UNIVERSIDAD ESTATAL

PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍA DE LA INFORMACIÓN

TRABAJO DE INTEGRACION CURRICULAR

previo a la obtención del título de:

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

“Desarrollar un algoritmo para el control de peticiones Web mediante código Python para la detección de trafico de red anómalo para una empresa de productos enlatados”

AUTOR

JOSÉ DANIEL GÓMEZ RUIDIAZ

PROFESOR TUTOR

Lsi. DANIEL QUIRUMBAY YAGUAL, MSIA

LA LIBERTAD – ECUADOR

2022

AGRADECIMIENTO

Primero agradecer a dios por haber guiado el camino, por haber brindado la sabiduría y la fuerza para afrontar los problemas que se me presento en el camino y permitiendo cumplir unos de mis objetivos que me propuse desde el comienzo de la carrera universitaria.

A mi madre Nancy Ruidiaz Yagual, por ser madre y padre a la vez, por haberme apoyado en estos años, por ser mi fortaleza, por llenarme de sabiduría y por darme los consejos que necesite para no rendirme y seguir hasta el final.

A mi hermano Ángel Gómez por ser esa persona que siempre escucho, quien siempre me ayudo a buscar una solución ante un problema.

A mis abuelos, María Yagual y Moisés Ruidiaz, por ser los promotores de la sabiduría, por darme consejos, y estar en los momentos difíciles.

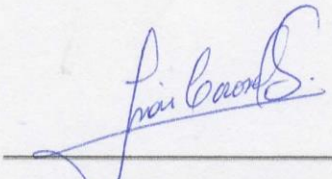
A los docentes de la facultad de Sistemas y Telecomunicaciones por impartir los conocimientos, sus experiencias para poder alcanzar el objetivo.

Un agradecimiento al Msc. Daniel Quirumbay Yagual, por ser un guía desde que comenzó en la elaboración del algoritmo, siendo parte fundamental para culminación de este proyecto.

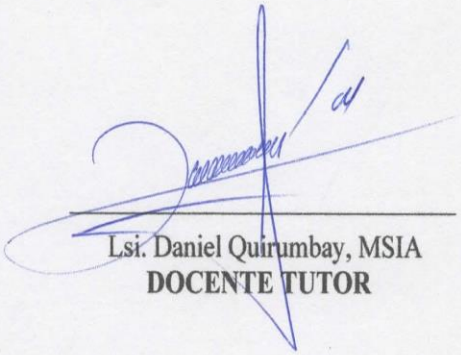
Gómez Ruidiaz José Daniel

TRIBUNAL DE GRADO

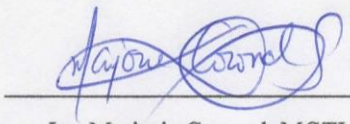
Ing. Jaime Orozco I, MGT
DIRECTOR DE CARRERA



Ing. Iván Coronel S, MSIA
DOCENTE ESPECIALISTA



Lsi. Daniel Quirumbay, MSIA
DOCENTE TUTOR



Ing.Marjorie Coronel, MGTI
DOCENTE GUÍA UIC

APROBACIÓN DEL TUTOR

En calidad de Tutor de trabajo de titulación denominado: **"Desarrollar un algoritmo para el control de peticiones Web mediante código Python para la detección de trafico de red anómalo para una empresa de productos enlatados"**, elaborado por el estudiante **Gómez Ruidiaz José Daniel,** de la carrera de Tecnología de Información de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes y autorizo al estudiante para que inicie los trámites legales correspondientes.

La Libertad, agosto del 2022

Lsi. Daniel Quirumbay Yagual, MSIA.

RESUMEN

La empresa de productos enlatados es una de la empresa exportadora de sardina que tiene como destino a países como Chile, México, Costa Rica y Estados Unidos, su objetivo principal es expandirse a más países en la venta de sus productos enlatados y poder abarracar más mercados internacionales brindando la calidad que sugieren el mercado internacional. La empresa carece de software que le permita identificar malwares dentro de su tráfico de red, por lo que tardan en identificar un ataque o infección a la infraestructura de la red, por lo que se propone en desarrollar un algoritmo para la identificación de malware dentro del tráfico de red y enviar notificaciones a la red social telegram en caso de encontrar alguna anomalía.

El algoritmo está desarrollado en el lenguaje de Python por lo que usa librerías para la captura de datos como es el caso de Pyshark, también usa librería de comunicación como Request que es el medio de la cual nos comunica con la red social de Telegram, además de incorporar APIS que son esenciales para recibir los datos que nos proporciona VirusTotal y el BOT de telegram, adicional se usa una librería de DASH que es para la elaboración de un reporte en formato de HTML para la visualización estadística de los reporte de anomalías dentro del tráfico de red en un día especifico. Como resultado final se obtuvo un algoritmo que captura tramas de red dentro de una infraestructura de red.

Palabra clave: Algoritmo, Python, Tráfico anómalo, Seguridad web.

ABSTRACT

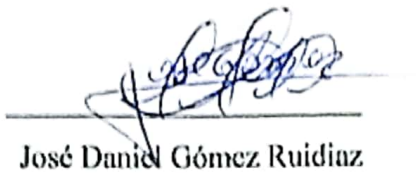
The canned products company is one of the sardines exporting company that is destined for countries such as Chile, Mexico, Costa Rica and the United States, its main objective is to expand to more countries in the sale of its canned products and to be able to cover more markets. offering the quality suggested by the international market. The company lacks software that allows it to identify malware within its network traffic, so it takes time to identify an attack or infection to the network infrastructure, so it proposes to develop an algorithm for the identification of malware within the network. network traffic and send notifications to the telegram social network in case of finding any anomaly.

The algorithm is developed in the Python language, so it uses data capture libraries such as Pyshark, it also uses a communication library such as Request, which is the means by which it communicates with the Telegram social network, in addition to incorporate APIs that are essential to receive the data provided by VirusTotal and the Telegram BOT, an additional DASH library is used that is for the elaboration of a report in HTML format for the statistical visualization of the anomaly reports within the network traffic on a specific day. As a result, an algorithm that captures network frames within a network infrastructure was obtained.

Keywords: Algorithm, Python, Abnormal traffic, Web security.

DECLARACIÓN

El contenido del presente Trabajo de Graduación es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.



José Daniel Gómez Ruidiaz

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

El presente proyecto tiene como propósito el desarrollo de un algoritmo para el control de peticiones Web para la empresa de productos enlatados, en esta institución se implementará el script en unos de los servidores para la captura de datos dentro de la trama de red, el mismo que será almacenado en una base de datos para su posterior análisis en forma estadística para una mejor toma de decisiones.

En el capítulo 1 se explica la información de la empresa, como también la problemática que presenta al momento de recopilar la información, también se detalla sobre las metodologías que se van a emplear para la ejecución del algoritmo como una breve descripción del contenido de cada fase que va a contener el proyecto para su implementación.

En el capítulo 2 trata principalmente en el desarrollo del proyecto que cuenta con marco contextual, conceptual y teórico como también el desarrollo de las fases junto con las evidencias de cada fase lo amerita y dando como resultado las pruebas del sistema y los resultados obtenido en la ejecución.

CAPITULO I

1. FUNDAMENTACIÓN

1.1. ANTECEDENTES

Mientras el covid-19 se propaga por el mundo, los piratas informáticos aprovechan esta situación para expandir virus que afectan tanto a las empresas como a los usuarios del hogar. Ecuador no se libra de estos programas maliciosos [1]. Según la empresa de seguridad Kaspersky, nuestro país se ha mantenido en la posición 49 dentro de las estadísticas de países con mayores incidencias de software malicioso o malware [1].La modalidad del teletrabajo, por la pandemia, trajo consigo un mayor número de ataques [1]. En Ecuador, el informe 'ESET Security Report 2020 de Latinoamérica' indica que el 70% de las empresas que trabajan con esta marca de antivirus en el país reportó incidentes de seguridad [1].

La empresa de productos enlatados tiene como meta principal, colocar sus productos en el mercado internacional y poder ocupar unos de los primeros lugares en la exportación de estos alimentos enlatados. Actualmente esta empresa tiene como destino de sus productos los países: Chile, Estados Unidos, Guatemala, Costa Rica y México. (Ver Anexo 1) Esta empresa fue fundada el 25 de noviembre del 2015, comenzando con la elaboración de atún y sardina, en la actualidad solo importa sardinas, pero con diferentes formas de consumirlas dependiendo del país de destino.

El Lcdo. Iván León jefe de recurso humanos de la empresa de productos enlatados, en la entrevista realizada (ver anexo 1), nos explica que la empresa cuenta con personal que son fijos y eventuales, no todos deberían tener acceso a internet porque la empresa tiene una política de seguridad la cual es que no se deben ingresar dispositivos móviles, política que no se cumple porque el personal ingresa estos artefactos obteniendo acceso a la red por medio de la contraseña y sin ninguna restricción.

El Ing. Miguel Delgado del área de TI de la empresa de enlatados, en la entrevista realizada (ver anexo 2), nos comenta que en control de los sitios webs no se realiza de manera correcta, los empleados no tienen ninguna restricción en su navegación y tampoco un control de los archivos que descargan.

También nos menciona que no tienen un programa que permita ver cuál es un tráfico normal de red, y los equipos que tiene la empresa no permite cumplir con los roles de

seguridad que debería tener sus sistemas, dando acceso a malware que acceso que sus equipos no sean eficientes.

Un estudio realizado en la Universidad Autónoma de Madrid (UAM) de la Ciudad de España con el tema de “Contribución al análisis del tráfico de Internet” [2]. En este proyecto nos explicó cómo analiza el tráfico de red a través de algoritmos para detectar peticiones que realiza un usuario de forma anómala, sin embargo, no realiza un aviso en tiempo real a una red social.

Otro proyecto que podemos tomar como referencia es de la Universidad Pedagógica y Tecnológica de Colombia, con el tema “Estudio del tráfico de red por medio de un análisis estadístico de los paquetes de datos que viajan a través de los diferentes nodos y hacia cada uno de los usuarios que posee la empresa "FSD S.A.S."” [3], este proyecto analiza el tráfico de red de cada nodo que posee la empresa, usando aplicaciones ya desarrolladas para poder determinar que tráfico es anómalo, pero este proyecto utiliza herramientas muy limitadas que no permite el envío de avisos al usuario.

En la Universidad de la Fuerzas Armadas (ESPE) de la ciudad de Sangolquí, Ecuador con el tema “Análisis de tráfico de datos en la capa de enlace de una Red LAN, para la detección de posibles ataques o intrusiones sobre Tecnologías Ethernet y WIFI 802.11” [4]. En esta tesis el análisis de red lo realiza con la herramienta WIRESHARK, para identificar el tráfico que realiza una empresa e identificar cual es un tráfico anómalo que pueda impedir un funcionamiento óptimo de los servicios, pero las herramientas que usa son muy limitadas y no permite la notificación sobre un tráfico anómalo

Después de describir proyectos antes mencionados y de explicar la problemática que presenta la empresa, se desea implementar un algoritmo de control de peticiones de https, para reconocer que tramas de red vienen con anomalías detrás de una navegación web y poder notificar en tiempo real al encargado de TI.

1.2. DESCRIPCIÓN DEL PROYECTO

El proyecto consiste en desarrollar un mecanismo de análisis de peticiones Https para evitar que malware ingresen al sistema, para eso se va a recopilar la información de que servicios y equipos se encuentra implementado en la institución, además reconocer que

tipos de vulnerabilidades, presentan en el momento de recopilar los datos, también se solicitará los mecanismos que tiene implementado ante un riesgo de seguridad de TI.

El presente proyecto se adaptará en la ISO 27032 y constará de las siguientes fases:

Fase 1 Entendimiento de la Organización: En esta fase se va a revisar los productos y servicios que actualmente utiliza la empresa, además de revisar la documentación de seguridad que ellos están utilizando. Se observará las medidas técnicas de seguridad que están implementando. Toda esta información se va a obtener a través de entrevistas y por el uso de aplicaciones que nos permitirá recopilar datos.

Fase 2 Análisis de Riesgos La fase permitirá encontrar amenazas que actualmente existe en la organización, además de vulnerabilidades que presentan al momento de obtener la información y luego comparar los datos con información que se encuentre publicado en sitios oficiales.

Fase 3 Plan de Acción: Se va a reestructurar las políticas de seguridad que actualmente tienen implementada, además de identificar que otros roles deberá cumplir el personal de TI.

Fase 4 Implementación: Se implementará las medidas de seguridad antes mencionada en las anteriores fases junto con la herramienta que va a monitorear las peticiones Web que utilizan otras áreas, con esto van a tener un reporte en tiempo de real de algún malware que quiera comprometer algún servicio.

Este proyecto contribuirá con la línea de investigación Tecnología y Sistemas de la Información (TSI) con la sub - línea de investigación TSI en las organizaciones y en la sociedad debido que la propuesta está relacionada con temas de seguridad de las tecnologías de la información, virtualización, seguridad de la información que permitan generar información indispensable para la toma de decisiones [5].

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Desarrollar un algoritmo para el control de peticiones Http y Https mediante código Python para la detección malware en un tráfico de red en una empresa de productos enlatados.

1.3.2. OBJETIVOS ESPECÍFICOS

- Recopilar la información de los equipos que estén conectados en la red para verificar que tipos de vulnerabilidades puedan tener.
- Proponer normativas de seguridad para garantizar el correcto funcionamiento del sistema y prevenir problemas de seguridad.
- Evidenciar de manera documental los resultados obtenidos para visualizar de forma estadística la actividad que se presenta en la trama de red.

1.4. JUSTIFICACIÓN

Las amenazas web (o amenazas online) son programas de malware que pueden atacar a un usuario cuando utilice Internet [6]. Estas amenazas basadas en el navegador incluyen una gama de programas de software malicioso diseñados para infectar los ordenadores de las víctimas [6]. La herramienta principal que se encuentra detrás de estas infecciones del navegador es el paquete de exploits, que proporciona a los cibercriminales una ruta para infectar ordenadores [6].

Las ciberamenazas mundiales siguen desarrollándose a un ritmo rápido, con una cantidad cada vez mayor de filtraciones de datos cada año [7]. En un informe de RiskBased Security, se reveló que unos alarmantes 7900 millones de registros han sido expuestos por filtraciones de datos solo en los primeros nueve meses del 2019 [7]. Esta cifra es más del doble (112 %) de la cantidad de registros expuestos en el mismo período durante el 2018 [7].

Previo a un análisis a las problemáticas que presenta la empresa se propone la implementación de un control de peticiones Https que permita la revisión de cada página web en caso de ingresos de malware de forma no autorizada con el fin de mejorar la seguridad de los sistemas y de la infraestructura que maneja la empresa.

Durante la implementación de este sistema de control se revisará toda la documentación que maneja la institución sobre seguridad para poder considerar las medidas de ciberseguridad que se está empleando ante un ataque.

El control del sistema de seguridad se realizará en tiempo real a través de un servicio de mensajería Telegram, que nos permitirá recibir la notificación ante un posible ingreso de una actividad no permitida.

La autenticación de las peticiones https se realizará por medio del servicio de virus total que tiene la base de datos de todos los reportes de eventos de seguridad, esto nos permitirá comparar que peticiones son anómalas y cual es normal para su posterior notificación al jefe de TI, además de tener todos estos datos almacenados.

Cada evento que se registre será almacenado para su posterior reporte de seguridad, esto permitirá hacer un análisis de cuanta actividad anómala puede ser transmitida durante una visita de una página web.

El tema planteado está alineado con los objetivos del Plan de Creación de Oportunidades la cual se va a describir a continuación:

Directriz 1: Soporte Territorial para la garantía de derechos.

Lineamiento territorial A. Acceso equitativo a servicios u reducción de brechas territoriales [8].

A4. Fortalecer la conectividad y el acceso a las TIC como una vía para mejorar el acceso a otros servicios [8].

Objetivos del Eje Económico [8]**.**

Objetivo 5. Proteger a las familias, garantizar sus derechos y servicios, erradicar la pobreza y promover la inclusión social [8]**.**

Política 5.5.- Mejorar la conectividad digital y el acceso a nuevas tecnologías de la población [8].

1.5. ALCANCE

El propósito del proyecto es realizar un algoritmo de control de tráfico HTTPS para una empresa de productos enlatados, que pueda tener una medida de seguridad antes los posibles ataques que la empresa pueda recibir. En el sistema va a poder recibir alertas de cualquier malware que quiera ingresar mediante métodos de comprobación de un listado de datos anómalos registrados en la base de datos.

Para lo antes mencionado va a tener las siguientes fases:

Fase 1 Entendimiento de la Organización:

- **Revisar Productos y servicios**

- **Revisar documentación de seguridad**
- **Revisar Medidas técnicas de implementación de seguridad**

Fase 2 Análisis de Riesgo:

- **Reconocer las amenazas**
- **Reconocer las vulnerabilidades**

Fase 3 Plan de Acción:

- **Reestructurar políticas de seguridad**
- **Asignación de roles del Personal de TI**

Fase 4 implementación:

- **Implementar las medidas de seguridad**
- **Implementar el control de peticiones https y monitorear**

EL análisis de las peticiones https solo se realizará para el protocolo de IPV4, también el análisis se realizará a la navegación que realiza un usuario mas no la comunicación que puede haber entre equipos. Las notificaciones que se envíen a la plataforma de Telegram no se repetirán durante el día.

1.6. METODOLOGÍAS DEL PROYECTO

Para la elaboración de lo narrado anteriormente se necesitará seleccionar una correcta metodología, que permita la gestión desde que se empieza como el progreso de las diferentes fases de acuerdo con los objetivos ya establecidos. De tal forma que se lleva un control para resolver problemas que se puedan presentar en el transcurso del desarrollo del tema.

Las metodologías que se va a emplear son la de OSMTD que es una metodología para el desarrollo del script y la ISO 27032 que es la principal para la implementación del algoritmo, en la cual nos permitirá hacer la recopilación de la información de la empresa y la posterior implementación del script.

1.6.1. METODOLOGÍAS DE LA INVESTIGACIÓN

Debido a que existen vacíos en cuanto a la información y lo relevante de los datos incluyendo la obtención de éstos, se escoge utilizar para esta investigación la metodología

exploratoria. [9] Tomando de referencia trabajos que tenga similitud o relación la implementación y control de peticiones Https para examinar las fases que se realiza antes de la culminación del proyecto.

Con el uso de esta metodología podemos obtener una perspectiva general de la funciones y procesos que se lleva a cabo en la ciberseguridad, especialmente en la protección de datos, dejando que se familiarice con los asuntos esenciales que se ejecutan para obtener una indagación profunda y dejar establecidos los requerimientos más exactos.

Para la obtención de la información importante que permita determinar el alcance del control de Https, se procederá a realizar una entrevista con el jefe de recurso humanos de la empresa de productos enlatados, quien es el beneficiario directo de la implementación. Con el fin de cumplir con los objetivos establecidos anteriormente, en esta parte de la documentación se usa la metodología de tipo diagnóstica. [9] En este tipo de metodología, su fin es poder llevar un análisis de situaciones puntuales sobre la seguridad que mantiene la empresa en base a la observación, esto nos permitirá tomar en cuenta con mayor profundidad la situación. Con el fin de disminuir el tiempo de respuesta que debe tener el jefe de TI ante un evento de seguridad.

Con la propuesta se busca mejorar la seguridad de la infraestructura de TI que tiene la empresa reduciendo el tiempo en la que el personal de TI identifica un malware en la red de la institución, para cumplir este propósito se realizar un reporte de como la institución mantiene su seguridad y un reporte luego de la implementación de sistema de detección de malware.

Para la recopilación, procesamiento y análisis de la información se basará en la observación de las instalaciones de la empresa, se analizará las actividades cotidianas que se realiza con el servicio de internet, y los procesos que se realiza en dentro el ámbito web. En cuanto al análisis que se utilizará es la metodología de la ISO 27032, el cual constará de una fase inicial hasta la implementación del sistema de control.

1.6.2. TÉCNICA DE RECOLECCIÓN DE INFORMACIÓN

Entrevistas: En esta parte de la recolección de información, se realiza un diálogo de manera de entrevista al jefe de recurso humanos. Donde se nos proporcionaran datos más

importantes con el fin de establecer los requerimientos puntuales con respecto a las funciones que desempeñan sus sistemas y las medidas de seguridad que están empleando.

1.6.2.1. ANÁLISIS DE LA TÉCNICA DE RECOLECCIÓN DE INFORMACIÓN EMPLEADAS

Para la entrevista realizada al jefe de Recurso humanos (ver anexo 1) nos da a conocer un poco a lo que se dedica la empresa como también sobre el personal que trabaja, pero en algo que uno puede hacer énfasis es en la cantidad de personas que se conecta a la red wifi, pero adicional nos menciona sobre la normativa que tiene la institución sobre el uso de equipos tecnológicos y como él ha evidenciado por medio de las cámaras como ese reglamento no se está cumpliendo en su totalidad.

En la entrevista realizada al jefe del are de TI (ver anexo 2), vemos que si existe un número considerable de los equipos que mantiene la empresa por lo cual se ve la necesidad de tener un gran control de todos ellos, además de que vemos que el método de ingreso a una red wifi en una autenticación muy básica y esto se suma que el cambio de la contraseña sea cada 6 meses si se cree conveniente. Otras de las cosas que podemos tomar en cuenta que los equipos si tiene un método de autenticación para hacer su respectivo uso, es decir que no cualquiera puede acceder a la información, pero en cuanto a la restricción de la navegación, no tiene un mecanismo de control, esto no se realiza por molestias que puede provocar al personal administrativo como ejecutivo.

En cuanto la detección del malware menciona que no tiene un método asertivo para detectar una infección y que las causas que provoca que un equipo tenga un virus es debido a que los usuarios instalan o abren archivos contagiados, pero problemas de seguridad interno no ha tenido el sistema ya que se ha mantenido intacto, pero si han tenido ataques de phishing que si se han detectado con anterioridad tomando las medidas de prevención contra una vulnerabilidad por parte de los usuarios.

Por el tiempo de detección de malware dentro de la infraestructura de TI, no tiene un tiempo estimado, pero es consciente que puede tardar horas o semana para que puedan detectar una actividad anómala, lo que si preocupa es que no mantiene una normativa de seguridad vigente, esto es un caso crítico ya que no existe un mecanismo de contingencia en caso de presentarse un problema.

Por último, en la entrevista realizada a las asistentes del área de contabilidad y del área de compras (ver anexo 3) y (ver anexo 4), mencionaron que utilizan servicios que están dedicados a su ámbito laboral, los cuales tienden a presentar fallas que inmediatamente se les avisa a las personas de sistemas. Correspondiente a la navegación de internet solo utilizan lo esencial para cumplir su cronograma de trabajo, pero la asistente de área de compras si suele estar navegando en otros sitios ajenos a la institución pero que está relacionado a su ámbito laboral.

Tras el cambio de contraseña de wifi, se sienten incomodas al tratar de pedir nuevamente el acceso de internet. Sobre la seguridad de internet mencionan que es muy importante mantener la información de la empresa asegurada y además de los servicios que mantienen contratados especialmente los datos personales, y confían que esta seguridad se está aplicando y aspiran a nuevas mejoras para mayor eficacia en la ciberseguridad.

1.6.3. METODOLOGÍA DE DESARROLLO

1.6.3.1. Metodología OSMTD

Es una metodología para las buenas prácticas en Python para el desarrollo de herramienta de seguridad [10]. La metodología está pensada para trabajar en Python, pero se puede extender las mismas ideas para otros lenguajes de programación [10].La metodología se divide en dos formas [10].

Bloques

La forma de bloques que se utilizara para elaborar los scripts tiene los siguientes subtemas [10].

- **Organización y estructura (ST):** Se recopiló la información necesaria en la metodología de investigación para organizar la estructura del código.
- **Interacción (IT):** con la interacción se verá qué tan amigable es la relación entre la infraestructura que mantiene la empresa con el usuario.
- **Entrada y salida de Información (IO):** el script permitirá obtener todos los datos del tráfico de red y guardarlos en una base de datos para la generación de reporte en formato HTML.
- **Redistribución**: Se realizó varios scripts para ejecutar en varios sistemas operativos y su posterior implementación en cualquier infraestructura de TI.

- **Despliegue**: Se va a considerar las guías de implementación que maneje la empresa para poder implementar el script en la infraestructura de TI.

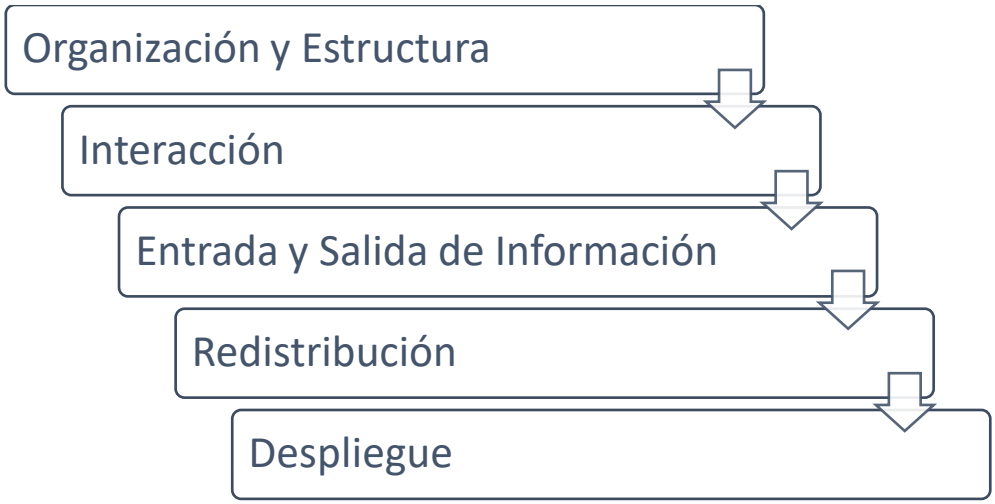


Figura 1.Metodología OMSTD

1.6.3.2. Metodología de la ISO 27032

Se aborda el tema de las directrices para la ciberseguridad, donde los interesados cumplen un papel fundamental en cuanto a la protección de sus activos [11].Tras la presencia de un gran número de transacciones que realizan los usuarios al utilizar varios servicios de la red trae consigo retos y riesgos emergente frente al mal uso de la TI [11].

Fase 1 Entendimiento de la Organización: Se recopilará la información sobre los procedimientos de seguridad que mantiene la empresa, los sistemas que tienen implementado y la normativa de ciberseguridad que actualmente la empresa utiliza.

Fase 2 Análisis de Riesgos: Se analizará los riesgos de seguridad que tiene la empresa, los sistemas que están comprometidos y las vulnerabilidades que existe en los servicios alámbricos.

Fase 3 Plan de Acción: Se realizará cambios en las normativas de seguridad que mantiene la empresa, se procederá a realizar la documentación respectiva de las vulnerabilidades encontradas y el plan de contención que debe emplear la empresa.

Fase 4 Implementación: Se realizará la implementación de un control de peticiones HTTPS para los servicios Web y tener sistema de monitoreo de todo el flujo de tráfico web para evitar malware en una petición de HTTPS.

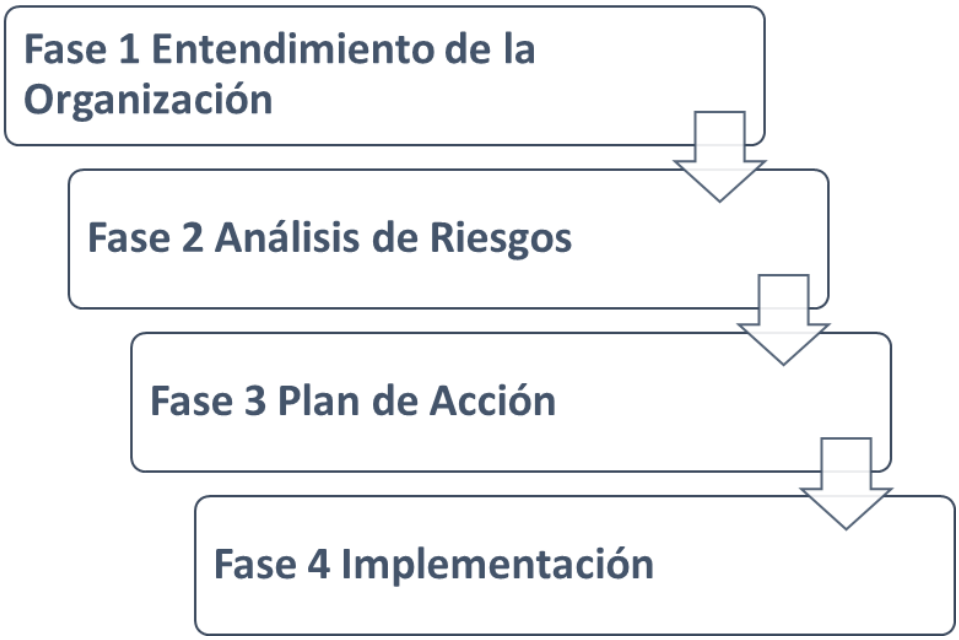


Figura 2 Metodología Adaptado a la ISO 27032

CAPÍTULO II

2. PROPUESTA

2.1. MARCO CONTEXTUAL

2.1.1. EMPRESA DE PRODUCTOS ENLATADOS

La empresa de productos enlatados fundada el 25 de noviembre del 2015, conformado por el personal administrativo, producción y de bahía, se dedica al abastecimiento de materia prima para la elaboración de latas de sardina como producto final, basándose en normativas de calidad para el expendio en el mercado nacional e internacional.

Actualmente la empresa mantiene la venta de sus productos en mercado nacional y en los países de Chile, México, Costa Rica y Estados Unidos, su objetivo principal es expandirse a más países en la venta de sus productos enlatados y poder abarracar más mercados internacionales brindando la calidad que sugieren el mercado internacional (Ver anexo 1).

2.1.2. BASE LEGAL

2.1.2.1. Seguridad de datos personales

Articulo 37.- Seguridad de datos personales

El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de la información personal, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo con la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos [12].

El responsable o encargado del tratamiento de los datos personales, deberá implementar un proceso de verificación, evaluación, valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole con la finalidad de mitigar de forma adecuada los riesgos identificados [12].

Entre otras medidas, se podrán incluir las siguientes:

1) Medidas de anonimización, seudonomización o cifrado de datos personales.

2) Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento y el acceso a los datos personales, de forma rápida en caso de incidentes.
3) Medidas dirigidas a mejorar la resiliencia técnica, física, administrativa, y jurídica.
4) Los responsables y encargados del tratamiento de datos personales podrán acogerse a estándares internacionales para una adecuada gestión de riesgos enfocada a la protección de derechos y libertades, así como para la implementación y manejo de sistemas de seguridad de la información o códigos de conducta reconocidos y autorizados por la autoridad de protección de datos personales.

Artículo 40.- Análisis de riesgo, amenazas y vulnerabilidades.

Para el análisis de riesgos, amenazas y vulnerabilidades, el responsable y el encargado del tratamiento de los datos personales deberán utilizar una metodología que considere, entre otras [12].

1) Las particularidades del tratamiento.
2) Las particularidades de las partes involucradas.
3) Las categorías y el volumen de datos personales objeto de tratamiento.

Artículo 41.- Determinación de medidas de seguridad aplicables.

Para determinar las medidas de seguridad, aceptadas por el estado de la técnica, a las que están obligadas el responsable y el encargado de tratamiento de los datos personales se deberán tomar en consideración, entre otros [12].:

1) Los resultados del análisis de riesgos, amenazas y vulnerabilidades.
2) La naturaleza de los datos personales.
3) Las características de las partes involucradas.
4) Los antecedentes de destrucción de datos personales, la pérdida, alteración, divulgación o impedimento de acceso a los mismos por parte de titular, sean accidentales e intencionales, por acción u omisión, así como los antecedentes de transferencia, comunicación o de acceso no autorizado o exceso de autorización de tales datos.

2.2. MARCO CONCEPTUAL

2.2.1. SISTEMAS VIRTUALIZADOS

La virtualización consiste en ejecutar varias máquinas virtuales sobre una física para poder aprovechar el máximo rendimiento de ésta, en ella se asignan los recursos necesarios y la selección del sistema operativo que van a utilizar [13].

2.2.1.1. VIRTUALBOX

VirtualBox es un potente producto de virtualización x86 y AMD64 / Intel64 para uso empresarial y doméstico [14]. VirtualBox no solo es un producto extremadamente rico en funciones y de alto rendimiento para clientes empresariales, sino que también es la única solución profesional que está disponible gratuitamente como software de código abierto bajo los términos de la GNU General Public License (GPL) [14].

2.2.1.2. KALI LINUX

Conocido como BackTrack Linux es un código abierto, Linux basada en Debian distribución destinada a avanzado pruebas de penetración y auditoría de seguridad [15]. Kali Linux contiene varios cientos de herramientas dirigidas a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa [15].

2.2.2. BASE DE DATOS

Una base de datos es una recopilación organizada de información o datos estructurados, que normalmente se almacena de forma electrónica en un sistema informático [16]. Los datos de los tipos más comunes de bases de datos en funcionamiento actualmente se suelen utilizar como estructuras de filas y columnas en una serie de tablas para aumentar la eficacia del procesamiento y la consulta de datos [16].

2.2.2.1. SISTEMA DE GESTIÓN DE BASE DE DATOS

Una base de datos requiere un programa de software de bases de datos completo, conocido como sistema de gestión de bases de datos, sirve como interfaz entre la base de datos y sus programas o usuarios finales, lo que permite a los usuarios recuperar, actualizar y gestionar cómo se organiza y se optimiza la información [16].

2.2.2.2. SQLITE

SQLite es una biblioteca en proceso que implementa un motor de base de datos SQL transaccional autónomo, sin servidor ni configuración [17]. El código de SQLite es de dominio público y, por lo tanto, es de uso gratuito para cualquier propósito, comercial o privado. SQLite es la base de datos más implementada en el mundo con más aplicaciones de las que podemos contar, incluidos varios proyectos de alto perfil [17].

2.2.3. API

API significa “interfaz de programación de aplicaciones” [18]. En el contexto de las API, la palabra aplicación se refiere a cualquier software con una función distinta [18]. La interfaz puede considerarse como un contrato de servicio entre dos aplicaciones [18]. Este contrato define cómo se comunican entre sí mediante solicitudes y respuestas [18]. La documentación de su API contiene información sobre cómo los desarrolladores deben estructurar esas solicitudes y respuestas [18].

2.2.3.1. API BOTS TELEGRAM

Esta API le permite conectar Bots a nuestro sistema. Los Telegram Bots son cuentas especiales que no requieren un número de teléfono adicional para configurar [19]. Estas cuentas sirven como interfaz para el código que se ejecuta en algún lugar de su servidor [19].

Para usar esto, no necesita saber nada sobre cómo funciona nuestro protocolo de cifrado MTProto: nuestro servidor intermediario se encargará de todo el cifrado y la comunicación con la API de Telegram por usted [19].Permite la comunicación con el servidor a través de una interfaz HTTPS simple que ofrece una versión simplificada de la API de Telegram [19].

2.2.3.2. API VIRUSTOTAL

La API de VirusTotal permite cargar y escanear archivos, URL, acceder a informes de escaneo terminado, así como hacer comentarios automáticos en URL sin necesidad de usar la interfaz del sitio web HTML [20]. En otras palabras, te permite construir scripts simples para acceder a la información generada por VirusTotal [20].

2.2.4. PYTHON

Python es un lenguaje de programación interpretado, interactivo y orientado a objetos [21]. Incorpora módulos, excepciones, tipificación dinámica, tipos de datos dinámicos de muy alto nivel y clases [21]. Admite múltiples paradigmas de programación más allá de la programación orientada a objetos, como la programación funcional y de procedimientos [21].

2.2.4.1. PYSHARK

Es una librería que permite el análisis de paquetes en lenguaje de Python que utiliza procedimientos similares a Wireshark [22]. La librería trae todo el tráfico de red que puede detectar por nuestra tarjeta de ethernet, tanto del equipo en donde se está implementando como de los que estén conectados en nuestra red [22].

2.2.4.2. REQUESTS

Es una biblioteca HTTP que permite enviar solicitudes HTTP/1.1 con mucha facilidad. No hay necesidad de agregar manualmente cadenas de consulta a sus URL o de codificar sus datos POST [23].

2.2.4.3. PANDA

Es un paquete de Python que proporciona estructuras de datos rápidas, flexibles y expresivas diseñadas para el fácil e intuitivo manejo de datos "relacionales" o "etiquetados" [24]. Su objetivo es ser el bloque de construcción fundamental de alto nivel para realizar análisis prácticos de datos del mundo real en Python [24].Además, tiene el objetivo más amplio de convertirse en la herramienta de manipulación/análisis de datos de código abierto más poderosa y flexible disponible en cualquier idioma [24]. Ya está bien encaminado hacia este objetivo [24].

2.2.4.4. DASH

Las aplicaciones Dash brindan una interfaz de apuntar y hacer clic a los modelos escritos en Python, ampliando enormemente la noción de lo que es posible en un "tablero" tradicional [25]. Las aplicaciones de Dash se representan en el navegador web. Puede implementar sus aplicaciones en VM o clústeres de Kubernetes y luego compartirlas a través de direcciones URL. Dado que las aplicaciones de Dash se ven en el navegador web, Dash es inherentemente multiplataforma y está listo para dispositivos móviles [25].

2.2.5. WIRESHARK

Es un analizador de protocolos de red, le permite capturar y navegar de forma interactiva el tráfico que se ejecuta en una red informática [26]. Tiene un conjunto de características ricos y poderoso [26]. Se ejecuta en la mayoría de las plataformas informáticas, incluidas Windows, macOS, Linux y UNIX [26]. Los profesionales de la red, los expertos en seguridad, los desarrolladores y los educadores de todo el mundo lo utilizan con regularidad [26].

2.2.6. NMAP

Es una herramienta de código abierto para exploración de red y auditoría de seguridad [27]. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales; Nmap utiliza paquetes IP "crudos" en formas originales para determinar qué equipos se encuentran disponibles en una red, los servicios (nombre y versión de la aplicación) que ofrecen y los sistemas operativos (y sus versiones) ejecutan, así como también los filtros de paquetes o cortafuegos que se utilizan, entre otras características [27].

2.2.7. VISUAL STUDIO CODE

Es un editor de código libre que permite conectarse a servicios adicionales para su funcionamiento además de agregar más extensiones para su mayor manejo como Angular, Python, HTML5 y PHP [28].

2.2.8. SANS

Sans es un instituto que fue creada en 1989 con el único objetivo de formar profesionales en el campo de ciberseguridad por lo que producen miles de recursos gratuitos para la comunidad de seguridad, estos recursos están destinado a proporcionar lo último en investigación y tecnología en el campo de la seguridad [29].

2.3. MARCO TEÓRICO

2.3.1. ATRAPANDO SITIOS WEB MALICIOSOS

Una de las principales técnicas utilizadas por los ciberdelincuentes son los ataques del lado del cliente (client side attacks), los cuales aprovechan vulnerabilidades en las aplicaciones para ejecutar código malicioso, sin la intervención del usuario [29]. El navegador web es uno de los principales vectores de ataques contra los usuarios [29].

De acuerdo con las estadísticas de los sitios NetMarketShare, W3Counter y StatCounter basado en el análisis del comportamiento de los usuarios en Internet, el navegador más utilizado es Google Chrome, seguido principalmente de Safari y Firefox [29].

2.3.2. MALWARE UNA AMENAZA DE INTERNET

Para el análisis de malware de códigos maliciosos es necesario contar con mecanismos que permitan estudiar la manera en que opera el malware, uno de éstos consiste en la realización de un análisis bajo ambiente controlado que permita generar información para mitigar el impacto, alertando a los involucrados, comprende de dos principales técnicas [30].

El análisis de comportamiento del malware es un proceso mucho más atractivo para los investigadores y por el cual prefieren comenzar, éste se puede observar a través de un ambiente controlado, ya sea virtual o por medio de una red donde esté limitado el tráfico con el propósito de evitar la propagación e infección hacia otros equipos dentro de la organización [30].

En este punto, se monitorea la actividad de los procesos maliciosos que ejecuta el malware, los puertos que abre, su actividad en la red (es decir, si se comunica a un servidor remoto o a algún dominio), el tipo de protocolo que utiliza para comunicarse con él (HTTP, IRC, etc.) y la manera en que se activa en el sistema comprometido (que puede ser mediante la activación de un servicio o iniciándolo directamente desde los archivos de inicio) [30]. Para este proceso, resulta más sencillo utilizar equipos virtuales, pues permiten regresar al escenario original de manera más sencilla, aunque algunos binarios maliciosos ya son capaces de detectar este tipo de ambientes para evitar su ejecución y de esta forma dificultar su análisis [30].

La ventaja que tiene el malware, en comparación con otras sofisticadas técnicas de intrusión, es que aprovecha, la mayoría de las ocasiones, la inocencia de los usuarios; es decir, los desarrolladores de malware utilizan técnicas como ingeniería social para engañar y abusar de sus víctimas, aunque no debemos dejar de lado el hecho de que las técnicas evolucionan de manera permanente [30]. Anteriormente, los intrusos desarrollaban códigos maliciosos para poner a prueba sus conocimientos en cómputo y era común propagarlos a través de dispositivos de almacenamiento como diskettes y CD-

ROM, los cuales se infectaban los sectores de arranque y renombraban algún archivo válido del sistema para evitar su adecuado funcionamiento. [30].

2.3.3. RIESGOS DE SEGURIDAD EN LAS ORGANIZACIONES

La gran mayoría de los componentes tecnológicos que usan todas las organizaciones a nivel mundial tienen vulnerabilidades [31]. Según la compañía CYBSEC Security muchas de estas debilidades pueden nacer con el producto como parte del diseño, tal vez por la omisión de los requisitos mínimos de seguridad de la información que todo nuevo producto software debe cumplir que debe considerarse por el analista de sistemas desde la fase misma de ingeniería de requisitos [31].

Aunque la mayor cantidad de vulnerabilidades son adicionadas al producto en la fase de implementación y desarrollo del software, éstas incluyen en la construcción de la aplicación a través del uso de funciones, métodos y procedimientos débiles del lenguaje de programación elegido en el proyecto [31]. El desarrollo de aplicaciones de muchos fabricantes de software es una carrera contra el tiempo con el fin de sacar al mercado nuevas versiones de sus aplicaciones, que finalmente son productos que deben ser comercializados lo más rápido posible para no perder mercado [31].

Esta carrera contra reloj, junto con las malas prácticas de ingeniería de software, la ausencia o pobre adopción de metodologías de calidad de software como CMMI más la falta de entrenamiento en "desarrollo seguro" y la concienciación en ciberseguridad, garantiza la presencia de "Bugs" en las aplicaciones, como los errores de división por cero, bucles infinitos, deadlocks, etc [31]. Estos hechos conllevan a la aparición de vulnerabilidades en el código fuente que podrían ser explotables, cabe mencionar que muchas de estas vulnerabilidades son comercializadas en el mercado negro por hacker maliciosos con fines de lucro [31].

2.4. REQUERIMIENTOS

Según la implementación del algoritmo los requerimientos son los siguientes:

R01. El algoritmo deberá ser ejecutado basado en requisitos del sistema

Procesador	Intel Core I3 de cuarta generación
Memoria RAM	4 GB de RAM
Disco duro	128 GB
Tarjeta de video	Integrada al procesador

Tarjeta de red	802.11 b/g/n 2.4GHZ

Tabla 1 Requisitos mínimos del equipo

Procesador	Intel Core 7 de octava generación o Ryzen 7 3700H
Memoria RAM	8 GB de RAM
Disco duro	256 GB
Tarjeta de video	Envidia GeForce GTX 1650
Tarjeta de red	802.11 b/g/n/ac 2.4 GHZ y 5 GHZ

Tabla 2 Requisitos recomendados del equipo

R02. El usuario deberá tener una cuenta en telegram para poder crear el Bot y recibir las notificaciones.

R03. El usuario debe crear una cuenta en VirusTotal para obtener la API y enlazarla al script de análisis.

R04. El algoritmo podrá ser utilizado por los sistemas operativos Windows, Linux y OSX.

R05. La aplicación podrá ser utilizado siempre y cuando tenga instalado la aplicación de Python3 junto con las librerías de Pyshark y VirusTotal.

R06. Las notificaciones que lleguen a telegram pueden ser visualizadas en un computador con cualquier navegador o desde un dispositivo móvil.

R07. Los reportes de seguridad que se envían a telegram pueden visualizarse en cualquier navegador solo ingresando al enlace que se adjunta a la notificación.

R08. El sistema debe ser capaz de procesar N análisis por segundo.

R09. Todo análisis de tráfico de red será respaldado y clasificado automáticamente entre tráfico normal y tráfico anómalo.

R10. Toda amenaza encontrada deberá ser notificada en menos de 10 segundos.

R11. El administrador de TI tendrá acceso al sistema por lo que tendrá la posibilidad de iniciar y culminar el proceso de análisis.

R12. El tiempo de aprendizaje del sistema por el administrador debe ser menor a 4 horas.

R13. Si se identifica vulnerabilidad de seguridad en el sistema el administrador deberá interrumpir el análisis.

2.5. DESARROLLO DE LA PROPUESTA

En esta sección se procederá a demostrar la parte práctica de la propuesta tecnológica, donde se realizó el script de escaneo de malware mediante la captura de paquetes en un tráfico de red.

Para el desarrollo del algoritmo fue necesario investigar acerca de la metodología de ISO 27032 (Gestión de la Ciberseguridad) que fue parte referencial para realizar la recopilación de la información institucional como para la implementación. Mencionado lo anterior se divide en las siguientes fases:

- **Fase 1**: Entendimiento de la Organización
- **Fase 2**: Análisis de Riesgos
- **Fase 3**: Plan de Acción
- **Fase 4**: Implementación

2.5.1. FASE 1: ENTENDIMIENTO DE LA ORGANIZACIÓN

El personal encargado del área de sistemas no cuenta con la información necesaria de como mitigar un ciberataque, puesto que el conocimiento que mantiene es básico. Mediante esta fase va a identificar la ubicación física de cada dispositivo que forma parte de la infraestructura de TI obteniendo la siguiente topología:

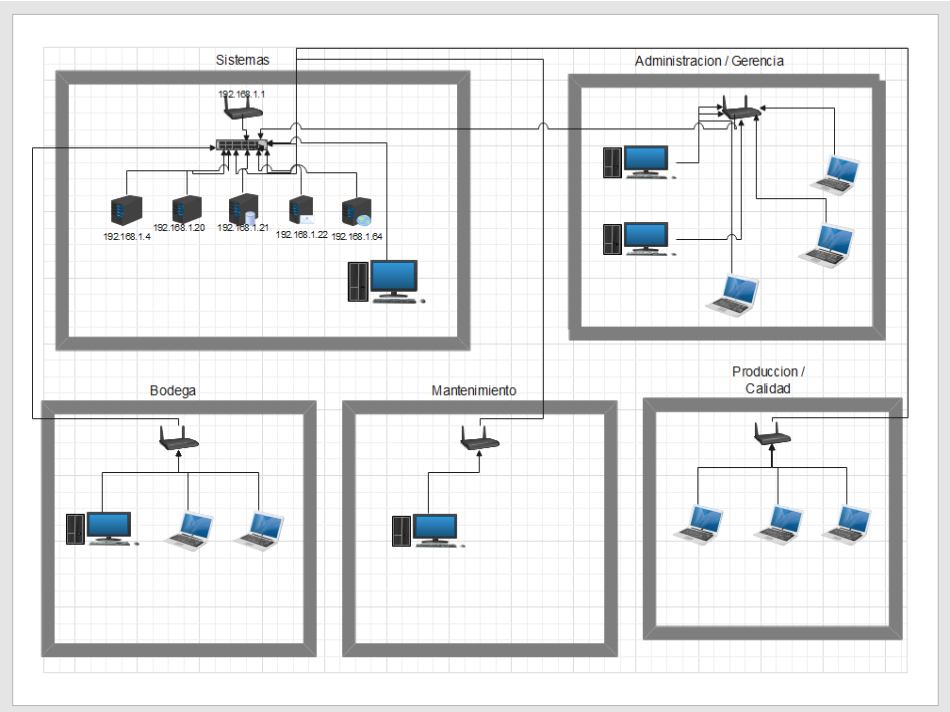


Figura 3 Topología de la red

Después de determinar la topología de red implementada en la institución se procedió a recopilar la información de los equipos y servicios que posee la empresa, la cual es detallada en el siguiente reporte:

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Sistema de control de peticiones https mediante Algoritmo de Python para la detección de tráfico de red anómalo para una empresa de productos enlatados

Realizado por:	Gómez Ruidiaz José	**Nombre del reporte:**	Reporte Fase Entendimiento de la Organización
Fecha	15/05/2022		

Fase Entendimiento de la Organización

Objetivos de la fase:

- Extraer la información de la infraestructura de red de la institución.
- Revisar la documentación de seguridad informática que mantiene implementada la institución.

Técnica:

La técnica que se empleó fue la observación para obtener la información de la topología y medidas de seguridad.

Herramientas Tecnológicas aplicadas:

Se procedió a utilizar el navegador web para evidenciar los servicios que tienen contratado en la empresa.

Tiempo de ejecución:

El tiempo que tomó en la ejecución fue de 2 horas.

Procedimiento:

Mediante la observación se obtuvo la infraestructura de red de la institución, con el uso del navegador se constató de los servicios que mantiene actualmente la empresa.

Resultados obtenidos:

Durante la resolución de la fase se obtuvo la infraestructura de la red, está conformada por:

- 1 Router Huawei HG8245Q2
- 1 switch Linksys SE3024 24 puertos
- 4 Router TP-Link TL-WR940N (Repetidores)
- 5 máquinas de escritorio distribuida en varias áreas
- 8 laptops distribuida en varias áreas
- 1 servidor HP PROLIANT DL360 (Base de datos)
- 1 servidor HP PROLIANT ML31E (Servidor de Windows server 2016 archivos compartidos)
- 1 servidor DELL POWEREDGE T130 (Servidor de Linux para SAP BISNES ONE)

Además, la empresa mantiene servicios contratados, como:

- Servicio de internet del proveedor de Netlife

- Servicio SAP BISNES ONE
- Servicio de Microsoft Empresarial
- Servicio de EXXIS

Al momento de recopilar la información la empresa no mantiene una normativa de seguridad vigente, pero mantiene un modelo de seguridad básica:

- Cambio de la contraseña wifi cada 6 meses.
- Prohibición de ingresos de equipos que no sean de la empresa, que el mayor tiempo no se cumple.
- Prohibición de salida de información de la empresa sin autorización por dispositivos digitales.

Mantener la confidencialidad de la información que la empresa brinda al personal.

Recursos Tecnológicos de la Empresa

Marca de Router	Huawei
Modelo	HG8245Q2
Velocidad de Internet Contratado	200 Mbps
Standard Transmisión	IEEE 802.11AC
Tipo de Frecuencia	2.4 GHZ y 5 GHZ
Velocidad 2.4 GHZ	450Mbit/s
Velocidad 5 GHZ	1300 Mbit/s
#Puertos Ethernet	4
# Puerto Telefónico	1
# Puerto USB	2

Tabla 3 Servicio de internet Netlife

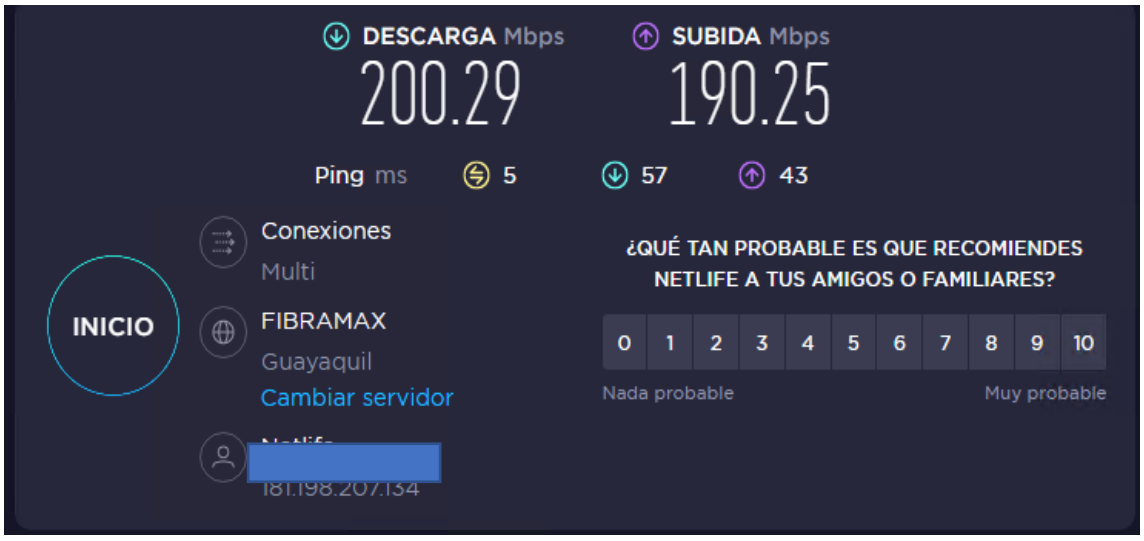


Figura 4 Comprobación de la velocidad de internet con el servicio de speedtest

Número de equipos	5
Procesador	I5 de quinta generación
Memoria RAM	4gb ddr4
Placa de BIOS	Mainboard biostar b250-mhc
Disco duro	500 GB HDD
Tarjeta gráfica	N/A
Tarjeta de red	LAN rtl811h
# de puertos USB 2.0	2
#de puertos USB 3.0	4
# puerto HDMI	1
# puerto VGA	1
# puerto LAN	1
# puertos de Audio	3
#Pantallas	7
Marca	LG
Dimensiones	18.5''
# Puerto VGA	1
Sistema operativo	Windows 10

Tabla 4 Especificaciones de equipos de escritorio

Número de equipos	2
Procesador	I5 de 11Th Generación
Memoria RAM	12GB ddr4
Disco duro	256 GB M.2
Tarjeta gráfica	Intel Iris Xe Graphics
Tarjeta de red	Realtek RTL8821CE-M 802.11a/b/g/n/ac
# de puertos USB 2.0	0
#de puertos USB 3.0	2
# puerto Tipo C	1
# puerto HDMI	1
# puerto VGA	0
# puerto LAN	0
# puertos de Audio	3
Marca	LG
Dimensiones	17.3''
Sistema operativo	Windows 11

Tabla 5 Especificaciones de Laptop HP 17-cn1053cl

Número de equipos	1
Procesador	I7 de 11Th generación
Memoria RAM	8GB ddr4
Disco duro	256 GB SSD
Pantalla	HD Retroiluminada con Truelife - Aplica Modelo 348 15.6 ''
Tarjeta Gráfica	GeForce GTX 1050 (movilidad) (2 GB) de NVIDIA
Interfaz de red	802.11ac 2x2 WiFi + Bluetooth 5.0
#de puertos USB 3.0	2
# puerto USB 2.0	0

# puerto HDMI	1
# puerto tipo C	1
# puerto LAN	0
Batería	4 celdas 70Wh li-ion
Sistema operativo	Windows 10

Tabla 6 Especificaciones de la Laptop Lenovo ideapad 5

Número de equipos	2
Procesador	I7 de séptima generación
Memoria RAM	8GB ddr4
Disco duro	256 GB SSD
Pantalla	Pantalla Full HD 15.6 ‘’
Tarjeta Gráfica	NVIDIA GeForce MX450
Interfaz de red	802.11ac 2x2 WiFi + Bluetooth 5.0
#de puertos USB 3.0	1
# puerto USB 2.0	2
# puerto HDMI	1
# puerto tipo C	1
# puerto LAN	0
Sistema operativo	Windows 10

Tabla 7 Especificaciones de la Laptop Asus VivoBook 15 FE12D

Número de equipos	1
Procesador	I7 de octava generación
Memoria RAM	8GB ddr4
Disco duro	256 GB M.2
Pantalla	Pantalla Full HD 15.6 ‘’
Tarjeta Gráfica	Intel UHD Graphics 620
Interfaz de red	Intel Dual Band Wireless-AC 3168 802.11a/b/g/n/ac (1x1) WiFi con Bluetooth 4.2
#de puertos USB 3.0	1
# puerto USB 2.0	1
# puerto HDMI	1
# puerto VGA	1
# puerto tipo C	1
# puerto LAN	1
Sistema operativo	Windows 10

Tabla 8 Especificaciones de la Laptop HP PRO 450G5

Número de equipos	1
Procesador	Ryzen 7 5700u
Memoria RAM	12GB ddr4
Disco duro	512 GB M.2
Pantalla	Pantalla Full HD 15.6 ‘’
Tarjeta Gráfica	AMD RADEON
Interfaz de red	802.11ac 2x2 WiFi + Bluetooth 5.0
#de puertos USB 3.0	1
# puerto USB 2.0	1

# puerto HDMI	1
# puerto VGA	0
# puerto tipo C	1
# puerto LAN	0
Sistema operativo	Windows 10

Tabla 9 Especificaciones de la Laptop Asus M515u

Número de equipos	1
Procesador	I5 11Th Generación
Memoria RAM	8GB ddr4
Disco duro	512 GB SSD
Pantalla	Pantalla Full HD 15.6 ‘’
Tarjeta Gráfica	Intel® Iris® Xᵉ Graphics
Interfaz de red	MediaTek WiFi 6 MT7921 (2x2) and Bluetooth® 5.2
#de puertos USB 3.0	1
# puerto USB 2.0	1
# puerto HDMI	1
# puerto VGA	0
# puerto tipo C	1
# puerto LAN	1
Sistema operativo	Windows 11

Tabla 10 Especificaciones de la Laptop DELL INSPIRON 15

Número de equipos	1
Procesador	Intel® Xeon® E5-2650 v3 (10 núcleos, 2,3 GHz, 25 MB, 105 W)
# procesadores	2
Memoria RAM	16GB RDIMM
# Ranuras RAM	24
Disco duro	5 TB SSD
Interfaz de red	Broadcom 5720 Gigabit Ethernet
#de puertos USB 3.0	3
# puerto USB 2.0	0
# puerto VGA	1
# puerto serial	1
# puerto LAN	4
Sistema operativo	Linux

Tabla 11 Especificaciones del servidor HP PROLIANT DL360 GEN9

Número de equipos	1
Procesador	Intel Xeon E3-1240V3 (3.8 GHz, 8 MB de caché, 4 núcleos)
Memoria RAM	8GB DDR3
# Ranuras RAM	4
Disco duro	14 TB
Interfaz de red	Gigabyte Ethernet 10/100/1000 Mbits/s
#de puertos USB 3.0	2

# puerto USB 2.0	4
# puerto VGA	2
# puerto LAN	2
Sistema operativo	Windows Server 2016

Tabla 12 Especificaciones del servidor HP PROLIANT ML320e

Número de equipos	1
Procesador	Procesador Intel® Xeon® de la familia de productos E3-1200 v6
Memoria RAM	8GB DDR4
# Ranuras RAM	4
Disco duro	2 TB
Interfaz de red	Broadcom® BCM5720
#de puertos USB 3.0	3
# puerto USB 2.0	5
# puerto VGA	2
# puerto LAN	2
Sistema operativo	Windows Server 2016

Tabla 13 Especificaciones del servidor DELL POWEREDGE T130

Número de equipos	1
Estándares de red	• IEEE 802.3 • IEEE 802.3u • IEEE 802.3x • IEEE 802.3ab • IEEE 802.3az • IEEE 802.3af • IEEE 802.3at (PoE+)
Ancho de Banda	48Gbps (sin bloqueo)
Consumo de Energía	7.79 W / 17.65 W
Velocidad de conexión por cable	1000 Mbps
Temperatura de funcionamiento	De 0°C a 50 °C
Montaje	Montaje en Rack
Quality Of Service	802.1p y DSCP
Cumplimiento de las normativas	FCC clase A, CE, UL, CB

Tabla 14 Especificaciones del Switch Linksys 24 puertos

Tipo de cable	Categoría 6
Tipo de TJ45	Categoría 6
Tiempo en uso	1 año
Certificación	No

Tabla 15 Característica del cableado de red

Número de usuarios contratados	10
Módulos que integra	• Módulo MRP • Módulo de Producción

	• Módulo de Servicios • Módulo Recursos Humanos • Módulo CRM-Ventas • Módulo Finanzas • Módulo Contabilidad • Módulo Compras • Módulo Bancos • Módulo inventario
Tipo de pago	Pago anual

Tabla 16 Especificaciones del servicio de SAP BUSINESSS ONE

Figura 5 Servicio de SAP BUSINESS ONE

2.5.2. FASE 2: ANÁLISIS DE RIESGOS

Para el análisis de riesgo se procedió a ingresar a la infraestructura de red de la empresa para evidenciar que tipos de vulnerabilidades presenta, para este tipo de análisis se procedió a usar las herramientas de NMAP y WIRESHARK en la cual detallamos en el siguiente informe:

UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA **FACULTAD DE SISTEMAS Y TELECOMUNICACIONES** **CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN**			
Sistema de control de peticiones https mediante Algoritmo de Python para la detección de tráfico de red anómalo para una empresa de productos enlatados			
Realizado por:	Gómez Ruidiaz José	**Nombre del reporte:**	Reporte Fase Análisis de Riesgos
Fecha	15/05/2022		
Fase Análisis de Riesgos			

Objetivos de la fase:

- Reconocer las amenazas y vulnerabilidades dentro de la infraestructura de TI

Técnica:

La técnica que se empleó fue la observación usando recursos tecnológicos para recopilar la información.

Herramientas Tecnológicas aplicadas:

Se procedió a utilizar un computador utilizando máquina virtual para emplear las herramientas de Nmap y Wireshark adicional se empleó el navegador para la búsqueda de información.

Tiempo de ejecución:

El tiempo que tomó en la ejecución fue de 3 días.

Procedimiento:

Mediante la observación se obtuvo la infraestructura de red de la institución, con el uso del navegador se constató los servicios que mantiene actualmente la empresa.

Resultados obtenidos:

Durante el análisis, usando la herramienta de Nmap se pudo determinar las vulnerabilidades de algunos equipos conectados a la red además de conseguir las características de éstos como el sistema operativo.

Empleando la herramienta de Wireshark se constató que dentro el tráfico de red existe amenazas, que están siendo ejecutadas en cada momento.

Haciendo uso del navegador se procedió a buscar la información de las vulnerabilidades encontradas.

Conclusión

Luego del análisis y la recopilación de la información obtenidas por las herramientas Nmap y Wireshark, se determinan que algunas vulnerabilidades como, sistemas con posibles problemas de seguridad, puertos abiertos, adicional a eso, los equipos presentan problemas de sistemas operativos mostrando actividad anómala en el tráfico de red, dando como consecuencia la lentitud en las comunicaciones y posible malware dentro cada uno de los equipos

Resumen del Análisis desde la Aplicación NMAP

Se realizó el escaneo de la infraestructura de TI para determinar que equipos están conectados y determinar los puertos que están abiertos para eso se realizó una matriz donde se detalla los siguientes datos:

IP de Análisis	MAC Address	Sistema Operativo	Puertos Abiertos
192.168.1.1	00:0C: 29:4A: 3C:2B	FreeBSD 11.X	22/TCP 53/ TCP 80/TCP

			443/ TCP
192.168.1.4	50:9A: 4C:A5: 91:98	VMware ESXi 5.0	22/TCP 80/TCP 427/TCP 443/TCP 902/TCP 5988/TCP 5989/TCP 8000/TCP 8300/TCP 9080/TCP
192.168.1.20	3C:A8:2A: 12:94:50	Linux 3.0	22/TCP 111/TCP 139/TCP 445/TCP 2049/TCP 3389/TCP 5801/TCP 5901/TCP 8000/TCP 50000/TCP 50001/TCP 50002/TCP 50003/TCP
192.168.1.21	64:51:06: F9:6D:3D	Windows Server 2016	80/TCP 135/TCP 139/TCP 445/TCP 3306/TCP 3389/TCP 49154/TCP
192.168.1.22	00:0C: 29:6A:68:CC	Windows Server 2016 virtual	53/TCP 80/TCP 88/TCP 135/TCP 139/TCP 389/TCP 443/TCP 445/TCP 464/TCP 593/TCP 636/TCP 2179/TCP 3268/TCP 3269/TCP 3389/TCP
192.168.1.41	4C:F5: DC: A0:09:EE	Linux 3.5	80/TCP 443/TCP 554/TCP 8000/TCP
192.168.1.64	4C:F5: DC: 9A:9A:BF	Linux 3.5	80/TCP 443/TCP

			554/TCP 8000/TCP
192.168.1.95	D8:C0: A6:0F: 78:6F	Microsoft Windows 10	135/TCP 139/TCP 445/TCP 1042/TCP 1043/TCP 3389/TCP 5357/TCP
192.168.1.102	70: F1:A1: 20:4D: F6	Microsoft Windows 11	135/TCP 139/TCP 445/TCP 1042/TCP 1043/TCP 5357/TCP
192.168.1.125	38:1A: 52:48:54:89	Linux 2.6	80/TCP 443/TCP 515/TCP 631/TCP 9100/TCP
192.168.1.126	E4:02:9B: BC: 68:26	Linux 2.4	135/TCP 139/TCP 445/TCP 5357/TCP
192.168.1.127	20:4E: F6:08: EF:73	Linux 2.4	1042/TCP 2968/TCP 5357/TCP 7070/TCP
192.168.1.129	D8:D3: 85:1F: 25:11	Microsoft Windows 11	135/TCP 139/TCP 445/TCP 3580/TCP 5357/TCP
192.168.1.131	EC: C8:9C: 77:1A:80	Linux 2.4	80/TCP 443/TCP 554/TCP 8000/TCP
192.168.1.154	50:3E: AA:20:AF:DB	Linux 2.6	2968/TCP 5357/TCP 7070/TCP 8090/TCP
192.168.1.165	AC: 16:2D:0A: FE:AE	Microsoft Windows 11	2968/TCP 3389/TCP 5357/TCP
192.168.1.167	90: E8:68:06:3E:75	Unknown	2968/TCP 7070/TCP 8090/TCP
192.168.1.172	1C: 69:7A:1D: 04:0A	Microsoft Windows 10	2968/TCP 5357/TCP
192.168.1.176	0C:96: E6:39: DA: D5	Linux 2.4	2968/TCP 5357/TCP

192.168.1.177	3C:7C:3F:12:C9: EB	Microsoft Windows 11	135/TCP 139/TCP 445/TCP 5357/TCP 7070/TCP
192.168.1.194	EC: C8:9C: 77:1A:23	Linux 2.4	80/TCP 443/TCP 554/TCP 8000/TCP
192.168.1.219	38:1A: 52:4E:CA:42	Linux 2.4	80/TCP 443/TCP 515/TCP 631/TCP 9100/TCP
192.168.1.221	10:27: F5:F3: 9D:E1	Linux 2.4	80/TCP 443/TCP
192.168.1.223	E0:DB:55:C2: DA: F3	Microsoft Windows 11	135/TCP 139/TCP 445/TCP 2968/TCP 3580/TCP 5357/TCP 7070/TCP
192.168.1.228	AC: 16:2D: 12:1D:26	Microsoft Windows 10	135/TCP 139/TCP 445/TCP 2968/TCP 3580/TCP 5357/TCP 7070/TCP

Tabla 17 Escaneo de IP de la aplicación NMAP

Ç

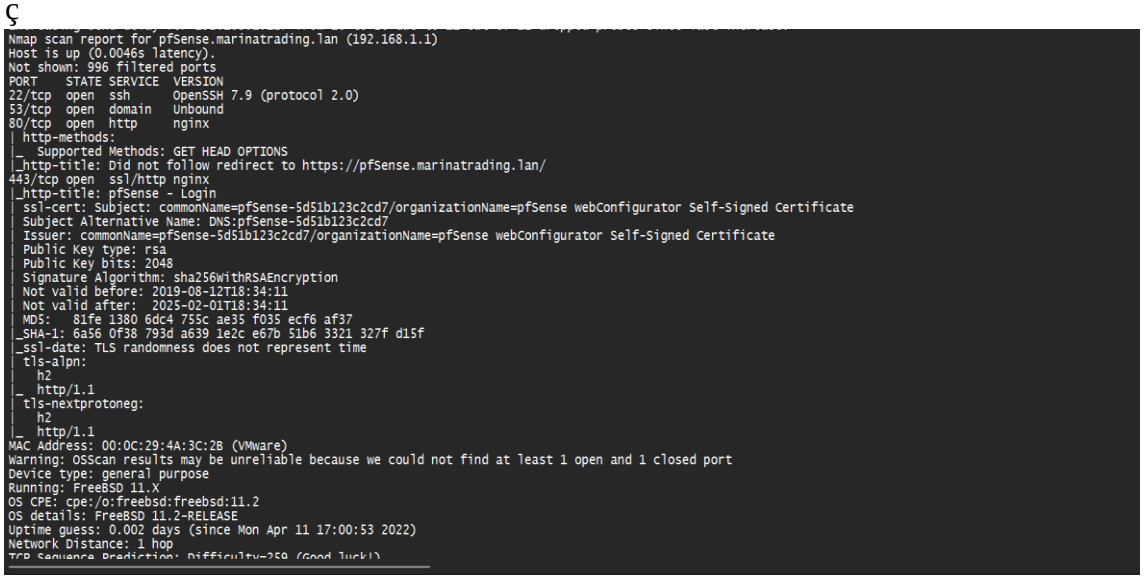


Figura 6 Resultado del análisis de NMAP

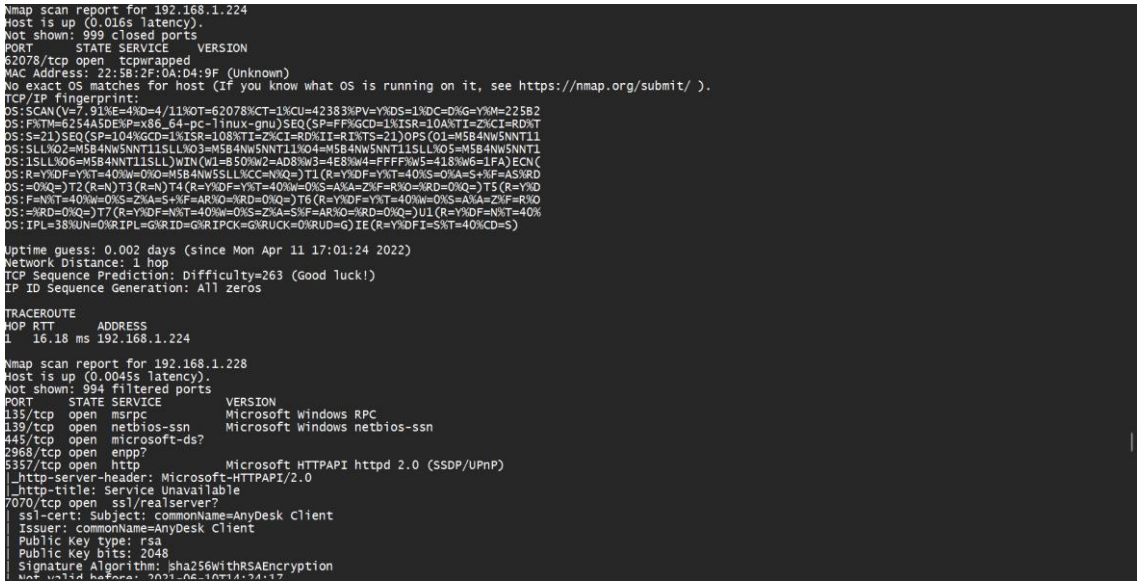


Figura 7 Resultado del análisis de NMAP

Vulnerabilidades en la ejecución de los servicios de los puertos

Puertos	Servicios
22/TCP	ssh
443/TCP	ssl/http
902/TCP	wbem-http
5988/TCP	wbem-https
9080/TCP	gSOAP 2.8
139/TCP	netbios-ssn
445/TCP	netbios-ssn
636/TCP	tcpwrapped
3269/TCP	tcpwrapped
443/TCP	ssl/https
80/TCP	tcpwrapped
443/TCP	tcpwrapped
631/TCP	tcpwrapped
135/TCP	tcpwrapped
139/TCP	tcpwrapped
445/TCP	tcpwrapped
5357/TCP	tcpwrapped
1042/TCP	tcpwrapped
2968/TCP	tcpwrapped
7070/TCP	tcpwrapped

Tabla 18 Puertos y Servicios ejecutándose

Vulnerabilidad SSH

El protocolo SSH-1 permite que los servidores remotos realicen ataques de intermediario y reproduzcan una respuesta de desafío del cliente a un servidor de destino mediante la creación de una ID de sesión que coincida con la ID de sesión del objetivo, pero que use un par de claves públicas que es más débil que la clave pública del objetivo, lo que le permite al atacante calcular la clave privada correspondiente y usar la ID de sesión del objetivo con el par de claves comprometidas para hacerse pasar por el objetivo [32].

Puntación CVSS	7.5
Impacto de la Confidencialidad	Parcial, Hay una divulgación de información considerable
Impacto de integridad	Parcial, la modificación de algunos archivos o información del sistema es posible, pero el atacante no tiene control sobre lo que puede modificar, o el alcance de lo que el atacante puede afectar es limitado
Impacto en la disponibilidad	Parcial, hay un rendimiento reducido o interrupciones en la disponibilidad de recursos
Complejidad de acceso	Bajo, no existen condiciones de acceso especializadas o circunstancias atenuantes. Se requiere muy poco conocimiento o habilidad para explotar
Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 19 Vulnerabilidad Reportada del Servicio SSH

Vulnerabilidad SSL/HTTP

El servidor SSL HTTP en HP Web-enabled Management Software 5.0 a 5.92, con acceso anónimo habilitado, permite a atacantes remotos comprometer los certificados confiables cargando sus propios certificados [33].

Puntación CVSS	7.5
Impacto de la Confidencialidad	Parcial, Hay una divulgación de información considerable
Impacto de integridad	Parcial, la modificación de algunos archivos o información del sistema es posible, pero el atacante no tiene control sobre lo que puede modificar, o el alcance de lo que el atacante puede afectar es limitado
Impacto en la disponibilidad	Parcial, hay un rendimiento reducido o interrupciones en la disponibilidad de recursos
Complejidad de acceso	Bajo, no existen condiciones de acceso especializadas o circunstancias atenuantes. Se requiere muy poco conocimiento o habilidad para explotar
Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 20 Vulnerabilidad reportada de SSl/HTTP

Vulnerabilidad de WBem-http

Vulnerabilidad no especificada en la implementación de WBEM en HP HP-UX 11.11 y 11.23 permite a atacantes remotos obtener acceso a información de diagnóstico a través de vectores desconocidos [34].

Puntación CVSS	5.8
Impacto de la Confidencialidad	Parcial, Hay una divulgación de información considerable
Impacto de integridad	Parcial, la modificación de algunos archivos o información del sistema es posible, pero el atacante no tiene control sobre lo que puede modificar, o el alcance de lo que el atacante puede afectar es limitado
Impacto en la disponibilidad	Ninguno, no hay impacto en la disponibilidad del sistema
Complejidad de acceso	Medio, las condiciones de acceso son algo especializadas. Se deben cumplir algunas condiciones previas para explotar
Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 21 Vulnerabilidad reportada Wbem-Http

Vulnerabilidad gSOAP 2.8

Genivia gSOAP 2.7.x y 2.8.x anteriores a la 2.8.75 permite a los atacantes causar una denegación de servicio (cancelación de la aplicación) o posiblemente tener otro impacto no especificado si una aplicación de servidor se construye con el indicador -DWITH_COOKIES. Esto afecta a las bibliotecas C/C++ libgsoapck/libgsoapck++ y libgsoapssl/libgsoapssl++, ya que están construidas con esa bandera [35].

Puntación CVSS	6.8
Impacto de la Confidencialidad	Parcial, Hay una divulgación de información considerable
Impacto de integridad	Parcial, la modificación de algunos archivos o información del sistema es posible, pero el atacante no tiene control sobre lo que puede modificar, o el alcance de lo que el atacante puede afectar es limitado
Impacto en la disponibilidad	Ninguno, no hay impacto en la disponibilidad del sistema
Complejidad de acceso	Medio, las condiciones de acceso son algo especializadas. Se deben cumplir algunas condiciones previas para explotar
Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 22 Vulnerabilidad reportada gSOAP 2.8

Vulnerabilidad de netbios-ssn

Windows NetBIOS en Windows Server 2008 SP2 y R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold y R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703 y Windows Server 2016 permite una vulnerabilidad de denegación de servicio cuando maneja incorrectamente los paquetes NetBIOS, también conocido como "vulnerabilidad de denegación de servicio de Windows NetBIOS" [36].

Puntación CVSS	6.1
Impacto de la Confidencialidad	Ninguno, no hay impacto en la confidencialidad del sistema
Impacto de integridad	Ninguno, no hay impacto en la integridad del sistema
Impacto en la disponibilidad	Completo, hay un cierre total del recurso afectado, El atacante puede hacer que el recurso no esté disponible por completo
Complejidad de acceso	Bajo, no existe condiciones de acceso especializadas o circunstancias atenuantes. Se requiere muy poco conocimiento o habilidad para explotar
Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 23 Vulnerabilidad reportada de netbios-ssn

Vulnerabilidad de tcpwrapped

TCP Wrappers (tcp_wrappers) en FreeBSD 4.1.1 a 4.3 con la opción PARANOID ACL habilitada no verifica correctamente el resultado de una búsqueda inversa de DNS, lo que podría permitir a los atacantes remotos eludir las restricciones de acceso previstas a través de la suplantación de DNS [37].

Puntación CVSS	7.5
Impacto de la Confidencialidad	Parcial, Hay una divulgación de información considerable
Impacto de integridad	Parcial, la modificación de algunos archivos o información del sistema es posible, pero el atacante no tiene control sobre lo que puede modificar, o el alcance de lo que el atacante puede afectar es limitado
Impacto en la disponibilidad	Parcial, hay un rendimiento reducido o interrupciones en la disponibilidad de recursos
Complejidad de acceso	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 24 Vulnerabilidad reportada tcpwrappers

Vulnerabilidad de Sistemas Operativos (OS)

Sistema operativo FreeBSD

En FreeBSD 11.x antes de 11.1-RELEASE y 10.x antes de 10.4-RELEASE, el algoritmo qsort tiene un patrón de recursión determinista. Alimentar una entrada patológica al algoritmo puede conducir a un uso excesivo de la pila y un posible desbordamiento [38]. Las aplicaciones que usan qsort para manejar grandes conjuntos de datos pueden bloquearse si la entrada sigue el patrón patológico [38].

Puntación CVSS	6.1
Impacto de la Confidencialidad	Ninguno, no hay impacto en la confidencialidad del sistema
Impacto de integridad	Parcial, hay un rendimiento reducido o interrupciones en la disponibilidad de recursos.
Impacto en la disponibilidad	Completo, hay un cierre total del recurso afectado, El atacante puede hacer que el recurso no esté disponible por completo
Complejidad de acceso	Bajo, no existe condiciones de acceso especializadas o circunstancias atenuantes. Se requiere muy poco conocimiento o habilidad para explotar
Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 25 Vulnerabilidad reportada FreedBSD

Sistema VMware ESXi 5.0

La implementación de VMware Tools HGFS (también conocido como Carpetas compartidas) en VMware Workstation 11.x antes de 11.1.2, VMware Player 7.x antes de 7.1.2, VMware Fusion 7.x antes de 7.1.2 y VMware ESXi 5.0 a 6.0 permiten que los usuarios obtengan privilegios del sistema operativo invitado provocan una denegación de servicio (corrupción de la memoria del kernel del sistema operativo invitado) a través de vectores no especificados [39].

Puntación CVSS	7.5
Impacto de la Confidencialidad	Parcial, Hay una divulgación de información considerable
Impacto de integridad	Parcial, la modificación de algunos archivos o información del sistema es posible, pero el atacante no tiene control sobre lo que puede modificar, o el alcance de lo que el atacante puede afectar es limitado
Impacto en la disponibilidad	Parcial, hay un rendimiento reducido o interrupciones en la disponibilidad de recursos
Complejidad de acceso	Bajo, no existen condiciones de acceso especializadas o circunstancias atenuantes. Se requiere muy poco conocimiento o habilidad para explotar

Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 26 Vulnerabilidad reportada de VMware Esxi 5.0

Sistema Linux 3.5

El inicio de sesión en Slackware Linux 3.2 a 3.5 no verifica correctamente si hay un error cuando falta el archivo /etc/group, lo que evita que pierda privilegios, asignándolos de raíz a cualquier usuario local que inicie sesión en el servidor [40].

Puntación CVSS	7.2
Impacto de la Confidencialidad	Completo, hay una divulgación total de la información, lo que da como resultado que se revelen todos los archivos del sistema
Impacto de integridad	Completo, hay un compromiso total de la integridad del sistema. Hay una perdida completa de la protección del sistema, lo que da como resultado que todo el sistema se vea comprometida
Impacto en la disponibilidad	Completa, hay un cierre total del recurso afectado. El atacante puede hacer que el recurso no esté disponible por completo
Complejidad de acceso	Bajo, no existe condiciones de acceso especializadas o circunstancias atenuantes. Se requiere muy poco conocimiento o habilidad para explotar
Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 27 Vulnerabilidad reportada linux 3.5

Sistema Linux 2.6

drivers/scsi/mpt2sas/mpt2sas_ctl.c en el kernel de Linux 2.6.38 y anteriores no valida (1) la longitud y (2) los valores de desplazamiento antes de realizar operaciones de copia de memoria, lo que podría permitir a los usuarios locales obtener privilegios y provocar una denegación de servicio (corrupción de la memoria), obteniendo información confidencial de la memoria del kernel a través de una llamada ioctl diseñada, relacionada con las funciones _ctl_do_mpt_command y _ctl_diag_read_buffer [41].

Puntación CVSS	7.2
Impacto de la Confidencialidad	Completo, hay una divulgación total de la información, lo que da como resultado que se revelen todos los archivos del sistema
Impacto de integridad	Completo, hay un compromiso total de la integridad del sistema. Hay una perdida completa de la protección del sistema, lo que da como resultado que todo el sistema se vea comprometida
Impacto en la disponibilidad	Completa, hay un cierre total del recurso afectado. El atacante puede hacer que el recurso no esté disponible por completo
Complejidad de acceso	Bajo, no existe condiciones de acceso especializadas o circunstancias atenuantes. Se requiere muy poco conocimiento o habilidad para explotar

Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 28 Vulnerabilidad reportada Linux 2.6

Vulnerabilidad Linux 2.4

La implementación de asn1 en (a) el kernel de Linux 2.4 antes de 2.4.36.6 y 2.6 antes de 2.6.25.5, como se usa en los módulos cifs e ip_nat_snmp_basic; y (b) el paquete gxsnmp; no valida correctamente los valores de longitud durante la decodificación de los datos BER ASN.1, lo que permite a atacantes remotos causar una denegación de servicio (caída) o ejecutar código arbitrario a través de (1) una longitud mayor que el búfer de trabajo, lo que puede conducir a un error no especificado Desbordamiento; (2) una longitud oid de cero, que puede dar lugar a un error de uno; o (3) una longitud indefinida para una codificación primitiva [42].

Puntación CVSS	10.2
Impacto de la Confidencialidad	Completo, hay una divulgación total de la información, lo que da como resultado que se revelen todos los archivos del sistema
Impacto de integridad	Completo, hay un compromiso total de la integridad del sistema. Hay una perdida completa de la protección del sistema, lo que da como resultado que todo el sistema se vea comprometida
Impacto en la disponibilidad	Completa, hay un cierre total del recurso afectado. El atacante puede hacer que el recurso no esté disponible por completo
Complejidad de acceso	Bajo, no existe condiciones de acceso especializadas o circunstancias atenuantes. Se requiere muy poco conocimiento o habilidad para explotar
Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 29 Vulnerabilidad reportada Linux 2.4

Sistema Windows 10

Sistema de archivos de cifrado de Windows (EFS) Vulnerabilidad de elevación de privilegios [39].

Puntación CVSS	6.0
Impacto de la Confidencialidad	Parcial, Hay una divulgación de información considerable
Impacto de integridad	Parcial, la modificación de algunos archivos o información del sistema es posible, pero el atacante no tiene control sobre lo que puede modificar, o el alcance de lo que el atacante puede afectar es limitado
Impacto en la disponibilidad	Ninguno, no hay impacto en la disponibilidad del sistema

Complejidad de acceso	Medio, las condiciones de acceso son algo especializadas. Se deben cumplir algunas condiciones previas para explotar
Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 30 Vulnerabilidad reportada Windows 10

Sistema Windows 11

Vulnerabilidad de elevación de privilegios de llamada a procedimiento local avanzado de Windows [44].

Puntación CVSS	6.9
Impacto de la Confidencialidad	Completo, hay una divulgación total de la información, lo que da como resultado que se revelen todos los archivos del sistema
Impacto de integridad	Completo, hay un compromiso total de la integridad del sistema. Hay una perdida completa de la protección del sistema, lo que da como resultado que todo el sistema se vea comprometida
Impacto en la disponibilidad	Completa, hay un cierre total del recurso afectado. El atacante puede hacer que el recurso no esté disponible por completo
Complejidad de acceso	Medio, las condiciones de acceso son algo especializadas. Se deben cumplir algunas condiciones previas para explotar
Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 31. Vulnerabilidad reportada Windows 11

Análisis de resultados de Wireshark

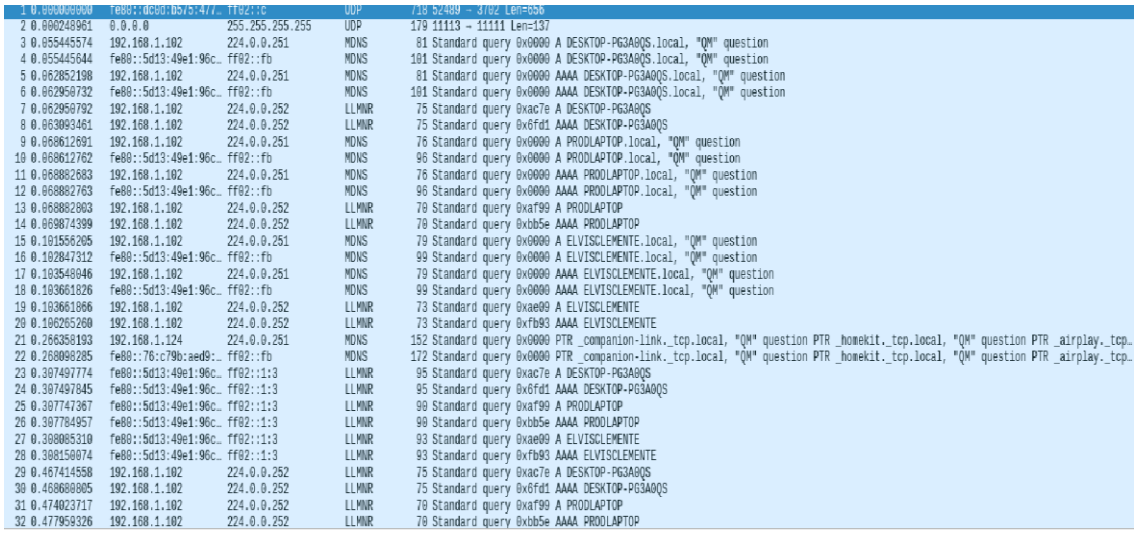
Las alertas presentadas en la aplicación de Wireshark se dan por problemas en la comunicación entre dispositivos por alguna anomalía que Wireshark detecta [40]. Esto se debe a que algún paquete llegó incompleto por alguna afectación al momento de llegar al receptor puede haciendo que la longitud del paquete no coincida o esté fuera del rango esperado por lo que el dispositivo pide que se reenvíe el paquete para poder concretar la comunicación [40]. El problema de paquete duplicado se refiere que algún punto de la comunicación entre esos dispositivos se duplicó la información enviada [40].

Ip origen	Ip destino	Color de reporte	Protocolo	Análisis
192.168.1.84	192.168.1.20	plomo	TCP	Flags de Syn y Fin, Término de comunicación
192.168.1.84	192.168.1.1	plomo	TCP	Flags de Syn y Fin, Término de comunicación

192.168.1.1	192.168.1.84	Rojo	TCP	Error en la comunicación reenvió de paquete
192.168.1.84	192.168.1.1	Rojo	TCP	Error en la comunicación reenvío de paquete
192.168.1.84	192.168.1.16	plomo	TCP	Flags de Syn y Fin, Término de comunicación
192.168.1.84	192.168.1.14	plomo	TCP	Flags de Syn y Fin, Término de comunicación
192.168.1.84	192.168.1.10	plomo	TCP	Flags de Syn y Fin, Término de comunicación
192.168.1.84	192.168.1.10	Rojo	TCP	Error en la comunicación reenvío de paquete
192.168.1.84	192.168.1.14	Rojo	TCP	Error en la comunicación reenvío de paquete
192.168.1.10	192.168.1.84	Rojo	TCP	Error en la comunicación reenvío de paquete
255.255.255.255	192.168.1.165	Rojo	TCP	Error en la comunicación reenvío de paquete
192.168.1.165	255.255.255.255	Rojo	TCP	Error en la comunicación reenvío de paquete
74.125.34.46	192.168.1.84	Negro	TCP	El envío de paquete está fallando, paquete duplicado, fallo de comprobación de paquetes
192.168.1.84	74.125.34.46	Negro	TCP	Él envió de paquete está fallando, paquete duplicado, fallo de comprobación de paquetes
192.168.1.85	192.168.1.2	Rojo	TCP	Error en la comunicación reenvío de paquete
192.168.1.2	192.168.1.85	Rojo	TCP	Error en la comunicación reenvío de paquete
192.168.1.85	192.168.1.20	Rojo	TCP	Error en la comunicación reenvío de paquete

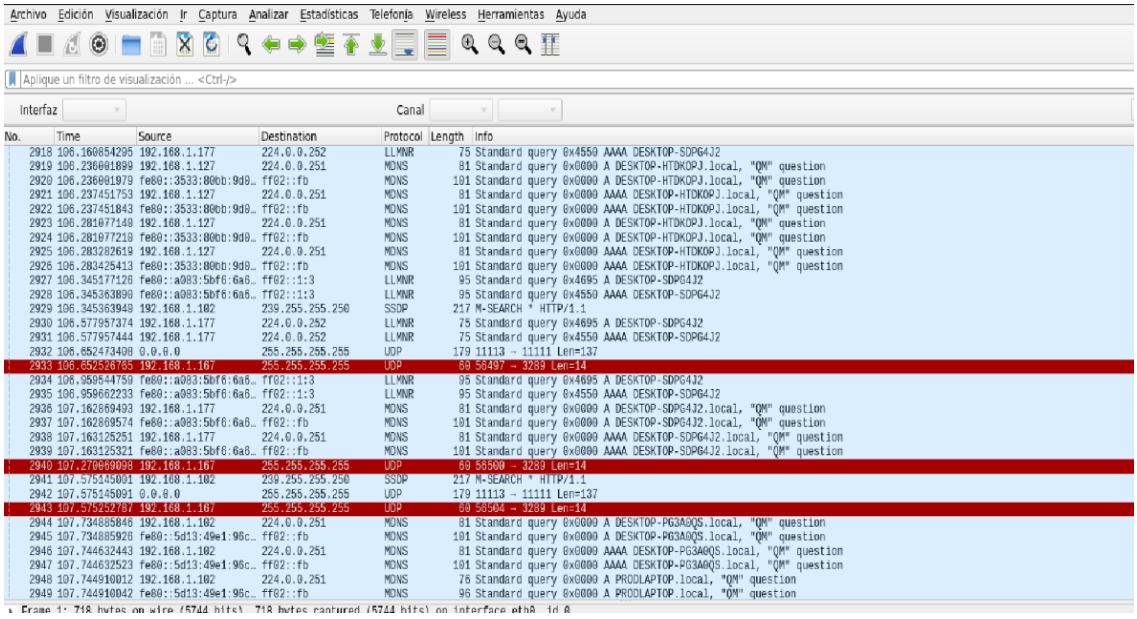
192.168.1.85	192.168.1.24	Rojo	TCP	Error en la comunicación reenvío de paquete
192.168.1.20	192.168.1.85	Rojo	TCP	Error en la comunicación reenvío de paquete
192.168.1.22	192.168.1.85	Rojo	TCP	Error en la comunicación reenvío de paquete

Tabla 32. Reporte de problemas en Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::dc0d:b575:477…	ff02::c	UDP	718	52489 → 3702 Len=656
2	0.000248961	0.0.0.0	255.255.255.255	UDP	179	11113 → 11111 Len=137
3	0.055445574	192.168.1.102	224.0.0.251	MDNS	81	Standard query 0x0000 A DESKTOP-PG3A0QS.local, "QM" question
4	0.055445644	fe80::5d13:49e1:96c…	ff02::fb	MDNS	101	Standard query 0x0000 A DESKTOP-PG3A0QS.local, "QM" question
5	0.062852198	192.168.1.102	224.0.0.251	MDNS	81	Standard query 0x0000 AAAA DESKTOP-PG3A0QS.local, "QM" question
6	0.062950732	fe80::5d13:49e1:96c…	ff02::fb	MDNS	101	Standard query 0x0000 AAAA DESKTOP-PG3A0QS.local, "QM" question
7	0.062950792	192.168.1.102	224.0.0.252	LLMNR	75	Standard query 0xac7e A DESKTOP-PG3A0QS
8	0.063093461	192.168.1.102	224.0.0.252	LLMNR	75	Standard query 0x6fd1 AAAA DESKTOP-PG3A0QS
9	0.068612691	192.168.1.102	224.0.0.251	MDNS	76	Standard query 0x0000 A PRODLAPTOP.local, "QM" question
10	0.068612762	fe80::5d13:49e1:96c…	ff02::fb	MDNS	96	Standard query 0x0000 A PRODLAPTOP.local, "QM" question
11	0.068882683	192.168.1.102	224.0.0.251	MDNS	76	Standard query 0x0000 AAAA PRODLAPTOP.local, "QM" question
12	0.068882763	fe80::5d13:49e1:96c…	ff02::fb	MDNS	96	Standard query 0x0000 AAAA PRODLAPTOP.local, "QM" question
13	0.068882803	192.168.1.102	224.0.0.252	LLMNR	70	Standard query 0xaf99 A PRODLAPTOP
14	0.069874399	192.168.1.102	224.0.0.252	LLMNR	70	Standard query 0xbb5e AAAA PRODLAPTOP
15	0.101556205	192.168.1.102	224.0.0.251	MDNS	79	Standard query 0x0000 A ELVISCLEMENTE.local, "QM" question
16	0.102847312	fe80::5d13:49e1:96c…	ff02::fb	MDNS	99	Standard query 0x0000 A ELVISCLEMENTE.local, "QM" question
17	0.103548046	192.168.1.102	224.0.0.251	MDNS	79	Standard query 0x0000 AAAA ELVISCLEMENTE.local, "QM" question
18	0.103661826	fe80::5d13:49e1:96c…	ff02::fb	MDNS	99	Standard query 0x0000 AAAA ELVISCLEMENTE.local, "QM" question
19	0.103661866	192.168.1.102	224.0.0.252	LLMNR	73	Standard query 0xae09 A ELVISCLEMENTE
20	0.106265260	192.168.1.102	224.0.0.252	LLMNR	73	Standard query 0xfb93 AAAA ELVISCLEMENTE
21	0.266358193	192.168.1.124	224.0.0.251	MDNS	152	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question PTR _airplay._tcp…
22	0.268098285	fe80::76:c79b:aed9:…	ff02::fb	MDNS	172	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question PTR _airplay._tcp…
23	0.307497774	fe80::5d13:49e1:96c…	ff02::1:3	LLMNR	95	Standard query 0xac7e A DESKTOP-PG3A0QS
24	0.307497845	fe80::5d13:49e1:96c…	ff02::1:3	LLMNR	95	Standard query 0x6fd1 AAAA DESKTOP-PG3A0QS
25	0.307747367	fe80::5d13:49e1:96c…	ff02::1:3	LLMNR	90	Standard query 0xaf99 A PRODLAPTOP
26	0.307784957	fe80::5d13:49e1:96c…	ff02::1:3	LLMNR	90	Standard query 0xbb5e AAAA PRODLAPTOP
27	0.308085310	fe80::5d13:49e1:96c…	ff02::1:3	LLMNR	93	Standard query 0xae09 A ELVISCLEMENTE
28	0.308150874	fe80::5d13:49e1:96c…	ff02::1:3	LLMNR	93	Standard query 0xfb93 AAAA ELVISCLEMENTE
29	0.467414558	192.168.1.102	224.0.0.252	LLMNR	75	Standard query 0xac7e A DESKTOP-PG3A0QS
30	0.468680805	192.168.1.102	224.0.0.252	LLMNR	75	Standard query 0x6fd1 AAAA DESKTOP-PG3A0QS
31	0.474023717	192.168.1.102	224.0.0.252	LLMNR	70	Standard query 0xaf99 A PRODLAPTOP
32	0.477959326	192.168.1.102	224.0.0.252	LLMNR	70	Standard query 0xbb5e AAAA PRODLAPTOP

Figura 8 Escaneo de la red con Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
2918	106.160854295	192.168.1.177	224.0.0.252	LLMNR	75	Standard query 0x4550 AAAA DESKTOP-SDPG4J2
2919	106.236001899	192.168.1.127	224.0.0.251	MDNS	81	Standard query 0x0000 A DESKTOP-HTDKOPJ.local, "QM" question
2920	106.236001979	fe80::3533:80bb:9d8…	ff02::fb	MDNS	101	Standard query 0x0000 A DESKTOP-HTDKOPJ.local, "QM" question
2921	106.237451753	192.168.1.127	224.0.0.251	MDNS	81	Standard query 0x0000 AAAA DESKTOP-HTDKOPJ.local, "QM" question
2922	106.237451843	fe80::3533:80bb:9d8…	ff02::fb	MDNS	101	Standard query 0x0000 AAAA DESKTOP-HTDKOPJ.local, "QM" question
2923	106.281077140	192.168.1.127	224.0.0.251	MDNS	81	Standard query 0x0000 A DESKTOP-HTDKOPJ.local, "QM" question
2924	106.281077210	fe80::3533:80bb:9d8…	ff02::fb	MDNS	101	Standard query 0x0000 A DESKTOP-HTDKOPJ.local, "QM" question
2925	106.283282619	192.168.1.127	224.0.0.251	MDNS	81	Standard query 0x0000 AAAA DESKTOP-HTDKOPJ.local, "QM" question
2926	106.283425413	fe80::3533:80bb:9d8…	ff02::fb	MDNS	101	Standard query 0x0000 AAAA DESKTOP-HTDKOPJ.local, "QM" question
2927	106.345177126	fe80::a083:5bf6:6a8…	ff02::1:3	LLMNR	95	Standard query 0x4695 A DESKTOP-SDPG4J2
2928	106.345363890	fe80::a083:5bf6:6a8…	ff02::1:3	LLMNR	95	Standard query 0x4550 AAAA DESKTOP-SDPG4J2
2929	106.345363948	192.168.1.102	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2930	106.577957374	192.168.1.177	224.0.0.252	LLMNR	75	Standard query 0x4695 A DESKTOP-SDPG4J2
2931	106.577957444	192.168.1.177	224.0.0.252	LLMNR	75	Standard query 0x4550 AAAA DESKTOP-SDPG4J2
2932	106.652473408	0.0.0.0	255.255.255.255	UDP	179	11113 → 11111 Len=137
2933	106.652526765	192.168.1.167	255.255.255.255	UDP	60	56497 → 3289 Len=14
2934	106.959544759	fe80::a083:5bf6:6a8…	ff02::1:3	LLMNR	95	Standard query 0x4695 A DESKTOP-SDPG4J2
2935	106.959662233	fe80::a083:5bf6:6a8…	ff02::1:3	LLMNR	95	Standard query 0x4550 AAAA DESKTOP-SDPG4J2
2936	107.162869493	192.168.1.177	224.0.0.251	MDNS	81	Standard query 0x0000 A DESKTOP-SDPG4J2.local, "QM" question
2937	107.162869574	fe80::a083:5bf6:6a8…	ff02::fb	MDNS	101	Standard query 0x0000 A DESKTOP-SDPG4J2.local, "QM" question
2938	107.163125251	192.168.1.177	224.0.0.251	MDNS	81	Standard query 0x0000 AAAA DESKTOP-SDPG4J2.local, "QM" question
2939	107.163125321	fe80::a083:5bf6:6a8…	ff02::fb	MDNS	101	Standard query 0x0000 AAAA DESKTOP-SDPG4J2.local, "QM" question
2940	107.270069098	192.168.1.167	255.255.255.255	UDP	60	56500 → 3289 Len=14
2941	107.575145091	192.168.1.102	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2942	107.575145091	0.0.0.0	255.255.255.255	UDP	179	11113 → 11111 Len=137
2943	107.575252787	192.168.1.167	255.255.255.255	UDP	60	56504 → 3289 Len=14
2944	107.734885846	192.168.1.102	224.0.0.251	MDNS	81	Standard query 0x0000 A DESKTOP-PG3A0QS.local, "QM" question
2945	107.734885926	fe80::5d13:49e1:96c…	ff02::fb	MDNS	101	Standard query 0x0000 A DESKTOP-PG3A0QS.local, "QM" question
2946	107.744632443	192.168.1.102	224.0.0.251	MDNS	81	Standard query 0x0000 AAAA DESKTOP-PG3A0QS.local, "QM" question
2947	107.744632523	fe80::5d13:49e1:96c…	ff02::fb	MDNS	101	Standard query 0x0000 AAAA DESKTOP-PG3A0QS.local, "QM" question
2948	107.744910012	192.168.1.102	224.0.0.251	MDNS	76	Standard query 0x0000 A PRODLAPTOP.local, "QM" question
2949	107.744910042	fe80::5d13:49e1:96c…	ff02::fb	MDNS	96	Standard query 0x0000 A PRODLAPTOP.local, "QM" question

Figura 9 Escaneo de la red con Wireshark

2.5.3. FASE 3: PLAN DE ACCIÓN

En esta fase se va a proponer políticas de seguridad por lo que la empresa no mantiene normativas de seguridad vigentes ni documentadas como lo cual se detalla a continuación:

Desarrollo de la política de seguridad

2.5.3.1. PLANIFICACIÓN DE LA POLÍTICA

Debido a que en los equipos actuales se han identificado los riesgos antes expuestos, es necesario la creación de políticas de seguridad.

Según el análisis de riesgos realizado a los equipos se ha logrado determinar cuáles son aquellos que necesitan una política de seguridad para reforzar su seguridad y cuidar la información que contiene el equipo.

2.5.3.2. CREACIÓN DE LA POLÍTICA

Políticas Adaptado a Sans

Política de respuesta a la violación de datos

Alcance

- Firewall
- Equipos involucrados

Responsabilidad

- Finanzas
- Legal
- Recurso Humanos
- Jefe de departamento afectado
- Jefe del Área de TI

Política:

Se notificará el robo, incumplimiento o exposición [46]. TI, junto con el equipo forense designado, analizará la infracción o exposición para determinar la causa raíz [46]:

- Poner una denuncia de robo de datos del sistema

- Proporcionar acceso a los investigadores
- Determinar cómo ocurrió la violación o exposición
- Determinar los tipos de datos involucrados
- Determinar el origen del ataque
- El departamento legal notificará a los afectados sobre los datos vulnerados

Política de seguridad del laboratorio DMZ

Alcance:

- Firewall
- Switch Principal
- Red de Datos

Responsabilidad:

- Jefe corporativo
- Recurso Humano
- Jefe del Área de TI
- Asistente del Área de TI

Política:

Propiedad y Responsabilidades [47].

- Todos los laboratorios DMZ nuevos deben presentar una justificación comercial con aprobación a nivel de presidente de la institución.
- La organización que es propietaria de los laboratorios es responsable de asignar gerentes de laboratorios.
- Los gerentes y sus asistentes de los laboratorios deberán estar disponible las 24 horas para emergencias.
- La organización debe mantener un dispositivo de firewall entre los laboratorios DMZ e Internet.

Requisitos generales de configuración [47].

- Los laboratorios DMZ no deben estar conectados a las redes internas corporativas, ya sea directamente o mediante una conexión inalámbrica.

- Los dispositivos de firewall mantenidos por la organización deben configurarse de acuerdo con los principios de acceso mínimo y las necesidades del laboratorio DMZ.
- El dispositivo de firewall debe ser el único punto de acceso entre el laboratorio DMZ y el resto de las redes. Cualquier forma de conexión cruzada que pase por alto el dispositivo de firewall esta estrictamente prohibida.
- Las configuraciones originales del firewall y cualquier cambio en las mismas deben ser revisadas y aprobadas por el jefe de TI, quien puede requerir medidas de seguridad adicionales según sea necesario.
- Los servicios y aplicaciones que no cumplan con los objetivos institucionales deben deshabilitarse.

Política de uso de Internet

Alcance:

- Herramientas de monitoreo
- Switch
- Router

Responsable

- Jefe del Área de TI
- Asistente de TI
- Recurso Humano

Política:

Uso de Recursos [48].

- El acceso a internet se aprobará y proporcionará solo si se identifican necesidades razonables.
- Los servicios de internet se otorgarán en función de las responsabilidades laborales actuales del empleado.
- Los requisitos de acceso a internet de los usuarios serán revisados periódicamente por los departamentos de la empresa para garantizar que existan necesidades continuas.

Uso permitido [48].

- El uso de internet se otorga con el único propósito de apoyar las actividades para llevar a cabo las funciones laborales.
- Todos los usuarios deben seguir los principios corporativos con respecto al uso de recursos y ejercer buen juicio al usar internet.
- El uso aceptable de internet para realizar funciones laborales puede incluir:
    - ✓ Comunicación entre empleados y no empleados con fines comerciales.
    - ✓ Soporte técnico de TI descargando actualizaciones y parches de software.
    - ✓ Investigar.

Uso personal [48].

- El uso de los recursos informáticos de la empresa para acceder a internet con fines personales, sin la aprobación de recurso humanos y del departamento de TI, puede considerarse causa de acción disciplinaria que puede incluir el despido.
- Los usuarios que eligen almacenar o trasmitir información personal, como claves privadas, números de tarjetas de crédito o certificados, o hacer uso de "billeteras" de internet, lo hacen bajo su propio riesgo, la empresa no es responsable de ninguna perdida de información consecuente de propiedad personal.

Uso prohibido [48].

- Se prohíbe específicamente la adquisición, el almacenamiento y difusión de datos que sean ilegales, pornográficos o que representen negativamente la raza, el sexo o el credo.
- La compañía también prohíbe la realización de una empresa comercial, la actividad política, la participación en cualquier forma de recopilación de inteligencia de nuestras instalaciones, la participación en actividades fraudulentas o la difusión deliberada de materiales falsos o difamatorios.
- Acceder a información de la empresa que no está dentro del ámbito de su trabajo. Esto incluye la lectura no autorizada de la información de la cuenta del cliente, el acceso no autorizado a la información del archivo del personal y el acceso a información que no es necesaria para la ejecución adecuada de las funciones laborales

- Usar indebidamente, divulgar sin la debida autorización o alterar la información del cliente o del personal. Esto incluye realizar cambios no autorizados en un archivo de personal o compartir datos electrónicos del cliente o del personal con personal no autorizado.

Monitoreo [48].

- La gerencia se reserva el derecho de examinar el correo electrónico, los directorios de archivos personales, el acceso web y otra información almacenada en las computadoras de la empresa, en cualquier momento y sin previo aviso.

Política de protección contra malware del servidor

Alcance:

- Firewall
- Servidores

Responsabilidad:

- Jefe de Área de TI
- Asistente del área de TI

Política:

Antivirus [49].

- Todos los servidores deben tener instalada una aplicación antivirus que ofrezca protección de escaneo en tiempo real para archivos y aplicaciones que se ejecutan en el sistema de destino.

2.5.3.3 Revisión de la Política

Al término del diseño de la política de seguridad, la institución deberá asignar un personal para su posterior revisión independiente sobre la vigencia e implementación de las Políticas de seguridad. La política de seguridad de la información se debe revisar en una frecuencia establecida para determinar si ocurrieron o no cambios significativos, para asegurar que siga siendo apropiada, adecuada y efectiva.

Una parte principal de la revisión periódica es el mantenimiento, donde se debe tomar en cuenta estas revisiones para mejoras futuras. Deberán crear procedimientos definidos de revisión por el gerente, que estará incluido en un cronograma de la ejecución de las políticas de seguridad.

2.5.3.4 Aprobación de la Política

El último paso para el diseño de la política de seguridad es la aprobación, como objetivo es tener el apoyo de la institución, por lo que deberá ser firmado por una persona que tenga autoridad en la organización. Una vez realizada la aprobación se deberá ejecutar las políticas de seguridad, por lo que es necesario escoger a la persona que va a estar a cargo de la ejecución de la política seguridad.

El personal encargado de la aprobación de la política será quien tenga la responsabilidad de reconocer la importancia de proteger los equipos por medio de la aprobación y ejecución de las políticas.

2.5.3.5 Conclusiones y Recomendaciones de las Políticas

Conclusiones

- La empresa no cuenta con medidas de seguridad que puedan guiarse o que estén documentados, como consecuencias se puede estimar los riesgos que los equipos puedan presentar y que afecten a las actividades de la empresa.
- La institución actualmente presenta riesgos en sus equipos, lo cual se puede contrarrestar con la aplicación de actividades y tareas descritas en la política, así como llevar el control de estas medidas de seguridad.

Recomendaciones

- Es necesario que la documentación generada para las medidas de seguridad sea revisada una vez por año para mantener la eficacia de las políticas.
- Es necesario actualizar las políticas de seguridad, revisando si los estándares de seguridad tienen nuevas versiones para garantizar el correcto funcionamiento de los equipos.
- Se recomienda implementar un sistema de control de peticiones HTTPS para monitorear el tráfico de red de la institución.

2.5.4. FASE 4: IMPLEMENTACIÓN

En esta fase se va a detallar los procedimientos que se realizó para la implementación del script dentro de la infraestructura de institución en la cual se detalla en el siguiente reporte:

<table>
<tr><td colspan="4">UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN</td></tr>
<tr><td colspan="4">Sistema de control de peticiones https mediante Algoritmo de Python para la detección de tráfico de red anómalo para una empresa de productos enlatados</td></tr>
<tr><td>Realizado por:</td><td>Gómez Ruidiaz José</td><td rowspan="2">Nombre del reporte:</td><td rowspan="2">Reporte Fase de Implementación</td></tr>
<tr><td>Fecha</td><td>15/05/2022</td></tr>
<tr><td colspan="4">Fase de Implementación
Objetivos de la fase:
Implementar el sistema de control de peticiones HTTPS
Técnica:
La técnica que se empleó fue la investigación, usando recursos tecnológicos para recopilar la información
Herramientas Tecnológicas aplicadas:
Se procedió a utilizar un computador para ejecutar el sistema de control desarrollado en lenguaje Python y con ayuda del navegador para búsquedas de amenazas.
Tiempo de ejecución:
El tiempo que tomó en la ejecución fue de 2 meses
Procedimiento:
Se desarrolló el algoritmo en base a la indagación en los sitios web para poder capturar el tráfico, luego de obtener la información, se procedió a la codificación del script que está diseñado para trabajar en cualquier sistema operativo siempre y cuando tenga instalado las librerías, lo único que se diferencia es la declaración del hardware que se va a utilizar ya que para identificación y captura de datos se utilizó Wireshark para identificar la interfaz de WiFi y posteriormente realizar el análisis del tráfico de red mediante el sistema que se implementó.
Resultados obtenidos:
Durante el análisis se recopiló todo el tráfico que se realiza por lo cual se catalogó como tráfico normal y anómalo, para luego ser analizado en caso de ser necesario.</td></tr>
</table>

Además de recibir las respectivas alertas a un dispositivo que tiene instalado telegram, para poder ver la información de la actividad anómalo que fue encontrada en el tráfico de red.

Arquitectura del Script

En la siguiente arquitectura Figura 10 se explica como el algoritmo va a trabajar, que comienzo con las solicitudes que se recopila desde la Ethernet que pasa por el ordenador donde se encuentre la ejecución del script y él toma la decisión de enviar a la base de datos en caso de ser una tráfico normal o si envía la notificación a telegram y guarda la información en la base de datos en caso de ser un tráfico anómalo.

Figura 10 Arquitectura del Script

Elaboración del Script

Como primeros pasos se procedió a detallar como iba a ejecutar el código, con la ayuda de la librería socket en Python capturamos los datos que pasaba por nuestra tarjeta de red, con el inconveniente que debíamos definir que protocolo pasaba por la tarjeta de red y si existía pérdida de paquetes, solo hacia el análisis del tráfico de red interna del equipo.

```
import socket
import struct
import textwrap
import requests
from virus_total_apis import PublicApi
TAB_1 ='\t -'
TAB_2 ='\t\t -'
TAB_3 ='\t\t\t -'
TAB_4 ='\t\t\t\t -'

DATA_TAB_1 ='\t -'
DATA_TAB_2 ='\t\t -'
DATA_TAB_3 ='\t\t\t -'
DATA_TAB_4 ='\t\t\t\t -'

def main():
    API_KEY="4f278505cb5bdba811cb3c117457db459c8b3334e7f2d74d34f16d4b3bd7e4a0"
    conn=socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.ntohs(3))
    while True:
        raw_data, addr = conn.recvfrom(65536)
        dest_mac, src_mac, eth_proto, data = ethernet_frame(raw_data)
        print('\n  Encabezado de la trama de Ethernet')
        print(TAB_1+ 'Destinatario:{}, Emisor:{}, protocologo: {}'.format(dest_mac,src_mac,eth_proto))
        #telegram_bot_sendtext(TAB_1 + 'IPv4 Packet: ')
        #telegram_bot_sendtext(TAB_1+ 'Destinatario:{}, Emisor:{}, protocologo: {}'.format(dest_mac,src_mac,eth_proto) )
        # 8 bits para IPV4
        if eth_proto == 8:
            (version, header_length, ttl, proto, src, target, data) =ipv4_packet(data)
            print(TAB_1 + ' Paquete de IPV4')
            print(TAB_2 + 'Version: {},Llongitud de la cabecera: {}, TTL: {}'.format(version, header_length, ttl))
            print(TAB_2 + 'Numero de bits: {}, Emisor: {}, Objetivo: {}'.format(proto, src, target))
```

Figura 11 Primera estructura del script parte 1

```python
#descomprimiendo el paquete de ethernet
def ethernet_frame(data):
    dest_mac,src_mac,proto=struct.unpack('! 6s 6s H', data[:14])
    return get_mac_addr(dest_mac), get_mac_addr(src_mac), socket.htons(proto), data[14:]

#formato de la Mac Address (AAA:BBB:CCC:EEE)
def get_mac_addr(bytes_addr):
    bytes_str=map('{:02x}'.format, bytes_addr)
    return ':'.join(bytes_str).upper()

#descomprimir paquete de ipv4
def ipv4_packet(data):
    version_header_length= data[0]
    version = version_header_length >> 4
    header_length = (version_header_length & 15) * 4
    ttl, proto, src, target = struct.unpack('! 8x B B 2x 4s 4s', data[:20])
    return version, header_length, ttl, proto, ipv4(src), ipv4(target), data[header_length:]

#retorno  del formato de Ipv4 address(192.168.1.1)
def ipv4(addr):
    return '.'.join(map(str, addr))


#descomprimiendo paquete de ICMP
```

Figura 12 Primera estructura del script parte 2

Al ver que el código era ineficiente se procedió a cambiar las librerías, por lo que se decidió a usar Pyshark, en cual tiene el mismo propósito que el software de Wireshark, pero en este caso se utilizó para la captura de datos de manera eficiente, pero existían algunos problemas, el primero que tenía un número exacto de repeticiones cosa que debía ejecutarse hasta que el administrador decida parar el algoritmo y segundo solo se guardaba en un archivo txt, pero debía ser almacenado en una base de datos para luego hacer su respetivo análisis.

```python
import pyshark
import time
import requests
from virus_total_apis import PublicApi
TAB_1 ='\t -'
TAB_2 ='\t\t -'
TAB_3 ='\t\t\t -'
TAB_4 ='\t\t\t\t -'
# definicion de interfaz
#networkInterface = "eth0"
API_KEY="4f278505cb5bdba811cb3c117457db459c8b3334e7f2d74d34f16d4b3bd7e4a0"
bloqueo=[]
valor=False
def main():

# captura del trafico
    capture = pyshark.LiveCapture(interface='eth0')
    for packet in capture.sniff_continuously(packet_count=100000000000000000000000000000000000000000):

        try:
            # Obteniendo la fecha y hora actua
            localtime = time.asctime(time.localtime(time.time()))

            # Obteniendo el contenido de la IPV4
            protocol = packet.transport_layer   # protocol type
            src_addr = packet.ip.src            # source address
            src_port = packet[protocol].srcport   # source port
            dst_addr = packet.ip.dst            # destination address
            dst_port = packet[protocol].dstport   # destination port
```

Figura 13 Segunda estructura del script parte 1

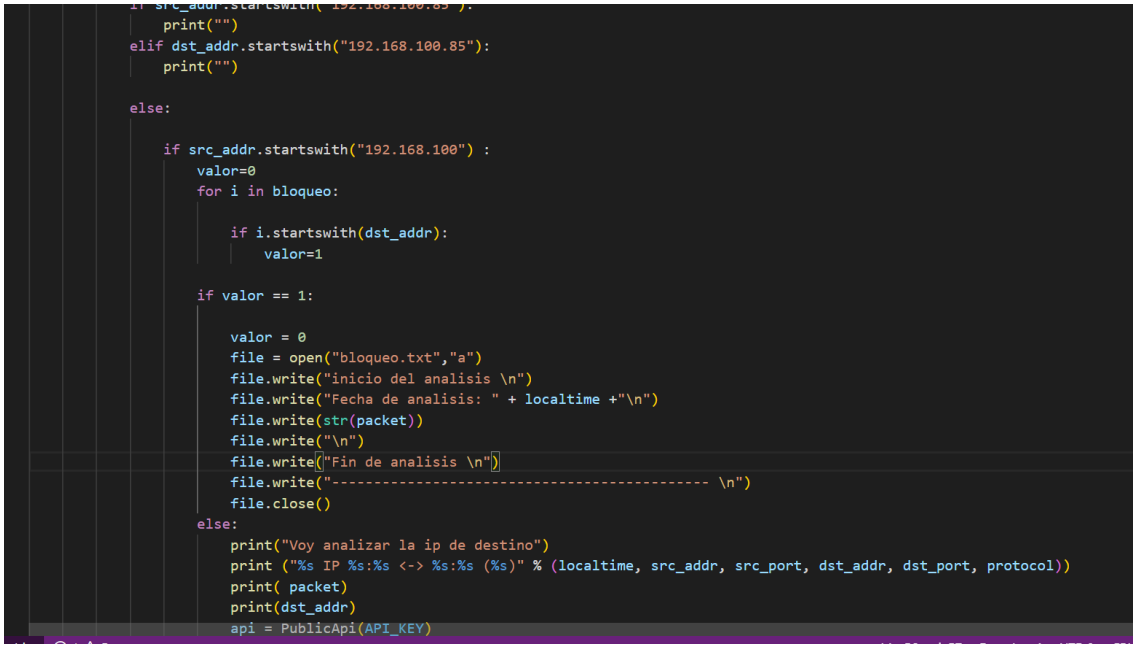
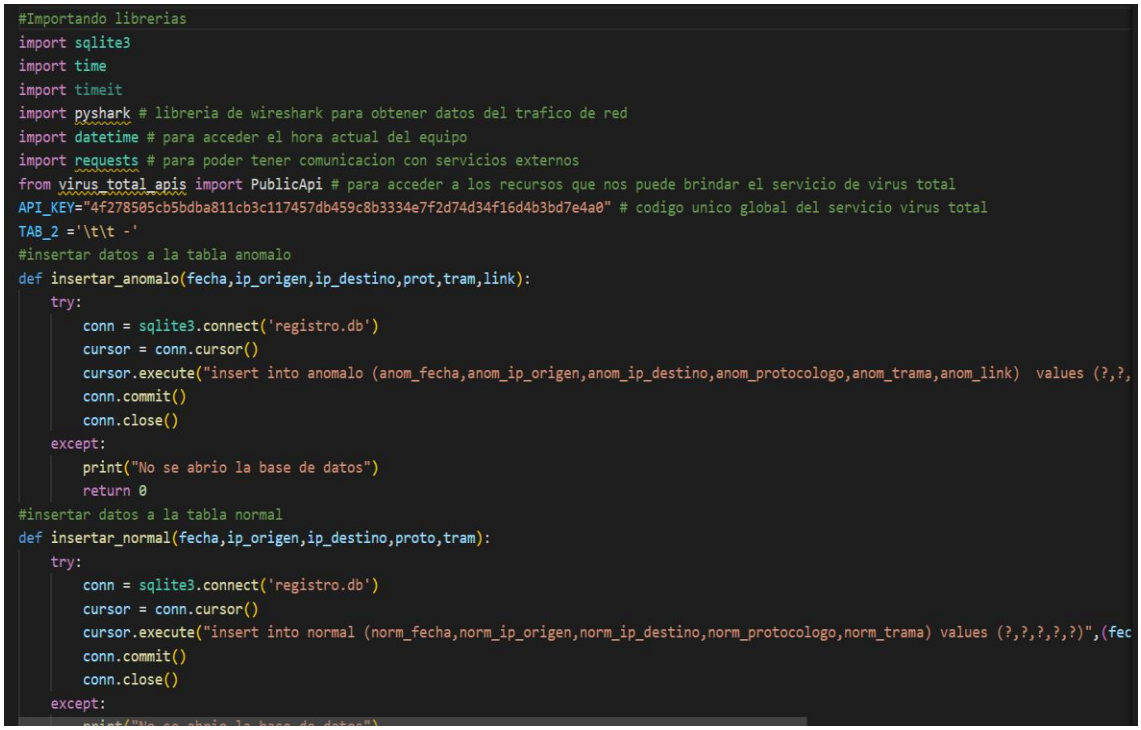


Figura 14 Segunda estructura del script parte 2

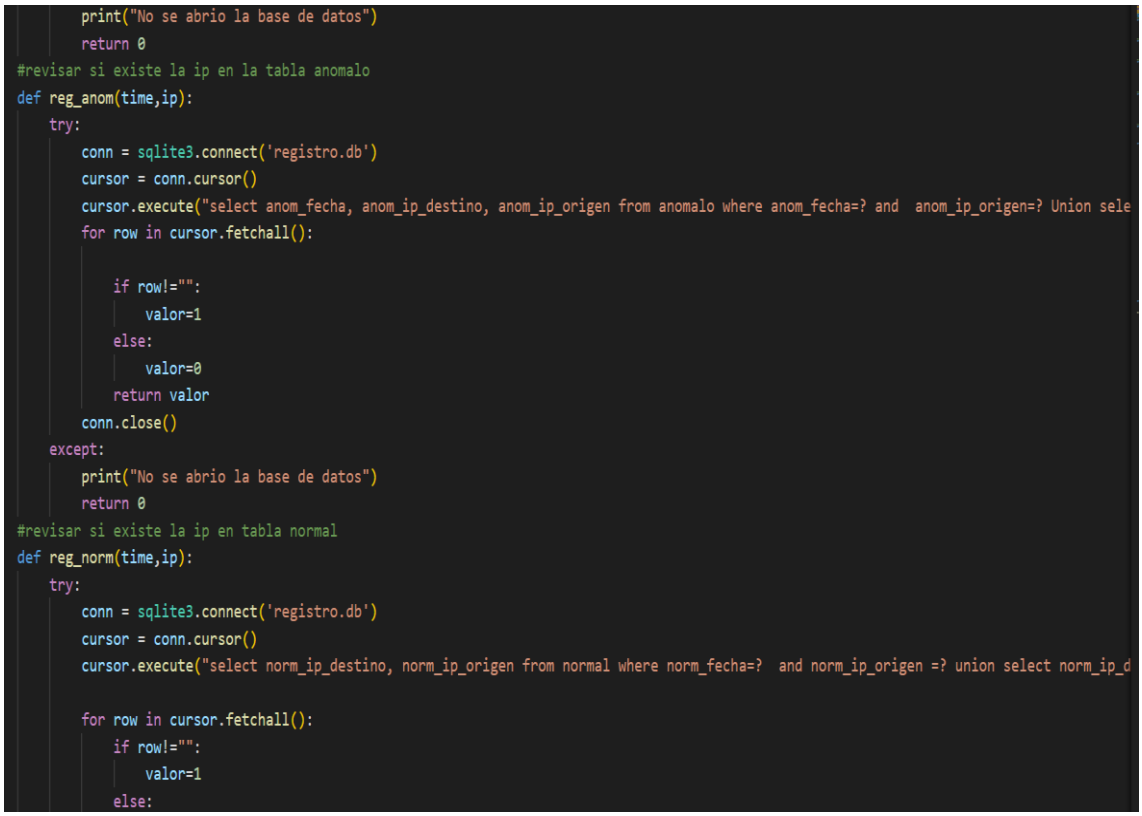
Figura 15 Segunda estructura del script parte 1

Luego de ver los problemas que tenían las versiones anteriores se procedió a corregirlas implementando cambios de librerías, incorporación de base de datos y hacer que el código se termine de ejecutar cuando el administrador lo desee y por último la incorporación de una gráfica estadística en donde podrá visualizar la cantidad de tráfico que ha analizado el script.



```
#Importando librerias
import sqlite3
import time
import timeit
import pyshark # libreria de wireshark para obtener datos del trafico de red
import datetime # para acceder el hora actual del equipo
import requests # para poder tener comunicacion con servicios externos
from virus_total_apis import PublicApi # para acceder a los recursos que nos puede brindar el servicio de virus total
API_KEY="4f278505cb5bdba811cb3c117457db459c8b3334e7f2d74d34f16d4b3bd7e4a0" # codigo unico global del servicio virus total
TAB_2 ='\t\t -'
#insertar datos a la tabla anomalo
def insertar_anomalo(fecha,ip_origen,ip_destino,prot,tram,link):
    try:
        conn = sqlite3.connect('registro.db')
        cursor = conn.cursor()
        cursor.execute("insert into anomalo (anom_fecha,anom_ip_origen,anom_ip_destino,anom_protocologo,anom_trama,anom_link)  values (?,?,
        conn.commit()
        conn.close()
    except:
        print("No se abrio la base de datos")
        return 0
#insertar datos a la tabla normal
def insertar_normal(fecha,ip_origen,ip_destino,proto,tram):
    try:
        conn = sqlite3.connect('registro.db')
        cursor = conn.cursor()
        cursor.execute("insert into normal (norm_fecha,norm_ip_origen,norm_ip_destino,norm_protocologo,norm_trama) values (?,?,?,?,?)",(fec
        conn.commit()
        conn.close()
    except:
```

Figura 16 Estructura final del script parte 2



```
        print("No se abrio la base de datos")
        return 0
#revisar si existe la ip en la tabla anomalo
def reg_anom(time,ip):
    try:
        conn = sqlite3.connect('registro.db')
        cursor = conn.cursor()
        cursor.execute("select anom_fecha, anom_ip_destino, anom_ip_origen from anomalo where anom_fecha=? and  anom_ip_origen=? Union sele
        for row in cursor.fetchall():

            if row!="":
                valor=1
            else:
                valor=0
            return valor
        conn.close()
    except:
        print("No se abrio la base de datos")
        return 0
#revisar si existe la ip en tabla normal
def reg_norm(time,ip):
    try:
        conn = sqlite3.connect('registro.db')
        cursor = conn.cursor()
        cursor.execute("select norm_ip_destino, norm_ip_origen from normal where norm_fecha=?  and norm_ip_origen =? union select norm_ip_d

        for row in cursor.fetchall():
            if row!="":
                valor=1
            else:
```

Figura 17 Estructura final del script parte 3

```
def telegram_bot_sendtext(bot_message):

    bot_token = '2079185114:AAGF0FrUh2OAoALbtCqC8vL34s396D32jCk'
    bot_chatID = '1298272687'
    send_text = 'https://api.telegram.org/bot' + bot_token + '/sendMessage?chat_id=' + bot_chatID + '&parse_mode=Markdown&text=' + bot_mess

    response = requests.get(send_text)

    return response.json()
def trama():
     guia="192.168.1"
     capture = pyshark.LiveCapture(interface='eth0')
     i=5
     while capture.sniff_continuously(packet_count=i):
         i=i+2
         for packet in capture.sniff_continuously(packet_count=i):
            try:
             localtim = time.asctime(time.localtime(time.time()))
             localtime = datetime.date.today()
          # Obteniendo el contenido de la IPV4
             protocol = packet.transport_layer   # protocol type
             src_addr = packet.ip.src            # source address
             src_port = packet[protocol].srcport   # source port
             dst_addr = packet.ip.dst            # destination address
             dst_port = packet[protocol].dstport   # destination port
             if src_addr.startswith(guia):
                 v=reg_anom(localtime,dst_addr)
                 s=reg_norm(localtime,dst_addr)
                 if v == 1:
                     l=""
```

Figura 18 Estructura final del script parte 4

```
             elif dst_addr.startswith(guia):
                 v=reg_anom(localtime,src_addr)
                 s=reg_norm(localtime,src_addr)
                 if v == 1:
                     l=""
                     pack=str(packet)
                     insertar_anomalo(localtime,src_addr,dst_addr,protocol,pack,l)
                 elif s==1:
                     pack=str(packet)
                     insertar_normal(localtime,src_addr,dst_addr,protocol,pack)
                 else:
                     print ("%s IP %s:%s <-> %s:%s (%s)" % (localtime, src_addr, src_port, dst_addr, dst_port, protocol))
                     print( packet)
                     response = api.get_url_report(src_addr)
                     if response ["response_code"] == 200:
                        print(response)
                        if response["results"]["positives"] >0:
                            print ("Pagina con Malware")
                            print(response["results"]["permalink"])
                                #print(response["results"]["verbose_msg"])
                            lin=str(response["results"]["permalink"])
                            anomalia = str(response["results"]["positives"])
                            telegram_bot_sendtext('Hora de Registro: '+ localtim + TAB_2 + 'IP Origen: '+ src_addr + TAB_2 + 'Puerto Origen
                            insertar_anomalo(localtime,src_addr,dst_addr,protocol,pack,lin)
                        else:
                            print ("Pagina segura")
                            insertar_normal(localtime,src_addr,dst_addr,protocol,pack)
                     else:
                         insertar_normal(localtime,src_addr,dst_addr,protocol,pack)
             else:
```

Figura 19 Estructura final del script parte 5

```python
import sqlite3 #libreria de base de datos
import dash
import dash_core_components as dcc # renderiza objetos en dash
import dash_html_components as html #renderiza html
#import plotly.express as go
import plotly.graph_objs as go #renderiza objetos de plotly
import pandas as pd #libreria comun para manejar datos
from dash.dependencies import Input, Output

def consulta_base_fecha():
    try:
        conn = sqlite3.connect('registro.db')
        df=pd.read_sql_query("select anom_fecha as fecha from anomalo union select norm_fecha as fecha from normal",conn)
        print(df.head())
        conn.close()
        fecha= df['fecha'].unique()
        fecha.sort()
        op= [{'label':c, 'value':c} for c in fecha]
        print(op)
        return op

    except:
        print("No se abrio la base de datos")
        return 0

app= dash.Dash()
def dashboard(fe):
```

Figura 20 Estructura del script del reporte parte 1

```python
    external_stylesheet=['https://codepen.io/chriddyp/pen/bWLwgP.css']
    tickFont = {'size':9, 'color':"rgb(30,30,30)"}
    #app = dash.Dash(external_stylesheets=external_stylesheet)
    app.title = 'Reporte'
    app.layout = html.Div([

        html.H1('Nombre y Logo de la empresa'),
        html.H2('Reporte de Analisis de Trafico de red'),
        html.Div(
            dcc.Dropdown(
                id = 'fechas',
                options= fe,
                value = "2022-04-13"
            ),
            style={'width':'20%'}
        D
        ),
        dcc.Graph(
            id='cases',
            config= {'displayModebar':False}
        ),
        # html.H2(children='Tabla de RePorte de IP'),
        #tabla(s)
            #generate_table()



    ])
    app.run_server()
@app.callback(Output(component_id='cases',component_property='figure'),
```

Figura 21 Estructura del script del reporte parte 2

```
    app.run_server()
@app.callback(Output(component_id='cases',component_property='figure'),
[Input(component_id='fechas',component_property='value')])

def consulta_fec_dato(dato):

    try:
        a=['trafico anomalo','trafico normal','trafico total']
        conn = sqlite3.connect('registro.db')
        df=pd.read_sql_query("Select Sum(t.tota)as total from (select count(*) as tota,anom_fecha as fec from anomalo GROUP by fec  union
        # conn.close()
        tota= df['total'].unique()
        print(tota)
        fig=go.Figure(data=[go.Bar(y=tota,x=a)],layout=go.Layout(height=600, width=800,barmode='stack'))
        fig.update_layout(title='Reporte de la fecha {}'.format(dato))

        #tabla(s)
        return fig

    except:
        print("No se abrio la base de datos")
        return 0

def main():

    fec=consulta_base_fecha()
    dashboard(fec)

main()
```

Figura 22 Estructura del script del reporte parte 3

Ejecución en el sistema operativo Linux

Para la ejecución en el sistema operativo en linux se comprobó la actualización de las librerías, luego de verificar las actualizaciones se determinó que interfaz de red íbamos a utilizar para poder hacer la captura del tráfico de red.

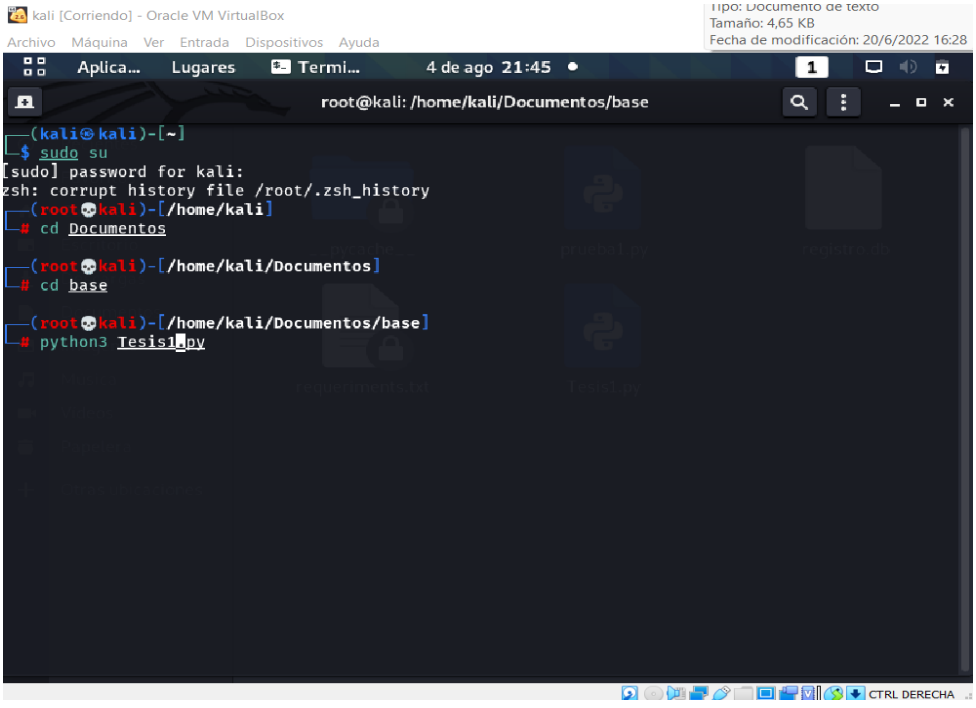


Figura 23 Ejecución de script en el sistema operativo Linux parte 1

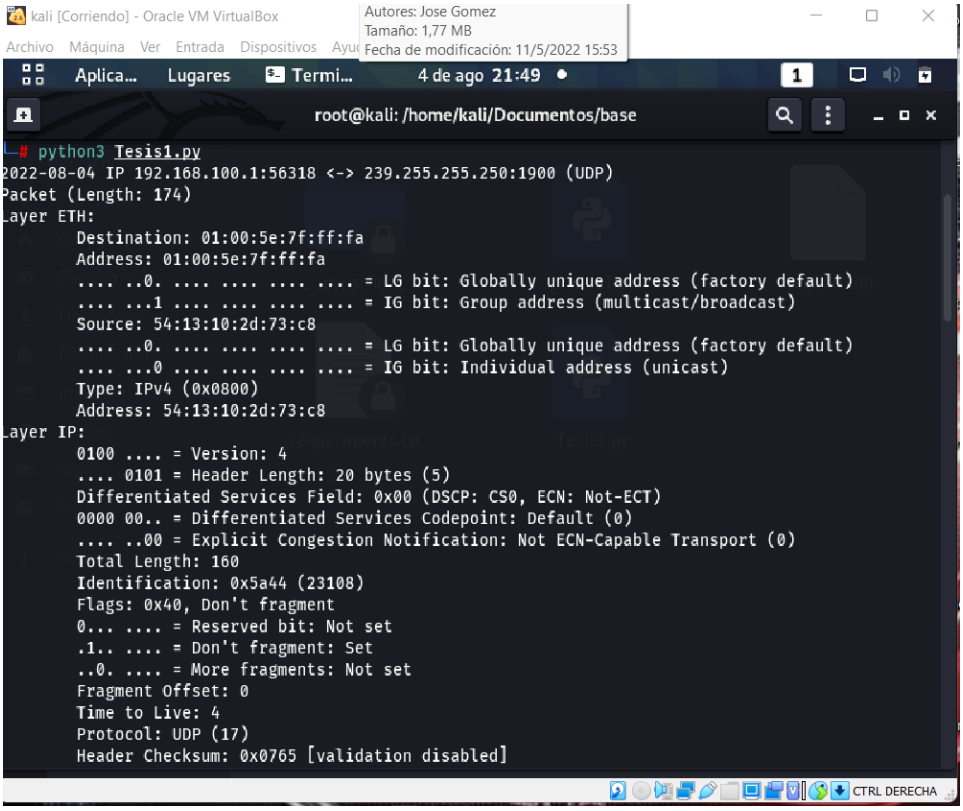


Figura 24 Ejecución del script en el sistema operativo Linux parte 2

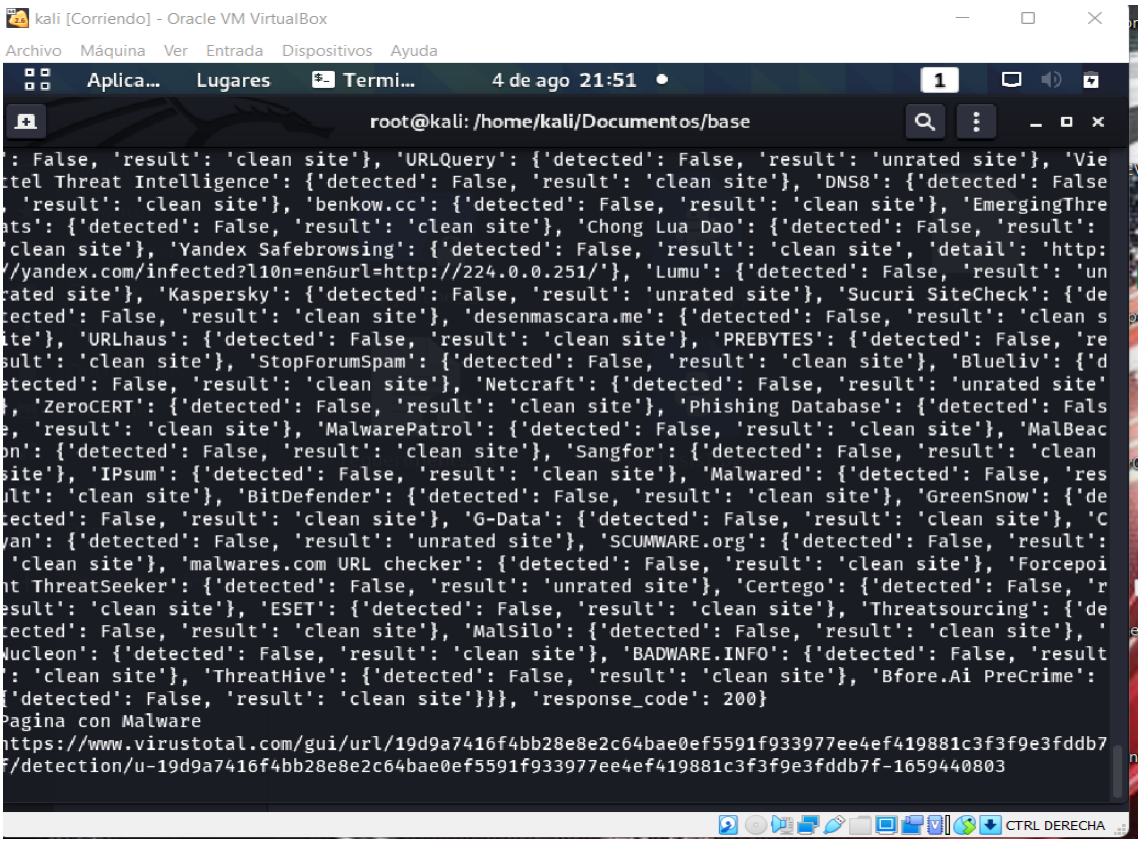


Figura 25 Ejecución del script en el sistema operativo Linux parte 3

Ejecución en el sistema operativo Windows

Para la ejecución en el sistema operativo en Windows se procedió a instalar las librerías necesarias para la ejecución del script y con la ayuda de Wireshark determinar la ruta de donde se encuentra los drivers de la interfaz de red para la captura de datos desde el algoritmo.

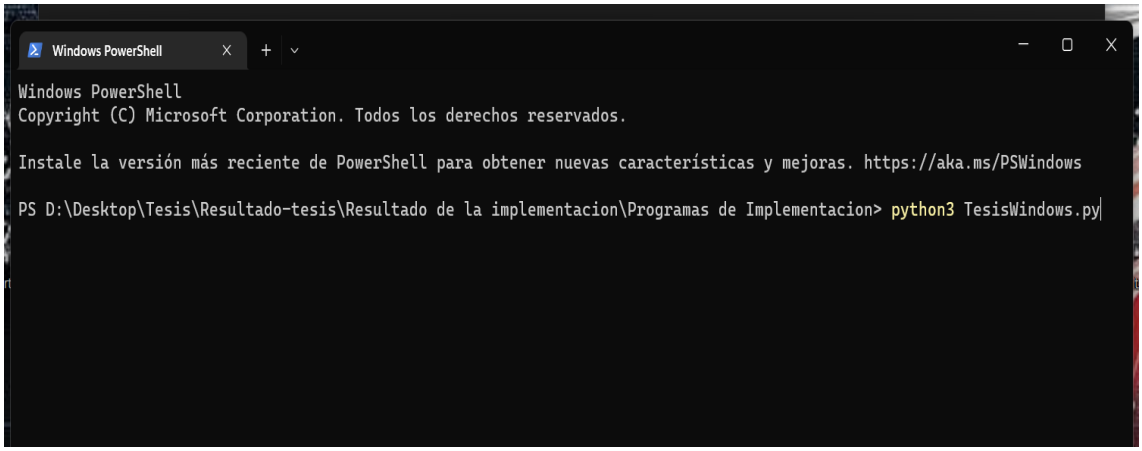


Figura 26 Ejecución del script en el sistema operativo Windows parte 1

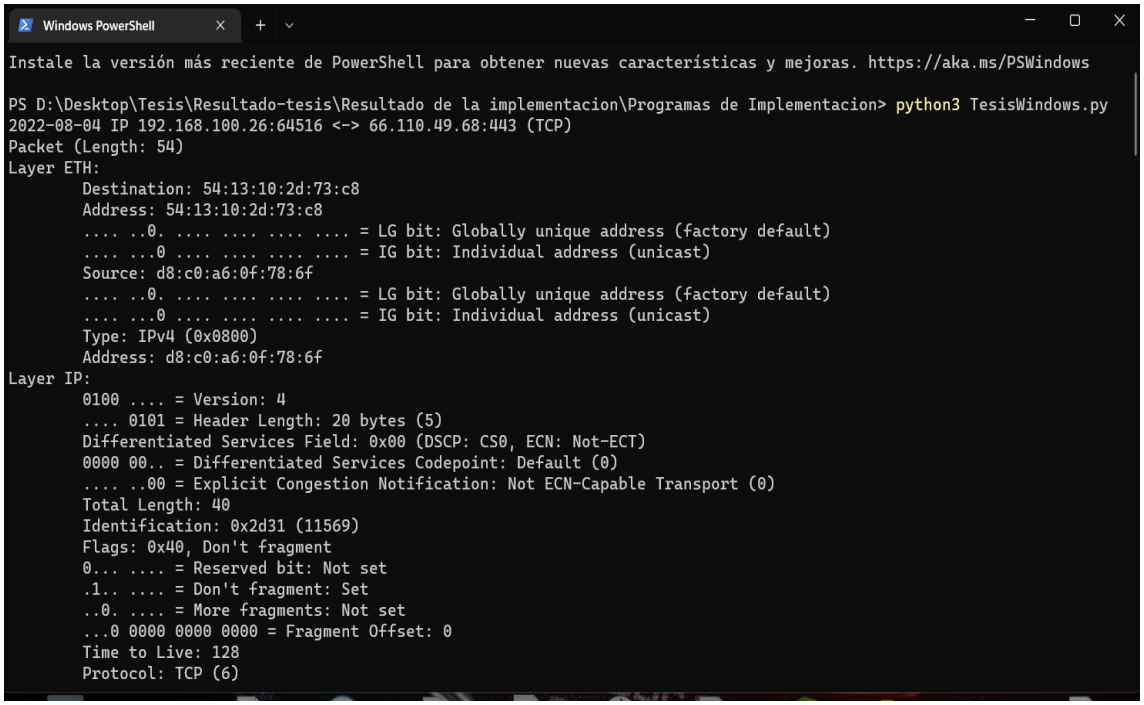


Figura 27 Ejecución del script en el sistema operativo Windows parte 2

Figura 28 Ejecución del script en el sistema operativo Windows parte 3

Resultado de la implementación

Análisis del día 25 de abril del 2022 se realizó un análisis de 1473 peticiones

IP de Origen	IP de Destino	Fecha y hora del evento	Protocolo	Puerto origen	Puerto destino
192.168.1.102	224.0.0.251	25-04-2022 16:20:37	UDP	5353	5353
192.168.1.250	255.255.255.255	25-04-2022 16:20:43	UDP	45970	29810
192.168.1.97	74.125.34.46	25-04-2022 16:21:01	TCP	53440	443
35.244.181.201	192.168.1.97	25-04-2022 16:27:31	TCP	443	38708

Tabla 33 Reporte de malware en *VirusTotal* del 25 de abril del 2022

Reporte del análisis 74.125.34.46

País del servicio	Servicio	Dominio	Políticas de certificación X509v3
Estados Unidos	Google	Virustotal.com	2.23.140.1.2.2

Tabla 34 Información del malware IP:74.125.34.46

Detalles de VirusTotal

La IP encontrada y catalogada como malware, tiene como dominio VirusTotal, pero adicional a eso la IP mencionada en anteriores reportes se definía como un ataque de fuerza bruta, también se realizan varias peticiones más de una vez debido a la existencia de varias bases de datos en el mundo definiéndolos como un tráfico anómalo.

Detalles de CVE Details

Existe una vulnerabilidad de desbordamiento de búfer en VirusTotal YARA git commit: 605b2edf07ed8eb9a2c61ba22eb2e7c362f47ba7 a través de yr_set_configuration en yara/libyara/libyara.c, lo que podría causar una denegación de servicio [46].

Puntación CVSS	4.3
Impacto de la Confidencialidad	Ninguno, no hay impacto en la confidencialidad del sistema
Impacto de integridad	Ninguno, No hay impacto en la integridad del sistema
Impacto en la disponibilidad	Parcial, hay un rendimiento reducido o interrupciones en la disponibilidad de recursos
Complejidad de acceso	Medio, las condiciones de acceso son algo especializadas, se deben cumplir algunas condiciones previas para explotar
Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 35 Reporte de malware de CVE IP:74.125.34.46

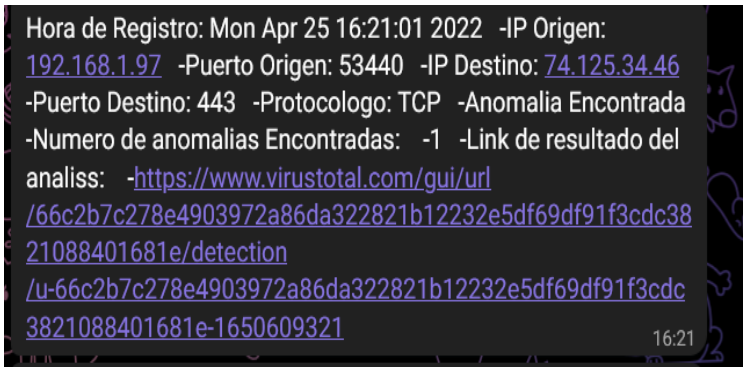


Figura 29 Reporte de malware de VirusTotal en telegram IP: 74.125.34.46

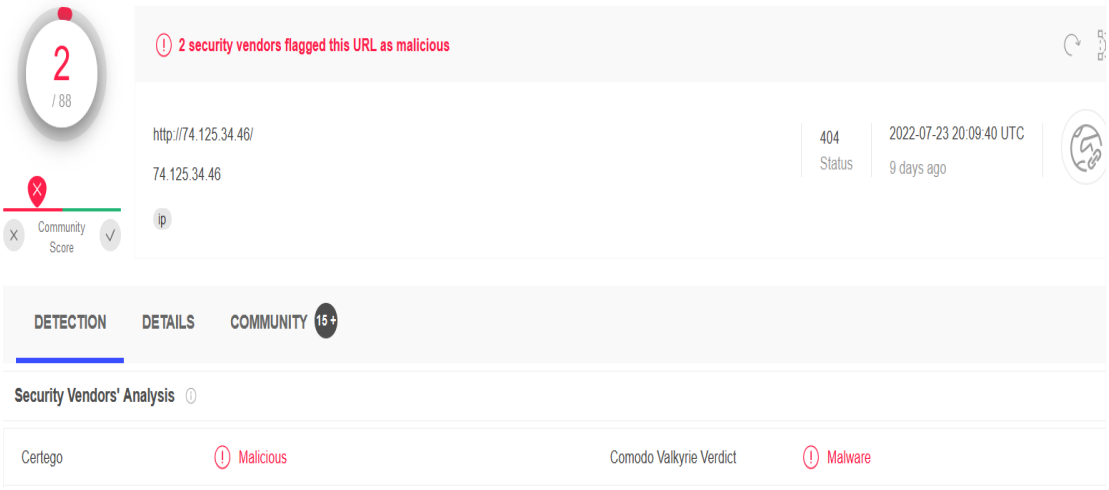


Figura 30 Visualización del reporte en VirusTotal IP:74.125.36.46

Reporte del análisis 35.244.181.201

País del servicio	Servicio	Dominio	Políticas de Seguridad de contenido
Estados Unidos	Mozilla	https://aus5.mozilla.org/	predeterminado-src 'ninguno'; marco-ancestros 'ninguno

Tabla 36 Información del malware IP: 35.244.181.201

Detalles de VirusTotal

La IP detectada y catalogada como malware se trata de unas de las extensiones que tiene la aplicación de Mozilla, en VirusTotal lo catalogaron como malicioso por lo que se encuentra deportada por algunas bases de datos de antivirus del mundo.

Detalles de CVE

El paquete convicto anterior a 6.2.2 es vulnerable a la contaminación de prototipos a través de la función de convicto debido a la falta de validación de parentKey [47].

Puntación CVSS	4.3
Impacto de la Confidencialidad	Parcial, hay una divulgación de información considerable
Impacto de integridad	Parcial, la modificación de algunos archivos o información del sistema es posible, pero el atacante no tiene control sobre lo que puede modificar, o el alcance de lo que el atacante puede afectar es limitado
Impacto en la disponibilidad	Parcial, hay un rendimiento reducido o interrupciones en la disponibilidad de recursos
Complejidad de acceso	Bajo, no existen condiciones de acceso especializadas o circunstancias atenuantes. Se requiere muy poco conocimiento o habilidad para explotar
Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 37 Reporte de malware en CVE IP: 35.244.181.201

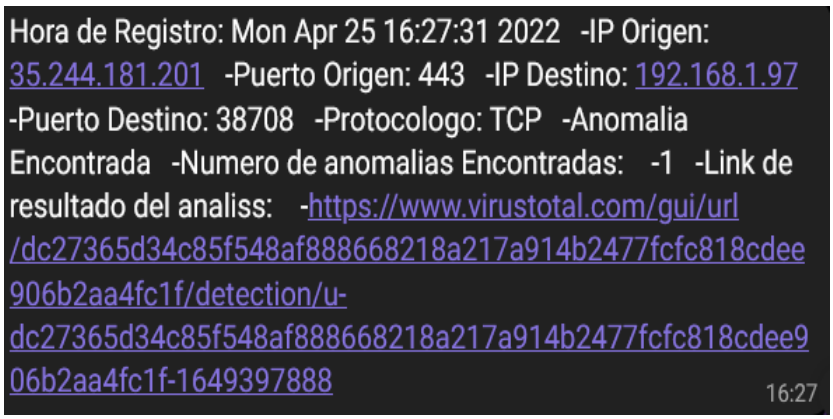


Figura 31 Reporte de malware de VirusTotal en telegram IP: 35.244.181.201

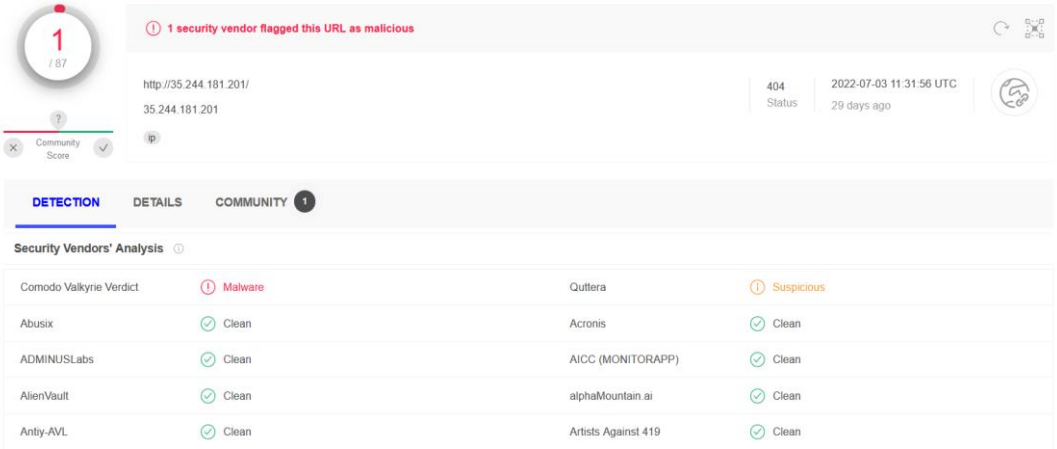


Figura 32 Visualización del reporte en VirusTotal IP:149.154.167.220

Para este día de análisis se recopiló 1473 peticiones durante un análisis aproximado de 2 horas de ejecución de las cuales 654 fueron peticiones con malware y 819 fueron peticiones de actividad normal.

Gráfica 1. Análisis de peticiones realizada el 25 de abril del 2022

Análisis del día 16 de mayo del 2022 se realizó un análisis de 278 peticiones

IP de Origen	IP de Destino	Fecha y hora del evento	Protocolo	Puerto origen	Puerto destino
192.168.1.126	224.0.0.251	16-05-2022 15:08:53	UDP	5353	5353
192.168.1.126	224.0.0.252	16-05-2022 15:08:59	UDP	50897	5355
192.168.1.250	255.255.255.255	16-05-2022 15:09:09	UDP	56368	29810

Tabla 38 Reporte de malware en virustotal del 16 de mayo del 2022

Reporte del análisis 224.0.0.251

País del servicio	Servicio	Dominio	Políticas de certificación X509v3
Estados Unidos	MCAST-NET	http://www.iana.org/assignments/multicast-addresses	

Tabla 39 Información del malware IP: 224.0.0.251

Detalles de VirusTotal

En la captura de esta IP nos menciona que es un malware, el motivo es porque este servicio hace comunicación con varios equipos para poder interactuar, en cual ha sido blanco por los atacantes en contagiar a otras máquinas que están dentro de la red.

Detalles de CVE

Una vulnerabilidad en la función de multidifusión independiente del protocolo (PIM) del software Cisco IOS XR podría permitir que un atacante remoto no autenticado haga que el proceso PIM se reinicie, lo que resultará en una condición de denegación de servicio en un dispositivo afectado [48]. La vulnerabilidad se debe al procesamiento incorrecto de los paquetes AutoRP creados. Un atacante podría aprovechar esta vulnerabilidad enviando paquetes manipulados al puerto UDP 496 en una dirección IP accesible en el dispositivo. Una explotación exitosa podría permitir que el atacante haga que el proceso PIM se reinicie [48].

Puntación CVSS	5.0
Impacto de la Confidencialidad	Ninguno, no hay impacto en la confidencialidad del sistema.
Impacto de integridad	Ninguno, no hay impacto en la integridad del sistema
Impacto en la disponibilidad	Parcial, hay un rendimiento reducido o interrupciones en la disponibilidad de recursos.
Complejidad de acceso	Bajo, no existen condiciones de acceso especializadas o circunstancias atenuantes. Se requiere muy poco conocimiento o habilidad para explotar
Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 40. Reporte de malware en CVE IP: 224.0.0.251

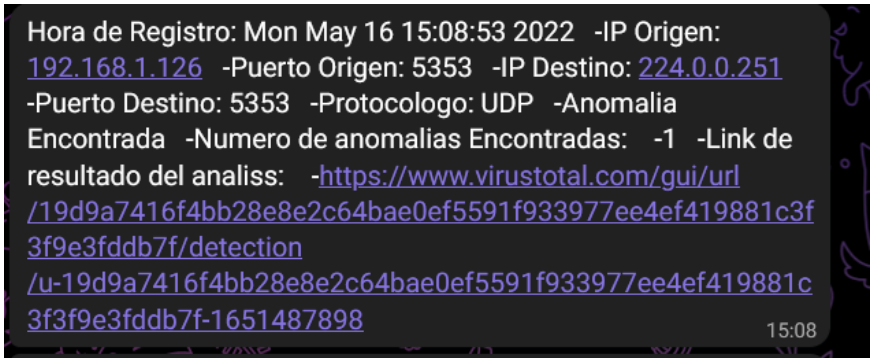


Figura 33 Reporte de malware de VirusTotal en telegram IP: 224.0.0.251

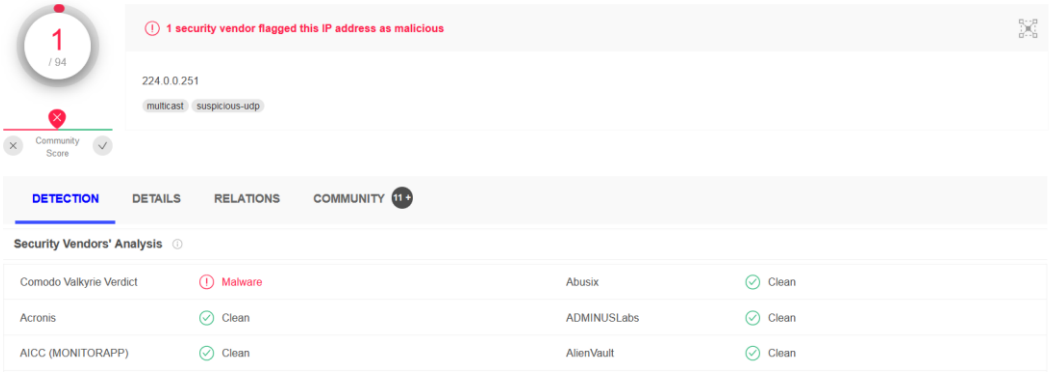


Figura 34 Visualización del reporte en VirusTotal IP:224.0.0.251

Análisis del día 20 de junio del 2022

Se realizó un análisis de 734 peticiones

IP de Origen	IP de Destino	Fecha y hora del evento	Protocolo	Puerto origen	Puerto destino
192.168.1.220	255.255.255.255	20-06-2022 09:25:28	UDP	34724	29810
192.168.1.70	20.190.154.138	20-06-2022 09:28:37	TCP	61347	443
192.168.1.70	20.189.173.9	20-06-2022 09:29:19	TCP	61484	443
192.168.1.70	31.13.67.16	20-06-2022 09:30:20	TCP	62823	443

Tabla 41 Reporte de malware en virustotal del 20 de Junio del 2022

Reporte del análisis 20.190.154.138

País del servicio	Servicio	Dominio	Políticas de certificación X509v3
Estados Unidos	Microsoft-Azure	https://cert.microsoft.com.	2.23.140.1.2.2

Tabla 42 Información del malware IP: 20.190.154.138

Detalles de Virus Total

La IP detectada está catalogada como malware porque en algún momento sus servicios fueron utilizados para un ataque de denegación de servicio por lo que algunas bases de datos de antivirus la siguen reportando como un intento de ataque a otros equipos.

Detalles de CVE

Existe una vulnerabilidad de ejecución remota de código cuando Azure App Service/Antares en Azure Stack no comprueba la longitud de un búfer antes de copiar la memoria en él [48]. Un atacante que aprovecha esta vulnerabilidad podría permitir que el usuario ejecute una función sin privilegios en el contexto de NT AUTHORITY\system, por lo tanto, escapa del Sandbox [48]. La actualización de seguridad aborda la vulnerabilidad al garantizar que Azure App Service desinfecte las entradas del usuario, también conocido como 'Vulnerabilidad de ejecución remota de código de Azure App Service' [48].

Puntación CVSS	10.0
Impacto de la Confidencialidad	Completo, hay una divulgación total de la información, lo que da como resultado que se revelen todos los archivos del sistema.
Impacto de integridad	Completo, hay un compromiso total de la integridad del sistema. Hay una perdida completa de la protección del sistema, lo que da como resultado que todo el sistema se vea comprometido
Impacto en la disponibilidad	Completo, hay un cierre total del recurso afectado. El atacante puede hacer que el recurso no esté disponible por completo
Complejidad de acceso	Bajo, no existen condiciones de acceso especializadas o circunstancias atenuantes. Se requiere muy poco conocimiento o habilidad para explotar.
Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 43 Reporte de malware en CVE IP: 20.190.154.138

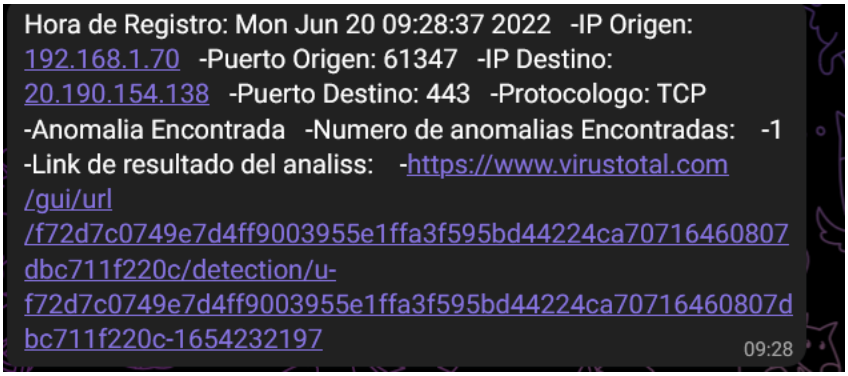


Figura 35 Reporte de malware de VirusTotal en telegram IP: 20.190.154.138

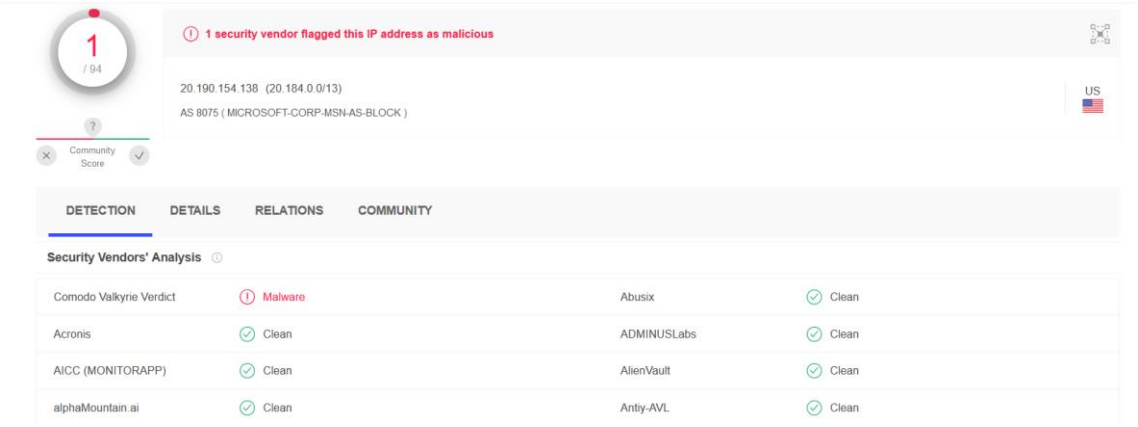


Figura 36 Visualización del reporte en VirusTotal IP:20.190.154.138

Para este día de análisis se recopiló 278 peticiones durante un análisis aproximado de 2 horas de ejecución de las cuales 110 fueron peticiones con malware y 168 fueron peticiones de actividad normal.

Gráfica 2. Análisis de peticiones realizada el 16 de mayo del 2022

Reporte de análisis 20.189.173.9

País del servicio	Servicio	Dominio	Políticas de certificación X509v3
Estados Unidos	Microsoft-Azure	https://cert.microsoft.com.	2.23.140.1.2.2

Tabla 44 Información del malware IP: 20.189.173.9

Detalles de Virus Total

La IP detectada está catalogada como malware porque en algún momento sus servicios fueron utilizados para un ataque de denegación de servicio por lo que algunas bases de datos de antivirus la siguen reportando como un intento de ataque a otros equipos.

Detalles de CVE

Existe una vulnerabilidad de ejecución remota de código cuando Azure App Service/Antares en Azure Stack no comprueba la longitud de un búfer antes de copiar la memoria en él [48]. Un atacante que aprovechan esta vulnerabilidad podría permitir que el usuario ejecutara una función sin privilegios para ejecutar código en el contexto de NT AUTHORITY\system, por lo tanto, escapa del Sandbox [48]. La actualización de seguridad aborda la vulnerabilidad al garantizar que Azure App Service desinfecte las entradas del usuario, también conocido como 'Vulnerabilidad de ejecución remota de código de Azure App Service' [48].

Puntación CVSS	10.0
Impacto de la Confidencialidad	Completo, hay una divulgación total de la información, lo que da como resultado que se revelen todos los archivos del sistema.
Impacto de integridad	Completo, hay un compromiso total de la integridad del sistema. Hay una perdida completa de la protección del sistema, lo que da como resultado que todo el sistema se vea comprometido
Impacto en la disponibilidad	Completo, hay un cierre total del recurso afectado. El atacante puede hacer que el recurso no esté disponible por completo
Complejidad de acceso	Bajo, no existen condiciones de acceso especializadas o circunstancias atenuantes. Se requiere muy poco conocimiento o habilidad para explotar.
Autentificación	No se requiere, no se requiere autenticación para aprovechar la vulnerabilidad
Acceso obtenido	Ninguna

Tabla 45. Reporte de malware en CVE IP: 20.189.173.9

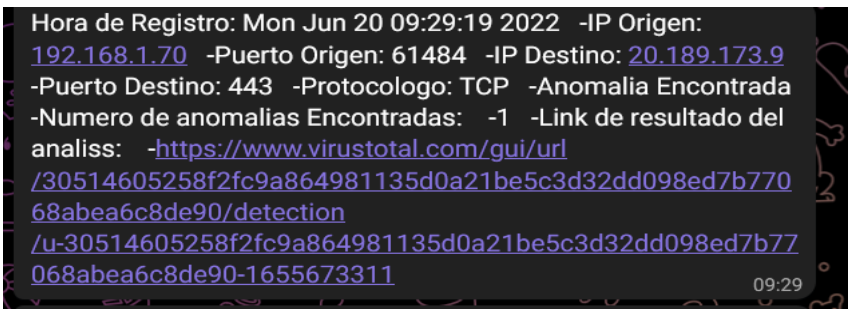


Figura 37 Reporte de malware de VirusTotal en telegram IP: 20.189.173.9

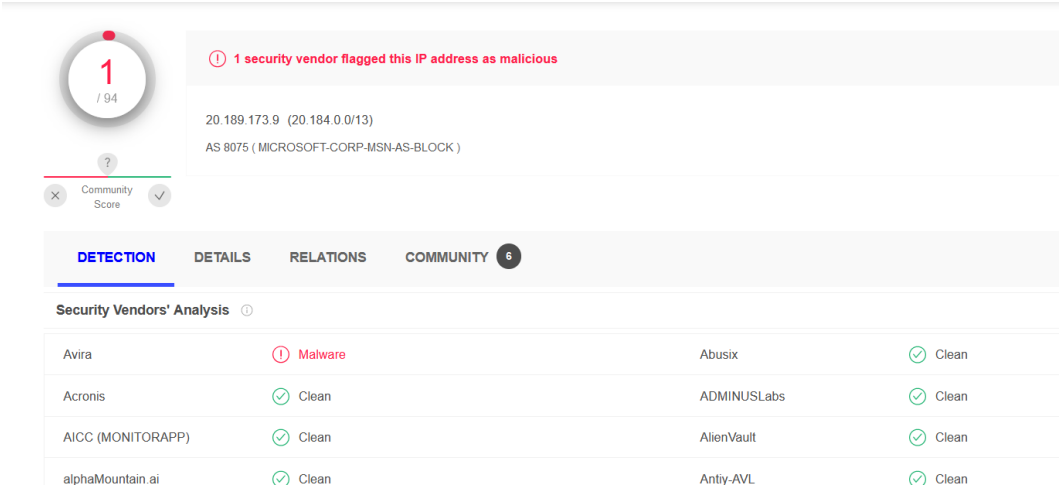
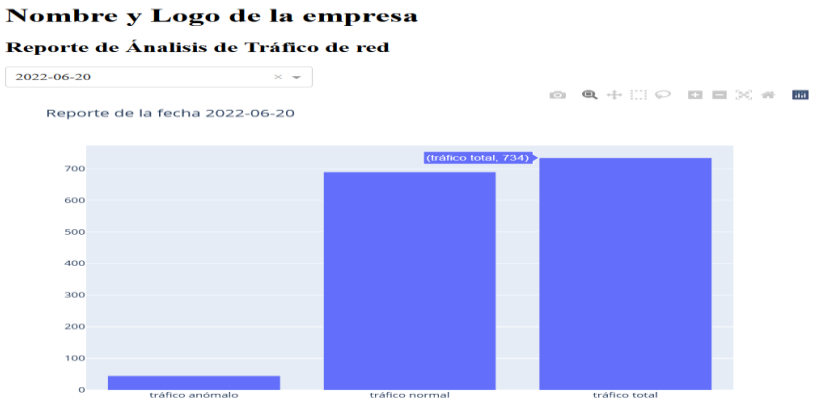


Figura 38 Visualización del reporte en VirusTotal IP:20.189.173.9

Para este día de análisis se recopiló 734 peticiones durante un análisis aproximado de 2 horas de ejecución de las cuales 45 fueron peticiones con malware y 689 fueron peticiones de actividad normal.



Gráfica 3. Análisis de peticiones realizada el 20 de junio del 2022

2.6. RESULTADOS

2.6.1. RESULTADOS FINALES

La propuesta tecnológica del desarrollo de un algoritmo para el control de peticiones web mediando código Python para la detección de trafico de red anómalo en una empresa de productos enlatados tiene como resultado los siguientes puntos:

- Para establecer los requerimientos del algoritmo se tomó en cuenta la información que manteníamos de la institución para la ejecución del script.

- El algoritmo esta desarrollado para que pueda interactuar en varios sistemas operativos siempre y cuando tenga las librerías instaladas para su implementación.

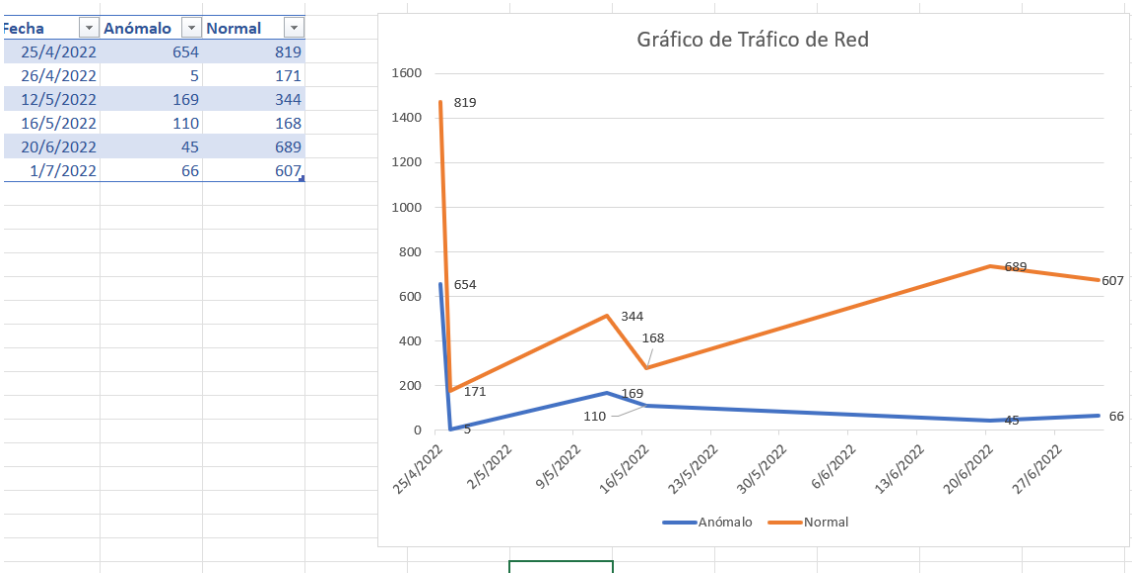
- El algoritmo puede capturar las peticiones de todos los equipos que están en la red, pero solo a los que están dentro de la trama de red.

- El algoritmo es capaz de procesar N peticiones por lo que la cifra exacta de la que puede visualizarse dependerá de la capacidad de la infraestructura de red como el equipo.

- El usuario final puede ver los reportes en telegram de manera más detalla, pero a la vez puede revisar en forma estadística los resultados del análisis que se hace por día.

- Para las pruebas realizadas se determinó que existe pequeñas anomalías que fueron reportadas, en lo que se hace énfasis en la revisión periódica de los sistemas informáticos para su solución.

- En la Gráfica 4 se puede visualizar los reportes que se ha almacenado en la base de datos, donde se muestra la cantidad de tráfico que fue reportada como malware por lo que se enciende una alerta en los sistemas de esta institución, pero también se visualiza que existe más tráfico normal que lo que se puede determinar que existe un pequeño grupo de equipos que están infectados.



Gráfica 4. Resultados del Tráfico de Red

2.6.2. RESULTADO DE LA VARIABLE

Variable: Tiempo en la identificación un equipo con malware

Proceso antes del script: 3 – 20 días

Proceso usando el script: 1 – 5 minutos

Mejora: 10 días aproximadamente

De acuerdo con los resultados mostrado, se puede observar que existe una reducción del tiempo en determinar un equipo con malware, por lo que se puede tomar decisiones correctivas para la eliminación y la implementación de las medidas de seguridad apropiada para que este evento no vuelva a presentarse.

CONCLUSIONES

- El uso de la técnica de recopilación de la información permitió analizar varias librerías y escoger las más eficiente para la captura del tráfico de red, además del envió de la información a una red social de su reporte.

- El desarrollo del script se basa en los requerimientos que tiene el área de sistemas, por las medidas de ciberseguridad que no mantiene y ante la exigencia de la implementación de una normativa de seguridad informática.

- La información recopilada en el script se podrá visualizar en cualquier momento, para su análisis más detalla de la actividad reportada, como también el cambio que puede tener un servicio de estar infectado al estar libre de malware.

- Las notificaciones que se envíen al telegram solo será del análisis que se realiza por el día, la información que hoy tenga en su telegram no será la misma para el día posterior.

- El reporte de telegram esta resumido para el mejor entendimiento del administrador por lo que si desea ver una información más detalla deberá acceder al link adjunto al mensaje enviado.

RECOMENDACIONES

- Se recomienda que se instalen las librerías necesarias para la ejecución del script en el sistema operativo adecuado.

- Se sugiere que el script se coloque en un servidor para la mejor captura del tráfico de red de la infraestructura de una institución.

- Para aprovechar la funcionalidad del script se recomienda que se revise en cada cierto tiempo, que el script este ejecutando se forma correcta.

- Se recomienda que se verifique que la información almacenada en la base de datos sean las apropiadas, se deberá acceder por comandos a las tablas de anomalías y normal para verificar que los datos sean los correctos.

- Se sugiere que la institución analice cada cierto tiempo las anomalías reportadas para una mejor toma de decisiones, en la cual se recomienda la visualización de gráficos estadísticos para su mejor comprensión.

BIBLIOGRAFÍA

[1] A. Rodriguez, «El Comercio,» 13 Enero 2021. [En línea]. Available: https://www.elcomercio.com/tendencias/ecuador-naciones-atacadas-hackers-tecnologia.html. [Último acceso: 17 Abril 2021].

[2] C. S. Antonio, «Universidad Autonoma de Madrid,» 26 Junio 2017. [En línea]. Available: https://repositorio.uam.es/handle/10486/679946. [Último acceso: 25 Octubre 2021].

[3] T. R. J. Alberto, «Universidad Pedagogica y Tecnologica de Colombia,» 2015. [En línea]. Available: https://repositorio.uptc.edu.co/handle/001/1724. [Último acceso: 25 Octubre 2021].

[4] O. V. V. d. Rocío, «Universidad de Las Fuerzas Armadas,» Diciembre 2011. [En línea]. Available: http://repositorio.espe.edu.ec/handle/21000/4984. [Último acceso: 25 Octubre 2021].

[5] Facsistel, «Resolución RCF-FST-SO-09 No. 03-2021,» Universidad Estatal Peninsula de Santa Elena, Santa Elena, 2021.

[6] Kaspersky, «Kaspersky,» [En línea]. Available: https://www.kaspersky.es/resource-center/threats/web. [Último acceso: 12 Noviembre 2021].

[7] Kaspersky, «Kaspersky,» [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security. [Último acceso: 12 Noviembre 2021].

[8] G. Nacional, «Planificacion,» Noviembre 2021. [En línea]. Available: planificacion.gob.ec/wp-content/uploads/2021/09/Plan-de-Creación-de-Oportunidades-2021-2025-Aprobado.pdf. [Último acceso: 30 Noviembre 2021].

[9] R. Hernandez Sampieri, C. Fernandez Collado y M. Del Pilar Baptisra, Metodologia de la Investigacion, Mexico: McGRAW-HILL, 2014.

[10] J. Ortega Candel, «Hacking Etico con Herrmientas Python,» Ra-MA, Madrid, 2018.

[11] D. Parada Serrano, A. Florez Abril y U. Gomez Prada, Modelo estructural de los observatorios de ciberseguridad: Perspectiva desde la dinamica de sistemas, Colombia: Editorial Univerdidad Pontificia Bolivariana, 2018.

[12] Asamblea Nacional Republica del Ecuador, «Telecomunicaciones,» 7 Junio 2022. [En línea]. Available: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf.

[13] VMware, «VMware,» [En línea]. Available: https://www.vmware.com/latam/solutions/virtualization.html. [Último acceso: 5 Mayo 2022].

[14] Oracle, «VirtualBox,» [En línea]. Available: https://www.virtualbox.org/. [Último acceso: 5 Noviembre 2021].

[15] g0tmi1k, «Kali,» [En línea]. Available: https://www.kali.org/docs/introduction/what-is-kali-linux/. [Último acceso: 5 Noviembre 2021].

[16] Oracle, «Oracle,» [En línea]. Available: https://www.oracle.com/mx/database/what-is-database/#WhatIsDBMS. [Último acceso: 25 Mayo 2022].

[17] MySQL, «MySQL,» [En línea]. Available: https://www.mysql.com/products/enterprise/. [Último acceso: 5 Noviembre 2021].

[18] AMAZON, «AMAZON,» [En línea]. Available: https://aws.amazon.com/es/what-is/api/. [Último acceso: 29 Mayo 2022].

[19] Telegram, «Telegram,» [En línea]. Available: https://core.telegram.org/api. [Último acceso: 29 Mayo 2022].

[20] VirusTotal, «VirusTotal,» [En línea]. Available: https://support.virustotal.com/hc/en-us/articles/115002100149-API. [Último acceso: 29 Mayo 2022].

[21] Python, «Python,» [En línea]. Available: https://docs.python.org/3/faq/general.html#what-is-python. [Último acceso: 5 Noviembre 2021].

[22] kiminewt, «GIthud,» 2021. [En línea]. Available: https://github.com/KimiNewt/pyshark. [Último acceso: 13 Abril 2022].

[23] GITHUD, «GITHUD,» [En línea]. Available: https://github.com/psf/requests. [Último acceso: 29 Mayo 2022].

[24] GITHUD, «GITHUD,» [En línea]. Available: https://github.com/pandas-dev/pandas. [Último acceso: 29 Mayo 2022].

[25] Plotly, «Plotly,» [En línea]. Available: https://dash.plotly.com/introduction. [Último acceso: 29 Mayo 2022].

[26] Wireshark, «Wireshark,» [En línea]. Available: https://www.wireshark.org/faq.html#wheretogethelp. [Último acceso: 06 Noviembre 2021].

[27] Nmap, «Nmap,» [En línea]. Available: https://nmap.org/man/es/index.html. [Último acceso: 6 Noviembre 2021].

[28] V. S. Code, «Visual Studio Code,» [En línea]. Available: https://code.visualstudio.com/docs/supporting/faq. [Último acceso: 6 Noviembre 2021].

[29] SANS, «SANS,» [En línea]. Available: https://www.sans.org/mlp/espanol/. [Último acceso: 1 Agosto 2022].

[30] A. T. Balderas Sergio, «Seguridad,» 7 Junio 2022. [En línea]. Available: https://revista.seguridad.unam.mx/numero30/thug-honeyclient-atrapando-sitios-web-maliciosos.

[31] L. F. Fuentes, «MALWARE, UNA AMENAZA DE INTERNET,» Universidad Nacional Autónoma de México, Mexico, 2008.

[32] S. Erique Javien y J. Sanchez Allende, «RIESGOS DE CIBERSEGURIDAD EN LAS EMPRESAS,» *TECNOLOGI@ Y DESARROLLO,* vol. XV, pp. 11-12, 2017.

[33] «CVE Details,» 11 Julio 2017. [En línea]. Available: https://www.cvedetails.com/cve/CVE-2001-1473/. [Último acceso: 12 Enero 2022].

[34] CVEDetails, «CVEDetails,» 31 Julio 2022. [En línea]. Available: https://www.cvedetails.com/cve/CVE-2004-1811/.

[35] C. Details, «CVE Details,» [En línea]. Available: https://www.cvedetails.com/cve/CVE-2012-0126/. [Último acceso: 31 Julio 2022].

[36] C. Details, «CVE Details,» [En línea]. Available: https://www.cvedetails.com/cve/CVE-2019-7659/. [Último acceso: 31 Julio 2022].

[37] C. Details, «CVE Details,» [En línea]. Available: https://www.cvedetails.com/cve/CVE-2017-0174/. [Último acceso: 31 Julio 2022].

[38] C. Details, «CVE Details,» [En línea]. Available: https://www.cvedetails.com/cve/CVE-2001-1155/. [Último acceso: 31 Julio 2022].

[39] C. Details, «CVE Details,» [En línea]. Available: https://www.cvedetails.com/cve/CVE-2017-1082/. [Último acceso: 31 Julio 2022].

[40] C. Details, «CVE Details,» [En línea]. Available: https://www.cvedetails.com/cve/CVE-2015-6933/. [Último acceso: 31 Julio 2022].

[41] C. Details, «CVE Details,» [En línea]. Available: https://www.cvedetails.com/cve/CVE-1999-1434/. [Último acceso: 31 Julio 2022].

[42] C. Details, «CVE Details,» [En línea]. Available: https://www.cvedetails.com/cve/CVE-2011-1495/. [Último acceso: 31 Julio 2022].

[43] C. Details, «CVE DEtails,» [En línea]. Available: https://www.cvedetails.com/cve/CVE-2008-1673/. [Último acceso: 31 Julio 2022].

[44] «CVE DETAILS,» 1 Enero 2022. [En línea]. Available: https://www.cvedetails.com/cve/CVE-2021-43893/. [Último acceso: 7 Enero 2022].

[45] C. Details, «CVE Details,» [En línea]. Available: https://www.cvedetails.com/cve/CVE-2022-30224/. [Último acceso: 31 Julio 2022].

[46] A. Nath, Packet Analisis with Wireshark, Livery: Packt Publishing ltd, 2015.

[47] Sans Institute, «Sans,» 17 abril 2016. [En línea]. Available: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltab7d19ca9100e50e/5e9ddae7674ec260f325c3ca/data_breach_response.pdf. [Último acceso: 1 Agosto 2022].

[48] Institute Sans, «Institute Sans,» Julio 2014. [En línea]. Available: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt3ba0e9955d967921/5e9e07f6c81c45292c0d4fee/dmz_lab_security_policy.pdf. [Último acceso: 1 Agosto 2022].

[49] Institute Sans, «Institute Sans,» Diciembre 2013. [En línea]. Available: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltec1d5c2b1e7d13b3/5e9e04a233f6b8718946a34d/internet_usage_policy.pdf. [Último acceso: 1 Agosto 2022].

[50] Institute Sans, «Institute Sans,» Diciembre 2013. [En línea]. Available: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltbbe3f7ae34a0ef6c/5e9e06fef923401150072159/server_malware_protection_policy.pdf. [Último acceso: 1 Agosto 2022].

[51] C. Details, «CVE Details,» [En línea]. Available: https://www.cvedetails.com/cve/CVE-2021-45429/. [Último acceso: 1 Agosto 2022].

[52] C. Details, «CVE Details,» [En línea]. Available: https://www.cvedetails.com/cve/CVE-2022-22143/. [Último acceso: 1 Agosto 2022].

[53] C. Details, «CVE Details,» [En línea]. Available: https://www.cvedetails.com/cve/CVE-2019-1712/. [Último acceso: 1 Agosto 2022].

[54] C. Details, «CVE Details,» [En línea]. Available: https://www.cvedetails.com/cve/CVE-2019-1372/. [Último acceso: 1 Agosto 2022].

ANEXOS

Anexo 1. Entrevista realizada al Lic. Iván león jefe de recurso humanos de la empresa de productos enlatados.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES TECNOLOGÍAS DE LA INFORMACIÓN
Entrevista realizada al Lic. Iván León jefe de recurso humanos de la empresa de productos enlatados.
Objetivo: Conocer el funcionamiento de la empresa de enlatados y quienes tiene acceso a la red wifi.
1. ¿Cuál es la historia de la empresa?
La empresa fue creada el 25 de noviembre del 2015, en las instalaciones donde se encuentra actualmente antes estaba una empresa que distribuía bebidas alcohólicas, hoy en día la empresa tiene la venta de productos enlatados que distribuye a otros países americanos, como México, Guatemala, Costa Rica, Chile y Estados Unidos. La empresa tiene la misión de colocar sus productos en el mercado internacional y poder ocupar unos de los primeros lugares en la exportación de estos alimentos enlatados.
2. ¿Cuántas personas trabajan en la empresa?
Actualmente disponemos 80 personas que trabajan en las diferentes áreas.
3. ¿Todas las personas que laboran en la empresa son fijas?
No, al personal lo dividimos entre personal fijo y eventuales.
4. ¿Cuántas personas tiene autorización en usar la red WiFi?
Según la normativa que mantiene la empresa de que solo personal autorizado debe tener ingreso de productos electrónicos se estima que son 20 personas que se dividen en personal administrativo y supervisores de planta
5. ¿Ha notado que personas no autorizadas hace uso de la red?
Si, por las cámaras puedo darme cuenta quien está realizando el trabajo y quienes no. Por lo que son sancionados si se lo llega a encontrar, pero no tenemos un número exacto de quienes ingresan accesorios electrónicos.

Anexo 2. Entrevista Realizada a Ing. Miguel Delgado jefe del área de TI de la empresa de productos enlatados

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES TECNOLOGÍAS DE LA INFORMACIÓN
Entrevista realizada a Ing. Miguel Delgado jefe del área de TI de la empresa de productos enlatados.
Objetivo: Conocer las vulnerabilidades que presenta la infraestructura de TI.
1. ¿Cuántos equipos maneja la empresa?
Son 20 equipos que actualmente tiene la empresa, que se dividen en servidores, máquinas de escrito del personal como laptops, también están incluidos los equipos de wifi.
2. ¿Cuál es método de acceso a la red wifi?
Son se tiene por método de autentificación de contraseña que tiene como wap2 personal.

3. ¿Cuántas veces al año hace cambio de la contraseña wifi?
Por lo general cada 6 meses, pero se puede prolongar o disminuir dependiendo de la necesidad.
4. ¿Qué controles de seguridad tiene los equipos de la empresa?
Los controles de seguridad que tiene los equipos son los de clave de acceso y si los equipos están siendo compartidos por otra persona, tiene divididos por usuarios.
5. ¿Tiene restricción de navegación para los empleados?
No existe un mecanismo de control en la navegación, por lo que no se tiene una información acertada de que sitios navegan el personal. Esto no se controla por motivo que los jefes suelen traer diversos equipos a la empresa, esto provocaría molestias tanto para ellos y también para las visitas que puedan tener.
6. **¿Ha detectado que los equipos de la empresa están infectados por un malware?**
No todo el tiempo se logra detectar una maquina infectada, pero las veces que se ha detectado son por programas que los empleados instalan.
7. ¿Ha detectado intentos de ataques a sus sistemas?
Pues al sistema como tal, no se ha detectado un ataque que provoque la caída de los servicios, lo que se ha detectado es ataques al personal administrativo o a los jefes por el método de Phishing, pero se ha detectado a tiempo y logrado minimizar el riesgo.
8. ¿Qué tiempo se demora en detectar un equipo infectado?
Pues el tiempo no lo he tomado en cuenta, quizás semanas, porque cuando se infecta un equipo, tardo demasiado en darme cuenta.
9. ¿Tiene un plan de contingencia ante un ataque en la red de la empresa?
No, no tengo una medida de seguridad que me permita realizar una contingencia ante un ataque en la red.

Anexo 3. Entrevista realizada a Lic. María Balón asistente del área de contabilidad de la empresa de productos enlatados.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA **FACULTAD DE SISTEMAS Y TELECOMUNICACIONES** **TECNOLOGÍAS DE LA INFORMACIÓN**
Entrevista realizada a Lic. María Balón asistente del área de contabilidad de la empresa de productos enlatados
Objetivo: Conocer la deficiencia de los servicios que utiliza el personal administrativo.
1. ¿Qué tipos de servicios por lo general utiliza en un día laboral?
Por lo general utilizo los servicios contables que tiene la empresa, además de los programas de office que me ayuda a tener un control contable de la empresa, además de hacer las respetivas declaraciones del SRI, como también los pagos del personal por las bancas Web.
2. ¿Ha presentado algún inconveniente con los servicios que suele usar?
Por lo general siempre hay problemas con los servicios que utilizo, especialmente con el servicio contable, pero es rara vez, que apenas se detecta se da aviso al encargado del sistema.
3. ¿Cuánto tiempo dedica en la navegación de otros sitios ajenos al trabajo?
No siempre navego en sitios ajenos a la empresa, por lo general es en la hora de almuerzo que hago uso del internet o cuando en el trabajo lo necesite.
4. ¿Le presenta molestia cuando se cambia la contraseña de wifi?
Pues si es una molestia que cambie la contraseña, y tengamos que estar pidiendo acceso para poder trabajar.

5. ¿Qué opina sobre la seguridad Informática?
Es importante, ya que es el único medio de mantener los datos de manera segura y además de que impide un posible ataque a los servicios.
6. ¿Confía en la seguridad de los servicios informáticos que tiene la empresa?
Si, no conozco como está elaborado la seguridad de los sistemas, pero sé que están protegiendo los datos críticos de la empresa.

Anexo 4. Entrevista realizada a Lic. Katherine Pita asistente de compras de la empresa de productos enlatados.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA **FACULTAD DE SISTEMAS Y TELECOMUNICACIONES** **TECNOLOGÍAS DE LA INFORMACIÓN**
Entrevista realizada a Lic. Katherine Pita asistente de compras de la empresa de productos enlatados
Objetivo: Conocer la deficiencia de los servicios que utiliza el personal administrativo.
1. ¿Qué tipos de servicios por lo general utiliza en un día laboral?
La mayor parte de tiempo utilizo un servicio que está dedicada a la compra de productos, además de revisar las finanzas para la compra y facturar servicios o comprar que se realiza para la empresa.
2. ¿Ha presentado algún inconveniente con los servicios que suele usar?
No tengo problema con los servicios que la empresa me brinda, salvo cuando sea un problema general que de inmediato aviso al personal de sistemas.
3. ¿Cuánto tiempo dedica en la navegación de otros sitios ajenos al trabajo?
Por lo que implica en mi área constantemente tengo que estar revisando sitios ajenos a la empresa para adquirir productos, además de estar conectándome vía remota a otra sucursal, pero de ahí en mi tiempo de comida revisa otros sitios.
4. ¿Le presenta molestia cuando se cambia la contraseña de wifi?
Si me da un poco de incomodidad cada vez que cambian la contraseña, ya que tengo que molestar al personal de sistema para que me facilite la conexión.
5. ¿Qué opina sobre la seguridad Informática?
Si, yo creo que es la parte esencial de cualquier empresa, porque de ella dependemos de que tan protegida es la información que utilizamos todos los días en nuestro ámbito laboral.
6. ¿Confía en la seguridad de los servicios informáticos que tiene la empresa?
Si, no sé qué normas o sistema tienen implementado para la protección del sistema, pero sé que está en correcto funcionamiento y sé que implementaran mejoras en algún momento si en caso necesite hacerlo.

La libertad, 06 de Octubre del 2022

CERTIFICADO ANTIPLAGIO

001-TUTOR MACS-2022

En calidad de tutor del trabajo de titulación denominado "**Desarrollar un algoritmo para el control de peticiones Web mediante código Python para la detección de trafico de red anómalo para una empresa de productos de enlatados",** elaborado por el estudiante José Gomez Ruidiaz, egresado de la carrera de Tecnología de la Información, de la Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, previo a la obtención del título de Ingeniero en TICs., me permito declarar que una vez analizado en el sistema anti plagió Urkund, y luego de haber cumplido los requerimientos exigidos de valoración ,el presente proyecto ejecutado, se encuentra con el 9% de valoración permitida, por consiguiente se procede a emitir el presente informe.

Adjunto reporte de similitud,

Ouriginal

Document Information

Analyzed document	Jose_Gomez_Ruidiaz_Titulacion2022.docx (D142681233)
Submitted	8/5/2022 3:11:00 PM
Submitted by	DANIEL IVAN QUIRUMBAY YAGUAL
Submitter email	dquirumbay@upse.edu.ec
Similarity	9%
Analysis address	dquirumbay.upse@analysis.urkund.com

Atentamente,

Daniel Quirumbay Yagual.
C.I 0919659672
DOCENTE TUTOR