UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

IMPLEMENTACIÓN DE TECNOLOGÍA SANDBOX PARA PROTEGER DE ATAQUES RANSOMWARE EN UNA RED INFORMÁTICA LOCAL DE UNA ENTIDAD FINANCIERA

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autor (es):

Bach. Perez Diaz Neiler Wilter

ORCID: https://orcid.org/0000-0002-5131-6094

Bach. Chinchay Maldonado Jorge Obed

ORCID: https://orcid.org/0000-0001-5586-9799

Asesor:

Dr. Ramos Moscol Mario Fernando.

ORCID: https://orcid.org/0000-0003-3812-7384

Línea de Investigación:

Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú 2021

APROBACIÓN DEL JURADO

IMPLEMENTACIÓN DE TECNOLOGÍA SANDBOX PARA PROTEGER DE ATAQUES RANSOMWARE EN UNA RED INFORMÁTICA LOCAL DE UNA ENTIDAD FINANCIERA.

Bach. Chinchay Maldonado Jorge Obed
Autor

Bach. Pérez Díaz Neiler Wilter
Autor

Dr. Ramos Moscol Mario Fernando.
Asesor

Mg. Bravo Ruiz Jaime Arturo
Presidente de Jurado

Mg. Bances Saavedra David Enrique
Secretario de Jurado

Dr. Tuesta monteza victor alexci
Vocal de Jurado

Dedicatorias

Con mucho cariño dedico el presente trabajo de investigación a Dios, a mis padres, esposa e hijos, quienes son mi razón de superación.

Neiler Wilter Pérez Díaz.

El presente trabajo de investigación está dedicado a:

Mi Dios, por darme fortaleza para seguir adelante en medio de la dificultad, siempre está a mi lado, a él sea la gloria y la honra, también a mi madre aya en el cielo, que me enseñó la perseverancia de seguir adelante, a mi padre por su apoyo incondicional, a mi esposa y mi hijo que son el motor para seguir adelante.

Jorge Obed Chinchay Maldonado.

Agradecimientos

Agradezco a Dios porque es mi guía día a día, a mis padres Lindaura y Eulogio, por educarme y enseñarme a caminar en valores, a mi esposa Yaquelin por demostrarme su amor, paciencia y constante apoyo, a mis hijos Sophía y Antony quienes me motivan a no rendirme y ser un ejemplo para ellos, a mi profesor de tesis el Ing. Heber Mejía y el asesor Dr. Mario Ramos, por su paciencia y brindar sus conocimientos científicos para el desarrollo de esta investigación.

Neiler Wilter Pérez Díaz.

Agradezco primero a Dios, por darnos la vida y la fortaleza en aquellos momentos de dificultad y de debilidad, agradecer también a mi familia: mi esposa Diana y mi hijo Jorge Adrián por ser el motor de mis sueños y confiar siempre en mí, a mi profesor de tesis el Mg. Heber Mejía y al asesor Dr. Mario Ramos, por sus conocimientos científicos y comprensión en el desarrollo de esta investigación.

Jorge Obed Chinchay Maldonado.

Resumen

América Latina sufrió más de 41 billones de intentos de ciberataques en el año 2020, de ellos, Perú sufrió 2,6 billones, esto se debe a que la pandemia del COVID-19 aperturó el trabajo remoto, generando condiciones para que los ciberdelincuentes se aprovechen de las vulnerabilidades de las redes empresariales y de usuarios comunes a través de sus conexiones a internet, en este aspecto tanto las entidades estatales como privadas quedaron expuestas, porque no contaban con una protección perimetral robusta en sus redes informáticas, en ese sentido los Ransomware que más vulneraron son: Maze, Doppelpaymer, Netwalker, Conti y Revil/Sodinokibi, aumentando sus ganancias en un máximo del 300% con relación al año 2019 en Latinoamérica. Las empresas de ciberseguridad como: Cisco, Eset, Kaspersky y otros, han implementado soluciones tecnológicas para mitigar estas amenazas, los cuales se adquieren mediante licencias de uso limitado sujetas a previo pago para su actualización, generando un costo adicional a las entidades, de lo contrario quedarían expuestas a todo tipo de ataques cibernéticos. Es por ello que en esta investigación se propuso la implementación de Cuckoo Sandbox que es de código abierto para el análisis de Ransomware, el cual se implementó en Ubuntu 20.04 LTS sobre un servidor torre Core i5 con 16 gb de RAM, se configuró el archivo cuckoo.conf donde se asignó el IP de servidor, VirtualBox.conf para la asignación del IP y nombre del cliente, reporting.conf para los reportes en HTML, posteriormente se instaló el laboratorio de pruebas virtualizado con 5 equipos Windows 10 y se configuró como escenario similar a la red informática local de la Coopac Norandino Ltda., para la ejecución de las pruebas se inyectó un Ransomware por cada máquina virtual y los resultados arrojaron que de los 5 Ransomware inyectados el 100% fueron detectados y aislados satisfactoriamente, utilizando en promedio 0.89 Gb de memoria RAM y con un tiempo promedio de 123.6 segundos, lo que demuestra que Cuckoo Sandbox es efectivo, contribuyendo en la seguridad perimetral de la red informática.

Palabras Clave:

Cuckoo Sandbox, Ransomware, Ciberataques, Tráfico malicioso, Kali Linux, seguridad perimetral, vulnerabilidades.

Abstract

Latin America suffered more than 41 billion attempted cyber-attacks in 2020, 2.6 billion of which Peru suffered, This is because the COVID-19 pandemic opened up remote work, creating conditions for cybercriminals to exploit vulnerabilities in corporate networks and common users through their Internet connections, both state and private entities were exposed in this regard, because they did not have robust perimeter protection on their computer networks, In this sense, the Ransomware that have been the most vulnerable are: Maze, Doppelpaymer, Netwalker, Conti and Revil/Sodinokibi, increasing its earnings by a maximum of 300% over 2019 in Latin America. Cybersecurity companies such as Cisco, Eset, Kaspersky and others have implemented technological solutions to mitigate these threats, which are acquired by means of limited-use licenses subject to prior payment for their update, generating an additional cost to the entities, otherwise they would be exposed to all kinds of cyber-attacks. That is why in this research we proposed the implementation of Cuckoo Sandbox which is open source for Ransomware analysis, which was deployed on Ubuntu 20.04 LTS on a Core i5 tower server with 16 gb of RAM, the cuckoo.conf file was configured where the server IP was assigned, VirtualBox.conf for IP and client name assignment, reporting.conf for HTML reports, Subsequently, the virtualized test lab was installed with 5 Windows 10 computers and was configured as a similar scenario to the local computer network of Coopac Norandino Ltda, for the execution of the tests, one Ransomware was injected per virtual machine and the results showed that 100% of the 5 Ransomware injected were detected and successfully isolated, using on average 0.89 Gb of RAM and with an average time of 123.6 seconds, which proves that Cuckoo Sandbox is effective, contributing to the perimeter security of the computer network.

Keywords:

Cuckoo Sandbox, Ransomware, Cyber-attacks, Malicious traffic, Kali Linux, perimeter security, vulnerabilities.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

I. INTRODUCCIÓN

1.1. Realidad Problemática.

La ciberseguridad es un aspecto crítico en todo el mundo, a nivel global las empresas tienen un arduo trabajo que tratar frente a los ataques cibernéticos. (Fernandez, 2020); la digitalización y la globalización ha cambiado el mundo, hoy en día es más fácil poder realizar tareas; la tecnología revoluciona constantemente, como consecuencia a ello las empresas tienen que estar a la vanguardia de las innovaciones, y desde la perspectiva de la ciberseguridad protegerse de las amenazas y ataques cibernéticos a las cuales están propensos, para no sufrir pérdidas de información e incluso pérdidas económicas.

En la figura 1, se muestran los riesgos más relevantes presentes en las empresas.

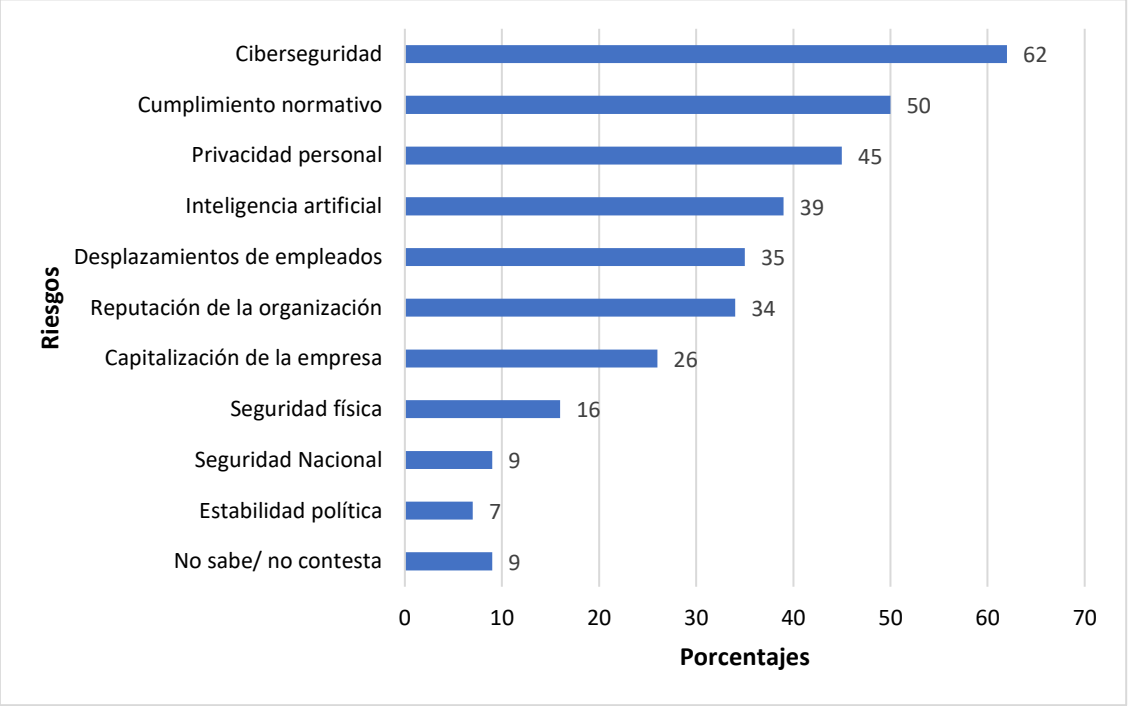


Figura 1: Riesgos que las organizaciones consideran más relevantes y están trabajando para mitigar. Fuente*. (Fernandez, 2020).*

Las pérdidas económicas en el año 2018 a nivel mundial ascienden a 119.01 millones de dólares distribuidos entre los siguientes países: Canadá (9.25), EE. UU (22.37), Reino Unido (11.46), Francia (9.72), España (8.16), Brasil (7.24), Alemania

(13.12), Italia (8.01), Singapur (9.32), japón (13.57) y Australia (6.79). (Fernandez, 2020).

En la figura 2, se muestra la evaluación de las consecuencias ocasionadas por los ciberataques a nivel mundial, donde se tiene que los daños que más afectaron a las empresas son: la pérdida de información, el cierre de negocios, equipos dañados y beneficios perdidos. (Accenture, 2018).

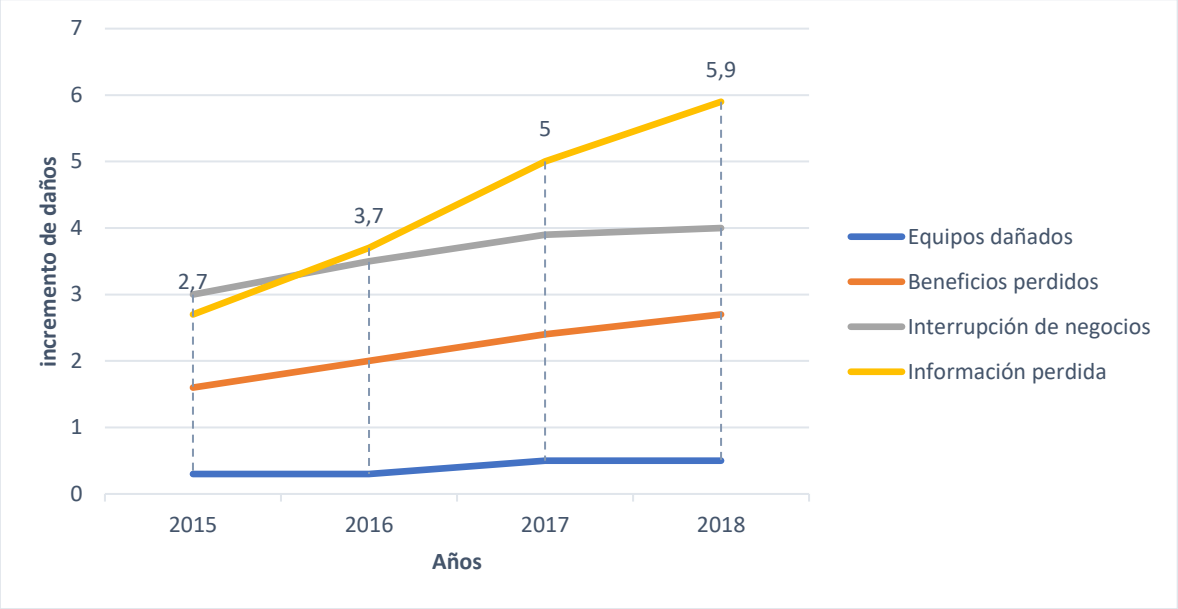


Figura 2 Evaluación de las consecuencias que dejan los ciberdelincuentes en las empresas a nivel mundial, en los años 2015 al 2018. Fuente: *(Fernandez, 2020)*.

La pandemia del COVID 19, revolucionó la tecnología, las diversas empresas por disposición de los gobiernos en los países, abrieron el llamado trabajo remoto, el cual fue un acceso para que los ciber atacantes aprovechen las vulnerabilidades de las conexiones remotas empresariales, donde se detectó numerosos ataques maliciosos de diversas índoles como troyanos, ejecución remota de código contra ThinkPHP y PHPUnit, marco web, botnet Mirai, (FORTINET, 2020); Botnet Mirai es un malware dirigido a dispositivos internet de las cosas (IoT), que se ha vuelto más potente y es el más usado por los ciber atacantes. (FORTINET, 2020).

América Latina sufrió más de 41 billones de intentos de ciberataques en el año 2020, siendo en el Perú más de 2,6 billones de intentos de ciberataques durante el 2020. (FORTINET, 2020), Considerando el cuarto trimestre del año 2020, según

informe de Fortinet, fueron 801 millones de atentados de código malicioso en el Perú, los ataques más conocidos fueron los phishing que se infiltraron por los correos electrónicos y se extendieron por América Latina mediante adjuntos con archivos HTML, dirigiendo a web maliciosos por el navegador, convirtiéndose este tipo de ataques en el acceso idóneo para el Ransomware. (FORTINET, 2020)

En los últimos años, los ataques Ransomware han tenido un protagonismo mayor con relación a los años anteriores. En el año 2020 tuvo un máximo del 300%, equivalente a un promedio de 350 millones de dólares, con relación al año 2019, que no superó los 100 millones de dólares; este incremento se vio reflejado en las pérdidas financieras de las entidades, dinero que recibieron los ciberdelincuentes, por el pago de rescate que realizaron sus víctimas. (ESET, 2021), las familias Ransomware que generaron estas pérdidas económicas son Ryuk, Maze, Doppelpaymer, Netwalker, Conti y REvil/Sodinokibi, de las cuales las que tuvieron mayor actividad durante el año 2020 a nivel mundial fueron Ryuk, Maze y REvil/Sodinokibi. (ESET, 2021)

La ciberdelincuencia se ha convertido en un negocio cada vez más lucrativo y devastador, las inversiones en gastos por seguridad para las empresas alcanzó un promedio de 124.000 millones de dólares en el año 2019, un 8% más respecto al año 2017 y en relación con el año 2018 que los delitos informáticos llegaron al pico de hasta los 110.613 casos detectados, un promedio de 5.000 personas, fueron detenidas en España, y puestos a derecho ante la justicia por delitos relacionados con ciberdelincuencia. (Fernandez, 2020)

La Reserva Federal americana (Fed), dió a conocer detalles de su estudio, donde muestra que la ciberdelincuencia enfoca principalmente sus ataques al sector de la banca, pero también da a conocer que es este sector el que más invierte en ciberseguridad, (Fernandez, 2020); el pago por rescate de Ransomware tuvo un aumento del 60% en el primer trimestre del año 2020 en comparación al año 2019, llegando hasta US$ 178.254. (Accenture, 2020).

Como métodos utilizados en las soluciones de ingeniería para contrarrestar la pérdida de información, se tiene:

- ✓ Firewall: Es un método de seguridad que funciona como un cortafuegos, encargado de controlar los accesos de los dispositivos a la red. (OWASP, 2015).
- ✓ Servidor Proxy / Filtro Web: Gestiona el tráfico de datos frente a peticiones de clientes hacia un servidor, restringiendo determinados tipos de tráfico, bloqueando así amenazas delictivas. (OWASP, 2015).
- ✓ Filtro de SPAM: Distingue correos maliciosos y no maliciosos, bloqueando así el filtro de código malicioso en una PC. (OWASP, 2015).
- ✓ Segmentación de la red: Dividir la red en subredes, para otorgarles controles y servicios de seguridad. (OWASP, 2015).
- ✓ Aislamiento de Aplicaciones (Sandboxing): Permite aislar una red para restringir el acceso a los recursos, minimizando de esta forma el tráfico de código malicioso en la red. (OWASP, 2015).

Estas vulnerabilidades tienen su enfoque de mitigación a través de las soluciones de ingeniería que desarrollan las diferentes empresas de ciberseguridad.

CISCO SYSTEM ha implementado tecnología para hacer frente al ciberataque, denominándolo Advanced Malware Protection, que se encarga de proteger a los dispositivos, mitigando amenazas desconocidas. Cisco Umbrella, es dedicado a la protección en la nube, bloqueando las conexiones IP, URL y dominios maliciosos. (CISCO, 2019).

La firma rusa Kaspersky junto a National High Tech Crime Unit de la policía de Países Bajos, el European Cybercrime Centre de Europol y McAfee (Europol, Politie, Kaspersky, & McAfee, 2016) desarrollaron un proyecto mancomunado de descifradores Ransomware, para su uso de forma gratuita a quienes hayan sido afectados por este ataque, Kaspersky a este descifrador lo denomina No Ransom (Kaspersky, noransom, 2021) y por su lado la firma norteamericana McAfee lo denomina No More Ransom. (Europol, Politie, Kaspersky, & McAfee, 2016).

ESET es una compañía de seguridad informática, de buen prestigio y siempre está a la vanguardia de la tecnología, su principal activo comercial es el software antivirus, en la cuál siempre está innovando y sacando al mercado nuevos productos para mitigar los ciberataques, según su reporte al año 2021, los productos para la mejora de la seguridad informática que presenta son:

- ✓ ESET ENDPOINT SECURITY: Para proteger la red contra ataques Ransomware.
- ✓ ESET Dynamic Threat Defense: Proporciona una capa de seguridad para los productos de ESET, como Mail Security y Endpoint, brindando detección basada en el comportamiento, aprendizaje automático, detección de amenazas día cero y prevención de Ransomware. (ESET, 2021).
- ✓ ESET File Security: Proporciona protección avanzada para servidores generales, almacenamiento de archivos de red, incluido OneDrive, garantizando protección contra Ransomware, amenazas día cero, violaciones de datos y protección de botnets. (ESET, 2021).
- ✓ ESET Mail Security: Proporciona una capa de seguridad a las organizaciones que desean evitar que las amenazas lleguen a sus usuarios, a través de: anti-spam, Anti-phishing, Anti-malware, Optional Cloud Sandbox análisis, Comprehensive mail server protection, Protection of the host server. (ESET, 2021).
- ✓ ESET Full Disk Encryption: Aumenta la seguridad de la información en una organización, mediante el cifrado de discos del sistema, particiones o unidades completas. (ESET, 2021).
- ✓ ESET Cloud Office Security: Protección para aplicaciones de Microsoft 365 contra spam, ataques de phishing y malware. (ESET, 2021)

Trend Micro Deep Security; Proporciona recursos de protección para entornos virtuales y en la nube, así como para entornos físicos tradicionales y mixtos. (Reis, 2013), debido a la complejidad y sofisticación del Ransomware, para mitigar a esta amenaza Trend Micro se enfocó en el desarrollo de protección en capas, obteniendo los productos de protección para web, correo, redes, endpoints y protección de servidores. (Micro Trend, 2016).

Existen soluciones en ingeniería para mitigar los posibles ataques de malware, pero que no son suficientes para acaparar los problemas vistos en este trabajo de investigación, porque los desarrolladores de malware innovan en técnicas de ataques, dando consecuencia las manifestaciones del problema en la ingeniería las cuales se describen a continuación.

La existencia de software antivirus, como soluciones para proteger de ataques maliciosos, no son 100% seguros, porque los software maliciosos están en constante cambio en su comportamiento y técnicas de ataque, llegando a sofisticarse y ser más potentes. (Mera, Casanova, Vergara, & Bayas, 2021)

Las actualizaciones de firmas existentes como módulo en los antivirus, necesariamente deben contener internet para acceder a actualizar el producto, para ello se requiere que el producto antivirus sea una versión de paga, lo cual genera un costo adicional que se tiene que renovar cada determinado periodo, la limitación de estas actualizaciones es para caso de los ataques “zero day”, que son nuevos ataques y pueden pasar por desapercibidos por la seguridad que ofrecen los software antivirus. (ESET, 2020)

Implementar infraestructuras de seguridad, técnicas de protección y mitigación para proteger la información, es posible gracias al desarrollo de tecnologías como la Tecnología Sandbox, que ayuda a mejorar la seguridad de las empresas empleando técnicas de protección (Sanz, 2019), y la tecnología Palo Alto Networks Wildfire que abarca el servicio basado en la nube para análisis de amenazas en ciberseguridad. (Castro, 2016)

La tecnología Sandbox, es una tecnología openSource para Linux, y las empresas del Perú lo implementarán como un ambiente de análisis centralizado en un servidor, podrían mejorar la seguridad en sus redes informáticas, mitigando los ataques cibernéticos, como consecuencia se tendría la reducción de costos de rescate por encriptación de datos.

1.2. Trabajos previos.

Buchyk, Yudin, Ziubina, Bondarenko, & Suprun; (2021), realizó la investigación, Devising a method of protection against zero-day attacks based on an analytical model of changing the state of the network Sandbox. En Ucrania se incrementó 10 veces el número de ciberataques. Ahora todos comentan acerca de "ataque dirigido", "vulnerabilidad de día cero", "día 0" o amenazas persistentes avanzadas (ATP). Estos temas son la tendencia principal en el campo de la seguridad de la información. Por tal motivo, el propósito de este estudio es crear un método para proteger el sistema de información de ataques de "día cero", que empleó la clasificación probabilística de estados de un sistema dado en condiciones de incertidumbre. Los resultados que se obtuvieron al probar el tráfico de correo, los medios de protección tradicionales solamente detectaron 1 código malicioso de cada 15 malware inyectados, enviando los 14 malware restantes para su análisis en Sandbox, los cuales fueron detectados al 100%. Posteriormente, se utilizaron 55 archivos maliciosos diferentes para el tráfico web, 23 de los 55 archivos fueron bloqueados por las características de seguridad existentes (puerta de enlace de acceso seguro a Internet), enviando los 32 archivos maliciosos restantes a Sandbox para su prueba, siendo detectados al 100%. La aplicación de métodos de protección Sandbox permite evaluar objetivamente las actividades en una red informática y permite detectar tráfico malicioso al 100% en la red informática.

Yu, Liu, Tan, Zhao, & Zhang, (2020), realizó la investigación denominada Scheduling and Deploying Distributed Sandboxes for Cyber-Attack Detection. desarrollado en China. La amenaza persistente avanzada (APT) orquestada por los ciberdelincuentes para vulnerar los sistemas informáticos. La implementación dinámica de un clúster de Sandboxes distribuidos de acuerdo con un enfoque de optimización y un análisis de asociación de ataque basado en DAG. Los resultados que se obtuvieron experimentando con 10 Sandboxes equipados con diferentes capacidades, enfrentaron 6 posibles tipos de amenazas/ataques que aparecen con las probabilidades correspondientes. Cuantos más tipos de amenazas pueda detectar una caja de arena, mayor flexibilidad tendrá. Este experimento establece tres niveles de flexibilidad: alto para indicar que es capaz de detectar todos los ataques con diferentes probabilidades. Medio: para indicar que puede detectar de

2 a 3 tipos de ataques. Bajo para indicar que puede detectar solamente un tipo de ataque. El desempeño de DAG se ve afectado por dos factores: la tasa de transacción y la política de selección de verificación. La alta tasa de transacciones indica que un grupo de Sandbox distribuidos genera más transacciones con una unidad de tiempo y más capacidades de revisión para cumplir con las tareas. Los Sandbox distribuidos implementados detectaron tráfico sospechoso en la red informática de manera colaborativa y muestra un informe de resultados como transacciones en un gráfico acíclico dirigido (DAG) a expensas de verificar las transacciones existentes en DAG en términos de firmas y amenazas/ataques relevantes.

Huthifh, Mohammad, & Sharhabeel, (2020). Realizó la investigación denominada On Detection and Prevention of Zero-Day Attack Using Cuckoo Sandbox in Software-Defined Networks. En Jordania. Las redes informáticas, aún están expuestas a ataques desconocidos, denominados día cero, Este término se refiere al tiempo disponible que tienen los proveedores de ciberseguridad para corregir la vulnerabilidad que ha sido expuesta, para que el atacante no obtenga un acceso ilegal. Por lo que propone desarrollar un nuevo mecanismo de prevención y detección de ataques de día cero para SDN mediante la modificación de la herramienta Cuckoo Sandbox, El mecanismo se implementa y se prueba en el sistema UNIX. Los resultados obtenidos muestran que Cuckoo Sandbox ha identificado con éxito 353 malwares de 361. Por lo tanto, el porcentaje de éxito es del 97,78%. El tiempo de análisis es de aproximadamente 132 s y 152 s, cuando el tamaño del malware es de 2 KB y 1400 KB respectivamente. Cuando el tamaño del malware aumenta drásticamente de 2 KB a 1400 KB, el tiempo de análisis aumenta solamente un 15,1%. Claramente, esto demuestra la efectividad de nuestra técnica propuesta. Los resultados obtenidos muestran que el mecanismo implementado detiene exitosamente los malwares de día cero aislando a los clientes infectados, Además, muestran la efectividad de nuestro mecanismo en términos de precisión de detección y tiempo de respuesta.

Kamal, y otros; (2020). Realizó la investigación denominada A User-friendly Model for Ransomware Analysis Using Sandboxing. realizado en Arabia. El Ransomware

es un tipo de software malicioso que cifra los archivos de un cliente, con el objetivo de pedir rescate por la recuperación de dichos archivos. Las pérdidas para personas y empresas que han sido blanco de los ciberdelincuentes Ransomware superan los mil millones de dólares en el mundo. La finalidad de esta investigación es desarrollar un modelo fácil de usar para comprender la taxonomía y el análisis de los ataques de Ransomware implementado con tecnología Sandbox de Cuckoo para la identificación del Ransomware. Los resultados obtenidos demostraron una eficiencia del 92% en el método desarrollado para el análisis de Ransomware. En conclusión, la tecnología Sandbox Cuckoo como entorno aislado es eficiente para mitigar vulnerabilidades, para este caso se obtuvieron que el 92% de Ransomware que fueron filtrados en la red, han sido bloqueados.

GyungMin, ShinWoo, ByoungMo, TaeKyu, & Kyounggon, (2020). Realizó la investigación denominada Fileless cyberattacks: Analysis and classification. Desarrollado en Arabia. Los ciberdelincuentes están desarrollando malware sin archivos para eludir las técnicas de detección existentes. Por lo que propone una metodología de clasificación basada en las técnicas y características de ataque utilizadas. Se Recolectó una serie de muestras de ciberataques, pasando a ser analizados por Cuckoo Sandbox el cual brindará un informe reportando una clasificación de los archivos analizados. Este estudio analizó 10 ciberataques sin archivos que han surgido recientemente. El análisis de estos ciberataques reveló las características y técnicas específicas utilizadas. A través de este proceso, los ciberataques sin archivos se clasificaron en las siguientes categorías: Evasión, Ataque o Recolección. A través de esta investigación, se proporciona un marco fundamental para identificar y clasificar las características de los ciberataques sin archivos que probablemente surjan en el futuro. A medida que los ciberataques continúan avanzando y se vuelven más complejos, las técnicas utilizadas para detectar y prevenir tales ataques también se están desarrollando de manera constante. Además, los ciberataques sin archivos continúan eludiendo las técnicas de detección de malware.

Humayun, Jhanjhi, Alsayat, & Ponnusamy, (2021) realizó la investigación, Internet of things and Ransomware: Evolución, mitigación and prevention, en la Facultad de

Computación e Información de la Universidad de El Cairo. Evolución, prevención y mitigación de Ransomware en el contexto de IoT. Presenta su metodología de encuesta donde detalla la Evolución, prevención y mitigación de Ransomware en el contexto de IoT. Los resultados de esta investigación concluyen que para proteger completamente los dispositivos de IoT de un ataque de Ransomware, la capacidad de mitigación debe incorporarse en los dispositivos de IoT durante todo el ciclo de vida de la ejecución de la aplicación. La literatura muestra una curva más alta hacia los ataques de Ransomware, que se espera que sea 5 veces mayor para 2020 y supere los 6 billones de dólares como rescate contra ataques de Ransomware.

Shammugam, y otros, (2021). Realizó la investigación, Information security threats encountered by Malaysian public sector data centers, en los centros de datos del sector público de Malasia. Los centros de datos son principalmente los principales objetivos de los ciberdelincuentes y las amenazas a la seguridad, ya que albergan diversos servicios críticos de tecnología de la información y la comunicación. Este estudio empleó el método de entrevista estructurada para la recopilación de datos, las preguntas de la entrevista se prepararon con base a una lista de 86 posibles amenazas a la seguridad de la información que se identificaron mediante una revisión sistemática de la literatura, que cubre varios aspectos de las operaciones de TIC, que pueden causar interrupciones y daños a las operaciones comerciales de una organización. Los resultados revelaron que las amenazas técnicas, spyware, phishing, amenazas bluesnarfing, ingeniería social y virus, troyanos, malware, Ransomware, las amenazas de sitios web virales son las principales categorías de amenazas que a menudo encuentran las organizaciones del sector público de Malasia. Las principales causas de estas amenazas son la falta de recursos en términos de presupuesto y personal competente, falta de conciencia y educación de los usuarios, políticas y procedimientos de seguridad.

Maurer, Kim, Dan, & Kappelman, (2021). Realizó la investigación, Cybersecurity: Is It Worse than We Think, en organizaciones de renombre de EE. UU. El análisis de la ciberseguridad en varias organizaciones y empresas para determinar su estado, por esta razón. Presentó en una investigación que intentó determinar si las

empresas contrataron oficiales de información, compraron seguros cibernéticos y el grado de consideración que se le dio a la ciberseguridad durante el desarrollo de software, la gestión de cambios y estrategia. Las organizaciones que dan prioridad a la ciberseguridad tienen puntuaciones de preparación más altas por encima del resto. Esto sugiere que las organizaciones que desvían su atención de la ciberseguridad prácticamente no ven mejoras, mientras que aquellas que toman una decisión consciente están listas para comenzar a tener mejoras. Dado nuestro análisis, creemos que hay una dura realidad que acecha bajo la superficie dentro de muchas organizaciones. Si bien pueden estar diciendo las cosas correctas en público para satisfacer a los inversores, aseguradores y clientes, existe una aparente falta de urgencia en promover una organización verdaderamente resistente y segura.

Wojciech & Luca, (2021). Realizó la investigación, Cyber reconnaissance techniques, en la Agencia Nacional de Intercambio Académico Polaco. Los ciberataques exitosos, que están creciendo en términos de complejidad y volumen, ocasionando daños económicos relevantes. Por esta razón, se presenta la clasificación y la evolución de los métodos de reconocimiento más populares para luego discutir posibles contramedidas y presentar algunas direcciones futuras. Por lo tanto, se espera que la superficie de ataque potencial explotable para las técnicas de reconocimiento continúe creciendo, al menos en un futuro próximo. Como tendencia general, la evolución de los dispositivos inteligentes, las redes sociales y las aplicaciones con capacidad de IoT impulsó la cantidad de información que puede recopilar un atacante y también multiplicó las rutas de comunicación que se pueden utilizar para llegar a la víctima.

Ahmad, (2019). Realizó la investigación, Theo V-Network: A Testbed For Malware Analysis, en la Universidad Estatal de Kaduna Nigeria. El software malicioso (malware) es un riesgo significativo para la seguridad de los sistemas informáticos, en particular el malware de auto propagación (denominado gusano) debido a su naturaleza altamente virulenta. Por esta razón, presentó una metodología de experimentación en un entorno de red virtualizado denominado V-Network, con el objetivo de estudiar los patrones de infección y propagación de gusanos de red. La

propagación del pseudo-gusano Slammer infectó al 95% (1004) de los hosts en 90 segundos. El modelo virtualizado V-Network respondió al escenario implantado de brote de gusano previamente conocido y gusano contemporáneo; los resultados muestran que el banco de pruebas de V-Network es una plataforma estable y conveniente para el análisis de malware de auto propagación.

Morato, Berrueta, Magaña, Izal (2018). Realizaron una investigación sobre, Ransomware early detection by the analysis of file sharing traffic. En un escenario de volumen compartido, donde el cifrado de toda la red de datos, es objeto de infección desde un solo host. Por lo que se planteó el framework REDFISH, como método para la detección y bloqueo de ransomware. Según el experimento desarrollado con más de 50 muestras de 19 familias ransomware, la detección fue al 100% utilizando tiempos inferiores a 20 s, por tanto el framework REDFISH, demostró ser efectivo para la mitigación de ataques ransomware en una red de datos compartida.

Ketzaki, Petros, Giannoutakis, Drosou, Tzovaras (2020). Desarrollaron una investigación sobre A Behaviour based Ransomware Detection using Neural Network Models, en Grecia. El ransomware es un malware de encriptación de datos que ataca sobre todo a las instituciones financieras con el fin de obtener un pago por el rescate de estos archivos, que oscilan entre 300 y 700 dólares, para mitigar estos ataques, se propuso una metodología de redes neuronales para detectar el ransomware en función de su comportamiento, esta metodología es aplicable a las PYME. Los resultados obtenidos en las pruebas se basaron en una validación cruzada de 10 veces en la que las métricas como la precisión fueron del 99,83%, el Score fue de 99.61% y el recall fue de 99.97%, logrando resultados que demuestran el éxito de la metodología propuesta.

1.3. Teorías relacionadas al tema.

1.3.1. Malware

El Malware es un software que se apropia de la información, generalmente creado por hackers y desarrollado para múltiples sistemas, con el objetivo de apropiarse de la data o secuestrar la información. (Sierra, Hernández, & Héctor, 2020)

1.3.1.1. Tipos de malware:

a. Gusanos

Es un programa que se propaga automáticamente de computador a computador, creando copias de sí mismo en la memoria, permitiéndole tomar el control para transferir información gracias a que pueden aprovechar las vulnerabilidades del sistema para expandirse a otras computadoras sin necesidad de ser transferidos, puesto que no necesitan un portador, pueden crear túneles en los sistemas, esto permite que usuarios maliciosos tomen el control del equipo de forma remota. (Hernández & Mauricio, 2019)

Son muy peligrosos debido a su habilidad de autorreplicarse de forma exponencial con tal frecuencia que el computador colapse. (Hernández & Mauricio, 2019)

Estos malware para poder tener un mayor resultado aprovechan técnicas de ingeniería social, como los correos maliciosos denominados phishing o los dispositivos de almacenamiento extraíble con software infectados llamados baiting. (Hernández & Mauricio, 2019)

b. Virus:

Es un programa tipo malware que tiene por finalidad modificar o alterar el correcto funcionamiento en un computador y que se copia automáticamente sin el consentimiento ni permiso del usuario, pero que necesita de la intervención humana para poder difundirse, visto que usa como transporte los medios extraíbles, medios de almacenamiento y la web, aunque también existen otro tipo de virus que sólo se caracterizan por ser molestosos al mostrar diferentes mensajes en pantalla. (Jaén, 2018)

c. Adware:

Es un tipo de malware que recaba información personal, registra los sitios web que se visitan e incluso anota todo lo que escribimos, este tipo de

malware lo encontramos en la publicidad o anuncios que aparecen por la navegación en internet; los adware más potentes abren ventanas pop up, y es capaz de simular un navegador para siempre navegar dentro de sus redes. (Jaén, 2018)

d. Troyanos:

El troyano generalmente se disfraza de un programa de computador que le permite al hacker acceder a la data o la información, incluso espiar el comportamiento de actividades a través de la red. (Jaén, 2018), esto porque los troyanos usan el mismo nombre de programas o aplicaciones reales que un computador utiliza.

Este programa o aplicación provoca daños y vulnera la seguridad, estos se difunden engañando al usuario aparentando ser un programa útil y legítimo con la finalidad de obtener la información personal y tener el control remoto de la computadora para fines malintencionados. (Jaén, 2018)

Este tipo de malware tiene la particularidad que no se puede propagar por sí mismo, ello significa que para que se multiplique tiene que ser descargado e instalado en el computador. (Microsoft, Microsoft, 2021)

e. Rootkit:

Es un conjunto de software que permanece oculto en un ordenador, brindando accesos privilegiados a los hackers y encubriendo procesos maliciosos en el sistema; para el caso de los antivirus, Rootkit falsea los datos de los procesos que están en ejecución, confundiendo en el análisis con información incorrecta por ende llevaría a cabo una desinfección del sistema errónea. (Jaén, 2018)

f. Bomba Fork:

También denominada wabbit, es un código malicioso, que está diseñado principalmente para ocupar una gran cantidad de recursos del sistema, creando copias infinitas de él mismo recursivamente, agotando así recursos como la memoria del sistema y la CPU, logrando que el rendimiento del sistema se reduzca, (Rodríguez, 2019). Se trata de un malware muy antiguo y que actualmente es muy fácil de detener. (Rodríguez, 2019)

g. Ransomware

El Ransomware es una categoría de malware que se dirige a los archivos del usuario y / o recursos relacionados, e impide que el computador funcione, secuestra y hace inaccesibles los datos, hasta que el usuario haya pagado un rescate a cambio de esta información. Este malware comúnmente se propaga a través del envío de email infectado con malware Ransomware, este adjunta un archivo infectado que al hacer clic lleva al sitio web del atacante para luego infectar el equipo, esta cifra los archivos del usuario o víctima, impidiendo su acceso a esta información para luego pedir el rescate de dicha información. (Jaén, 2018)

1. Taxonomía de Ransomware

a. Taxonomía general de Ransomware.

Varios factores rigen la categorización del Ransomware, como su gravedad, los medios de extorsión, las víctimas objetivo y los sistemas afectados. (Al-rimy, Maarof, & Zainuddin, 2017)

- ✓ Según el grado de intensidad, el Ransomware es clasificado como farol y Ransomware real.

  - Ransomware farol: Intenta engañar a las víctimas para que paguen por advertencias falsas.
  - Ransomware real: Es una amenaza real, que se divide en un ataque simple y un ataque RSA con diferentes longitudes de clave de cifrado. (Al-rimy, Maarof, & Zainuddin, 2017)

- ✓ Según los medios de extorsión: El Ransomware se categorizó en criptográfico y no criptográfico, es decir, si el cifrado se utiliza o no contra los datos del usuario. (Al-rimy, Maarof, & Zainuddin, 2017)

El Ransomware también se categorizó, en tres tipos, scareware, Ransomware de bloqueo y Ransomware de criptografía. (Al-rimy, Maarof, & Zainuddin, 2017)

Mientras que los scareware son advertencias falsas que engañan a la víctima para que pague por amenazas falsas, el Ransomware de bloqueo y criptografía son amenazas reales que emplean diferentes mecanismos contra los datos y / o recursos de la víctima. (Al-rimy, Maarof, & Zainuddin, 2017)

b. Taxonomía del Ransomware con base en la literatura actual.

Con base en la literatura actual se presenta una taxonomía de Ransomware más genérica que clasifica el Ransomware desde tres perspectivas: basada en la gravedad, basada en la plataforma y basada en el objetivo. (Al-rimy, Maarof, & Zainuddin, 2017)

- ✓ **Clasificación basada en la gravedad.**

  En esta categoría, clasificamos el Ransomware según el grado de gravedad que representa para el sistema infectado. Esta gravedad varía según varios factores, como el tipo de víctima y el objetivo del ataque. Por lo tanto, desde una perspectiva basada en la gravedad, el Ransomware se clasifica en scareware y Ransomware perjudicial.

- ✓ **Clasificación basada en plataforma.**

  Las cepas de Ransomware también se pueden clasificar según la plataforma a la que se dirigen, esas plataformas de ataques pueden

ser dispositivos como televisores inteligentes, IoT, dispositivos portátiles y sistemas basados en la nube.

- ✓ **Clasificación basada en objetivos.**

  El Ransomware también se puede clasificar según los tipos de víctimas; es decir, personas físicas o jurídicas, no sólo los usuarios normales son vulnerables a los ataques de Ransomware, sino también las organizaciones y entidades comerciales, a pesar de las contramedidas proactivas que normalmente practican.

2. Familia de Ransomware.

La proliferación de Ransomware ha hecho que este tenga una lista de grupos o familias que han tenido una participación activa a lo largo desde su aparición, de los cuales describiremos las familias de Cryrar, Reveton, Locky, Petya, Cryptowall, Teslacrypt, Wannacry, Cryptolocker (Al-rimy, Maarof, & Zainuddin, 2017), Ryuk, Maze, Doppelpaymer, Netwalker, Conti y Revil/Sodinokibi. (ESET, 2021)

a. Cryrar.

Coloca la información de la víctima en archivos RAR-sfx legales y encriptados. (Al-rimy, Maarof, & Zainuddin, 2017)

b. Reveton.

Chantajean a los usuarios impidiéndoles acceder al sistema operativo. (Al-rimy, Maarof, & Zainuddin, 2017)

c. Locky.

Usa el algoritmo AES para cifrar una gran cantidad de archivos cuando se habilitan macros en archivos maliciosos. (Al-rimy, Maarof, & Zainuddin, 2017)

d. Petya.

Cifra la tabla maestra de archivos (MFT) y cada uno de los archivos que contiene un equipo para luego chantajear a los usuarios con un rescate e impidiéndoles acceder al sistema operativo. (Belcic, 2021)

e. Cryptowall.

Cifra los archivos de los usuarios mediante el algoritmo RSA. (Al-rimy, Maarof, & Zainuddin, 2017)

f. Teslacrypt.

Cifrar archivos relacionados con el juego en el sistema del usuario. (Al-rimy, Maarof, & Zainuddin, 2017)

g. Wannacry.

Ataca el equipo mediante el cifrado de archivos de tal manera que no puedes acceder a ellos, bloquea el acceso al ordenador. (Al-rimy, Maarof, & Zainuddin, 2017)

h. Cryptolocker.

Cifran los archivos de los usuarios mediante el algoritmo RSA. (Al-rimy, Maarof, & Zainuddin, 2017)

i. Ryuk.

Este tipo de Ransomware se hizo conocido por tener su objetivo en entidades gubernamentales, infecta el sistema y encripta los datos, a tal forma que hace inaccesible acceder a los datos, solamente hasta que se pague un rescate, que generalmente el pago se hace mediante Bitcoin. (Al-rimy, Maarof, & Zainuddin, 2017)

j. Maze.

Utiliza vínculos maliciosos y archivos adjuntos infectados a través de email no deseado, utiliza la fuerza bruta a través de exploit. (Kaspersky, Kaspersky, 2021)

k. Doppelpaymer.

Este Ransomware se caracteriza por llevar su infección a través de la red, este se infiltra y utiliza la ingeniería social para llevar a cabo su objetivo, generalmente con correos electrónicos maliciosos, que usan enlace spear-phishing, para luego cifrar la información del usuario la cual podrá acceder pagando un rescate. (kaspersky, 2021)

l. Netwalker.

Se propaga usando enlaces phishing y a través de VbScripts, este tipo de infección la hace más certera, incluso llegando a toda la red de computadores que usan Windows. (kaspersky, 2021)

m.Conti.

Utiliza ataques de cifrado de datos, para solicitar rescate, su infiltración es a través de las redes empresariales y utiliza técnicas de doble extorsión. Este malware roba primero los datos para luego cifrarlos, después amenazan en hacer pública la información en la página web “Conti News” si la empresa no hace el pago del rescate. (kaspersky, 2021)

n. Revil/Sodinokibi.

Es un Ransomware para sistemas Windows, es de origen Ruso, tiene como característica la modalidad de RaaS (Ransomware-as-a-Service), este roba la información personal de empresas, explota la vulnerabilidad CVE-2018-8453 para poder entrar al sistema. (kaspersky, 2021)

3. Propagación o distribución

a. Propagación de malware.

En general, el malware se instala en el computador sin que tengamos conocimiento y lo hace a través de descargas o enlaces maliciosos, que simulan los contenidos en los que estamos buscando. (Jaén, 2018)

Una vez que el malware se haya alojado en el computador, los ciberdelincuentes toman posesión de la data de estos equipos, controlando la actividad en los ordenadores, llevando incluso a sitios web maliciosos sin nuestra autorización. (Jaén, 2018).

Los efectos que causa el malware pueden llegar a ser muy perjudiciales a tal grado del robo de la información, pero también hay algunos que son inofensivos. (Jaén, 2018)

b. Propagación de Ransomware.

Específicamente en Ransomware la propagación de este malware, la realiza utilizando múltiples mecanismos con el fin de dejar los datos inaccesibles con el fin de exigir un pago a cambio de acceder a la información.

Un método típico de propagación de Ransomware es mediante los emails maliciosos o email falsos, que aparentan ser seguros provenientes de una empresa, banco o entidad gubernamental, estos engañan al usuario y al descargarlos trae consigo archivos maliciosos Ransomware, que luego pondrá la información inaccesible pues el equipo estará bloqueado.

Otro mecanismo de propagación que usa el Ransomware son los exploit, toda vez que este aprovecha las vulnerabilidades del sistema para ejecutar su código en el equipo y lanzar el Ransomware en este.

También hace su propagación a través de la red, donde busca vulnerabilidades en equipos que estén conectados en la red, una vez introducido en uno de los equipos este es capaz de transmitirse y reproducirse automáticamente en el resto de equipos. (ESET, 2017)

✓ **Mecanismo de propagación Ransomware.**

Hay varias formas en que un atacante puede iniciar un ataque con el objetivo final de plantar el malware / Ransomware en la máquina del usuario. (Mehmoon, Enterprise Survival Guide for Ransomware Attacks, 2016)

Generalmente, la forma más común de ataque es a través de un correo electrónico de phishing en el que se engaña a la víctima (Mehmoon, Enterprise Survival Guide for Ransomware Attacks, 2016), Los ataques Ransomware tienen un mecanismo de propagación, los cuales se describen a continuación:

- Selección de una víctima: El atacante selecciona a su víctima mediante ataques phishing, vulnerabilidades en el sistema de la computadora o por acceso a sitios web maliciosos o infectados. (Mehmoon, Enterprise Survival Guide for Ransomware Attacks, 2016)
- Llevando la carga útil a la computadora: en esta fase se muestra generalmente un ataque phishing por correo malicioso donde al hacer clic o descargar el archivo adjunto, se descarga e instala el Ransomware. (Mehmoon, Enterprise Survival Guide for Ransomware Attacks, 2016)
- Contacto con mando y control: Donde se pone en contacto con el servidor de comando y control (C&C), para obtener indicaciones de clave de cifrado, de tal modo que la computadora queda comprometida y bajo el control del atacante. (Mehmoon, Enterprise Survival Guide for Ransomware Attacks, 2016)
- Descarga de claves públicas: Utiliza el sistema vulnerado como plataforma de retransmisión de Ransomware, propagando el malware por toda la red. (Mehmoon, Enterprise Survival Guide for Ransomware Attacks, 2016)
- Cifrar los archivos infectados: En esta fase el atacante cifra los datos e incluso las copias de seguridad generalmente comienzan con archivos / carpetas con la fecha de acceso más reciente.

(Mehmoon, Enterprise Survival Guide for Ransomware Attacks, 2016)

- Extorsión: La siguiente fase es notificar a la víctima sobre el daño y facilitar la recuperación y accesibilidad de la información, ello tras el pago del rescate. (Mehmoon, Enterprise Survival Guide for Ransomware Attacks, 2016)

4. Ataques día cero

Una vulnerabilidad de día cero o ataque día cero es un riesgo de seguridad, donde un desarrollador de software libera un código malicioso que no se conoce públicamente y que los proveedores de ciberseguridad no conocen. Esto se conoce también como un exploit de día cero, este método utiliza el atacante para acceder al sistema vulnerable. (ESET, 2015)

Estos ataques son amenazas de seguridad graves con altas tasas de éxito, porque las empresas no cuentan con seguridad informática adecuada para mitigar y prevenirlas, visto que ocurre antes de que el objetivo se dé cuenta de que existe la vulnerabilidad. (ESET, 2015)

El ciberdelincuente que lanza este tipo de ataque, no da opción a bloquearlos, dado que los desarrolladores, tendrán que estudiar el nuevo código malicioso para crear una corrección frente a este ataque día cero. (ESET, 2015).

El término "día cero" proviene del mundo de los medios digitales pirateados (ESET, 2015), una película, música o software pirateado se denomina "día cero", cuando es publicado en paralelo o antes del lanzamiento oficial. (ESET, 2015).

✓ Casos relevantes de ataques día cero.

- Sony Pictures: En el año 2014, sufrió el ataque potencialmente más famoso de día cero, dejando como consecuencia la divulgación de

la información confiscada por este ataque, en sitios utilizados para el intercambio de archivos. (Pardo, 2021).

- Google: Descubrió múltiples vulnerabilidades para Zero-Day, que permitía ejecutar código arbitrario en el navegador, para la cual tuvo que lanzar una actualización para reparar el ataque Zero-Day, ello a finales del año 2020. (Owaida, 2021).

- Microsoft: Corrigió 19 vulnerabilidades, entre las cuales cuatro de Microsoft Exchange Server, para la cual lanza una actualización en el mes de abril 2021. (Harán, 2021).

5. Medio de pago

El modo más común de pago de rescate es por Bitcoins, es una moneda digital que ha sido diseñada con un objetivo, para realizar transacciones anónimas en línea, Es lamentable que esta revolucionaria moneda electrónica se utilice casi exclusivamente para cometer delitos, de hecho, muchos de sus usuarios llegan a conocerlo cuando se les pide que paguen un rescate a través de Bitcoin. (Mehmoon, Enterprise Survival Guide for Ransomware Attacks, 2021)

1.3.2. Soluciones Tecnológicas.

1.3.2.1. Tecnología Sandbox

a. Definición de Sandbox

La terminología “Sandbox”, proviene de las palabras inglesas “Sand” y “Box” que significa “arena” y “caja” respectivamente, la definición para el mundo tecnológico parte de este significado, llevándolo a la seguridad informática y definiéndose como un entorno aislado que permite la ejecución de códigos potencialmente peligrosos, otorgando a estos, acceso sólo a ciertos recursos, previamente establecidos con el fin de restringir la capacidad de accesibilidad del programa. (Rodríguez, 2019).

Un Sandbox es una medida de seguridad asociada a la prevención y no a la detección de malware, ya que previene la ejecución de actividades

maliciosas por parte del malware y no detecta la realización de estas, aunque como se mostrará posteriormente, existen soluciones como Cuckoo Sandbox que permiten detectar dichas actividades tras la ejecución del malware. (Rodríguez, 2019).

b. Finalidad de un Sandbox:

Existen diversas aplicaciones peligrosas o código malicioso, en las diversas páginas web por donde los usuarios finales navegan, saber en qué momento pueden ser infectados por un virus, malware o algún otro código malicioso es incierto, y en las instituciones por el alto grado de responsabilidad de los datos de los clientes o usuarios, Es más usual ser atacados por los ciberdelincuentes, por lo que se requiere que las computadoras de usuarios finales tengan herramientas de seguridad, para evitar daños financieros y daños en los equipos, por lo dicho se presentan necesidades como:

- ✓ Prevenir que el malware modifique programas o información existente en el equipo.
- ✓ Evitar la ejecución de código malicioso en una red informática.

c. Objetivos de un Sandbox:

Para tratar estas necesidades existe la tecnología Sandbox, cuyos principales objetivos son:

- ✓ Prevenir de ataques zero-day
- ✓ Restringir el acceso a determinados recursos, memoria y CPU, evitando que acciones maliciosas puedan llevar a cabo infección al sistema y por ende su bloqueo.
- ✓ Limitar el número de procesos creados a partir de una aplicación para así evitar el consumo excesivo de memoria.
- ✓ Controlar la comunicación con la red por parte de los procesos.
- ✓ Controlar la comunicación con el resto de los procesos del equipo.

d. Arquitectura Sandbox

Existen dos modos de desplegar un Sandbox, ya sea basado en el aislamiento completo del programa del resto de recursos y aplicaciones, o basado en reglas, para permitir el acceso a determinados recursos, permitiendo así la compartición de estos con el resto de los programas que se encuentran en el equipo. (Borate & Chavan, 2016)

- ✓ Arquitectura basada en el aislamiento de recursos y el proceso del resto del sistema: Esta arquitectura es utilizada por los diversos métodos de virtualización existentes, como pueden ser el software de virtualización como VirtualBox o VMware y el software que permite crear contenedores como Docker o LXC. (ver fig. 3)

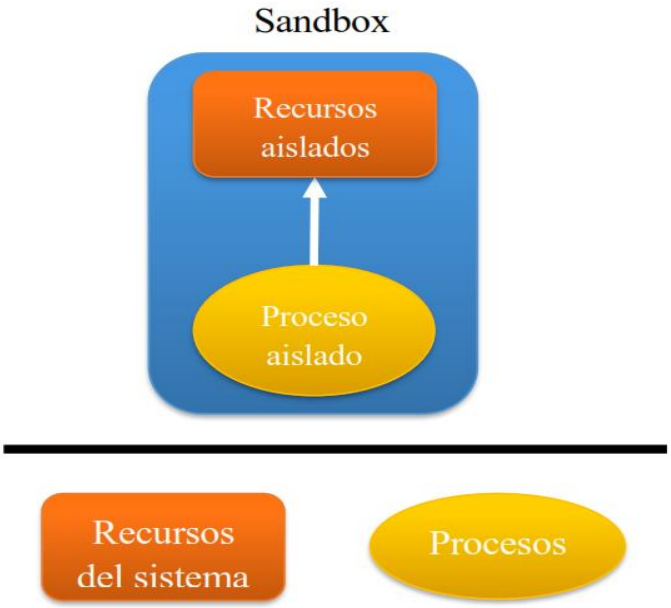


Figura 3. Sandbox basado en aislamiento. Fuente*:* (Borate & Chavan, 2016).

- ✓ El Sandbox basado en reglas: sigue una estructura distinta, ya que este comparte los recursos del sistema con el resto de los procesos.

En la Figura 4 se puede apreciar la arquitectura de un Sandbox basado en el aislamiento de procesos mediante reglas, pues en este tipo de implementaciones los procesos comparten los mismos recursos, aunque el proceso aislado tiene restringido ciertas llamadas al sistema con el fin de controlar las acciones que realiza.

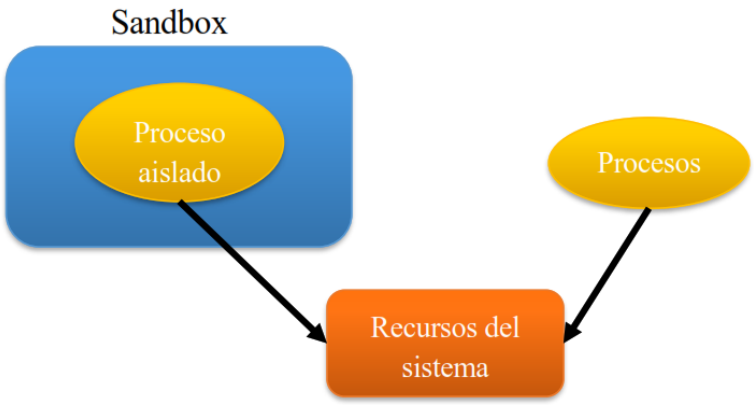


Figura 4. Sandbox basado en reglas. Fuente*: (Borate & Chavan, 2016).*

e. Sandbox en los Sistemas Operativos (S.O)

1. Sandbox en Windows

En la actualización de mayo de 2019 de Windows 10, siendo esta la versión 1903, en la cual se ha implementado la funcionalidad de un entorno aislado denominado Windows Sandbox, para la seguridad de todos los usuarios Windows que cuenten con la versión de Windows Pro y Enterprise. (Microsoft, 2021)

Windows Sandbox es técnicamente una máquina virtual que crea una réplica del sistema operativo existente en el equipo a través del hipervisor de Microsoft, asegurando que lo que ocurra dentro de dicho entorno quedará dentro de él, ofreciendo así máxima seguridad. (Microsoft, 2021), Esta funcionalidad permite ejecutar aplicaciones sospechosas, dentro de un entorno ligero y aislado, corriendo independientemente de nuestra instalación. (Microsoft, 2021)

Cada vez que se utiliza esta funcionalidad se crea una máquina virtual completamente nueva.

Propiedades de Windows Sandbox

- ✓ Parte de Windows: todo lo primordial para esta función está integrado en Windows 10, versión Pro y versión Enterprise, por lo que no hay necesidad de descargar un Virtual Hard Disk (VHD).
- ✓ Prístino: cada vez que se ejecuta Windows Sandbox, es tan limpio como una instalación nueva de Windows.
- ✓ Desechable: Cada vez que se cierra una sesión en Windows Sandbox, automáticamente este se libera de todos los procesos, no quedando rastro alguno de la sesión finalizada en el dispositivo.
- ✓ Seguro: Se fundamenta en el hipervisor de Microsoft para realizar un kernel separado que aísla Windows Sandbox del host, utilizando hardware para una virtualización del Kernel.
- ✓ Eficiente: Usa el desarrollador integrado de kernel, la gestión de memoria inteligente y la GPU virtual. (Microsoft, 2021)

2. Sandbox en MacOs

El sistema operativo macOS, lanzado por la empresa Apple, posee una funcionalidad que permite controlar el acceso a nivel del kernel, denominada App Sandbox y que es proporcionada en este sistema operativo. (Apple, 2016)

La aplicación (App) está diseñada para proteger al sistema de posibles daños, así como a los datos del usuario sí se ejecuta alguna aplicación maliciosa. (Apple, 2016).

La App Sandbox, no previene los ataques contra una aplicación, pero sí minimiza el daño que pueda sufrir. (Apple, 2016).

Una App, que no utiliza Sandbox, cuenta con todos los accesos a los recursos que dicha App le otorga, si esta App es vulnerable en su

seguridad, un atacante puede aprovechar esta vulnerabilidad y controlar la aplicación, teniendo acceso a todos los recursos que la App vincula. (Apple, 2016).

La App Sandbox, está diseñada para mitigar las vulnerabilidades y la estrategia con la cual está desarrollada es doble.

- La App Sandbox, le brinda acceso a una aplicación, sólo para que pueda realizar su trabajo, el resto de accesos son restringidos por ser ejecutado en un entorno aislado
- La desApp Sandbox, permite otorgar acceso adicional a una App, a través de cuadros de diálogo como abrir, guardar, arrastrar y soltar y mediante otras interacciones familiares al usuario. (Apple, 2016)

3. Sandbox en Android

El sistema operativo Android es usado en dispositivos móviles basados en el kernel de Linux, este sistema operativo hereda funciones de seguridad propias de un kernel Linux, como puede ser SELinux. (Android, 2021)

A nivel del sistema operativo, los dispositivos Android proporcionan la seguridad del kernel de Linux, conocida como comunicación segura entre procesos (IPC, del inglés Inter-Process Communication), que facilita la seguridad entre la comunicación de diferentes procesos. Esta característica de seguridad permite incluso asegurar que el código nativo esté restringido por el Sandbox de aplicaciones. (Android, 2021)

Como el sistema operativo se basa en el kernel de Linux, posee varias funcionalidades claves para la seguridad, aunque las más destacadas son:

- Modelo de permisos basado en usuarios
- Aislamiento de procesos

- IPC

Además, como Android está basado en un sistema operativo multiusuario, posee una medida de seguridad para aislar los recursos entre ellos, para ello Linux:

- No permite que un usuario lea los ficheros de otro usuario.
- Asegura que un usuario no agote ni la memoria ni la CPU ni otros dispositivos externos de otro usuario.

Para aumentar la seguridad de las App se utiliza una parte del modelo de seguridad de Android denominado SELinux para aplicar el control de acceso obligatorio (MAC, del inglés Media Access Control) sobre todos los procesos; con esta herramienta se mejora la protección y se restringen los servicios del sistema, el control de acceso a los datos de la información y se protegen de actividades maliciosas por parte de software peligroso. (Android, 2021)

Android se aprovecha de las ventajas que proporciona el sistema de permisos basado en usuarios para identificar y aislar los recursos de las aplicaciones. Las aplicaciones se encuentran aisladas entre ellas para proteger así el sistema y otras aplicaciones de aquellas que realicen acciones maliciosas. Para llevar a cabo esto, el sistema operativo se basa en la asignación de un identificador único de usuario para cada App y la ejecuta en un proceso propio del usuario. (Android, 2021)

Como se ha comentado anteriormente, las aplicaciones no pueden interactuar entre ellas por defecto y tienen un acceso limitado al sistema operativo. Esto restringe que cualquier aplicación intente ejecutar acciones maliciosas como puede ser leer datos de otra aplicación o realizar alguna acción sin los permisos necesarios. (Android, 2021)

4. Sandbox en Linux

La implementación de los diferentes Sandbox se realiza en las diferentes distribuciones de Linux:

a. Distribuciones de Linux

- Distribución Debian, Se trata de una distribución de Linux que consta de un sistema GNU. (Debian, 2021)
- distribución Red Hat Enterprise Linux, mantenida por la empresa Red Hat destinada a un uso general. (RedHat, 2021)
- Kali Linux: orientado a la seguridad de la red. (kali.org, 2021)

b. Módulos de seguridad del kernel de Linux

El núcleo de Linux posee un proyecto denominado Módulos de Seguridad de Linux (LSM, del inglés Linux Security Module) cuyo principal objetivo es el de añadir un módulo de seguridad al núcleo de Linux.

Este proyecto surge de otros proyectos, entre los cuales se encuentran SELinux y AppArmor. (Borate & Chavan, 2016); en la Figura 5 se puede ver el funcionamiento del módulo LSM dentro del núcleo de Linux. Este se basa en la existencia de hooks, que son llamadas al módulo, que se realizan cuando una llamada del sistema a nivel de usuario va a dar acceso a un elemento interno del núcleo. Estos hooks son ejecutados cuando una aplicación realiza una llamada al sistema, para así, poder gestionar la seguridad del núcleo mediante el control de acceso a los recursos.

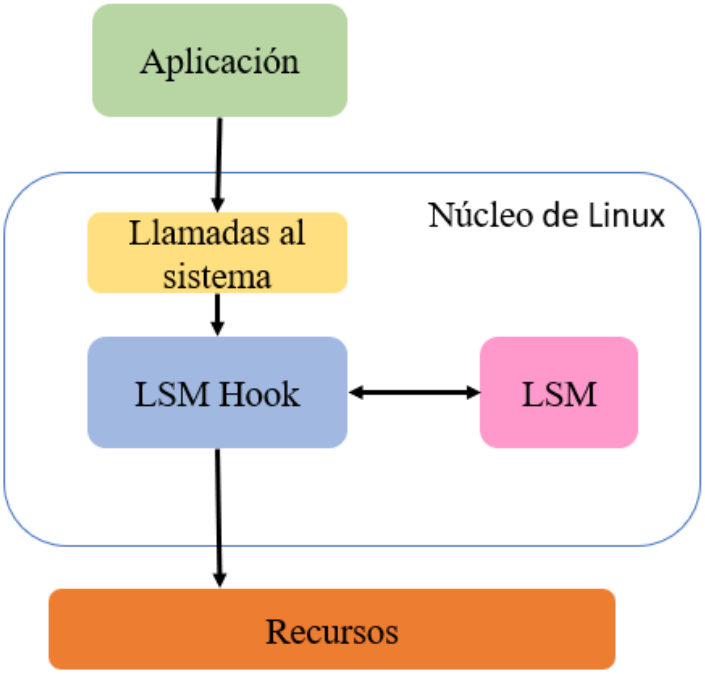


Figura 5: Funcionamiento de LSM. Fuente: *(Borate & Chavan, 2016)*.

- **AppArmor**

Es un mecanismo Mandatory Access Control (MAC), Control obligatorio de acceso, que limita la capacidad de los procesos de realizar llamadas al sistema, pues el núcleo se comunica con esta herramienta para conocer si el proceso puede realizar la llamada al sistema que desea, restringiendo de esta forma las llamadas al sistema que un proceso puede realizar. (Borate & Chavan, 2016)

AppArmor al igual que SELinux se basa en la aplicación de reglas para conocer los permisos de acceso al sistema, pero AppArmor aplica dichas reglas a procesos determinados variando en función de la ruta en la que se encuentra el programa instalado. (Borate & Chavan, 2016)

- **SELinux**

Security-Enhanced Linux (SELinux), se trata al igual que AppArmor de un mecanismo MAC en el que se apoya el núcleo

del sistema para saber sí un programa posee los permisos necesarios para realizar una llamada al sistema determinado. (Borate & Chavan, 2016)

SELinux otorga permisos en función del contexto de seguridad en el que se ejecuta un determinado proceso. Este contexto se encuentra definido por la identidad del usuario que ejecuta el proceso, así como el rol y el dominio en el que se encuentra este en el momento de ejecutar el proceso. (Borate & Chavan, 2016)

- **Cgroups**

Los grupos de control (Cgroups), es una funcionalidad que se encuentra en el kernel de Linux y que permite limitar, aislar y priorizar los recursos del sistema, como pueden ser la memoria, el acceso a la red o la CPU, sin la necesidad de crear una máquina virtual. (Borate & Chavan, 2016)

Cgroups, se trata de un grupo de procesos que tienen establecidos unos determinados límites y uso de los recursos en función del grupo, se puede determinar una serie de usos que son:

- Registrar: Permite llevar la contabilidad de los recursos.
- Limitar: Restringir la máxima asignación de recursos.
- Priorizar: Intenta asignar recursos en función de valores de prioridad, permitiendo así que algunos procesos accedan prioritariamente a determinados recursos.
- Aislar: Proporciona diferentes puntos de vista de los recursos del sistema para los procesos. (Borate & Chavan, 2016)

En la Figura 6, se puede apreciar como la herramienta cgroups asigna una serie de recursos, como son la memoria, la CPU, el

acceso a la red, y la entrada y salida del disco, a un grupo de control.

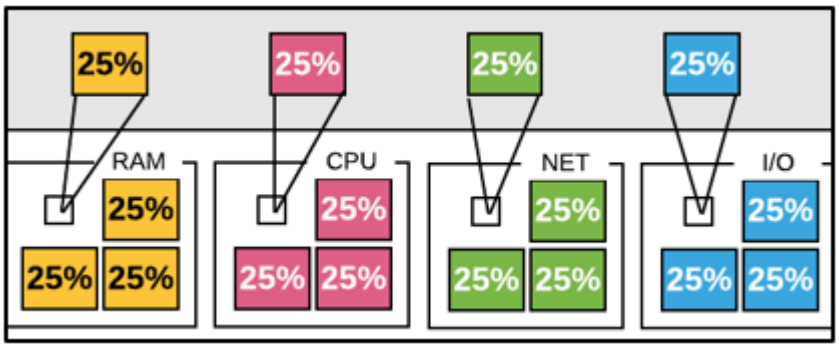


Figura 6. Asignación de recursos de Cgroups. Fuente: *(Linux, 2019).*

f. Tipos de Sandbox

1. Firejail:

Firejail se encuentra escrito en C y puede ser ejecutado en cualquier equipo que use un núcleo de Linux con versión 3.x o posteriores. Se trata de un programa que permite restringir el entorno de ejecución de los programas que son potencialmente peligrosos, utilizando otras herramientas como Namespaces y Seccomp. (Firejail, 2021)

Para cumplir su objetivo, permite que un proceso y todos los que este pueda crear tenga una visión propia de los recursos del núcleo. Permite crear un Sandbox para cualquier proceso, ya sean servidores, o aplicaciones gráficas, entre otros. (Firejail, 2021)

Esta herramienta se basa en el uso conjunto de funcionalidades de seguridad existentes en el núcleo de Linux.

El programa configura estas funcionalidades y espera en segundo plano. Las tecnologías usadas para crear el Sandbox son: Namespaces, Chroot, Seccomp, “Capabilities”, AppArmor y SUID, que son los permisos de acceso que pueden asignarse a los ficheros.

2. Seccomp:

Seccomp, cuyo nombre proviene de las palabras “Secure Computing Mode”, viene incorporado con el núcleo de Linux desde el año 2005, y se trata de una funcionalidad de seguridad del kernel de Linux. (Community, 2019)

Este restringe las llamadas al sistema que un proceso puede realizar y en caso de que se realice alguna distinta, termina el proceso. Las llamadas al sistema permitidas son:

- write()
- read()
- sigreturn()
- exit()

Cuando se intenta realizar una llamada al sistema, no nombrada anteriormente, el proceso termina inmediatamente, pues esto mejora la seguridad del sistema, ya que cualquier fallo que ocurra es propenso a provocar errores en el sistema. (Community, 2019)

Por otra parte, con esta herramienta, no se obtiene ninguna advertencia sobre la finalización del proceso debido al intento de ejecutar una llamada al sistema no autorizada. Además, como las llamadas al sistema que se permiten requieren del uso de la memoria para escribir ciertos datos, es necesario inspeccionar los argumentos utilizados para las llamadas al sistema para comprobar que no trata de realizar ninguna acción maliciosa. (Community, 2019)

Existe una extensión de Seccomp, denominada Seccomp-bpf que permite el filtrado de las llamadas del sistema usando políticas implementadas basadas en las reglas Berkeley Packet Filter. Se encuentra disponible desde la versión 3.5 de Linux. Esta extensión de Seccomp es la usada por Firejail. (IBM, 2019)

Estos filtros son utilizados para permitir o denegar un conjunto de llamadas del sistema, así como para filtrar argumentos de estas llamadas. Cuando un proceso ejecuta una llamada del sistema prohibida, el filtro genera una señal para que el gestor de señales simule una llamada no permitida al sistema. (IBM, 2019).

3. Chroot

Chroot se trata de una herramienta implementada en los sistemas Linux desde 1982, que permite cambiar el directorio raíz para un proceso que se está ejecutando a otro directorio específico, mediante lo cual se consigue la creación de una jaula o “jail”. (Borate & Chavan, 2016).

El programa percibe el árbol de directorios dado como su directorio raíz, impidiendo el acceso a aquellos ficheros que se encuentren fuera del nuevo directorio raíz. Esta herramienta únicamente funciona para proteger el sistema de ficheros, pero no protege otros recursos como pueden ser la memoria o los puertos de red. (Borate & Chavan, 2016)

En la Figura 7 se puede apreciar cómo se encuentra el árbol de directorios del sistema una vez creado un entorno restringido. Una nueva aplicación puede ser ejecutada dentro de este nuevo árbol de directorios, simulando así un nuevo directorio raíz para este, evitando así su acceso a directorios fuera del entorno. (Borate & Chavan, 2016).

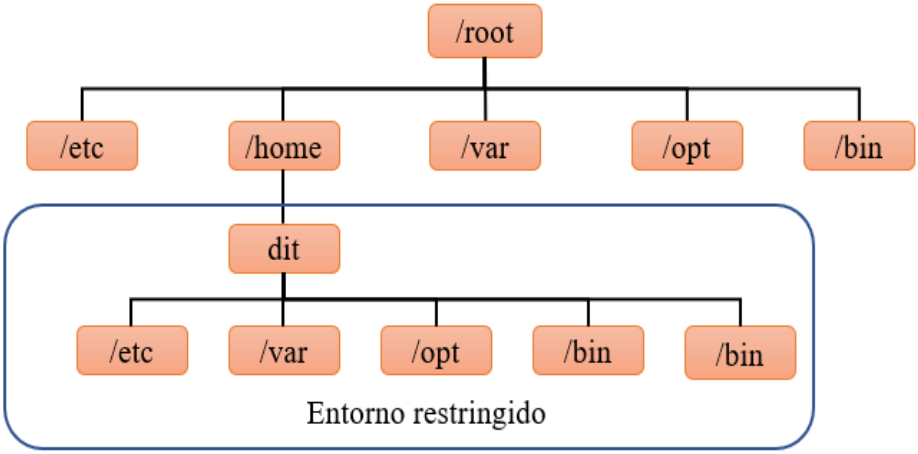


Figura 7. Árbol de directorios de linux una vez creado el entorno restringido. Fuente. *(Borate & Chavan, 2016).*

4. Capabilities

En los sistemas Linux existen privilegios de usuario para determinar las acciones que los procesos pueden realizar, diferenciándose entre dos tipos, procesos con privilegios y sin privilegios. (López, 2015)

- Procesos con privilegios: Se refiere a los procesos con permisos de superusuario.

  Los procesos con privilegios pueden sobrepasar cualquier restricción del kernel, mientras que los procesos sin privilegios están sujetos a las credenciales del proceso, siendo estos normalmente el identificador de User Identification (UID), el identificador Group Identification efectivo (GID) y una lista suplementaria de grupos. (López, 2015)

  Desde la versión 2.2 del núcleo de Linux, los privilegios asociados a los superusuarios se distinguen en diferentes unidades llamadas “capabilities” con el fin de dividir el poder de un superusuario en privilegios específicos, de modo que, si se vulnera un proceso que posee una serie de “capabilities”, el daño potencial es limitado en comparación con el mismo proceso que se ejecuta como superusuario.

> Las “capabilities” permiten conceder a un proceso los privilegios que sean necesarios para su ejecución, sin la obligación de otorgar todos los permisos asociados a un superusuario. Debido a la granularidad que esta funcionalidad proporciona, se puede ejecutar tareas privilegiadas únicamente con los privilegios mínimos requeridos. Esta herramienta es usada comúnmente para entornos de virtualización cómo LXC o Docker, con el fin de restringir las capacidades usadas a la hora de crear un contenedor. (López, 2015)

5. Cuckoo Sandbox

Destaca por ser Open Source. Es una herramienta que permite el análisis automático del malware, en sistemas operativos como: Windows, macOS, Linux y Android. (Cuckoo, 2019)

Al igual que el resto de Sandbox protege de las actividades maliciosas que puedan ejecutar, pero además otorga un reporte detallado acerca del comportamiento tras su ejecución. (Zutphen, 2019)

Para ejecutar la batería de pruebas en este entorno, se requiere de la instalación de un entorno de virtualización, para la realización de las pruebas en un entorno aislado. Tras su ejecución, Cuckoo Sandbox proporciona un análisis completo de las acciones llevadas a cabo por el código con el objetivo de poder examinar su comportamiento. (Zutphen, 2019)

6. LXC

Los contenedores de Linux (LXC) se tratan de una herramienta que permite la virtualización a nivel del sistema operativo, también llamadas virtualización basadas en contenedores, para así ejecutar diferentes sistemas Linux aislados donde ejecutar diferentes aplicaciones en un único núcleo de Linux. (Linux, 2021)

Para ello, utiliza diferentes herramientas existentes en el núcleo de Linux, como son las herramientas seccomp, SELinux, AppArmor y Namespaces, con lo que permite crear estos entornos. (Linux, 2021)

g. Evasión de Sandbox

El malware ha ido incrementando con el transcurrir del tiempo, y su resistencia ha evolucionado por la complejidad en su código, para contrarrestar estos códigos maliciosos, las empresas en seguridad informática, han ido implementando tecnología, capaz de salvaguardar a los usuarios frente a estos ciberdelincuentes, como antivirus, sistemas de detección de intrusos (IDS, del inglés Intrusion Detection System), o el Sandbox, que está materia de estudios en esta tesis.

Por su parte, los ciber delincuentes, han ido desarrollando formas de detectar la existencia de dichas herramientas de seguridad, así como técnicas para evadir y poder llevar a cabo sus actividades maliciosas.

En este apartado se describen las diferentes técnicas desarrolladas por los atacantes expertos para poder detectar y evadir los Sandbox, así como las acciones de contramedidas que se pueden implementar para contrarrestar estas técnicas.

En estas técnicas se tiene: Las técnicas de detección, técnicas de evasión y acciones de contramedidas.

1. **Técnicas de detección:**

   Se describen las principales técnicas utilizadas por el malware para detectar que el código malicioso se está ejecutando dentro de un Sandbox, para así evitar mostrar las acciones maliciosas que realiza y que el usuario se percate de la existencia de estas. (Keragala, 2021)

   - **Interacción del usuario:**

     Para evadir Sandbox, los programas maliciosos tratan de detectar las interacciones entre el usuario y el equipo como:

- ✓ Pulsaciones de teclas.
- ✓ Comprobación de velocidad y frecuencia de pulsaciones del ratón.
- ✓ Cambios en la interfaz de usuario.

- **Tiempo de encendido:**

  El tiempo de encendido del equipo, así como el tiempo que ha transcurrido desde la última interacción del usuario con el sistema, brinda indicios si el entorno en el que se ejecuta la aplicación se encuentra dentro de un Sandbox; debido a que se espera que la última interacción del usuario con el sistema sea reciente y el tiempo de encendido sea propenso para garantizar que el entorno se está ejecutando fuera de un Sandbox.

- **Identificación digital de un Sandbox**

  Sandbox está diseñado para replicar de la mejor manera a un sistema real, sin embargo, existen modos de detectar que el sistema está aislado.

  La diferencia entre la ejecución de un sistema real y un sistema aislado, se basa por los ficheros de configuración, información del sistema, procesos, registros, servicios o adaptadores de red. Habitualmente, el malware suele investigar acerca de los siguientes puntos clave:

  - ✓ Dispositivos conectados: busca controladores instalados de dispositivos internos o externos conectados al sistema, la falta de estos, puede indicar que el programa está siendo ejecutado en un entorno aislado Sandbox.

  - ✓ Procesos y servicios ejecutados: Usualmente, el software de virtualización, utilizado como un entorno aislado Sandbox, posee servicios o procesos que son ejecutados para su funcionamiento. Por lo tanto, la detección de

algunos de estos servicios o procesos indicaría la existencia de un Sandbox.

- ✓ Ficheros y registros: búsqueda de ficheros y registros que son característicos de un sistema operativo o de un Sandbox.

- ✓ Número de procesadores: Usualmente, Sandbox trabaja con uno o dos procesadores por lo que la detección de esta cantidad de procesadores podría indicar la presencia de un entorno aislado.

- ✓ Tamaño y nombre del disco: El tamaño asignado al disco virtual del entorno, puede dar indicios de la ejecución del sistema dentro de un entorno aislado.

- ✓ Dirección MAC: Existe software que, al virtualizar el sistema operativo, crea interfaces de red virtuales, a las cuales asigna una determinada dirección MAC, normalmente siguiendo un patrón en concreto y que denota que dicha MAC pertenece a un entorno virtual.

- **Comprobación del hardware**

  Algunos, malware tienen la posibilidad de verificar valores asociados a datos del hardware, como puede ser la temperatura a la que se encuentra el sistema o si el sistema está siendo recargado, entre otros. Este tipo de indicios puede indicar que el malware se encuentre en un entorno aislado del real.

2. Técnicas de evasión

Para la tecnología en estudio, existen métodos que permiten evadir la seguridad que este brinda, porque los atacantes crean nuevos malware más sofisticados, incorporando ataques más completos.

A continuación, se mencionan algunas de las técnicas usadas por estos atacantes para evadir esta tecnología.

- **Ocultación de Sandbox**

  El objetivo del malware es, ocultar su comportamiento, al detectar que han ingresado a un entorno aislado, evitando ser detectado y filtrándose como un software en beneficio para el usuario, y así este pueda ejecutarlo en un entorno real.

  En esta técnica se puede mencionar a los siguientes malware:

  - ✓ BadPatch: Detecta sí se está ejecutando en una máquina virtual, obteniendo información sobre el nombre del disco, la BIOS e información de la placa base.
  - ✓ Dyre: Detecta sí se encuentra en un Sandbox mediante la inspección de los procesos y los registros.
  - ✓ OopsIE: Trata de comprobar la temperatura del sistema para ver sí se está ejecutando en un entorno virtual.
  - ✓ ROKRAT: Detecta sí se encuentra en un Sandbox mediante la búsqueda de librerías.

- **Detección de interacciones del usuario**

  Para este caso el malware ha sido ejecutado en el sistema, pero no realiza ninguna acción maliciosa, a no ser que el usuario interactúe concretamente con el sistema. En esta técnica se puede nombrar a los siguientes malware.

  - ✓ FIN7: Utiliza una imagen adjuntada en un documento, y este malware es solamente activado cuando un usuario realiza una pulsación doble sobre dicha imagen.
  - ✓ BaneChant: Espera a que se produzcan un número determinado de pulsaciones para comenzar a ejecutar sus acciones malintencionadas.

- **Inicio aplazado**

  Utilizada para poder evadir un Sandbox, para que se ejecute este tipo de malware, espera un determinado tiempo, o se ejecutan solamente en ciertos días u horas establecidas en su código.

  A partir de esta definición aparecen tres técnicas:

  - ✓ Sleep: Esta técnica espera un cierto tiempo tras la ejecución del programa para ejecutar sus actividades. Está asociada a la técnica del sistema Linux denominada “sleep”. (Linux, linux.die.net, 2021)
  - ✓ Delay: Esta técnica es similar a la técnica nombrada anteriormente, realizando durante el tiempo de espera acciones sin maldad para simular que realiza acciones benignas, además de tratar en detectar interacciones por parte del usuario con el sistema.
  - ✓ Time attacking: Esperan a la llegada de una hora o día en concreto, para ejecutar sus acciones maliciosas.

Ursnif: es un malware que utiliza alguna de estas técnicas, espera 30 minutos tras su ejecución para llevar a cabo sus acciones malignas. (Njccic, 2016)

- **Escape de máquinas virtuales**

  Las máquinas virtuales son entornos virtuales aislados que ejecutan un sistema operativo aislado dentro del sistema operativo anfitrión, y en ambos sistemas no debería existir forma de interacción. (Ramírez, 2020)

  Se dice escape de una máquina virtual porque los dos sistemas operativos tienen interacción al romper este aislamiento, tras este rompimiento se suscitan vulnerabilidades que se escapan de una máquina virtual. (Descalzo, 2016)

  - ✓ Se puede realizar una denegación de servicio debido a una vulnerabilidad que permite escribir fuera de los límites y que es provocado por archivos de sombreado especialmente diseñados (TALOS-2019-0757). Además, si el equipo anfitrión usa una tarjeta gráfica de NVIDIA, la denegación de servicio se puede convertir en una ejecución arbitraria de código, permitiendo ejecutar dicho código en el sistema anfitrión (TALOS-2019-0779) (CISCO, 2019). Esta vulnerabilidad afecta al software de virtualización de VMware. (VMware, 2019)
  - ✓ La vulnerabilidad CVE-2015-6240, permite escapar de un entorno aislado creado mediante la herramienta Chroot debido a la posibilidad de acceder a ficheros externos del entorno virtual a través de enlaces simbólicos. (Nvd, 2015)
  - ✓ La vulnerabilidad CVE-2017-5123 permite aprovechar un fallo en una función de Linux en las versiones 4.12 y 4.13

que realiza un escalado de privilegios y escape de un contenedor Docker. (RedHat, Redhat.com, 2019)

3. **Acciones de contramedidas**

- Configuración Sandbox: Para las técnicas de detección mencionadas, ciertos Sandbox permiten la configuración de registros, ficheros, información del sistema, etc. con el fin de ocultar su entorno de modo que el malware no pueda detectar indicios de que se encuentra en un entorno virtualizado.

  Además, algunas herramientas dan la posibilidad de simular interacciones entre el usuario y el sistema como pulsaciones de teclas o del ratón para así engañar al malware.

  Para contrarrestar los ataques asociados a un inicio retardado de la ejecución de las acciones maliciosas, se pueden llevar a cabo las siguientes acciones:

  - ✓ Cambiar la hora del sistema con el fin de que se avance en el tiempo para engañar al malware y que este realice sus acciones malintencionadas.
  - ✓ Por otra parte, al ejecutarse un programa y ver que este no realiza ninguna acción, proporciona indicios de que pueda poseer actividad maliciosa en él, provocando así que se monitorice su ejecución.
  - ✓ Además, existen herramientas como pinVMShield, que permite engañar al malware, para así evadir las técnicas de detección de máquinas virtuales y Sandbox. (Rjrodriguez, 2019)

1.4. Formulación del Problema.

¿Cómo mejorar la protección de una red informática local de una entidad financiera en la prevención de ataques Ransomware?

1.5. Justificación e importancia del estudio.

América Latina, durante el cuarto trimestre del año 2020, fue atacado por virus en un 15.11%, por Exploits en un 14,67% y por Bolnet un 12,72% (Tabla 1).

Tabla 1.
Porcentajes de ataques en el cuarto trimestre del año 2020 en América Latina.

	% Virus	% Exploits	% Bolnet	Total
América Latina	15.11%	14,67 %	12,72%	42.5 %
Perú	1.07 %	1.33 %	0.64 %	3.04 %

Fuente Elaboración propia.

Perú se encuentra en el ranking número 5 entre los países de Latinoamérica, según Fortinet con 3.04 % que equivalen a 800 669 544 ataques, efectuados entre los meses de octubre a diciembre del año 2020, Por tal motivo, es necesario que las empresas cuenten con una infraestructura tecnológica adecuada y robusta, para prevenir los ciberataques.

Es importante resaltar que las entidades financieras son afectadas por estos atacantes cibernéticos; disminuir las brechas de vulnerabilidad dentro de una red financiera, para salvaguardar la información que es su principal activo, es el objeto principal de este estudio.

Por lo que, en la presente investigación se propuso la implementación de tecnología Sandbox para proteger de ataques Ransomware en una red informática local de una entidad financiera.

1.6. Hipótesis.

La implementación de la tecnología Sandbox mejora la protección de una red informática local frente a los ataques de Ransomware en una entidad financiera.

1.7. Objetivos.

1.7.1. Objetivo general.

Implementar tecnología sandbox para proteger de ataques de Ransomware en una red local de una entidad financiera.

1.7.2. Objetivos específicos.

a) Realizar el análisis del estado actual de la red informática local de la entidad financiera.

b) Implementar el servidor con tecnología sandbox para la protección de ataques Ransomware en la red informática local de la entidad financiera.

c) Realizar pruebas de laboratorio para determinar la eficiencia de la tecnología sandbox para proteger de ataques Ransomware.

II. MATERIAL Y MÉTODO

2.1. Tipo y Diseño de Investigación.

2.1.1. Tipo de investigación

La investigación desarrollada fue de tipo cuantitativa, porque se logró identificar una técnica para la recolección de datos, en un contexto de estudio científico, en donde se desarrolló de manera satisfactoria el objetivo general planteado, y con la recolección de datos se comprobó la hipótesis planteada.

2.1.2. Diseño de la investigación

La investigación fue de diseño cuasi experimental, porque la muestra utilizada de la población no se eligió aleatoriamente, sino que fue elegida por el alto grado de consecuencias que este ocasiona al filtrarse en una víctima.

2.2. Población y muestra.

2.2.1. Población

La población de esta investigación se basó en los malware tipo Ransomware. (anexo 5).

2.2.2. Muestra

Para esta investigación se utilizó una muestra no probabilística, siendo la muestra 5 tipos de Ransomware (anexo 6), estas se han elegido por ser los principales Ransomware que atacan a las instituciones en Latino América (ESET, 2021) y que se encuentran más activas del resto, en los 5 últimos años, cifrando datos y exigiendo un alto rescate económico por la liberación de la información secuestrada. (Kaspersky, 2021)

2.3. Variables, operacionalización.

Tabla 2.
Instrumentos de recolección de datos, fórmulas para obtención de datos por cada indicador de las variables dependiente e independiente.

Variables	Dimensión	Indicador	Ítem	Técnica e instrumentos de recolección de datos
Variable Independiente	Tecnología Sandbox	Promedio del consumo de memoria.	$\overline{cm} = \frac{\sum cm_i}{n}$	Instrumentos mecánicos o electrónicos / Registro Electrónico
		Tiempo promedio de duración para el análisis de ataques sospechosos	$\bar{t} = \frac{\sum x_i}{n}$	
Variable Dependiente	Protección de una red informática local	Porcentaje de efectividad de Sandbox, frente a ataques sospechosos.	$e = \frac{aa * 100}{n}$	
		Respuesta a incidentes de ataques maliciosos notificados a tiempo.	$e = \frac{int * 100}{ti}$	
		Cobertura de host para detección y tratamiento de Ransomware.	$chost = \frac{pr * 100}{thost}$	
		Cobertura de análisis de riesgos de los hosts.	$car = \frac{ca * 100}{ta}$	

Fuente. Elaboración propia.

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad.

2.4.1. Técnicas e Instrumentos

- ✓ Las técnicas utilizadas en esta investigación fueron mecánicos o electrónicos; porque se obtuvieron reportes brindados por la tecnología Sandbox, los cuales se analizaron, midiendo de esa forma los indicadores y se evaluó cada una de las variables que han sido materia de estudio.
- ✓ Se elaboró 2 formatos que se utilizaron como instrumentos para la recolección de datos por cada indicador, los cuales mostramos a continuación:

1. Formato para las pruebas de laboratorio.

Este formato (anexo 3), permitió obtener los datos generales de los ataques Ransomware realizados en el laboratorio de pruebas, los datos que se registraron en este formato fueron:

N°. Ataque, Nombre de Ransomware, Fecha, Hora inicio, Hora Fin, Tiempo de duración del ataque y estado (Aislado, No aislado), además se registró la memoria inicial y memoria final utilizado en cada ataque, con ello se evaluó el indicador PROMEDIO CONSUMO DE MEMORIA.

Los datos de este formato fueron registrados antes y después de finalizado cada prueba de ataque, obteniendo los datos de consumo de memoria en Linux con el comando TOP o HTOP y fue validado dicha información por los tesistas.

2. Formato de resultados de las pruebas de laboratorio.

Este formato (anexo 4), permitió registrar los resultados de las pruebas de laboratorio indicado en porcentaje, para ello se trabajó con los indicadores propuestos:

- ✓ Tiempo promedio de duración para el análisis de ataques sospechosos.

Permitió obtener como resultado el tiempo promedio que Sandbox utilizó en analizar los ataques en el laboratorio de pruebas, los datos que se registraron en este formato fueron:

La sumatoria del tiempo empleado para el análisis de Ransomware y el número de ataques de laboratorio.

- ✓ porcentaje de efectividad de Sandbox, frente a ataques sospechosos.

Permitió obtener el porcentaje de efectividad de Sandbox, los datos que se registraron en este formato fueron:

Total de ataques aislados, total de ataques en la prueba.

- ✓ porcentaje de respuesta a incidentes de ataques maliciosos notificados a tiempo.

Permitió obtener la respuesta de ataques maliciosos notificados por Sandbox, los datos que se registraron en este formato fueron:

Total de respuestas a tiempo, total de infecciones que pasaron a la red.

- ✓ Porcentaje de cobertura de host para de detección y tratamiento de malware

Permitió obtener el porcentaje de host coberturados en la red, para detección y tratamiento de Ransomware, los datos que se registraron en este formato fueron:

total de host coberturados en la red y el total de pruebas de Ransomware.

- ✓ Porcentaje de cobertura de análisis de riesgos de los hosts.

Permitió obtener la cobertura de análisis de riesgos de los hosts, los datos que se registraron en este formato fueron:

Total de hosts coberturados y total de hosts en la red.

Los datos de este formato fueron registrados antes y después de finalizado cada prueba de ataque, y fue validado dicha información por los tesistas.

2.5. Procedimiento de análisis de datos.

2.5.1. Tecnología Sandbox

En esta investigación la dimensión estudiada fue la Tecnología Sandbox que también se denominó variable independiente.

Para la obtención de los resultados esperados, se elaboraron una serie de indicadores, las cuales fueron analizadas del recojo de información obtenida en los instrumentos de recolección de datos, los cuales fueron procesados y operados mediante fórmulas matemáticas, las cuales se explican por cada indicador a continuación.

2.5.1.1. Promedio de consumo de memoria:

Es el promedio de consumo de memoria que utilizó la tecnología Sandbox en la ejecución de toda la prueba de laboratorio y se representa con la siguiente fórmula:

$$\overline{cm} = \frac{\sum cm_i}{n}$$

Donde:

$\overline{cm}$ = promedio del consumo de memoria

$\sum cm_i$ = Es la sumatoria del consumo de memoria por prueba de código malicioso (i).

n = Es el total de pruebas inyectadas.

2.5.1.2. Tiempo promedio de duración para el análisis de ataques sospechosos

Es el tiempo promedio de duración que empleó Sandbox para el análisis de ataques sospechosos y se representa con la siguiente fórmula:

$$\bar{t} = \frac{\sum x_i}{n}$$

Donde:

$\bar{t}$ = Tiempo promedio empleado por Sandbox para el análisis de código malicioso

$\sum x_i$ = Es la sumatoria del tiempo empleado por cada análisis de código malicioso (i) en las pruebas.

n = Es el total de código malicioso inyectado.

2.5.1.3. Porcentaje de efectividad de Sandbox, frente a ataques sospechosos.

Es el porcentaje de la efectividad de Sandbox para aislar ataques sospechosos y se representa con la siguiente fórmula:

$$e = \frac{aa * 100}{n}$$

Donde

e = es el porcentaje de efectividad de Sandbox.

aa = Es el total de ataques aislados por Sandbox.

n = Es el total de ataques inyectados a Sandbox.

2.5.2. Protección de una red informática local

La variable independiente es la protección de la red informática local, en este punto se tomaron indicadores existentes en la norma ISO 27001, con la finalidad de medir mediante fórmulas matemáticas, el estado de la red post-Sandbox, a continuación, se describe cada indicador con su respectiva fórmula de medición.

2.5.2.1. Respuesta a incidentes de ataques maliciosos notificados a tiempo.

Es el porcentaje de respuestas a incidentes de ataques maliciosos que la red notificó a tiempo, y se representa con la siguiente fórmula:

$$e = \frac{int * 100}{ti}$$

Donde

e = es el porcentaje de respuestas de la red frente a ataques maliciosos.

int = Es el total de respuestas notificadas a tiempo.

ti = Es el total de infecciones que no pasaron a la red.

2.5.2.2. Porcentaje de cobertura de host para detección y tratamiento de malware.

Es el porcentaje de host que se encuentran en la red y que Sandbox detecta y trata actividad maliciosa.

$$chost = \frac{pr * 100}{thost}$$

Donde

$chost$ = Es el porcentaje de host coberturados.

pr = Es el total de Ransomware aislados.

$thost$ = Es el total de host utilizados en la red.

2.5.2.3. Porcentaje de cobertura de análisis de riesgos de los host

Es el porcentaje de cobertura de análisis de riesgo de los host de toda la red, y se representa con la siguiente fórmula:

$$car = \frac{ca * 100}{ta}$$

Donde

car = Es el porcentaje de análisis de riesgo de los host coberturados.

ca = Total de aplicaciones coberturadas.

ta = Es el total de aplicaciones en la red.

2.6. Criterios éticos.

2.6.1. Consentimiento o aprobación de la participación

Orientado a obtener el consentimiento o la aprobación de los participantes; en este criterio se encuentra la entidad financiera que brindará el espacio para la implementación del laboratorio de pruebas requerido en este trabajo de investigación.

2.6.2. Confidencialidad

Orientado a salvaguardar la identidad de los participantes que apoyaron en este trabajo de investigación, entre ellos se encuentra la institución financiera donde se realizarán las pruebas de laboratorio, donde los datos permanecerán en el anonimato, y solamente se mostrarán los resultados de las variables operadas.

2.6.3. Originalidad

Orientado a salvaguardar la originalidad del trabajo de investigación, donde se respeta los derechos de autor con previas citas y referencias a la información obtenida y plasmada de cualquier autor en esta línea de investigación.

2.7. Criterios de Rigor Científico.

2.7.1. Consistencia:

Esta investigación es consistente porque cuenta con valores reales, obtenidos de las pruebas realizadas en laboratorio y operadas de acuerdo a las fórmulas matemáticas de cada indicador estudiado.

2.7.2. Validez:

Se utilizarán los instrumentos desarrollados para la recolección de datos, de acuerdo a cada indicador especificado en la operacionalización de variables, que servirán para dar validez a este trabajo de investigación.

2.7.3. Neutralidad

Esta investigación es neutral porque se basa en los resultados adquiridos de las pruebas realizadas, no se presta a ningún interés personal, ni institucional, es una

investigación realizada con todas las garantías de no favorecer a ninguno de los participantes involucrados en el desarrollo, implementación y ejecución de esta tesis.

III. RESULTADOS.

3.1. Resultados en Tablas y Figuras.

a. Estado actual de la red – antes de instalar el servidor cuckoo Sandbox.

Antes de instalar el servidor Cuckoo Sandbox se probó la seguridad perimetral de la red existente en la entidad financiera, con el objetivo de desterminar el porcentaje de seguridad en la red informática existente en la entidad, Mostrándose el resultado en la figura N. 8.

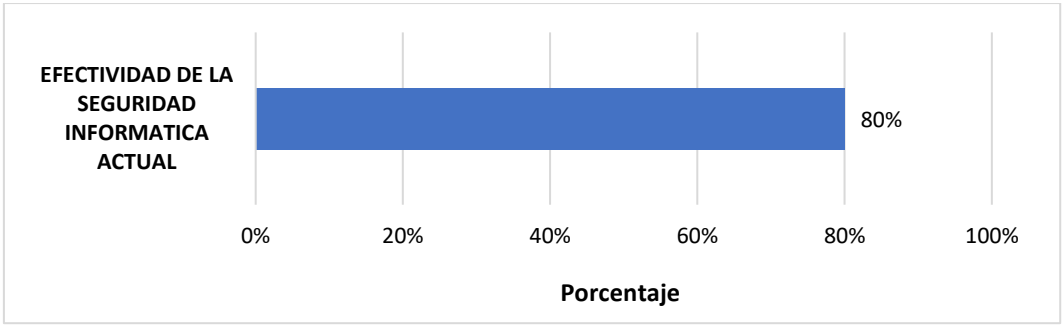


Figura 8. Porcentaje de efectividad de la seguridad informática actual.

Como se puede observar en la figura N. 8, el porcentaje de efectividad con la que cuenta la red informática de la entidad financiera es del 80%, esto debido a que el Ataque exploit inyectado logró vulnerar la seguridad informática por el puerto 4443, como se muestra en la Figura N. 39.

b. Después de la instalación de la tecnología Sandbox.

En la presente investigación se planteó como objetivo Implementar tecnología Sandbox para proteger de ataques de Ransomware en una red local de una entidad financiera; para lograr el objetivo planteado, se instaló el Sistema Operativo Ubuntu 20.04, que fue base para la implementación de

la tecnología Sandbox, se implementó un laboratorio de pruebas virtualizado con el software VirtualBox, posteriormente se descargó la muestra de Ransomware (anexo 5) para las pruebas de laboratorio cuyo resultado sería la efectividad de la tecnología Sandbox frente a ataques Ransomware, para lo cual se elaboró una ficha de recolección de datos con base a indicadores los cuales fueron procesados y los resultados obtenidos se detallan a continuación.

El primer indicador evalúa el **promedio del consumo de memoria RAM** expresado en gigabytes (Gb), para ello se ha obtenido el consumo de memoria RAM por cada análisis de Ransomware como se muestra en la figura N. 8 y el promedio de memoria RAM se ha obtenido desarrollando la siguiente ecuación.

$$\overline{cm} = \frac{\sum cm_i}{n}$$

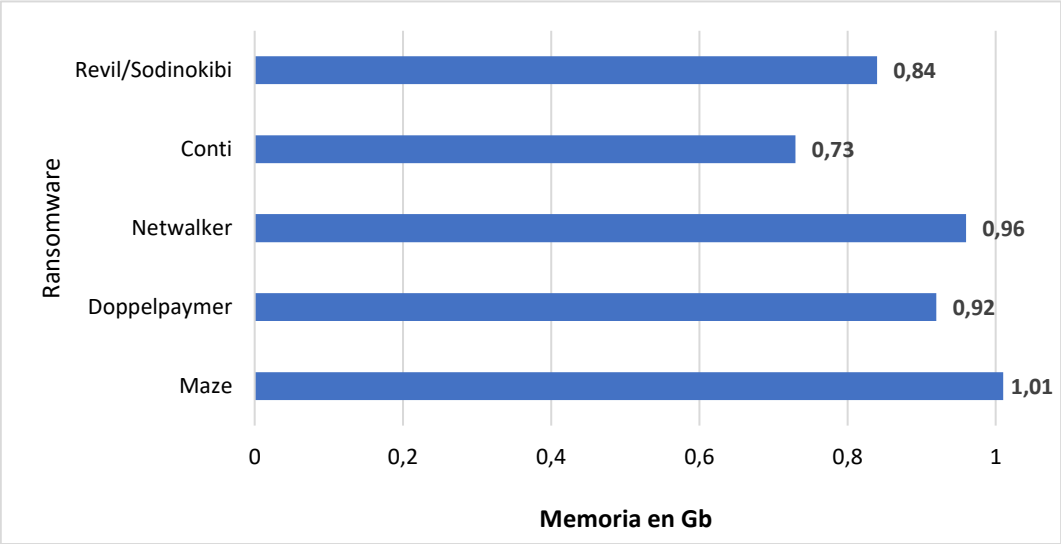


Figura 9. Memoria usada por cada análisis Ransomware*, expresado en gb*.

Como se puede observar en la figura N. 9, el promedio de consumo de memoria RAM, que la tecnología Sandbox utilizó para el análisis de Ransomware fue de 0.89 Gb, el cual es un promedio óptimo obtenido en esta investigación, considerando que Cuckoo Sandbox utiliza 7.5 Gb para su ejecución.

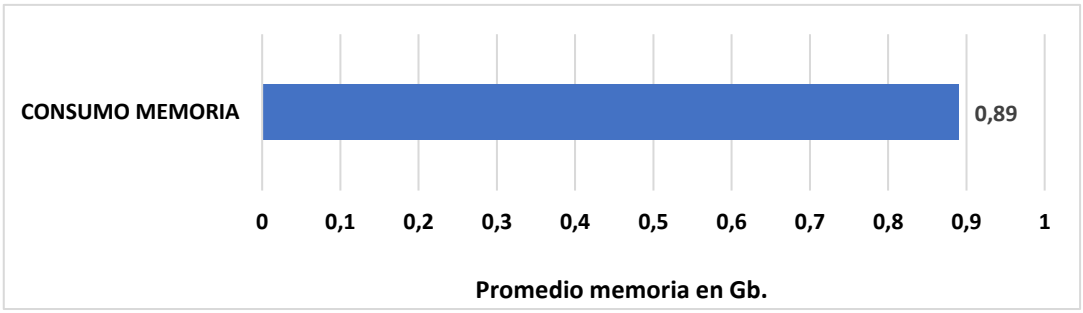


Figura 10. Promedio consumo de memoria, expresado en Gb

El segundo indicador evalúa el **tiempo promedio de duración para el análisis de ataques sospechosos** expresado en segundos, para ello se ha obtenido el tiempo de duración por cada análisis de Ransomware, como se muestra en la figura N. 10 y el tiempo promedio se ha obtenido desarrollando la siguiente ecuación.

$$\bar{t} = \frac{\sum x_i}{n}$$

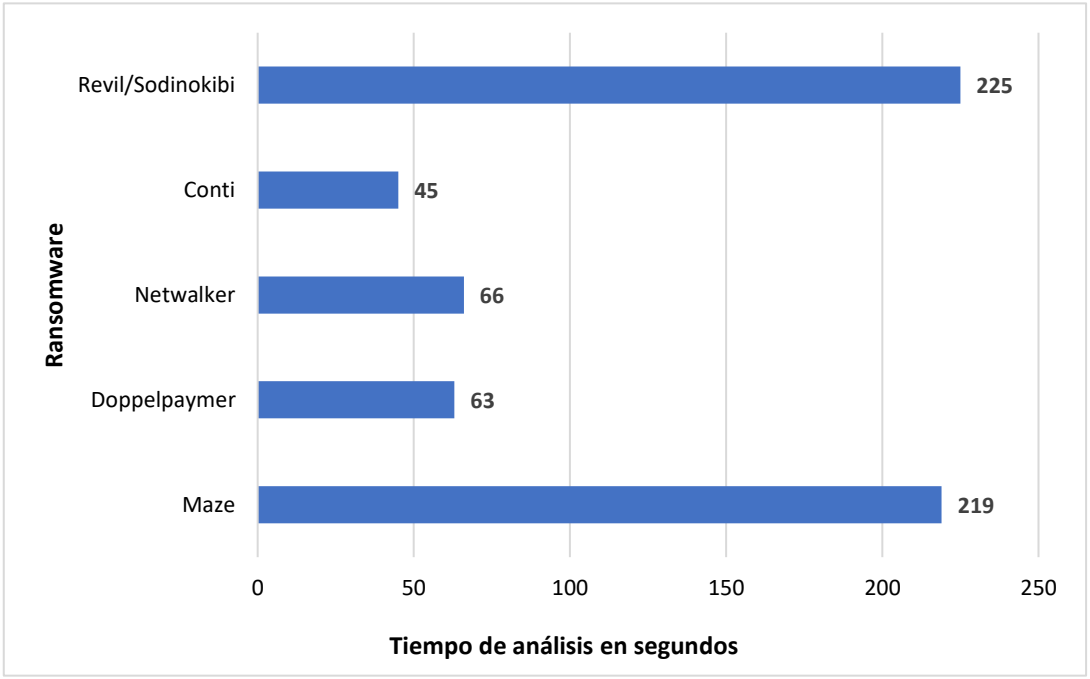


Figura 11. Tiempo de duración de análisis por Ransomware, expresado en segundos.

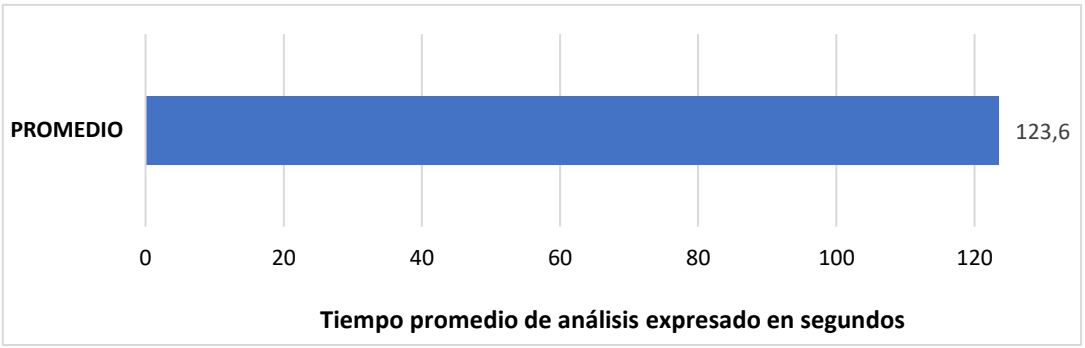


Figura 12. Tiempo promedio de análisis Ransomware expresado en segundos.

Como se puede observar en la figura N. 11 el tiempo promedio que utilizó cuckoo sandbox en el análisis de pruebas de laboratorio fue de 123.6 segundos, este resultado obtenido es óptimo porque se encuentra por debajo del tiempo de otras investigaciones realizadas.

El tercer indicador evalúa el **porcentaje de efectividad de Sandbox, frente a ataques sospechosos**, el cual se obtiene desarrollando la siguiente ecuación.

$$e = \frac{aa * 100}{n}$$

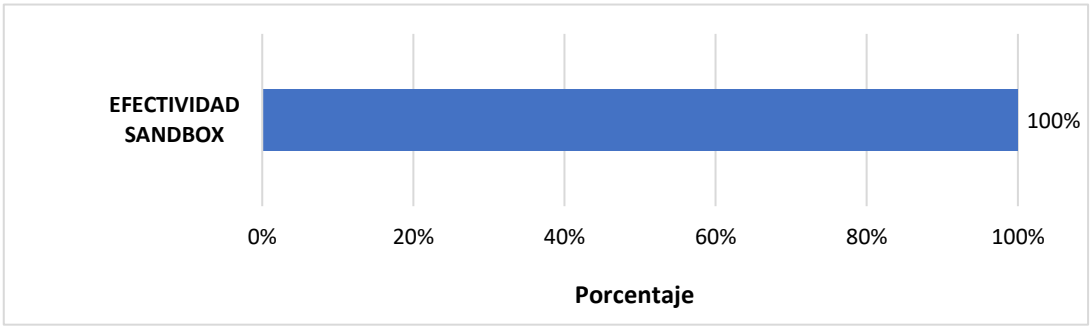


Figura 13. Porcentaje de efectividad de Sandbox.

Como se puede observar en la figura N. 12, el porcentaje de efectividad que obtuvo Cuckoo Sandbox en el análisis de pruebas de laboratorio fue del 100%, lo que significa que aisló a todos los ataques ejecutados, por ende demuestra su efectividad.

El cuarto indicador evalúa la **Respuesta a incidentes de ataques maliciosos notificados a tiempo por Sandbox**, el cual se obtiene desarrollando la siguiente ecuación.

$$e = \frac{int * 100}{ti}$$

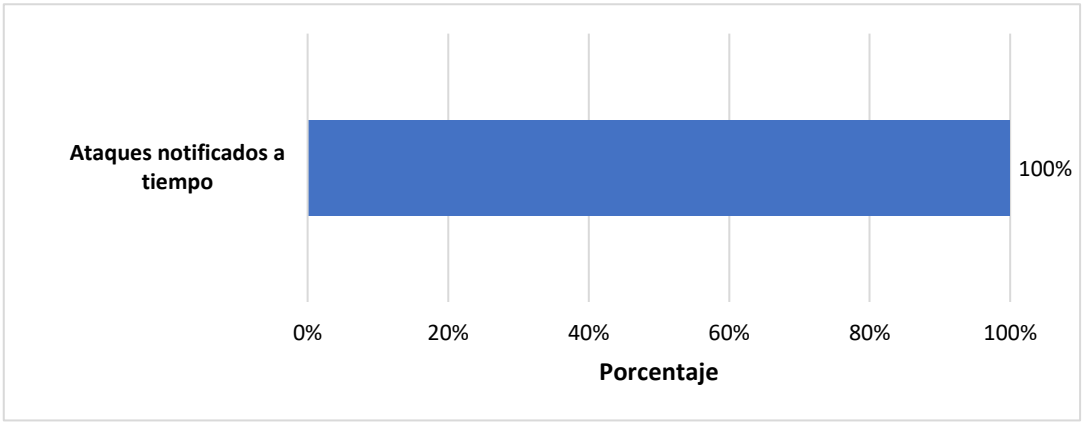


Figura 14. Porcentaje de ataques notificados a tiempo.

Como se puede observar en la figura N. 13, el porcentaje de ataques notificados a tiempo fue del 100%, esto se debe porque Cuckoo Sandbox aisló a los 5 Ransomware inyectados en el laboratorio de pruebas, lo que significa que los Ransomware filtrados en la red informática no llegaron a su destino, porque Cuckoo Sandbox los detectó a tiempo

El quinto indicador **evalúa la cobertura de hosts para detección y tratamiento de Ransomware**, el cual se obtiene desarrollando la siguiente ecuación.

$$chost = \frac{pr * 100}{thost}$$

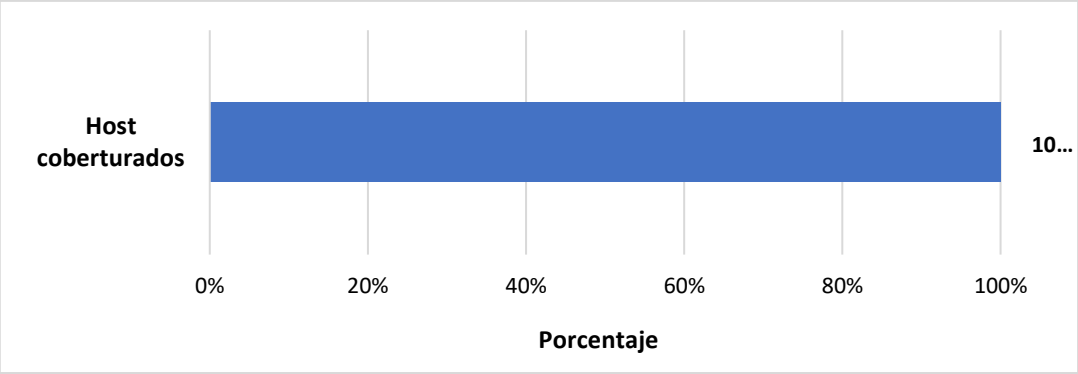


Figura 15. Hosts coberturados

Como se puede observar en la figura N. 15, de los 5 hosts virtualizados para el laboratorio de pruebas, el 100% han sido coberturados, esto demuestra que los hosts de la red están siendo analizados por Cuckoo Sandbox.

El sexto indicador evalúa la **cobertura de análisis de riesgos de los hosts**, el cual se obtiene desarrollando la siguiente ecuación.

$$car = \frac{ca * 100}{ta}$$

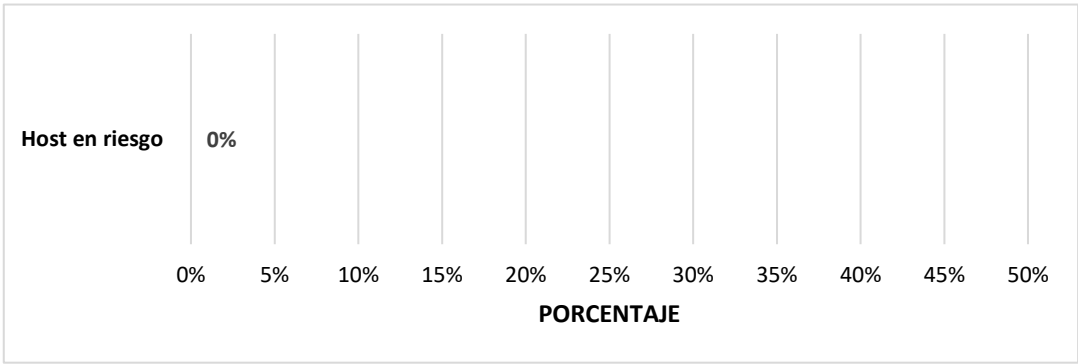


Figura 16. Análisis de Hosts en riesgo.

Como se puede observar en la figura N. 16, No hay host en riesgo porque todos fueron protegidos por sandbox en las pruebas de laboratorio.

3.2. Discusión de resultados.

La presente investigación se enfocó en el análisis de Ransomware de tipo Maze, Doppelpaymer, Netwalker, Conti y Revil/Sodinokibi, que fueron los que más daño ocasionaron al sector financiero, y que fueron analizados en el laboratorio de pruebas y aislados al 100% por Cuckoo Sandbox. En comparación a los resultados obtenidos por Buchyk et al, en su modelo analítico desarrollado, donde utilizó 32 tipos diferentes de malware en su prueba de laboratorio, obteniendo como resultado que el 91% de muestras fueron aisladas, demostrando la efectividad de Sandbox.

El tiempo promedio por Cuckoo Sandbox en esta investigación es de 123.6 segundos y el promedio de memoria RAM utilizada es de 0.89 gb, comparado con la investigación de Huthifh et al, denominada On Detection and Prevention of Zero-Day Attack Using Cuckoo Sandbox, donde obtuvo como resultado que de 361 malwares enviados al laboratorio de pruebas solo el 98% de las muestras fueron aisladas, y que el tiempo de análisis fue aproximadamente entre 132 a 152 segundos, demostrando que Cuckoo Sandbox es un entorno eficiente en el análisis de Ransomware en las dos investigaciones.

Así mismo, la investigación denominada A User-friendly Model for Ransomware Analysis Using Sandboxing, desarrollada por Kamal et al., obtuvieron como resultado que del 100% de ataques realizados con Ransomware a la red, el 92% fue aislado por Cuckoo Sandbox, el estudio no especifica la cantidad de Ransomware utilizados en relación a esta investigación que se analizó 5 Ransomware resultando el 100% aislados por Cuckoo Sandbox, lo que demuestra su efectividad.

3.3. Aporte práctico.

Para el análisis del estado actual de la seguridad informática del área local de la COOPAC Norandino LTDA. Se desarrolló como se muestra en la figura N. 16.

Figura 17. Procesos para analizar el estado de la red actual.

La red LAN de la COOPAC Norandino LTDA, está distribuido en un edificio de 3 pisos, cuenta con una topología tipo estrella, el que se grafica en la figura N. 17; la red principal se encuentra en el Datacenter ubicado en el piso 2, la misma que se conecta a todos los hosts como se detalla en la tabla N. 3.

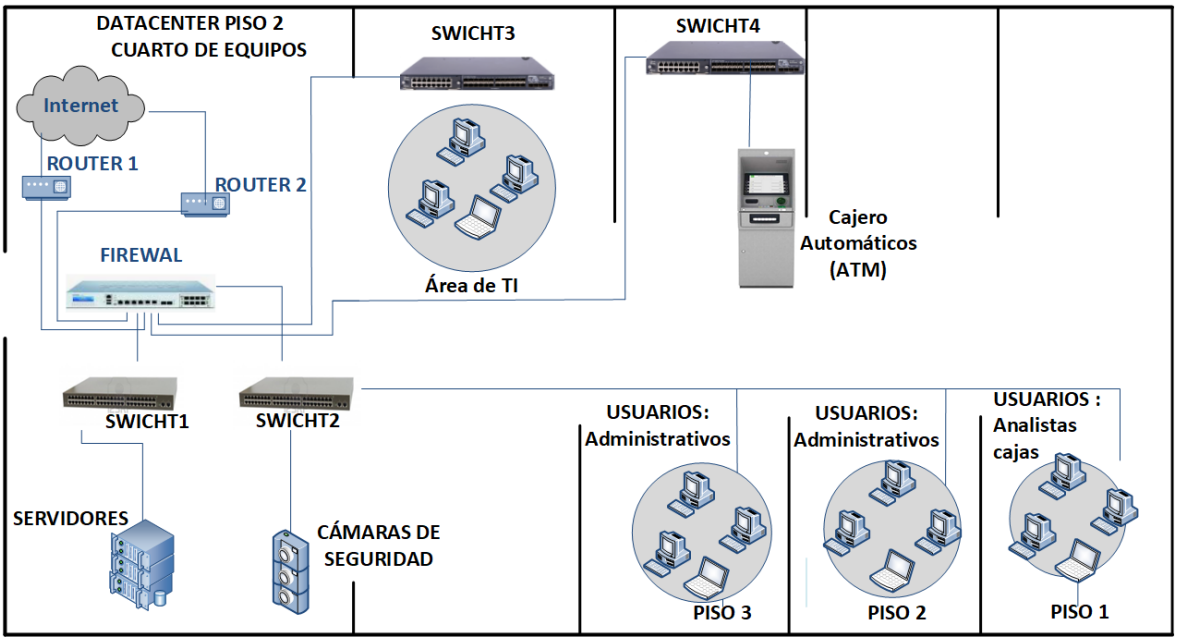


Figura 18. Esquema físico de Red LAN *Fuente*. COOPAC Norandino LTDA.

Tabla 3.
Hosts distribuidos en la Red LAN.

Cantidad	Host	Piso	Ubicación
6	Computadoras de escritorio	Piso 1, 2 y 3	
24	Laptops		
2	Acces point	Piso 2, 3	
3	Servidores	Piso 2	Datacenter
2	Routers (claro y global)	Piso 2	Datacenter

1	Circuito Cerrado de Televisión (CCTV)	Piso 2	Datacenter
1	Firewall perimetral	Piso 2	Datacenter
4	Switches	Piso 2	Datacenter
1	Automated Teller Machine (ATM)	Piso 1	

Fuente. COOPAC Norandino LTDA.

Los equipos de la red están conectados mediante cableado estructurado categoría 6 y cuenta con 2 líneas de internet (Claro y Global) de fibra óptica, llegando estas al dispositivo Sophos Xg-210 Firewall Perimetral UTM ubicado en el datacenter, desde donde se distribuye mediante reglas y políticas de tráfico a toda la red LAN, a través de los 4 switches existentes, como se muestra en la figura N. 18.

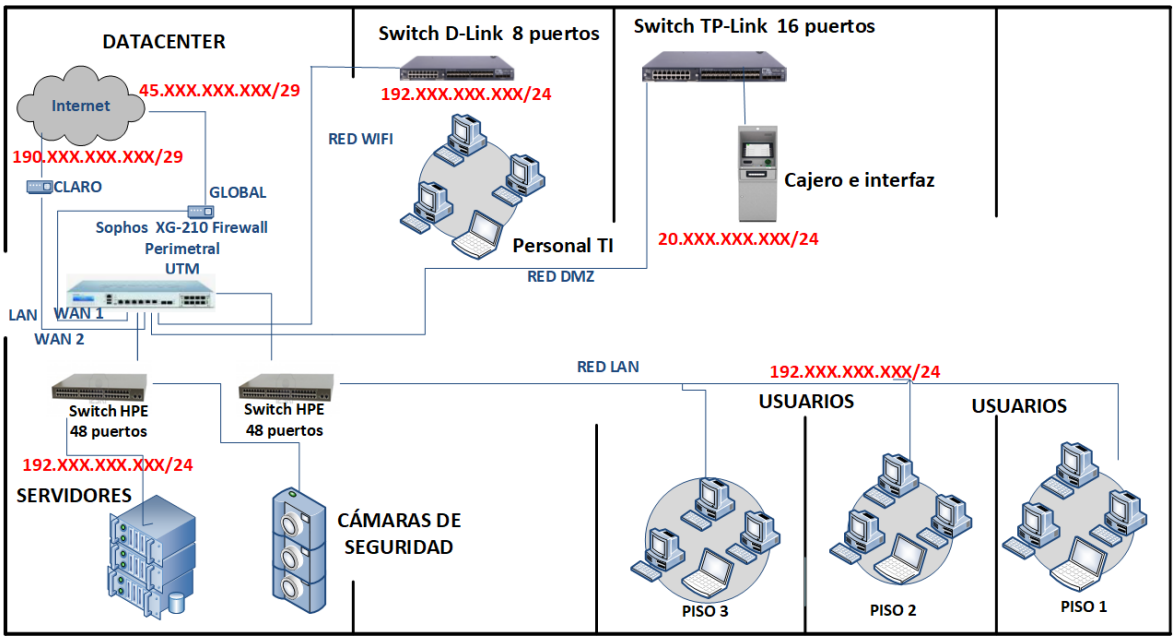


Figura 19. Esquema lógico de la red LAN. Fuente. COOPAC Norandino LTDA.

Previamente, al proceso de identificación de vulnerabilidades, la jefatura de TI de la COOPAC Norandino LTDA, brindó las facilidades y suministró uno de los servidores de su ambiente de pruebas, implementado con las herramientas de Kali Linux basado en Debian GNU/Linux, Masscan y Nmap, que fueron necesarias para el desarrollo de este proceso.

Para la identificación de vulnerabilidades se realizó el pentesting externo e interno con base a las Ips públicas y privadas de la COOPAC Norandino LTDA respectivamente, La finalidad fue la detección de puertos abiertos y servicios asociados, del dispositivo Sophos Xg-210 Firewall Perimetral UTM, en todas las ip listadas en la tabla N. 4, cabe resaltar que por políticas internas y de seguridad de la entidad, se muestran las ip mediante **"XXX",** y en las figuras se colocó un recuadro de color rojo para ocultar las Ip.

Tabla 4
Ips públicas y privadas de la COOPAC Norandino LTDA.

Tipo de ip	Ip Pública	Servicio
Públicas	45.XXX.XXX.XXX	Internet Global
	190.XXX.XXX.XXX	Internet Claro
	192.XXX.XXX.XXX	Servidores, firewall
Privadas	192.XXX.XXX.XXX	Usuarios TI
	192.XXX.XXX.XXX	Usuarios general
	20.XXX.XXX.XXX	Cajeros automáticos

Fuente. COOPAC Norandino LTDA.

Pentesting Externo

Para iniciar el pentesting externo se procedió de acuerdo a los siguientes pasos:

1. Se inició sesión en el servidor Kali Linux, como se muestra en la figura N. 19.

Figura 20. Inicio de sesión en Kali Linux.

2. Se procedió a abrir la consola de líneas de comando (CLI), con el objetivo de correr las herramientas Masscan y Nmap implementadas en Kali Linux, iniciando de esta forma el análisis de vulnerabilidades en la red, como se muestra en la figura N. 20.

Figura 21. Terminal Kali Linux.

3. Se utilizó la herramienta Masscan para el análisis de vulnerabilidades en las ip públicas.

   a. Se analizó el servicio de internet Global, como se muestra en la figura N. 21.

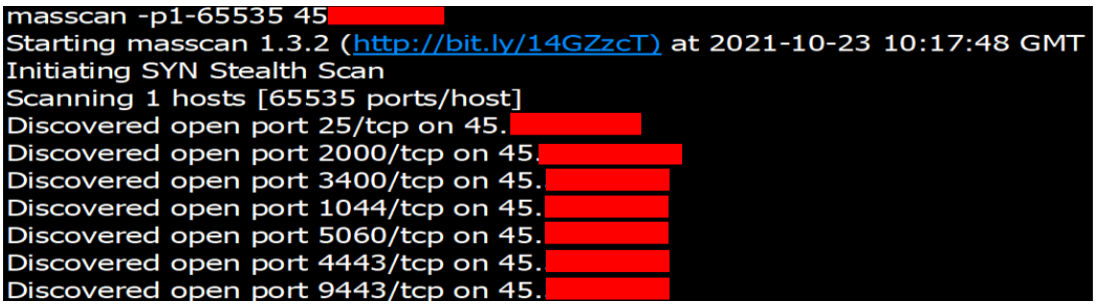


Figura 22. Escaneo de puertos al servicio internet Global.

Donde:

Masscan = herramienta utilizada.

-p1-65535 = desde el puerto 1, hasta el puerto 65535.
45.XXX.XXX.XXX = Ip pública.

Como resultado del análisis para la ip pública 45.XXX.XXX.XXX del servicio Internet Global, Se identificaron 7 puertos abiertos, que pueden ser vulnerados.

b. Se analizó el servicio de internet Claro, como se muestra en la figura N. 22.

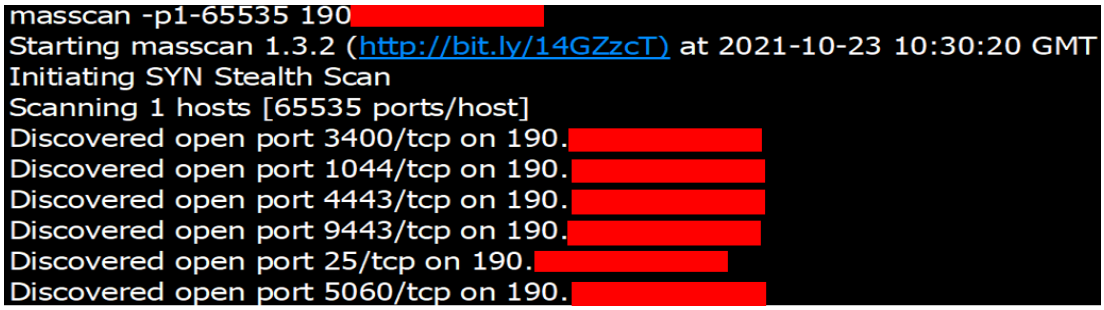


Figura 23. Escaneo de puertos al servicio internet Claro.

4. Se utilizó la herramienta Nmap para un segundo escaneo de puertos abiertos en las ip públicas.

a. La detección de vulnerabilidades en el servicio de internet Global fue como se muestra en la figura N. 23.

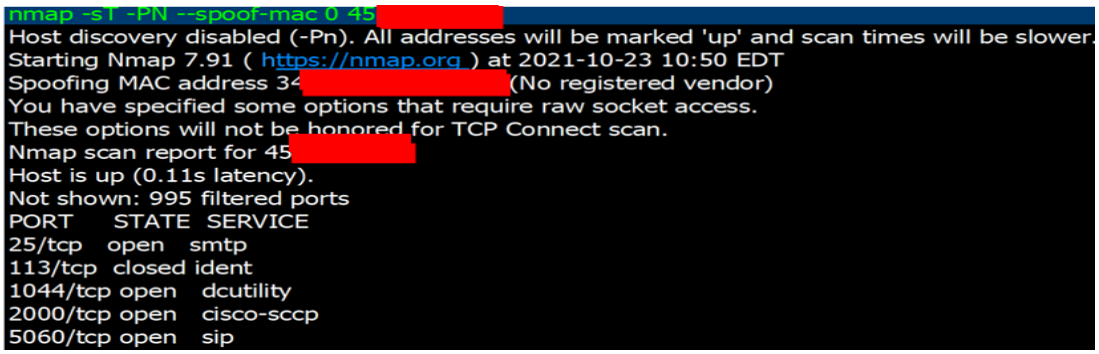


Figura 24. Escaneo de puertos al servicio internet Global.

b. La detección de vulnerabilidades en el servicio de internet Claro fue como se muestra en la figura N. 24.

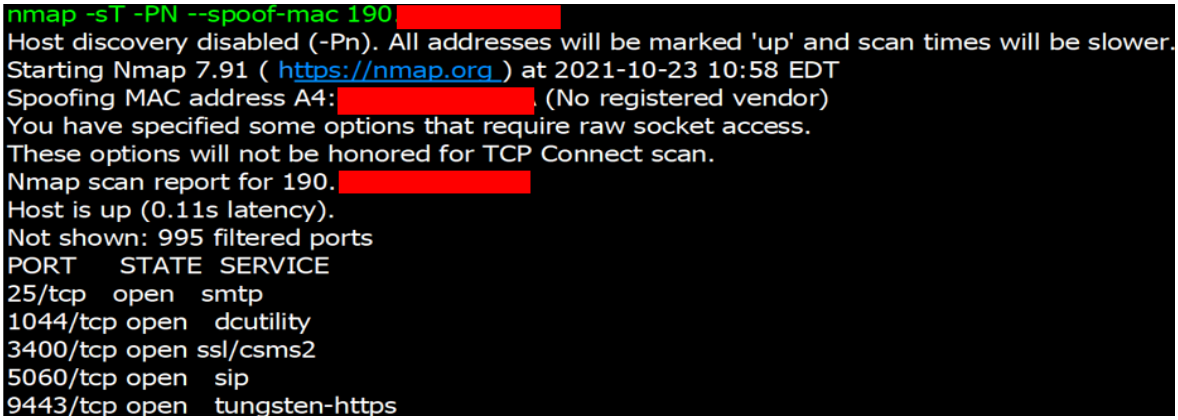


Figura 25. Escaneo de puertos al servicio internet Claro.

c. Se identificaron los servicios asociados de los puertos abiertos en el Sophos Xg-210 Firewall Perimetral UTM, se muestra el resumen de puertos abiertos con su respectivo servicio asociado. Como se muestra en la tabla N. 5

Tabla 5
Resumen de puertos abiertos y servicios asociados en la red externa.

Puertos	Servicios asociados	Descripción	Estado
25/tcp	filtered smtp	Servidor de correo electrónico	open
1044/tcp	Administración web Sophos	Acceso a sophos.	open
2000/tcp	cisco-sccp?	Acceso a escritorio remoto	open
3400/tcp	ssl/csms2?	Acceso a escritorio remoto	open
4443/tcp	sistema de mensajería.	sistema de mensajería.	open
5060/tcp	SIP	Acceso a escritorio remoto	open
9443/tcp	Portal de Usuarios Sophos	Acceso al portal de usuario sophos.	open

Fuente. Elaboración propia.

5. Se procedió a verificar los accesos a los puertos abiertos encontrados según consta en la tabla N. 5, como se detalla a continuación.

   a. Se valida el acceso al puerto abierto 1044, que sirve para loguearse al Sophos Xg-210 Firewall Perimetral UTM, como se muestra en la figura N. 25

Figura 26. Accediendo al puerto 1044.

b. Se validó el acceso al puerto abierto 9443, que sirve para loguearse al Sophos Xg-210 Firewall Perimetral UTM. Como se muestra en la figura N. 26.

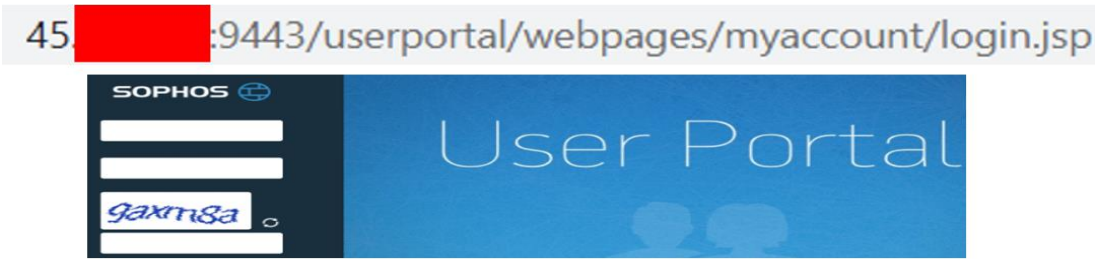


Figura 27. Accediendo al puerto 9443.

c. Se valida el acceso al puerto abierto 2000, que es una conexión remota. Según se muestra en la figura N. 27.

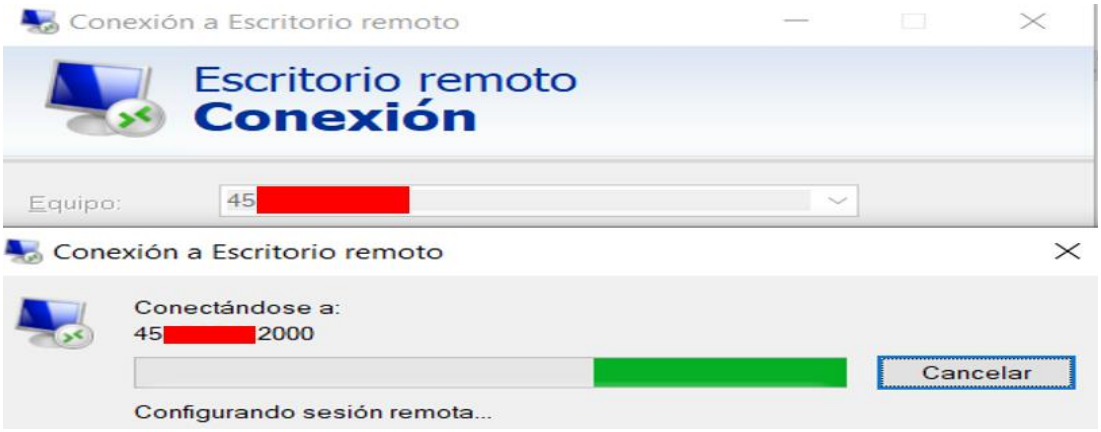


Figura 28. Accediendo al puerto 2000.

d. Se valida el acceso al puerto abierto 3400, que es para una conexión remota. Como se muestra en la figura N. 28.

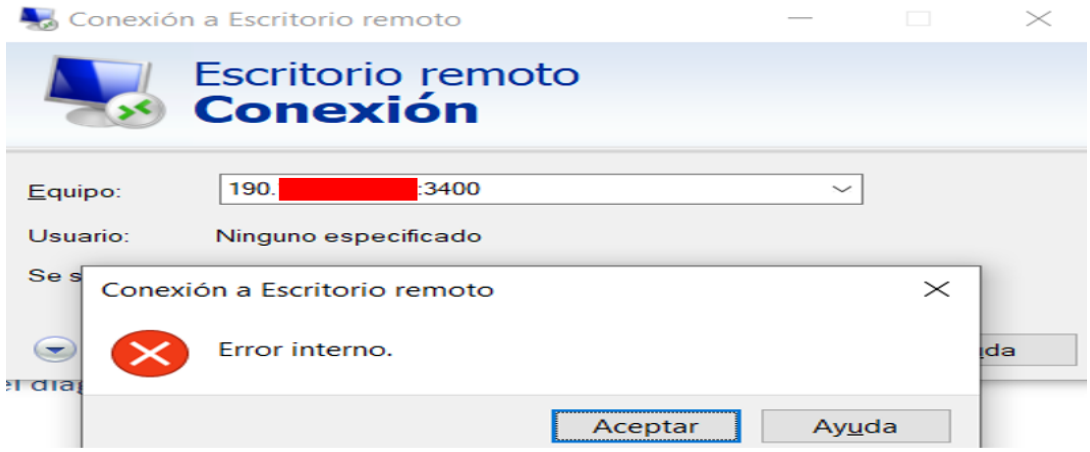


Figura 29. Accediendo al puerto 3400.

e. Se valida el acceso al puerto abierto 5060, que es para una conexión remota. Como se muestra en la figura N. 29.

Figura 30. Accediendo al puerto 5060

Pentesting interno

Se utilizó la herramienta Masscan para el análisis de vulnerabilidades en las ip privadas, mostrando como resultados los puertos abiertos existentes en la red, y que pueden ser blancos para posibles ataques informáticos, este análisis se desarrolló de acuerdo a los siguientes pasos:

a. Se identificaron 11 puertos abiertos asociados a la red de servidores de la COOPAC Norandino LTDA., como se muestra en la figura N.30.

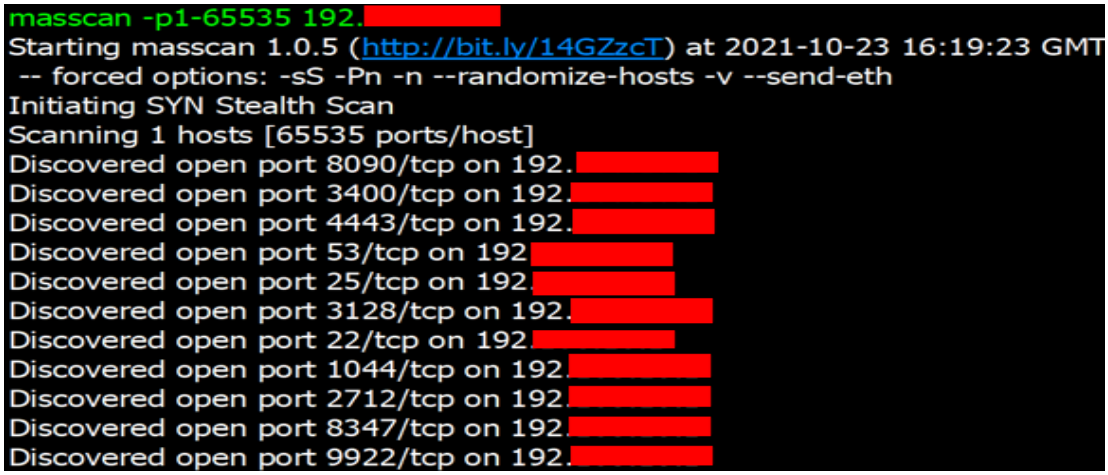


Figura 31. Escaneo de puertos a la red de servidores.

b. Se identificaron 10 puertos abiertos asociados a la red de usuarios TI de la COOPAC Norandino LTDA., como se muestra en la figura N. 31.

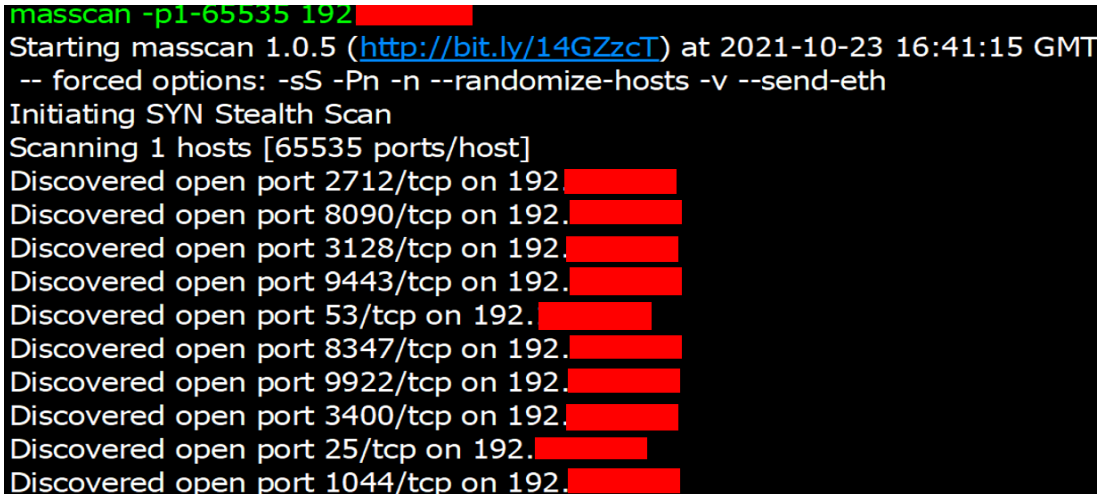


Figura 32. Escaneo de puertos a la red de usuarios TI.

c. Se identificaron 10 puertos abiertos asociados a la red de usuarios en general de la COOPAC Norandino LTDA., como se muestra en la figura N. 32.

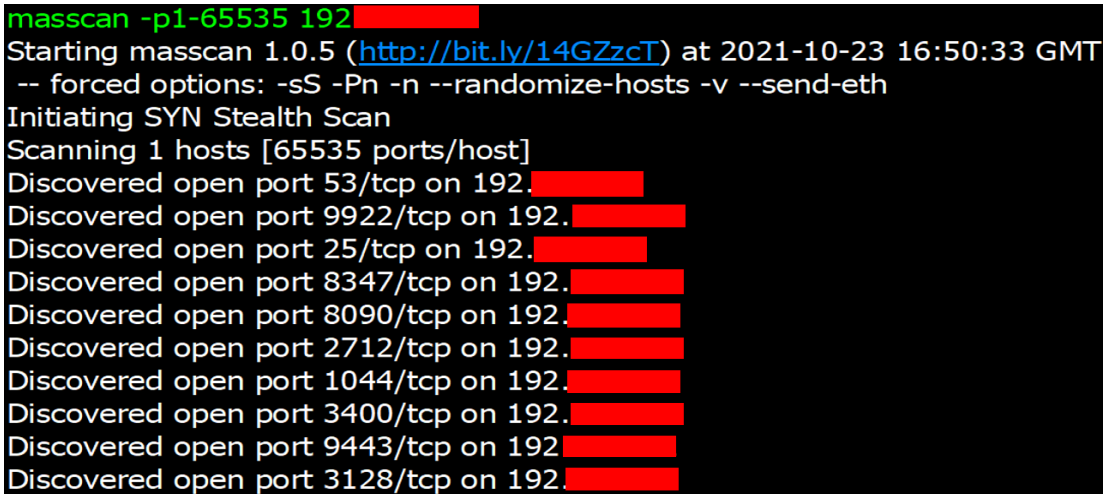


Figura 33. Escaneo de puertos a la red de usuarios en general.

d. Se identificaron 10 puertos abiertos asociados a la red de cajeros automáticos de la COOPAC Norandino LTDA., como se muestra en la figura N. 33.

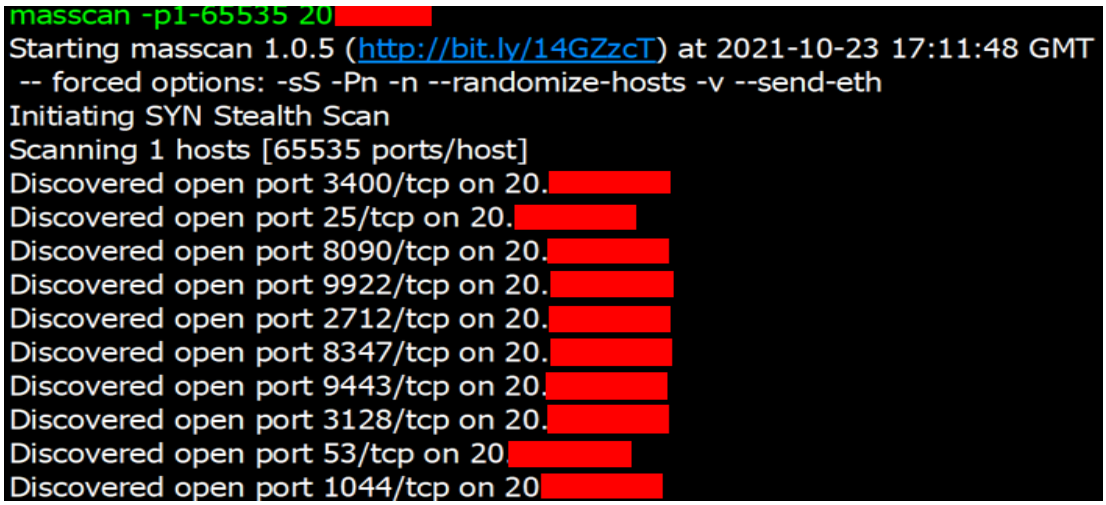


Figura 34. Escaneo de puertos a la red de cajeros automáticos.

e. Se identificaron 6 puertos abiertos asociados a la red de servidores de la COOPAC Norandino LTDA., como se muestra en la figura N. 34.

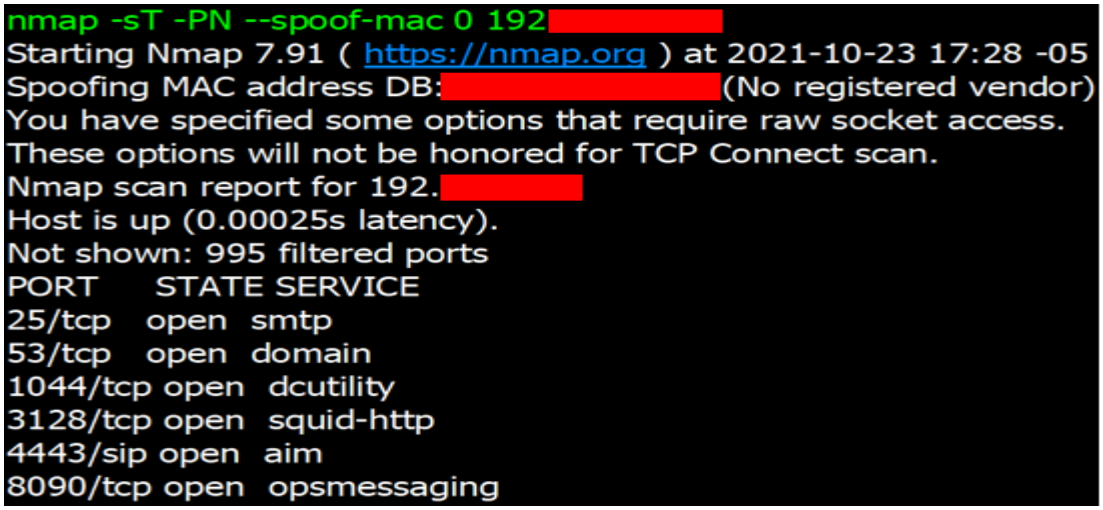


Figura 35. Escaneo de puertos a la red de servidores.

f. Se identificaron 5 puertos abiertos asociados a la red de usuarios TI, como se muestra en la figura N. 35.

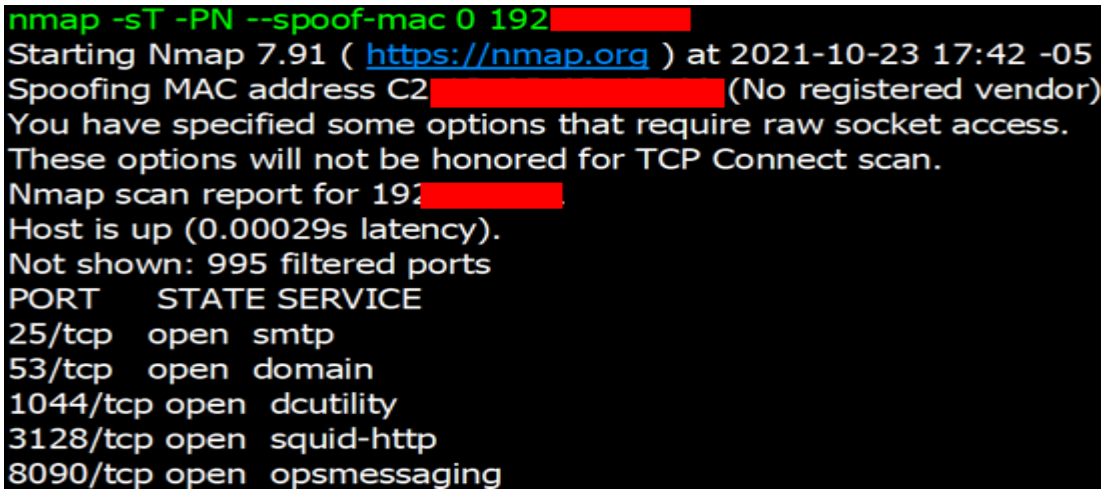


Figura 36. Escaneo de puertos a la red de usuarios TI.

g. Se identificaron 5 puertos abiertos asociados a la red de usuarios en general, como se muestra en la figura N. 36.

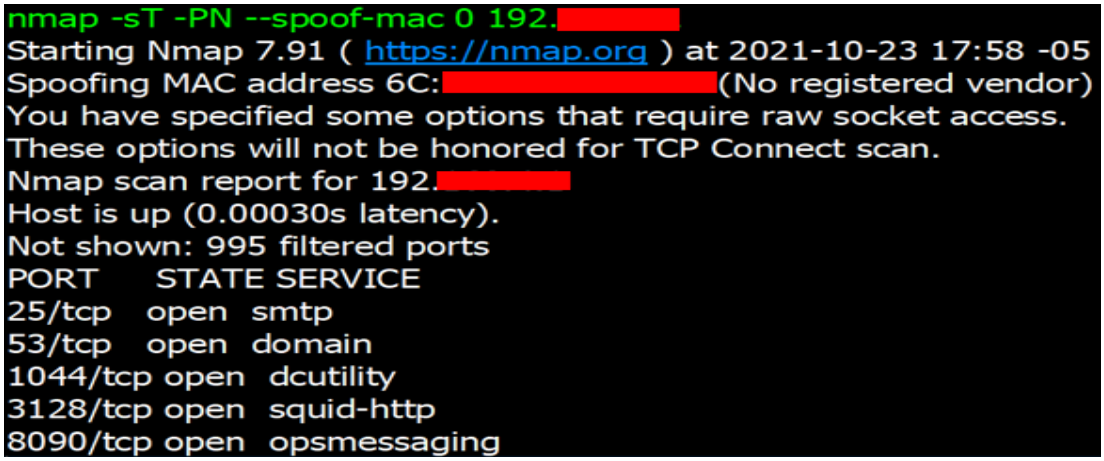


Figura 37. Escaneo de puertos a la red de usuarios en general.

h. Se identificaron 5 puertos abiertos asociados a la red de cajeros automáticos, como se muestra en la figura N. 37.

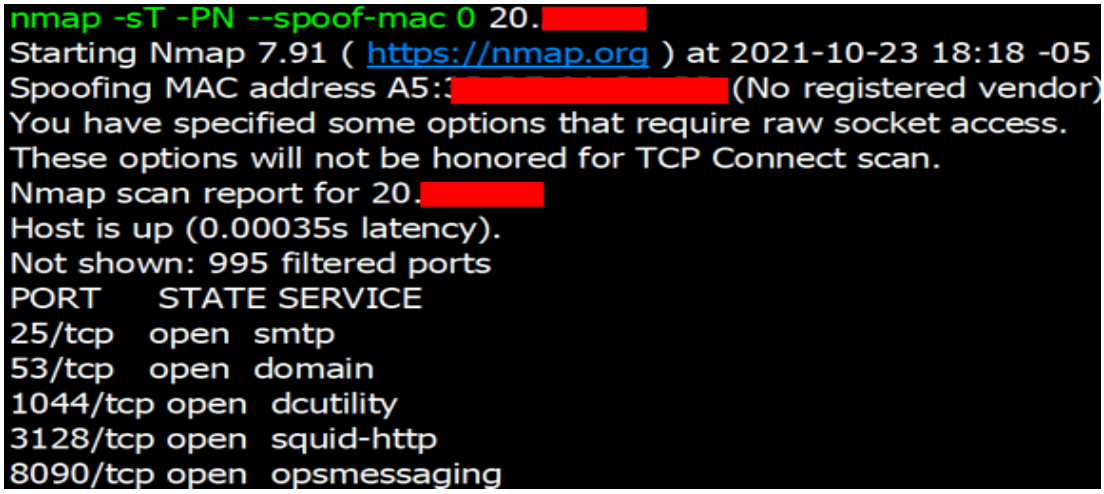


Figura 38. Escaneo de puertos a la red de cajeros automáticos.

Terminado el pentesting externo e interno, se elaboró el resumen de puertos internos abiertos y servicios asociados que las herramientas utilizadas encontraron, como se muestra en la tabla N. 6.

Tabla 6
Resumen de puertos abiertos y servicios asociados en la red interna.

Puertos	Servicios asociados	Descripción	Estado
25/tcp	filtered smtp	Servidor de correo electrónico	open
53/tcp	Administración web Sophos	Acceso a sophos.	open
1044/tcp	cisco-sccp?	Acceso a escritorio remoto	open
3128/tcp	ssl/csms2?	Acceso a escritorio remoto	open
4443/tcp	AIM	Mensajería	open
8090/tcp	Portal de Usuarios Sophos	Acceso al portal de usuario sophos.	Open
3400/tcp 22/tcp 2712/tcp 8347/tcp 9922/tcp	Otros	Otros	Open

Fuente. Elaboración propia.

Posteriormente, se elaboró una tabla conteniendo los puertos abiertos comunes y servicios asociados en las 2 redes (interna y externa), como se muestra en la tabla N.7. El puerto N. 25, es un puerto asociado al servidor de correo electrónico que no está habilitado porque la entidad no cuenta con ese servicio, pero que los responsables de la entidad han visto por conveniente parametrizar en el Sophos Xg-210 Firewall Perimetral UTM.; el puerto 1044, es un puerto utilizado para el acceso del Sophos Xg-210 Firewall Perimetral UTM.; el puerto 4443 es un puerto abierto que no está asociado a ningún servicio de la entidad, por lo que no está parametrizado en el Sophos Xg-210 Firewall Perimetral UTM., por lo que el acceso a ese puerto es libre.

Tabla 7
Resumen de puertos abiertos y servicios comunes de la red externa e interna.

Puertos	Servicios asociados	Descripción	Estado
25/tcp	filtered smtp	Servidor de correo electrónico	open
1044/tcp	Administración web Sophos	Acceso a sophos.	open
4443/tcp	Sistema de mensajería	Sistema de mensajería	open

Fuente. Elaboración propia.

El objetivo de la explotación de vulnerabilidades de la red de la COOPAC Norandino LTDA fue comprobar si el Sophos Xg-210 Firewall Perimetral UTM, permite la conexión reversa ante la descarga de un MALWARE dentro de la red LAN configurada con 5 host en un entorno virtual, para ello se tomó el puerto 4443, como se muestra en la figura N. 39.

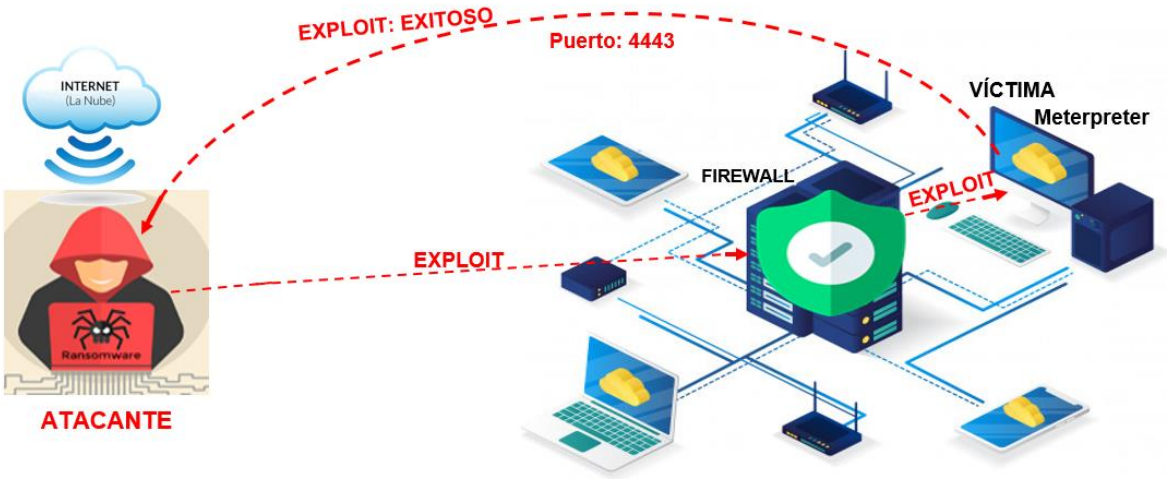


Figura 39. Ataque exploit. Fuente. Elaboración propia.

Para el desarrollo de esta tarea se utilizó Kali Linux como servidor, para la ejecución del ataque se creó un malware ejecutable para windows utilizando TheFatRat, como se detalla a continuación:

a. Se creó el archivo ejecutable (malware) denominado WindowsUpdate.exe, como se muestra en la figura N. 39.

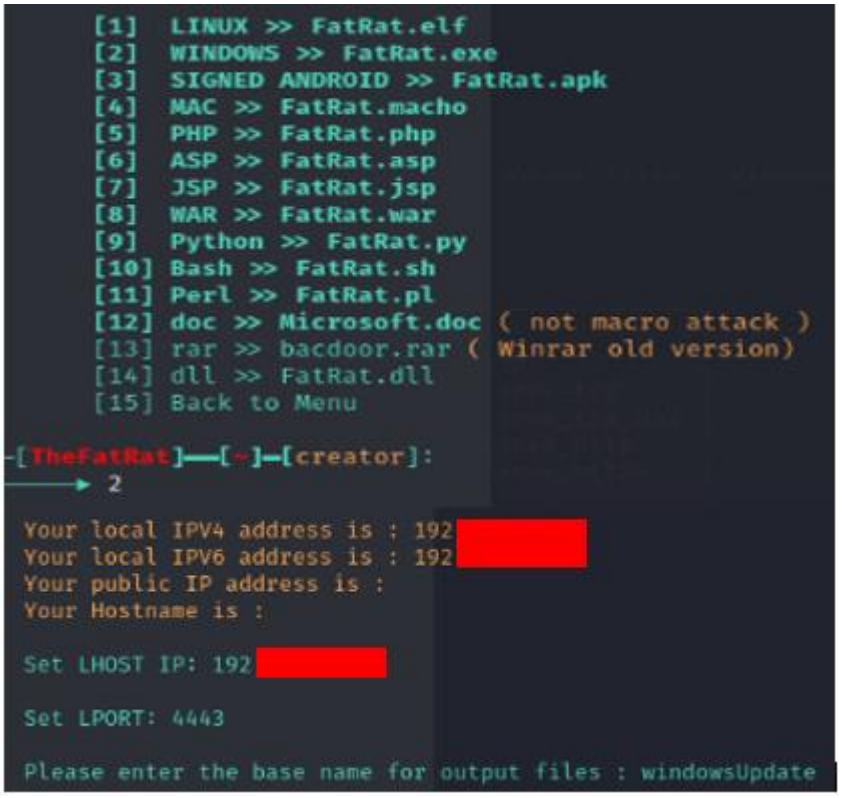


Figura 40. Creación de malware.

b. Se habilitó el puerto 4443 por donde será atacado y a la vez devuelto la alerta de ejecución de malware mediante el comando exploit, como se muestra en la imagen N. 40.

Figura 41. Víctima meterpreter. Fuente. Elaboración propia.

c. Se procede a acceder desde la víctima mediante la web al ip del servidor donde se observa el malware creado. Como se muestra en la figura N. 41.

Figura 42. Visualizando malware crear desde el cliente.

d. Al acceder desde el cliente, en el servidor se muestra la alerta detallando el ip desde donde se accedió, como se muestra en la figura N. 42.

Figura 43. Sesión iniciada en la víctima

La implementación del servidor con tecnología Sandbox, se realiza bajo los procesos indicados en la figura N. 43.

Figura 44. Procesos a ejecutar para la implementación de Sandbox.

1. Instalación del sistema operativo Ubuntu

El instalador de Ubuntu se descargó desde su página oficial **https://ubuntu.com/download/desktop,** la instalación se realizó en un equipo físico con las características descritas en la tabla N. 8.

Tabla 8.
Resumen de características para la instalación del Sistema Operativo Ubuntu con Cuckoo Sandbox.

	Características mínimas de servidor		**Características de equipo a implementar**	
	Descripción	**capacidad**	**Descripción**	**capacidad**
Hardware	Procesador	doble núcleo 2Gh.	Procesador	Core i3, 4 núcleos 3.6gh
	Memoria RAM	16Gb	Memoria RAM DDR4	16 Gb
	Disco duro	500 gb	Disco duro	1 Tb

Fuente. (Ubuntu, 2021).

Se procedió a la instalación de ubuntu como se muestra en la figura N. 44.

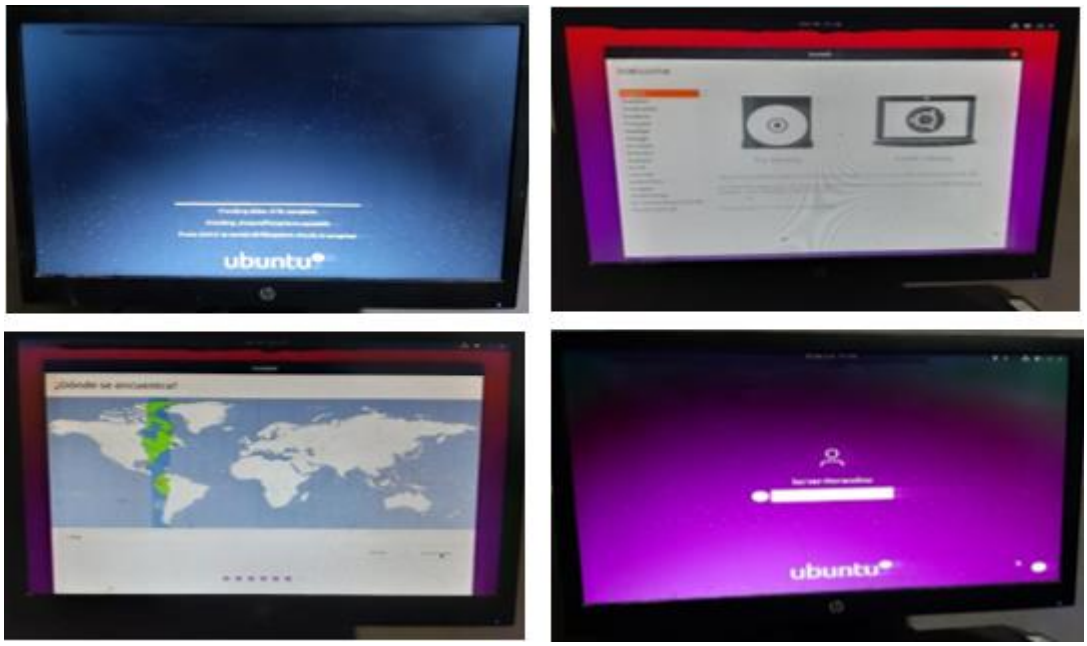


Figura 45. Instalación de sistema operativo ubuntu 20.04 LTS

Después de instalado el sistema operativo ubuntu, se procedió a aperturar la interfaz de líneas de comandos, para la actualización de paquetes del sistema, como se muestra en la figura N. 45.

```
sudo apt-get update && sudo apt-get upgrade -y
```

Figura 46. Actualización de paquetes del sistema operativo Ubuntu.

Los requisitos mínimos para la instalación de Cuckoo Sandbox que se encontró en su página oficial “https://Cuckoo.sh/docs/installation/host/index.html”. se detalla en la tabla N. 9.

Tabla 9
Requisitos para la instalación de Cuckoo Sandbox.

Requisitos	Finalidad
Instalación de bibliotecas de Python	Necesarios para la funcionalidad de Cuckoo Sandbox.
Instalación de bibliotecas de Python en windows	Necesarios para la funcionalidad de Cuckoo Sandbox en windows.
Software de virtualización	Implementación de laboratorio de pruebas virtualizado.
Instalación de tcpdump	Analiza el tráfico que circula por la red.
Instalación de volatility	para realizar análisis en volcados de memoria.
Instalación de M2Crypto	kit de herramientas de cifrado y SSL de Python

Fuente. (Foundation, 2019).

2. Instalación de Cuckoo Sandbox.

La instalación de Cuckoo Sandbox se realizó con la finalidad de obtener un ambiente aislado para mitigar ataques Ransomware en la red de la COOPAC Norandino LTDA., por lo que se procedió a su implementación mediante líneas de comando utilizando el terminal del SO Ubuntu V. 20.04 para la instalación de librerías Python, instalación del software de virtualización VirtualBox, configuración de Cuckoo Sandbox, instalado anteriormente, como se muestra en la figura N. 41, para ello se realizó una serie de pasos descritos literalmente a continuación.

a. Se procedió a crear un usuario denominado Cuckoo, dedicado para la configuración de Sandbox, y se agregó al grupo sudo, como se muestra en la figura N. 46.

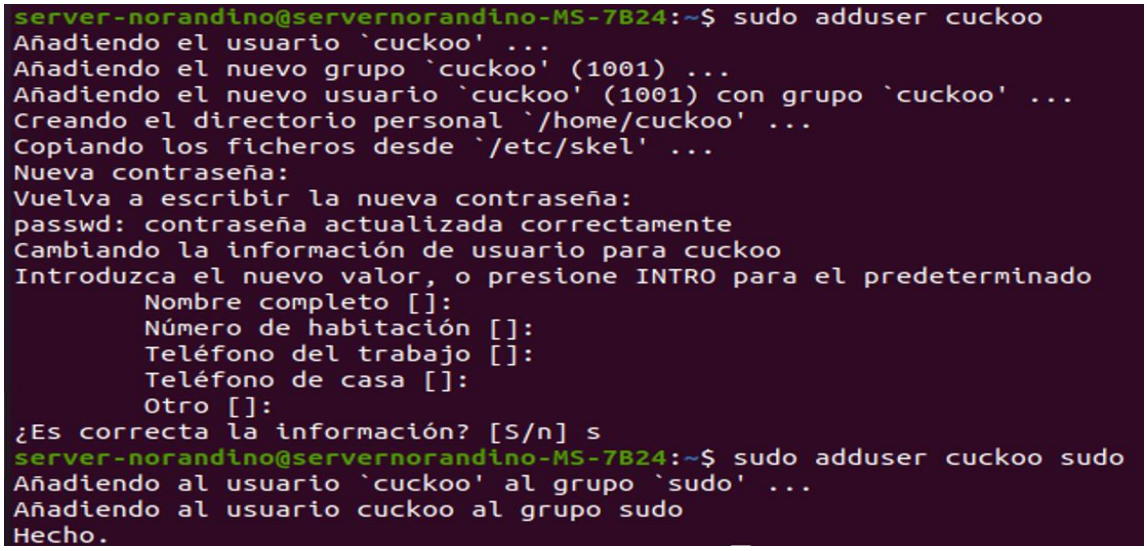


Figura 47. Creación de usuario dedicado para Sandbox.

b. Instalación del complemento CURL de ubuntu, para la verificación de conectividad a las URL y la verificación de la transferencia de datos, dicha instalación se ejecutó como se muestra en la figura N. 47.

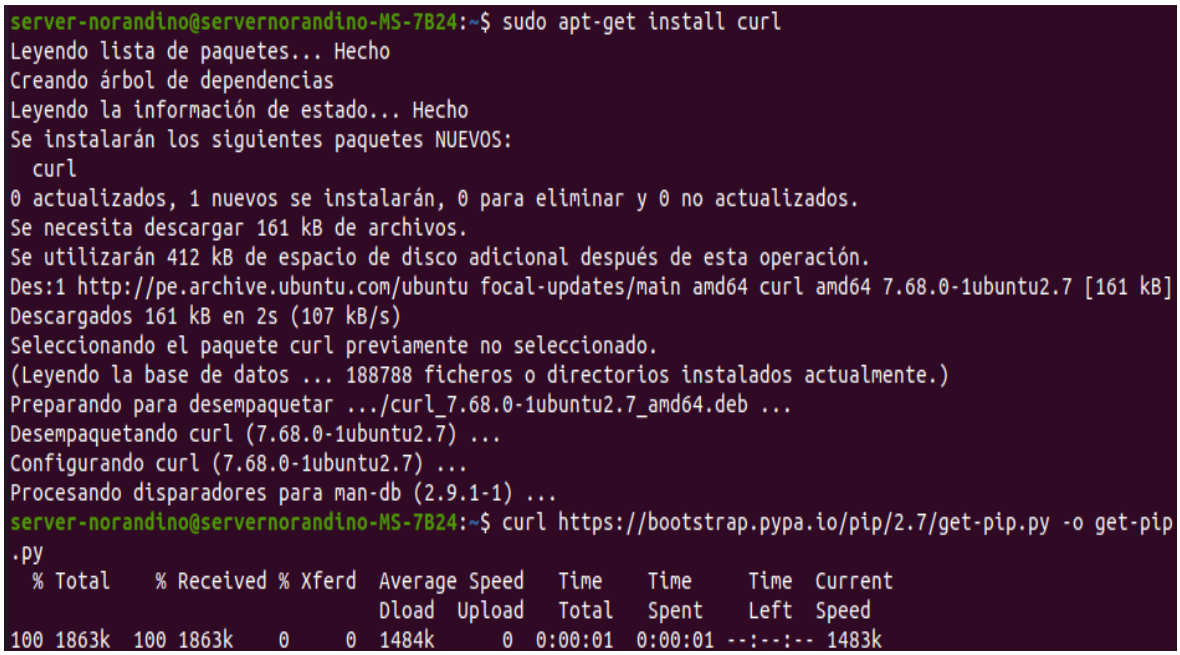


Figura 48. Instalación de complemento CURL.

c. Instalación de python 2.7, para el correcto funcionamiento de Cuckoo Sandbox. como se muestra en la figura N. 48.

```
sudo apt-get install python
sudo python get-pip.py
sudo apt-get install -y python-dev libffi-dev libssl-dev libfuzzy-
dev libtool flex autoconf libjansson-dev git
sudo apt-get install -y python-setuptools
```

Figura 49. Instalación Python

d. Instalación de la librería jpeg, para la lectura y escritura de archivos de imagen. como se muestra en la figura N. 94.

```
sudo apt-get install -y libjpeg-dev zlib1g-dev swig
```

Figura 50. Instalación de librerías jpeg.

e. Instalación de mongodb, para utilizar la interfaz web basada en Django. como se muestra en la figura N. 50.

```
sudo apt-get install -y mongodb
```

Figura 51. Instalación mongodb.

f. Instalación de base de datos postgreSQL, como se muestra en la figura N. 51.

```
sudo apt-get install -y postgresql libpq-dev
```

Figura 52. Instalación base de datos

g. Instalación de virtualBox para la virtualización de la red, como se muestra en la figura N. 52.

```
sudo apt-get install -y virtualbox
```

Figura 53. Instalación virtualbox

h. Clonación de Cuckoo desde github, como se muestra en la figura N. 53.

```
git clone https://github.com/volatilityfoundation/volatility.git
```

Figura 54. Clonación de Cuckoo

i. Instalación de complementos en volatility, como se muestra en la figura N. 54.

```
cd volatility
sudo python setup.py build
sudo python setup.py install
```

Figura 55. Instalación complementos volatility

j. Instalación de Distorm, como se muestra en la figura N. 55.

```
sudo -H pip install distorm3==3.4.4
```

Figura 56. Instalación Distorm.

k. Instalación Yara, como se muestra en la figura N. 56.

```
sudo -H pip install yara-python==3.6.3
```

Figura 57. Instalación Yara.

l. Instalación ssdeep, como se muestra en la figura N. 57.

```
sudo apt-get install -y ssdeep
```

Figura 58. Instalación ssdeep.

m. Instalación pydeep, como se muestra en la figura N. 58.

```
sudo -H pip install pydeep
```

Figura 59. Instalación pydeep

n. Instalación pydeep, como se muestra en la figura N. 59.

```
sudo -H pip install openpyxl
```

Figura 60. Instalación openpyxl

o. Instalación ujson, como se muestra en la figura N. 60.

```
sudo -H pip install ujson
```

Figura 61. Instalación ujson.

p. Instalación ujson, como se muestra en la figura N. 61.

```
sudo -H pip install jupyter
```

Figura 62. Instalación jupyter.

q. Instalación de tcpdump, para el análisis de las conexiones que realiza el host infectado con el malware, como se muestra en la figura N. 62.

```
sudo apt-get install tcpdump
sudo apt-get install libcap2-bin
sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
getcap /usr/sbin/tcpdump
sudo apt-get install -y apparmor-utils
sudo aa-disable /usr/sbin/tcpdump
```

Figura 63. Instalación tcpdump

r. Instalación de setuptools, como se muestra en la figura N. 63.

```
pip install -U pip setuptools
```

Figura 64. Instalación setuptools

s. Instalación Cuckoo, como se muestra en la figura N. 64.

```
sudo -H pip install -U cuckoo
cuckoo
                          __
  .----..--.--..-----.|  |--..------..-----.
  |  __||  |  ||  __||     <|  _  ||  _  |
  |____||_____||____||__|__||_____||_____|

Cuckoo Sandbox 2.0.7
```

Figura 65. Instalación Cuckoo

3. Configuración de Cuckoo Sandbox

a. Creación de host virtualizado para la conectividad entre Cuckoo Sandbox y máquinas clientes, como se muestra en la figura N. 65.

```
vboxmanage hostonlyif create
```

Figura 66. Comando para la configuración de Cuckoo Sandbox

b. Configuración del host creado asignándole un ip, como se muestra en la figura N. 66.

```
vboxmanage hostonlyif ipconfig vboxnet0 --ip 192
```

Figura 67. Asignación de Ip a host creado.

c. Validación de la existencia del host creado, como se muestra en la figura N. 67.

```
vboxnet0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192          netmask 255.          broadcast 192
        ether 0a:00:27:00:00:00  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figura 68. Validación de host creado y configurado.

d. Configuración de archivos para el correcto funcionamiento de Cuckoo Sandbox, como se muestra en la figura N. 68.

```
~$ cd ~/.cuckoo/conf
~/.cuckoo/conf$ sudo nano cuckoo.conf
~/.cuckoo/conf$ sudo nano auxiliary.conf
~/.cuckoo/conf$ sudo nano auxiliary.conf
~/.cuckoo/conf$ sudo nano virtualbox.conf
~/.cuckoo/conf$ sudo nano processing.conf
~/.cuckoo/conf$ sudo nano memory.conf
~/.cuckoo/conf$ sudo nano reporting.conf
```

Figura 69. Configuración de archivos Cuckoo

e. Se valida que Cuckoo Sandbox inicia correctamente y se pone a la escucha de los clientes, como se muestra en la figura N. 69.

```
srv-norandino@srvnorandino-MS-7B24:~$ cuckoo web runserver 0.0.0.0:8000
Performing system checks...

System check identified no issues (0 silenced).
October 31, 2021 - 23:50:05
Django version 1.8.4, using settings 'cuckoo.web.web.settings'
Starting development server at http://0.0.0.0:8000/
Quit the server with CONTROL-C.
```

Figura 70. Inicio de Cuckoo Sandbox

Para las pruebas de laboratorio se procedió de acuerdo a las tareas, que se muestran en la figura N. 70.

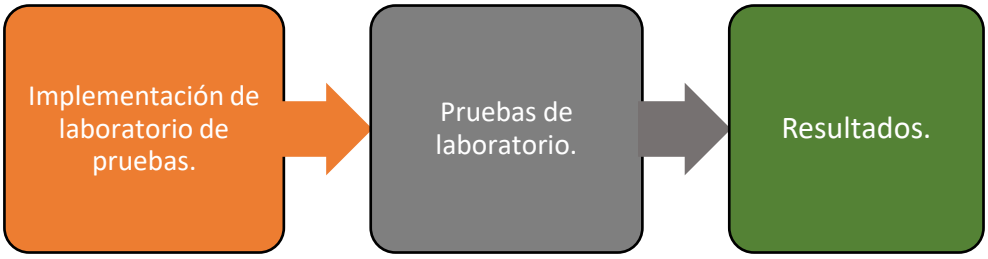


Figura 71. Procedimientos para alcanzar el objetivo 4.

Se implementó la red para las pruebas de laboratorio de forma virtualizada con la herramienta VirtualBox Como se muestra en la figura N. 71, no se realizó en la red física de la COOPAC Norandino para no comprometer la data y configuración de su infraestructura; para ello se instaló 5 computadoras virtuales, que representan el 50% de host (computadoras de escritorio y laptop) con el objetivo de ejecutar un

Ransomware en cada computadora virtual, se configuró la conectividad entre Cuckoo Sandbox y los clientes virtualizados; se descargaron los Ransomware y se ejecutaron desde los clientes para determinar la eficiencia de Cuckoo Sandbox.

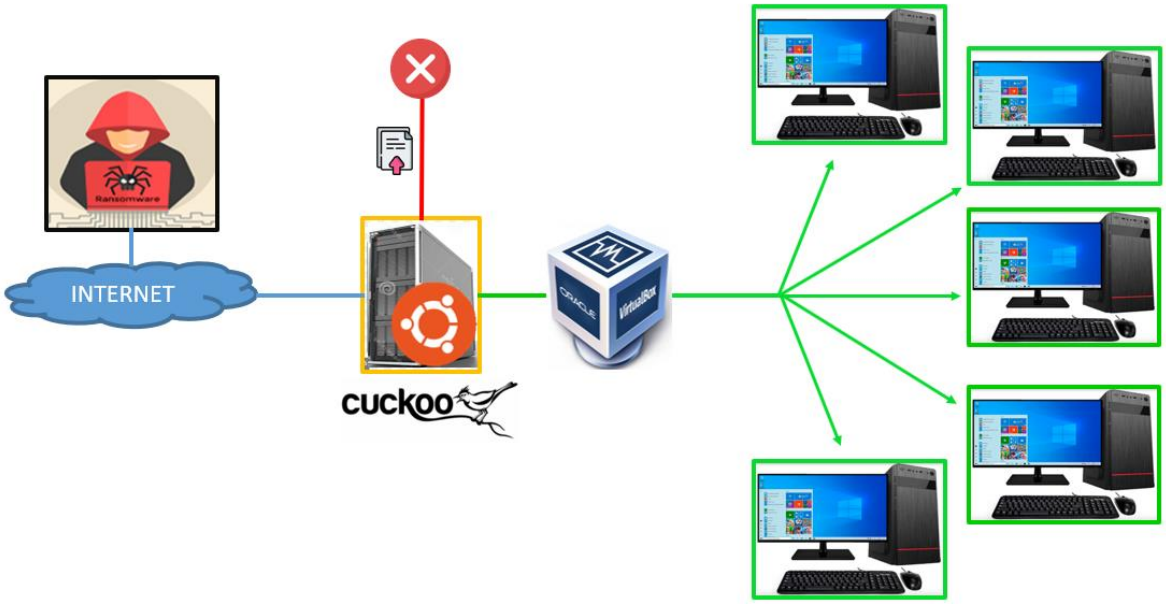


Figura 72. Ambiente aislado virtualizado para laboratorio de pruebas.
Fuente. Elaboración propia.

Implementación de laboratorio de pruebas.

a. Se instalaron las 5 máquinas virtuales con windows 10 mediante virtualbox, en la configuración de red de la máquina virtual se configuró el tipo de adaptador de red, visualizando la red virtual creada en la instalación de Cuckoo Sandbox, el cual se conectó como adaptador-sólo anfitrión, para que haya comunicación entre el servidor y los clientes, como se muestra en la figura N. 72.

Figura 73. Configuración de red en PC virtual.

b. Se añadió en las computadoras cliente la carpeta denominada SHARED que contiene los archivos necesarios para la comunicación entre el servidor y el cliente, con la finalidad de compartir información, como se muestra en la figura N. 73.

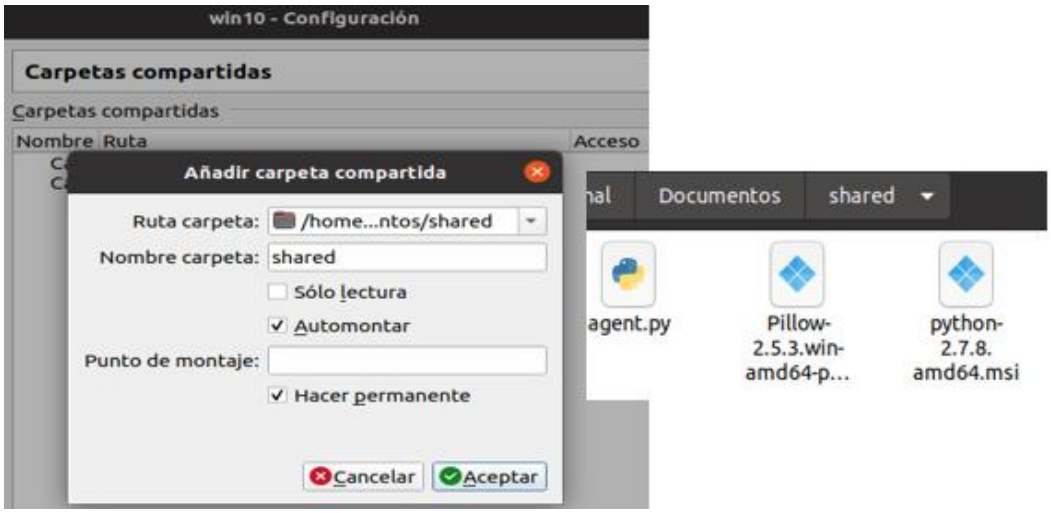


Figura 74. Carpeta compartida entre servidor y cliente.

c. Posteriormente se procedió abrir la guest para que haya mejor rendimiento entre el servidor y el cliente, tanto la Shared y el VirtualBox Guest Addition y se visualizaron en el explorador de windows como se visualiza en la figura N. 74.

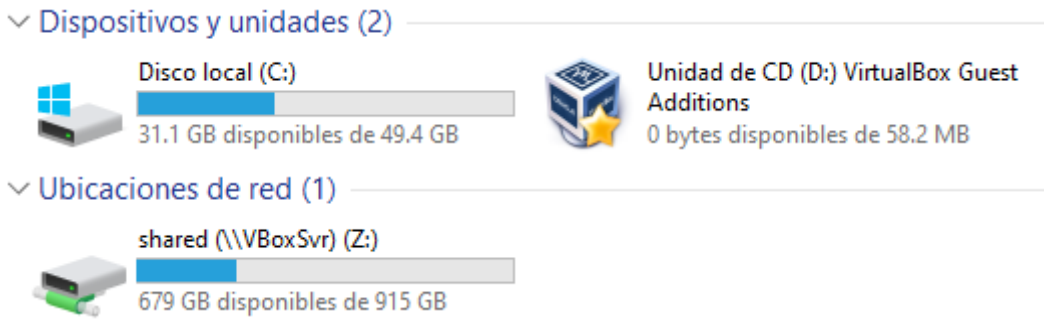


Figura 75. Visualización de Shared y la Guest en el explorador de Windows.

d. Se procedió a instalar el VirtualBox Guest Addition en el cliente como se muestra en la figura N. 75.

Figura 76. Instalación de VirtualBox Guest Addition en Windows.

e. Se realizó la instalación de python en el cliente, como se muestra en la figura N. 76.

Figura 77. Instalación de Python

f. Se configuró la dirección IP, puerta de enlace y DNS en Windows, para conectividad como se muestra en la figura N. 77.

Figura 78. Configuración de IP para conectividad.

Para las pruebas de laboratorio se descargaron Ransomware como se muestra en la tabla N. 10.

Tabla 10.
Descarga de Ransomware.

Ransomware	Link de descarga	Nombre de archivo
Maze	https://www.tutorialjinni.com/maze-Ransomware-sample-download.html	067f1b8f1e0b2bfe286f5169e17834e8cf7f4266b8d97f28ea78995dc81b0e7b.zip

Doppelpaymer	https://www.tutorialjinni.com/doppelpaymer-Ransomware-sample-download.html/	801b04a1504f167c25f568f8d7cbac13bdde6440a609d0dcd64ebe225c197f9b.py
Netwalker	https://www.tutorialjinni.com/netwalker-Ransomware-sample-download.html/	416556c9f085ae56e13f32d7c8c99f03efc6974b2897070f46ef5f9736443e8e.py
Conti	https://www.tutorialjinni.com/download-Conti-Ransomware-sample/	ebeca2df24a55c629cf0ce0d4b703ed632819d8ac101b1b930ec666760036124.py
Revil/Sodinokibi	https://www.tutorialjinni.com/download-Revil.sodinokibi-Ransomware-sample/	52612bceee07152f2e2e6699b3c085149e11979f34fe248bda14e03a0d950e85.py

Fuente (Jinni, 2020).

a. Se ejecutaron los Ransomware en el laboratorio de pruebas virtualizado y Cuckoo Sandbox procedió con el respectivo análisis a continuación se muestra el análisis para cada Ransomware:

✓ Se analizó el Ransomware Maze, como se muestra en la figura N. 78.

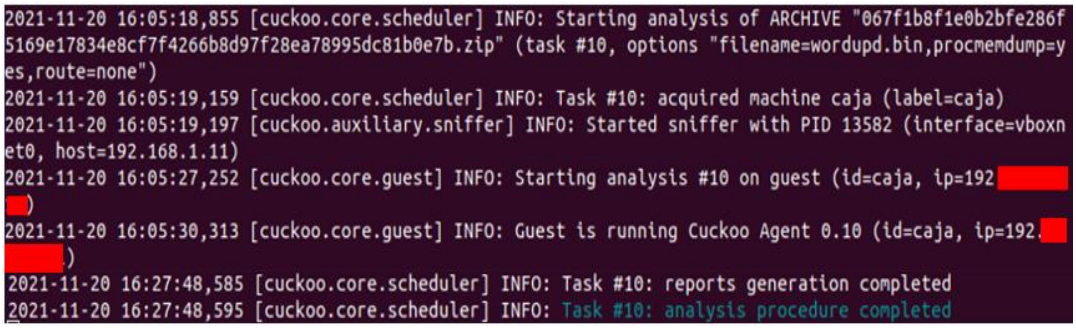


Figura 79. Análisis de Ransomware Maze.

Información obtenida

a. La información que se logra obtener después de analizado un Ransomware en Cuckoo Sandbox es mediante un reporte html, Como se muestra en la figura N. 79.

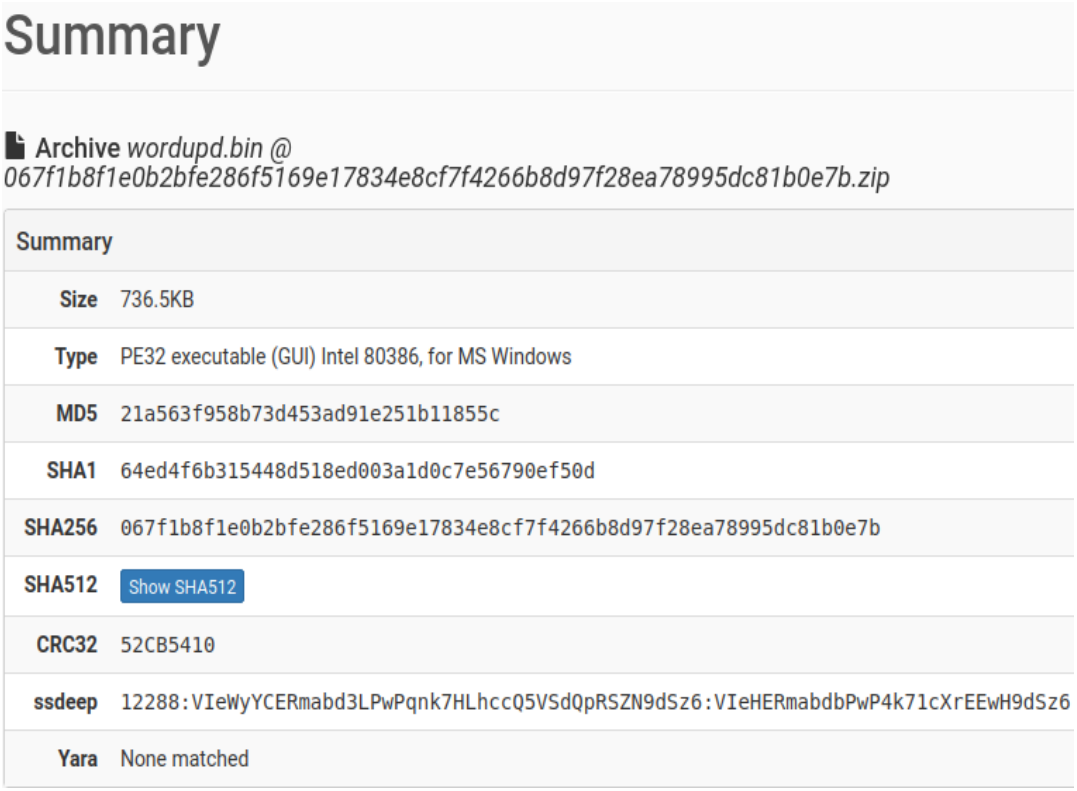


Figura 80. *Reporte de análisis Ransomware*

Dicho reporte html contiene el peso de archivo, tipo de archivo, CRC32 (función para detectar errores), algoritmo hash (MD5, SHA1, SHA256 y SHA512) identificando de forma única cada muestra, y algoritmo Ssdeep (para comparar tipos de archivos), entre otros para constatar la precisión de los datos.

b. Brinda una puntuación sobre 10, denominado score, el que permite verificar que tan malicioso es el archivo analizado, como se muestra en la figura N. 80.

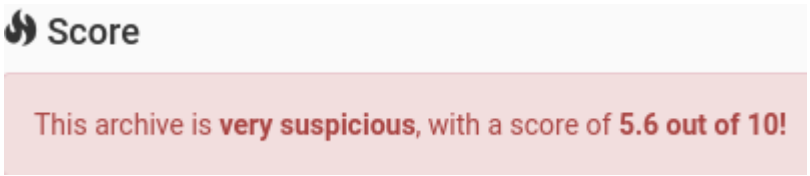


Figura 81.Score

c. Muestra información acerca del tiempo de duración del análisis, la categoría del Ransomware, fecha y hora de inicio y término y la duración total en segundos y otros, como se muestra en la figura N. 81.

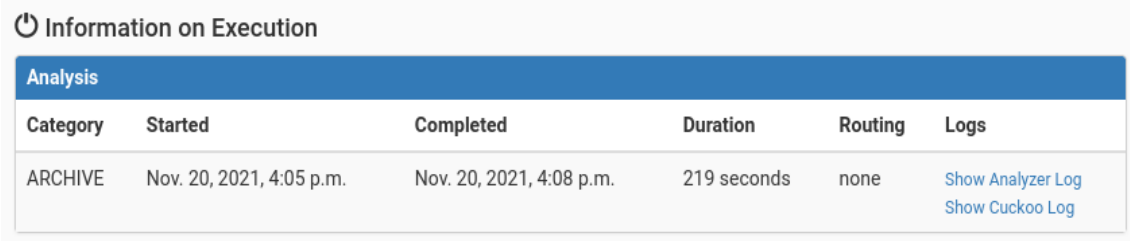


Figura 82. Información del tiempo de análisis.

d. Contiene el detalle de firmas del análisis del Ransomware, como se muestra en la figura N. 82.

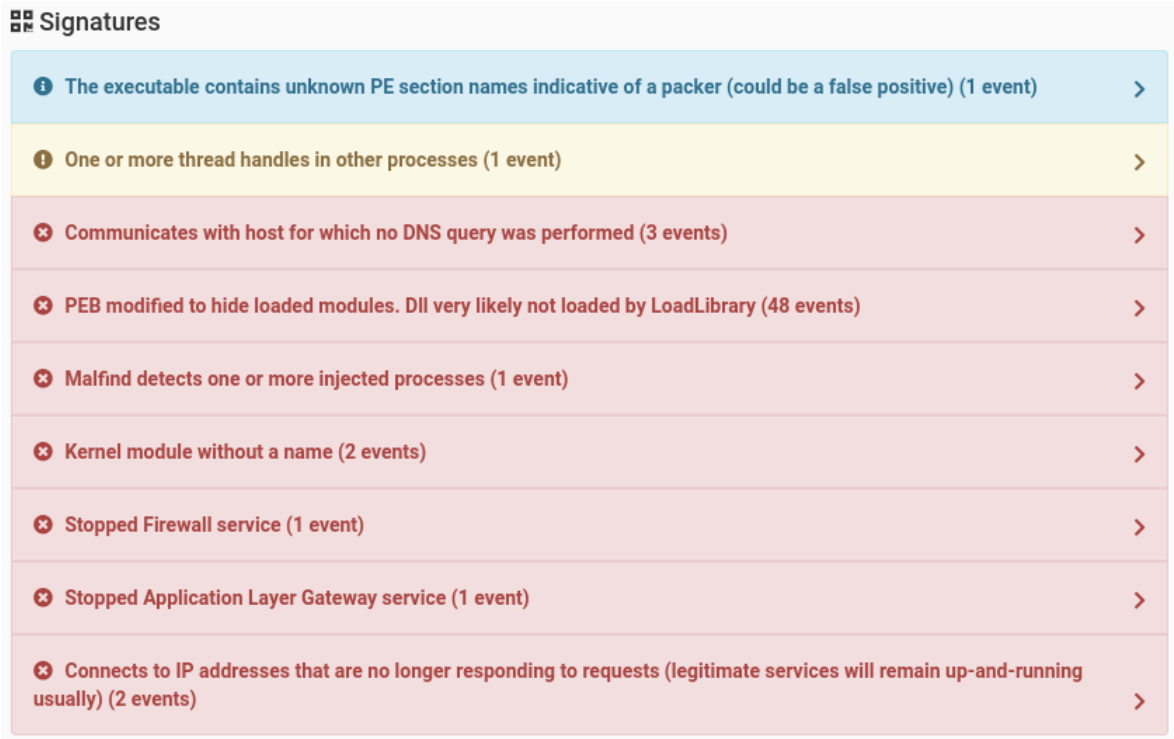
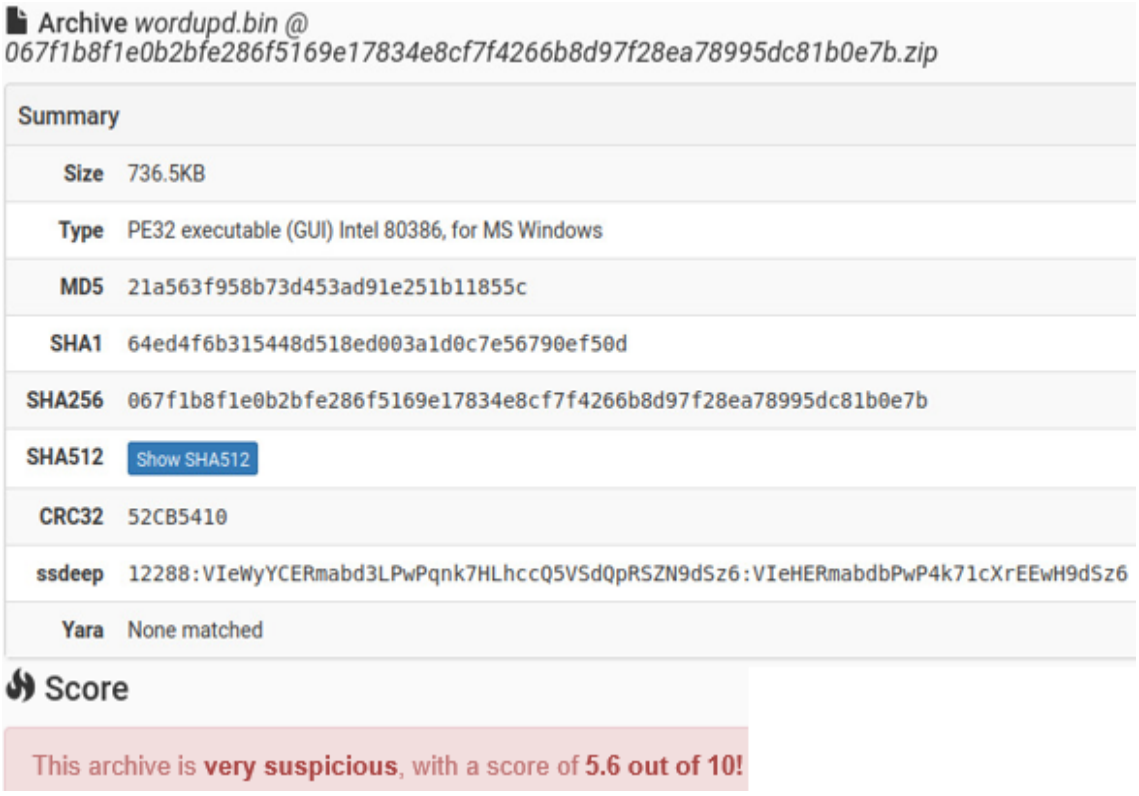


Figura 83. Detalle de firmas del análisis de Ransomware.

Los resultados obtenidos en el análisis de pruebas, se muestran mediante figuras que contienen el resumen y el score del Ransomware analizado como se muestran a continuación:

a. Ransomware Maze



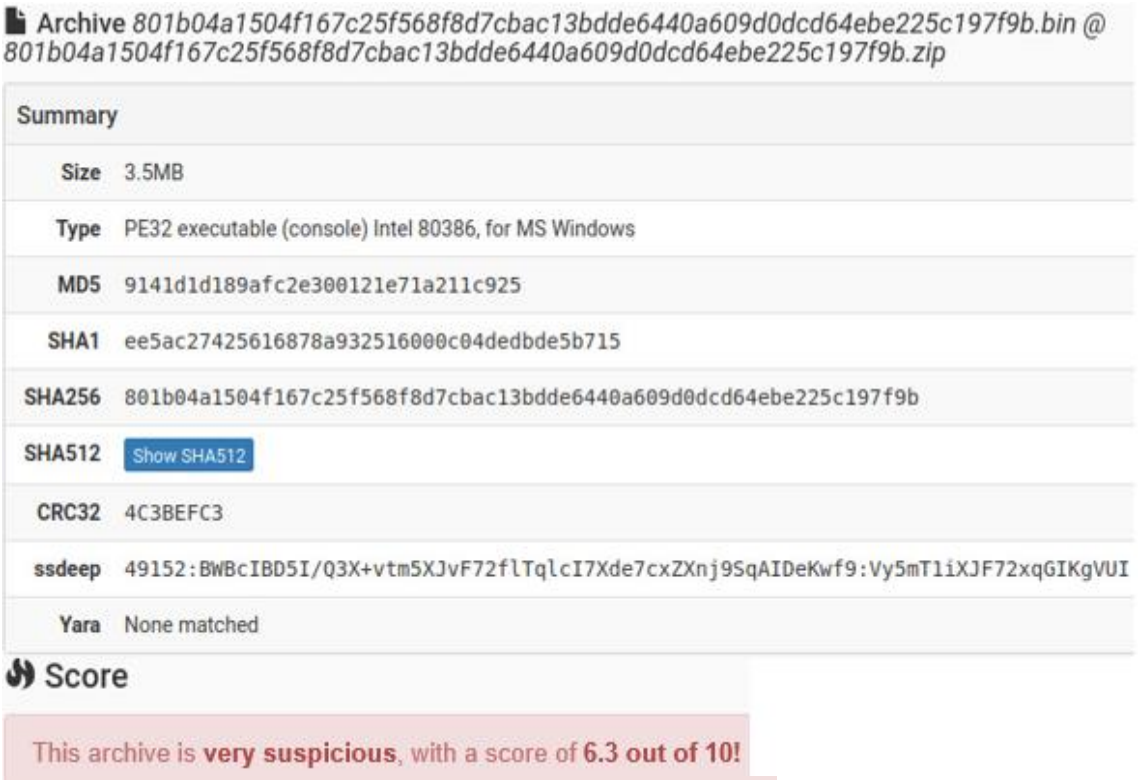
Archive *wordupd.bin @ 067f1b8f1e0b2bfe286f5169e17834e8cf7f4266b8d97f28ea78995dc81b0e7b.zip*

Summary	
Size	736.5KB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	21a563f958b73d453ad91e251b11855c
SHA1	64ed4f6b315448d518ed003a1d0c7e56790ef50d
SHA256	067f1b8f1e0b2bfe286f5169e17834e8cf7f4266b8d97f28ea78995dc81b0e7b
SHA512	Show SHA512
CRC32	52CB5410
ssdeep	12288:VIeWyYCERmabd3LPwPqnk7HLhccQ5VSdQpRSZN9dSz6:VIeHERmabdbPwP4k71cXrEEwH9dSz6
Yara	None matched

Score

This archive is **very suspicious**, with a score of **5.6 out of 10!**

b. Ransomware Doppelpaymer



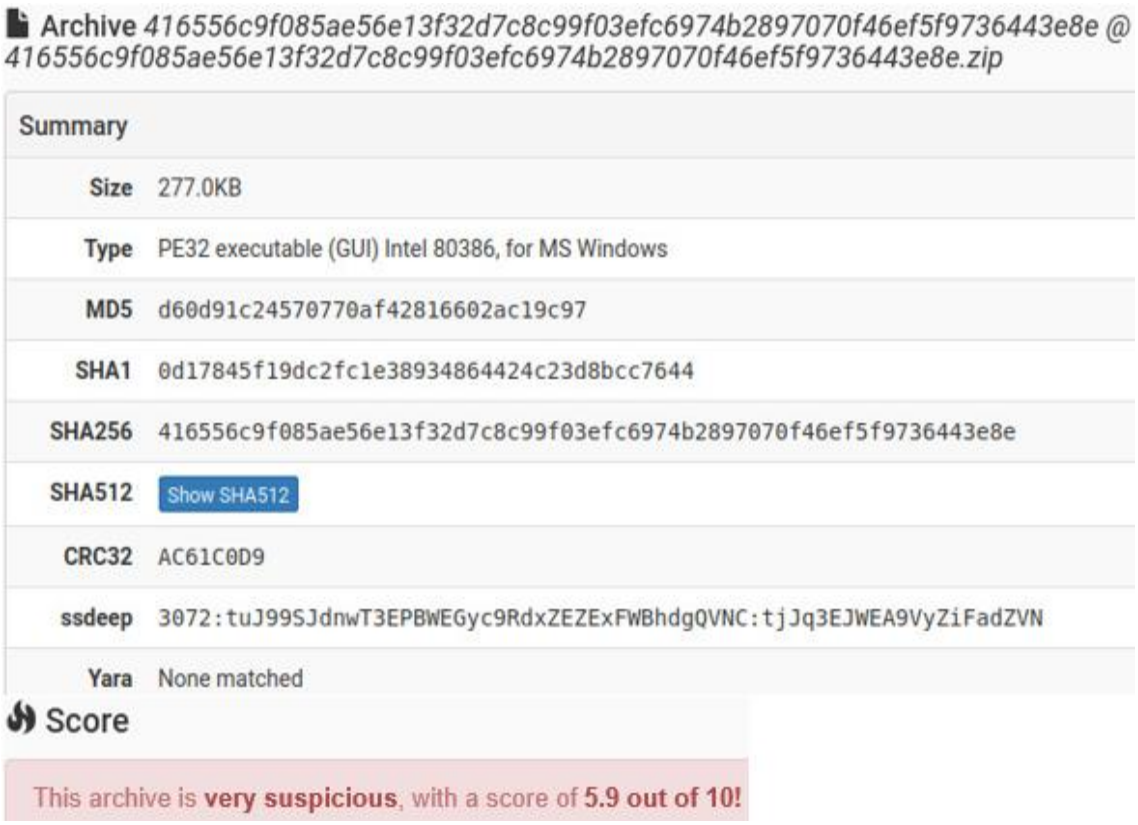
Archive *801b04a1504f167c25f568f8d7cbac13bdde6440a609d0dcd64ebe225c197f9b.bin @ 801b04a1504f167c25f568f8d7cbac13bdde6440a609d0dcd64ebe225c197f9b.zip*

Summary	
Size	3.5MB
Type	PE32 executable (console) Intel 80386, for MS Windows
MD5	9141d1d189afc2e300121e71a211c925
SHA1	ee5ac27425616878a932516000c04dedbde5b715
SHA256	801b04a1504f167c25f568f8d7cbac13bdde6440a609d0dcd64ebe225c197f9b
SHA512	Show SHA512
CRC32	4C3BEFC3
ssdeep	49152:BWBcIBD5I/Q3X+vtm5XJvF72flTqlcI7Xde7cxZXnj9SqAIDeKwf9:Vy5mT1iXJF72xqGIKgVUI
Yara	None matched

Score

This archive is **very suspicious**, with a score of **6.3 out of 10!**

c. Ransomware Netwalker



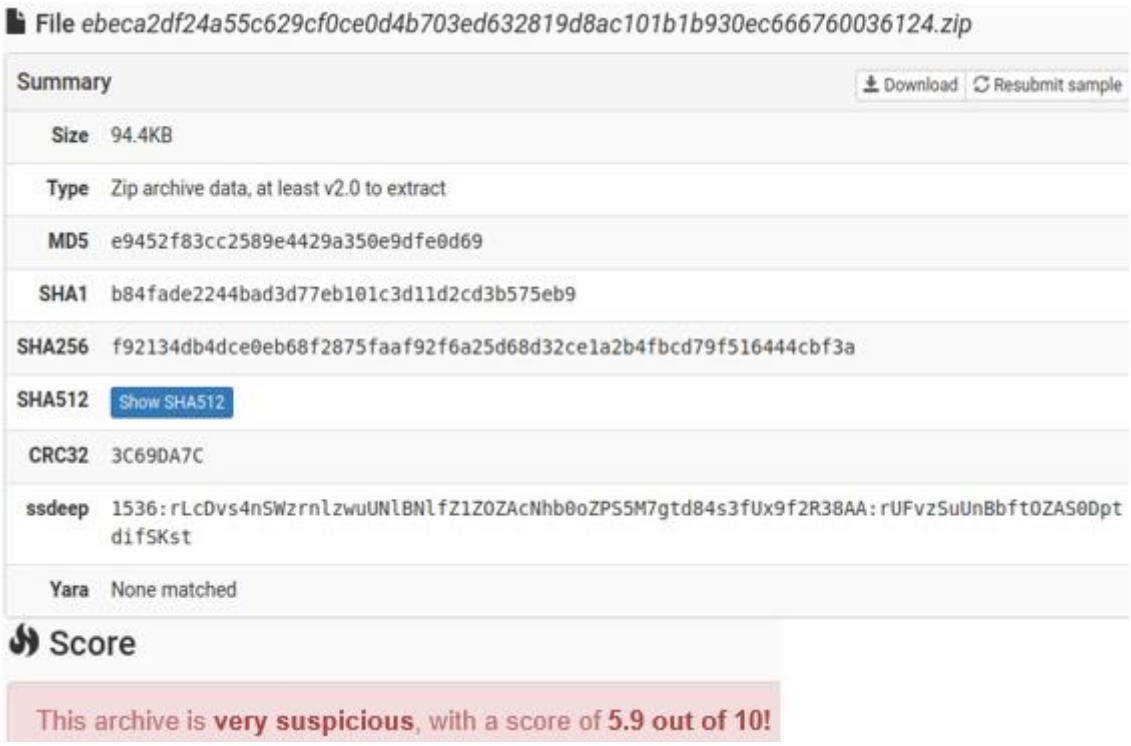
Archive *416556c9f085ae56e13f32d7c8c99f03efc6974b2897070f46ef5f9736443e8e @ 416556c9f085ae56e13f32d7c8c99f03efc6974b2897070f46ef5f9736443e8e.zip*

Summary	
Size	277.0KB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	d60d91c24570770af42816602ac19c97
SHA1	0d17845f19dc2fc1e38934864424c23d8bcc7644
SHA256	416556c9f085ae56e13f32d7c8c99f03efc6974b2897070f46ef5f9736443e8e
SHA512	Show SHA512
CRC32	AC61C0D9
ssdeep	3072:tuJ99SJdnwT3EPBWEGyc9RdxZEZExFWBhdgQVNC:tjJq3EJWEA9VyZiFadZVN
Yara	None matched

Score

This archive is **very suspicious**, with a score of **5.9 out of 10!**

d. Ransomware Conti



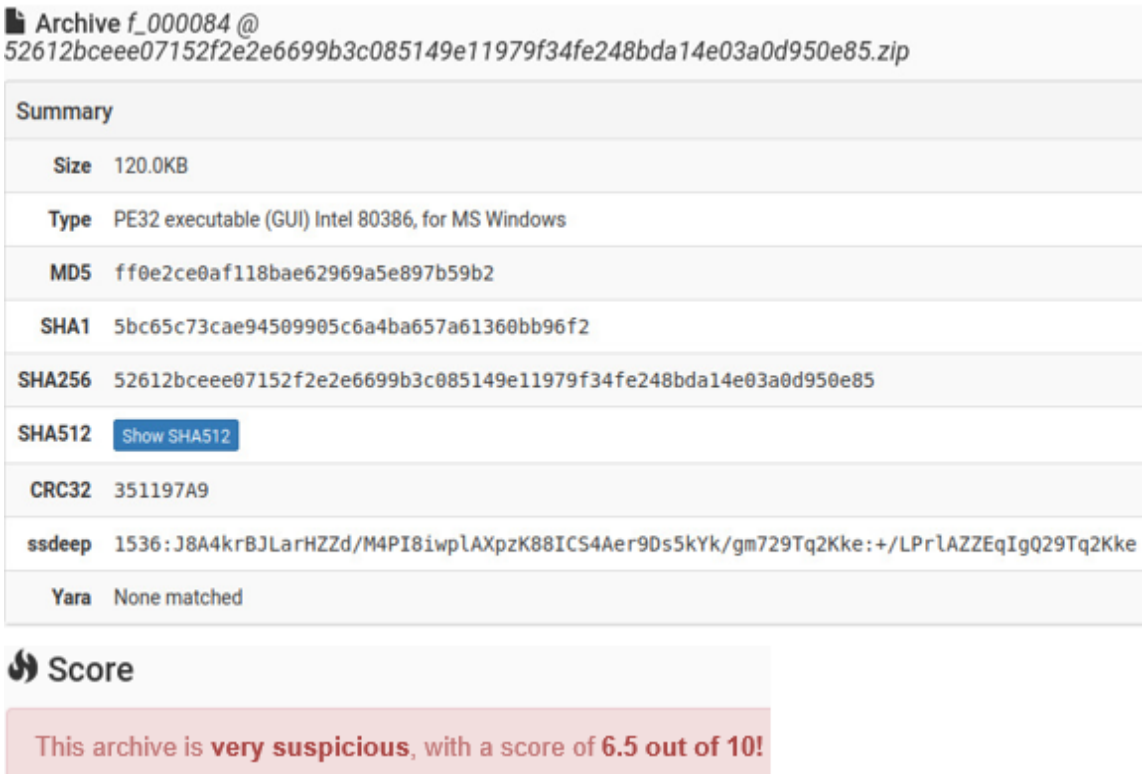
File *ebeca2df24a55c629cf0ce0d4b703ed632819d8ac101b1b930ec666760036124.zip*

Summary	Download / Resubmit sample
Size	94.4KB
Type	Zip archive data, at least v2.0 to extract
MD5	e9452f83cc2589e4429a350e9dfe0d69
SHA1	b84fade2244bad3d77eb101c3d11d2cd3b575eb9
SHA256	f92134db4dce0eb68f2875faaf92f6a25d68d32ce1a2b4fbcd79f516444cbf3a
SHA512	Show SHA512
CRC32	3C69DA7C
ssdeep	1536:rLcDvs4nSWzrnlzwuUNlBNlfZ1ZOZAcNhb0oZPS5M7gtd84s3fUx9f2R38AA:rUFvzSuUnBbftOZAS0Dptdif SKst
Yara	None matched

Score

This archive is **very suspicious**, with a score of **5.9 out of 10!**

e. Ransomware Revil/Sodinokibi



IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones.

a) En el estado actual de la red – antes de la implementación de Cuckoo Sandbox, se identificó puertos abiertos vulnerables, por donde se realizó ataques meterpreter a la red informática de la entidad, quedando comprobado que la seguridad de la red perimetral informática es efectivo en un 80%.

b) Se implementó la tecnología Sandbox en un ambiente virtualizado simulando la red informática local de la entidad y tomando sus políticas actuales implementadas, donde en el laboratorio de pruebas implementado, se consolidó los ataques controlados, dando de esa forma los resultados esperados.

c) Con los resultados obtenidos para cada métrica evaluada en el entorno de pruebas, se evidenció que Cuckoo Sandbox utiliza 0.89 Gb de memoria RAM para la evaluación de los ataques de Ransomware, en un tiempo mínimo de 123.6”, lo que hace que este método de detección de Ransomware sea eficiente, aprovechando mínimos recursos de hardware e identificando el 100% de los ataques inyectados.

d) La efectividad de Cuckoo Sandbox para esta investigación llegó al 100%, evitando la penetración de ransomware a la red informática de la entidad financiera.

e) Según los resultados obtenidos, se confirma la hipótesis planteada en esta investigación, donde se demuestra que la tecnología Sandbox mejoró la protección de la seguridad perimetral de la red informática local en la entidad financiera en un 20% con respecto a los resultados de la evaluación obtenida antes de su implementación, llegando a brindar el 100% de seguridad para la red informática en esta investigación.

4.2. Recomendaciones.

a) Para analizar el estado actual de una red informática de una entidad se debe obtener previamente la autorización del gerente o administrador de la entidad y utilizar mínimo dos herramientas de testeo de red, para obtener mejores resultados de vulnerabilidades en los puertos de la red.

b) Para la implementación de Cuckoo Sandbox, se recomienda que las características del servidor donde se instalará este implementado con 16 Gb de memoria RAM, microprocesador doble núcleo 2Gh y 500 Gb de disco duro, para obtener mejores resultados con respecto al tiempo de análisis y consumo de memoria, destinando este recurso solamente para la instalación de Cuckoo Sandbox.

c) Para obtener resultados similares o mejores a esta investigación se recomienda utilizar la versión más actualizada de Ubuntu, para la configuración de la red virtualizada se recomienda utilizar el sistema operativo Windows 10.

d) Para la obtención de resultados óptimos, la configuración en la virtualización de la red informática debe tener similitud con la configuración de la red informática física en donde se va a implementar.

REFERENCIAS

Accenture. (2018). *Consecuencias del ataque 2018.* Irlanda: Accenture.

Al-rimy, B. A., Maarof, M. A., & Zainuddin, S. (2017). *Factores de éxito de las amenazas de ransomware, taxonomía y contramedidas: una.* Malasia.

Ahmad.: THE V-NETWORK: A TESTBED FOR MALWARE ANALYSIS. Nigeria: Science World Journal. (2019).

Android. (25 de enero de 2021). *Source Android*. Obtenido de https://source.android.com/security/app-sandbox

Apple. (13 de setiembre de 2016). *Developer.apple*. Obtenido de https://developer.apple.com/library/archive/documentation/Security/Conceptual/AppSandboxDesignGuide/AboutAppSandbox/AboutAppSandbox.html#//apple_ref/doc/uid/TP40011183-CH1-SW1

Belcic, I. (19 de mayo de 2021). *AVAST*. Obtenido de https://www.avast.com/es-es/c-petya

Borate, I., & Chavan, R. K. (2016). *Sandboxing in Linux: From Smartphone to Cloud.* India: International Journal of Computer Applications.

Buchyk., Yudin., Ziubina., Bondarenko., Suprun.: Devising a method of protection against zero day attacks based on an analytical model of changing the state of the network sandbox. UCRANIA: Revista-european journal of enterprise technologies issn1729-3774. (2021).

Castro, I. (2016). *Conoce WildFire de Palo Alto Networks.* Mexico.

CISCO. (2019). *Anticipando lo desconocido.* San José, California: CISCO.

CISCO. (2019). *Talosintelligence.com*. Obtenido de https://talosintelligence.com/vulnerability_reports/TALOS-2019-0779

Community, K. d. (2019). *The Linux Kernel*. Obtenido de https://www.kernel.org/doc/html/v4.16/userspace-api/seccomp_filter.html

Cuckoo, F. S. (2019). *Cuckoo*. Obtenido de https://cuckoosandbox.org/

Debian. (27 de marzo de 2021). *Debian.org*. Obtenido de https://www.debian.org/intro/about

Descalzo, F. (2016). *Riesgos actuales en entornos virtualizados.* Obtenido de http://www.cybsec.com/upload/Descalzo_Riesgos_Virtualizacion_v1.pdf

ESET. (25 de febrero de 2015). *Welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2015/02/25/que-es-un-0-day/

ESET. (2017). *Guía de Ransomware.* Bratislava, Slovak Republic: ESET, spol. s r.o.

ESET. (23 de marzo de 2020). *ESET*. Obtenido de https://support.eset.com/es/kb2767-deshabilitar-las-actualizaciones-automaticas-en-los-productos-eset-hogarenos-para-windows

ESET. (2021). *5 grupos de ransomware con más impacto en América Latina en 2020.* Bratislava, Slovak Republic: ESET, spol. s r.o.

ESET. (2021). *Dynamic Thread Defense.* Bratislava, Slovak Republic: ESET, spol. s r.o.

ESET. (2021). *ESET Cloud Office Security.* Bratislava, Slovak Republic: ESET, spol. s r.o.

ESET. (2021). *ESET File Security.* Bratislava, Slovak Republic: ESET, spol. s r.o.

ESET. (2021). *ESET Full Disk Encryption.* Bratislava, Slovak Republic: ESET, spol. s r.o.

ESET. (2021). *ESET Mail Security.* Bratislava, Slovak Republic: ESET, spol. s r.o.

Europol, Politie, Kaspersky, & McAfee. (Julio de 2016). *nomoreransom*. Obtenido de nomoreransom: https://www.nomoreransom.org/es/about-the-project.html

Fernandez, M. (16 de Febrero de 2020). Ciberataques que matan a las empresas. *EL PAIS*.

Firejail. (16 de marzo de 2021). *Firejail Security Sandbox*. Obtenido de https://firejail.wordpress.com/

FORTINET. (2020). *Thread intelligence insider.* Estados Unidos - California.

Foundation, C. (2019). *Cuckoo*. Obtenido de https://cuckoo.sh/docs/installation/host/index.html

GyungMin, L., ShinWoo, S., ByoungMo, C., TaeKyu, K., Kyounggon, K.: Fileless cyberattacks Analysis and classification. Arabia: ETRI Journal. (2020).

Harán, J. M. (12 de mayo de 2021). *Welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2021/05/12/actualizacion-seguridad-microsoft-mayo-corrige-tres-zero-day/

Hernández, C., & Mauricio, A. (2019). *Ingeniería socia: Phishing y Baiting.* Colombia.

Humayun., Jhanjhi., Alsayat., Ponnusamy.: Internet de las cosas y ransomware: evolución, mitigación y. Arabia: Egyptian Informatics Journal. (2021).

Huthifh, A., Mohammad, S., Sharhabeel, A.: On Detection and Prevention of Zero-Day Attack Using Cuckoo Sandbox in Software-Defined Networks. Jordania: The International Arab Journal of Information Technology. (2020).

IBM. (2019). *IBM.com*. Obtenido de https://www.ibm.com/docs/en/qsip/7.3.2?topic=queries-berkeley-packet-filters

Jaén, U. d. (2018). *Guías de seguridad UJA - Software malicioso (malware).* Jaén.

Jinni. (2020). *Tutorialjinni*. Obtenido de https://www.tutorialjinni.com/

kali.org. (2021). *kali*. Obtenido de https://www.kali.org/

Kamal, A., Morched, D., Jan, S., Iqbal, J., Qudus, F., Jerbi, H., Ahmad, G. A.: User-friendly Model for Ransomware Analysis Using. Arabia: Computers, Materials and Continua. (2020).

kaspersky. (2021). *kaspersky*. Obtenido de https://www.kaspersky.es/blog/top5-ransomware-groups/25126/

Kaspersky. (2021). *Kaspersky*. Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-maze-ransomware

Kaspersky. (2021). *noransom*. Obtenido de noransom: https://noransom.kaspersky.com/

Keragala, D. (2021). *Detecting Malware and Sandbox, Evasion Techniques.* SANS Institute.

Ketzaki., Toupas., Giannoutakis., Drosou., Tzovaras.: "A behaviour based ransomware detection using neural network models". (2020).

Linux. (08 de junio de 2021). *Contenedores de Linux*. Obtenido de linuxcontainers.org/: https://linuxcontainers.org/lxc/introduction/

Linux. (08 de junio de 2021). *linux.die.net*. Obtenido de https://linux.die.net/man/3/sleep

López, A. (04 de junio de 2015). *incibe-cert*. Obtenido de https://www.incibe-cert.es/blog/linux-capabilities

Ltd, C. (2021). *Ubuntu*. Obtenido de https://ubuntu.com/download/desktop

Maurer., Kim., Dan., Kappelman.: Cybersecurity Is It Worse than We Think? EE.UU: Communications of the ACM. (2021).

Mehmoon, S. (2016). *Enterprise Survival Guide for Ransomware Attacks.*

Mehmoon, S. (2021). *Enterprise Survival Guide for Ransomware Attacks.*

Mera, E. Z., Casanova, O. J., Vergara, J. T., & Bayas, B. O. (2021). Análisis dinámico de malware en ambiente de red virtualizado. *Revista Conrado*, 113-120.

Micro Trend. (2016). *Proteja su organización.* Hoboken, New Jersey: John Wiley & Sons, Inc.

Microsoft. (01 de Junio de 2021). *Microsoft*. Obtenido de https://docs.microsoft.com/es-es/windows/security/threat-protection/intelligence/trojans-malware

Microsoft. (24 de marzo de 2021). *Microsoft Windows Sandbox*. Obtenido de https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-sandbox/windows-sandbox-overview

Morato., Berrueta., Magaña., Izal.: Ransomware early detection by the analysis of file sharing traffic. Spain: Journal of Network and Computer Applications 124 (2018) 14–32.

Njccic. (27 de setiembre de 2016). *Cyber.nj.gov*. Obtenido de https://www.cyber.nj.gov/threat-center/threat-profiles/trojan-variants/ursnif

Nvd. (2015). *nvd.nist.gov*. Obtenido de https://nvd.nist.gov/vuln/detail/CVE-2015-6240

Owaida, A. (22 de abril de 2021). *elivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2021/04/22/google-lanza-apuro-actualizacion-repara-nueva-zero-day-chrome/

OWASP. (2015). *Guia Contra Ransomware.*

Pardo, M. (12 de marzo de 2021). *Infrasoftcorp*. Obtenido de https://www.infrasoftcorp.com/en-busqueda-del-error-vulnerabilidades-del-dia-cero-zero-day-exploit/

Ramírez, I. (31 de enero de 2020). *Xataka*. Obtenido de https://www.xataka.com/especiales/maquinas-virtuales-que-son-como-funcionan-y-como-utilizarlas

RedHat. (11 de setiembre de 2019). *Redhat.com*. Obtenido de https://access.redhat.com/security/cve/cve-2017-5123

RedHat. (2021). *Red Hat*. Obtenido de https://www.redhat.com/en

Reis, D. (2013). *Seguridad para la nube y la virtualización.* Hoboken, New Jersey: John Wiley & Sons, Inc.

Rjrodriguez. (2019). *Bitbucket*. Obtenido de https://bitbucket.org/rjrodriguez/pinvmshield/src/master/

Rodríguez, P. R. (2019). Análisis de técnicas de aislamiento de procesos (Sandbox) en Linux. Sevilla.

Sanz, M. (2019). *¿Qué es Sandbox y en qué consiste?* España: computerhoy.

Shammugam., Narayana., Magalingam., Maarop., Perumal., Shanmugam.: Information security threats encountered by Malaysian public. Malasia: Indonesian Journal. (2021).

Sierra, A. F., Hernández, M. J., & H. F. (2020). Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware. *UIS Ingenierías*, 13.

SuperIntendencia de Banca, Seguros y AFP. (s.f.). *SBS*. Obtenido de https://www.sbs.gob.pe/usuarios/informacion-financiera/relacion-de-entidades-autorizadas-a-captar-depositos-en-cada-region

VMware. (2019). *Vmware.com*. Obtenido de https://www.vmware.com/es/products/workstation-pro.html

Wojciech, Luca.: Cyber reconnaissance techniques. Polonia: Communications of the ACM. (2021).

Yu, L., Liu, L., Tan, C., Zhao, B., Zhang, C.: Scheduling and Deploying Distributed Sandboxes for Cyber-Attack Detection. China: International Journal of Performability Engineering. (2020).

Zutphen, R. v. (19 de junio de 2019). *Cuckoo*. Obtenido de https://cuckoosandbox.org/blog/207-interim-release

ANEXOS.

Anexo 1. Resolución del proyecto.

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N°0445-2021/FIAU-USS

Pimentel, 27 de mayo de 2021

VISTO:

El Acta de reunión N°1305-2021 del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS remitida mediante oficio N°0227-2021/FIAU-IS-USS de fecha 19 de mayo de 2021, y;

CONSIDERANDO:

Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48° que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21° señala: "Los temas de trabajo de investigación, trabajo académico y tesis son aprobados por el Comité de Investigación y derivados a la Facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El periodo de vigencia de los mismos será de dos años, a partir de su aprobación. En caso un tema perdiera vigencia, el Comité de Investigación evaluará la ampliación de la misma.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24° señala: La tesis es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado; es individual o en pares para obtener un título profesional. Asimismo, en su artículo 25° señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C.".

Que, según documentos de Vistos el Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS acuerdan aprobar los temas de las Tesis a cargo de los estudiantes del curso de Investigación I que se detallan en el anexo de la presente Resolución.

Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

SE RESUELVE:

ARTÍCULO 1°: APROBAR, el tema de la Tesis perteneciente a la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE, a cargo de los estudiantes del Programa de estudios de INGENIERÍA DE SISTEMAS según se detalla en el anexo de la presente Resolución.

ARTÍCULO 2°: ESTABLECER, que la inscripción del Tema de la Tesis se realice a partir de emitida la presente resolución y tendrá una vigencia de dos (02) años.

ARTÍCULO 3°: DEJAR SIN EFECTO, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Dr. Manli Portocarrero Barnos Moscol
Docente - Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Mba. María Emilia Núñez Rivera
Secretaria Académica / Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Cc: Interesado, Archivo

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N°0445-2021/FIAU-USS

Pimentel, 27 de mayo de 2021

ANEXO

N°	AUTOR (ES)	TEMA DE TESIS
1	RIMARACHIN ESCRIBANO NERI RUT NIÑO MORENO NAJHELY YAMILETT	EVALUACIÓN DE TÉCNICAS DE CIFRADO PARA EL INTERCAMBIO DE DATOS DE INTERNET DE LAS COSAS EN EL ÁMBITO DE LA SALUD
2	GUEVARA CHAMBERGO JHON DENNIS BOBADILLA CAMPOS ROLANDO MARTIN	DESARROLLO DE UNA METODOLOGÍA DE GESTIÓN DE RIESGOS AD HOC BASADA EN MARCOS INTERNACIONALES Y BUENAS PRÁCTICAS PARA UNA EMPRESA MANUFACTURERA PERUANA
3	CIEZA CELIS JESUS ABELARDO OJEDA ROMERO ANTHONNY JHONATAN	EVALUACIÓN DEL DESEMPEÑO DE LOS ESQUEMAS DE SEGURIDAD DE RED PARA COMBATIR VULNERABILIDADES EN REDES INALÁMBRICAS BASADAS EN EL PROTOCOLO WPA2
4	MENDOZA FERRÉ ESPERANZA NATALY CABRERA SANCHEZ KEVIN ALONSO	COMPARACIÓN DEL RENDIMIENTO DE TECNOLOGÍAS DE VIRTUALIZACIÓN PARA EL DESPLIEGUE DE APLICACIONES CON ARQUITECTURA DE MICROSERVICIOS
5	TEMOCHE GOMEZ LENNIN BILLEY	DESARROLLO DE UN MÉTODO PARA DETECTAR CON EFICIENCIA LAS VULNERABILIDADES INFORMÁTICAS DE ATAQUE CROSS-SITE SCRIPTING UTILIZANDO TÉCNICAS DE APRENDIZAJE AUTOMÁTICO
6	CASTRO MEDINA MIGUEL ANGEL	IMPLEMENTACIÓN DE UNA METODOLOGÍA AD HOC DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA EDITORA DE DIARIO REGIONAL PERUANO
7	MURO ESPINOZA JUAN JOSE	DESARROLLO DE UNA METODOLOGÍA AD HOC DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA UN INSTITUTO SUPERIOR PEDAGÓGICO PERUANO
8	DIAZ ZAVALA ROXANA KARINA FRIAS VASQUEZ LADY	DESARROLLO DE UNA METODOLOGÍA AD HOC DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA UNA UNIDAD DE GESTIÓN EDUCATIVA PERUANA
9	CARRASCO BORDA APARICIO	DESARROLLO DE UN MODELO DE PROCESOS AD HOC PARA EL DESARROLLO DE SOFTWARE POR LICENCIA PARA UNA MYPE DE SERVICIOS DE TI BASADO EN ISO/IEC 29110
10	OTERO MORALES JAVIER LIZARDO AQUINO SOSA NOELIA STEPHANY	DESARROLLO DE UN MODELO DE PROCESOS BASADO EN NORMAS DE PEQUEÑAS ORGANIZACIONES PARA MEJORAR LA CONSTRUCCIÓN DE SOFTWARE EN UN ÁREA DE DESARROLLO DE GOBIERNO MUNICIPAL
11	CALDERON YNOÑAN PAMELA DEL CARMEN PRIETO NEIRA FRANCK ALBERSON	DESARROLLO DE UN MÉTODO BAJO EL ENFOQUE ÁGIL EN ENTORNOS DE EXPERIENCIA DE USUARIO UI/UX PARA ASEGURAR LA USABILIDAD WEB
12	FLORES TINEO HUGO GALVANI DOLORIER POMA RONY RAUL	EVALUACIÓN DE LA USABILIDAD EN ENTORNOS VIRTUALES DE APRENDIZAJE PARA USUARIOS DE LAS ZONAS RURALES DEL PERU UTILIZANDO LA NORMA ISO/IEC 25010
13	CHANCAFE CASTRO JULIO JOEL	DESARROLLO DE UN MODELO DE PROCESOS AD HOC PARA EL DESARROLLO DE SOFTWARE PARA UNA MUNICIPALIDAD BASADO EN ISO/IEC 29110
14	SALAZAR DAVILA GIANFRANCO STEVEN	COMPARACIÓN DE TÉCNICAS DE VALIDACIÓN DE REQUISITOS DE SOFTWARE PARA MEDIR LA INFLUENCIA EN EL ÉXITO DE LOS PROYECTOS DE DESARROLLO EN PEQUEÑAS EMPRESAS PERUANAS
15	RIOJA MESIA CHARLES SEGUNDO FERNANDEZ RIOJA JUAN NICANOR	IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN DE INCIDENCIAS BASADO EN ITIL PARA MEJORAR EL SERVICIO DE TI EN UNA MUNICIPALIDAD DISTRITAL DE LA REGIÓN LAMBAYEQUE
16	ALFARO PAJARES JUAN PEDRO	EVALUACIÓN DEL DESEMPEÑO DE PROCESOS DE NEGOCIO GESTIONADOS POR BPM EN UNA EMPRESA CONSTRUCTORA PERUANA
17	MONSALVE FERNANDEZ LENIN ESTALIN	IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN DE SERVICIOS DE TI BASADO EN ITIL PARA MEJORAR LA GESTIÓN DE LOS SERVICIOS DE LA DIRECCIÓN DE TECNOLOGÍA DE UN GOBIERNO REGIONAL PERUANO
18	PEREZ CAMPOS DE QUIROZ BETTY MAGALY	EVALUACIÓN DEL DESEMPEÑO DE PROCESOS DE NEGOCIO GESTIONADOS POR BPM EN UNA MICRO EMPRESA PERUANA DESARROLLADORA DE SOFTWARE
19	MONTJOY PITA BRUNO	DESARROLLO DE UN SISTEMA DE RECOMENDACIÓN AUTOMÁTICA PARA EL TRATAMIENTO DE LAS PLAGAS EN CULTIVOS DE ARROZ DE LAS VARIEDADES QUE SE PRODUCEN EN LA REGIÓN LAMBAYEQUE
20	CRUZ FLORES JOSE ANTONIO CHAVEZ ANGULO GERMAN NEPTALI	IMPLEMENTACIÓN DE ARQUITECTURA EMPRESARIAL BASADO EN METODOLOGÍA ÁGIL PARA ALINEAR LAS TECNOLOGÍAS DE INFORMACIÓN CON LOS OBJETIVOS DE NEGOCIO DE UN ESTABLECIMIENTO PERUANO DE SALUD BUCAL

Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN S.A.C.

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N°0445-2021/FIAU-USS

Pimentel, 27 de mayo de 2021

N°	AUTOR (ES)	TEMA DE TESIS
21	PISFIL CORONADO JOSE LUIS FELIPE	IMPLEMENTACIÓN DE ARQUITECTURA EMPRESARIAL BASADA EN METODOLOGÍA ÁGIL PARA ALINEAR TI CON LOS PROCESOS DE NEGOCIO EN UNA EMPRESA CONSTRUCTORA PERUANA DE OBRAS CIVILES
22	ABAD HERRERA JOHNNY RENSO TEPE ESPINOZA LUIS RAMON	IMPLEMENTACIÓN DE ITIL V4 PARA MEJORAR LOS SERVICIOS DE TI EN EL CENTRO DE SISTEMAS DE INFORMACIÓN DE UNA UNIDAD DE GESTIÓN EDUCATIVA LOCAL PERUANO
23	URRUTIA VASQUEZ MIGUEL JULCA ROJAS ALEX ROGELIO	DESARROLLO DE UN MÉTODO DE IDENTIFICACIÓN AUTOMÁTICA DE ATAQUES SPOOFING DE ENVENENAMIENTO ARP EN LA SUPLANTACIÓN DE IDENTIDAD EN REDES LAN
24	SANCHEZ CELADA ERLIN FERNANDEZ ROMAN ISMAEL	COMPARACIÓN DE ARQUITECTURAS DE IDS HÍBRIDO PARA LA IDENTIFICACIÓN DE ATAQUES DE DOS EN LOS SERVIDORES WEB DE UNA MUNICIPALIDAD PROVINCIAL PERUANA
25	PERALES CHAVEZ JEFFERSON ADRIAN	IMPLEMENTACIÓN DE UN MODELO DE ARQUITECTURA DE INDUSTRIA 4.0 PARA MEJORAR LA INTEROPERABILIDAD ENTRE SISTEMAS DE UNA EMPRESA PERUANA
26	MAGALLANES CARBAJAL KENSER	EVALUACIÓN DE LA EFICIENCIA DE LOS ALGORITMOS DE CRIPTOGRAFÍA PARA CUMPLIR CON LOS NIVELES DE SEGURIDAD DE DATOS DE UNA EMPRESA FINANCIERA PERUANA
27	RACCHUMI LECCA JESÚS MANUEL	DESARROLLO DE UN MIDDLEWARE PARA MEJORAR LA COMUNICACIÓN ENTRE DOS INTERFACES DE LMS Y CRM EN EL PROCESO DE REGISTRO Y EMISIÓN DE CREDENCIALES DE USUARIOS
28	CASTRO QUESQUEN JAIME ELTON	COMPARACIÓN DE ALGORITMOS DE CIFRADO DE DATOS EN EL ASEGURAMIENTO DE VIDEO LLAMADA SOBRE REDES IP
29	PEREZ DIAZ NEILER WILTER CHINCHAY MALDONADO JORGE OBED	IMPLEMENTACIÓN DE TECNOLOGÍA SANDBOX PARA PROTEGER DE ATAQUES RANSOMWARE EN UNA RED INFORMÁTICA LOCAL DE UNA ENTIDAD FINANCIERA
30	MOSCOSO PAREDES ANIBAL	DISEÑO DE UN MODELO DE ARQUITECTURA DE SEGURIDAD DE BAJO COSTO PARA REFORZAR LA SEGURIDAD DE LA RED DEL HOGAR ANTE ATAQUES INFORMÁTICOS
31	MARTINEZ CUMPA JORGE JOSE	EVALUACIÓN DE FACTIBILIDAD DE USO DE TECNOLOGÍA WIRELESS 5GHZ PARA PROPORCIONAR SERVICIOS DE COMUNICACIÓN INALÁMBRICA EN LOS CENTROS POBLADOS RURALES DE LA REGIÓN LAMBAYEQUE
32	CAMPOS BARRERA SANDRO PAUL PASTOR OLIVA CESAR AUGUSTO	IMPLEMENTACIÓN DE UN MÉTODO DE CLASIFICACIÓN PARA DETECTAR LA DESERCIÓN DE ESTUDIANTES DE LA CARRERA DE INGENIERÍA DE INDUSTRIAS ALIMENTARIAS DE UNA UNIVERSIDAD NACIONAL PERUANA BASADO EN APRENDIZAJE DE MAQUINA
33	PICON VASQUEZ ANGEL GABRIEL CESPEDES SALAZAR JUAN CARLOS	DESARROLLO DE UN MÉTODO DE CLASIFICACIÓN AUTOMÁTICA BASADA EN TÉCNICAS ESTADÍSTICAS Y DE MACHINE LEARNING PARA CLASIFICAR A LOS POSTULANTES DE ACUERDO AL PERFIL DE TRABAJO DE UN CALL CENTER
34	MIÑANO SANCHEZ CARLOS JOHNY	COMPARACIÓN DE TÉCNICAS DE MINERÍA DE DATOS PARA DESCUBRIR INFORMACIÓN RELEVANTE DE VENTAS DE UNA MYPE COMERCIAL
35	MARTOS PAREDES JOEL HAROLD VILLAZON SOSA JAIR AUGUSTO	IMPLEMENTACIÓN DE UN MODELO DE PROCESOS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA PYME PERUANA BASADO EN LA NORMA ISO/IEC 27005 Y LA METODOLOGÍA OCTAVE-S
36	QUISPE PUEMAPE LUIS ALONSO	IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA ISO/IEC 27001:2014 EN UNA EMPRESA PERUANA DE TELECOMUNICACIONES
37	CHUCO AGUILAR GERSON RAUL	IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADA EN ISO/IEC 27001 PARA MEJORAR EL NIVEL DE SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN EN UNA EMPRESA CONSTRUCTORA DE OBRAS CIVILES
38	CAJUSOL ROJAS JOSE DEL CARMEN	IMPLEMENTACIÓN DE UNA PLATAFORMA WEB PARA LA PLANIFICACIÓN Y MONITOREO DE RUTAS DE RECOJO DE RESIDUOS SÓLIDOS DE UN MUNICIPIO DE LA REGIÓN LAMBAYEQUE
39	VALLEJOS RAMOS FERNANDO RAFAEL	DESARROLLO DE UN MÉTODO DE OPTIMIZACIÓN DE USO DE TELA EN EL PROCESO DE ELABORACIÓN DE PRENDAS TEXTILES DE MICROEMPRESAS PERUANAS
40	REQUEJO NAVARRO JERSONS EXFRANSHER	EVALUACIÓN DE ALGORITMOS CRIPTOGRÁFICOS PARA MEJORAR SEGURIDAD EN UNA RED PRIVADA VIRTUAL

Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN S.A.C.

Anexo 2. Carta de aceptación de la empresa.

NORANDINO
COOPERATIVA DE AHORRO Y CRÉDITO

Tu desarrollo, nuestro compromiso.

Año del Bicentenario del Peru:200 Años de Independencia

Jaén 08 de Julio del 2021

Mg. Ing. Víctor Tuesta Monteza
Director de la Escuela de Ingeniería de Sistemas
Universidad Señor de Sipán

Presente:

REF: Solicitud de fecha 28/05/2021

Tengo el agrado de dirigirme a usted con la finalidad de hacer de su conocimiento que el **Sr. Chinchay Maldonado Jorge Obed** y el **Sr. Pérez Díaz Neiler Wilter**, alumnos de la Escuela de Ingeniería de Sistemas de la institución Universitaria que usted representa, han sido admitidos para realizar su investigación en el desarrollo de su tesis denominada **"IMPLEMENTACIÓN DE TECNOLOGÍA SANDBOX PARA PROTEGER DE ATAQUES RANSOMWARE EN UNA RED INFORMÁTICA LOCAL DE UNA ENTIDAD FINANCIERA"**.

Sin otro particular me suscrito de usted.

COOPAC NORANDINO LTDA.
Econ. Cleiver Rojas Hernández
GERENTE GENERAL

AGENCIA PRINCIPAL
Calle Pardo Miguel N°417-Jaén. TELÉF: 076-433327

www.coopacnorandino.com /

PUNTOS DE ATENCIÓN:
PIURA: Jr. Libertad N°534 Telef. 073-306 005 **26 DE OCTUBRE:** Av. Grau N° 1853 Urb. San José Telef: 073- 527 970 **AYABACA:** Av. Andrés Avelino Cáceres N°234 Telef. 073-526 030 **PONTEZO:** Jr. Ernesto Merino S/N Cel: 932 045 493 **SAN MIGUEL DEL FAIQUE:** Jr. Piura S/N Telef. : 992 063 278 **HUANCABAMBA:** Calle 2 De Mayo N° 203 Cel: 982 703 575 **TARAPOTO:** Jr. Nicolás de Piérola N°256 Telef. 042-586385 **LAMAS:** Jr. San Martin N° 506 Telef: 042-543 736 **SAN JOSÉ DE SISA:** Av. Grau S/N Cuadra 4 Cel:982 703 395 **JUANJUI:** Jr.Progreso N° 410 Telef: 042-594 603 **SAN IGNACIO:** Av. San Ignacio N° 454 Cel: 982 703 453 **PANCHIA:** Av. Hitos N° 280 Cel: 999 595 213 **CHURUYACU:** Nicolás Adrianzén N° 258Cel:976 196 103 **SANTA ROSA DE LA YUNGA:** Av. Jesús Calador S/N Cel: 992 064 278 **LA COPA:** Av. Martín Cuestas N° 405 Cel: 982 703 457 **SAN JOSÉ DE LOURDES:** Jr. Manco Cápac N° 106Cel: 982 703 396 **CHIRINOS:** Calle San Ignacio N° 298 Cel: 982 703 371.

Anexo 3. Instrumentos de recolección de datos. Pruebas de laboratorio

Pruebas de laboratorio 'Ataques Ransomware en Sandbox'	
Descripción	**Valor**
Fecha	
N°. Ataque.	
Nombre de Ransomware:	
Memoria Inicial:	
Memoria Final:	
Hora inicio:	
Hora Fin:	
Tiempo de duración del análisis:	
Estado:	☐Aislado ☐No aislado

Anexo 4. Instrumentos de recolección de datos. Resultados

Reporte de pruebas de laboratorio 'Ataques Ransomware en Sandbox'	
Descripción	**Valor**
Promedio de consumo de memoria.	
tiempo promedio de análisis.	
Porcentaje de efectividad de Sandbox	
Porcentaje de respuesta a incidentes de ataques maliciosos	
Porcentaje cobertura de los host de detección y tratamiento de malware	
Porcentaje de cobertura de de riesgos de los host	

Anexo 5. Tipos de Ransomware.

Ransomware	Año de aparición	Exploit Kits	Técnicas de ataque EEscaneo y explotación de vulnerabilidades	Ataques a servicios RDP
Cryrar	2015	X	X	X
Reveton	2015	X	X	X
Locky	2014	X	X	X
Petya	2014	X	X	X
Cryptowall	2014	X	X	X
Teslacrypt	2014	X	X	X
Wannacry	2017	X	X	X
Cryptolocker	2007	X	X	X
Ryuk	2018	X	X	X
Maze	2019		✓	
Doppelpaymer	2020		✓	
Netwalker	2020		✓	
Conti	2019		✓	
Revil/Sodinokibi	2019		✓	

Fuente: (Al-rimy, Maarof, & Zainuddin, 2017).

Anexo 6. Ransomware más activos en los últimos 5 años.

Maze	2019	✓
Doppelpaymer	2020	✓
Netwalker	2020	✓
Conti	2019	✓
Revil/Sodinokibi	2019	✓

Fuente: (ESET, 2021).