kali GNU/Linux se iniciará el sistema operativo y se podrá acceder con el usuario root como en la figura 122, posterior a eso pedirá la contraseña que se digito en la instalación para el superusuario, y dando enter mostrará la pantalla de inicio del Kali Linux tal como se ve en la figura 123.

Figura 121. Opciones para iniciar Kali Linux u Opciones avanzadas. (Autoridad propia)

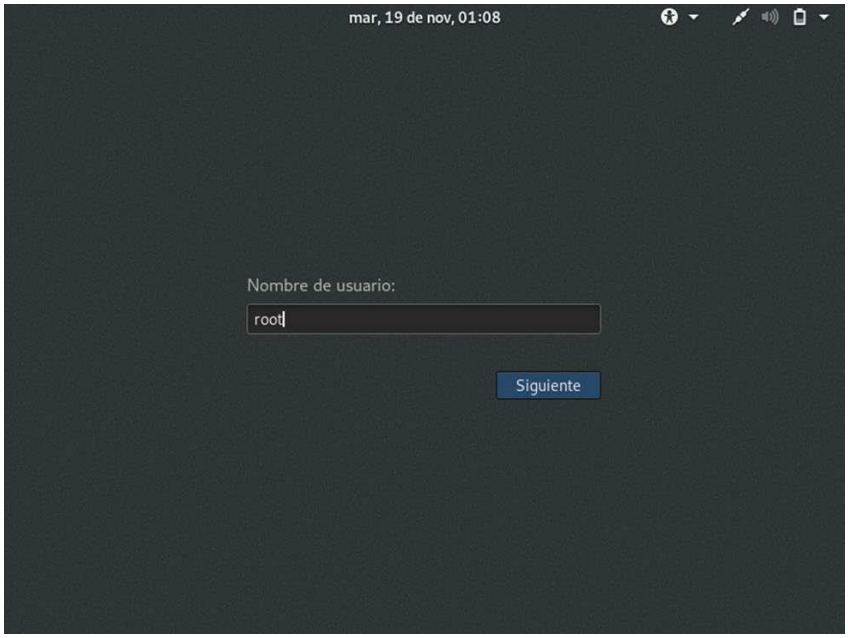


Figura 122. Inicio de sesión con usuario root Kali. (Autoridad propia)

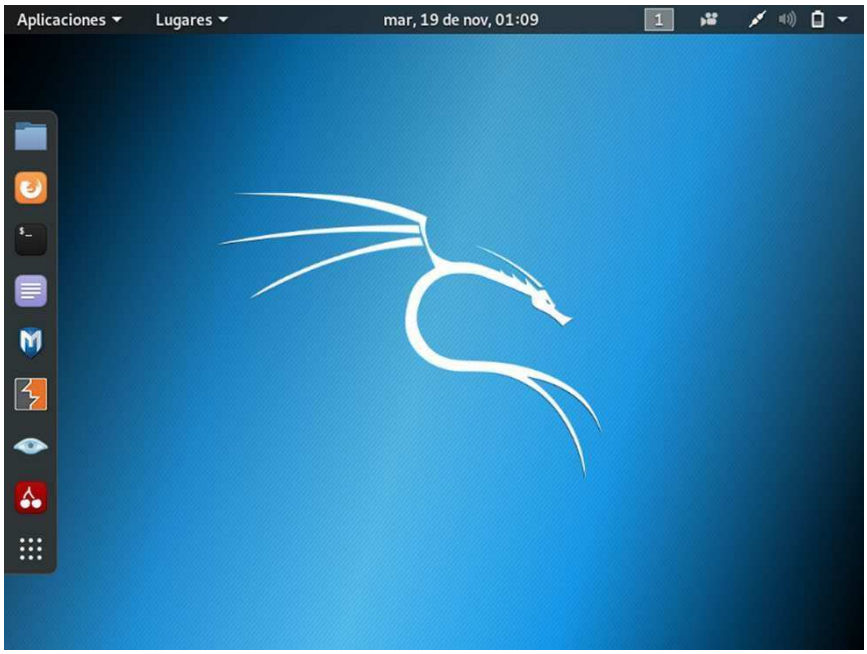


Figura 123. Pantalla inicio Kali Linux. (Autoridad propia)