Medir el nivel de Exposición y Posibles Vulnerabilidades Existentes en la red Corporativa de la Empresa LAZARO SOFTWARE S.A.S

Jeobany Andrés Ramos Gasca

Asesor

Juan Manual Aldana Porras

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Ingeniería de Sistemas

Ibagué - Tolima

2024

Juan Manual Aldana Porras

Daniel Felipe Palomo

Jurado

2024

Dedicatoria

Dedico principalmente este trabajo a Dios. Por haberme permitido llegar a estas instancias de mi vida como persona y brindarme principalmente la salud para lograr tan importante objetivo. A mis padres Ana Dolores Gasca Zambrano y Luis Felipe Ramos Zuñiga mis tres hijos ypor ultimo a mi esposa Yuri Herlid Angarita por ser el motor fundamental en cada uno de los avances en mi vida tanto como persona y profesional, por su incondicional apoyo.

Agradecimientos

Agradezco a mi universidad, por haberme permitido formarme como profesional en el area de Ingeniero de sistemas, al Ingeniero docente Juan Manuel Aldana por brindarme su conocimiento, principalmente en el area de ciberseguridad. A cada uno de los tutores por brindarme su apoyo durante cada una de las etapas del proceso formativo en esta profesión, les agradezco infinitamente que Dios los bendiga a todos.

Resumen

Este proyecto aplicado abordo principalmente el tema relacionado con la validación de una forma efectiva el nivel de seguridad de los activos a la empresa LAZARO SOFTWARE S.A.S en un entorno productivo, Este proyecto se realizó con el interés de dar a conocer que la información, sistemas operativos, redes de datos y la continua manipulación inapropiada de los usuarios, faciliten a diario a que lo ciberdelincuentes aprovechen estas vulnerabilidades ingresen a la red de la compañía, por ello la importancia de ser proactivos con respecto a posibles intrusiones, con el fin de limitar la fuga de información y la manipulación de los activos comprometidos. Para ello surge la necesidad de validar el nivel de seguridad a la red y principalmente al servidor de la base de datos de desarrollo, para así minimizar los riesgos, pérdidas económicas y la poca credibilidad de los clientes de Lázaro software.

Seguidamente detectar posibles vulnerabilidades en los activos por medio de pruebas de intrusión utilizando herramientas open source con variadas características de detección y finalmente realizar la entrega de un informe detallado de las posibles vulnerabilidades encontradas en los activos de la empresa.

***Palabras clave*:** ciberseguridad, vulnerabilidades, activos

Abstract

This applied project mainly addressed the topic related to validating in an effective way the level of security of the assets of the company LAZARO SOFTWARE S.A.S in a productive environment. This project was carried out with the interest of making known that the information, operating systems, data networks and the continuous inappropriate manipulation of users, make it easier for cybercriminals who take advantage of these vulnerabilities to enter the company's network on a daily basis, hence the importance of being proactive with respect to possible intrusions, in order to limit the information leakage and manipulation of compromised assets. For this, the need arises to validate the security level of the network and mainly the development database server, in order to minimize the risks, economic losses and the low credibility of Lázaro software's clients.

Next, detect possible vulnerabilities in the assets through penetration tests using open source tools with various detection characteristics and finally deliver a detailed report of the possible vulnerabilities found in the company's assets.

Keywords**:** cybersecurity, vulnerabilities, assets

Tabla de Contenido

Introducción

El presente proyecto aplicado como opción de grado se refiere principalmente, a validar de una forma efectiva el nivel de seguridad de los activos a la empresa LAZARO SOFTWARE S.A.S en un entorno productivo.

Las características principales de este proyecto son poder aplicar, conceptos fundamentales con respecto a la disponibilidad, integridad, confidencialidad y autenticación de cada uno de los activos la empresa.

Para analizar la problemática del proyecto aplicado necesariamente se deben mencionar las causas y consecuencias; esto se da por la transformación digital que en la actualidad experimentan las empresas ya que existe mayor conectividad y acceso a mucha información, creándose así una mayor vulnerabilidad en los sistemas informáticos permitiendo así divulgación de la información confidencial por parte de los empleados de la empresa, perdida y robo de dispositivos electrónicos a cargo, empleados con malas intenciones brechas o falta de controles, por último la manipulación de personas especificas con la finalidad de obtener contraseñas perjudicando la empresa en el cese de actividades, produciendo afectaciones económicas y la pérdida de clientes.

Este proyecto se realizó con el interés de dar a conocer que la información, sistemas operativos, redes de datos y la continua manipulación inapropiada de los usuarios, faciliten a diario a que lo ciberdelincuentes aprovechen estas vulnerabilidades ingresen a la red de la compañía, por ello la importancia de ser proactivos con respecto a posibles intrusiones, con el fin de limitar la fuga de información y la manipulación de los activos comprometidos. Para ello surge la necesidad de validar el nivel de seguridad a la red y principalmente al servidor de la base

de datos de desarrollo, para así minimizar los riesgos, pérdidas económicas y la poca credibilidad de los clientes de Lázaro software.

Igualmente analizar puertos abiertos y los métodos de ingreso por parte de intrusos informáticos, implementar el uso de contraseñas en cada uno de los funcionarios de la empresa, sniffers, criptografía y el debido uso de las políticas de seguridad.

Como se verá a lo largo del desarrollo del proyecto aplicado, se vera la necesidad de bloquear a los usuarios servicios, limitación del software y el bloqueo de aplicaciones que permitan con facilidad el ingreso a la red, realizando este tipo de medidas se reduce el gran volumen las posibles vulnerabilidades al interior de la compañía. Las empresas tienen necesidades distintas, al momento de realizar este proyecto se pretende utilizar varias herramientas para detectar vulnerabilidades (Zmap, VEGA, Kaly Linux y NESSUS) las cuales son OPEN-SOURCE.

Posteriormente se estará realizando un informe que arroje las pruebas de vulnerabilidad aplicadas a la red de la empresa, con esto se quiere que el gerente de LAZARO SOFTWARE y el personal técnico tengan presente que existen diversas herramientas que brindan opciones para su uso las cuales reflejan niveles importantes de confiabilidad y así reducir las vulnerabilidades.

Cabe resaltar que cualquier proceso de aseguramiento en una empresa sea exitoso, se deben implementar políticas de seguridad robustas que exige capacitación tanto al personal encargado de la administración de los activos y a usuarios, en general que los sistemas no son en su totalidad inmunes a cualquier ciberataque, por eso la idea de implementar el proceso de detección de vulnerabilidades importante para la seguridad informática de la empresa.

Planteamiento del Problema

La transformación digital ha facilitado la vida de las personas y ha generado espacios que mejoran la funcionalidad y rendimiento de las empresas; sin embargo, esto también ha propiciado espacios para nuevas amenazas, tal como lo son los riesgos asociados a la seguridad informática, que comprometen la seguridad de los sistemas y la privacidad de la información (Prieto,2023).

Así pues, dentro de los diferentes factores de riesgo a los cuales está expuesto un sistema informático, destacan los servicios en la Nube donde se aprovechan las vulnerabilidades en los sistemas Cloud y así, se obtiene acceso a información sensible de los clientes.

Los servicios de Cloud Computing son una opción llamativa para todo tipo de empresas a nivel mundial, que desean tener sus servicios disponibles en todo momento para sus usuarios y sus aliados de negocios, pero primero en la estrategia de TI debe hacerse un análisis sobre los riesgos de seguridad que se tendrían si al dar este paso se cumplen las necesidades del negocio y están alineados con las políticas de seguridad interna de la compañía; adicional a esto se debe evaluar si se estaría preparado para asumir los nuevos riesgos que este gran paso traería consigo. No sería conveniente tomar una decisión solo pensando en costos de servicios operativos, pues las consecuencias que se llegarían a tener serian complejas (Castillo, 2015. p.2).

Por otro lado, cabe mencionar para esta problemática el bloqueo del acceso al sistema exigiendo rescate para liberar la información. En esta misma línea, el usuario es uno de los eslabones más débiles de la cadena de seguridad, siendo los correos electrónicos los medios más comunes para vulnerar los sistemas y engañar a los usuarios. Igualmente, el internet de las cosas (IoT) es otro elemento susceptible para vulnerar, ya que si estos dispositivos no se encuentran

actualizados y con una adecuada configuración pueden ser un foco para ataques dentro de la red en general (Cáceres, 2023).

Por otra parte, es importante tener en cuenta los controles tanto físicos y lógicos al interior de la empresa con respecto a la seguridad informática, puesto que se pueden identificar amenazas y tratar de minimizar las vulnerabilidades reconocidas, garantizando la confidencialidad, privacidad e integridad de la información, previniendo que los datos sean manipulados por personal no autorizado:

La seguridad de la información consiste en la preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, también pueden estar involucradas otras propiedades, como la autenticidad, responsabilidad, la confiabilidad y el no repudio (calderón, 2015, p.1).

En tal sentido, en la parte física recurrir a procedimientos de control como medidas de prevención y contramedidas pueden mitigar riesgos que atenten contra la disponibilidad de la información ante desastres naturales, sabotajes internos o externos etc. De igual forma dependiendo el grado de vulnerabilidad del sistema es posible tomar el control de la información de los usuarios cambiando y/o extrayendo las contraseñas de ingreso que supone un riesgo mayor para cualquier organización (Montes, 2014).

Es así, como en la actualidad las empresas a nivel mundial deben de tomar las medidas necesarias en aras de no ser víctimas de este tipo de delitos, donde la prevención y mitigación de riesgos informáticos es uno de los pilares que contribuye al cuidado del activo más importante de toda empresa en la actualidad, la información.

En ese orden de ideas, mencionar la importancia de realizar auditoria a los sistemas de información buscando identificar, enumerar y evaluar los controles que tengan las empresas para

así garantizar la confidencialidad, integridad y disponibilidad de la información. Este tipo de auditorías también ayudan a establecer medidas preventivas y correctivas que tengan relación con la seguridad al interior de la empresa, donde al momento de detectar algún tipo de vulnerabilidad realizar las correcciones necesarias y poder mitigar las falencias detectadas:

Con el propósito de enfrentar correctamente los procesos de auditoría y a la vez para satisfacer un adecuado nivel de control interno en las actividades de TIC, se deben diseñar controles, de manera que ellos abarquen a todos los procesos que se manejan por medio de las TIC en una organización (Salazar, 2015, p.244).

Justificación

Este proyecto aplicado tiene como finalidad realizar pruebas tanto a los activos como a la red de la empresa LAZARO SOFTWRAE, para detectar posibles vulnerabilidades, por eso nace la necesidad de que las empresas deben realizar estas pruebas periódicamente para encontrar posibles grietas en su infraestructura, fortaleciendo así las áreas expuestas a los hackers.

Estas vulnerabilidades serán realizadas recurriendo a software open source bastante eficientes en detección de puertos y aplicaciones expuestas en la red, también serán utilizados referentes bibliográficos de diferentes autores que ayuden a fortalecer el proyecto.

Hay que mencionar que las pruebas de vulnerabilidad benefician la empresa pues se mejorara la seguridad, se reducirán los riesgos y aumento de forma exponencial de la visibilidad de la postura de seguridad, llevando así a la empresa a tomar correctivos para abordar y mejorar la postura de la seguridad de la organización, reducción de la filtración de datos además de otros incidentes cibernéticos.

Todo esto, en respuesta a los riesgos que a diario las empresas en el ámbito local e internacional están expuestas puesto que existen varios tipos de amenazas, esto es causado principalmente por las acciones mal intencionadas de las personas; de allí, que nace la necesidad de realizar un adecuado análisis de las vulnerabilidades en todas y cada una de las áreas de la empresa obteniendo así un panorama general del estado de está buscando estabilidad y seguridad.

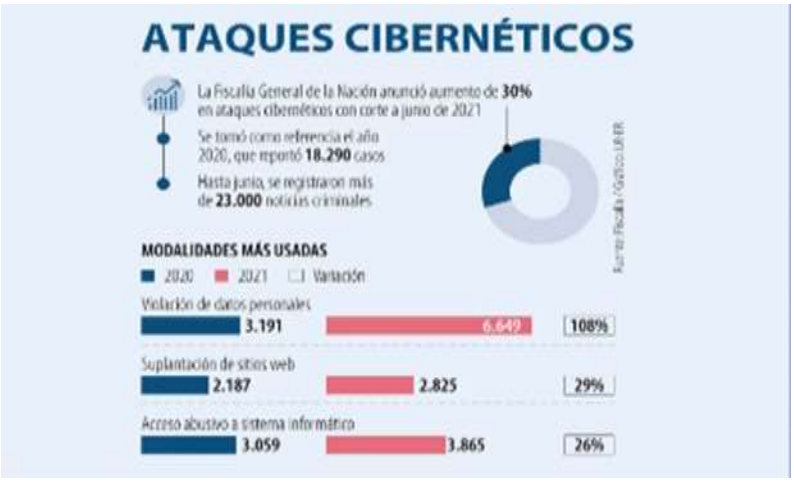
Así pues, según el reporte “Reforzando la Resiliencia en Ciberseguridad”, hoy los ciberataques figuran como el riesgo "más relevante desplazando al narcotráfico," con pérdidas que podrían alcanzar a nivel global los US$ 24 billones (millones de millones) a 2027, equivalente al Producto Interno Bruto (PIB) de todo Estados Unidos (según WTW 2023).

Los sectores más afectados son el financiero con un (35%), seguido por grupos empresariales (27%), el legal (14%), Gubernamental (11%) y por último el sector educativo (8%), la mayor herramienta utilizada por los ciberdelincuentes es el ransomware (secuestro de información). (según diario La república 2023).

Con respecto a los ataques cibernéticos a nivel nacional, aumentaron en un 30% durante el primer semestre del presente año según la fiscalía. Siendo Bogotá la mayor afectada con 8.355 casos, Antioquia 1.664 y Cali con 1.569 incidentes tal como se ilustra en la Figura 1.

Figura 1

Ataques cibernéticos con corte a junio de 2020



Fuente: Fiscalía (2020)

Por otro lado, cuando se refiere a las modalidades mas usadas para la realización de estos ataques cibernéticos en primer lugar, aparece la violación de datos personales con 108%, posteriormente suplantación de sitios web el 29%, para terminar el acceso abusivo a sistema informático 26% tal como se ilustra en la Figura 2.

Figura 2

Modalidades más usadas para realizar ataques cibernéticos junio de 2021

Fuente: Fiscalía (2021)

Paralelamente, los datos a nivel mundial según tasa de cibercriminalidad en el año 2022 por cada millón de usuarios de internet, afirma que el Reino Unido se encuentra en la cima con 4371 casos, las menores proporciones España con 11 tal como se ilustra en la Figura 3.

Figura 3

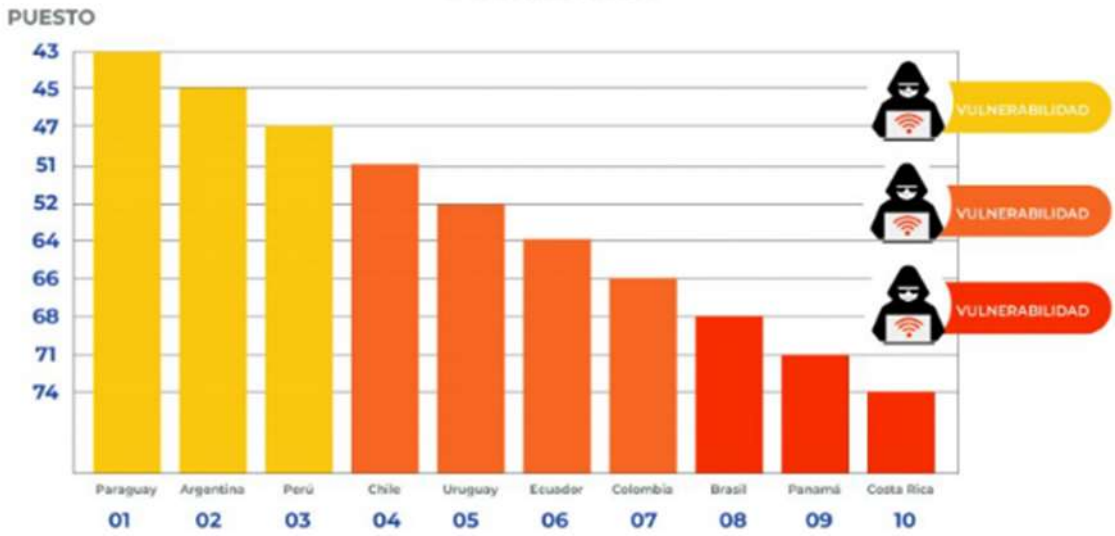
Tasa de cibercriminalidad en 2022

Fuente: Surfshark (2022)

Para terminar, evidenciar que en Colombia según datos estadísticos se ubica según el ranking mundial en el puesto 66 siendo la principal causa la falla masiva y fuga de información en instituciones de salud y bancarias tal como se ilustra en la Figura 4.

Figura 4

Capacidad Seguridad Cibernética



Fuente: NCSI

Objetivos

Objetivo General

Medir el nivel de exposición y posibles vulnerabilidades existentes en la red corporativa de la empresa LAZARO SOFTWARE S.A.S, por medio de la ejecución de metodologías de intrusión que permitan evidenciar el estado actual de la seguridad en la entidad.

Objetivos Específicos

Establecer los activos de información objeto de análisis red local y servidor DDNS.

Examinar las diferentes herramientas open source de análisis de vulnerabilidades disponibles para auditar los activos de la organización mediante un comparativo de ventajas y desventajas que permitan perfilar su utilización.

Evaluar la seguridad de los activos de información mediante la ejecución de pruebas de vulnerabilidad siguiendo metodologías de testing e intrusión.

Proponer acciones de mejora a partir del resultado obtenido en las diferentes pruebas realizadas a los activos de la empresa Lázaro Software S.A.S, para obtener como resultado un alto impacto en la seguridad de la empresa LAZARO SOFTWARE S.A.S.

Marco Teórico

En el campo de la informática el termino vulnerabilidad se refiere explícitamente, “debilidad existente en un sistema que puede ser utilizada por una persona malintencionada”. Estas se pueden dar de varias formas como por ejemplo de tipo hardware, software, procedimentales o humanas donde puede ser explotadas o utilizadas por intrusos o ciber atacantes (B. Santander, 2012).

Cuando se refiere al termino vulnerabilidad se mencionará a continuación algunos ejemplos como:

- Un servicio de un sistema de computación corriendo en un determinado puerto lógico.
- Sistemas y aplicaciones no actualizados o parcheados que presentan múltiples vulnerabilidades.
- Una red Wifi abierta.
- Un puerto abierto en un firewall.
- Un insuficiente o inexistente control de acceso físico a las instalaciones.
- La no aplicación de una política de gestión de contraseñas.

Posteriormente, al referenciar el termino vulnerabilidad implica una amenaza al sistema. Por ende, también existe un riesgo, definiendo la amenaza es una violación de la seguridad en potencia existente a partir de unas circunstancias, capacidad, acción o evento que pueda llegar a causar una infracción de la seguridad y/o causar algún tipo de daño en el sistema. Por otro lado, al referirse al riesgo es una expectativa de perdida expresada como la probabilidad de que una amenaza particular explote una vulnerabilidad particular con resultados especialmente perjudiciales (Navarro, 2012).

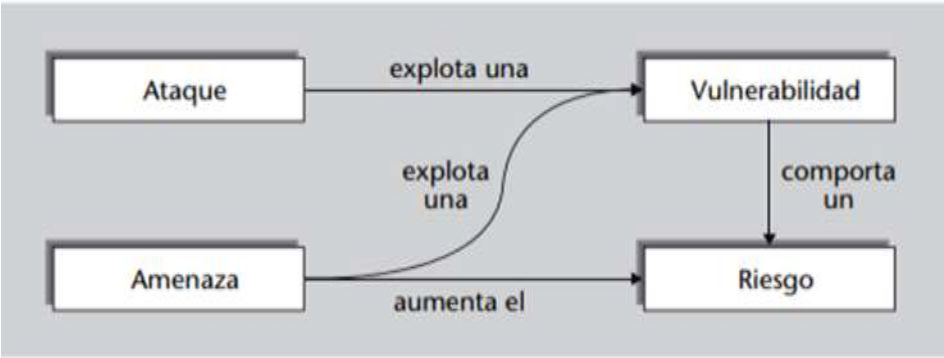
Con respecto, a la seguridad informática esta inicia a partir de la existencia de vulnerabilidades relativas en los sistemas de información. Una vulnerabilidad a nivel general no tendría ningún fin si luego de existir no pudiese ser explotada por un atacante con el objetivo principal de violentar la seguridad del sistema.

Una vulnerabilidad de seguridad es un fallo o debilidad en el diseño, la implementación, la operación o la gestión de un sistema, que puede ser explotado con el fin de violar la política de seguridad del sistema (Navarro, 2012, p.8).

Esta Finalmente, hay que referirse a la importancia de la seguridad informática y el de evaluar el riesgo asociado a un servicio o sistema. Seguidamente este riesgo suele ser directamente proporcional a la existencia de vulnerabilidades y amenazas. Por otra parte, hay que tener en cuenta que no siempre a mayor número de vulnerabilidades mayor es el riesgo asociado a un sistema, el riesgo también vendrá determinado por la criticidad o gravedad de la vulnerabilidad tal como se ilustra en la Figura 5.

Figura 5

Conceptos de Seguridad



Fuente: Elaboración Propia

Luego para el tema de identificar vulnerabilidades, existen identificadores únicos que impiden que sean difundidos, duplicados y facilitan la posibilidad de hacer referencia a

vulnerabilidades concretas. El sistema de documentación más relevante a escala internacional es el CVE (Common Vulnerabilities and Exposures). Se presenta como un estándar de nombres de vulnerabilidades de seguridad informática de uso gratuito y público.

Seguidamente para etiquetar una vulnerabilidad en el CVE, se debe seguir el siguiente procedimiento:

- Se descubre una vulnerabilidad.
- Se le asigna un identificador CVE con el estado candidato. Esta asignación la hace un CVE Candidate Numbering Authority (CNA), que son los principales fabricantes de software y hardware, así como organizaciones y empresas del sector, autorizados por CVE.
- La vulnerabilidad se publica en la página web de CVE y se propone al consejo editor de CVE su aprobación.
- El consejo editor decide mediante votación si acepta la vulnerabilidad, con lo que pasa a estado entry y se añade a la lista de CVE, o si por el contrario se desestima.

Según CVE, una vulnerabilidad es un estado de un sistema informático que cumple alguno de los siguientes casos:

1. Permitir a un atacante ejecutar comandos como otro usuario.
2. Permitir a un atacante acceder a datos violando las restricciones de control de acceso específicas para dichos datos.
3. Permitir a un atacante suplantar a otra entidad.
4. Permitir a un atacante llevar a cabo una denegación de servicio.

Bases de datos de Vulnerabilidades:

- The Open Source Vulnerability Database (OSVD): Base de datos de código abierto creada de modo independiente, que esta gestionada por la organización sin ánimo de lucro OSF.
- National Vulnerability Database (NVD): Base de datos perteneciente al gobierno de Estados Unidos de acceso público.
- SecurityFocus Vulnerability Database: Base de datos mantenida por la empresa Symantec. Esta también dispone de la lista de distribución BugTraq, que llego a ser el principal canal de difusión de vulnerabilidades en los años noventa.
- Exploit DB: Esta base de datos de vulnerabilidades tiene la particularidad de que, además de publicar las vulnerabilidades, publica los exploits correspondientes. Son programas o scripts que permiten explorar dicha vulnerabilidad, programas que permiten realizar un ataque que se aproveche de la vulnerabilidad.

PTEST ((Penetration Testing Execution Standard): El estándar de ejecución de pruebas de penetración está enfocado hacia la auditoría de sistemas permitiéndole a las empresas y los proveedores de servicios de seguridad tener un mismo lenguaje (Fernández, 2023, p.20).

Etapas de la metodología PTES:

- Interacciones previas al compromiso: En esta se plantean los preacuerdos con el cliente donde se expondrán los alcances de la prueba de penetración, las herramientas a usar y los resultados esperados.
- Recopilación de información: Se establecerá los mecanismos para recopilar la información de la empresa a realizar la prueba, se utilizará información pública y la que pueda dar el cliente y la que por medio de otros métodos podamos extraer de los empleados.

- Modelado de amenazas: Se planifica el ataque de acuerdo con la información obtenida en los pasos anterior. Este estándar no requiere la utilización de un modelo específico, por lo que de acuerdo con las características de la empresa se van definiendo, teniendo en cuenta que este esté dentro de los parámetros establecidos por este estándar, centrándose en el modelado de amenazas activos y atacante.
- Análisis de vulnerabilidades: En este proceso se descubre las vulnerabilidades de ciberseguridad de los sistemas auditados que puedan ser explotadas por un atacante. De acuerdo con lo pactado se realiza las pruebas: permisividad de ataques, enfoque o tipo de la prueba, presentación de evidencias recolectadas.
- Explotación: Teniendo las vulnerabilidades analizadas, se procede al ingreso al sistema saltando las seguridades existentes. Con esto se podrá identificar un punto por donde el atacante podrá tener el acceso.
- Informes: Se entrega un informe ejecutivo y técnico al responsable del área
- de sistemas en un lenguaje fácil de entender, dando solución a los problemas
- planteados al inicio de la prueba. Se informará de las contramedidas que
- puedan ser aplicadas para mitigar los riesgos encontrados durante la prueba.

Para lograr el desarrollo de este proyecto aplicado para detectar posibles vulnerabilidades al interior de la empresa LAZARO software se ha seleccionado la metodología PTES para realizar dicha prueba.

La metodología PTES fue creado en 2009 por seis consultores de seguridad informática que, tras encontrar problemas recurrentes en las pruebas de penetración, crearon un estándar para ayudar a los clientes y a los especialistas de ciberseguridad con herramientas, técnicas y elementos que les permitieran realizar una prueba de penetración o intrusión de forma

generalizada. Lo cual es ideal para su aplicación en la empresa de estudio de este trabajo. PTES al ser una reciente metodología de pruebas de penetración, su uso es algo limitado, sin embargo, se ha venido adelantando desde el área de la academia investigaciones de su aplicabilidad en las empresas colombianas como es el caso del proyecto aplicado “Aplicación de la metodología PTES en la clínica Medellín para la identificación de vulnerabilidades en historia clínica electrónica” donde a través de la metodología propuesta se adelanta el análisis de vulnerabilidades con el fin de aumentar la ciberseguridad de la empresa de estudio. Teniendo en cuenta lo anterior y la gran importancia de que la seguridad de la información para la continuidad de los negocios tiene, se hace muy pertinente la metodología PTES con miras de fortalecer los niveles de ciberseguridad en las empresas (Fernández, 2023 p.22).

Marco Conceptual

Conocer un término relacionado con pruebas de vulnerabilidad informática permite identificar las causas que posiblemente son generadas, y además al interior de la empresa admiten crear métodos de prevención y mitigación de intrusiones a los activos, fortaleciendo así los puntos débiles relacionada con robo de información, inhabilitación de la base de datos, bloqueos en el sistema. Por lo anterior, es necesario realizar una corta descripción de los principales conceptos asociados al tema análisis de amenazas y vulnerabilidades.

Seguridad Informática: Es la disciplina que, con base en políticas y normas internas y externas de la empresa, es la encargada de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenaza, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta para que un sistema sea lo suficientemente sea fiable debe contener las siguientes propiedades (Urbina, 2016).

Efectividad: Se trata de lograr que la información sea en realidad la necesaria para desarrollar cualquiera de las tareas que se desarrollan en la empresa u organización y sea adecuada para realizar los procesos del negocio, proporcionando de manera oportuna, correcta, consistente y accesible.

Eficiencia: Significa que la información sea generada y procesada utilizando de manera óptima los recursos que tiene la empresa para este fin.

Confidencialidad: Se refiere principalmente a que, en todas las etapas del procesamiento de la información, esta se encuentre protegida contra accesos no autorizados, los cuales pueden derivar en la alteración o robo de información confidencial.

Integridad: Significa que la información que se recibe sea precisa y este completa para los fines que se persiguen con su procesamiento, así como su validez, de acuerdo con los valores y las expectativas del negocio.

Disponibilidad: Hace referencia a que la información necesaria para para realizar cualquiera de las etapas del proceso administrativo este a la mano cuando sea requerida por los procesos del negocio en cualquier momento.

Apego a estándares: Significa principalmente que en el procesamiento de la información se deberán acatar leyes de uso general o reglamentos y acuerdos internos y contractuales a los cuales está sujeto el proceso de negocios.

Confiabilidad: la información no haya sido alterada inapropiadamente.

Tipos de Ataques: En primer lugar, definir como un ataque cibernético al intento programado e intencionado que tiene como fin explotar algún tipo de vulnerabilidad o debilidad en los activos informáticos, tanto en el hardware o software, seguidamente esto se da con el objetivo de recaudar un beneficio económico o simplemente causar algún tipo de caos al interior de las organizaciones los ataques más comunes serán mencionados a continuación (Fortinet, 2023).

-Malware: Software malicioso cuyo principal objetivo es infiltrarse en un sistema para destruirlo (gusanos, Troyanos).

-Virus: Es una combinación que infecta de forma directa los archivos del sistema mediante un código maligno, para que esto suceda debe necesariamente el usuario ejecutarlo, posteriormente entre en funcionamiento se esparce por todo el sistema donde todo elemento al que la cuenta de usuario tenga acceso como dispositivos de hardware, unidades virtuales e incluso ubicaciones remotas en la red.

-Gusanos: Programa que una vez ingresa e infecta el equipo de cómputo, realiza copias de si mismo y las esparce por la red (se transmiten por las redes o correo electrónico). Su detección no es fácil no afectan el sistema, pero se recomienda utilizar soluciones tipo XDR, tipo de monitoreo de la red y equipos en búsqueda de comportamientos anómalos.

-Troyanos: Tienen similitud con los virus, pero persiguen objetivos diferentes cuando se refiere al virus este su función principal es la de destruir por otro lado, el troyano su objetivo es abrir una puerta trasera para el ingreso de otros programas maliciosos (Caballo de Troya), pasar desapercibido e ingresar al sistema sin ser detectado como una amenaza potencial.

-Spyware: Programa espía para obtener información es decir recolectan información de los dispositivos e instalan programas sin que el usuario se de cuenta.

-AdWare: Muestran publicidad de forma invasiva su misión es la de recolectar y transmitir información de datos para el estudio del comportamiento de los usuarios y así poder orientar la publicidad.

-Ransonware: Es una especie de programa maligno ya que secuestra la información (Encripta) para después pedir rescate. Los principales son: REvil, LockBit, Conti, Maze, Petya.

-Doxing: Es una práctica en internet de investigación y publicación privada sobre una persona o una organización con la finalidad de intimidar, humillar o amenazar.

-Phishing: Técnica de Ingeniera Social como es la de suplantación de identidad, con la finalidad de obtener datos privados de la víctima, como contraseñas o datos bancarios. Los principales medios de recolección de este tipo de información son el correo electrónico, mensajería o llamadas telefónicas. Este método a la fecha es uno de los mas habituales dirigido principalmente a miembros de una empresa, mediante una practica llamada spear fishing (hurtar la identidad) a una persona seleccionada por su alto nivel de vulnerabilidad.

-Denegación de servicio distribuido (DDoS): Estos ataques consisten en realizar repetidas peticiones a un servidor, hasta que colapse y deje de funcionar de todos los ataques este es el mas utilizado ya que es económica su ejecución y muy difícil de rastrear al atacante. Su eficiencia radica en que no supera las medidas de seguridad que protegen un servidor, ya que no intentan penetrar en su interior solo bloquearlo.

-Injection SQL o SQL Injection: su principal objetico son las aplicaciones web como los campos de formularios de acceso, registro o búsqueda que explota los errores y vulnerabilidades de una página web, se utiliza para acceder a las bases de datos y robar, manipular, destruir información.

-Whaling o "caza de ballenas": sus ataques son dirigidos a perfiles C-Level (CEO, CMO, CFO, CIO) para robarles credenciales de alto nivel.

Prueba de intrusión o Pentesting: Una de las definiciones es la dada por la NIST "Prueba de seguridad donde los evaluadores imitan los ataques del mundo real en un intento de identificar formas de eludir las características de seguridad de una aplicación, sistema o red. Las pruebas de penetración a menudo implican la emisión de ataques reales a sistemas y datos reales, utilizando las mismas herramientas y técnicas que utilizan los atacantes reales" (Fernández, 2023 p.23).

Tipos de Pruebas de intrusión Text White box (Caja Blanca): Es un método bastante largo con el que más profundo se puede llegar a tener resultados, pero los costos son más elevados. Tiene la misión de probar cada servicio, verificación de la configuración, posibles vulnerabilidades y hacen una revisión completa para garantizar el blindaje.

Text grey box (Caja Gris): El consultor solo puede tener cierta cantidad de información, donde puede llegar un poco más lejos que con las pruebas realizadas con el escaneo de caja negra.

Text black box (Caja Negra): Método con resultados reales, donde la persona que realiza esta prueba no posee información acerca de la empresa donde simula un vector de ataque para detectar algún tipo de vulnerabilidad para poder ser explotada.

Metodologías de intrusión Es aquel conjunto de fases documentales que necesariamente se deben cumplir el propósito de analizar la seguridad de la información de los activos, con el cual se busca penetrar una infraestructura para así posiblemente encontrar vulnerabilidades.

Metodología

Este proyecto aplicado está orientado principalmente a detectar las posibles vulnerabilidades existentes en los activos informáticos de la empresa LAZARO SOFTWARE, la cual es una empresa netamente Tolimense con 20 años en el mercado donde se dedica principalmente a desarrollar soluciones informáticas eficientes. Sus principales productos como Ventas e Inventarios Contable y Financiero, Talento Humano y servicios Adicionales se destacan por su flexibilidad y calidad. Por otra parte, para la evolución del proyecto se planeó un enfoque cuantitativo utilizando herramientas de análisis que posteriormente evidencian cuales son los equipos que están sujetos a un ataque por parte de ciberdelincuentes, para la realización de las pruebas de vulnerabilidad se tendrá en cuenta la Metodología PTEST.

Penetration Testing Execution Standard (PTEST), es el marco diseñado para realizar pruebas de penetración o pentesting llamadas también auditorias técnicas de seguridad. Finalmente hay que afirmar que esta metodología surgió de la necesidad de controlar vulnerabilidades en entidades financieras, proveedores de servicios y de seguridad.

La puesta en marcha de esta metodología se ilustra en la Figura 6.

Figura 6

Metodología PTEST

METODOLOGIA PTEST		
INTERACCIONES PREVIAS	DESCRIPCION GENERAL	Se explica sobre las herramientas tecnologicas y tecnicas a utilizar para realizar las pruebas de vulnerabilidad
	INTRODUCCION AL ALCANCE	Explicacion del objetivo de la prueba
	METRICAS PARA ESTIMULACION DEL TIEMPO	Se definen tiempos en los cuales se realizaran las pruebas de intrusion
	REUNION DE ALCANCE	Donde se firma el documento de confidencialidad
	CUESTIONARIOS	Se realiza entrevista el gerente de la empresa LAZARO SOFTWARE con la finalidad de conocer sobre la estructura organizacional y el administrador del sistema sobre la infraestructura tecnologica

METODOLOGIA PTEST		
RECOLECCION DE INFORMACION	RECOPILACION DE INFORMACION	Se emplea la recopilacion de informacion de nivel 2 la cual cuenta con herramientas de deteccion de vulnerabilidades como:Namp,VEGA,KALY LINUX,TENABLE NESSUS.
	CORPORATIVO	Direccion Fisica y Representante legal
	ORGANIGRAMA	Se identifica la estructura de la empresa y de las personas importantes dentro de la organización (Desarrolladores de Software).
	ACTIVOS DE INFRAESTRUCTURA	Direeciones IP , direcciones de correos electronicos de funcionarios
	HUELLA ACTIVA	escaneo de puertos
	IDENTIFICACION DE MECANISMOS DE PROTECCION	Activos de la empresa LAZARO SOFTWARE

Fuente: *Elaboración Propia*

Fase 1 Reunión previa con el gerente de la empresa Lázaro software para realizar una explicación detallada de cuál es la finalidad y los alcances del proyecto aplicado, técnicas y herramientas tecnológicas a utilizar.

Fase 2 Identificación de la estructura organizacional en la empresa Lázaro Software y nivel de importancia al interior, seguidamente la dirección física de los equipos de cómputo objetivo para la realización de las pruebas de vulnerabilidad.

Fase 3 Ejecución de las pruebas de vulnerabilidad principalmente al area de desarrollo y servidor de base datos.

Fase 4 Posteriormente para la detección de las posibles vulnerabilidades al interior de LAZARO SOFTWARE, se utilizarán herramientas open source como:

1.1 NMAP (Zenmap) la puesta en marcha de esta herramienta permitirá escanear que rango de puertos se encuentran abiertos y se deberán cerrar para evitar ingreso de intrusos además de posibles virus, se ejecuta bajo la plataforma Windows, LINUX y OSX.

1.2 VEGA SUBGRAPH su principal función es la de realizar un escaneo a fondo de seguridad de páginas y aplicaciones WEB. Al mismo tiempo encuentra y valida inyección en el lenguaje SQL, secuencias de comandos entre sitios (XSS).

1.3 reNgine herramienta para un reconocimiento optimizado y configurable a través de motores y monitoreo continuo el cual es respaldada por una base de datos y una interfaz de usuario fácil de reconocer su forma de ejecución es bajo la plataforma Linux Ubuntu.

Fase 5 Para la prueba de intrusión utilizar KALY LINUX (Metasploit) Herramienta bastante importante, donde se realizarán pruebas de penetración, Escaneó y recopilación de información, identificación y exploración de vulnerabilidades, escalada de privilegios, instalación de backdoors (extracción de información), Fuzzing.

Fase 6 Recolección de la información de cada una de las pruebas realizadas tanto al area técnica, soporte y Desarrolladores para detectar la cantidad de puertos y posibles vulnerabilidades detectadas.

Fase 7 Realización de la respectiva entrega del informe técnico detallado especificando claramente como será el proceso de recolección de los resultados obtenidos en cada una de las fases del proyecto.

Instrumentos Para la realización del proyecto se implementarán pruebas de vulnerabilidad mediante diferentes softwares (open source), el cual permitirá detectar posibles vulnerabilidades y debilidades con respecto a la seguridad de la información al interior de la empresa LAZARO SOFTWARE, todo esto con el fin de lograr evitar accesos no permitidos y escalamiento a los sistemas operativos, para este tipo de pruebas se utilizará:

Zenmap “Zenmap es la Nmap Security Scanner GUI oficial. Es una multiplataforma (Linux, Windows, Mac OS X, BSD, etc.) la aplicación gratuita y de código abierto que tiene como objetivo hacer Nmap fácil de usar para principiantes mientras que proporciona características

avanzadas para los usuarios de Nmap experimentados. Frecuentes exploraciones utilizadas se pueden guardar como perfiles para que sean fáciles de ejecutar repetidamente. Un creador de comandos permite la creación interactiva de líneas de comandos de Nmap. Los resultados del análisis se pueden guardar y ver más tarde. Los resultados del análisis guardado se pueden comparar entre sí para ver qué tan diferente. Los resultados de las exploraciones recientes se almacenan en una base de datos (Gordon, 2015).

VEGA “Subgraph Vega permite introducir una URI para escanear, en este caso, para este caso usaremos la página de LAZARO SOFTWARE” es un escáner de Vulnerabilidades de código abierto para probar la seguridad de aplicaciones web, en la cual puede ayudarle a encontrar y validar las Inyecciones SQL, Cross-Site Scripting (XSS), Shell Injection, Local File

Inclusión, Integer Overflow y otras vulnerabilidades. Está programada en Java y basado en una interfaz gráfica por la cual se puede ejecutar en Linux, OS X y Windows.

Vega incluye un escáner automatizado para pruebas rápidas y también un Proxy para proteger nuestra IP cuando realizamos alguna auditoria web.

Vega fue desarrollado por Subgraph en Montreal. Actualmente esta herramienta viene incorporada en el BackTrack a partir de la versión R1 y R2.

KALY LINUX

Kali Linux es una distribución de Linux basada en Debian, específicamente diseñada para temas de seguridad muy variados, como análisis de redes, ataques inalámbricos, análisis forenses y otros que más adelante citaremos. Contiene herramientas para llevar a cabo todas estas pruebas de seguridad y análisis.

Fue desarrollado en base a la reescritura de BackTrap, otra distribución de Linux para semejantes usos, por Mati Aharoni y Devon Kearns de Offensive Security.

Kali Linux se encuentra entre las distribuciones de seguridad de Linux más usadas, ya que es una de las mejores, tanto para uso personal como profesional, proporcionando a los usuarios paquetes de herramientas como Foremost, Wireshark, Maltigo as-Aircrack-ng, Kismet y más" (Altube, 2021).

reNgine es una herramienta de reconocimiento muy completa que puede resultar muy útil para centralizar todo su reconocimiento en un solo sitio.

Resultados

Fase 1. Exposición del proyecto aplicado en la oficina del Gerente Lázaro Humberto Jaramillo Duque, donde de forma detallada se le expone cual era la finalidad de la actividad a realizar durante el periodo académico los acuerdos, autorización, herramientas tecnológicas y el alcance. Se definió la realización de las pruebas de vulnerabilidad, además de una prueba de intrusión (pentest), seguidamente auditar los equipos del area técnica donde se brinda soporte al software UNICO, servidor bases de datos clientes y desarrolladores del aplicativo como se ilustra en la Figura 7.

Figura 7. *Reunión con el Gerente. Autor Jeobany Ramos*

Fase 2. En esta fase con respecto a la estructura interna, está compuesta por Gerencia, Area de desarrollo, soporte técnico a usuarios del programa UNICO, soporte de hardware y software, Contabilidad y Recepción, en relación al proveedor ISP cuenta con los servicios de Movistar y Tigo, con respecto a los dispositivos de conexión a la red lógica en su rack principal encontramos instalado y configurado una Mikrotik RB2011UiAS-IM Multi-port Router con 1 puerto Sfp Plus de 10 puertos y un switch qpcom de 16 puertos como se ilustra en la Figura 8.

Figura 8. *Rack principal. Autor Jeobany Ramos*

Mikrotik RouterOS el software de este dispositivo ofrece principalmente gran flexibilidad para su configuración, con amplias posibilidades de actualización su funcionamiento es exactamente igual que un router, pero con costos significativamente inferiores. Además, permite aplicaciones de seguridad de gestión y Control (Anrrango, 2014).

Por otro lado, se evidencia la configuración de una VLAN (redes lógicas independientes dentro de una red física), para el area donde se encuentra el servidor base de datos clientes y desarrollador administrador del Software UNICO. La ip de configuración del servidor asignada es 192.168.1.x y la del equipo desarrollador 192.168.1.x como se ilustra en la Figura 9.

Figura 9. *Area de Desarrollo y servidor BD. Autor Jeobany Ramos*

Finalmente, hay que afirmar que en la otra sección de la VLAN se encuentra configurada, un area también de suma importancia para la empresa LAZARO software como es el soporte técnico a los clientes del software UNICO los cuales tienen asignada las ip 192.168.1.x y 192.168.1.x respectivamente como se ilustra en la Figura 10.

Figura 10. *Area Soporte clientes software UNICO. Autor Jeobany Ramos*

Fase 3: Modelado de amenazas

En esta fase se realizó la detección de puertos abiertos con el único propósito de que puedan ser utilizados para llevar a cabo un ataque al interior de la empresa. Se empleó una de las herramientas más usadas en temas seguridad informática de software libre llamada KALY LINUX, ya que esta es una de las mejores tanto para uso personal como profesional.

En primer lugar, se realizó el proceso de escaneo con el servidor de base de datos ip:192.168.1.x, con sistema operativo Windows server 2016 el cual reporto 16 puertos abiertos como se ilustra en la Figura 11.

Sudo Nmap -O 192.168.1.x/24

Figura 11. Escaneo puertos abiertos Servidor BD. Autor Jeobany Ramos

Figura 11. *Escaneo puertos abiertos Servidor BD. Autor Jeobany Ramos*

Posteriormente, se le realizo el escaneo al equipo del profesional en desarrollo de software ip:192.168.1.x, sistema operativo Windows 10 revelando 9 puertos abiertos como se ilustra en la Figura 12.

```
Nmap scan report for 192.168.1.5 (Cristian Molina)
Host is up (0.0031s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
7070/tcp open  realserver
MAC Address: 74:D4:35:2F:DB:CF (Giga-byte Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10|2019 (90%)
OS CPE: cpe:/o:microsoft:windows_10
Aggressive OS guesses: Microsoft Windows 10 1909 (90%), Microsoft Windows Server 2019 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

Figura 12. *Escaneo puertos Desarrollador Software UNICO. Autor Jeobany Ramos*

Paralelamente se le realizo el mismo escaneo para detectar puertos abiertos a los dos equipos de soporte técnico 1 a usuarios del programa UNICO ip:192.168.1.x sistema operativo Windows 10 arrojando una cifra de 6 puertos abiertos como se ilustra en la Figura 12.

```
Nmap scan report for 192.168.1.8
Host is up (0.0034s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
7070/tcp open  realserver
MAC Address: 74:27:EA:30:E6:84 (Elitegroup Computer Systems)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10|XP (91%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows Server 2019 (91%), Microsoft Windows 10 1909 (90%), Microsoft Windows XP SP3 (85%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

Figura 14. *Escaneo puertos abiertos Soporte 2. Autor Jeobany Ramos*

Para terminar con los escaneos de puertos también hace parte de los activos de la empresa y de uso constante por los empleados la impresora JET DIRECT marca HP LASERJET ip:192.168.1.x, arrojando una cifra de 3 puertos abiertos como se ilustra en la Figura 15.

```
Nmap scan report for 192.168.1.6
Host is up (0.0029s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
515/tcp   open  printer
631/tcp   open  ipp
5200/tcp  open  targus-getdata
9100/tcp  open  jetdirect
10001/tcp open  scp-config
MAC Address: 30:CD:A7:A6:7A:00 (Samsung Electronics)
Device type: printer
Running: HP embedded
OS CPE: cpe:/h:hp:laserjet_cp4525 cpe:/h:hp:laserjet_m451dn
OS details: HP LaserJet M451dn, CM1415fnw, or CP4525
Network Distance: 1 hop
```

Figura 15. *Escaneo puertos abiertos Impresora. Autor Jeobany Ramos*

Fase 4: Herramientas utilizadas para el desarrollo de los escaneos.

La primera herramienta VEGA SUBGRAPH bastante importante para escaneo de vulnerabilidades en páginas web, inicialmente se le dio clic derecho al icono con un “+” situado en la parte superior izquierda como se muestra en la Figura 16.

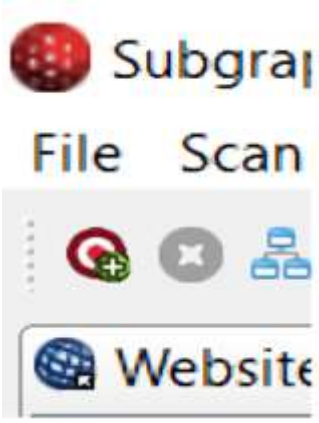


Figura 16. *Inicio ejecución del programa. Autor Jeobany Ramos*

A continuación, se digita la dirección ip o la URL como se muestra en la Figura 17.

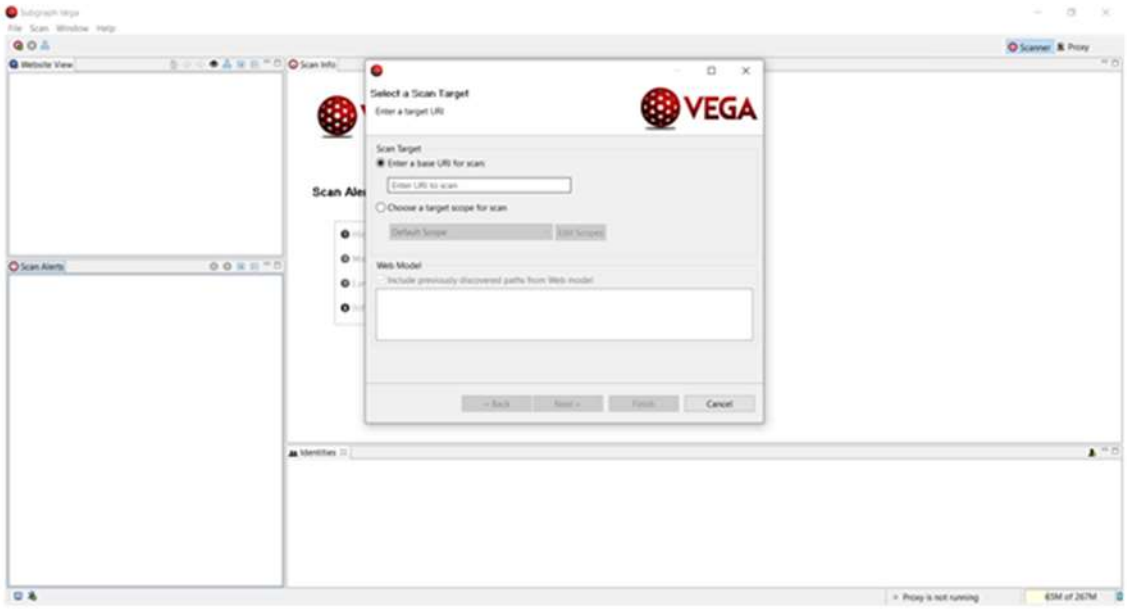


Figura 17. *Sitio Web Lázaro Software. Autor Jeobany Ramos*

Finalmente, el resultado de escaneo del sitio web de LAZARO software se encontró un tipo de vulnerabilidad MEDIA como se muestra en la Figura 18.

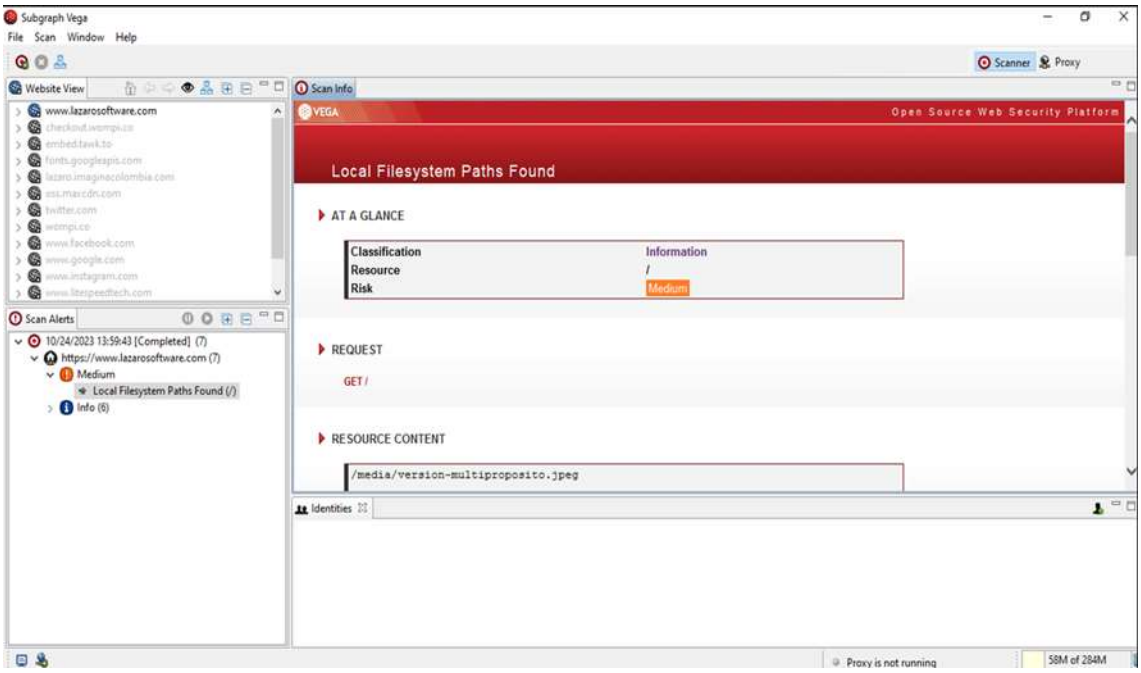


Figura 18. *Resultado del escaneo sitio WEB. Autor Jeobany Ramos*

Zenmap esta herramienta se empleó principalmente para el escaneo de la ip publica Office-server.ddns.net (181.129.223.154) como se ilustra en la figura 19

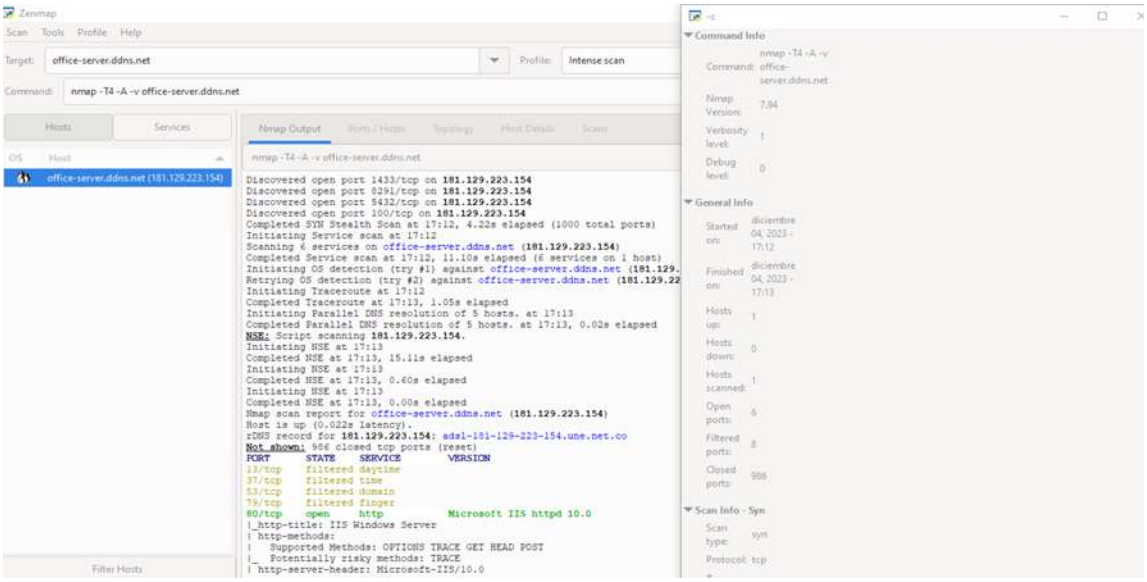


Figura 19. *Resultado del escaneo ip pública. Autor Jeobany Ramos*

Como resultado de la ejecución de esta importante herramienta no se detectaron vulnerabilidades como se muestra en la Figura 20.

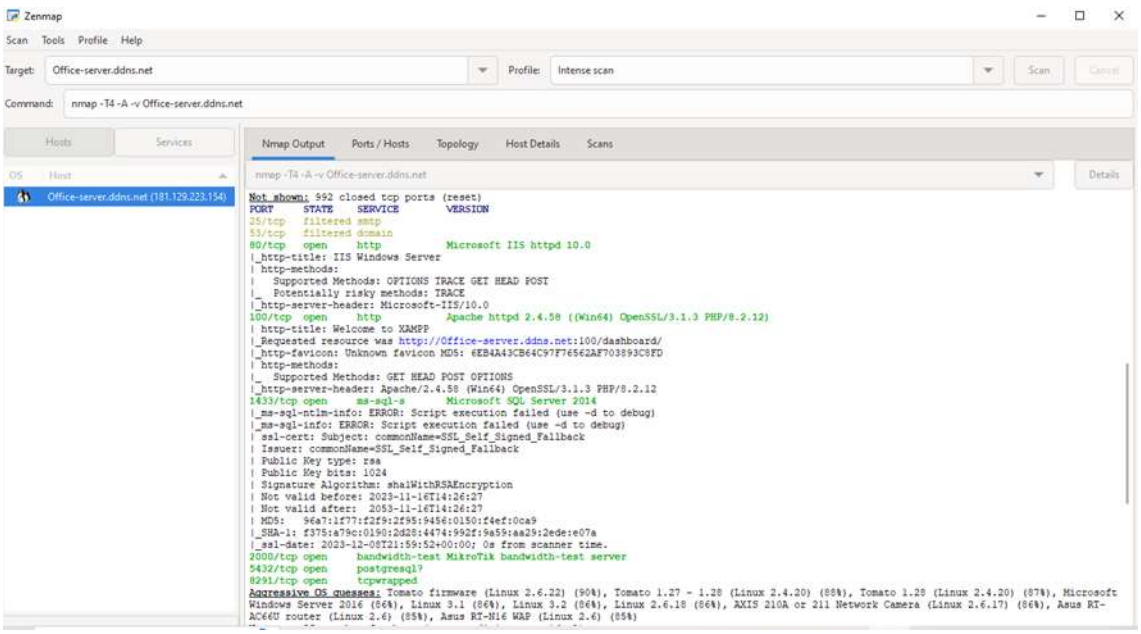


Figura 20. *Resultado del escaneo. Autor Jeobany Ramos*

Por último, en cuanto se refiere a los Host el protocolo smtp transferencia de correo electrónico se encuentra filtrado evitando así el ingreso de algún tipo de ataque de phishing como se ilustra en la Figura 21.

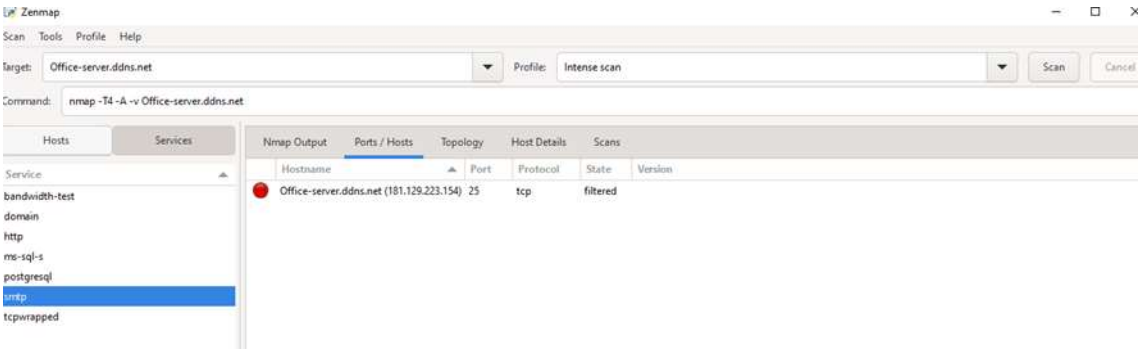


Figura 21. *Puerto smtp Filtrado. Autor Jeobany Ramos*

ReNgine. Para la realización de este procedimiento se utilizó la herramienta virtual (VirtualBox), donde se instaló el sistema operativo UBUNTU para realizar la conexión remota a la página web de escaneo 192.168.1.x esto se realizó con la finalidad de centralizar las pruebas de escaneo como se muestra en la Figura 22.

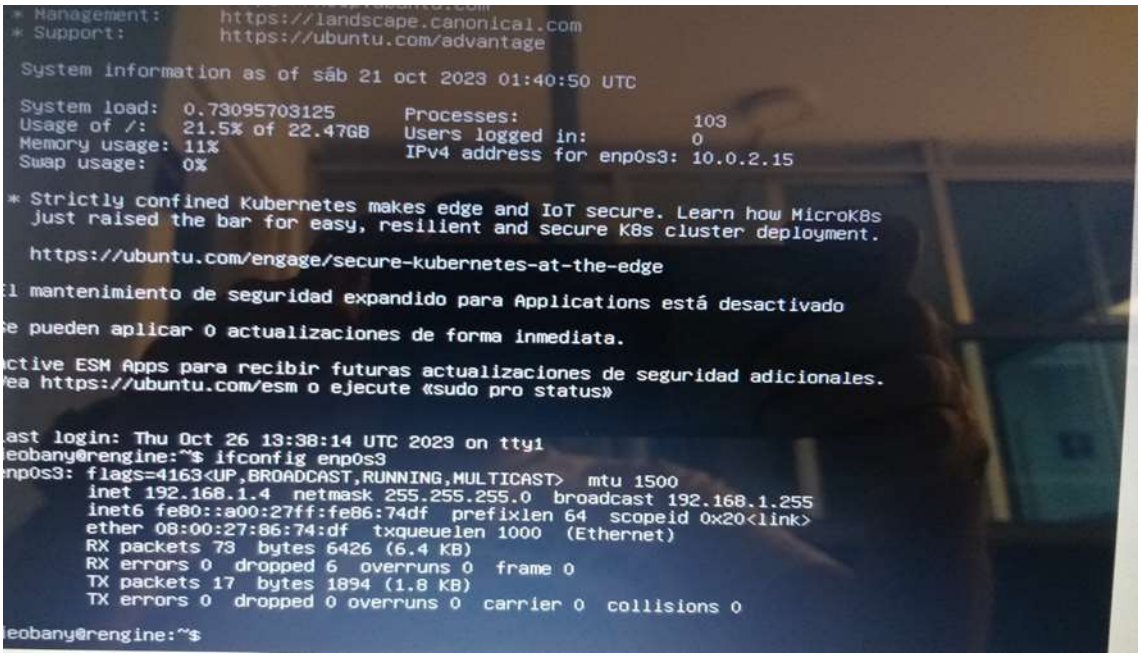


Figura 22. *Conexión remota al equipo de escaneo. Autor Jeobany Ramos*

En primer lugar, se le realizaron las pruebas de escaneo a los equipos objetivo servidor bases de datos digitando ip en la opción de Targets y en el transcurso del día evidencio vulnerabilidades 0 como se ilustra en la Figura 23.

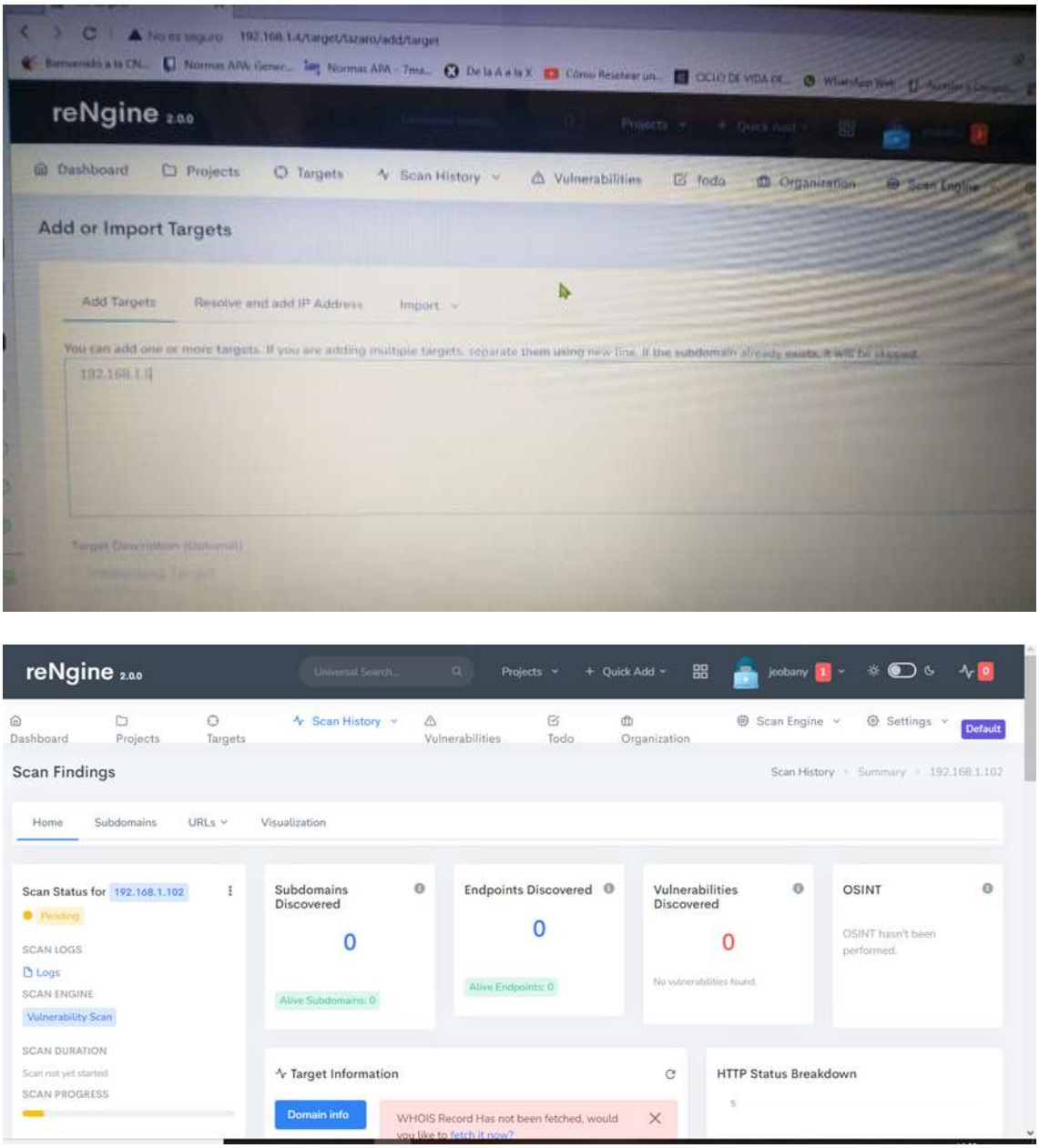


Figura 23. *Resultado escaneo Prueba de Vulnerabilidad. Autor Jeobany Ramos*

Fase 5: Resultados de la prueba de Intrusión

Para la prueba de intrusión y previamente establecida, se seleccionó y realizó tan importante procedimiento al activo de mayor relevancia al interior de la empresa LAZARO SOFTWARE como es el servidor de Bases de Datos de clientes, para esta prueba se utilizó el software KALY LINUX donde se ejecutaron una serie de comandos los cuales nos evidenciaron las siguientes conclusiones:

-exploración de todo el segmento de red con el comando como se muestra en la Figura 24.

Figura 24. *Exploración del segmento de Red. Autor Jeobany Ramos*

Verificación de puertos con el comando que se muestra en la Figura 25.

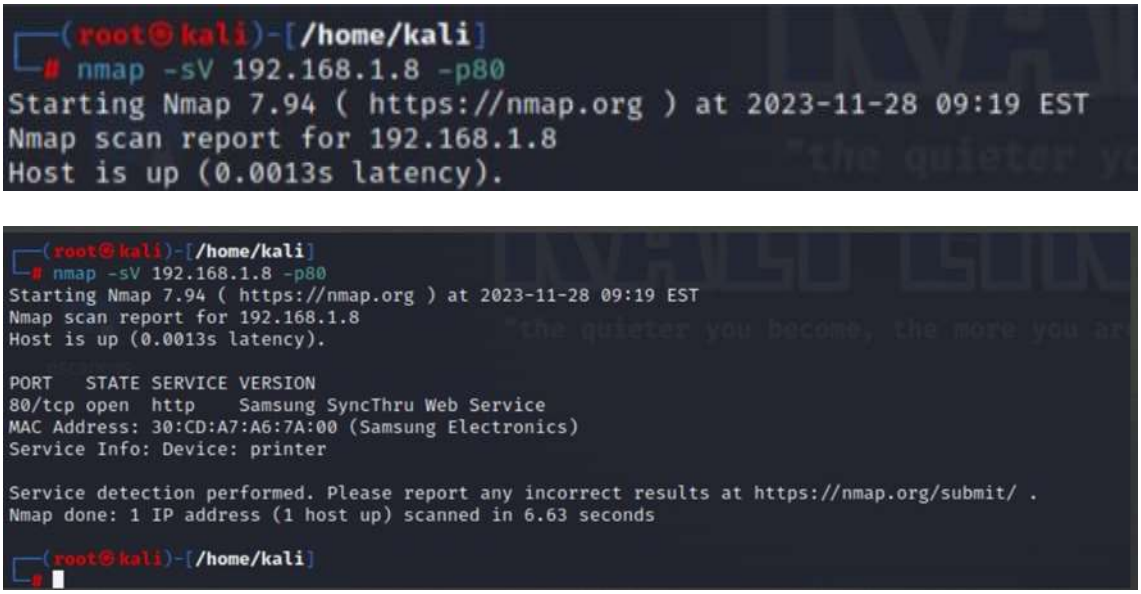


Figura 25. *Verificación de Puertos. Autor Jeobany Ramos*

Verificación si el equipo se encuentra detrás de un firewall, la prueba nos muestra que efectivamente los puertos del equipo se encuentran filtrados como se muestra en la Figura 27.

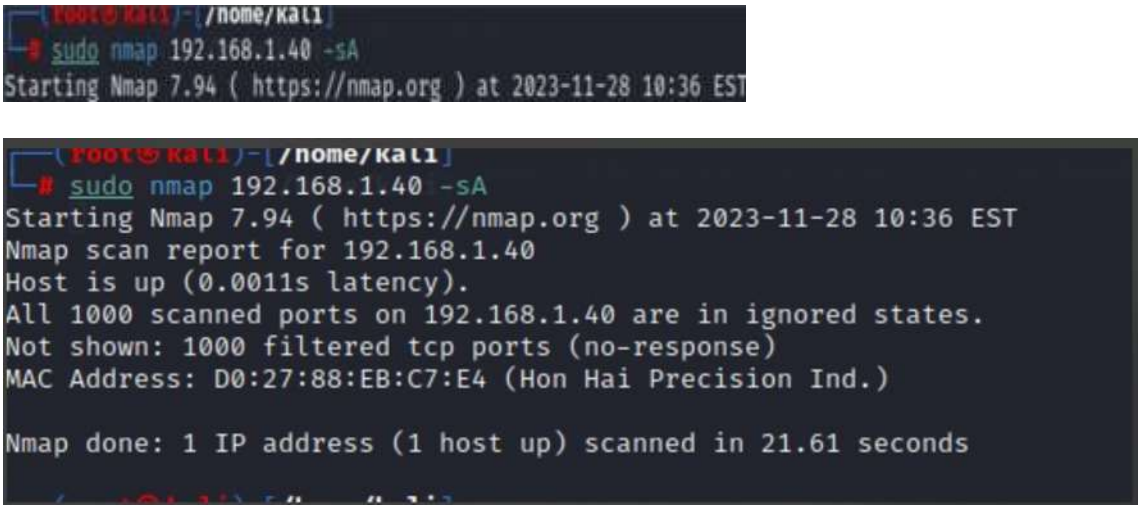


Figura 27. *Puerto filtrado. Autor Jeobany Ramos*

Por último, se realizó la prueba de vulnerabilidad para realizar la explotación con el siguiente comando como ilustra la Figura 28.

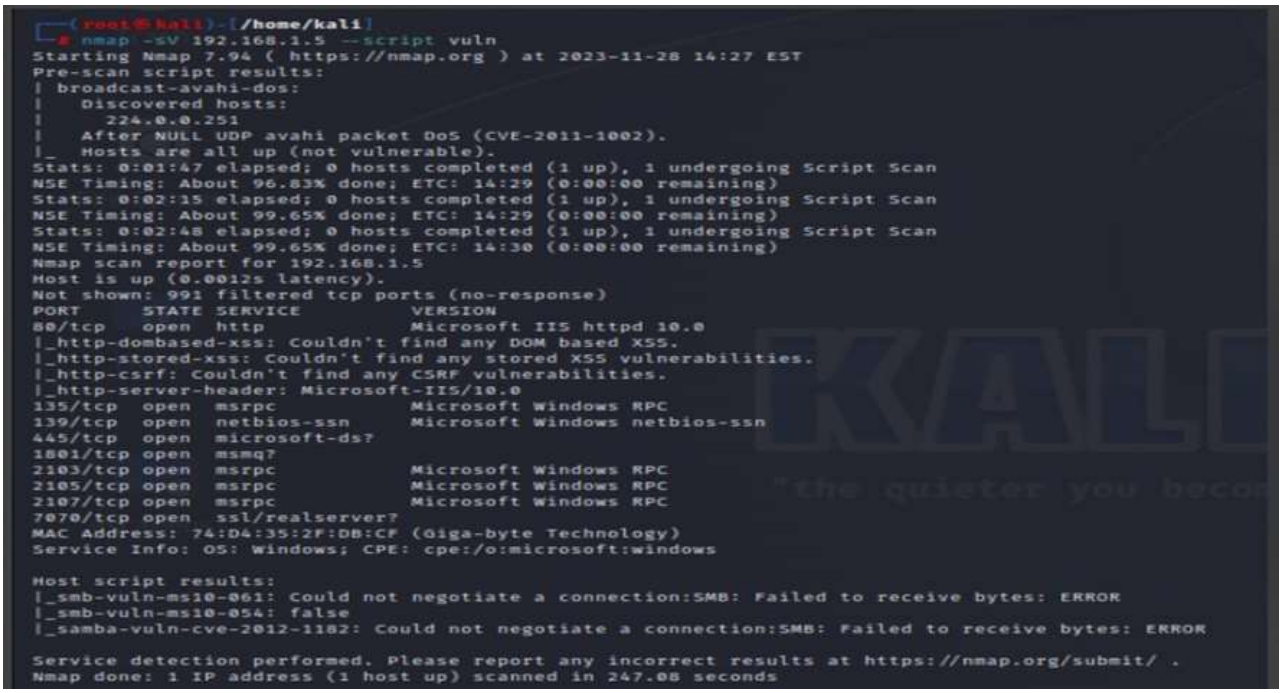


Figura 28. *Prueba de Script de Vulnerabilidad. Autor Jeobany Ramos*

En definitiva, en esta fase y de acuerdo con la respectiva metodología cuando se refiere a pruebas de explotación se puedo evidenciar que una vez realizado el procedimiento se detectó que debido a la correcta configuración del Router Mikrotik, no se detectó ningún tipo de vulnerabilidad o filtración que ponga en riesgo los activos de la empresa LAZARO software como se muestra en la Figura 29.

Figura 29. *Puerto filtrado. Autor Jeobany Ramos*

Conclusiones

En primer lugar, con relación a los activos objeto de análisis y en cuanto a los parámetros de configuración, se ajustan a las normativas establecidas para su realización (La dirección IP, nombres de host de cada sistema de la red), con respecto al servidor afirmar que se encuentra con las configuraciones adecuadas de seguridad las cuales evitan así posibles intrusiones.

En cuanto a, las herramientas Open Source utilizadas tanto para escaneo de vulnerabilidades y la prueba de intrusión, afirmar que cada una presenta una característica distinta, pero a su vez efectiva, donde fueron más las ventajas obtenidas al momento de exponer los resultados.

Con respecto a las pruebas de vulnerabilidad realizadas a los activos objeto de estudio en su gran mayoría se encontraron puertos abiertos, pero sin ningún tipo de riesgo de estar expuestos a un vector de ataque. Por otro lado, definir que al momento de realizar la prueba de intrusión su resultado fue la de no vulnerable.

Para terminar en relación con las acciones de mejora es fortalecer los planes de prevención y buenas prácticas a los empleados tanto administrativos y parte técnica con respecto a temas relacionados a la seguridad informática al interior de la compañía, adquirir software de protección del servidor de bases de datos de los clientes (Firewall).

Recomendaciones

En primer lugar, cuando nos referimos al termino de Ciberseguridad y específicamente a puertos abiertos es de mencionar una relación principalmente a un numero de puerto TCP o UDP (Protocolo de Control de transmisión), los cuales aceptan en su gran parte conexiones y paquetes de datos. Posteriormente los servicios dependientes de internet como los navegadores, páginas web y servicios de transferencias de archivos principalmente dependen de puertos específicos para recibir y enviar información (Infosegur, 2020).

En lo concerniente a un puerto abierto no necesariamente es un riesgo para la seguridad, se convierten en agentes peligrosos principalmente cuando en los activos se instalan software no autorizados y contraseñas no seguras los cuales ponen en riesgo datos e información confidencial.

Para terminar, es de mencionar algo muy importante y es el saber por qué un ciber atacante busca puertos abiertos para ejecutar exploits, para ello necesita detectar vulnerabilidades tanto en puertos abiertos, en el sistema operativo o en programas instalados en el mismo objetivo, para el atacante es importante saber los servicios que se ejecutan en la maquina junto con programas y principalmente sus versiones (W&T conecta, 2019).

En segundo lugar, ya teniendo claro los conceptos de puertos abiertos y los respectivos escaneos en busca de vulnerabilidades en la empresa LAZARO software, es de mencionar como principal activo el servidor de bases de datos de clientes el cual se detectaron 8 puertos abiertos como se muestra en la Figura 27. Donde se enumerarán y además definiremos los más relevantes.

Puerto 135/tcp: Es uno de los principales protocolos en redes su principal función está orientada a la conexión, además garantiza la entrega de paquetes en el mismo orden.

Puerto 139/tcp: Su principal funcionamiento es el de acceder a un archivo compartido o a una impresora compartida en la red LAN.

Puerto 445/tcp: Su principal funcionamiento es el de acceder a un archivo compartido o a una impresora compartida en la red LAN.

Puerto 443/tcp: Es puerto es el encargado de la navegación, lo realiza mediante el protocolo HTTPS brindando seguridad para la comunicación.

Puerto 80/tcp: Se usa principalmente para la navegación web mediante el protocolo HTTP, aunque se encuentre instalado en el servidor no cumple ninguna acción al interior de la red ya que no se encuentra configurado.

Paralelamente recomendar al Gerente de la empresa LAZARO software que los escaneos de puertos no solo tienen la finalidad de identificar posibles vulnerabilidades en algún sistema especifico o alguno desactualizado. Por el contrario, es el de detectar riesgos de seguridad de la información a través de los controles, los cuales serán evaluados de forma precisa con la finalidad de tomar medidas de prevención y disminuir los riesgos (MINTIC, 2021)

Por otra parte, evidenciar e informar que con respecto al Mickotik (Router Board), cuando se requiera configurar un enrutamiento estático no se adapta con facilidad a las redes en crecimiento es más amigable con redes pequeñas, la configuración y mantenimiento son más prolongados, presenta errores evidentes en redes extensas al momento de ser configurado. Por otro lado, cuando se refiere al enrutamiento dinámico el administrador requiere de mucho conocimiento para su configuración, verificación y resolución de problemas. En definitiva, gran parte de los recursos del router son tomados para el funcionamiento del protocolo, tiempo de CPU y el ancho de banda del enlace de red (Arrango, 2021).

Posteriormente como una recomendación de suma importancia ya que LAZARO software es una empresa dedicada al desarrollo, implementar un software en su servidor principal como es el WAF (Web Application Firewall), cuya función principal es la de proteger de múltiples ataques web en el backend.

Por último con respecto a las recomendaciones de seguridad y aunque en la actualidad la empresa LAZARO software presenta bajos niveles de vulnerabilidad en sus activos, se deben establecer líneas de comunicación tanto con el administrador y desarrolladores del software de cada sistema a evaluar, reportar de forma parcial avances de las pruebas de vulnerabilidad con una frecuencia definida, Manejo de las evidencias o soportes de las actividades , Medir la efectividad de un sistema de monitoreo o detección es decir, si se están realizando actividades de escaneo, ataques, infiltración, alteración de la información, exista una respuesta eficaz (MINTIC , 2021).

Referencias

Argote, C. (2021). Los ataques cibernéticos aumentaron 30% durante el primer semestre de este año según la Fiscalía. https://www.asuntoslegales.com.co/actualidad/los-ataques-ciberneticos-aumentaron-30-durante-el-primer-semestre-de-este-ano-3198212.

Baca, G. (2016). Introducción a la seguridad informática. Patria. https://books.google.es/books?id=IhUhDgAAQBAJ&printsec=frontcover&hl=es#v=onepage&q&f=false.

Escobar, J. (2023). Los delitos cibernéticos se han reducido en el 2023: PolicíaNacional. https://www.radionacional.co/actualidad/delitos-ciberneticos-en-colombia-estadisticas-actuales.

Fernández, Eduard. (2023). APLICACIÓN DE LA METODOLOGÍA PTES EN LA PYME COLOMBIA LEDS SAS PARA LA IDENTIFICACIÓN DE VULNERABILIDADESDECIBERSEGURIDAD. https://repository.unad.edu.co/bitstream/handle/10596/58062/eafernanadezp.pdf?sequence=1&isAllowed=y.

Fong, J. (2020). Informe global sobre ciberdelincuencia: ¿Qué países corren mayor riesgo?. https://seon.io/es/recursos/informe-global-sobre-ciberdelincuencia-que-paises-corren-mayor-riesgo/#h-Los-10-paises-con-mayor-riesgo-de-ciberamenazas.

Get Nmap 7.94 here [software]. Nmap. https://nmap.org.

GSITIC. (19,01,2018). Seguridad física y lógica de un sistema de información. Riesgos, amenazas y vulnerabilidades. Medidas de protección y aseguramiento. Auditoría de seguridad física. https://gsitic.wordpress.com/2018/01/19/bii13-seguridad-fisica-y-logica-de-un-sistema-de-informacion-riesgos-amenazas-y-vulnerabilidades-medidas-de-proteccion-y-aseguramiento-auditoria-de-seguridad-fisica/.

Historia y Secretos del Pentesting en Colombia. (s.f). SIGUARD. https://seguridadinformatica.com.co/pentesting/pentesting-en-colombia/.

Infobae. (2,08,2022). Colombia está entre los países que más ataques cibernéticosreciben. https://www.infobae.com/america/colombia/2022/08/02/colombia-esta-entre-los-paises-que-mas-ataques-ciberneticos-reciben/.

Kali LINUX v.2023.3 [software]. Kali LINUX. https://www.kali.org/get-kali/#kali-platforms.

LA REPUBLICA. (21,12,2023). Las pérdidas globales por ciberataques representarían hasta US$24 billones en 2027. https://www.larepublica.co/globoeconomia/las-perdidas-globales-por-ciberataques-representarian-hasta-us-24-billones-en-2027-3723386.

MINTIC. (2021). Seguridad y Privacidad de la Información. https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf.

Navarro, G. (s.f). Introducción a las vulnerabilidades. https://openaccess.uoc.edu/bitstream/10609/142846/25/PLA7_Introducción%20a%20las%20vulnerabilidades.pdf.

PenetrationTestingExecutionStandard (PTES).https://www.ciberseguridad.eus/ciberpedia/marcos-de-referencia/penetration-testing-execution-standard-ptes.

Prieto, E. (20203). Seguridad informática en las empresas: Concepto e importancia. https://es.snhu.edu/noticias/que-es-la-seguridad-informatica-en-las-empresas.

¿Qué es una Vulnerabilidad informática? (s.f). Santander. https://www.bancosantander.es/glosario/vulnerabilidad-

informatica#:~:text=En%20informática%2C%20una%20vulnerabilidad%20es,malintencionada%20para%20comprometer%20su%20seguridad.

ReNgine v1.2.0 [software]. ReNgine. https://yogeshojha.github.io/rengine/.

Salazar, J. B., & Campos, P. G. (2008). Modelo para Seguridad de la Información en TIC. Concepción, Chile: Universidad del Bío-Bío, 234-253.

Sánchez, C, Gutiérrez, M, Gavilán, M, Serrato, Y. (2022). Buenas prácticas en seguridad de la información para el teletrabajo en Colombia. https://repository.libertadores.edu.co/bitstream/handle/11371/5040/Gavilán_Mateus_Sánchez_2022.pdf?sequence=1&isAllowed=y.

Vega Subgraph 1.0 [software]. Vega Subgraph. https://subgraph.com/vega/download/index.en.html