UNIVERSIDAD DEL SINÚ
Elías Bechara Zainúm
Seccional Cartagena

MODELO DE DETECCIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIO AL PROTOCOLO DHCP USANDO TÉCNICAS DE MACHINE LEARNING

BRANDON ALFREDO PEREZ LARA

UNIVERSIDAD DEL SINÚ ELÍAS BECHARA ZAINÚM
FACULTAD DE CIENCIAS EXACTAS E INGENIERÍAS
ESCUELA DE INGENIERÍA DE SISTEMAS
CARTAGENA-COLOMBIA
Junio 2021

UNIVERSIDAD DEL SINÚ
Elías Bechara Zainúm
Seccional Cartagena

MODELO DE DETECCIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIO AL PROTOCOLO DHCP USANDO TÉCNICAS DE MACHINE LEARNING

Estudiantes:
Brandon Alfredo Perez Lara

Asesor Disciplinar:
Wilson Moscote Casseres

Asesor Metodológico:
Eugenia Arrieta Rodriguez

UNIVERSIDAD DEL SINÚ ELÍAS BECHARA ZAINÚM
FACULTAD DE CIENCIAS EXACTAS E INGENIERÍAS
ESCUELA DE INGENIERÍA DE SISTEMAS
CARTAGENA-COLOMBIA
Junio 2021

Agradecimientos

En primer lugar, quiero agradecer a mi familia, por apoyarme aun cuando mis ánimos decaían. En especial, quiero hacer mención de mis padres, que siempre estuvieron ahí para darme palabras de apoyo y un abrazo reconfortante para renovar energías.

quiero agradecer a mi tutor Wilson Moscote, quien con sus conocimientos y apoyo me guio a través de cada una de las etapas de este proyecto para alcanzar los resultados que buscaba. También quiero agradecer a la docente Eugenia por brindarme todos los conocimientos como tutor metodológico y en el área de la inteligencia artificial que fueron necesarios para llevar a cabo el proceso de investigación. No hubiese podido arribar a estos resultados de no haber sido por su incondicional ayuda.

Agradezco a la institución universitaria Universidad del Sinu por apoyarme en este proceso de investigación y aprendizaje donde se me han abierto las puertas en muchos aspectos de mi vida y que siempre estaré agradecido. Agradezco a la Doctora Maria Claudia Bonfante por su apoyo y gestión en materiales necesarios para el desarrollo de la investigación.

Que no se nos acaben las ganas de soñar.

Muchas gracias a todos.

CONTENIDO

LISTADO DE TABLAS

TABLA DE ILUSTRACIONES

RESUMEN

La siguiente investigación busca aplicar técnicas de inteligencia artificial a la seguridad informática, en búsqueda de la implementación de metodologías modernas al análisis de los datos para la protección de los sistemas. En esta ocasión se realizó la detección de ataques de denegación de servicio de tipo agotamiento al protocolo DHCP desde el cual se obtuvieron resultados positivos, también realizó la implementación de los recursos obtenidos de la investigación mostrando que si puede ser funcional en un ambiente real poniendo a prueba el modelo de inteligencia artificial diseñado capaz de detectar dichos ataques.

INTRODUCCIÓN

El Protocolo de configuración dinámica de host (DHCP) permite la configuración automática de los clientes con la dirección IP y otras características de la red. Debido a que no posee autenticación, el protocolo es vulnerable a una clase de ataques de denegación de servicio (DoS), conocidos popularmente como ataques de inanición DHCP.

Además, se demostró la efectividad del ataque en las redes IPv4 y que puede evitar con éxito que otros clientes obtengan la dirección IP, lo que provoca el escenario DoS. Esto obliga a los mecanismos de detección a implementar metodologías y técnicas avanzadas capaces de identificar dichos ataques.

Para detectar el ataque mencionado, fue planteado un marco de detección de anomalías basado en Machine Learning sin afectar el rendimiento de la red. En el cual se captura el tráfico de la red y se estructura un conjunto de datos que permita alimentar un modelo de aprendizaje automático que sea capaz de evaluar el comportamiento de la red en estado normal y durante un ataque, para así validar que tan efectiva es la técnica.

1 DISEÑO METODOLÓGICO

1.1 Descripción del problema

La seguridad de la información ha evolucionado a lo largo del tiempo, siendo el aseguramiento de los datos uno de los principales retos establecidos desde el principio de los sistemas informáticos. Cada adelanto tecnológico implica un reto en seguridad, desde evitar el robo de datos de los computadores hasta mantener su disponibilidad. No obstante, sigue siendo una problemática constante para la industria de la informática debido a que cada día los vectores de ataque son más indetectables y eficaces.

Uno de los ataques informáticos más comunes son los ataques de denegación de servicio a través del cual se reduce o anula la capacidad de servidores o recursos informáticos de ofrecer servicio. Existen diferentes escenarios en los que se aplica, como por ejemplo la saturación de servicios online mediante el envío masivo de peticiones o la explotación de vulnerabilidades de programas o servicios que dejan de funcionar total o parcialmente. En la mayoría de estos ataques, los atacantes emplean una gran variedad de técnicas y herramientas con las que ocultar su identidad, por lo que resulta un gran problema para capturar a los responsables. En la mayoría de los casos este tipo de ataque supone un gran problema para quien lo recibe debido a que ya no es solo que tus potenciales clientes no puedan acceder a tus servicios, sino que los empleados también podrían ser incapaces de acceder a los recursos o a la gestión del servicio para actuar en el mismo y tratar de impedir o mitigar el incidente.

Sin embargo, existen varios tipos de ataque de denegación de servicio, entre estos están los realizados al protocolo DHCP, El Protocolo de configuración dinámica de host que se utiliza para obtener parámetros de configuración de red en Incluyendo la dirección IP de un servidor DHCP. Este protocolo es vulnerable a una clase de ataques de denegación de servicio (DoS) conocidos popularmente como DHCP Exhaustion Attack [1]. Este ataque requiere que un cliente

malintencionado inyecte una gran cantidad de solicitudes de IP utilizando direcciones MAC falsificadas. Por cada solicitud recibida, un servidor DHCP entrega una nueva dirección IP. Por lo tanto, eventualmente el servidor DHCP se queda sin direcciones IP. Teniendo en cuenta que el servicio DHCP es el que se encarga de ofrecer la configuración en una red, su inanición o no disponibilidad generará que los dispositivos no puedan conectarse a la red.

1.2 Justificación

Con la realización de este trabajo de investigación se espera aportar a la industria innovación y tecnología, contribuyendo a la mejora de la seguridad de la información indicados en Objetivos de Desarrollo Sostenible (ODS), generando conocimiento e investigación útil a la comunidad [2].

Los ataques informáticos provocan cuantiosas pérdidas en las empresas, personas comunes y sistemas de información. Según el Instituto Nacional de Ciberseguridad (INCIBE), las pérdidas medias causadas por los incidentes de seguridad más comunes en las pymes son ciberespionaje, intrusión en la red de la empresa y la denegación de servicio. (ver Figura 1).

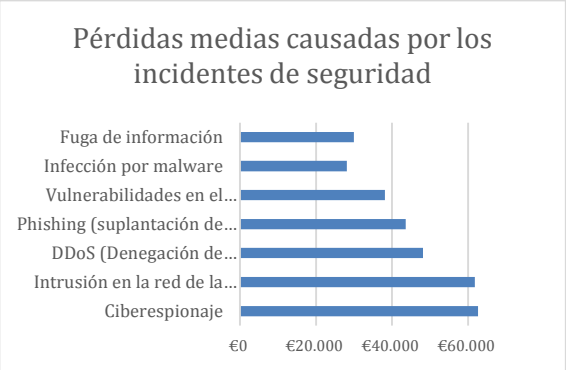

Figura 1. Pérdidas medias causadas por los incidentes de seguridad (INCIBE 2018)

De todos los tipos de ataques informáticos los ataques de denegación de servicio son los más conocidos y temidos, ya que es muy económico su ejecución y muy difícil de rastrear al atacante. En la Figura 2 se observa un estudio del diario el país, donde este ataque fue el tercero más realizado en el año 2018. *(ver Figura 2)*

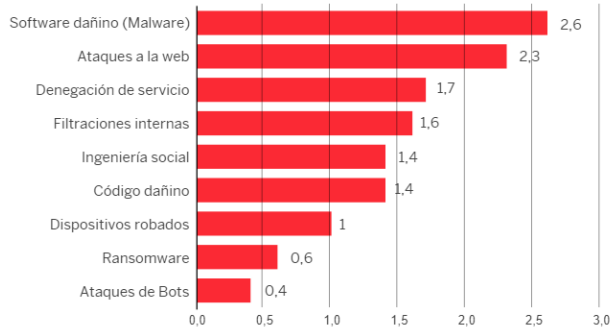

Figura 2. Ataques de informáticos más populares (El País, 2018)

Adicionalmente, la empresa Akamai publicó un artículo donde expone cuales son los principales orígenes de costes de los ataques de denegación de servicios que pueden perturbar una organización ocasionando pérdidas hasta de 1,7 millones de dólares al año por organización [3]:

- Servicios no disponibles
- Asistencia técnica
- Perturbaciones operativas
- Productividad de los usuarios
- Robo o daño de activos

1.3 Alcance

Se espera diseñar un modelo de aprendizaje automatizado capaz de detectar ataques de denegación de servicio al protocolo DHCP, consigo la implementación de un laboratorio que permita capturar el trafico de la red para generar el conjunto

de datos adecuado para entrenar el modelo. Finalmente evaluar el desempeño y asertividad de predicción de ataques.

1.4 Pregunta de investigación

¿La identificación de ataques de denegación de servicio por agotamiento al protocolo DHCP utilizando técnicas de inteligencia artificial pueden ayudar a la mitigación de estos?

1.5 Objetivos

1.5.1 General

Desarrollar un modelo de aprendizaje automático capaz de detectar ataques de denegación de servicios por agotamiento al protocolo DHCP.

1.5.2. Específicos

Diseñar un ambiente de captura de datos que permita recolectar información del tráfico en la red durante un ataque de denegación de servicio al protocolo DHCP.

Analizar la información recolectada y lograr un conjunto de datos apropiados para alimentar un modelo de aprendizaje automático.

Entrenar un modelo de aprendizaje automático a partir de los datos obtenidos para que sea capaz de detectar los ataques presentados en la red.

Evaluar el desempeño del modelo con nuevos datos obtenidos del tráfico de red para así validar su efectividad.

1.6. Estado del arte

Se han realizado diversos estudios acerca de detección de ataques de denegación de servicios, algunos apuntan a ataques en general y otros a técnicas específicas como en este caso al protocolo DHCP, sin contemplar este campo científico de la informática como es la inteligencia artificial. No obstante, el doctor Nikhil Tripathi en el año 2017 publica un artículo llamado “Detecting Stealth DHCP Starvation Attack using Machine Learning Approach” en el cual se realiza una investigación que trata de detección de ataques de denegación de servicio al protocolo DHCP aplicando técnicas de inteligencia artificial planteando un modelo de aprendizaje automatizado. Se demostró que el ataque propuesto puede eludir fácilmente los mecanismos de detección / mitigación conocidos y evitar que los clientes adquieran una dirección IP. También se planteó un marco de detección de anomalías basado en ML para detectar el ataque. El marco utiliza clasificadores de una clase para clasificar el tráfico en diferentes intervalos de tiempo. Se probó el rendimiento de detección del marco formulado en redes IPv4 e IPv6 utilizando tráfico capturado de una red real que conectaba miles de dispositivos heterogéneos y demostramos que el marco puede detectar el ataque propuesto con una precisión muy alta. [4].

Otro aporte importante, es presentado por el instituto de ciberseguridad de Canadá (Canadian Institute for Cybersecurity), que realiza diversos estudios acerca de la detección de ataques informáticos basados en IDS, aplicando técnicas de inteligencia artificial. En 2017 llevaron a cabo un laboratorio en el cual se realizaron diversos ataques a una red y fue capturado el tráfico para que

posteriormente fuese analizado con el fin de alimentar un modelo de inteligencia artificial. Se obtuvieron resultados positivos detectando ataques con alta probabilidad de aceptabilidad El conjunto de datos de CICIDS2017 contiene los ataques comunes benignos y más actualizados, que se asemejan a los verdaderos datos del mundo real (PCAP). También incluye los resultados del análisis de tráfico de red utilizando CICFlowMeter con flujos etiquetados basados en la marca de tiempo, IP de origen y destino, puertos de origen y destino, protocolos y ataque (archivos CSV) [5].

De igual forma, en 2019 la ingeniera Auz Cadena Fabiola realiza una investigación acerca de Implementación de controles en una red LAN para mitigar los ataques al protocolo DHCP utilizando las mejores prácticas del diseño de redes. En el cual logra implementar controles dentro de una red local(LAN) reforzando la seguridad y privacidad de los clientes que establecen comunicación entre ellos y su navegación dentro de la red. Se diseñó un escenario con la herramienta GNS3 que permitió la implementación del protocolo DHCP. Se investigó los controles necesarios como son la seguridad de puertos y la tecnología DHCP Snooping, para minimizar los riesgos de que los clientes maliciosos se filtren en la red y trunquen el correcto funcionamiento del servidor. [6]

Como fue expuesto anteriormente la inteligencia artificial puede ser utilizada con resultados positivos en la detección de ataques informáticos, correo no deseado (spam), antivirus, así como otras aplicaciones importantes. Los estudios que se realizan en el presente y futuro cercano avizoran la solución de problemas críticos que con la utilización de algoritmos tradicionales son muy difíciles o su complejidad es muy alta para su solución.

1.7. Marcos de referencia

1.7.1. Marco teórico

Las redes han tenido grandes cambios en los últimos años, lo que incrementa su uso y expone a los usuarios a ataques cibernéticos generando pérdidas a las organizaciones, es por tal que se debe priorizar la integridad de estos usuarios, su disponibilidad y la confiabilidad de poder dar sus datos personales. Para este proceso es necesario poder acceder a los sistemas informáticos que ayudan a organizar las tareas dentro de un sistema de información [5].

Los delitos informáticos o ciberdelincuencia, que afectan todo el ámbito tecnológico son toda aquella acción ilegal que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Muchos de estos delitos, al no estar tipificados en la ley, se definen como abusos informáticos. La criminalidad informática o cibercrimen tiene un alcance mayor, donde se incluyen delitos como el fraude, el robo, el chantaje, la falsificación y la malversación de caudales públicos utilizando ordenadores y redes como medio para realizarlos.

Básicamente el Ciberterrorismo podría definirse como “Ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos atacantes.” (Definición oficial del FBI) [8].

Hoy en día gran parte de la información del ser humano está procesada mediante los sistemas de red de informática, convirtiéndose en una operación esencial para mantenerse protegida generando confiabilidad, integridad y disponibilidad. Según la FBI los virus informáticos siguen siendo una de las mayores pérdidas financieras dentro de la empresa con una representación del 74% causando acceso no autorizado dentro del sistema [7].

Los ataques de denegación de servicio causan todos los años pérdidas millonarias a empresas, y muchos problemas a los administradores de sistemas. Esta facilidad de uso hace que muchos sin tener los conocimientos necesarios sobre un protocolo determinado o acerca de cómo funciona, puedan llegar a causar grandes daños a los servidores que tengan como objetivos.

1.7.2. Marco conceptual

Tráfico de datos

Tráfico es un concepto que tiene su origen en un vocablo italiano que se refiere al tránsito o desplazamiento de medios de transporte por algún tipo de camino o vía. El concepto de tráfico puede hacer mención tanto a la acción del movimiento como a las consecuencias de dicha circulación. Por tanto, el tráfico de red se puede definir como la cantidad de información o datos enviados y recibidos por todos aquellos equipos de una red computadoras [9].

DHCP (Protocolo de configuración dinámica de host)

Es un protocolo cliente/servidor en el que normalmente el servidor tiene una lista de direcciones IP dinámicas y éstas van siendo asignadas a los clientes por dicho servicio, sabiendo en todo momento qué máquina está en posesión de esa IP. El DHCP permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Este protocolo también permite al administrador supervisar y distribuir las direcciones IP de forma centralizada, automática, o incluso reservar direcciones IP's para equipos específicos dentro de la red. DHCP tiene tres formas distintas de asignar direcciones IP:

Asignación manual o estática: Distribuye una dirección IP a una máquina determinada. Esto suele ser usado cuando se quiere controlar la asignación de dirección IP a cada cliente y evita que se conecten clientes no autorizados a la red.

Asignación automática: Esta forma de distribución de direcciones IP es utilizada cuando el número de clientes en la red no varía demasiado. Funciona asignando una dirección IP a una máquina cliente la primera vez que ésta hace la solicitud

DHCP al servidor y la misma dirección es asignada cada vez que la máquina se conecta a la red.

Asignación dinámica: Este método de asignación permite que la dirección asignada a un cliente varíe, ya que normalmente una dirección IP es dada al cliente por un intervalo de tiempo. Una vez finalizado el cliente debe volver a hacer la petición para la obtención de una nueva o misma dirección IP. Esto es útil cuando el número de clientes en la red no es fijo [10].

DHCP funciona sobre un servidor central (servidor, estación de trabajo o incluso un PC) el cual asigna direcciones IP a otras máquinas de la red. Este protocolo puede entregar información IP en una LAN o entre varias VLAN. Esta tecnología reduce el trabajo de un administrador, que de otra manera tendría que visitar todos los ordenadores o estaciones de trabajo uno por uno. Para introducir la configuración IP consistente en IP, máscara, Gateway, DNS, etc. Un servidor DHSC (DHCP Server) es un equipo en una red que está corriendo un servicio DHCP. Dicho servicio se mantiene a la escucha de peticiones broadcast DHCP. Cuando una de estas peticiones es oída, el servidor responde con una dirección IP y opcionalmente con información adicional [11].

Cliente y servidor DHCP

La asignación automática de direcciones mediante el protocolo de configuración dinámica de host tiene lugar en cuatro pasos consecutivos:

El cliente DHCP envía un paquete DHCPDISCOVER a la dirección 255.255.255.255 desde la dirección 0.0.0.0. Con esta denominada difusión amplia o broadcast, el cliente establece contacto con todos los integrantes de la red con el propósito de localizar servidores DHCP disponibles e informar sobre su petición. Si solo hay un servidor, entonces la configuración es extremadamente sencilla.

Todos los servidores DHCP que escuchan peticiones en el puerto 67 responden a la solicitud del cliente con un paquete DHCPOFFER, que contiene una dirección IP libre, la dirección MAC del cliente y la máscara de subred, así como la dirección IP y el ID del servidor.

El cliente DHCP escoge un paquete y contacta con el servidor correspondiente con DHCPREQUEST. El resto de los servidores también reciben este mensaje de forma que quedan informados de la elección. Con esta notificación, el cliente también solicita al servidor una confirmación de los datos que le ha ofrecido. Esta respuesta también sirve para confirmar parámetros asignados con anterioridad.

Para finalizar, el servidor confirma los parámetros TCP/IP y los envía de nuevo al cliente, esta vez con el paquete DHCPACK (DHCP packnowledged o «reconocido»). Este paquete contiene otros datos (sobre servidores DNS, SMTP o POP3). El cliente DHCP guarda localmente los datos que ha recibido y se conecta con la red. Si el servidor no contara con ninguna dirección más que ofrecer o durante el proceso la IP fuera asignada a otro cliente, entonces respondería con DHCPNAK (DHCP not acknowledged o «no reconocido»).

La dirección asignada se guarda en la base de datos del servidor junto con la dirección MAC del cliente, con lo cual la configuración se hace permanente, es decir, el dispositivo se conecta a la red siempre con esa dirección que le ha sido asignada automáticamente y que ya no está disponible para ningún otro cliente, lo que significa que los clientes DHCP nuevos no pueden recibir ninguna dirección si ya están todas asignadas, incluso aunque algunas IP ya no se usen activamente. Esto ha llevado a la expansión de las direcciones dinámicas y, en casos especiales, a la asignación manual vía servidor DHCP [12].

Tipos de ataques al protocolo DHCP

Ataque de agotamiento DHCP

El servidor DHCP tiene un conjunto de direcciones IP que se alquilan a los hosts; pero el grupo de direcciones IP siempre tiene un número limitado de direcciones IP. En el ataque de agotamiento de DHCP, el atacante agota las direcciones IP en el grupo de direcciones DHCP [13]. El servidor DHCP distribuye felizmente todo el conjunto de direcciones disponibles para la red del cliente, porque no tiene forma de diferenciar entre un host genuino y uno falsificado. Si un cliente legítimo intenta obtener una dirección IP, no tendrá conectividad IP porque se han asignado todas las direcciones a los clientes falsificados.

Ataque al servidor DHCP Rogue

El servidor no autorizado es un servidor DHCP en una red que no está bajo el control administrativo del personal de la red. El ataque al servidor DHCP falso [13]es un famoso ataque de LAN en el que un usuario malintencionado se disfraza de servidor DHCP y responde a las solicitudes de DHCP con una dirección IP falsa. Cuando los clientes se conectan a la red, tanto el servidor DHCP legal como el falso reciben el mensaje DHCP DISCOVER; luego, ambos servidores les ofrecerán direcciones IP y una puerta de enlace predeterminada. El servidor no autorizado DHCP responde a las solicitudes DHCP con una configuración incorrecta. La información incorrecta puede ser una puerta de enlace predeterminada incorrecta, un servidor DNS incorrecto o una dirección IP incorrecta. Cuando el host del atacante (un servidor DHCP falso) se convierte en una puerta de enlace predeterminada, puede recibir todo el tráfico de la red. Entonces, puede analizar y modificar todos los paquetes enviados desde la máquina atacada y puede robar contraseñas e información de privacidad.

Inteligencia artificial

La IA es la ciencia e ingeniería que permite diseñar y programar ordenadores de forma que realicen tareas que requieren inteligencia. El objetivo de la IA es lograr que una máquina tenga una inteligencia de tipo general similar a la humana, es de lo más ambiciosos que se ha planteado la ciencia. Por su dificultad, es comparable

a otros grandes objetivos cientificos como explicar el origen de la vida, el origen del universo o conocer la estructura de la materia. [14]

Detección de anomalías

Detección de anomalías (o detección atípica) es la identificación de elementos raros, eventos u observaciones que generan sospechas al diferenciarse significativamente De la mayoría de los datos. Normalmente, los datos anómalos se pueden conectar a algún tipo de problema o evento raro como, por ejemplo, fraude bancario, problemas médicos, defectos estructurales, equipo defectuoso, etc. Esta conexión hace que sea muy interesante poder elegir qué puntos de datos pueden considerarse anomalías, ya que identificar estos eventos suele ser muy interesante desde una perspectiva empresarial. [15]

Redes neuronales

La neurona artificial por si sola posee una baja capacidad de procesamiento y su nivel de aplicabilidad es bajo, su verdadero potencial radica en la interconexión de estas, tal como sucede en el cerebro humano. Esto ha motivado a diferentes investigadores a proponer diversas estructuras para conectar neuronas entre sí, dando lugar a las redes neuronales artificiales. En la literatura encontramos múltiples definiciones, de las cuales queremos destacar las siguientes, que se ajustan muy bien al concepto de red que seguiremos a lo largo de este libro. La Agencia de Investigación de Proyectos Avanzados de Defensa (DARPA), define una red neuronal artificial como un sistema compuesto de muchos elementos simples de procesamiento los cuales operan en paralelo y cuya función es determinada por la estructura de la red y el peso de las conexiones, donde el procesamiento se realiza en cada uno de los nodos o elementos de cómputo [16].

Sniffer

Este tipo de aplicaciones tienen la responsabilidad de realizar la captura de distintos paquetes que se encuentran en circulación a través de una red

informática. La aplicación no se limita a capturar los paquetes de manera indiscriminada, sino que tiene capacidad para analizar la topología de la red y llevar a cabo la captura teniendo este factor en cuenta.

Además de esto, los sniffers tienen un uso fundamental, que viene a ser el de analizar los paquetes de la red y estudiarlos, no solo capturarlos. Debido a ello hay multitud de expertos, no solo aquellos que tienen buenas intenciones, que utilizan los sniffers con la intención de obtener información valiosa de los distintos paquetes que se encuentran desplazándose por la red [17].

1.7.3. Marco legal y consideraciones éticas

El presente proyecto tiene sus bases legales sobre los siguientes pilares de normas, decretos y leyes del estado colombiano:

I. Decreto 846 de 2016; Por el cual se modifica la estructura del Departamento Administrativo de Ciencia, Tecnología e Innovación - COLCIENCIAS.
II. Decreto 591 del 26 de febrero de 1991 por el cual se regulan las modalidades específicas de contratos de fomento de actividades científicas y tecnológicas.
III. Decreto 585 del 26 de febrero de 1991 por el cual se crea el Consejo Nacional de Ciencia y Tecnología, se reorganiza el Instituto Colombiano para el Desarrollo de la Ciencia y la Tecnología-Colciencias- y se dictan otras disposiciones.
IV. Decreto 2870 de 31 de julio de 2007, por medio del cual se adoptan medidas para facilitar la Convergencia de los servicios y redes en materia de Telecomunicaciones. (Diario oficial nº 46.706 de 31 de julio de 2007).
V. Decreto 393 del 26 de febrero de 1991 por el cual se dictan normas sobre asociación para actividades científicas y tecnológicas, proyectos de investigación y creación de tecnologías.
VI. Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
VII. Ley 1341 de 2009. “Tecnologías de la Información y aplicación de seguridad”.
VIII. Ley 1581 de 2012 y el Decreto 1377 de 2013, se desarrolla el derecho constitucional que tienen todas las personas a conocer, suprimir, actualizar y

rectificar todo tipo de datos personales recolectados, almacenados o que hayan sido objeto de tratamiento en bases de datos en las entidades del públicas y privadas.

IX. Decreto 2952 de 2010. “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”.

X. Decreto 886 de 2014. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”

XI. Decreto 1083 de 2015. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”

1.8. Metodología

1.8.1. Línea de Investigación

La Universidad del Sinú Seccional Cartagena cuenta con varios Grupos de Investigación que trabajan con el fin mostrar avances tecnológicos a la optimización de procesos y generación de nuevos conocimientos. Este proyecto aportará a la línea de investigación de inteligencia artificial del grupo de investigación DEARTICA. Debido a que este proyecto involucra técnicas de Machine learning que son unas de las temáticas de gran impacto a nivel de investigaciones en el campo de la ingeniería y ciencias de la computación.

1.8.2. Tipo de investigación

Esta investigación corresponde a una investigación aplicada, de cohorte retrospectiva en el cual se analiza el tráfico de la red. Los datos se obtendrán de los dispositivos de red; en el que se aplican los conocimientos y las técnicas de inteligencia artificial para contribuir en la solución de un problema de la vida real, como es el apoyo diagnóstico de ataques de denegación de servicio, específicamente aplicado al protocolo DHCP. En este tipo de investigación el

énfasis del análisis está en la aplicación efectiva de las técnicas de inteligencia artificial para obtener resultados positivos en términos de sensibilidad y especificidad.

1.8.3. Muestra y Población

En este trabajo no implica la interacción con individuos ni especies animales o vegetales, sino que se realizará a partir de unos datos generados en un laboratorio simulado, posteriormente a la generación de los datos se tomará una muestra teniendo en cuenta algunos criterios como la segmentación de paquetes.

1.9. Recolección de la información

Una vez el laboratorio se encuentre diseñado y configurado se procede a la ejecución y captura de tráfico, esta se realizará en dos escenarios, durante la red en estado normal y cuando se está realizando un ataque al protocolo DHCP, esto con el fin de segmentar la información y tener una mejor organización.

La captura de tráfico se realiza por medio de un switch con puerto SPAM por el que pasan todas las conexiones de la red. La máquina encargada de la captura y análisis de la información está conectada al puerto SPAM configurado en el switch y ejecutando un sniffer que en este caso es la herramienta Wireshark nos permitirá obtener todo el tráfico de la red y almacenarlo en archivos pcap (*ver figura 3*).

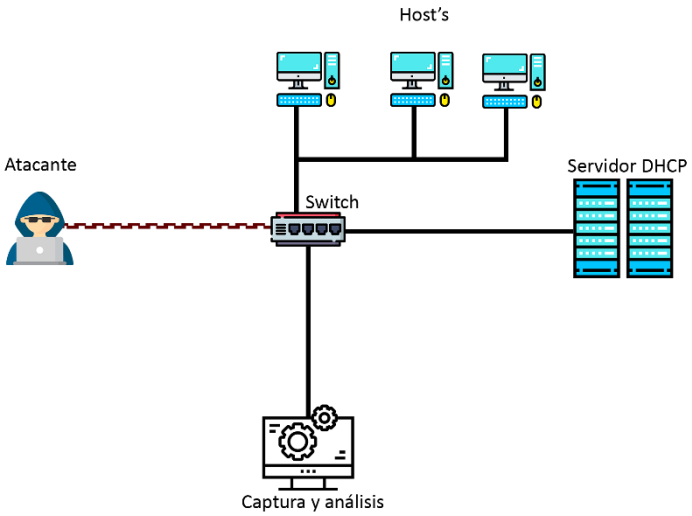

Figura 3. Esquema de laboratorio (Fuente propia)

El siguiente diagrama de flujo muestra los procesos que se realizarán durante la investigación. *(ver Figura 4)*

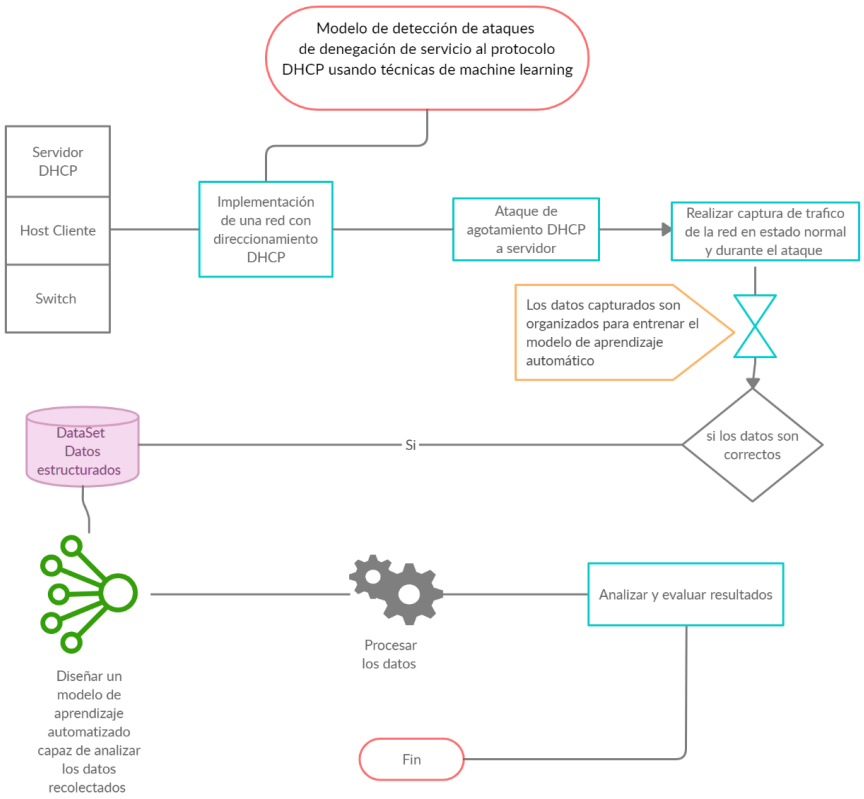

Figura 4. Diagrama de flujo (fuente propia)

Esta investigación es de tipo aplicada y de desarrollo tecnológico ya que sirve para generar conocimientos que se puedan poner en práctica en el sector productivo, con el fin de impulsar un impacto positivo de la seguridad en las redes. Es una investigación cuantitativa ya que se tiene en cuenta la recolección de datos y pone en práctica el uso de herramientas matemáticas, estadísticas e informáticas para medirlos. Esto permite hacer conclusiones generalizadas que pueden ser proyectadas en el tiempo. Ya que el estudio se realizará en un momento concreto se considera una investigación transversal durante un periodo determinado.

1.10. Fases y actividades

Para dar respuesta al cumplimiento de los objetivos planteados se presenta la siguiente matriz metodológica (*ver Tabla 1*).

Tabla 1. Fase de Actividades

Objetivos	Fases	Actividades
● Diseñar un ambiente de captura de datos que permita recolectar información del tráfico en la red durante un ataque de denegación de servicio al protocolo DHCP.	1. Análisis 2. Diseño 3. Implementación	1.1. Investigar acerca del funcionamiento del protocolo DHCP 1.2. identificar los múltiples ataques que puede presentar el protocolo DHCP 2.1. diseñar arquitectura de laboratorio en el cual se pueda realizar el ataque y captura de datos. 2.2. obtener los equipos necesarios para la implementación del laboratorio. 2.3. Implementar servidor DHCP 2.4. Seleccionar el vector de ataque al protocolo DHCP. 2.5. Configurar los clientes y el switch. 3.1. Configurar sniffer con switch 3.2. Inicializar la captura de datos con la herramienta Wireshark.
● Analizar la información recolectada y lograr un conjunto de datos apropiados para	4. Organización y limpieza de datos. 5. Diseño de modelo de	4.1 Identificar las variables y factores más influyentes en el resultado de la investigación.

alimentar un modelo de aprendizaje automático.	aprendizaje automatizado.	4.2 aplicar técnicas para la organización del conjunto de datos. 5.1 Una vez organizados y segmentos los datos se procede a la creación del modelo de aprendizaje automatizado
● Entrenar un modelo de aprendizaje automático a partir de los datos obtenidos que sea capaz de detectar los ataques presentados en la red.	6. Procesamiento de datos	6.1 Procesar los datos utilizando el modelo de aprendizaje ya creado teniendo en cuenta que se debe entrenar el modelo y probar con un conjunto de datos distintos
● Evaluar el desempeño del modelo con nuevos datos obtenidos del tráfico de red para así validar su efectividad.	7. Evaluación de resultados	7.1 recopilar los resultados que arroja el modelo 7.2 validar si los resultados son correctos o incorrectos checando la efectividad.

Modelo de detección de ataques de denegación de servicio al protocolo DHCP usando técnicas de machine learning			0																	
Actividades	Recursos en efectivo necesarios		Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May
	Rubro	Valor																	
1.1. Investigar acerca del funcionamiento del protocolo DHCP	1.Investigación y documentación.																		
1.2. identificar los múltiples ataques que puede presentar el protocolo DHCP	1.Investigación y documentación.																		
2.1. diseñar arquitectura de laboratorio en el cual se pueda realizar el ataque y captura de datos.	2.implementación de laboratorio.																		
2.2. obtener los equipos necesarios para la implementación del laboratorio.	2.implementación de laboratorio.																		
2.3. Implementar servidor DHCP	2.implementación de laboratorio.																		
2.4. Seleccionar el vector de ataque al protocolo DHCP.	2.implementación de laboratorio.																		
2.5. Configurar los clientes y el switch.	2.implementación de laboratorio.																		
3.1. Configurar sniffer con switch	3.recolección de información																		
3.2. Inicializar la captura de datos con la herramienta Wireshark.	3.recolección de información																		
4.1 investigar acerca de técnicas de limpieza de datos enfocados a inteligencia artificial	4.Organización y limpieza de datos.																		
4.2 identificar las variables y factores más influyentes en el resultado de la investigación	4.Organización y limpieza de datos.																		
4.3 aplicar técnicas para la organización del conjunto de datos.	4.Organización y limpieza de datos.																		
5.1 Una vez organizados y segmentos los datos se procede a la creación del modelo de aprendizaje automatizado	5.Diseño de modelo de aprendizaje automatizado.																		
6.1 Procesar los datos utilizando el modelo de aprendizaje ya creado teniendo en cuenta que se debe entrenar el modelo y probar con un conjunto de datos distintos	6.Procesamiento de datos																		
7.1 recopilar los resultados que arroja el modelo	7.Análisis de resultados																		
7.2 validar si los resultados son correctos o incorrectos checando la efectividad.	7.Análisis de resultados																		

Figura 5. Cronograma de actividades.

2. CONSTRUCCIÓN DE ARQUITECTURA DE LABORATORIO

El método de denegación de servicio al protocolo DHCP evaluado en esta investigación es llamado ataque de agotamiento DHCP (DHCP Starvation), el cual inunda con peticiones DHCP el servidor utilizando diferentes direcciones MAC como fue mencionado anteriormente. Para el estudio de este ataque se plantea un laboratorio capaz de capturar el tráfico de la red en un estado normar y durante un ataque para así estudiar procesar la información obtenida y efectuar un análisis.

2.1. Ataque de inanición de DHCP

Considerando la siguiente topología de red, hay tres entidades, a saber, servidor DHCP, cliente malicioso, cliente víctima. Todas las entidades están conectadas al router mediante conexión cableada, como lo muestra la siguiente figura (*ver figura 6*).

Figura 6. Topología ataque al protocolo DHCP

La secuencia de eventos ocurridos al lanzar un ataque de inanición DHCP:

i. Inicialmente se configuran todos los dispositivos permitiendo la conexión y recepción del servicio DHCP, estos deben ser capaz de recibir una IP del dispositivo que suministra el servicio.

ii. Utilizando la herramienta Yersinia desde la maquina atacante se lanza el ataque de inanición al servidor DHCP desde el cual se envían una alta cantidad de solicitudes de IP (DHCP DISCOVER) el cual intentará inundar el servicio con el fin de agotar el total de las direcciones. (ver Figura 7)

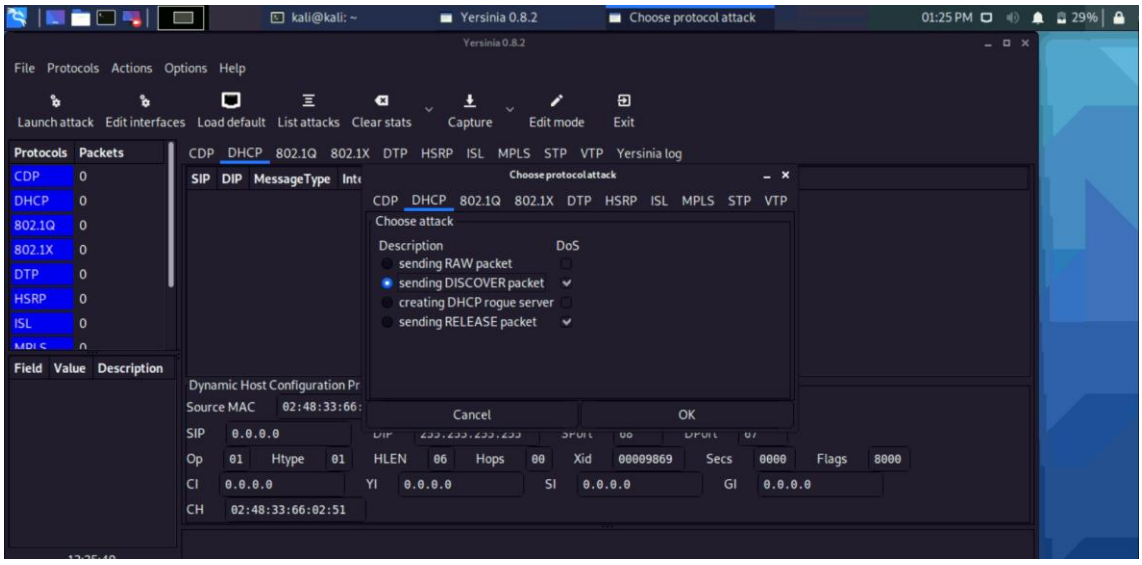

Figura 7. Herramienta Yersinia

iii. El servidor DHCP recibe las solicitudes procesando y entregando las ip que tiene disponible, sin embargo, si la cantidad de peticiones es muy alta Para el servidor no será posible continuar entregando más direcciones.

iv. Al conectar un nuevo dispositivo a la red no le será posible entregar una dirección ip ya que el servidor DHCP se encuentra colapsado.

2.2. Construcción de laboratorio

El marco de detección planteado para la detección del Ataque DHCP Starvation consta de la siguiente topología (*ver figura 8*):

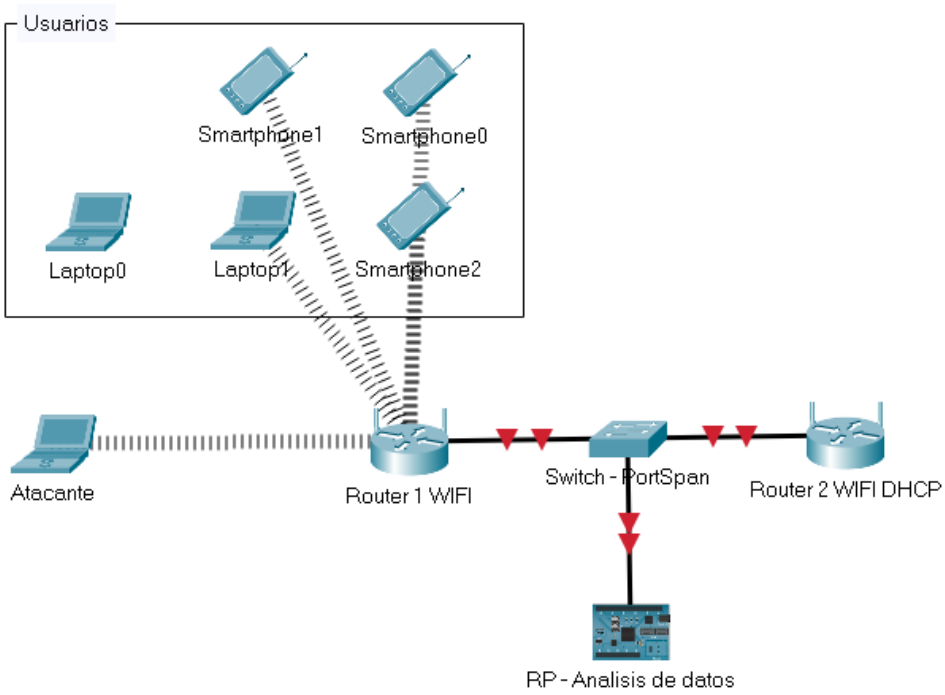

Figura 8. Topología de laboratorio

Los dispositivos que componen la topología tienen las siguientes funciones y características:

- Atacante

Esta máquina cuenta con sistema operativo Kali Linux y se encuentra conectada a la red de forma inalámbrica, desde la cual utilizando la herramienta Yersinia se realiza el ataque al servidor DHCP realizando una gran cantidad de peticiones Tipo DISCOVER.

- Usuarios

Dispositivos normales conectados a la red.

- Router1 WIFI

Funciona Como Punto de acceso a los dispositivos Atacante y Usuario con el fin de permitir múltiples conexiones sin embargo este no proporciona dirección IP, este dispositivo se encuentra conectado directamente al switch. (*ver figura 9*)

Figura 9. Router Tp-Link

- Switch -Port Span

Este Switch Cisco Permite la conexión del Router1 con el Router2 además admite configurar un puerto Span al cual redireccionará una copia del tráfico de la red a la raspberry. (*ver figura 10*)

Figura 10. Switch Tp-Link (Puerto spam)

- RP - Análisis de datos

Dispositivo Raspberry Pi 2, cuenta con el sistema operativo Kali Linux, que utilizando la herramienta Wireshark permite capturar el tráfico de la red proveniente del puerto spam. (*ver figura 11*)

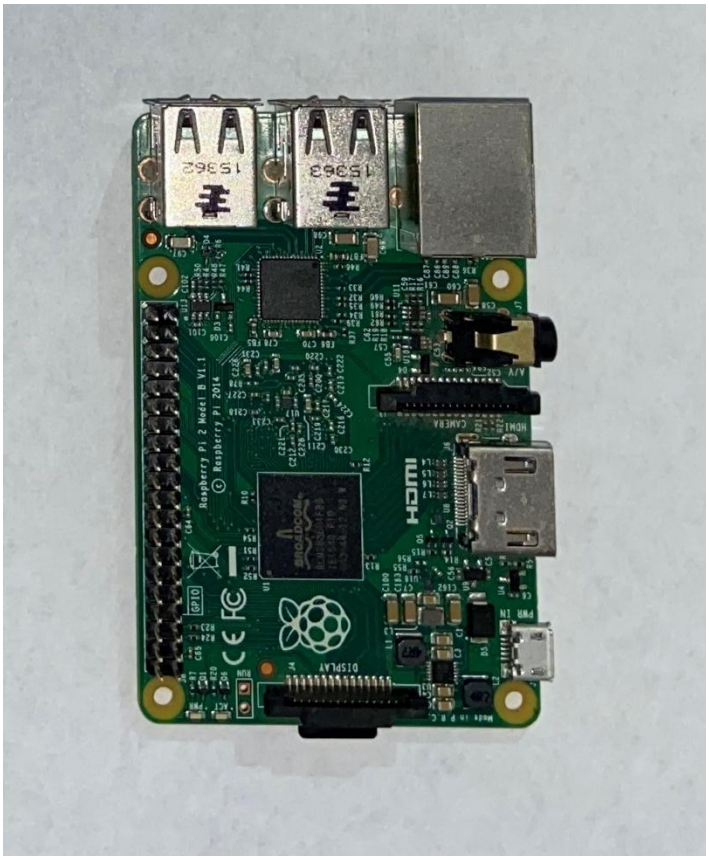

Figura 11. Raspberry Pi 2

- Router2 WIFI DHCP

Router principal, permite la conexión a internet y brinda el servicio DHCP, objetivo principal del atacante. (*ver figura 12*)

Figura 12. Router movistar. tomado de Movistar. 2021

2.3. Captura de tráfico

La captura de tráfico de red es necesaria para alimentar un conjunto de datos para posteriormente entrenar un modelo de inteligencia artificial, por lo cual se plantean dos escenarios:

Red estado normal

Se realiza la captura del tráfico de la red bajo un comportamiento normal, este proceso se lleva a cabo desde el dispositivo Rasberry, donde se ejecuta un script que utiliza la librería Tshark de Wireshark el cual realiza la captura de tráfico y la guarda en un dispositivo de almacenamiento. La captura fue realizada por un lapso de 20 horas en total. (*ver figura 13*)

Figura 13. Archivos .cap obtenidos de captura de tráfico normal.

Red bajo ataque

El proceso de captura de tráfico es igual al de la red en estado normal, sin embargo, durante este proceso se efectúa el ataque de parte del host malicioso al servicio DHCP en lapsos de 5 minutos durante 1,5 horas. (*ver figura 14*)

Figura 14. Archivos .cap obtenidos de captura de tráfico bajo ataque

Los scripts utilizados para la captura del tráfico fueron los siguientes:

>tshark -i eth0 -w ./CapturaTemporal.cap -a duration:60

>tshark -2 -R "dhcp" -r ./CapturaTemporal.cap -t ud -T fields -e _ws.col.No. -e _ws.col.Time -e _ws.col.Fecha -e _ws.col.Source -e _ws.col.Destination -e _ws.col.Protocol -e _ws.col.Length -e _ws.col.Info -E quote=d -E occurrence=f -E header=y -E separator=, > ./CapturaTemporal.csv

Una vez obtenidos los archivos de tráfico con formato .cap se procedió a convertir y transformar dicha información en .csv con el fin de ser interpretada por el aplicativo en Python que procesará los datos. Para esto se creó un script capaz de

tomar todos los archivos .cap y transformarlos a .csv extrayendo la información relevante y que será útil para nuestra investigación. (*ver figura 15*)

```
import os
import pathlib
import subprocess
from os import system

def cmd(commando):
            subprocess.run(commando, shell=True)
            # parzibyte.me/blog
            from subprocess import check_output


Normal_dir = 'Normal/'
Ataque_dir = 'Ataque/'
print("********Iniciando... Directorio de capturas de trafico en estado normal")
with os.scandir(Normal_dir) as ficheros:
    ficheros = [fichero.name for fichero in ficheros if fichero.is_file() and fichero.name.endswith('.cap')]
    for x in range(0,len(ficheros)):
        print(str(x) + " de "+str(len(ficheros))+" Iniciando convercion de => "+ficheros[x])
        system('tshark -2 -R "dhcp" -r Normal/'+ficheros[x]+' -T fields -e _ws.col.No. -e _ws.col.Time -e _ws.col.


print("********Iniciando... Directorio de capturas de trafico durante ataque")
with os.scandir(Ataque_dir) as ficheros:
    ficheros = [fichero.name for fichero in ficheros if fichero.is_file() and fichero.name.endswith('.cap')]
    for x in range(0,len(ficheros)):
        print(str(x) + " de "+str(len(ficheros))+" Iniciando convercion de => "+ficheros[x])
        system('tshark -2 -R "dhcp"  -r Ataque/'+ficheros[x]+' -T fields -e _ws.col.No. -e _ws.col.Time -e _ws.col
```

Figura 15. Script de conversión .cap a .csv

Una vez se convierte el trafico capturado a .csv se obtienen los siguientes archivos que alimentarán el modelo de aprendizaje automático convirtiéndose en su conjunto de datos. Como lo vemos en la siguiente figura. (*ver figura 16*)

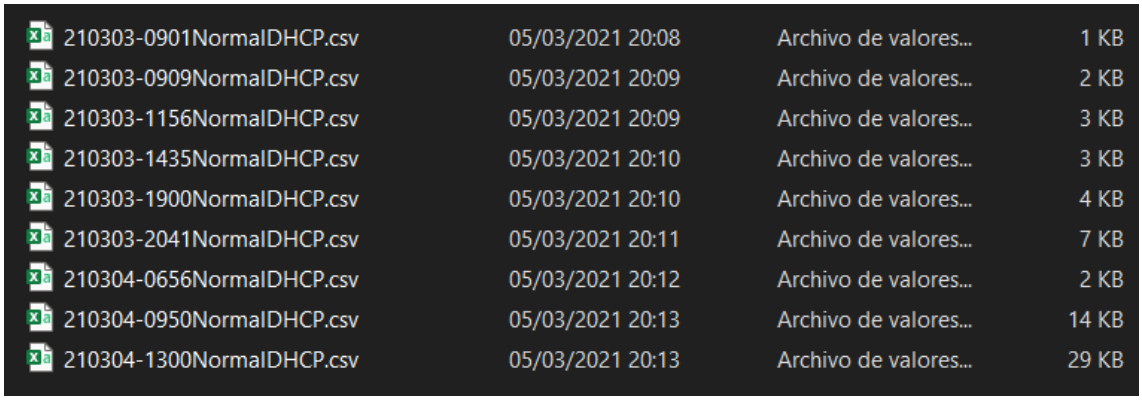

Figura 16. Archivos .csv

3. DISEÑO DE MODELO DE APRENDIZAJE AUTOMATIZADO

3.1. Limpieza de los datos

Luego de capturar el tráfico de la red y ser convertido en conjuntos de datos .csv se procede a la unificación en un solo dataframe el cual se manipula y se le aplican algunas técnicas de limpieza de datos que permiten optimizar el conjunto de información que se tiene. Para la segmentación de los datos se utilizaron múltiples librerías en Python que ayudaron a filtrar los datos de tipo DHCP y dividir las peticiones en cantidades de tiempo determinadas y generar registros que aporten información extraíble del comportamiento de la red. (*ver figura 17*)

```
# Strip spaces at the beginning and the end of column names
dfCapturaDeTrafico_Normal.columns = dfCapturaDeTrafico_Normal.columns.str.strip()
dfCapturaDeTrafico_Ataque.columns = dfCapturaDeTrafico_Ataque.columns.str.strip()

# Shape of data before cLeaning
dfCapturaDeTrafico_Normal.shape
dfCapturaDeTrafico_Ataque.shape
```

Figura 17. Instrucciones de limpieza de los datos.

Se procesa la información filtrando el tráfico DHCP y segmentando los registros en lapsos de tiempo con el fin de obtener la cantidad de peticiones DHCP realizadas (*ver tabla 2*).

Tabla 2. Funciones candidatas para detectar el ataque IPv4.

Características	Descripción	Tipo
Discover	Número de DHCPDISCOVER	Numérico
Offer	Número de DHCPOFFER	Numérico
Request	Número de DHCPREQUEST	Numérico
Ack	Número de DHCPACK	Numérico

Después de múltiples capturas se determinaron las variables anteriormente mencionadas, ya que los ataques realizados mostraban un aumento de peticiones de este tipo. Por lo cual se planteó estructurar un set de datos como lo muestra la siguiente tabla donde los valores de los correspondientes intervalos de tiempo perteneciente al flujo de la red en estado normal *(ver tabla 3)*.

Tabla 3. Registros de peticiones al protocolo DHCP por lapsos de tiempo

Intervalo	DISCOVER	OFFER	REQUEST	ACK	ATAQUE
1	22	34	2	0	0
2	12	2	3	7	0
3	6	7	8	0	0

3.2. Construcción de modelo

Se plantearon dos modelos de aprendizaje automatizado, Supervisado y no supervisado, esto con el fin de realizar una comparación y evaluar cual tiene una mejor efectividad.

3.3. Supervisado (RandomForest)

En la fase de clasificación, los registros de datos obtenidos de la etapa de preprocesamiento se clasifican como datos normales o de ataque. La fase de clasificación se divide en entrenamiento y período de prueba. En el período de entrenamiento, enseñamos al modelo teniendo en cuenta los registros de la red

durante un ataque o en estado normal. Una vez que se entrena el modelo de detección, probamos el modelo con un conjunto de datos nuevo o desconocido durante el período de prueba donde cada registro fue capturado en un entorno en tiempo real, como lo muestra la figura 18. (*ver figura 18*)

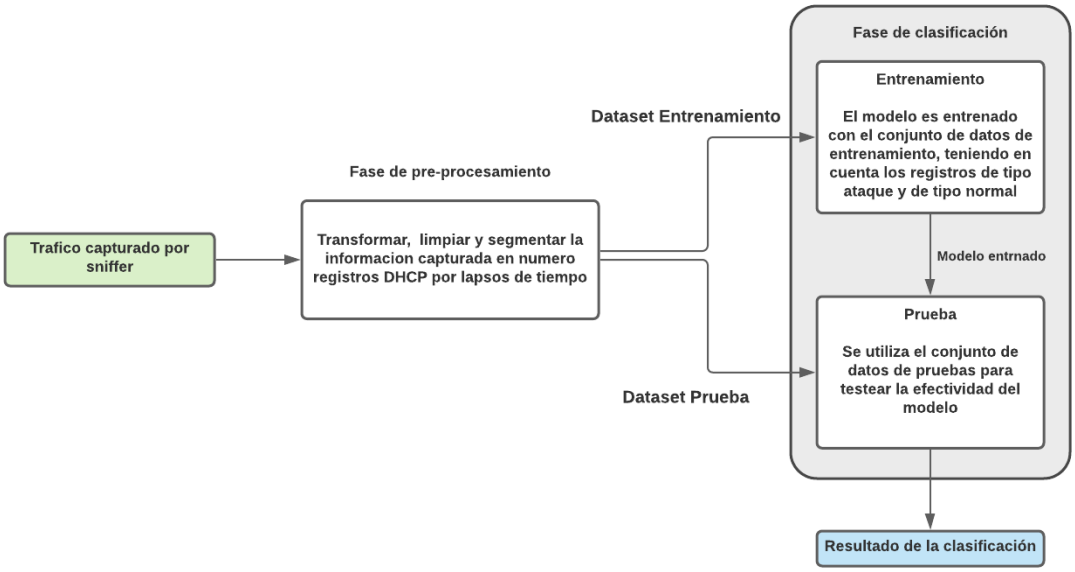

Figura 18. Marco propuesto para la detección de ataques con método RandomForest

Tabla 4. DataSet de consultas al protocolo DHCP normal y ataque.

Intervalo	Discover	Offer	ACK	Request	Ataque
0	0.0	0.0	1.0	1.0	0
1	0.0	0.0	1.0	1.0	0
2	1.0	1.0	1.0	1.0	0
3	0.0	0.0	1.0	1.0	0

4	1.0	1.0	1.0	1.0	0
...	...	...	...	...	...
17	90070.0	88.0	1.0	1.0	1
18	154568.0	86.0	0.0	0.0	1
19	161259.0	87.0	0.0	0.0	1
20	174610.0	87.0	0.0	0.0	1
21	147627.0	87.0	0.0	0.0	1

Para el entrenamiento del modelo se utilizó un 70% de los datos y un 30% la división de los datos se realizó utilizando la función train_test_split de la biblioteca sklearn, con una división estratificada y una aleatorización de 42. Posterior a esto se realizó la configuración de los hiperparametros del modelo para el cual se definió una profundidad del árbol máximo de dos con una aleatorización completa y se realizó el proceso de entrenamiento con el 70% de los datos.

Para verificar los resultados del modelo se utilizó la función *predict* que proporciona la misma librería a la cual se le envía el conjunto de datos no utilizado en el entrenamiento, esto se usa para garantizar que el modelo sea lo suficientemente generalizado y permita predecir con datos desconocidos.

3.4. No supervisado (OneClassSVM)

Para el diseño del modelo no supervisado se utilizó la librería OneClassSVM y se estructura un esquema de aprendizaje de la siguiente forma:

En la fase de clasificación, los registros de datos obtenidos de la etapa de preprocesamiento se clasifican como datos normales o de ataque. La fase de clasificación se divide en entrenamiento y período de prueba. En el período de entrenamiento, enseñamos al modelo teniendo en cuenta los registros de la red en estado normal. Una vez que se entrena el modelo de detección, probamos con un conjunto de datos nuevo o desconocido durante el período de prueba donde cada registro fue capturado en un entorno en tiempo real, como lo muestra la figura 19. (*ver figura 19*)

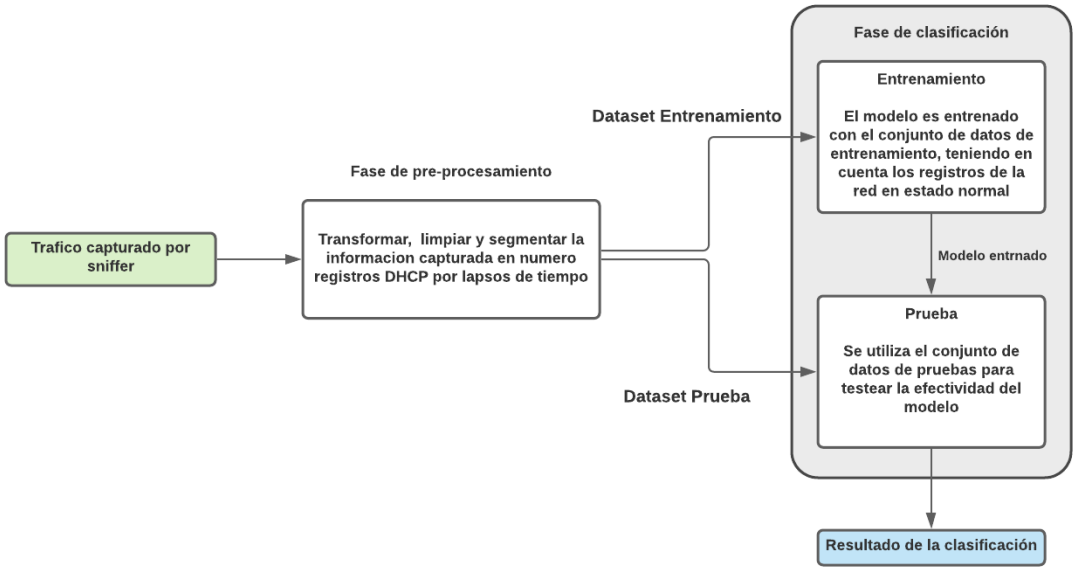

Figura 19. Marco propuesto para la detección de anomalías

Ya que se trata de un modelo no supervisado solo se entrenó con registros de la red en estado normal. (*ver tabla 5*)

Tabla 5. DataSet de consultas al protocolo DHCP normal

Intervalo	Discover	Offer	ACK	Request	Ataque
0	0.0	0.0	1.0	1.0	0
1	0.0	0.0	1.0	1.0	0
2	1.0	1.0	1.0	1.0	0
3	0.0	0.0	1.0	1.0	0
4	1.0	1.0	1.0	1.0	0

En la figura 9 podemos observar como el modelo ayuda a identificar esas anomalías presentes en los registros clasificando el tráfico normal de la red y cuando hay un dato anómalo, como lo muestra la figura 20. (*ver figura 20*)

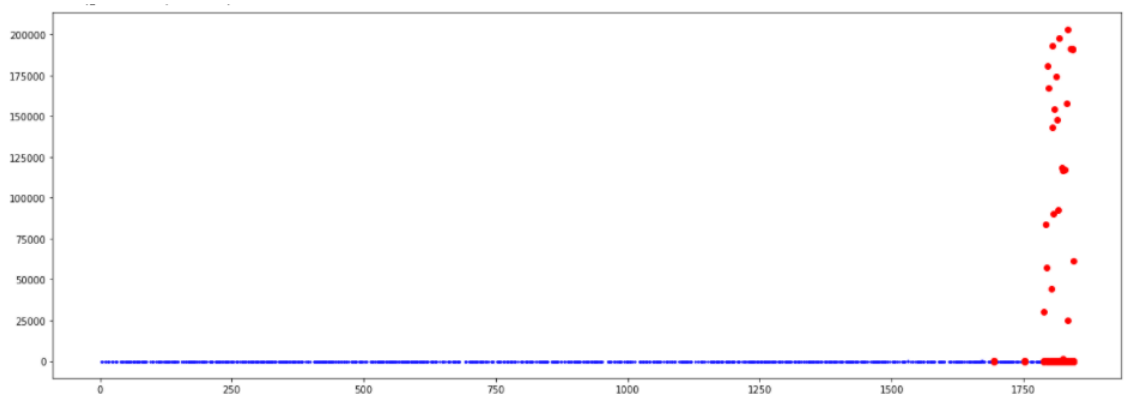

Figura 20. Gráfica de detección de datos anómalos.

Para verificar los resultados del modelo se utilizó la función *predict* que proporciona la misma librería a la cual se le envía el conjunto de datos no utilizado en el entrenamiento, esto se usa para garantizar que el modelo sea lo suficientemente generalizado y permita predecir con datos desconocidos.

4. RESULTADOS Y DISCUSIÓN

4.1. Evaluación de desempeño

Para evaluar el desempeño de los modelos diseñados se realizan predicciones a conjuntos de datos que no hayan sido con los que aprendió, para así calificar el porcentaje de efectividad de cada modelo, a continuación, se muestran las pruebas realizadas con cada modelo, en la cual se observan los valores obtenidos y que tan factible son para la detección de ataques de denegación de servicios al protocolo DHCP.

Adicional también se realizará la implementación de los modelos de forma muy simple en Python con el fin de realizar una prueba de concepto y experimentar el funcionamiento en la práctica y como este modelo interactúa con el flujo de la red en estado normal y durante un ataque.

4.2. Resultado con RandomForest

El modelo tiene una precisión del 98%, un 100% de probabilidades para detectar ataques de un y un 96% de detectar que la red se encuentra en estado normal. Los resultados obtenidos son positivos. (*ver figura 21*)

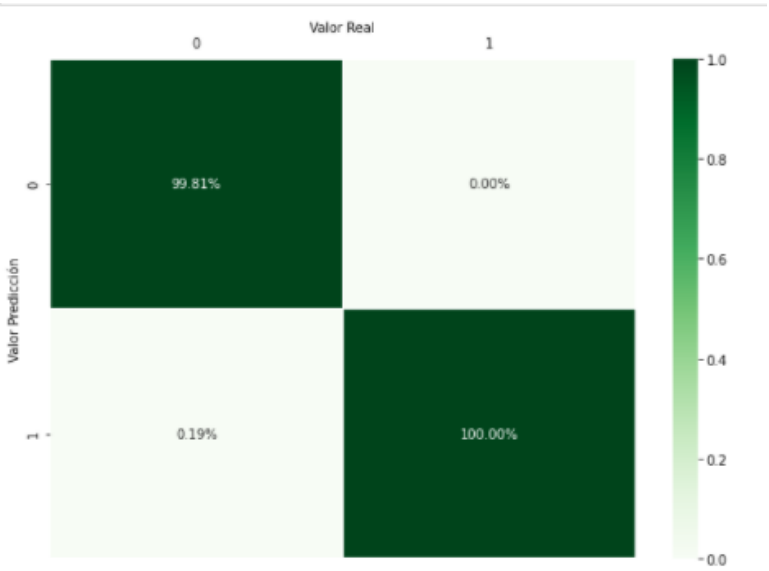

Figura 21. Matriz de confusión RandomForest

	precision	recall	f1-score	support
0	1.00	1.00	1.00	537
1	1.00	0.94	0.97	17
accuracy			1.00	554
macro avg	1.00	0.97	0.98	554
weighted avg	1.00	1.00	1.00	554

Figura 22. Métricas de modelo RandomForest

4.3. Modelo no supervisado (OneClassSVM)

El modelo tiene una precisión de casi el 100%, un 100% de probabilidades para detectar ataques de un y un 99% de detectar que la red se encuentra en estado normal. Los resultados obtenidos son positivos. (*ver figura 23*)

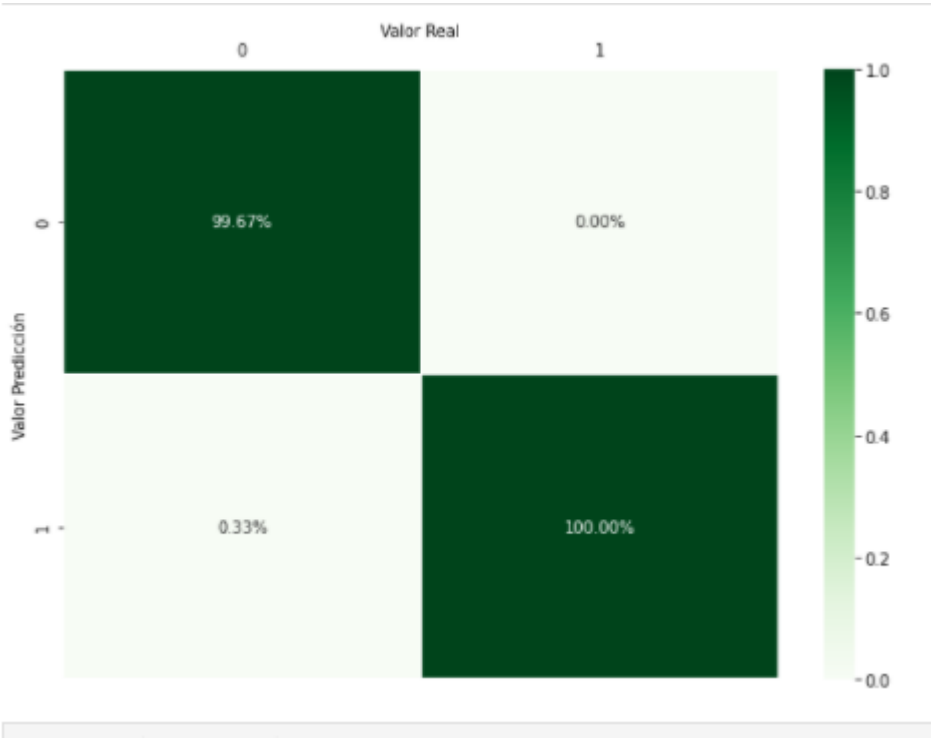

Figura 23. Matriz de confusión OneClassSVM

	precision	recall	f1-score	support
0	1.00	1.00	1.00	895
1	1.00	0.89	0.94	28
accuracy			1.00	923
macro avg	1.00	0.95	0.97	923
weighted avg	1.00	1.00	1.00	923

Figura 24. Métricas de modelo OneClassSVM

4.4. Implementación de modelos

Para la implementación de los modelos se creó un programa en Python capaz de capturar y procesar el tráfico de la red para luego clasificar la información e identificar ataques. Este script captura el tráfico por un minuto, aplica las segmentación y limpieza de datos correspondientes, suministra el conjunto de

datos al modelo para que este evalué si se trata de un ataque o no y lance una alerta en caso de ser positivo.

Al ejecutar el script inicia su proceso de procesamiento de tráfico, en la siguiente figura vemos como la red se encuentra en un estado normal y programa no se altera, durante ese minuto no se realizó ninguna petición de tipo DHCP. (*ver figura 25*)

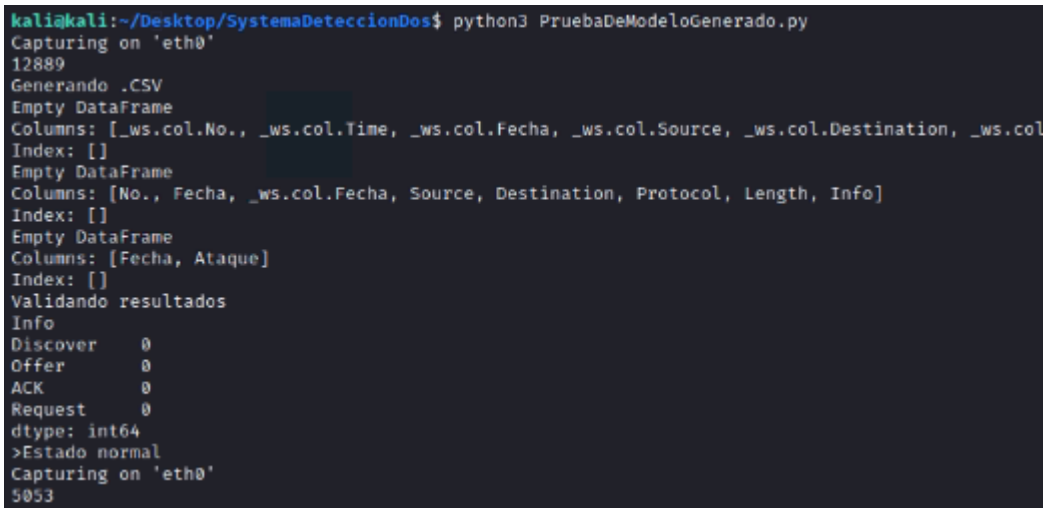

Figura 25. Aplicación RandomForest

Se realiza un ataque mientras se encontraba ejecutando la aplicación y fue capaz de detectar el ataque de denegación de servicio y enviar un correo de alerta como lo muestra la siguiente figura. (*ver figura 26*)

```
[81911 rows x 8 columns]
Info              Fecha  ACK  Discover  Offer  Request  Ataque
0     2021-05-07 19:55  1.0   44041.0   93.0      2.0       0
1     2021-05-07 19:56  1.0   37772.0    0.0      1.0       0
Validando resultados
Info
Discover    81813.0
Offer          93.0
ACK             2.0
Request         3.0
dtype: float64
>¡Ataque DoS Detectado!
successfully sent email to brandon.perez.lara@gmail.com:
Capturing on 'eth0'
152
```

Figura 26. Aplicación RandomForest durante ataque

Para efectos de experimentación se ejecutan ambos modelos de forma simultanea con el fin de identificar como es su comportamiento y probar si son capaces de detectar un ataque de denegación de servicios en el momento en que se encuentra ocurriendo. (*ver figura 27*)

```
kali@kali: ~/Desktop/SystemaDeteccionDos
File  Actions  Edit  View  Help
kali@kali:~/Desktop/SystemaDeteccionDos$ python3 PruebaDeModeloGenerado.py
Iniciando Captura: SUPERVISADO
Capturing on 'eth0'
2272
Generando .CSV
Empty DataFrame
Columns: [Fecha, Ataque]
Index: []
Validando resultados
Info
Discover    0
Offer       0
ACK         0
Request     0
dtype: int64
>Estado normal
---
Iniciando Captura: SUPERVISADO
Capturing on 'eth0'
8885
```

Figura 27. Aplicación de modelo supervisado

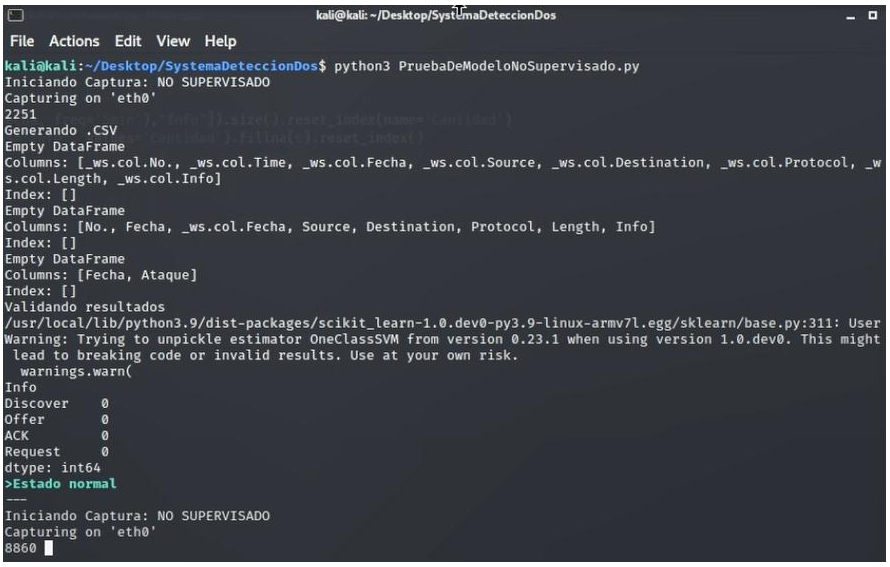

Figura 28. Aplicación no supervisado.

Al realizar el ataque ambos modelos lo detectan y lanzan una alerta por correo de la eventualidad ocurrida, además escribe el suceso en el archivo de logs de la aplicación donde adjunta la fecha del instante en el que ocurre. (*ver figura 29*)

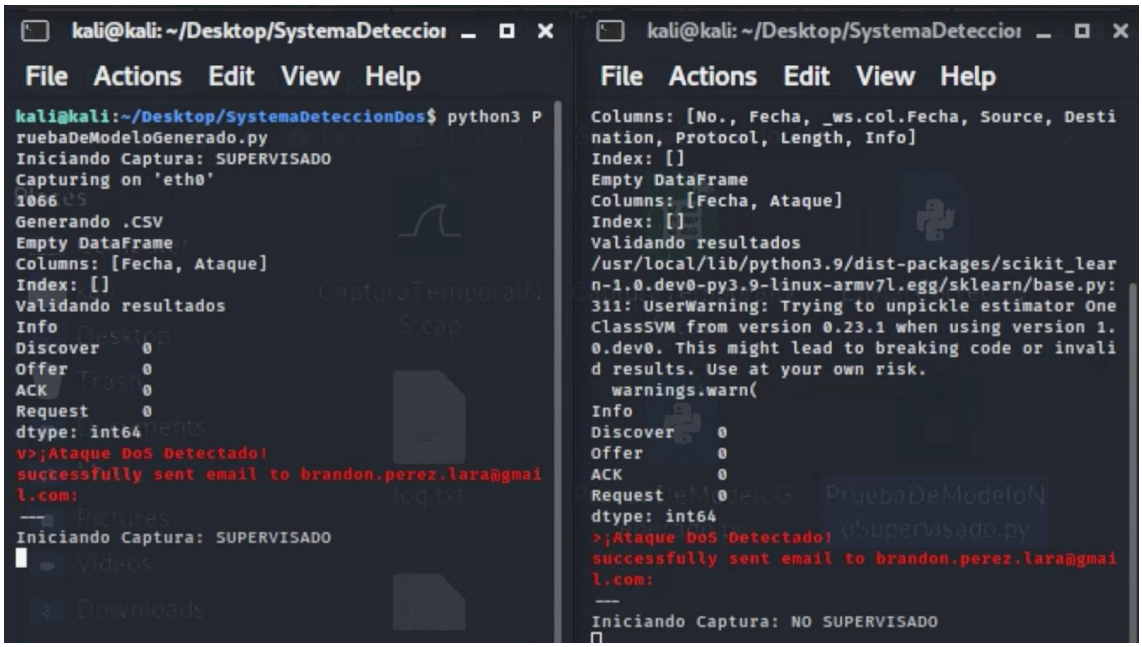

Figura 29. Detección de ataque de denegación de servicio

.

Como podemos observar en la bandeja de entrada se encuentra el correo de alerta de ataque y en el archivo de texto el registro se agrega una nueva línea. (*ver figura 30*)

Figura 30. Correo de alerta

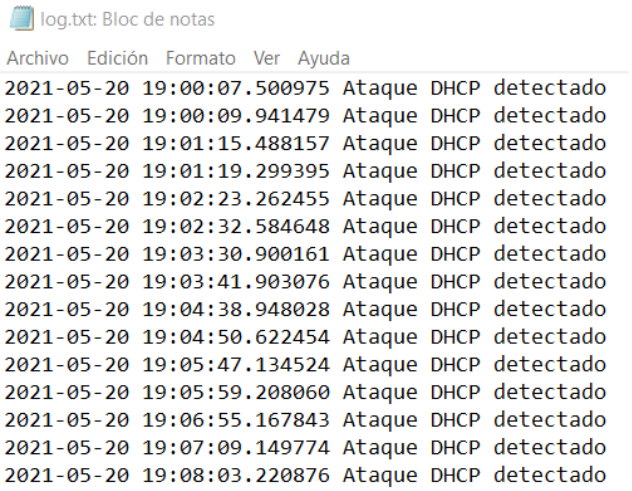

Figura 31. Log de ataques de anomalías detectadas.

DISCUSIÓN

En relación con la investigación realizada se logró la aplicación de inteligencia artificial en técnicas de detección de ataques de denegación de servicio al protocolo DHCP. Se llevó acabo la implementación de dos modelos de detección (supervisado y no supervisado) en un laboratorio de red controlado, con ambos modelos se obtuvieron resultados positivos por encima del 98% de asertividad, y se logró realizar la comparación entre ambos. Fueron utilizadas metodologías para la creación del modelo con una sola clase, esto implica que solo utilizando el trafico normal de la red se identifican situaciones anormales que pueden ser catalogadas como ataques de denegación de servicio. Además, se exportan estos modelos para ser implementados en tiempo real diseñando una aplicación capaz de notificar cuando el modelo detecta una anomalía.

De acuerdo a lo logrado en el proyecto se abre la puerta a investigadores que busquen profundizar e indagar en la aplicación de técnicas de inteligencia artificial en la detección de ataques en la red y el desarrollo de software orientado a la seguridad, ya que este es un problema que seguirá en aumento y se necesitan nuevas formas y metodologías de detección.

CONCLUSIONES Y RECOMENDACIONES

En este artículo se propuso un marco de detección de anomalías basado en inteligencia artificial para detectar ataques de denegación de servicios por agotamiento del protocolo DHCP. El marco utiliza clasificadores que permiten identificar comportamientos anómalos en diferentes intervalos de tiempo. Probamos el rendimiento de detección del marco propuesto en redes IPv4 utilizando tráfico capturado de una red que conectaba múltiples dispositivos y se demostró que el marco puede detectar el ataque propuesto con una precisión muy alta.

Este proyecto espera motivar a los investigadores en la búsqueda de nuevas metodologías de detección de vulnerabilidades y ataques con el fin de disminuir los vectores de amenaza a los que se enfrenta la presente generación informática.

Bibliografía

1. Fernández, M. (2020, 14 febrero). Ciberataques que matan a las empresas. EL PAÍS. https://elpais.com/economia/2020/02/14/actualidad/1581694252_444804.html

2. Mitigation of DHCP starvation attack. (2012, 1 septiembre). ScienceDirect. https://www.sciencedirect.com/science/article/abs/pii/S0045790612001140

3. Younes, O. S. (2016, 15 enero). A Secure DHCP Protocol to Mitigate LAN Attacks. Journal of Computer and Communications. https://www.scirp.org/journal/paperinformation.aspx?paperid=63134

5. Departamento nacional de planeación, D. N. E. (2019). Objetivos de desarrollo sostenible. https://www.ods.gov.co/es/objetivos/industria-innovacion-e-infraestructura

6. DDOS and web application attack stats infographic (2017). Akamai

6. Tripathi, N., & Hubballi, N. (2017). Detecting stealth DHCP starvation attack using machine learning approach. Journal of Computer Virology and Hacking Techniques, 14(3), 233-244. https://doi.org/10.1007/s11416-017-0310-x

7. Configuración de una Red Local. Rubén, Balirac Seijas. madrid : Instalación y Configuración de Computadores y Periféricos, mayo 2016.

8. Urueña Centeno, F. J. (2015). CIBERATAQUES, LA MAYOR AMENAZA ACTUAL. Instituto Español de Estudios Estrategicos, 1-18. https://d1wqtxts1xzle7.cloudfront.net/51097771

9. Lopez, J. Sistema de deteccion de ataques EDoS en entorno cloud. Cundinamaca : s.n., 2015.

10. Unb.ca. 2020. IDS 2017, Datasets, Research, Canadian Institute For Cybersecurity, UNB. [online] Available at: <https://www.unb.ca/cic/datasets/ids-2017.html> [Accessed 27 October 2020].

11. Pérez Porto, J. and Merino, M., 2012. Definición De Tráfico — Definicion.De. [online] Definición.de. Available at: <https://definicion.de/trafico/> [Accessed 27 October 2020].

12. Cerdan Lopez, Juan Francisco. Administración de sistemas corporativos basados en Windows 2012. Server. Protocolos de red. [En línea] 2015.

13. Barrios, Fernanda. El protocolo DHCP y su funcionamiento. [En línea] 2017. https://www.ugr.es/~fernanla/Untitled.pdf.

14. Q. funciona, "El DHCP y la configuración de redes", IONOS Digitalguide, 2020. [Online]. Available: https://www.ionos.es/digitalguide/servidores/configuracion/que-es-el-dhcp-y-como-funciona/. [Accessed: 27- Oct- 2020].

15. Altunbasak, H.C. Layer 2 Security Inter-Layering in Networks. Georgia Institute of Technology, Atlanta. (2006)

16. P. Meseguer González y Ramon López de Mántaras Badia, Inteligencia artificial. Madrid: Editorial CSIC Consejo Superior de Investigaciones Científicas, 2017.

17. "Aprendizaje automático para detección de anomalías - sitiobigdata.com", sitiobigdata.com, 2019.

18. E. F. Caicedo Bravo y J. A. López Sotelo, Una aproximación práctica a las redes neuronales artificiales. Programa Editorial Universidad del Valle, 2009.

19. E. Universidad Internacional de Valencia, "¿Qué es un sniffer? | VIU", Universidadviu.com, 2020.

20. 27. implementación de controles en una LAN para mitigar los ataques del DHCP utilizando las mejores prácticas del diseño de redes. Cecilia, Auz Cadena Fabiola. 29, manchala: Unidad Académica De Ingeniería Civil, 2019, Vol. 1.