REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN MENCIÓN EN SEGURIDAD INFORMÁTICA

TITULO DEL TRABAJO DE TITULACIÓN

EVALUACIÓN DE VULNERABILIDADES EN EL SISTEMA DE INFORMACIÓN DE LA EMPRESA MASTERNET A TRAVES DE TÉCNICAS DE PENTESTING PARA FORTALECER SUS ACTIVOS DIGITALES.

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con Mención en Seguridad Informática

AUTOR:

Diego Mauricio Silva Mora

DIRECTOR:

MSC. Cosme Macarthur Ortega Bustamante

Ibarra, diciembre 2024

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	172551588-4		
APELLIDOS Y NOMBRES	SILVA MORA DIEGO MAURICIO		
DIRECCIÓN	URB. VIRGEN DEL CISNE		
EMAIL	diego_s_31@hotmail.com		
TELÉFONO FIJO		**TELÉFONO MÓVIL:**	0996115295

DATOS DE LA OBRA	
TÍTULO:	EVALUACIÓN DE VULNERABILIDADES EN EL SISTEMA DE INFORMACIÓN DE LA EMPRESA MASTERNET A TRAVES DE TÉCNICAS DE PENTESTING PARA FORTALECER SUS ACTIVOS DIGITALES.
AUTOR (ES):	ING. DEIGO MAURICIO SILVA MORA
FECHA: DD/MM/AAAA	10 de diciembre del 2024
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA DE POSGRADO	MAESTRÍA EN COMPUTACIÓN MENCIÓN EN SEGURIDAD INFORMATICA
TITULO POR EL QUE OPTA	**MAGISTER EN COMPUTACIÓN**
DIRECTOR	**MSC. COSME MACARTHUR ORTEGA BUSTAMANTE**

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 10 días del mes de diciembre del 2024

EL AUTOR:

Firma_____

Firmado electrónicamente por:
DIEGO MAURICIO
SILVA MORA

Nombre Ing. Diego Mauricio Silva Mora

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

FACULTAD DE POSGRADO

Ibarra, 21 de octubre de 2024

Dra.
Lucía Yépez
DECANA FACULTAD DE POSGRADO

ASUNTO: Conformidad con el documento final

Señor(a) Decano(a):

Nos permitimos informar a usted que revisado el Trabajo final de Grado EVALUACIÓN DE VULNERABILIDADES EN EL SISTEMA DE INFORMACIÓN DE LA EMPRESA MASTERNET A TRAVES DE TÉCNICAS DE PENTESTING PARA FORTALECER SUS ACTIVOS DIGITALES, del maestrante **SILVA MORA DIEGO MAURICIO**, de la Maestría de Computación Mención en Seguridad Informática, certificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	Apellidos y Nombres	**Firma**
Director/a	MSc. Cosme Ortega Bustamante	1001580396 COSME MACARTHUR ORTEGA BUSTAMANTE Firmado digitalmente por 1001580396 COSME MACARTHUR ORTEGA BUSTAMANTE Fecha: 2024.10.23 22:49:48 -05'00'
Asesor/a	PhD. Jaramillo Alcázar Ángel	ANGEL GABRIEL JARAMILLO ALCAZAR

DEDICATORIA

A Dios, quien me a brindando la vida y ha sido mi fortaleza para seguir adelante por buen camino y nunca darme por vencido.

A mi futura esposa Nataly, por siempre estar a mi lado en los momentos buenos y malos.
A mis padres Aida y Juan que han sido mi guía y ejemplo incondicional desde pequeño, me han inculcado excelentes valores.

A mis hermanos Cristian y Danny, que han sido unos excelentes hermanos y en ellos veo reflejado el esfuerzo que dan en todo lo que se proponen.

A mi sobrina Aitana, cada que la veo me llena de mucha energía y eso me motiva para no decaer y esforzarme aún más.

A mi sobrino Juan Mathias +, desde el cielo sé que me está cuidando y este orgulloso de todo lo que eh logrado.

A mis futuros suegros Ines y Jesus, que sin duda se han convertido como mis segundos padres.

AGRADECIMIENTO

Agradezco a Dios por darme la vida, ya que es lo primordial para estar cumpliendo esta anhelada meta.

A mis padres, ya que ellos siempre me han apoyado en todo mi proceso de vida, agradecido por siempre ser el ejemplo para mí y mis hermanos.

A mi tutor Ing. Cosme Ortega Bustamante, asesor Ing. Ángel Jaramillo, que me brindaron su tiempo para ayudarme en desarrollo de este proyecto.

Para terminar, agradezco a la Universidad UTN y sus colaboradores por brindarme las enseñas, durante todo el periodo académico.

INDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO

PROGRAMA DE MAESTRÍA EN COMPUTACIÓN MENCIÓN EN SEGURIDAD INFORMÁTICA

EVALUACIÓN Y MITIGACIÓN DE VULNERABILIDADES EN EL SISTEMA DE INFORMACIÓN DE LA EMPRESA MASTERNET A TRAVES DE TECNICAS DE PENTESTING

Autor: Nombre completo del estudiante
Tutor: Nombre completo del tutor
Año: 2024

RESUMEN

La presente investigación consiste en la evaluación de vulnerabilidades dentro del sistema informático que tiene la empresa MASTERNET, aplicando técnicas de Pentesting para descubrir diversos fallos que van desde configuración hasta ataques de Fuerza Bruta (RDP), entre otros. Resaltando a tal manera la relevancia de implementar una cultura de comunicación y seguridad asertiva en toda la empresa. Esta propuesta se enfoca en los siguientes aspectos:

- Metodología de Pentesting.
- Herramienta y técnicas de Pentesting.
- Beneficios y limitaciones del Pentesting.

Este estudio no solo se centra en identificar de vulnerabilidades, sino que proporciona soluciones prácticas, en donde, con la validación de las medidas de mitigación presentada y con el análisis detallado durante todo el proceso de Pentesting que va desde la identificación y clasificación de vulnerabilidades de acuerdo al nivel de gravedad y posteriormente finaliza con la propuesta de una serie de recomendaciones viables y concretas para que la empresa Masternet pueda poner en práctica y mitigar dichas falencias técnicas.

Palabras clave: Riesgos informáticos, Pentesting, Vulnerabilidades, Seguridad informática.

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO

PROGRAMA DE MAESTRÍA EN COMPUTACIÓN MENCIÓN EN SEGURIDAD INFORMÁTICA

EVALUATION AND MITIGATION OF VULNERABILITIES IN THE INFORMATION SYSTEM OF MASTERNET COMPANY THROUGH PENTESTING TECHNIQUES

ABSTRACT

The present investigation consists of the evaluation of vulnerabilities within the computer system of the MASTERNET company, applying Pentesting techniques to discover various failures ranging from configuration to Brute Force attacks (RDP), among others. Highlighting in this way the relevance of implementing a culture of communication and assertive security throughout the company. This proposal focuses on the following aspects:

- Pentesting Methodology.
- Pentesting tools and techniques.
- Benefits and limitations of Pentesting.

This study not only focuses on identifying vulnerabilities, but also provides practical solutions, where, with the validation of the mitigation measures presented and with the detailed analysis throughout the Pentesting process that goes from the identification and classification of vulnerabilities to according to the level of severity and then ends with the proposal of a series of viable and concrete recommendations so that the Masternet company can put into practice and mitigate these technical shortcomings.

Keywords: Computer risks, Pentesting, Vulnerabilities, Computer security

INTRODUCCIÓN

Tras el avance tecnológico ha crecido digitalmente de una manera satisfactoria, a tal hecho, que en las organizaciones han trasladado toda su data y procesos a la nube. Al respecto, existen diversos beneficios, mejoras y aumentos del uso de las tecnologías de la información, internet, sistemas web, móviles, cloud computing, entre otros. Sin embargo, al mismo tiempo se han elevado el índice de ciberdelincuentes que buscan vulnerar y conseguir información para conseguir beneficios económicos o a su vez otro activo que sea de valor para una empresa cabe destacar que los ataques cibernéticos son cada vez más sofisticados y con una frecuencia significativa.

En tal sentido, Ecuador se ha convertido en un país que tiene altos índices de ataques cibernéticos, por lo cual implementar políticas que permitan salvaguardar todo tipo de información que sea de valor para una empresa son obligatorias para todos los miembros o personal que trabaje en dicha organización. A partir de aquí, se hace evidente la relevancia de entablar cierto control en relación con la seguridad de la información que se genere y de la seguridad física de los activos de una compañía. Es entonces que raíz de lo mencionado, se aplica ciertas auditorias que resultan ser un punto crítico de control para el flujo correcto de trabajo interno de la empresa, lo cual asegura los principios de la seguridad: confidencialidad, integridad, disponibilidad y ante sus activos.

Al respecto, surgen diversas herramientas y metodologías que permiten aplicar una correcta práctica de seguridad informática. El Pentesting es considerada como una herramienta que permite salvaguardar la información. Por tales razones en el presente estudio investigativo con título: “Evaluación de vulnerabilidades en el sistema de información de MASTERNET por medio del uso de técnicas de Pentesting para fortalecer sus activos digitales”, ejecuta dicha metodología ya que como propósito es la identificación de las vulnerabilidades presentes que mantiene la empresa para posteriormente aplicar ciertas recomendaciones y estrategias que la empresa deberá de aplicar para prevenir ciertos ataques cibernéticos. Para conseguirlo, se empleará

herramientas enfocadas en la seguridad informática, como el sistema operativo Kali Linux.

A continuación, es importante mencionar que este estudio consta de cuatro capítulos, de los cuales se detallan a continuación:

CAPÍTULO I. Se presenta una descripción en base al planteamiento del problema del presente estudio, así mismo consta de su respectiva justificación, objetivo general y específicos de los cuales permitirá exponer el alcance que se pretende alcanzar durante todo el proceso de ejecución de este.

CAPÍTULO II. Consta de la investigación de diferentes fuentes tanto a nivel nacional e internacional a fin de determinar las bases teóricas más relevantes, también, ciertos antecedentes que son presentados para reforzar y aclarar la viabilidad de esta propuesta técnica, finalmente, en este capítulo consta de ciertos términos que permitirán facilitar la comprensión lectora.

CAPÍTULO III. Consta de la presentación y estructuración del marco metodológico del presente estudio, tales como: técnicas, métodos, diseños, nivel y tipo de investigación. Posteriormente, se presenta la metodología de seguridad informática a utilizar.

CAPITULO IV. Se presentan los resultados conseguidos a raíz de la ejecución del Pestesting, para posteriormente presentas las recomendaciones y estrategias de mejora para la empresa MASTERNET.

Finalmente, y no menos importante, se describen aquellas conclusiones y recomendaciones para futuros investigadores quienes obtén por el uso de proyectos relacionados al Pentesting.

CAPÍTULO I

1. EL PROBLEMA

1.1 Problema de investigación

Es importante analizar la situación en materia de seguridad, sobre todo en las empresas que se encuentran ubicadas a nivel de Latinoamérica. En este sentido, según las últimas investigaciones mencionaron que en América Latina se reportaron más de 2 millones de ciberataques en un año, de agosto de 2022 a agosto de 2023 con un (61%), robo de información (58%) y protección de información (48%), junto con la preocupación por el código malicioso (57%), que es la principal herramienta usada por los ciberdelincuentes para controlar la data corporativa (Eset, 2020).

Otro incidente más común en las organizaciones de Latinoamérica es la explotación de vulnerabilidades, proceso por el cual se aprovechan las fallas de seguridad en sistemas informáticos, aplicaciones o redes con la finalidad de comprometer la seguridad informática. Los ciberdelincuentes buscan y explotan estas vulnerabilidades para conseguir acceso no autorizado a sistemas, robar data confidencial, distribuir malware o realizar otro tipo de actividades maliciosas (Túqueres, 2021).

En Ecuador hubo más de 51 mil registros (Alvarado, 2020) relacionados con cryptominers[1], alrededor de 140 mil detecciones de exploits[2], cerca de seis mil detecciones de ransomware[3] y casi ocho mil detecciones de spyware[4], como datos de algunos tipos de software malicioso.

De acuerdo con lo mencionado, en Santo Domingo, se encuentra ubicada la empresa MASTERNET dedicada a ofrecer soluciones tecnológicas avanzadas para pequeñas y medianas organizaciones. El objetivo es ser el líder en el mercado de servicios de IT, proporcionando productos y servicios innovadores que mejoren la eficiencia operativa y

[1] Malware utilizado para la minería de criptomonedas.
[2] Un exploit es cualquier ataque que aprovecha las vulnerabilidades de las aplicaciones, las redes, los sistemas operativos o el hardware
[3] El ransomware es un tipo de malware que bloquea los datos o el dispositivo de una víctima y amenaza con mantenerlo bloqueado hasta que se pague un rescate. Utiliza el cifrado a nivel de disco, lo que causa más daño que los ataques basados en archivos individuales
[4] El spyware es un tipo de malware que intenta mantenerse oculto mientras registra información en secreto y sigue sus actividades en línea, tanto en equipos como en dispositivos móviles. Puede supervisar y copiar todo lo que escribe, carga, descarga y almacena.

la competitividad de los clientes. Sin embargo, se ha evidenciado diversos inconvenientes técnicos, enfocados en la seguridad de la información, es decir; no cuenta con una política de acceso a la infraestructura de información, lo cual compromete la integridad, disponibilidad y confidencialidad de sus datos. Esta definición ocasiona interrupciones en las operaciones comerciales, afectando así la eficiencia, competitividad, y calidad en los servicios prestados.

La empresa MASTERNET ha sido testigo de varios ataques significativos en los últimos años, uno de los más notorios fue el ataque de Ransomware que sufrió la empresa en 2020, consiste en que este tipo es considerado como estrategia de extorción digital ya que permitió al atacante encriptar ficheros guardados en los dispositivos tecnológicos de la compañía, generando la propagación de toda la información interna que manejan. Este incidente paralizó varios de sus servicios y puso en evidencia la vulnerabilidad de las infraestructuras críticas de los servicios prestados. Otro caso relevante fue el ciberataque perpetrado en 2019, donde los atacantes lograron comprometer sistemas esenciales para la distribución de energía eléctrica.

1.2 Interrogantes de la investigación

Toda empresa que dependa de una plataforma tecnológica tiene que contar las normas, procedimientos, planes de seguridad y mitigación de riesgos informáticos, por ello, se plantea las siguientes interrogantes en la empresa MASTERNET.

RQ1: ¿Cuál es el estado actual de la empresa en términos de seguridad y cuáles son las necesidades más críticas que requieren atención?

RQ2: ¿Cómo escoger adecuadamente los mecanismos de salvaguarda para reducir los riesgos identificados?

RQ3: ¿Cómo se puede proteger los activos digitales y garantizar la calidad de la información crítica en la empresa MASTERNET?

1.3 Objetivos

1.3.1 Objetivo general

Evaluar las vulnerabilidades en el sistema de información de la empresa MASTERNET a través de técnicas de PENTESTING para fortalecer sus activos digitales.

1.3.2 Objetivos específicos

- Diagnosticar los mecanismos de seguridad, a nivel de servicios existente internacionalmente, para contrarrestar los ataques informáticos que puedan establecerse en la red telemática de la Empresa MASTERNET.
- Identificar las fallas que presenta la red telemática de la Empresa MASTERNET aplicando técnicas de PENTESTING.
- Proponer recomendaciones y estrategias específicas para mejorar la seguridad de la información en la empresa MASTERNET.

1.4 Justificación

Entre las razones por las cuales se justifica la presente propuesta tecnológica es debido a que proporcionará ciertos beneficios directamente al personal administrativo de la empresa MASTERNET, tales como: ayudará a identificar las necesidades más críticas en materia de seguridad y con el cual permita escoger las salvaguardas adecuadas para mitigar los riegos identificados, esto se propone con el fin fortalecer la protección de activos digitales, que implementen buenas prácticas de seguridad de la información.

Todo lo anterior garantizará la disponibilidad, confidencialidad e integridad de los datos, asegurando que la red de información sea segura. Además, se realizarán pruebas de penetración. El pentesting puede utilizar información de simulación, para evaluar el nivel de seguridad de la red de telecomunicaciones a través de ataques de información. La prueba de penetración permitirá la exploración de la red, el análisis de seguridad y las auditorias; una vez implementada la prueba, será posible identificar las debilidades de MASTERNET e identificar las actividades más riesgosas y las áreas que requieren el mayor esfuerzo para proteger los datos.

Por ello, se toma como punto de departida la Metodología Penetration Testing Execution Stándard (PTES). Esta se fundamenta en aplicar herramientas de hacking ético y las técnicas de Pentesting, para identificar las debilidades en cuanto a seguridad, obteniendo como resultando, las respuestas a las interrogantes de la formulación del problema y cristalizar una metodología que aporta para mantener la integridad, disponibilidad y privacidad de la información de la organización MASTERNET, y por ende evitar el impacto a la comunidad de usuarios que depende de estas instituciones.

No obstante, también se benefician de una manera indirecta los clientes quienes hayan proporcionado cierta información de valor hacia la empresa, misma que está almacenada en los servidores de la empresa, entonces, con la ejecución de esta propuesta la información estará protegida y libre de amenazas cibernéticas.

CAPITULO II

2 MARCO REFERENCIAL

En este capítulo se presenta tanto los antecedentes de la investigación como las bases teóricas necesarias para el entendimiento y correlación de los diversos planteamientos en pro de alcanzar los objetivos planteados.

2.1 Antecedentes

Conforme avanza la tecnología hoy día, son innumerables las amenazas cibernéticas, con las que pueden atentar contra las organizaciones, tanto de fuentes externas, siendo aplicadas a los sistemas utilizados en las operaciones tradicionales del negocio, o por medio de sus propios empleados, lo que se conoce como ataques internos. Sin embargo, indiferentemente de su origen los ataques se caracterizan por estar dirigidos con la intención de ocasionar daño, de lo que se deriva el esfuerzo de las empresas en invertir esfuerzos en obtener y mantener plataformas seguras.

La seguridad de la información se conforma por varias aristas la integridad, la disponibilidad, la confidencialidad y la auditoria de la misma, como pilares básicos para sistemas informáticos seguros, como el caso del estudio realizado por Gutiérrez (2014) en la Universidad de Valladolid, en lo cual se usó como herramienta principal el sistema operativo de evaluación Kali Linux, siendo su implementación mediante una aplicación de código abierto para el diseño, desarrollo e implementación virtual del laboratorio de *pentesting*, cuyo objetivo es educar y donde los estudiantes puedan conocer la importancia de la seguridad, así como la capacidad de construir sus redes, aplicaciones y sistemas de la forma más segura posible (Ortega-Garcés, 2023).

También, se hace referencia a otra propuesta investigativa, que consiste en un trabajo relacionado con el tema del tópico que es de interés para el estudio realizado por Valderrama (2017) en la Universidad Nacional Abierta y a Distancia de Chocó-Colombia ya que describe los problemas de seguridad de la red en la alcaldía del Municipio de Cantón de San Pablo, por medio del uso de pruebas de penetración que permita el mejoramiento continuo de la gobernación. En él se planteó como objetivo de

investigación aplicar las soluciones correctivas en cuanto a la problemática de la seguridad en la red de datos.

Al respecto, se presenta otro estudio donde el ciberespacio ha introducido una nueva dimensión de ciberdelincuencia en las sociedades digitales y su uso se ha incorporado de modo cotidiano y generalizado, en este sentido Muñoz (2017), de la Universidad del Cauca-Colombia, en el cual identifican de manera eficiente y eficaz las vulnerabilidades más comunes sobre los sistemas web, siguiendo estos la metodología OWASP e implementaron prototipos de hardware y software como generación de soluciones luego de aplicar Pentesting.

Finalmente, y no menos importante un estudio realizado por los autores Jaramillo y Riofrío (2015), desarrollaron una propuesta metodológica para la detección, evaluación, de riesgos, debilidades y contramedidas en el diseño e implementación de la infraestructura de la red de la Editorial Don Bosco, a través las pruebas de intrusión conocida como caja blanca, dentro del cual se identificaron las debilidades y dejaron al descubierto las vulnerabilidades. Las pruebas empleadas y en los resultados obtenidos se enfocaron esencialmente en los datos públicamente accesibles.

2.2 Marco Teórico

2.2.1 Introducción a la Seguridad informática

La seguridad informática (SI) surge de la necesidad de garantizar la privacidad e integridad de los datos guardados en todo tipo de sistema informático. En este sentido, la seguridad informática debe de ser cumplido con disciplina, los cuales se basan en políticas y regulaciones externas e Dentro de una empresa, la vulnerabilidad ante diversas amenazas cibernéticas aumenta, desde el robo de información hasta la interrupción de operaciones corporativas. Esto es impulsado por la creciente interconexión de dispositivos y las transferencias de datos en línea, lo que lleva a una mayor necesidad de seguridad informática.(Guaña-Moya, 2023).

2.2.2 Características fundamentales de la información

Al tratar el tema de seguridad informática, es importante destacar que toda información debe se poseer ciertas cualidades esenciales que permitan garantizar la seguridad y su utilidad, tales como:

Tabla 1.

Características fundamentales de la seguridad informática

CARACTERÍSTICA	DESCRIPCIÓN
EFICACIA	En este caso, debe de ser lo apropiada y suficiente para completar las tareas particulares que asigna una empresa. Para ello, debe de poseer sólo la cantidad adecuada de data.
EFICIENTE	Toda información tiene que ser creada y manejada de manera que permita maximizar los recursos de una empresa, incluso el tiempo y personas.
CONFIDENCIAL	Los datos deben de ser protegidos contra manipulaciones, accesos e incluso robos no deseados. De esta manera, la privacidad de los datos estará protegidos.
PRECISA	La data completa para su posterior uso y cumplir con los valores y estándares de la empresa, los cuales tiene que efectuar con estos requerimientos.
DISPONIBILIDAD	La data tiene que estar siempre disponible para su respectivo procesamiento y así la empresa pueda operar de la mejor manera.
LEYES Y REGULACIONES	La data tiene cumplir con todas las leyes y regulaciones externas como externas e internas.
CONFIABILIDAD	La data no puede ser editada sin una autorización previa.

Nota: Elaboración propia

2.2.3 Importancia de la Seguridad Informática

La importancia de la seguridad informática ha conllevado una creciente masiva de la necesidad de salvaguardar los datos que se manejan constantemente, en especial dentro

de una empresa, puesto que, aumenta significativamente la posibilidad de ciertas vulnerabilidades de ataques o ciber amenazas.

En este sentido, aplicar ciertos parámetros de seguridad como la atención y control de acceso son temas esenciales y de los cuales están cubiertos por la seguridad informática. Por ello, gestionar quién se encuentra autorizado a acceder a cierta data confidencial se conoce como control de acceso. Adicionalmente, verificar la identificación de entidades o personas que diariamente interactúan con sistemas informáticos por medio de técnicas como: la aplicación de huellas dactilares, contraseñas o incluso la autenticación multifactor que se conoce como autenticación (Guaña-Moya, 2023).

Ahora bien, en una empresa puede encontrar peligros y reducirlos con la finalidad de que los objetivos principales relacionados con la seguridad informática puedan ejercer las operaciones corporativas de manera eficiente y sin ninguna novedad. Para poder evitar este tipo de inconvenientes, es importante el uso de varias tácticas para proteger los sistemas de información que estos incluyen métodos técnicos, por ejemplo: sistemas de detección, instalación de cortafuegos y prevención de intrusos. Adicional, el uso de redes privadas virtuales (VPN) para añadir un grado adicional de protección en la red al instante que los dispositivos técnicos se conecten a las redes Wi-Fi inseguras.

Entonces, en tal sentido de lo expuesto, según investigaciones mencionan que es importante minimizar la susceptibilidad de una empresa a los ataques cibernéticos se necesita de capacitaciones continuas al personas que sean relacionados sobre los procedimientos de seguridad, agregado la creación de contraseñas seguras y la respectiva confirmación de la legitimidad de los correos electrónicos y sitio web (Llano et al., 2021).

2.2.4 SGSI (Sistema de Gestión de la Seguridad de la Información)

La seguridad de la información, según Guerra et al., (2021) “Esto incluye aplicar y ejecutar medidas de seguridad adecuadas para que la información esté asegurada y protegida en base a los tres aspectos claves, como: confidencialidad, disponibilidad e integridad” (p. 14).

2.2.5 Importancia de la seguridad de la información

Un Sistema de Información se considera seguro si está libre de riesgos y daños. No se puede garantizar la seguridad absoluta o la invulnerabilidad de un sistema informático,

por lo que gestionar su seguridad es el objetivo previsto por aquellos profesionales enfocados en el área de ciberseguridad.

La seguridad de la información se entiende como la preservación de las siguientes características:

- **Disponibilidad:** la capacidad de los usuarios autorizados para acceder y utilizar servicios, datos o sistemas según sea necesario.
- **Confidencialidad:** garantiza que la data sea accesible sólo a aquellas personas autorizadas. Al recto también menciona que hace referencia a la capacidad de comunicarse o de los datos que deben de ser entendidos o leídos únicamente por personas o sistemas autorizados (Jiménez, 2021, p. 146).
- **Integridad:** preserva la exactitud de los datos y los métodos de procesamiento.
- **Disponibilidad:** garantiza que, cuando sea necesarios, los usuarios admitidos tengan accesoa a los datos y recursos relacionados, puedan utilizarlo (Mogollon, 2022). Por otra parte, Guerra et al., (2021) “menciona que es la cualidad de un mensaje, comunicarse o datos que permitan corroborar que no se ha generado ningún tipo de cambio, es decir que no haya sido alterado o modificado” (p. 147).

Al respecto, se agrega ciertos conceptos en relación con lo mencionado anteriormente, tales como:

- **Autenticidad y No Repudio:** velar por la eficiencia de tiempo, forma y distribución de la información. También se aplica para evitar que la entidad que envía o recibe el mensaje reclame a un tercero que no envió ni recibió el mensaje.
- **Auditabilidad:** todos los eventos de un sistema tienen que poder registrarse para su posterior control posterior.
- **Protección frente a la duplicación:** esto es para garantizar que la transacción se ejecute solo una vez, a menos que se especifique lo contrario. Además, se debe evitar registrar y reproducir transacciones para simular múltiples solicitudes del mismo remitente original.
- **Legalidad:** basado en acatar y dar cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta una empresa.

- **Confiabilidad de la información:** toda data creada tiene que ser adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones (Michilena & Díaz, 2011).

Toda empresa debe de establecer una Política de Seguridad que englobará todas las normas, mismo que deberá de ser respetada y ejecutada tanto para colaboradores, procedimientos y activos.

2.2.6 Importancia de la Política de Seguridad

La política de seguridad es un conjunto de reglas que describen los aspectos esenciales de la seguridad de la información y las comunicaciones que todos los usuarios deben respetar y contantemente serán reguladas .

Si bien los miembros de la dirección de una organización tienen la mayor responsabilidad de gestionar e implementar controles adecuados de seguridad de la información, el cumplimiento de esos controles será responsabilidad de todos los que colaboran o cooperan en las actividades de una organización (Ministerio de telecomunicaciones y de la sociedad de la informacion, 2020).

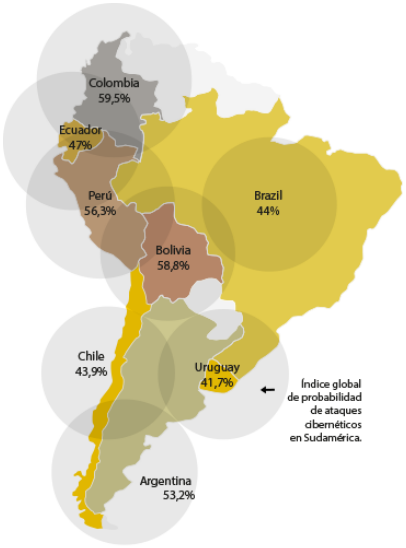
Se proporcionan los recursos y medios necesarios para la consecución efectiva de los objetivos de esta política de seguridad, y sus resultados se irán aplicando progresivamente a las diferentes áreas según un modelo de mejora continua, en el que se pondrá especial énfasis en los empleados, recursos humanos, formación y medición del desempeño.

2.2.7 Seguridad informática en Ecuador

Tras el avance de la tecnología, la transformación digital ha conllevado que exista una masiva creación de cantidades de datos, trae consigo el incremento de la posibilidad de infracciones y ataques a terceros. De hecho, en Ecuador presenta un alto impacto sobre este fenómeno, puesto que, las empresas se encuentran transfiriendo la data que manejan hacia la nube, lo que ha aumentado sus vulnerabilidades de los ciberataques (Mayacela & Guerrero, 2023).

Adicional, el incremento de los ciberataques en las empresas requiere que se implementen propuestas de salvaguardan la información y es importante actualizarse en relación a los avances en ciberseguridad para adaptarse a las amenazas en constante cambio y preservar una postura defensiva sólida.

Al respecto, según una investigación, indica que sobre todo en Ecuador por el año del 2022 se presentó un índice de probabilidad elevada de ataques cibernéticos de un 47 % siendo un porcentaje elevado en comparativa de todo Sudaamérica, entonces, se ha tenido un incremento de acuerdo al año 2021 hasta un 66% en la industria minorista y mayorista a nivel global (Mayacela & Guerrero, 2023).



ÍNDICE GLOBAL DE ATAQUES CIBERNÉTICOS SEMANALES POR INDUSTRIA 2022 COMPARADO CON EL 2021

Industria	Número de ataques	Incremento % vs 2023
Educación / Investigación	2.314	+43%
Gobierno / Milicia	1.661	+46%
Salud	1.463	+74%
Comunicación	1.380	+27%
ISP / MSP	1.372	+28%
Finanzas / Banca	1.131	+52%
Servicios públicos	1.101	+48%
Seguros / Legal	957	+47%
Manufactura	950	+36%
Ocio / Hotelería	943	+60%
SI/VAR/ Distribuidores	904	+18%
Minoristas / Mayoristas	871	+66%
Transporte	750	+41%
Vendores de *Software*	747	+37%
Consultores	689	+19%
Vendedor de *Hardware*	448	+25%

Figura 1. **Estadística de los ataques cibernéticos**

Nota: Tomado de (Mayacela & Guerrero, 2023)

En resumen, la figura 1 representa que Ecuador ha sido más vulnerable ante este tipo de ataques cibernéticos, de hecho, se han identificado amenazas desde Botnets hasta Ransomware. Dichos ataques corresponden a que se debe de implementar medidas proactivas y a una mayor concienciación para minimizar el riesgo de las vulnerabilidades (Mayacela & Guerrero, 2023).

Al respecto, el Ministerio de Telecomunicaciones ha trabajado en un componente esencial de la seguridad de la red, MINTEL, quien es el encargado de organizar trabajos técnicos a nivel nacional e internacional, con el objetivo de garantizar un correcto uso de las redes por medio del Centro de Respuestas a Incidentes Informáticos del Ecuador "EcuCERT", que forma parte de la Agencia de Regulación y Control de las Telecomunicaciones "ARCOTEL", Dichas entidades trabajan constantemente para proteger a los usuarios de TIC del país (Ministerio de telecomunicaciones y de la sociedad de la información, 2020).

En tal sentido, con la implementación del código penal ecuatoriano entablan ciertas medidas correctivas para sancionar aquellos delitos informáticos, el objetivo es salvaguardar los derechos de los usuarios, quienes a diario desarrollan diversas actividades en línea. Dichos delitos inician desde el fraude electrónico hasta la intercepción de mensajes de datos y el acceso no autorizado a toda data privada que maneje el usuario en las distintas plataformas que existen actualmente.

Al respecto, según investigaciones, indican que en Ecuador según datos del Instituto Nacional de Estadísticas y Censos (2020), el porcentaje de personas que utilizaron internet en el 2012 alcanzó 35,1%, incrementándose a un 59,2% para el 2019. Este crecimiento acelerado en el uso de las plataformas digitales es palpable, porque las organizaciones financieras y empresariales (bancos, industria, turismo, etc.) Han incrementado sus servicios online (banca electrónica, transacciones electrónicas, etc.). Incluso las autoridades han automatizado sus servicios (pagos de propiedades, pagos de impuestos, etc.) Incrementado la oferta de productos y servicios en línea (facturas electrónicas, sitios de compras, etc.).

Analizando el aumento descrito en el anterior apartado, podría deberse a varios motivos, así como menciona el (Ministerio de telecomunicaciones y de la sociedad de la informacion, 2020):

- Creación del plan de gobierno electrónico 2018-2021,
- Incremento de controles de calidad a las organizaciones que prestan servicios de internet por la extinta Supertel.
- Creación de redes comunitarias en las distintas zonas rurales.
- Las políticas de gobierno para la modificación productiva y el desarrollo del Ecuador, entre otros.

No se puede negar que la adopción de tecnología ha dado lugar a avances que, a su vez, han generado problemas de seguridad cibernética. Al menos en Ecuador, las estadísticas de violaciones de seguridad se concentran en el sistema financiero. Su aumento en números es una preocupación de ciberseguridad, especialmente para los bancos ecuatorianos. Por ejemplo, según el medio de comunicación Al respecto en una publicación efectuada por el diario (Universo, 2020), para el 2014 se había registrado 3.118 delitos informáticos y para el 2019, la cifra contabiliza fue 5.048.

2.3 Gestión de riesgos

Es necesario realizar un análisis de riesgos para anticipar los posibles riesgos y de alguna manera entablar medidas preventivas y así poder enfrentarlos, resultando un elemento esencial para salvaguardar los activos críticos de una empresa. Se debe de: identificar, evaluar y abordar dichas amenazas, pero hay que priorizar las acciones necesarias (Martín, 2018).

2.3.1 Identificación de Amenazas

En este punto se procede a identificar las posibles amenazas que afectan a los activos identificados (Martín, 2018). Estas amenazas surgen de distintas fuentes, por ejemplo:

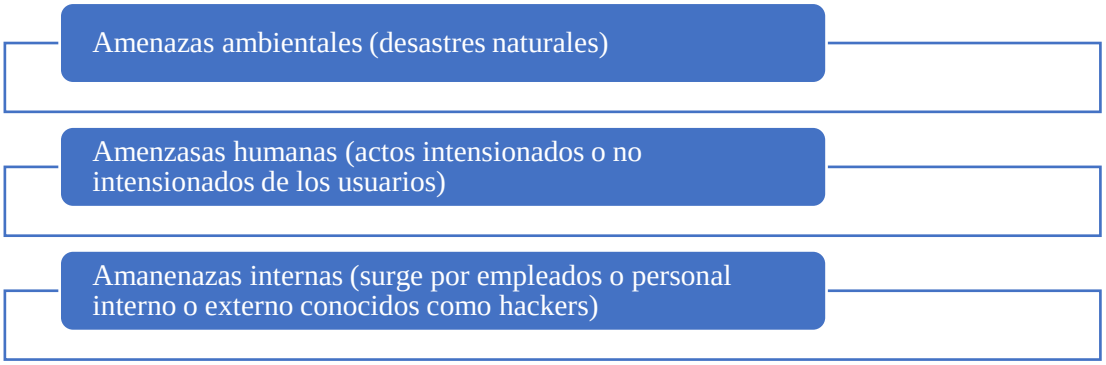


Figura 2. **Identificación de posibles amenazas**

Nota: Tomado de (Martín, 2018)

Para identificarlas se debe de aplicar una evaluación de riesgos precisa, dado que se requiere entender que las vulnerabilidades asociado a las malas configuraciones son las que generan amenazas que llegan a perjudicar significativamente a una empresa o usuario.

Análisis del Impacto

Luego de haber identificado las amenazas y activos se procede a realizar el análisis de impacto para determinar las consecuencias que podrían ser una amenaza y de las cuales puede materializar a un negocio o empresa. En este sentido, se examina si incluye la evaluación de pérdidas económicas, reputación y en general otros efectos intangibles o tangibles. Por tales razones, se debe de asimilar el impacto de las amenazas para priorizar la gestión de riesgos (Maillo, 2021).

Priorización de las Amenazas

En este punto se procede a priorizar las amenazas identificadas en los anteriores apartados, aquí se evalúa tanto el impacto como la probabilidad de ocurrencia (likelihood of occurrence) de cada amenaza. Para ello, se debe de centrarse en las amenazas más relevantes y críticas las que tienen mayor probabilidad de impacto. Se recomienda en utilizar CVSS (Common Vulnerability Scorin System) para asignar los respectivos valores identificados (Maillo, 2021).

Identificación de Técnicas de Mitigación del Riesgo

Luego de haber priorizado las amenazas, es fundamental buscar e implementar soluciones para mitigar el riesgo detectado. A continuación, se procede a presentar las posibles implementaciones de medidas y tecnología de seguridad.

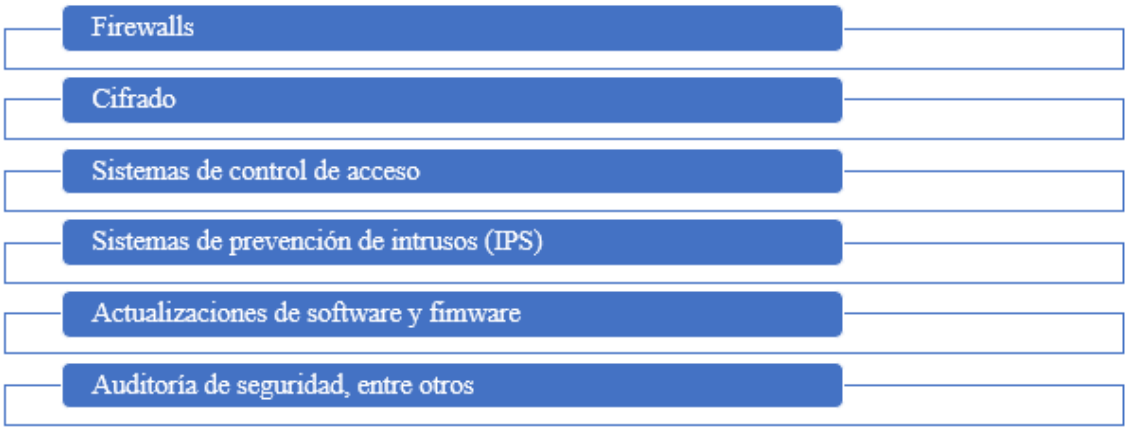


***Figura 3*. Identificación de técnicas de mitigación del riesgo**
Nota: Tomado de (Cuevas et al., 2018)

Con la ejecución de una correcta gestión de riesgos permitirá salvaguardar la data y proteger los activos críticos de la empresa. Sin embargo, con la implementación de

gestión de riesgos no solo se puede abordar las amenazas existentes si no también se puede anticipar diversos marcos y estándares, tales como: COBIT, ITIL, ISO 27001 y NIST, con ello permitirá que una organización pueda guiar y fortalecer su seguridad informática (Cuevas et al., 2018).

Evaluación del Riesgo Residual

Una vez aplicada la mitigación a los riesgos detectados se procede a aplicar una reevaluación y asegurarse de que las vulnerabilidades detectadas se han minimizado o suprimido. Sin embargo, cabe mencionar que cualquier tipo de amenaza que aún persista se considera riesgo residual y debe de gestionarse en base a las políticas de seguridad. Por tales razones este último proceso es crítica para asegurar que no pasen por alto los riesgos que podrían afectar la seguridad de la información.

2.3.2 Pentesting

Debido a los avances en el desarrollo de software malicioso, se propone la implementación y uso de esta tecnología de ciberseguridad en instituciones y empresas, que incluye ataques a entornos informáticos virtualizados o controlados con el objetivo de: descubrir y explotar vulnerabilidades, registrar ataques. La inteligencia de seguridad consiste en realizar una evaluación de seguridad de un sistema que simula un ciberataque destinado a manipular información, robar información o tomar el control de un sistema que es conocido por los expertos y no ha sido abordado o mal abordado, sin embargo, según (Altulaihan et al., 2023) mencionan en su artículo al Pentesting como "Una evaluación de seguridad del sistema que utiliza ataques del mundo real para determinar formas de eludir los mecanismos de seguridad de aplicaciones, sistemas o redes"(p. 10).

Al respecto se puede argumentar que la metodología denominada Pentesting es reconocido como pruebas de penetración, siendo así un método usado por los diversos tipos de hackers para evaluar y entender de manera controlada sistemas informáticos, redes, equipos tic dentro de una empresa. El alcance de este método es identificar y corregir proactivamente las vulnerabilidades encontradas. Por lo tanto, los procedimientos y técnicas utilizados durante todo el proceso de prueba son similares a los usados por los ciberdelincuentes en ataques reales, pero la diferencia es que los hackers buscan robar, destruir o editar información, esto con la finalidad de obtener ganancias financieras, los expertos en ciberseguridad en especial de penetración tienen como

objetivo descubrir vulnerabilidades existentes y contribuir a reforzar los sistemas para prevenir futuros ataques.

Adicional a ello, mencionan que es una práctica o método utilizado para revelar vulnerabilidades y/o fallos de seguridad en sistemas informáticos, páginas web, seguridad física o cualquier otro entorno relacionado con la tecnología, y es útil para las organizaciones, ya que pueden explorar el alcance de sus redes internas. Los sistemas informáticos están protegidos contra ataques informáticos y están diseñados para clasificar y establecer el alcance y el impacto de las fallas de seguridad, proporcionando a las empresas resultados que pueden identificar la información o el entorno que pudo haber estado expuesto a ellas durante un ataque, así como evaluar la efectividad. de sus defensas (Zafra, 2017).

2.3.3 Tipos de Pentesting

Las pruebas de penetración se clasifican de acuerdo a la investigación realizada por Gaviria (2015):

- **Pruebas de penetración con objetivo**: búsqueda de vulnerabilidades en partes específicas de los sistemas informáticos críticos dentro de una compañía.
- **Pruebas de penetración sin objetivo:** implican en analizar y validar todos los componentes de los sistemas informáticos de propiedad de una empresa.
- **Pruebas de penetración a ciegas:** estas pruebas utilizan únicamente información disponible públicamente sobre la compañía.
- **Pruebas de penetración informadas:** usa data privada de una compañía sobre sus sistemas informáticos. Este tipo de prueba implica simular un ataque por parte de una organización que tiene acceso limitado a información privilegiada.
- **Pruebas de penetración externas:** se realizan fuera de las instalaciones de la empresa. El objetivo es estimar los mecanismos de seguridad informática de la compañía.
- **Pruebas de penetración internas:** son ejecutados dentro de las instalaciones de la empresa, como meta es evaluar las políticas y mecanismos internos de seguridad en la misma (p. 100).

Sin embargo, al respecto se pueden presentar otros tipos de Pentesting, esto depende del tipo de data que se tenga sobre el sistema al que se quiere aplicar la evaluación, tales como:

Figura 4. **Tipos de Pentesting**

Nota: Tomado de Gaviria (2015)

- **Caja Blanca:** son más fáciles de practicar como parte de un análisis integral porque una organización proporciona todo tipo de data posible, como la cantidad de dispositivos, tipo de sistema, estructura de la red, entre otros. Se usa la mayor cantidad de datos posible para descubrir los puntos de falla o vulnerabilidades potenciales, lo que resulta en tiempos de ejecución más largos en comparación con otros tipos de pruebas. Al respecto, según Sekhon et al., (2022), define el white-box como "el pentester tiene conocimiento completo de la información sobre el objetivo y el tester deberá identificar cualquier debilidad conocida o desconocida que pueda existir" (p. 101).

- **Caja Negra:** este tipo de pruebas es ciega, debido a que no tiene información sobre sistemas de infraestructura, redes, contraseñas, entre otros. Se acerca a la realidad de una empresa y ayuda a comprender qué tan fuerte o frágil es una organización. Al respecto también, argumentan que según (Febriyanti et al., 2021) da la definición de que "los probadores de penetración no saben nada sobre el sistema. Normalmente se usa cuando una corporación constante realiza el trabajo desde la perspectiva de un posible atacante externo" (p. 99).

- **Caja Gris:** es una mezcla de las anteriores y se usa cuando se requieren saber las vulnerabilidades de determinados sectores, es muy rentable y facilitar información real sobre las amenazas (Zafra, 2017). Sin embargo, según (Nguyen et al., 2023)

menciona que este es un caso intermedio entre el White-Box y Black-Box, ya que como explica el indica, “el pentester hace pasar por un empleado interno, por lo cual recibe un nombre de usuario y una contraseña del sistema. El alcance es encontrar problemas que puedan ser aprovechados por los usuarios internos” (p. 100). El pentester tiene conocimiento del sistema de una pero no de su estructura en sí.

2.3.4 Alcance del Pentesting

Se delimita el alcance que tendrá el Pentesting y se establecen las personas a cargo, las reglas y normas deben estar muy bien detalladas para ver hasta qué nivel se podrá llegar con dichas pruebas.

Todas las pruebas que se ejecutan en el Pentesting se realizan con herramientas de software libre y propietario, se garantizara que la información obtenida no sea de alcance público y que sea lo más privada posible. Se determinan las amenazas y vulnerabilidades para observarlos riesgos funcionales a los que están expuestos los servicios de la red.

Al finalizar con el análisis se podrá establecer los informes en donde se contemplará una lista de todas las vulnerabilidades encontradas de cada una de sus aplicaciones. También se realizará las respectivas recomendaciones y corrección de una de las vulnerabilidades de una aplicación web para que se tomen más controles al momento de realizar una nueva aplicación en la institución (Gaviria et al., 2015).

2.3.5 Fases de Pentesting

Para aplicar el test de penetración tiene de diversas fases, mismas que pueden ir agrupando en tres bloques fundamentales: preparación, ejecución y penetración de resultados (Nuñez, 2021).

2.3.5.1 Fase de Preparación

En esta fase se comienza con el paso de preparación, también conocida como fase preliminar, donde se realiza diversos para determinar los parámetros y objetivos del examen. Entre otros que en brese se menciona:

- **Recolección de información inicial:** antes de iniciar, el equipo de pruebas de penetración tiene que poseer data elemental en base a la organización.

Incluyendo: ubicaciones geográficas, tamaño de la red, sistemas operativos usados y las aplicaciones críticas.

- **Definición del alcance:** determina claramente qué redes, sistemas o aplicaciones incluirán en la prueba y cuáles no se tomarán en cuenta.
- **Acuerdo de confidencialidad (NDA):** establece un acuerdo de confidencialidad entre el equipo de prueba y la empresa. El NDA brinda protección de la data sensible y garantoza que los resultados y hallazgos mantengan absoluta confidencialidad.
- **Roles y responsabilidades:** establece roles y responsabilidades para el equipo de test y la empresa. Incluye el punto de contacto en la compañía, duración de los test y detalles logísticos (Nuñez, 2021).

2.3.5.2 Fase de ejecución

Etapa central de las pruebas de penetración, donde se llevará a cabo su correcta ejecución, para lo cual se lleva a cabo las operaciones técnicas para detectar vulnerabilidades y testear la seguridad informática de una empresa. A continuación, se refleja algunas etapas que se debe de tomar en cuenta:

- **Escaneo y enumeración:** se debe de aplicar un escaneo profundo, donde se determinar los activos, sistemas operativos, puertos abiertos, aplicaciones activas y servicios de la infraestructura de la empresa, por medio la utilización de un software de escaneo de red.
- **Análisis de vulnerabilidades:** tras el escaneo, los sistemas y aplicaciones se someten a una investigación exhaustiva para detectar las vulnerabilidades particulares. Para ello se puede usar procedimientos de revisión manual, por ejemplo: herramientas de análisis de seguridad.
- **Exploración de vulnerabilidades:** hallan vulnerabilidades para entablar respectivas medidas preventivas de seguridad.
- **Limpieza y restauración:** una vez finalizada la etapa de la aplicación de medidas correctivas de vulnerabilidades, se debe de restaurar la red a su configuración inicial, borrar cualquier acceso o huella digital no deseada. Con ello, la empresa está protegida contra cualquier tipo de riesgos injustificado (Nuñez, 2021).

2.3.5.3 Fase de resultados

Para lograr asegurar los hallazgos se comuniquen los resultados conseguidos de manera efectiva a la empresa, consiguiendo un mejor enfoque de las vulnerabilidades encontradas. En breve, se presenta los detalles de esta fase.

- **Informe y documentación detallada:** presenta un informe completo, donde se detalla todas las vulnerabilidades encontradas, nivel de criticidad, evidencia de explotación y recomendaciones de mitigación. Dicho informe es considerado como una herramienta invaluable para la toma de decisiones.
- **Reunión y presentación:** coordina una reunión entre el cliente o la empresa para presentar dicho discutir e informe de los resultados encontrados, así también las implicaciones y las acciones que se deben de seguir. Dicha reunión permitirá aclarar cualquier tipo de pregunta y establecer un plan de acción.
- **Seguimiento y revisión:** una vez finalizada la presentación se debe de realizar un seguimiento para asegurar que las recomendaciones sean implementadas y las vulnerabilidades se corrijan. Con ello mejorará la seguridad general de la empresa (Nuñez, 2021).

2.3.6 Procedimientos Legales para el Pentesting

En las pruebas de penetración se necesita el permiso de las autoridades de los GADS, las mismas deben ser debidamente firmada y selladas por el responsable a cargo del departamento de Tic (Zhou et al., 2021).

2.3.7 Metodologías de Pentesting

Existen diferentes tipos de procesos que se puede seguir para desarrollar una prueba de penetración. Sin embargo, aquellos pentesters experimentados son capaces de generar su propia metodología, por ello es importante estar familiarizado con algunas definiciones, tales como:

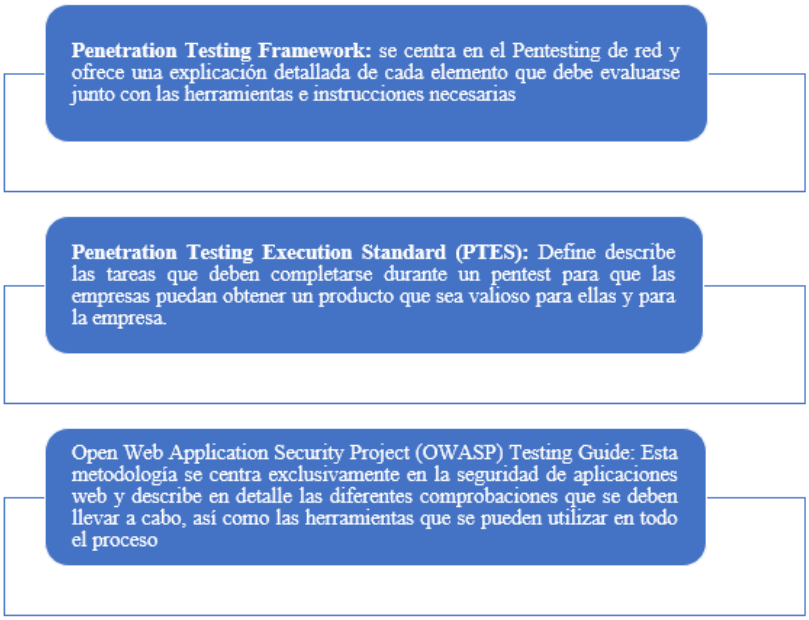


Figura 5. **Posibles metodologías pestesting**
Nota: Tomado de (Echeverría, 2024)

2.3.8 Introducción al Hacking Ético

Con la evolución de la tecnología, también con el avance de internet y las aplicaciones móviles y web, han surgido varios problemas de seguridad de datos públicos y privados, pérdida de data e intentos impredecibles de seguridad de la red e información. En general, en el campo de las tecnologías de la información, la palabra "hacker" se correlaciona generalmente con el crimen cibernético: pirateo informático, violación de las normas de la seguridad informática y todo lo que conduce al crimen cibernético. Ahora, además de la palabra "hacking", agregándole la palabra "ético", la sociedad regularmente piensa o asimila que se trata de cierta incoherencia, por lo que es esencial entender claramente lo que hace y provoca ejecutar hacking ético (Ortega-Garcés, 2023).

Al respecto Rodríguez (2020), menciona que a lo largo de los años el denominado "Hacking ético" ha sido combinado por dos vocablos: *ético* se refiere a que es algo correcto, bueno y en cambio *hacking* es todo lo contrario porque es considerado como una infiltración y sustracción de cierta información de único valor para una persona o empresa (p.23).

Este proyecto tiene como objetivo decidir si los sistemas informáticos son vulnerables y generar soluciones mediante el uso de un conjunto de herramientas informáticas para

dominios de pruebas de penetración; Pentests, ya que el evaluador o auditor que utilice las aplicaciones no es directamente un criminal o hacker, sino porque aplicaciones diferentes herramientas que pertenecen a la seguridad informática se logra demostrar las vulnerabilidades y las amenazas potenciales se encuentran en la red o el sistema informático a las víctimas y brindan la debida protección después de realizar la prueba, para determinar si ofrece un nivel de seguridad aceptable que pueda reducir la seguridad de la red o cualquier riesgo de ataque que perjudique a una empresa.

2.3.9 Hackers

Al respecto, firma Cuadros et al., (2022) el hacking ético o pruebas de penetración se considera un procedimiento de ciberseguridad porque implica infiltrarse en un sistema o red informática con el consentimiento del propietario, simulando un ataque del mundo real con el objetivo de exponer debilidades y vulnerabilidades que los ciberdelincuentes pueden aprovechar. Esto permite a las empresas comprender las necesidades de seguridad que enfrentan y mejorar sus sistemas según sea necesario (p. 145).

En conclusión, los *hackers* han tenido mala fama con el paso de los años, sin embargo, no todos son consideramos como cibernéticos. Para lo cual se han determinado diversas definiciones y términos como: *crakers* y *hackers éticos.* En donde: los primeros son aquellos que aplican técnicas de intrusión con la única finalidad de hacer daño y conseguir beneficios económicos, el segundo término son en cambio con fines éticos, quienes implementan soluciones ante un inconveniente relacionado con la seguridad informática.

En tal sentido, se plantean diversas preguntas como: ¿puede ser ético el hacking?

Para un mayor entendimiento se describen ciertas diferencias los siguientes términos relevantes.

- **Hacker:** nuevo término usado para designar expertos (maestros) en varios o específicos campos técnicos relacionados con las TIC y las telecomunicaciones: sistemas operativos, programación, redes, etc.
- **Cracker:** es una persona que vulnera la seguridad de un sistema informático de la misma forma que un hacker, excepto que, a diferencia de este último, ataca con fines de lucro y cualquier forma de beneficio personal.

- **Hacker ético:** un experto técnico en seguridad que utiliza sus conocimientos de hacking para lograr objetivos de seguridad en un entorno legal y controlado. (Bonilla, 2023).

2.3.10 Tipos de Hackers

La palabra hacker en sí no define si una persona utiliza su conocimiento para el bien o para el mal, por cual este término se divide en tres tipos, según (Scariot, 2022):

- **Hackers de sombrero blanco:** también conocido como hackers éticos, son considerados profesionales de la seguridad informática quienes realizan pruebas de penetración a una empresa para buscar vulnerabilidades de seguridad, siempre y cuando sea este ejecutado con el consentimiento de las personas encargas de TIC.
- **Hackers de sombrero negro:** son lo opuesto a los hackers de sombrero blanco, también son conocidos como crakcers ya que no cooperan con una organización, si no buscan causar daño y robar información para perturbar y dañar sistemas con fines propios o de terceros.
- **Hackers de sombrero gris**: aunque el término es un poco ambiguo, se puede argumentar que es una mezcla híbrida entre los hackers de sombrero blanco y sombrero negro (Scariot, 2022).

En relación con los tipos de hackers se puede argumentar que: sombrero blanco (*White hat*) y sombrero negro (*black hat*). Donde: los hackers que tienen sombrero blanco con los hackers éticos; mientras que los de sombrero negro son los que explotan las vulnerabilidades en los sistemas con el único fin de demostrar que han logrado vulnerar la seguridad de dicha entidad. En breve se presenta la siguiente figura para una mejor ilustración y entendimiento de lo expuesto. Finalmente, los de sombrero gris es una combinación de los tipos de hackers mencionados anteriormente.

Figura 6. **Tipos de hacking ético**

Nota: Elaboración propia

2.3.11 Hacking ético vs Auditoría Informática

En materia de seguridad, existe cierta confusión entre hacking ético y auditoría informática. De hecho, confunde a mucha gente. Sin embargo, existen diferencias significativas entre estos dos términos, donde: la auditoría informática se ocupa de las políticas de seguridad de una compañía y su cumplimiento o aplicación dentro de los procesos. Está diseñado para comprobar que existen controles de seguridad y en muchos casos puede no ser técnico. Por otra parte el hacking ético se centra en vulnerabilidades que pueden ser explotadas por terceros y que pueden utilizarse para comprobar que el sistema es resistente a ataques (Scariot, 2022); (Imbaquingo et al., 2020).

2.3.12 Definición de Penetration Test o Ethical Hacking

En cuanto al Pentesting Nur et al., (2020) explica que:
Las pruebas de penetración son un conjunto de métodos y técnicas para la evaluación integral de las vulnerabilidades de los sistemas informáticos. Consiste en un modelo que puede reproducir el intento de acceso de un potencial intruso a cualquier entorno informático desde varios puntos de entrada existentes (internos y externos). El propósito general de una prueba de penetración es obtener acceso al equipo informático de la

organización para obtener derechos de administrador del sistema y desarrollar cualquier tarea no permitida en el equipo. Además, se pueden establecer otros objetivos secundarios para permitir ejecutar pruebas específicas para áreas comerciales específicas.

2.3.13 Fuente de pruebas de la red

Según Léonard & Kaunert (2023) en el que citó a *European Union Agency For Network And Information Security* (2016), las pruebas de la red pueden obtenerse a partir de diversas fuentes, a continuación, se mencionan las siguientes:

- **Intervenir el cable y el aire:** una de las formas más directas de captura de información es colocar escuchas en los cables de red y cables de fibra óptica para monitorear el tráfico.
- **Tabla CAM en un conmutador de red:** contienen tablas de memoria direccionables por contenido que almacenan correspondencias entre las direcciones MAC del sistema y los puertos físicos. Con esta tabla, la dirección MAC de un sistema comprometido se puede encontrar en la red porque hay asignaciones disponibles para puertos físicos. Los conmutadores también proporcionan duplicación de red, lo que permite a los investigadores ver todo el tráfico de otras VLAN y sistemas.
- **Tablas de enrutamiento en los routers:** la tabla de enrutamiento de un router asigna los puertos este aparato a las redes a las que están conectados. Estas tablas le permiten explorar las rutas que toma el tráfico web a medida que avanza a través de diferentes dispositivos.
- **Registros del protocolo de configuración dinámica de host:** por sus siglas es denominado como (DHCP) registran entradas cuando se asigna una dirección IP específica a una dirección MAC concreta. Por lo tanto, la dirección IP específica se asigna a una dirección MAC particular, cuando se renovó la dirección en la red, la marca de tiempo en que se renovó, etc., por lo que son de utilidad en la red forense.
- **Registros del servidor DNS:** los registros de consulta de nombres del servidor pueden ayudar a entender la resolución de IP a nombre de host en momentos específicos. Por ejemplo, en un escenario en el que, tan pronto como un sistema se infectó con malware en la red, trató de conectarse de nuevo a un determinado dominio para el comando y control.

- **Registros de controladores de dominio/servidores de autenticación/sistemas:** Los servidores de autenticación pueden permitir a los investigadores ver los intentos de inicio de sesión, los tiempos de inicio de sesión y otras actividades relacionadas con el inicio de sesión en la red. En tal escenario, un grupo de atacantes, para iniciar sesión en un servidor de base de datos utilizando un host infectado como plataforma de lanzamiento o centro. En tales casos, los registros de autenticación revelan rápidamente no sólo el sistema infectado, sino también el número de intentos fallidos desde el sistema al servidor de la base de datos.
- **Registros de IDS/IPS:** desde una perspectiva forense, los registros de prevención y detección de intrusiones son registros IDS/IDPS prácticos que proporcionan no solo direcciones IP, sino también firmas relevantes, ataques en curso, presencia de malware, servidores de comando y control, IP y puertos de origen y destino, horarios, etc.
- **Registros del cortafuego:** los registros del firewall brindan una descripción detallada de la actividad de la red. Por lo tanto, una solución de firewall no solo protege un servidor o una red de conexiones no deseadas, sino que también puede ayudar a identificar patrones de tráfico, proporcionar una puntuación de confiabilidad para los puntos finales salientes y bloquear puertos e intentos de conexión no deseados.
- **Registros del servidor proxy:** son una de las herramientas más útiles en las investigaciones forenses. Los registros de agentes web ayudan a detectar amenazas internas y, al mismo tiempo, brindan información detallada sobre eventos como hábitos de navegación, origen de malware web y comportamiento de un usuario en la red.

CAPITULO III

3 MARCO METODOLOGICO

A continuación, en este apartado se procede a describir los elementos metodológicos que enmarcan la investigación, en función de alcanzar los objetivos trazados inicialmente.

3.1 Descripción del área de estudio / Descripción del grupo de estudio

El proyecto de estudio será validado en la compañía MASTERNET, ubicada en la Provincia de Santo Domingo de los Tsáchilas. Dicha corporación está dedica a la venta al por mayor y menos de equipos tecnológicos y brinda soporte técnico en sitio.

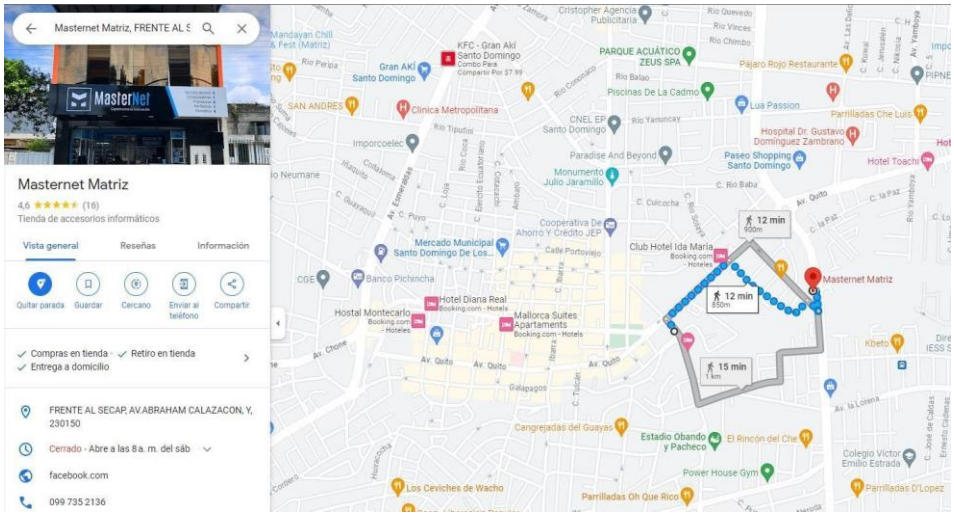


Figura 2. **Ubicación de la empresa MATERNET**
Nota: Tomado de Google Maps

Actualmente, MASTERNET está confirmado por alrededor de 12 colaboradores mismos que están distribuidos en 5 áreas en la matriz y sucursal: Ventas, Marketing, Talento Humano;Contabilidad y Soporte Técnico.

3.2 Método de investigación

En este apartado, se definen los principales elementos de la investigación, que son el tipo y nivel, de los cuáles se derivan el resto.

3.2.1 Método inductivo – deductivo

El presente estudio, inicia desde los hechos reales suscitados en la empresa MASTERNET, para posteriormente formular hipótesis para luego plantear y estructurar acordemente la problemática, en esta primera fase se utiliza la inducción. Posteriormente, se llega a la deducción por medio de la teoría existente para luego contrarrestarla nuevamente con la realidad. Ahora bien, en la ejecución del Pestesting, también se llega a formular hipótesis por medio de la inducción y de los hechos en base a la relevancia de usarlo para minimizar el nivel de impacto de los ciberataques que se han presentado en la corporación, seguidamente la aplicación apoyada por la teoría existente como metodologías, herramientas, análisis de expertos, casos reales, entre otros. De esta manera se podrá llegar a contrarrestar con la realidad.

3.2.2 Tipo de Investigación

Este estudio es aplicado, porque se usa el conocimiento teórico para proponer mejoras asertivas y minimizar inconvenientes relacionadas con la ciberseguridad. Por tales motivos, se encuentra bajo la perspectiva cuantitativa; esto tomando como referencia lo indicado por Chacma-Lara & Laura-Chávez (2021), quienes en su obra plasma que esta perspectiva responde al hecho de aplicar técnicas y herramientas de recolección y análisis de datos, de hecho no se presta atención a los estados subjetivos de quien actúa, también hace hincapié en que se utiliza medición controlada, de manera objetiva y con orientación a comprobación y al resultado, así como también utiliza el método hipotético-deductivo, pone énfasis en la confiabilidad de los datos, se centra en generalizar y asume una realidad con alteraciones despreciables.

Por tanto, este estudio se basa en supuestos cuantitativos, porque se va a recopilar, procesar y analizar información numérica sobre las variables preseleccionadas. Esto permite darle más que una simple lista de datos ordenados como resultados, ellos corresponden completamente a las variables declaradas desde el inicio, y los resultados resultantes darán la realidad específica a la que están expuestos.

Lo expresado anteriormente, se busca implementar la aplicación de los conocimientos adquiridos durante todo este proceso de aprendizaje relacionados al Pestesting, así mismo las herramientas de software para la ejecución de cada fase de esta metodología, mediante

su ejecución. Por tales motivos, se ve en la necesidad de proponer mejoras y estrategias más apropiadas para así reforzar la seguridad informática de MASTERNET.

3.2.3 Nivel de la Investigación

Por consecuente, dicha investigación se centra en un nivel descriptivo, por cuanto Condori-Ojeda (2020), quien plantea que este nivel de investigación se caracteriza por develar un hecho, individuo o grupo, fenómeno, con el fin de declarar un esquema de funcionamiento o comportamiento. El nivel descriptivo, posibilita comprender a través del registro, análisis e interpretación de la situación en tiempo real, de igual manera, los estudios descriptivos llegan finalmente a conclusiones generales construidas, que dan cuenta de los hechos observados y se llaman generalizaciones empíricas.

Las generalizaciones empíricas pueden ser consideradas como hipótesis teóricas o de trabajo, por quienes encaran otras investigaciones y usan dichas hipótesis para explicar hechos o quieren saber si las hipótesis funcionan. Por lo tanto, asumiendo este nivel de investigación descriptivo, se pudo explicar los diversos inconvenientes que ha presentado la empresa MASTERNET ante los ciberataques, evidenciado por los experimentos realizados.

3.3 Diseño de investigación

En este apartado el diseño de investigación se efectúa de manera no experimental, debido a que es aquella que no se controla ni manipula las variables de esta investigación. Dichos datos conseguidos a raíz de las fases del Pestesting: reconocimiento, escaneo, explotación y post explotación de vulnerabilidades. Debido a que cada fase se va a ir recolectando en función de la data real por medio de las herramientas de software.

3.4 Población y Muestra

3.4.1 Población

Al respecto (Condori-Ojeda, 2020b), en su investigación indica que población representa el conglomerados de individuos (personas u objetos) con características semejantes que pueden ser cuantificados o no, pero son sujetos a una investigación. Por tales motivos y según las características descritas, este estudio es ejecutable para una sola población la cual está conformada por 12 personas que trabajan y por lo cual existe un total de 12 equipos de cómputo en MASTERNET.

3.4.2 Muestra

Según (Condori-Ojeda, 2020b) en su estudio menciona que "es una parte representativa de la población, donde las características deben reproducirse con la mayor precisión posible, para lo cual se debe de poseer una población extensa y así determinar la muestra según la formula estipulada" (p. 141). Por otra parte, por tratarse de una población finita y su objeto de estudio es relativamente pequeña, para esta investigación se utilizó la población parcial, una muestra representativa; es decir de la población del personal de todas sus áreas no se le determinó ni se aplicó ningún muestreo, por tratarse de un grupo pequeño.

3.5 Técnicas e Instrumento de Recolección de Datos

Técnicas

- **Observación:** permite analizar y observar el impacto que causa de acuerdo al aprovechamiento de vulnerabilidades y materialización de los riesgos luego de un ciberataque.
- **Experimentación:** permite experimentar cada una de las herramientas de software inclinada a cada una de las fases de Pentesting con la finalidad de recaudar datos e identificar vulnerabilidades.
- **Encuesta:** permite usar una lista de verificación para saber si MASTERNET tiene controles o medidas de seguridad informática basado en el tratamiento de vulnerabilidades.

De la misma manera se recolectó información en base a cada fase de la metodología Pentesting, tales como:

Tabla 2.

Fase 1: Reconocimiento

FASE 1: Reconocimiento

TÉCNICA DE PESTESTING	HERRAMIENTA DE SOFTWARE
IDENTIFICACIÓN DE REDES	Nmap

Nota: Elaboración propia

Tabla 3.

Fase 2: Escaneo

FASE 2: Escaneo

TÉCNICA DE PESTESTING	HERRAMIENTA DE SOFTWARE
BARRIDO DE PUERTOS	Nmap

Nota: Elaboración propia

Tabla 4.

Fase 3: Explotación de vulnerabilidades

FASE 3: Explotación de vulnerabilidades

TÉCNICA DE PESTESTING	HERRAMIENTA DE SOFTWARE
EXPLOTACIÓN DE VULNERABILIDADES ENCONTRADAS EN LAS FASES PREVISTAS	Metasploit, Hydra

Nota: Elaboración propia

Análisis de datos

- **Análisis e interpretación:** aplica un análisis e interpretación de toda la información y desde luego aquellos resultados conseguidos en cada fase de la metodología Pentesting.
- **Gráficos y tablas:** con el uso de los gráficos dará lugar a una mejor presentación de los datos conseguidos, los gráficos se basarán en relación con el estudio del estado de la red que tiene actualmente la empresa.

3.6 Herramientas por utilizar

El sistema operativo para utilizar para realización de este trabajo es Kali Linux, el mismo está diseñado para desarrollar auditorías de seguridad, escaneos de puertos, escaneos de vulnerabilidad de redes y bases de datos, herramientas de auditoría, análisis forenses utilizados por "pentesters" o hackers éticos en pruebas de penetración para verificar el funcionamiento de servicios no autorizados o descubrir posibles objetivos de ataque.

Adicional a ello, en un caso en particular se utilizará para identificar y/o corregir problemas en la red telemática de la empresa MASTERNET:

En breve, se presenta una breve descripción de las herramientas usadas:

Tabla 5.

Herramientas usadas

HERRAMIENTA	**DESCRIPCIÓN**
MSF (METASPLOIT FRAMEWORK) METASPLOIT	Un desarrollo de código abierto relacionado con la seguridad informática que emite información sobre vulnerabilidades de seguridad y ayuda con las pruebas de penetración y el desarrollo de firmas para sistemas de detección de intrusiones. El subproyecto más famoso es Metasploit Framework, una herramienta para diseñar y ejecutar acciones maliciosas contra ordenadores remotos. Otros subproyectos importantes incluyen repositorios de códigos de operación, archivos de shellcode e investigación de seguridad. Fue creado originalmente usando el lenguaje de programación Perl, aunque el marco Metasploit ahora ha sido completamente reescrito en Ruby.
NMAP	Nmap ("Network Mapper") constituida como una herramienta de auditoría de seguridad y escaneo de redes de código abierto. Se encuentra diseñado para un análisis rápido de redes grandes, aunque también es muy eficiente para PC. Nmap usa paquetes IP "sin procesar" en su forma original para identificar las computadoras en la red, los servicios que brindan (nombre y versión de la aplicación) y el sistema operativo (versiones).
E**XPLOIT**	Es una pieza de software, un fragmento de datos o una secuencia de comandos o acciones que se usan para explotar las vulnerabilidades de seguridad en un sistema de información para lograr una acción no deseada. Se utiliza principalmente como vector para inyectar cargas útiles que le dan al atacante cierto acceso y/o control sobre la computadora infectada. Una sola carga útil puede ser utilizada por múltiples vulnerabilidades y la

	misma vulnerabilidad puede ser utilizada por múltiples cargas útiles.
ARMITAGE	(Herramienta que admite la utilización de un Scripts para Metasploit y que permite visualizar objetivos, recomienda exploits y expone las características avanzadas de post-explotación que tiene el framework)

Nota: Elaboración propia

Entre las herramientas técnicas que se utilizará en el desarrollo de esta propuesta son:

- Sistemas operativos: Windows, Linux.
- Aplicaciones: Web, móviles, de escritorio, software a medida.
- Redes: LAN, WAN, Wi-Fi, etc.

CAPITULO IV

4 DESARROLLO DE LOS OBJETIVOS

Para alcanzar el objetivo general de esta investigación, el esquema que se siguió fue aplicar la metodología de pentesting, como marco de referencia, lo que permitió evaluar el sistema de red informática de la empresa MASTERNET. Al aplicar las fases de estas guías, se validó su pertinencia y se identificaron las adaptaciones necesarias dadas las particularidades de la plataforma, así como también permitió determinar las herramientas disponibles y funcionales, que refuerzan las secuencias de actividades sugeridas por la metodología base. En los próximos apartados se detallan como se desarrolló cada uno de los pasos metodológicos.

4.1 Fase determinación alcance

Las variables estudiadas en la investigación fueron: Vulnerabilidades en la Red de Datos y Seguridad en Infraestructura Tecnológica.

4.2 Fase Recolección de información

Esta fase tiene como finalidad describir el sistema bajo estudio, mediante la adquisición de información relevante para identificar las vulnerabilidades en cuanto a seguridad de información. En el transcurso de la revisión se aplicó un cuestionario, plasmado en el anexo A, con el cual fue diseñado para conocer la existencia, uso y orientación de políticas de seguridad de información e históricos de eventos.

En breve se procede a presentar las siguientes representaciones gráficas, donde:

- El numeral 1 corresponde a la respuesta Nunca
- El numeral 2 corresponde a la respuesta Raramente
- El numeral 3 corresponde a la respuesta Ocasionalmente
- El numeral 4 corresponde a la respuesta Frecuentemente
- El numeral 5 corresponde a la respuesta Siempre

Tabla 6.

Diagnóstico del uso de la Red

	NUNCA		RARAMENTE		OCASIONALMENTE		FRECUENTEMENTE		SIEMPRE	
INDICADORES	R	%	R	%	R	%	R	%	R	%
1.- ¿EL USO DE LA RED ES ADECUADO?	0	0%	1	10%	2	20%	1	10%	8	80%
2.- ¿LOS NIVELES DE OPERATIVIDAD SON LOS ÓPTIMOS DE LOS DISPOSITIVOS?	3	30%	6	60%	1	10%	2	20%	0	0%
3.- ¿HAN RECIBIDO ATAQUES A LA RED?	0	0%	0	0%	0	0%	3	30%	9	90%
4.- ¿TIENEN SISTEMA DE RECUPERACIÓN DE FALLAS?	0	0%	0	0%	0	0%	3	30%	9	90%

Nota: Elaboración propia

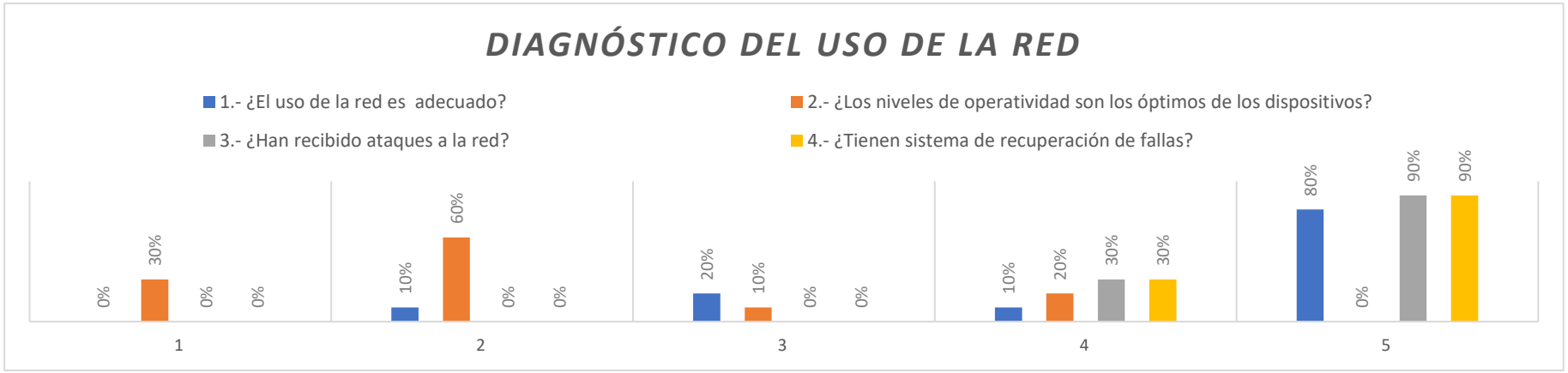


Figura 7. **Diagnóstico del uso de la Red -gráfico**

Nota: Elaboración propia

Los resultados presentados en la tabla 6 y la figura 7 señalan a pesar de no haber tenido ataques, 60% sus niveles de operación no son óptimos y el 90% no tienen sistema de recuperación, luego de la ocurrencia de eventos no deseados, lo que es una gran desventaja para la plataforma tecnológica.

Tabla 7.

Diagnóstico del mantenimiento de la Red

	NUNCA		**RARAMENTE**		**OCASIONALMENTE**		**FRECUENTEMENTE**		**SIEMPRE**	
USO DE LOS DISPOSITIVOS	R	%	R	**%**	R	**%**	R	**%**	R	**%**
1.- ¿UTILIZAN EQUIPOS ESPECIALIZADO CON FRECUENCIA PARA VERIFICAR SU FUNCIONAMIENTO?	9	90%	0	0%	0	0%	0	0%	0	0%
2.- ¿RECIBEN MANTEAMIENTO ADECUADO?	9	90%	2	20%	1	10%	0	0%	0	0%
3.- ¿LOS ESTADOS DE CONEXIÓN CON LOS DEMÁS ELEMENTOS DE LA RED SON LOS ÓPTIMOS?	8	80%	2	2%	2	20%	0	0%	0	0%
4.- ¿UTILIZAN DISPOSITIVOS DE SEGURIDAD SI HUBIERE ATAQUES?	0	0%	0	0%	0	0%	3	30%	9	90%

Nota: Elaboración propia

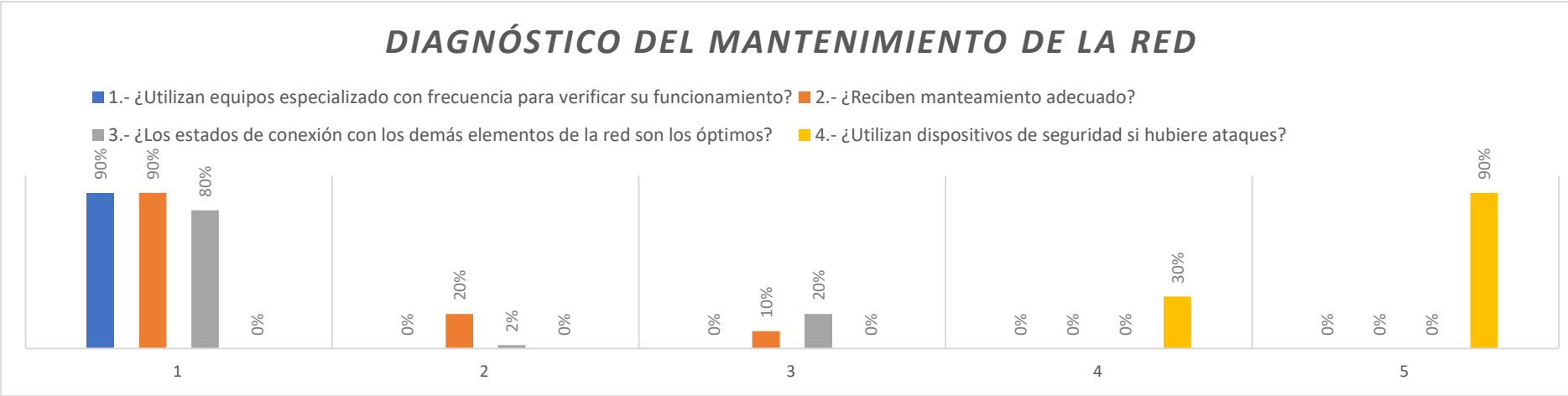


Figura 8. **Diagnóstico del mantenimiento de la Red -gráfico**

Nota: Elaboración propia

En la tabla 7 y la figura 8, se presenta el diagnóstico desde la perspectiva de mantenidito de red, en que se encontró que el 90% no se le ejecuta acciones para mantener la operatividad de red y se si hace no es con los instrumentos adecuados y el 90% no posee dispositivos de seguridad anti-ataques.

De lo expuesto anteriormente, la empresa MASTERNET presentan diversos tipos de problemas de interoperabilidad y de conexión dentro de la red, lo que limita el óptimo funcionamiento de los equipos y decanta en problemas de seguridad, por ende, por lo cual se argumenta que no responderán de manera adecuada ante un ataque cibernético.

4.3 Fase Análisis de vulnerabilidades y explotación.

Para la identificación de las vulnerabilidades, se creó un laboratorio de prueba virtual para el proceso de simulación, con la distribución Kali Linux, aplicativo que consta por un compendio de herramientas diseñadas para probar y encontrar vulnerabilidades en plataforma de información (Singh, 2022),. En tal sentido, con la aplicación de Pestenting resulta útil para la toma de decisiones y posterior la implementación de mejoras de la seguridad de la información que maneja la empresa Masternet.

4.3.1 Construcción del laboratorio de prueba virtual

El laboratorio virtual construido, cuenta con una red, que sirve de plataforma de comunicación a más de 100 equipos de informática, como computadores personales, routers, swich, entre otros equipos en general, los cuales poseen diferentes sistemas operativos y están configurados según las necesidades de sus usuarios.

Ahora bien, se procede en primeras instancias a describir las características técnicas del equipo anfitrión, el cual servirá como punto central, que en este caso se utiliza el ordenador que se usa para brindar soporte técnico en la empresa MASTERNET, para configurar el ambiente de trabajo en este caso cuenta con Procesador i5 Décima Generación, con una memoria RAM de 8192 MB y un sistema operativo Windows 10 Pro de 64 bits.

Figura 9. **Especificación técnica del equipo técnico para aplicar el análisis de vulnerabilidades**

Nota: Elaboración propia

Adicional a ello, se selecciona la siguiente herramienta tipo open source, donde se configuró la máquina virtual (VirtualBox en su última versión) con el sistema Kali Linux, descargado de la página oficial para ejecutar cada una de las fases que Pentesting propone, se configuró la máquina virtual con 8GB de memoria RAM y Unidad de almacenamiento de 60 GB y una tarjeta de red modo NAT para acceder a internet.

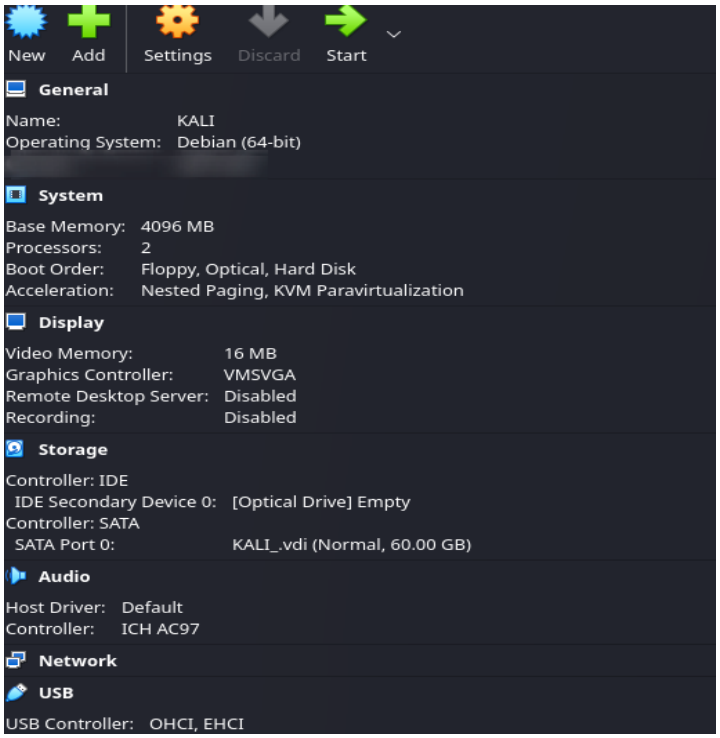


Figura 10. **Descripción técnica del ambiente virtual con Kali Linux**

Nota: Elaboración propia

Una vez instalado el sistema operativo se procede a iniciar y a realizar un Update, a continuación, se presenta el siguiente Dashboard principal de Kali Linux.

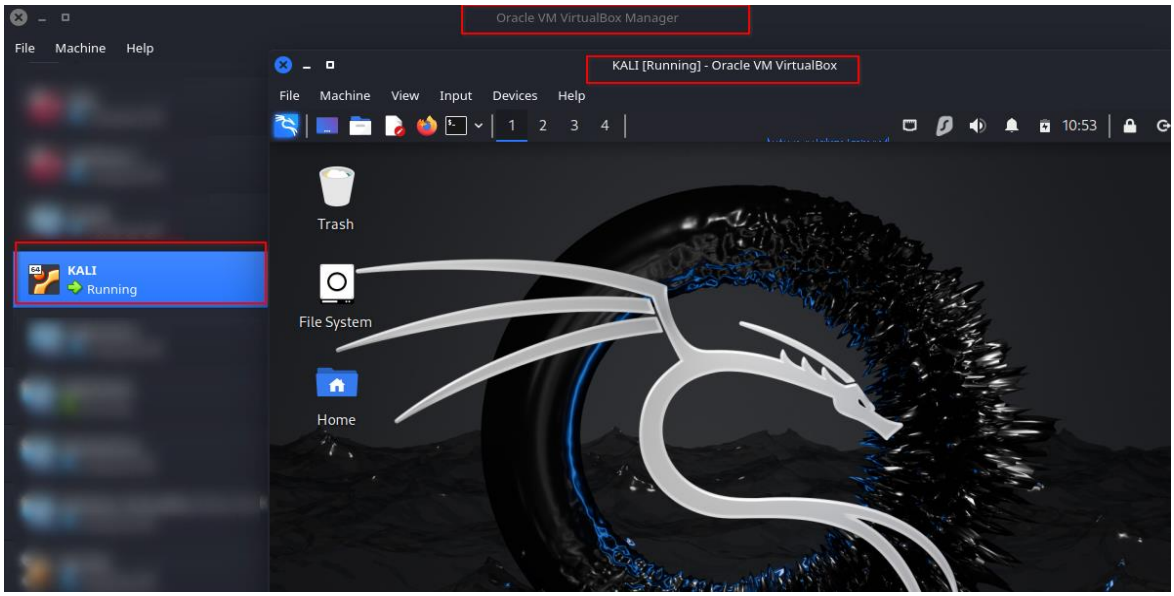


Figura 11. **Máquina Virtual Kali Linux**
Nota: Elaboración propia

4.3.1.1 Identificación y clasificación de vulnerabilidades

Se inició la aplicación de la metodología Pentesting con la actualización de Kali Linux con el usuario root *"apt update"* o con usuario local con los comandos de *sudo apt Update*, ver figura 12 *apt dist-upgrade*, ver figura 13.

4.3.1.2 Actualización en proceso UPDATE

Figura 12. **Actualización de repositorios de Kali Linux**

Nota: Elaboración propia

Posteriormente, se procede a actualizar el software Kali Linux, ver figura 6.

```
┌──(root㉿kali)-[~]
└─# apt dist-upgrade
The following packages were automatically installed and are no longer required:
  fonts-liberation2          libgfapi0          libpoppler134           libqt6sql6t64
  ibverbs-providers          libgfrpc0          libpython3.11-dev       libqt6test6t64
  libarmadillo12             libgfxdr0          libpython3.11-minimal   libqt6widgets6t64
  libassuan0                 libglusterfs0      libpython3.11-stdlib    libqt6xml6t64
  libavformat60              libgspell-1-2      libpython3.11t64        librados2
  libblosc2-3                libibverbs1        libqt6dbus6t64          librdmacm1t64
  libboost-iostreams1.83.0   libimobiledevice6  libqt6gui6t64           libssh-gcrypt-4
  libboost-thread1.83.0      libiniparser1      libqt6network6t64       libusbmuxd6
  libcephfs2                 liblua5.2-0        libqt6opengl6t64        libwireshark17t64
  libgdal34t64               libnghttp3-3       libqt6openglwidgets6t64 libwiretap14t64
  libgeos3.12.2              libplist3          libqt6printsupport6t64  libwsutil15t64
```

Figura 13. **Upgrade del Sistema Operativo**.

Nota: Elaboración propia

Se realizó un reconocimiento de la red de la empresa MASTERNET, la misma presentaba una topología tipo árbol[5], ver Figura 14, contaba con aproximadamente 15 equipos divididos entre las 2 sucursales y los trabajadores que se conectan remotamente, los cuales poseían diferentes sistemas operativos y estaban configurados según los servicios que prestaban.

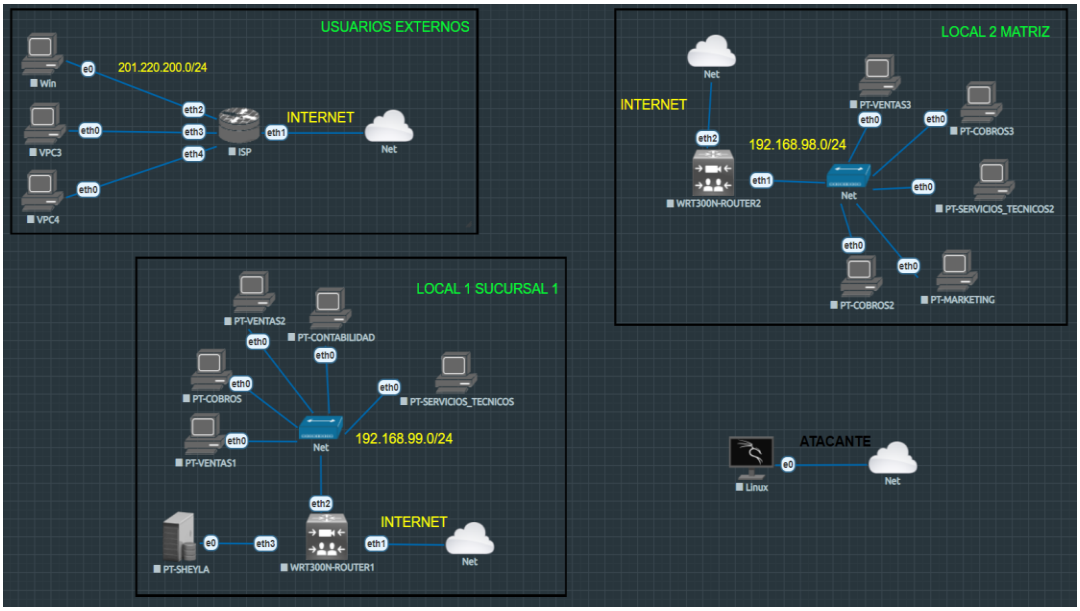


Figura 14. **Topología de Red Inicial**

Nota: Elaboración propia

4.4 Fase escaneo

Para la fase de búsqueda y reconocimiento de equipos y vulnerabilidades se usó NMAP como herramienta primaria NMAP.

[5] La topología de árbol es la combinación de la topología de bus y la topología en estrella. Esta combinación permite a los usuarios tener varios servidores en la red. Conecta múltiples topologías en estrella a otra red de topología en estrella. Se conoce también como topología de estrella expandida o topología jerárquica.

Entonces, se realizó un primer escaneo con esta herramienta para poder conocer aquellos puertos en abiertos y servicios que se encuentran disponibles. En tal sentido es importante mencionar que Nmap usa el protocolo TCP/UDP y para descubrir equipos dentro del mismo segmento de red. TCP se encuentra basado en una conexión y garantiza la conectividad de punto a otro punto. Por medio de la salida de tres vías SYN (saludo), SYN (saludo de retorno) + ACK (confirmación de recepción), ACK (confirmación) y finaliza la comunicación con FIN ACK en el origen y FIN ACK en el destino.

El protocolo UDP no establece una conexión entre el cliente y servidor simplemente envía los paquetes de datos a su destino.

Después del escaneo se encontraron los siguientes puertos abiertos, el resultado del escaneo de las dos sucursales se obtuvo la siguiente tabla 8:

Tabla 8.
Escaneo de dos sucursales

PUERTO	ESTADO	SERVICIO	VERSIÓN IDENTIFICACIÓN
21/TCP	Abierto	FTP	vsftpd 3.0.3
22/TCP	Abierto	SSH	OpenSSH 7.2p2 Ubuntu
445/TCP	Abierto	HTTP	Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/TCP	Abierto	ms-wbt-server	Microsoft Terminal Services
1433/TCP	Abierto	Mysql	Microsoft SQL Server 2016
139/TCP	Abierto	netbios-ssn	Microsoft Windows netbios-ssn
49152/TCP	Abierto	Msrpc	Microsoft Windows RPC
135/TCP	Abierto	Msrpc	Microsoft Windows RPC
49153/TCP	Abierto	Msrpc	Microsoft Windows RPC
49154/TCP	Abierto	Msrpc	Microsoft Windows RPC
49155/TCP	Abierto	Msrpc	Microsoft Windows RPC
49163/TCP	Abierto	Msrpc	Microsoft Windows RPC

445/TCP	Abierto	microsoft-ds	Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
80/TCP	Abierto	http	Microsoft IIS httpd 10.0
49152/TCP	Abierto	Upnp	Portable SDK for UPnP devices 1.4.7 (Windows 6.2.9200 2; UPnP 1.0)
5357/TCP	Abierto	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Nota: Elaboración propia

De acuerdo con la tabla de puertos abiertos mencionada en la tabla anterior se presenta de una manera gráfica la ejecución de la sintaxis de nmap se obtiene lo siguiente:

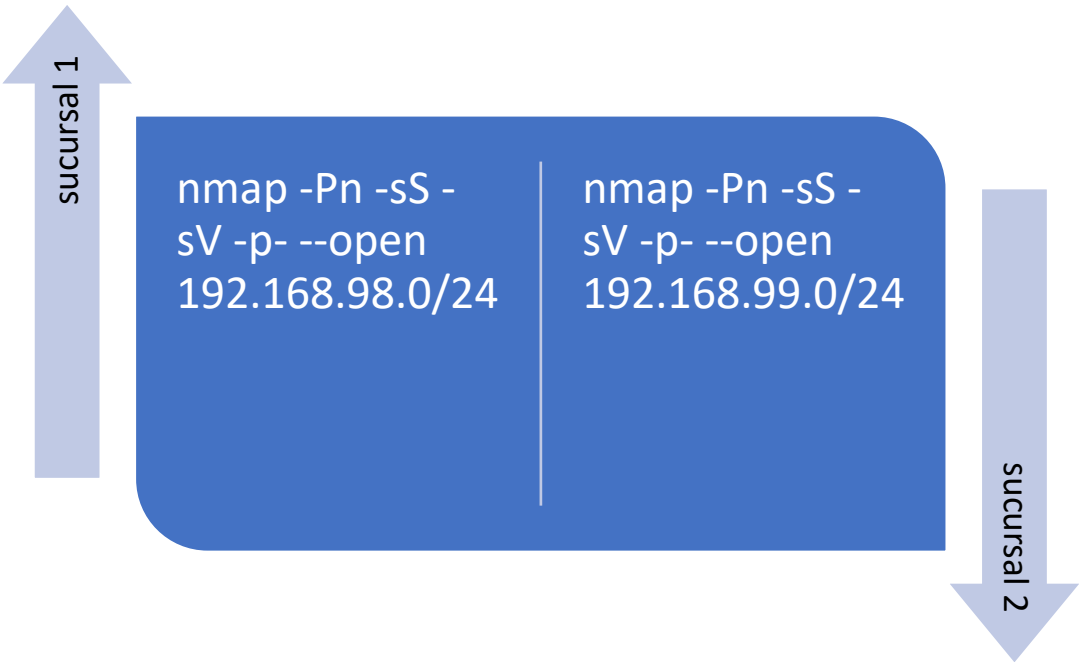


Figura 15. **Comando de escaneo para las dos redes de MASTERNET**

Nota: Elaboración propia

Como resultado del escaneo se posee las siguientes gráficas del proceso de escaneo real, sin embargo, solo se presentan dichas ilustraciones de ciertas ips, tales como:

Detalle técnico del escaneo con nmap según comando: Nmap scan report for 192.168.98.3

```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-09-05 15:02 EST
Nmap scan report for MARKETING
Host is up (0.00s latency).

Not shown: 996 closed ports
PORT     STATE SERVICE VERSION
135/tcp  open  epmap    Sun RPC map (RPCMAP)
139/tcp  open  netbios-ssn Microsoft SMB 3.1.1-SMB2
445/tcp  open  smb     Microsoft SMB 3.1.1-SMB2
1024/tcp open  ms-sql-s Microsoft SQL Server 2016
3389/tcp open  ms-rdp  Microsoft Terminal Services
3476/tcp open  unknown

OS detection performed. Please try enabling OS detection for
getting more accurate results.

Host script results:
|_smb-os: Windows 2016 (build 14393)
| smb-server-name: MARKETING
|_smb-domain: WORKGROUP

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

Figura 16. **Escaneo con NMAP Puertos y servicios abiertos**

Nota: Elaboración propia

Detalle técnico del escaneo con nmap según comando:

Nmap scan report for 192.168.98.4

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-01 16:36 -05
Nmap scan report for 192.168.98.4
Host is up (0.00016s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0            1675 Jan 08  2021 id_rsa
|_-rw-r--r--    1 0        0             159 Jan 10  2021 notas.txt
```

Figura 17. **Escaneo con NMAP FTP abierto**

Nota: Elaboración propia

Detalle técnico del escaneo con nmap según comando:

Nmap scan report for 192.168.98.11

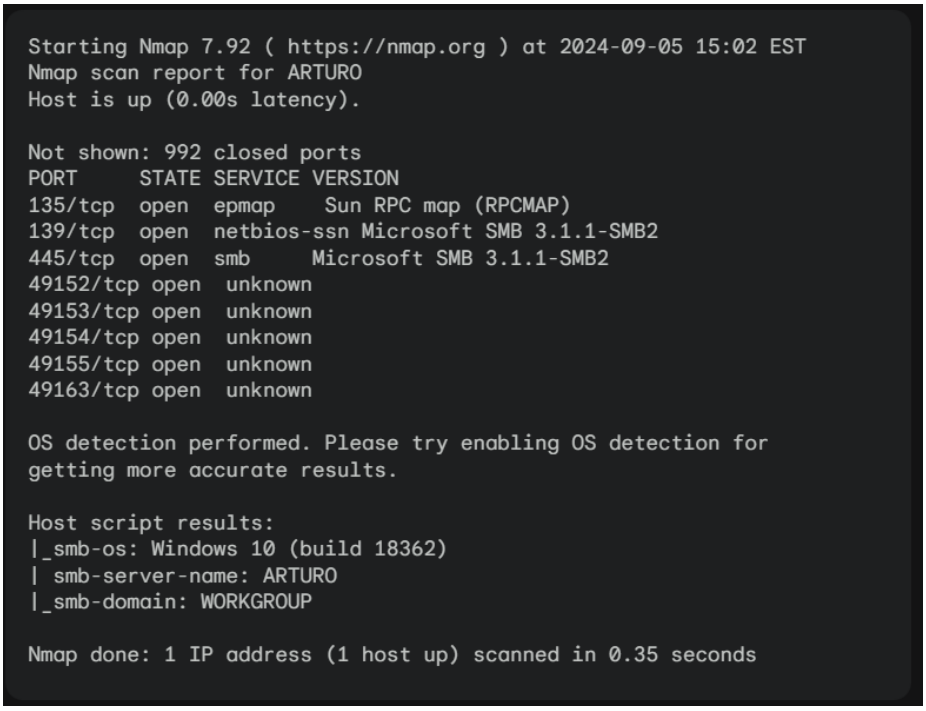


Figura 18. **Escaneo con NMAP Puertos abiertos**

Fuente: elaboración propia

Detalle técnico del escaneo con nmap según comando:

Nmap scan report for 192.168.98.7

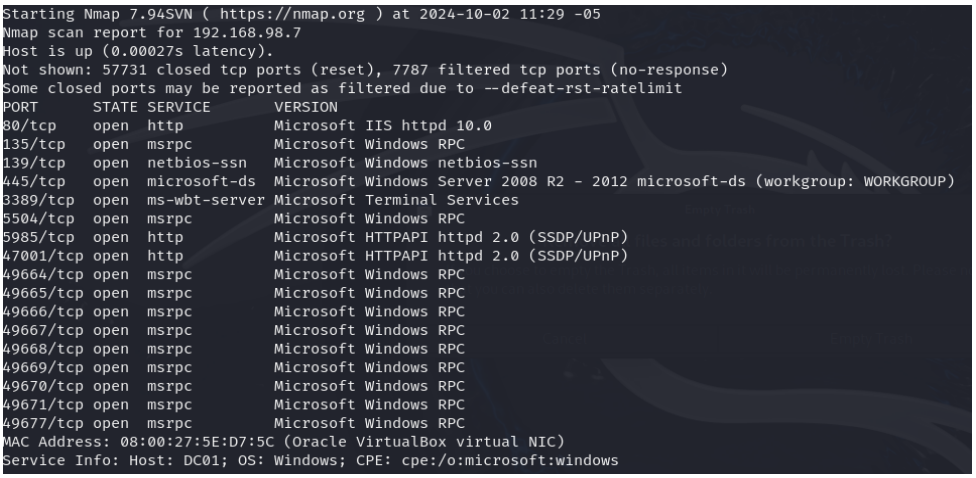


Figura 19. **Escaneo con NMAP Puertos abiertos**

Nota: Elaboración propia

Detalle técnico del escaneo con nmap según comando:

Nmap scan report for 192.168.99.10

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
MAC Address: 08:00:27:CD:49:F4 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
```

Figura 20. **Escaneo con NMAP Servicio SSH descubierto**

Nota: Elaboración propia

Una vez efectuado el proceso de escaneo se procede a detallar en la siguiente tabla 9 aquellos puertos que se encuentran abiertos, su posterior descripción, impacto y la posible solución que se puede implementar ante estas falencias.

Tabla 9.
Puertos que se encuentran abiertos

PUERTO	DESCRIPCIÓN	IMPACTO	SOLUCIÓN
21	Puerto 21 abierto login Anonymous por defecto.	Crítica	Deshabilitar servicio, deshabilitar usuario anónimo.
22	Puerto 22 abierto es posiblemente susceptible a ataques de fuerza bruta.	Medio	Autenticación con clave SSH, cambio de puerto por defecto, Fail2Ban bloquea direcciones IP después de múltiples intentos fallidos
445	Ejecución remota de código vía puerto 445 (MS17-010)	Crítica	Aplicar parches de seguridad (MS17-010), upgrade de Sistema Operativo, deshabilitar SMBv1 en toda la red.
3389	Fuerza bruta de credenciales para acceder al puerto 3389	Alta	Uso de MFA, limitar acceso a RDP, Para limitar el acceso ciertos usuarios o grupos, asignar permisos de acceso a Usuarios o Grupos.

ESCALADA DE PRIVILEGIOS	Explotación de permisos para obtener control total.	Alta	Restringir permisos, aplicar actualizaciones, revisar las configuraciones de los servicios.
49152,49154,49163,	Varios	Bajo	Configurar cortafuegos para restringir exposición y monitorear el tráfico, deshabilitar los servicios de no ser usados.

Nota: Elaboración propia

4.5 Explotación de vulnerabilidades

Para la validación de la metodología propuesta se simularon algunos ataques, utilización procedimientos *pentesting*, en los cuales se recrearon el acceso a la arquitectura bajo estudio, en el laboratorio construido. En las fases anteriores, se aplicó la instalación y actualización de Nmap, por lo tanto, se procedió a determinar los tipos de ataque a simular, de tal forma que nos proporcionan información de interés.

Ataques de fuerza bruta, exploits, siendo estos los que se efectúan con mayor frecuencia. A continuación, se describe como se logró simular cada uno de estos eventos, mostrando las evidencias.

4.5.1 Simulación de Ataque I- FTP y escalación de privilegios.

En el escaneo previo de detecto que hay un servicio FTP funcionando como se evidencia en la siguiente imagen:

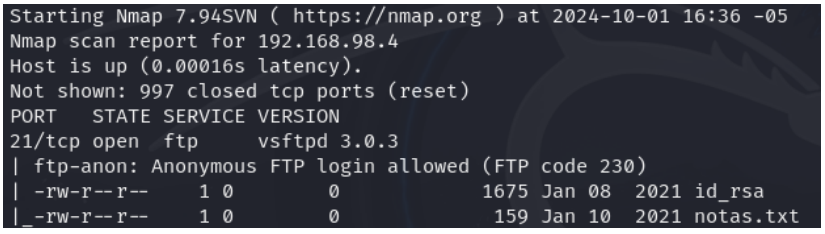


***Figura 21*. Escaneo con NMAP FTP abierto (usuario Anonymous habilitado)**

Nota: Elaboración propia

En este sentido se debe de conectar al equipo vía ftp con el usuario Anonymous y password Anonymous y se puede evidenciar que existen 2 archivos y procedemos a descargarlos para ver su contenido.

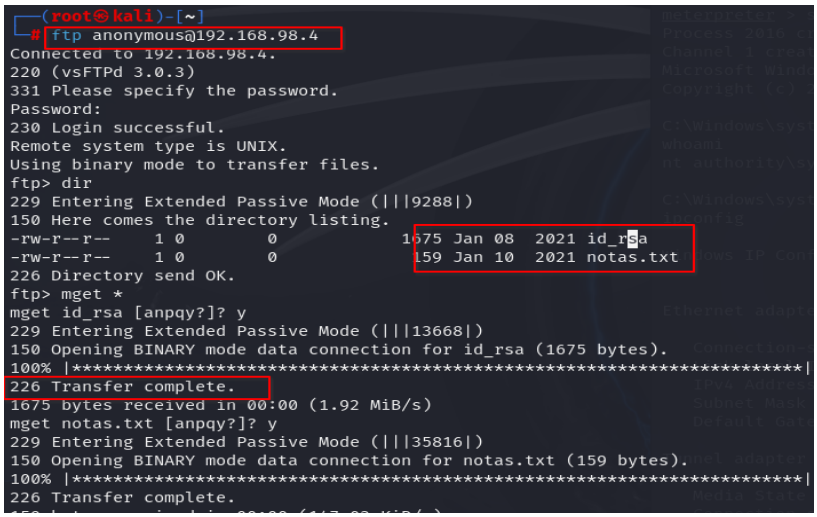


Figura 22. **Loggin al servidor FTP**

Nota: Elaboración propia

Al leer el archivo de nombre notas.txt da indicaciones de usar la clave privada “id_rsa” para conectarse al servidor con el usuario “viu”.

Figura 23. **Nota encontrada en el servidor FTP**

Nota: Elaboración propia

Posteriormente se procede a establecer conexión con el servidor usando la clave privada.

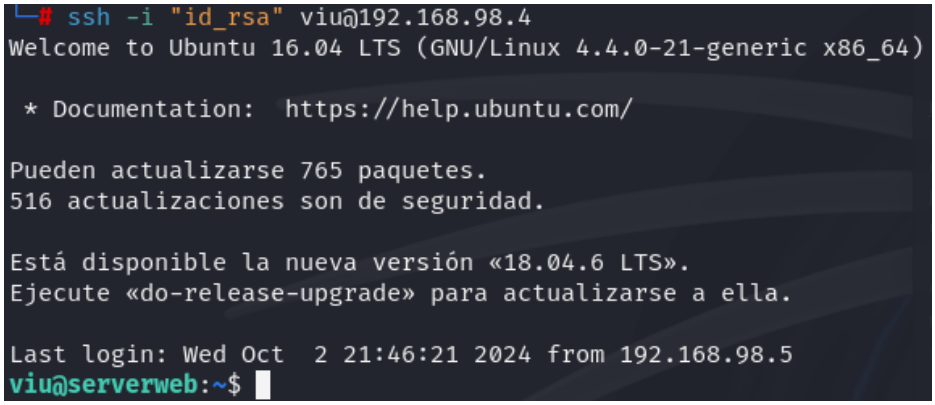


Figura 24. **Login con clave privada servidor FTP**

Nota: Elaboración propia

Se puede observar que ya ha permitido autenticarse al servidor con el usuario **viu**, posteriormente se verifica los privilegios del usuario y confirmamos que es un usuario normal del sistema.

Figura 25. ***Verificación de usuario del sistema***

Nota: Elaboración propia

Ahora bien, se procede a revisar si es que hay comandos que se ejecutan con el comando sudo y sin password para ello se debe de ejecutar la siguiente sintaxis:

sudo -l

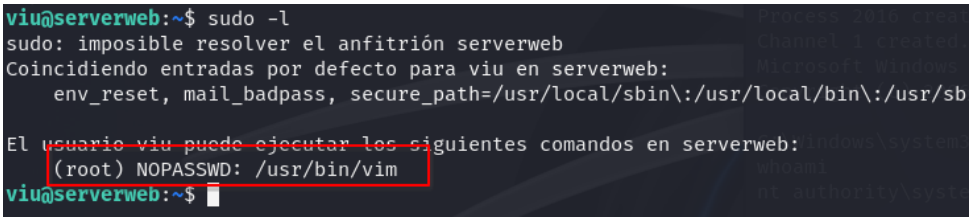


Figura 26. ***Lista de comandos que usuario puede ejecutar.***

Nota: Elaboración propia

Con se puede evidenciar el comando vim puede ejecutarse con privilegios de root sin password.

En vista de tal debilidad se aprovecha de eestá mala práctica para realizar una escala de privilegios y obtener una Shell de root, se ejecuta:

sudo vim -c ':!/bin/bash'

Y como se muestra en la imagen anterior ya somos root, se ha conseguido el máximo privilegio en el equipo.

Figura 27. ***Se ejecuta el comando VIM con sudo agregando una salida bash***

Nota: Elaboración propia

Análisis técnico:

El puerto FTP (21) es un puerto inseguro poco usado, pero aun existente en la actualidad y muy usado dentro de ambientes internos, este servicio permite subir y descargar información de forma remota.

Prevención y Mitigación:

- Cambiar el uso de FTP por SFTP que usa que cifra las transferencias de información.
- Deshabilitar el usuario anonymous que viene por defecto.
- Utilizar contraseñas fuertes: generar contraseñas seguras y únicas para cada cuenta.
- Habilitar la autenticación de dos factores: agregar una capa adicional de seguridad.
- Implementar un firewall: Bloquear el acceso al puerto 21 desde la red interna o Internet y solo permitir conexiones desde IPs o rangos de red conocidas.

4.5.2 Simulación de Ataque II- Fuerza Bruta RDP

A través del escaneo previo, se encuentra un número de pcs vulnerables a ciertos ataques informáticos. Haciendo uso del sistema operativo Kali se demostrará (solo para uso ético y estudiantil) lo enunciado anteriormente**.**

Para este ataque de fuerza bruta se usó la herramienta HYDRA, se usó el usuario administrator por defecto en todos los sistemas operativos Windows y un archivo con una lista password conocidos que la herramienta Kali Linux ya nos la proporciona y o podemos descargarlo desde fuentes abiertos como SECLIST, como se puede observar en la siguiente imagen el ataque fue exitoso.

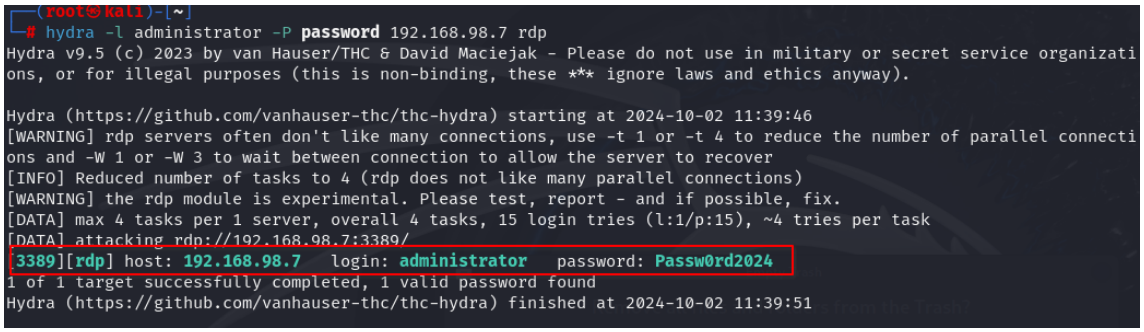


Figura 28. **Ataque con fuerza bruta RDP**

Nota: Elaboración propia

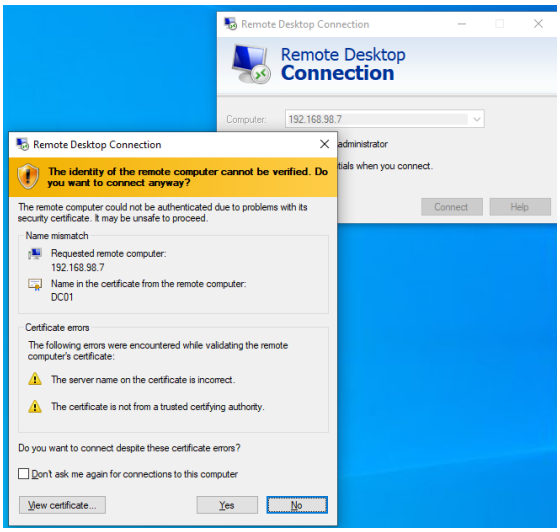


***Figura 29*. Login usando Remote Desktop de Windows**

Nota: Elaboración propia

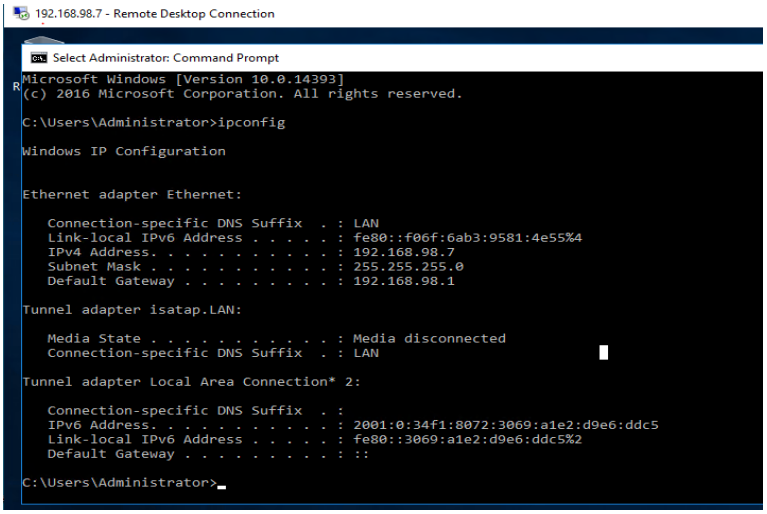


***Figura 30*. Login exitoso ejecución de mando ip config**.

Nota: Elaboración propia

Análisis técnico:

El puerto 3389 es el puerto predeterminado utilizado por el Protocolo de Escritorio Remoto (RDP) de Microsoft. Este protocolo permite a los usuarios conectarse a un ordenador de forma remota y controlarlo como si estuvieran sentados frente a él. Los atacantes a menudo explotan este servicio mal configurado y algunas vulnerabilidades que puedan asociarse en este servicio para obtener acceso no autorizado a sistemas.

Prevención y Mitigación:

- Mantener el sistema actualizado: Instalar los parches de seguridad más recientes.

- Cambiar el puerto por defecto: Configurar el puerto RDP a un número no estándar.
- Deshabilitar el usuario administrator que viene por defecto.
- Utilizar contraseñas fuertes: generar contraseñas seguras y únicas para cada cuenta.
- Habilitar la autenticación de dos factores: agregar una capa adicional de seguridad.
- Implementar un firewall: Bloquear el acceso al puerto 3389 desde Internet.
- Utilizar una VPN: Si es necesario el acceso remoto, utilizar una VPN para cifrar la conexión.

4.5.3 Explotación del Puerto 445 (SMB Exploit)

El puerto 445 es usado por el protocolo SMB en Windows para compartir archivos, impresoras y otros recursos en red. Una vulnerabilidad muy conocida es **EternalBlue**, que afecta a este puerto y permite ejecutar código remoto en máquinas Windows no parcheadas.

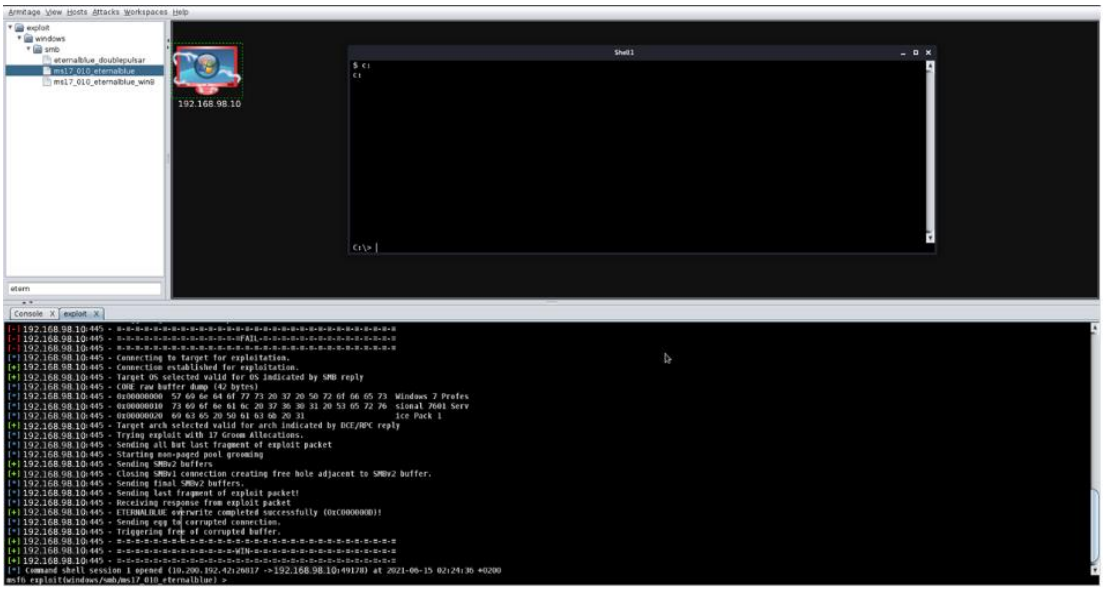


Figura 31. **Ataque con exploit (MS17-010) EternalBlue con Armitage**

Nota: Elaboración propia

4.5.3.1 Pasos para explotar el puerto 445 usando EternalBlue

1. **Escaneo del puerto**: Utiliza herramientas como **Nmap** para verificar si el puerto 445 está abierto.

nmap -p 445 192.168.98.10

Figura 32. **Escaneo nmap al puerto 445**

Nota: Elaboración propia

2. **Identificación de la vulnerabilidad**: Si el puerto está abierto, busca si el sistema está vulnerable a EternalBlue.

```
nmap --script smb-vuln-ms17-010 192.168.98.10
```

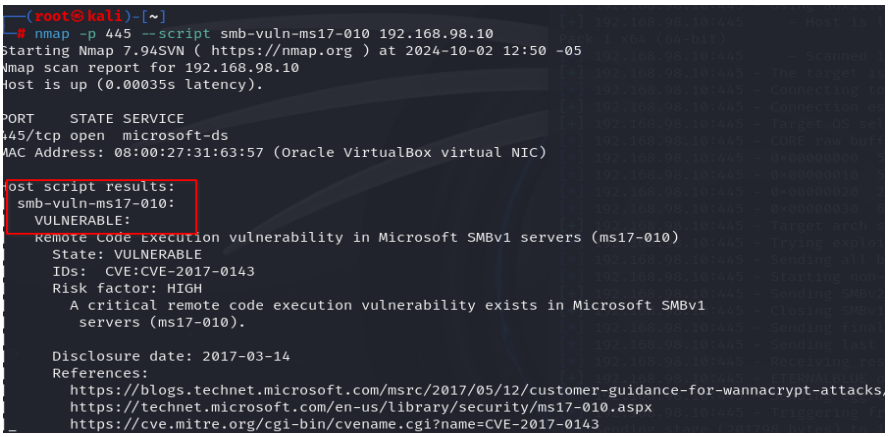


Figura 33. **Escaneo nmap al puerto con script para verificar si es vulnerable a ms17-010**

Nota: Elaboración propia

3. **Explotación**: Usar **Metasploit** para lanzar el exploit.

```
use exploit/windows/smb/ms17_010_eternalblue
set RHOST 192.168.98.10
exploit
```

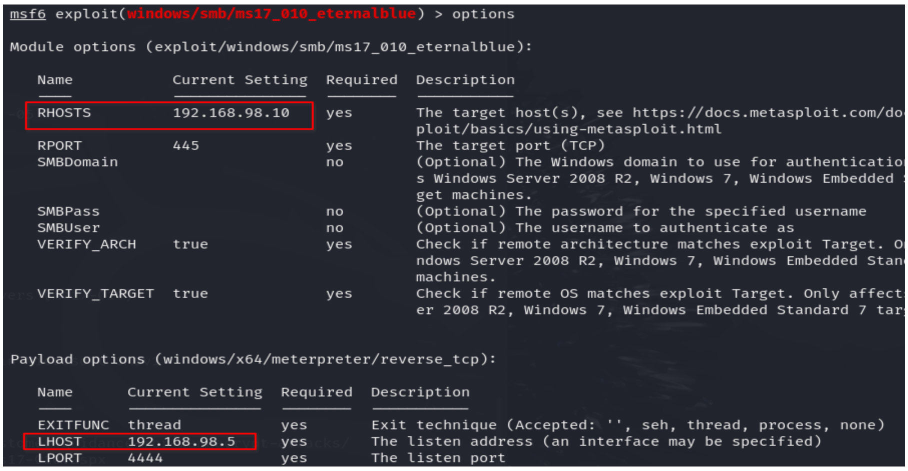


Figura 34. **Configurando metasploit para lanzar el ataque**

Nota: Elaboración propia

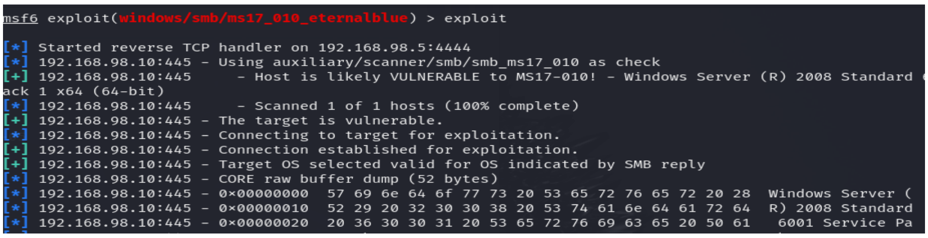


Figura 35**. Ejecución de ataque Eternalblue (MS17-010)**

Nota: Elaboración propia

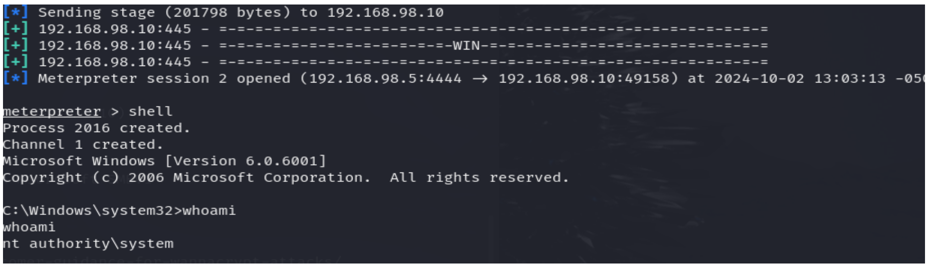


Figura 36. **Exploit ejecutado correctamente con sesión meterpreter**

Nota: Elaboración propia

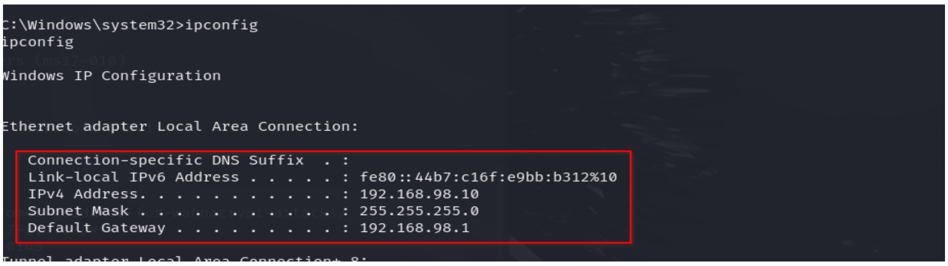


Figura 37**. Ejecución de comando ip config en servidor vulnerado.**

Nota: Elaboración propia

4. **Obtener acceso**: Se ejecuta el exploit correctamente y si tiene un Shell meterpreter y luego podemos cambiar a Shell de Windows y probar algunos comandos.

Análisis técnico:

1. **Deshabilitar SMBv1:** La forma más efectiva de protegerse contra EternalBlue es deshabilitar completamente SMBv1. Este protocolo antiguo es vulnerable y ya no es importante para la mayoría de las redes modernas.
2. **Mantener los sistemas actualizados:** es importante que todos los sistemas Windows estén actualizados con los últimos parches de seguridad. Puesto que, Microsoft ha lanzado parches para corregir esta vulnerabilidad y usar las ultimas de Windows server y Windows.
3. **Usar firewalls:** configura firewalls para bloquear el tráfico SMBv1 entrante y saliente.
4. **Segmentar la red:** dividir la red en diferentes segmentos para limitar el impacto de una posible infección.
5. **Implementar soluciones de seguridad:** usar soluciones de seguridad como antivirus, antimalware y sistemas de detección de intrusiones para detectar y bloquear ataques.

4.5.4 Simulación de Ataque II- Fuerza Bruta SSH

A través del escaneo la ip **192.168.99.10** se detectó que el puerto SSH se encuentra abierto, lo que hay una posibilidad de que sea susceptible a ataques de fuerza bruta si el servicio está mal configurado.

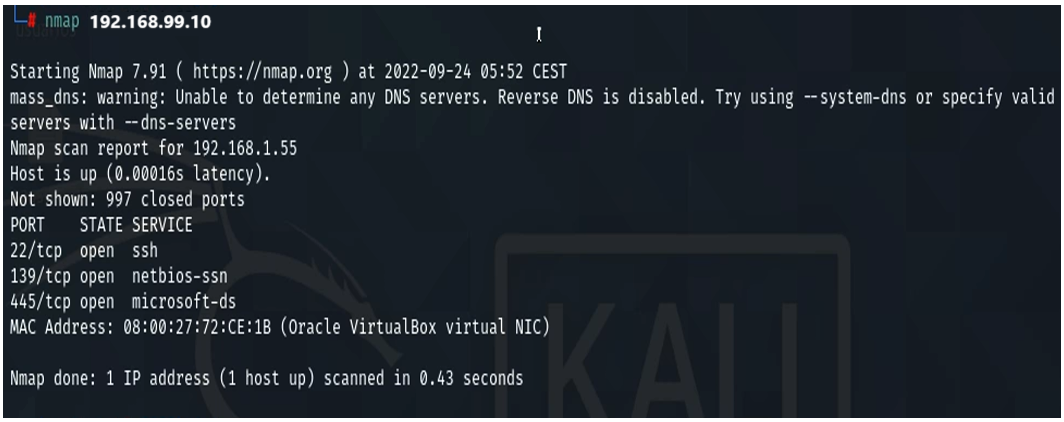


Figura 38. **Escaneo de puerto con NMAP puerto 22 abierto**

Nota: Elaboración propia

Se configura metasploit indicando la IP de la víctima y agregando una lista de usuario y otra de passwords para que la herramienta realice el ataque de fuerza bruta.

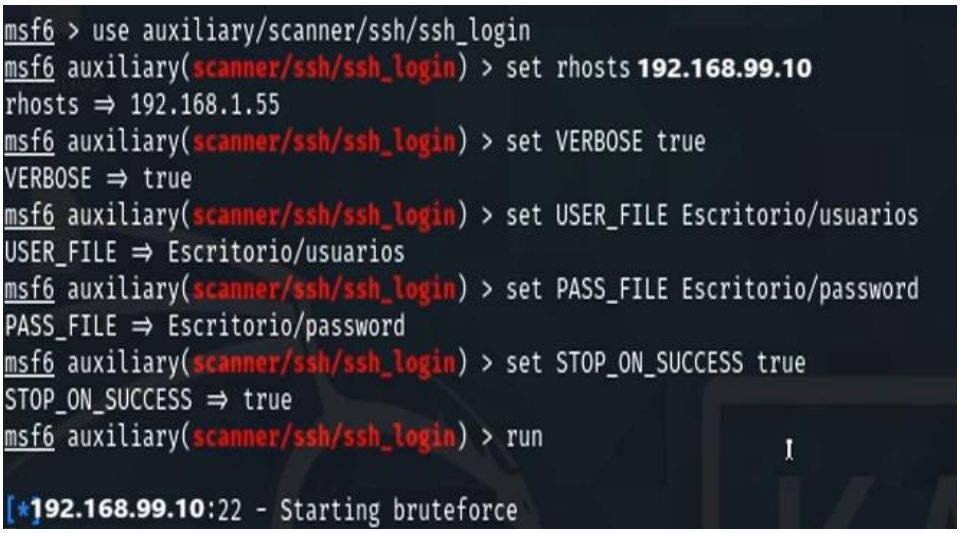


Figura 39. **Usando metasploit configuramos para realizar el ataque.**

Nota: Elaboración propia

Como se visualiza el ataque fue exitoso y se puedo acceder al equipo con el ataque de fuerza bruta vía SSH.

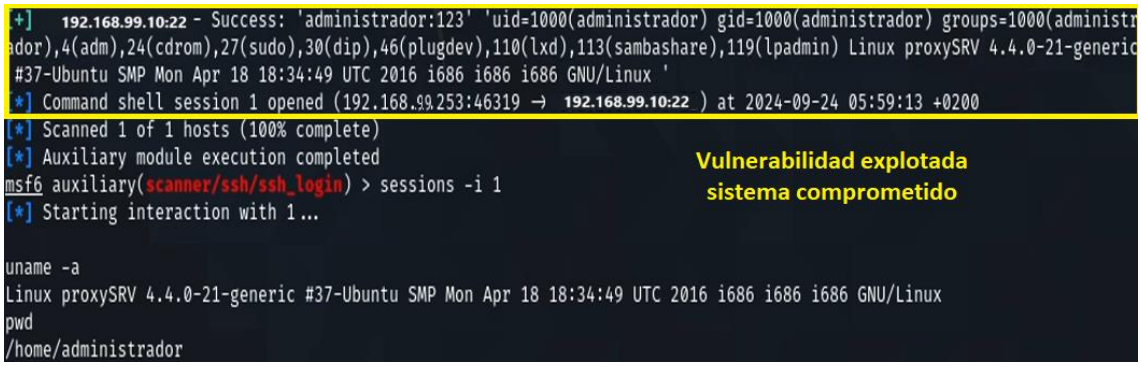


Figura 40. Ataque exitoso de pudo encontrar un usuario valido y password para el servidor.

Nota: Elaboración propia

El puerto 22 es el puerto predeterminado usado por el Protocolo SSH de Linux. Este protocolo permite a los usuarios conectarse a un ordenador de forma remota por medio de una Shell, Los atacantes a menudo explotan vulnerabilidades en este servicio para obtener acceso no autorizado a sistemas.

Prevención y Mitigación:

- Mantener el sistema actualizado: Instalar los parches de seguridad más recientes.
- Cambiar el puerto por defecto: Configurar el puerto SSH a un número no estándar.
- Utilizar contraseñas fuertes: generar contraseñas seguras y únicas para cada cuenta.
- Habilitar la autenticación de dos factores: crear una capa adicional de seguridad.
- Implementar un firewall: Bloquear el acceso al puerto 22 desde Internet.
- Deshabilitar el usuario root por defecto.
- Crear una política de bloqueo por intentos fallidos.
- Implementar fail2ban en el servidor para bloquear las IPs desde donde puedan provenir los ataques.

4.6 Evaluación de vulnerabilidades y análisis de riesgos

En este apartado se procede a evaluar cada vulnerabilidad encontrada, desde las configuraciones inseguras hasta los posibles riesgos más mínimos que se deben de subsanar, posteriormente, examinar el nivel de riesgo proporcionando una visión detallada de las amenazadas potenciales, evaluando su impacto y proponiendo medidas correctivas para fortalecer la seguridad y salvaguardar la integridad de toda la información que maneja MASTERNET.

Leyenda de la clasificación de las vulnerabilidades encontradas:

Tabla 10.

Leyenda de Clasificación de Vulnerabilidades de Acuerdo a Nivel de Gravedad.

DESCRIPCIÓN	CALIFICACIÓN	COLOR
VULNERABILIDAD DÉBIL O MUY COMPLEJA DE APROVECHAR CAUSA UN IMPACTO MÍNIMO.	Baja	
VULNERABILIDAD MODERADA QUE COMPROMETE MODERADAMENTE UNO O MÁS PRINCIPIOS DE SEGURIDAD. CAUSA UN IMPACTO MENOR.	Media	

VULNERABILIDADES MÁS PELIGROSAS. AFECTA A UN NIVEL ALTO LOS PRINCIPIOS CIA. CAUSA UN IMPACTO MODERNO.	Alta	
FALLO DE SEGURIDAD CRÍTICO. COMPROMETE GRAVEMENTE LOS PRINCIPIOS CIA. CAUSA UN GRAVE IMPACTO.	Crítica	

Nota: Tomado de (Gaviria et al., 2015)

A continuación, se procede a detallar cada una de las vulnerabilidades encontradas, de los cuales son:

Sistema Operativo:

Linux Kernel 4.4 on Ubuntu 16.04 (xenial)

IP 192.168.98.4

Tabla 11.

Análisis de vulnerabilidades FTP

VULNERABILIDAD	**CREDENCIALES POR DEFECTO**	**RIESGO**	**CRITICA**
		FACTIBILIDAD DE REMEDIACION	Media
ACTIVOS AFECTADOS	192.168.98.4	**CVSS**	9.0
PRE-REQUISITOS DE EXPLOTACION	El atacante puede estar dentro o fuera de la organización		
DESCRIPCION	El equipo se encuentra corriendo un servicio FTP con usuario Anonymous por defecto		
IMPACTO	Afecta a la integridad y disponibilidad de la data		
RECOMENDACIÓN	Actualizar a una versión SFTP, eliminar el servicio, crear usuarios personalizados y desactivar el usuario anonymous por defecto.		
REFERENCIA	https://nvd.nist.gov/vuln/detail/CVE-1999-0497		

Nota: Elaboración propia

Sistema Operativo: Microsoft Windows Server 2008 Standard Service Pack 1

IP 192.168.98.10

Tabla 12.

Análisis vulnerabilidad Eternalblue

VULNERABILIDAD	**MS17-010 (ETERNALBLUE)**	**RIESGO**	**CRITICA**
		FACTIBILIDAD DE REMEDIACION	Media
ACTIVOS AFECTADOS	192.168.98.10	**CVSS**	8.8
PRE-REQUISITOS DE EXPLOTACION	El atacante puede estar dentro o fuera de la organización		
DESCRIPCION	- Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido a un manejo incorrecto de ciertas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) - Existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido a un manejo incorrecto de ciertas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente diseñado, para revelar información confidencial. (CVE-2017-0147)		
IMPACTO	Afecta a la integridad y disponibilidad de la data		

RECOMENDACIÓN	Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016. Microsoft también ha lanzado parches de emergencia para los sistemas operativos Windows que ya no son compatibles, incluidos Windows XP, 2003 y 8. En el caso de los sistemas operativos Windows no compatibles, por ejemplo, Windows XP, Microsoft recomienda que los usuarios dejen de usar SMBv1. SMBv1 carece de las características de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1 se puede deshabilitar siguiendo las instrucciones del proveedor proporcionadas en Microsoft KB2696547. Además, US-CERT recomienda que los usuarios bloqueen SMB directamente bloqueando el puerto TCP 445 en todos los dispositivos de límite de red. Para SMB a través de la API de NetBIOS, bloquee los puertos TCP 137 / 139 y los puertos UDP 137 / 138 en todos los dispositivos de límite de red.
REFERENCIA	http://www.nessus.org/u?68fc8eff http://www.nessus.org/u?321523eb http://www.nessus.org/u?065561d0 http://www.nessus.org/u?d9f569cf https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/ http://www.nessus.org/u?b9d9ebf9 http://www.nessus.org/u?8dcab5e4 http://www.nessus.org/u?234f8ef8 http://www.nessus.org/u?4c7e0cf3 https://github.com/stamparm/EternalRocks/ http://www.nessus.org/u?59db5b5b

Nota: Elaboración propia

Tabla 13.

Análisis de vulnerabilidades Microsoft WDAC OLE

VULNERABILIDAD	**MICROSOFT WDAC OLE DB PROVIDER FOR SQL SERVER REMOTE CODE EXECUTION VULNERABILITY**	**RIESGO**	**CRITICA**
		FACTIBILIDAD DE REMEDIACION	Alta
ACTIVOS AFECTADOS	192.168.98.7	**CVSS**	8.8
PRE-REQUISITOS DE EXPLOTACION	El atacante puede estar dentro o fuera de la organización		
DESCRIPCION	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability		
IMPACTO	Afecta a la integridad y disponibilidad de la data		
RECOMENDACIÓN	Actualizar con la versión acumulativa de noviembre del 2023		
REFERENCIA	• https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-29372		

Nota: Elaboración propia

Sistema Operativo: Microsoft Windows 10 pro 64 bits. Compilación 19041

IP 192.168.98.11

Tabla 14.

Vulnerabilidad de Microsoft Windows Spooler remote

VULNERABILIDAD	**WINDOWS PRINT SPOOLER REMOTE CODE EXECUTION VULNERABILITY**	**RIESGO**	**CRITICA**
		FACTIBILIDAD DE REMEDIACION	alta
ACTIVOS AFECTADOS	192.168.98.11	**CVSS**	8.8

PRE-REQUISITOS DE EXPLOTACION	El atacante puede estar dentro o fuera de la organización
DESCRIPCION	Existe una vulnerabilidad de ejecución remota de código cuando el servicio Windows Print Spooler realiza incorrectamente operaciones de archivos con privilegios. Un atacante que aprovechara con éxito esta vulnerabilidad podría ejecutar código arbitrario con privilegios SYSTEM. Un atacante podría entonces instalar programas; ver, cambiar o eliminar datos; o crear nuevas cuentas con todos los derechos de usuario.
IMPACTO	Afecta a la integridad y disponibilidad de la información
RECOMENDACIÓN	Actualizar con cualquier parche de seguridad posterior a noviembre del 2021
REFERENCIA	• http://packetstormsecurity.com/files/167261/Print-Spooler-Remote-DLL-Injection.html • https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527

Nota: Elaboración propia

Tabla 15.

Análisis de vulnerabilidades Tencent Wechat Wxam

VULNERABILIDAD	**TENCENT WECHAT WXAM DECODER OUT-OF-BOUNDS READ INFORMATION DISCLOSURE VULNERABILITY**	**RIESGO**	**MEDIA**
		FACTIBILIDAD DE REMEDIACION	Baja
ACTIVOS AFECTADOS	192.168.98.11	**CVSS**	6.5
PRE-REQUISITOS DE EXPLOTACION	El atacante puede estar dentro o fuera de la organización		

DESCRIPCION	Esta vulnerabilidad permite a los atacantes remotos revelar información confidencial sobre las instalaciones afectadas de la versión de escritorio de Tencent WeChat 2.9.5. La interacción del usuario es necesaria para explotar esta vulnerabilidad, ya que el objetivo debe visitar una página maliciosa o abrir un archivo malintencionado. La falla específica existe dentro del decodificador WXAM. El problema se debe a la falta de validación adecuada de los datos proporcionados por el usuario, lo que puede dar lugar a una lectura más allá del final de un búfer asignado. Un atacante puede aprovechar esto junto con otras vulnerabilidades para ejecutar código arbitrario en el contexto del proceso actual. Era ZDI-CAN-11907
IMPACTO	Afecta a la integridad y disponibilidad de la información
RECOMENDACIÓN	Actualizar con cualquier parche de seguridad posterior a noviembre del 2021
REFERENCIA	• https://www.zerodayinitiative.com/advisories/ZDI-21-217/ • https://learn.microsoft.com/es-es/search/?terms=CVE-2021-27247

Nota: Elaboración propia

Sistema Operativo: Microsoft Windows 10 Pro 64 bits. Compilación 19045

IP 192.168.98.12

Tabla 16.

Análisis de vulnerabilidades Visual Studio Code

VULNERABILIDAD	**VISUAL STUDIO CODE ESLINT EXTENSION REMOTE CODE EXECUTION VULNERABILITY**	**RIESGO**	**CRITICA**
		FACTIBILIDAD DE REMEDIACION	Baja
ACTIVOS AFECTADOS	192.168.98.12	**CVSS**	8.8

PRE-REQUISITOS DE EXPLOTACION	El atacante puede estar dentro o fuera de la organización
DESCRIPCION	Existe una vulnerabilidad de ejecución remota de código en la extensión ESLint para Visual Studio Code cuando valida el código fuente después de abrir un proyecto, también conocida como 'Vulnerabilidad de ejecución remota de código de extensión ESLint de Visual Studio Code'.
IMPACTO	Afecta a la integridad y disponibilidad de la información
RECOMENDACIÓN	Actualizar con cualquier parche de seguridad posterior a noviembre del 2021
REFERENCIA	• https://msrc.microsoft.com/update-guide/en-us/advisory/CVE-2020-1481

Nota: Elaboración propia

Sistema Operativo: Microsoft Windows 10 pro 64 bits. Compilación 19045

IP 192.168.99.10

Tabla 17.

Análisis de vulnerabilidades Credenciales por defecto

VULNERABILIDAD	**CREDENCIALES POR DEFECTO**	**RIESGO**	**CRITICA**
		FACTIBILIDAD DE REMEDIACION	Baja
ACTIVOS AFECTADOS	192.168.99.10	**CVSS**	7.8
PRE-REQUISITOS DE EXPLOTACION	El atacante puede estar dentro o fuera de la organización		
DESCRIPCION	Esta vulnerabilidad permitía a un atacante remoto ejecutar código arbitrario en un sistema Windows 10 afectado si el usuario abría un documento de Office malicioso.		
IMPACTO	Afecta a la integridad y disponibilidad de la información		
RECOMENDACIÓN	Actualizar con cualquier parche de seguridad posterior a noviembre del 2020		

REFERENCIA	• https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1335

Nota: Elaboración propia

Sistema Operativo: Microsoft Windows 10 Pro 64 bits. Compilación 19045

IP 192.168.99.11

Tabla 18.

Análisis de vulnerabilidades Microsoft Excel remote

VULNERABILIDAD	**MICROSOFT EXCEL REMOTE CODE EXECUTION VULNERABILITY**	**RIESGO**	**CRITICA**
		FACTIBILIDAD DE REMEDIACION	Baja
ACTIVOS AFECTADOS	192.168.99.11	**CVSS**	8.8
PRE-REQUISITOS DE EXPLOTACION	El atacante puede estar dentro o fuera de la organización		
DESCRIPCION	Esta vulnerabilidad permitía a un atacante falsificar su identidad como otro usuario en una red Kerberos.		
IMPACTO	Afecta a la integridad y disponibilidad de la información		
RECOMENDACIÓN	Actualizar con cualquier parche de seguridad posterior a noviembre del 2020		
REFERENCIA	• https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1335		

Nota: Elaboración propia

Sistema Operativo: Microsoft Windows 10 pro 64 bits. Compilación 19045

IP 192.168.99.12

Tabla 19.

Análisis vulnerabilidades remote procedure call reuntime

VULNERABILIDAD	**REMOTE PROCEDURE CALL RUNTIME REMOTE CODE EXECUTION VULNERABILITY**	**RIESGO**	**CRITICA**
		FACTIBILIDAD DE REMEDIACION	Baja
ACTIVOS AFECTADOS	192.168.99.12	**CVSS**	8.8
PRE-REQUISITOS DE EXPLOTACION	El atacante puede estar dentro o fuera de la organización		
DESCRIPCION	Vulnerabilidad de ejecución remota de código en tiempo de ejecución de llamadas a procedimientos remotos. Puerto 445 (SMB) sin la debida protección.		
IMPACTO	Afecta a la integridad y disponibilidad de la información		
RECOMENDACIÓN	Actualizar con cualquier parche de seguridad posterior a junio del 2022		
REFERENCIA	• https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24528		

Nota: Elaboración propia

Sistema Operativo: Microsoft Windows 10 pro 64 bits. Compilación 19044

IP 192.168.99.13

Tabla 20.

Análisis de vulnerabilidades sistema operativo desactualizado

VULNERABILIDAD	**SISTEMA OPERATIVO DESACTUALIZADO**	**RIESGO**	**CRITICA**
		FACTIBILIDAD DE REMEDIACION	Baja
ACTIVOS AFECTADOS	192.168.99.13	**CVSS**	7.8
PRE-REQUISITOS DE EXPLOTACION	El atacante puede estar dentro o fuera de la organización		
DESCRIPCION	Windows 10 Pro for Workstation sigue siendo susceptible a ataques de phishing. Estos ataques de ingeniería social intentan engañar a los usuarios para que revelen información confidencial o hagan clic en enlaces maliciosos que podrían descargar malware.		
IMPACTO	Afecta a la integridad y disponibilidad de la data		
RECOMENDACIÓN	Las version workstation no recibe actualizaciones de seguridad desde diciembre del 2023. Por lo cual recomendamos cambiar la versión de Windows a Windows 10 22h2 pro.		
REFERENCIA	• https://learn.microsoft.com/es-es/windows/release-health/release-information • http://packetstormsecurity.com/files/164210/Microsoft-Windows-MSHTML-Overview.html • http://packetstormsecurity.com/files/165214/Microsoft-Office-Word-MSHTML-Remote-Code-Execution.html • http://packetstormsecurity.com/files/167317/Microsoft-Office-MSDT-Follina-Proof-Of-Concept.html • https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40444		

Nota: Elaboración propia

Sistema Operativo: Microsoft Windows 10 Pro 64 bits. Compilación 19044

IP 192.168.99.14

Tabla 21.

Análisis vulnerabilidades servicio RDP, puerto por defecto 3389

VULNERABILIDAD	**SERVICIO RDP, PUERTO POR DEFECTO 3389**	**RIESGO**	**MEDIA**
		FACTIBILIDAD DE REMEDIACION	Baja
ACTIVOS AFECTADOS	192.168.99.14	**CVSS**	4.4
PRE-REQUISITOS DE EXPLOTACION	El atacante puede estar dentro o fuera de la organización		
DESCRIPCION	Vulnerabilidad de divulgación de información del Protocolo de escritorio remoto (RDP) de Windows		
IMPACTO	Afecta a la integridad y disponibilidad de la información		
RECOMENDACIÓN	Filtrar o cerrar el puerto 3389 (Escritorio Remoto). Actualizar a Windows 10 22h2 pro.		
REFERENCIA	• https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38631		

Nota: Elaboración propia

4.7 Resumen de vulnerabilidades encontradas en las pruebas de penetración

En breve, se presenta un detalle de las alertas más relevantes o de riesgo que se realizó tras la aplicación de la fase de la explotación de vulnerabilidades.

Estas vulnerabilidades deben ser remediadas con prioridad ya que representan un alto riesgo dentro de la red ya que atacante puede explotar los mismo realizando ataques de fuerza bruta, el uso de exploits y CVE conocidos obteniendo control de los activos y poder realizar un mayor ataque comprometiendo aún más los activos en la red interna.

Tabla 22.

Resumen de la Metodología Propuesta

VULNERABILIDAD	DESCRIPCIÓN	MÉTODO DE EXPLOTACIÓN	SOLUCIÓN	ORIGEN	HERRAMIENTA	IMPACTO	CRITICIDAD	RECOMENDACIONES ADICIONALES
ETERNALBLUE (SMB)	Explotación de la vulnerabilidad en el protocolo SMB para ejecutar código remoto mediante el puerto 445 (MS17-010).	Metasploit, exploit SMB, escaneo de puertos.	Aplicar el parche MS17-010, deshabilitar SMBv1, segmentar la red para reducir la exposición.	CVE-2017-0144	Metasploit, Nmap	Compromiso total del sistema, ransomware (WannaCry).	Crítica	Habilitar firewalls, desactivar servicios innecesarios.
FUERZA BRUTA (RDP)	Ataques de fuerza bruta a través del puerto 3389 para obtener acceso a Escritorio Remoto mediante la explotación de credenciales débiles.	Hydra,ataques con diccionario de contraseñas.	Implementar MFA, usar contraseñas robustas, limitar el acceso por red privada o VPN, cerrar puertos no utilizados.	Escaneo de puertos y contraseñas débiles.	Hydra,	Acceso no autorizado, compromiso del sistema.	Alta	Configurar bloqueo por intento fallido, cambiar el puerto por defecto.

ESCALADA DE PRIVILEGIOS	Explotación de permisos mal configurados o vulnerabilidades en el sistema operativo para obtener privilegios de administrador.	Scripts locales, exploits específicos, vulnerabilidades en Windows (CVE-2020-0796).	Restringir permisos, aplicar parches de seguridad, usar herramientas de auditoría de privilegios.	Malas configuraciones y fallos en parches.	Exploits, scripts manuales	Control total del sistema, ejecución arbitraria.	Alta	Implementar medidas de privilegios mínimos, monitorear cuentas de usuarios.
SISTEMA OPERATIVO DESACTUALIZADO	Sistemas sin actualizaciones son vulnerables a exploits conocidos que pueden ser utilizados por atacantes para comprometer la infraestructura.	Explotación de vulnerabilidades conocidas (CVE), kits de exploits.	Mantener el sistema actualizado con parches de seguridad, configurar actualizaciones automáticas.	CVEs conocidos y exploits públicos.	Nessus	Vulnerabilidad crítica a múltiples ataques.	Alta	Automatizar la gestión de parches, realizar pruebas de actualización periódicas.

MICROSOFT EXCEL REMOTE CODE EXECUTION	Ejecución remota de código malicioso al abrir archivos Excel manipulados que contienen macros peligrosas o vulnerabilidades de software.	Scripts maliciosos, explotación de macros, archivos adjuntos.	Deshabilitar macros en Excel por defecto, evitar abrir archivos de remitentes desconocidos, aplicar parches de seguridad de Office.	CVE-2017-11882, archivos adjuntos de phishing.	Scripts maliciosos, malware	Ejecución de código no autorizado, robo de datos.	Media	Implementar políticas de seguridad en correos electrónicos, herramientas de sandboxing para archivos adjuntos.
FUERZA BRUTA (SSH)	Ataques de fuerza bruta a través del puerto 22 para obtener acceso no autorizado mediante la explotación de credenciales débiles.	Hydra,ataques con diccionario de contraseñas.	Implementar MFA, limitar acceso SSH, utilizar fail2ban para bloquear IPs, deshabilitar root login.	Contraseñas débiles, puertos abiertos sin restricciones.	Hydra	Acceso no autorizado a servidores, compromiso del sistema.	Alta	Configurar autenticación basada en claves públicas, cambiar el puerto SSH por defecto.

Nota: Elaboración propia.

4.8 Implementación de las recomendaciones

A modo general cuando se analizan los resultados conseguidos a través de la utilización de la metodología en cuestión (***pentesting***), concluimos que estamos frente a una red completamente vulnerable, mal configurada e ineficiente; los siguientes elementos evidencian dicha afirmación:

- Actualizaciones automáticas de software sin una planificación adecuada.
- Cambios en las regulaciones de seguridad/datos.
- Cambios de red no autorizados.
- Dificultad para monitorizar o actualizar sistemas remotos.
- Red no segmentada.
- Inexistencias de Firewalls o Cortafuegos en los servicios implementados.
- Inexistencias de parches de seguridad (donde sea posible) en las PCs de la empresa.
- Uso de softwares no autorizados.

En función de mitigar en su mayoría las vulnerabilidades encontradas se plantean una serie de soluciones enumeradas y explicadas a continuación:

1. Segmentar la red telemática de la empresa MASTERNET.
    a. Subred de empleados: 192.168.98.0/24
    b. DMZ para aislar los servidores: 10.0.0.0/29
    c. Subred de VPN: 172.16.1.0/32

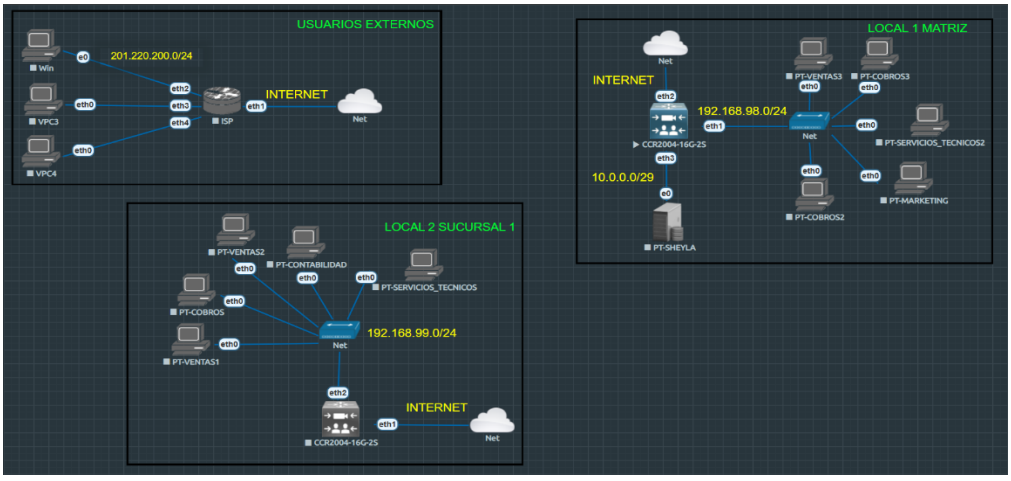


***Figura 41*. Segmentación de la red telemática de la empresa MASTERNET.**

Nota: Elaboración propia

2. Sustituir los enrutadores ***Linksys***[6] por enrutadores ***Mikrotiks***[7].

3. Implementar firewalls de alta disponibilidad en las dependencias de la empresa MASTERNET.
    a. Implementar reglas de tráfico que delimiten los niveles de accesos
    b. Bloquear todo tráfico mal intencionado o de subredes no permitidas
    c. Registrar y almacenar todos los eventos (Logs)

4. Implementar un servicio VPN para que el tráfico entre las sucursales de la empresa MASTERNET sea cifrado.
    a. Se implementó una VPN basadas en el protocolo L2TP/IPSec [8] donde la información que se comparte entre sucursales es encriptada.

5. Implementar un servicio VPN para que determinados usuarios accedan remotamente al sistema de gestión de MASTERNET.
    a. Se implementó una VPN OpenVPN, con certificados de seguridad personalizados y con direcciones IPs estáticas, con este tipo de implementación aseguramos un nivel de seguridad más sólido manejando los accesos de cada usuario y acceso a logs de conexión.

En relación con este aspecto de seguridad, las medidas prácticas de prevención se enfocan en:

[6] Linksys Holdings, Inc. es una marca estadounidense de productos para redes de datos que vende principalmente a usuarios domésticos y a pequeñas empresas, Los productos de Linksys incluyen routers inalámbricos, sistemas Wi-Fi en malla, extensores Wifi, puntos de acceso, y conmutadores de red.

[7] Los routers Mikrotik se utilizan para dirigir el tráfico de datos entre redes y asegurar que los dispositivos en una red se comuniquen eficazmente. Pueden utilizarse tanto en entornos domésticos como comerciales para gestionar la conectividad a Internet y las redes locales.

[8] L2TP, o Protocolo de Tunelización de Capa Dos, es un protocolo de tunelización de computadoras que las VPNs y los Proveedores de Servicios de Internet (ISPs) utilizan. Las VPNs aprovechan su conectividad y los ISPs lo usan para facilitar las operaciones de VPN. Aunque el protocolo fue diseñado para mejorar PPTP y L2F, no es perfecto por sí solo. L2TP se suele combinar con otro protocolo para aprovechar al máximo su potencial. La pareja más común es L2TP/IPSec. IPSec se usa para asegurar que los paquetes de datos estén seguros.

Tabla 23.

Medidas prácticas de prevención

MEDIDAS DE PREVENCIÓN	DESCRIPCIÓN
DESCARGA DE ACTUALIZACIONES	• No descargar actualizaciones desde sitios web que no se conocen. • Realizar la descarga de actualizaciones por medio de los procedimientos brindados por el mismo fabricante o programador de ciertos sistemas o softwares que use la empresa MASTERNET. • Es importante mantener las actualizaciones activas tanto en los sistemas operativos como en las aplicaciones instaladas. • Aplicar configuraciones en el sistema operativo para lograr que sea más seguro; entablar buenas prácticas es importante para un correcto funcionamiento.
CONFIGURACIONES ADICIONALES	• Es importante que se deshabilite las carpetas compartidas que están en la red, esto con e objetivo de que la propagación de gusanos o troyanos aprovechen cualquier vulnerabilidad. • Configurar un perfil como usuario con privilegios limitados. • Desconfigurar la ejecución automática de dispositivos de almacenamiento USB. • Para la autenticación de ingreso de sesión hacia el sistema operativo, debe de ser una contraseña fuerte, una combinación de caracteres alfanuméricos y de símbolos. • Se debe de configurar la visualización de archivos ocultos, porque en múltiples ocasiones pueden poseer virus escondidos en el sistema con este tipo de atributos.

	• Se debe de actualizar contraseñas de una manera periódica no mayor a 7 días para cierta información que es crítica. 30 días para información media y de 90 días para información de categoría baja. • Cualquier comunicación enviada por correo electrónico que contenga información confidencial sobre los clientes, socios comerciales o accionistas de la organización debe cifrarse utilizando las herramientas proporcionadas por el servicio de correo electrónico. Además, los documentos adjuntos deben estar protegidos con una contraseña segura de al menos 10 caracteres. Combinación de letras mayúsculas, minúsculas, números y símbolos. • Durante el ciclo de desarrollo de software seguro, el equipo es responsable de garantizar que las aplicaciones y servicios que requieren combinaciones de inicio de sesión y contraseña incluyan cifrado de credenciales y que las contraseñas no sean claramente visibles en el código. • Los sitios web de la empresa deben estar protegidos por certificados de seguridad emitidos por organismos reconocidos para evitar la interceptación de datos ingresados por clientes o socios comerciales.
TECNOLOGÍA	• Es importante que se trate de usar equipos de última tecnología, dado que los sistemas operativos desactualizados no cuentan con un soporte técnico. • Los discos duros de las computadoras del usuario final deben cifrarse utilizando herramientas o soluciones proporcionadas con el sistema operativo y deben ser adquiridos y administrados por el equipo técnico y verificados por el equipo de seguridad de la información. Asimismo, las unidades corporativas y las unidades flash USB deben estar cifradas.

Nota: Elaboración propia

Los ataques al puerto 22, especialmente cuando se combinan con ataques de diccionario, son una amenaza constante para la seguridad de los sistemas. A continuación, se evidencian algunas medidas preventivas efectivas:

Tabla 24.

Medidas de prevención

MEDIDAS PREVENTIVAS	DESCRIPCIÓN
FORTALECIMIENTO DE LAS CONTRASEÑAS	• **Complejidad:** Exige contraseñas que combinen mayúsculas, minúsculas, números y caracteres especiales. • **Longitud:** Implementa políticas de contraseñas que establezcan una longitud mínima considerable. • **Unicidad:** Evita el uso de contraseñas repetidas en diferentes cuentas. • **Caducidad:** Establece políticas de caducidad obligatoria para las contraseñas. • **Gestores de contraseñas:** Recomienda el uso de gestores de contraseñas para generar y almacenar de forma segura contraseñas complejas.
AUTENTICACIÓN DE DOS FACTORES (2FA)	• **Implementación:** Configura la autenticación de dos factores para agregar una capa adicional de seguridad. • **Métodos:** Utiliza métodos de 2FA como códigos enviados a dispositivos móviles, aplicaciones de autenticación o tokens de seguridad.

LIMITACIÓN DE INTENTOS DE INICIO DE SESIÓN	• **Bloqueo de IP:** Después de un número determinado de intentos fallidos, bloquea temporalmente la dirección IP. • **Períodos de espera:** Implementa períodos de espera entre intentos de inicio de sesión. • **Honeypots:** Utiliza honeypots para atraer a los atacantes y analizar sus técnicas.
CONFIGURACIÓN DEL SERVIDOR SSH	• **Deshabilitar el acceso root:** Evita el acceso directo al usuario root a través de SSH. • **Cambiar el puerto por defecto:** Utiliza un puerto no estándar para dificultar los ataques automatizados. • **Deshabilitar el acceso de clave pública:** Si no es necesario, deshabilita esta opción para reducir la superficie de ataque. • **Limitación de conexiones:** Configura límites en el número de conexiones simultáneas permitidas. • **Bloqueo de direcciones IP conocidas:** Bloquea las direcciones IP de las que se originan con frecuencia ataques.
MONITOREO Y DETECCIÓN	• **Sistemas de detección de intrusiones (IDS):** Implementa un IDS para detectar actividades sospechosas. • **Análisis de logs:** Revisa regularmente los logs de SSH para identificar patrones de ataque. • **Alertas:** Configura alertas para eventos como intentos de fuerza bruta o inicios de sesión fallidos.

Nota: Elaboración propia

4.9 Metodología propuesta

Como se mencionó anteriormente, para este proyecto de investigación se usó la Metodología de PENTESTING como marco referencial, la cual se adaptó a las necesidades de la red informática de MASTERNET., además se identificaron y se aplicaron las técnicas y herramientas entre las más reconocidas como eficientes en el entono de las evaluaciones de seguridad de información.

En la tabla 2, se puede apreciar cada una las fases de la metodología resultante de la investigación, por cada etapa se identifica el alcance, las técnicas y herramientas que se pueden aplicar, todas previamente probadas a lo largo de la investigación, ajustadas a los requerimientos previamente establecidos.

He generado una ilustración que muestra los tres escenarios de hacking:

1. **Explotación del puerto 445** utilizando el exploit EternalBlue.
2. **Explotación de puerto 21** (FTP). escalada de privilegios.
3. **Ataque de fuerza bruta en el puerto 3389** (RDP).
4. **Ataque de fuerza bruta en el puerto 22** (SSH).

Aquí tienes la imagen, que describe los pasos involucrados en cada ataque. Ahora generaré el resumen en tabla de control de vulnerabilidades.

Tabla 25.

Control de Vulnerabilidades

VULNERABILIDAD	DESCRIPCIÓN	IMPACTO	MÉTODO DE EXPLOTACIÓN	SOLUCIÓN
ETERNALBLUE (SMB)	Ejecución remota de código vía puerto 445 (MS17-010)	Crítica	Metasploit, SMB exploit	Aplicar parche MS17-010

EXPLOTACIÓN DE PUERTO 21	Explotación de puerto 21 abierto y mala configuración	Crítica	Scripts locales o vulnerabilidades	Actualizaciones y restricciones de permisos
FUERZA BRUTA (RDP)	Ataques de fuerza bruta a las credenciales del puerto 3389	Alta	Herramientas de fuerza bruta (Hydra)	Habilitar MFA, limitar acceso RDP
FUERZA BRUTA (SSH)	Ataques de fuerza bruta al puerto SSH		Metasploit	Hardening de servidores, configuración de servicio SSH solo para usuarios autorizados.

Nota: Elaboración propia

4.10 Discusión

La evaluación realizada sobre el sistema de información de MASTERNET mediante técnicas de pentesting permitió identificar varias vulnerabilidades críticas que amenazan la seguridad de la infraestructura tecnológica de la empresa. Este análisis, centrado en detectar debilidades que comprometen la confidencialidad, integridad y disponibilidad de los activos digitales, destacó la necesidad urgente de implementar medidas de mitigación para fortalecer las defensas de la empresa contra ciberataques.

Uno de los aspectos relevantes fue la falta de una política formal de seguridad en la empresa, lo cual expone su infraestructura a ataques como el ransomware y la explotación de puertos no seguros.

La implementación de la metodología Pentesting Execution Standard (PTES) resultó crucial para establecer un enfoque sistemático en la detección de vulnerabilidades, que incluyó desde la recopilación de datos hasta el aprovechamiento de las debilidades. Dentro de las etapas más cruciales se encontraban el escaneo y la explotación de vulnerabilidades, en las que se demostró la vulnerabilidad de diversos servicios, como FTP y RDP, frente a ataques de fuerza bruta y exploits denominados EternalBlue. Estos descubrimientos resaltan la relevancia de mantener los sistemas al día y fortalecer las acciones de autenticación, particularmente en los servicios presentados. Otro punto es la evaluación de riesgos residuales. A pesar de las medidas de mitigación que se pueden implementar, pueden persistir y deben gestionarse adecuadamente para evitar futuros incidentes, así como la capacitación de personal sobre las mejores prácticas de seguridad.

Finalmente, las recomendaciones propuestas, como la implementación de la autenticación multifactor (2FA), la limitación de intentos de inicio de sesión y la configuración segura de servicios como SSH, son pasos críticos hacia la mejora de la postura de seguridad de MASTERNET. Sin embargo, es necesario que la empresa adopte un enfoque integral y continuo de la seguridad para adaptarse a las nuevas amenazas que surgen constantemente en el panorama digital.

Este análisis destaca la necesidad de un enfoque preventivo y proactivo en la seguridad de la información.

5 CONCLUSIONES

Una vez finalizado el proceso de ejecución de la propuesta investigativa, se procede a concluir lo siguiente:

La seguridad de la red es fundamental para proteger la información confidencial y los activos de toda empresa. Una red vulnerable aumenta significativamente el riesgo de sufrir un ciberataque o una violación de datos. Puesto que, una red mal configurada puede provocar problemas de rendimiento, interrupciones en el servicio y dificultades para los empleados al acceder a los recursos necesarios para realizar su trabajo. Una red ineficiente puede impactar negativamente en la productividad de los empleados, generando demoras en la transferencia de archivos, caídas de conexión y otros problemas que afectan la eficiencia operativa.

En relación la identificación de las fallas encontradas durante el proceso de testeo de las vulnerabilidades es importante mencionar en primeras instancias el uso de la metodología Pentesting para posteriormente ejecutar según sus fases: reconocimiento, escaneo y explotación de vulnerabilidades, adicional a ello, determinar 4 vulnerabilidades explotadas que la empresa MASTERNET posee y son: Vulnerabilidad eternal blue, FTP usuario password por default, escala de privilegios, RDP ataque fuerza bruta, SSH ataque fuerza bruta los cuales fueron clasificados según su rango de gravedad, como: baja, media, alta y critica. Por medio de simulaciones y ataques autorizados con las herramientas Nmap, Metasploit Framework, hydra y Armitage, se logró determinar diversas vulnerabilidades a las que está expuesto el sistema tecnológico de la compañía, y así poder exponer a través de este estudio recomendaciones y soportes.

En relación a las recomendaciones y estrategias es crucial invertir en la mejora de la infraestructura de red, implementar medidas de seguridad adecuadas y garantizar una correcta configuración para proteger la empresa de posibles amenazas y mejorar la eficiencia en las operaciones diarias. Es recomendable realizar evaluaciones regulares de la red para identificar y corregir posibles vulnerabilidades, así como asegurarse de que la configuración de la red esté optimizada para brindar un rendimiento óptimo y seguro. Con el manejo de la tecnología y sobre todo el trabajo en red tanto para equipos conectados al

WIFI como a la LAN deja una brecha abierta a un activo relevante como lo es la información digital que maneja MASTERNET. Y para culminar, se encentraron sistemas operativos (Windows Server 2008, Windows10), versiones obsoletas otras sin actualizaciones, deshabilitadas la seguridad de firewall, update, y protección de antivirus, se hace recomendaciones como actualización de software y compra de licencias para mitigar fallas y vulnerabilidades a las que está expuesta la seguridad informática.

Finalmente, y no menos importante el proceso ha permitido descubrir varias de vulnerabilidades que pueden ser explotadas por atacantes malintencionados. Entre estas, se destacan fallos de seguridad en la configuración de servicios, estas vulnerabilidades presentadas tienen riesgos significativos para la confidencialidad, integridad y disponibilidad de los sistemas evaluados, la explotación de estas vulnerabilidades podría resultar en la pérdida de datos, acceso no autorizado a sistemas incluso el control estas vulnerabilidades coinciden con vectores de ataque ya conocidos como Eternalblue, fallos de configuración en servidores web, uso configuraciones de seguridad débiles en los activos de red y uso de software desactualizado esto es un mal manejo en gestión de actualizaciones.

6 RECOMENDACIONES

Se recomienda a futuros investigadores relacionados con la ciberseguridad, utilizar herramientas o técnicas como el Pentesting para identificar las vulnerabilidades, instruirse adecuadamente para tener en claro el funcionamiento de dicha metodología de manera constante, ya que los ciber atacantes buscan los mecanismos y usan herramientas actualizadas para lograr cumplir sus objetivos. Por tales motivos, la seguridad informática debe de ser tratado como un tema primordial en toda empresa porque ayudará a proteger y prevenir toda la información para potenciar los negocios.

Al instante de identificar las vulnerabilidades, se encomienda usar otras herramientas tales como: Acunetix, Nexpose o Nexus. Para posteriormente clasificar las vulnerabilidades en función de su tipo: error en la configuración, error generado por un usuario, entre otros. Adicionalmente, se puede anexar otro criterio de clasificación en base a la relación con las amenazadas a las que se encuentra asociado.

Finalmente, es recomendable en la empresa MASTERNET usar framewors de seguridad para una adecuada gestión de vulnerabilidades y riesgos. También, la aplicación inmediata de las recomendaciones mencionadas en el trabajo investigativo realizado. Se encomienda crear un plan de gestión de parches y actualizaciones para los sistemas, Además de, revisar las configuraciones de seguridad de los activos de empresa, realizar análisis de vulnerabilidades periódicamente. Aplicar políticas de acceso, así como autenticación de doble factor y el uso de VPN.

Realizar un plan de respuesta ante incidentes de seguridad esto ayudara al equipo a estar preparado a actuar rápidamente ante un incidente. Y brindar capacitación a los empleados, sobre las mejores prácticas como detección de ataques de phishing y el uso de contraseñas más robustas.

7 BIBLIOGRAFIA

Altulaihan, E., Alismail, A., & Frikha, M. (2023). A Survey on Web Application Penetration Testing. *Electronics (Switzerland)*, *12*(5). https://doi.org/10.3390/electronics12051229

Alvarado, J. (2020). Análisis De Ataques Cibernéticos Hacia El Ecuador. *Revista Científica Aristas*, *2*(1), 18–27.

Bonilla, J. (2023). *Importancia del uso de la ciberseguridad enfocada al hacking ético aplicados a las empresas: una revisión sistemática de la literatura*.

Chacma-Lara, E., & Laura-Chávez, T. (2021). Investigación cuantitativa: buscando la estandarización de un esquema taxonómico. *Revista Médica de Chile*, *149*(9), 1382–1383. https://doi.org/10.4067/S0034-98872021000901382

Condori-Ojeda, P. (2020a). *Niveles de investigación*.

Condori-Ojeda, P. (2020b). *Sesión 4 Universo, población y muestra*.

Cuadros, C., Veliz, V., Veloz, J., & Cruz, M. (2022). Dialnet-SeguridadOfensivaMedianteHackingEticoParaFortalece-8590601. *Serie Científica de La Universidad de Las Ciencias Informáticas*, *15*(1), 40–53.

Cuevas, J., Muñoz, R., Di Gionantonio, M., Gastañaga, I., Gibellini, F., Parisi, G., Barrionuevo, D., & Cárdenas, M. (2018). Análisis de Vulnerabilidades de Sistemas Web en desarrollo y en producción. *XX Workshop de Investigadores En Ciencias de La Computación*, 1033–1037.

Echeverría, R. (2024). *ESTUDIO COMPARATIVO DE METODOLOGÍAS DE PENTESTING PARA LA DETECCIÓN DE VULNERABILIDADES DE LA INFRAESTRUCTURA INFORMÁTICA DE UNA COOPERATIVA DE AHORRO Y CRÉDITO SEGMENTO TRES.*

Eset. (2020). *Security Report*. *Security*, 1–15.

Febriyanti, N., Oka, A., & Piarsa, N. (2021). *Implementasi Black Box Testing pada Sistem Informasi Manajemen Dosen*. *2*(3).

Gaviria, R., Cárdenas, J., & Supelano, J. (2015). *GUÍA PRÁCTICA PARA PRUEBAS DE PENTEST BASADA EN LA METODOLOGÍA OSSTMM V2.1 Y LA GUÍA OWASP*

V3.0 INVESTIGADOR PRINCIPAL RAÚL ALBERTO GAVIRIA VALENCIA INVESTIGADOR AUXILIAR.

Guaña-Moya, J. (2023). La importancia de la seguridad informática en la educación digital: retos y soluciones. *Recimundo*, *7*(1), 609–616. https://doi.org/10.26820/recimundo/7.(1).enero.2023.609-616

Guerra, E., Neira, H., Díaz, J., & Patiño, J. (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. *Información Tecnológica*, *32*(5), 145–156. https://doi.org/10.4067/S0718-07642021000500145

Imbaquingo, D., Díaz, J., Saltos, T., Arciniega, S., De La Torre, J., & Jácome, J. (2020). *Analysis of the main difficulties in Computer Auditing*.

Jiménez, J. (2021). *MAPEO SISTEMÁTICO DE METODOLOGÍAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL CONTROL DE LA GESTIÓN DE RIESGOS INFORMÁTICOS*.

Léonard, S., & Kaunert, C. (2023). *The Securitization of Migration in the European Union: Frontex and its Evolving Security Practices*.

Llano, A., Gaibor, M., Cruz, C., & Cadena, J. (2021). Importancia de políticas de seguridad Informática de acuerdo a las ISO 27001 para pequeñas y medianas empresas del Ecuador. *Ciencias de La Ingeniería y Aplicadas*, *5*(2), 82–98.

Maillo, J. (2021). *Hackers: Técnicas y herramientas para atacar y defendernos - Juan Andres Maillo Fernandez - Google Libros*. https://books.google.es/books?hl=es&lr=&id=pgNcEAAAQBAJ&oi=fnd&pg=PA76&dq=Hackers:+técnicas+y+herramientas+para+atacar+y+defendernos&ots=RG6wI7mykh&sig=_WpjPdzZFpAsjBbeffbWzs6kLVc#v=onepage&q=Hackers%3Atécnicas y herramientas para atacar y defendernos&f=false

Martín, G. (2018). *La gestión de los riesgos tecnológicos (ICT)*.

Mayacela, M., & Guerrero, M. (2023). *Los ciberataques incrementaron un 38% en 2022 | Ekosnegocios*. https://ekosnegocios.com/articulo/los-ciberataques-incrementaron-un-38-en-2022

Michilena, J., & Díaz, P. (2011). Sistema de Gestión de Seguridad de la Información

(SGSI) en el Comando Provincial de Policía “Imbabura N o. 12.” *Repositorio UTN*, 1–9.

Ministerio de telecomunicaciones y de la sociedad de la informacion. (2020). *Guia para la gestión de riesgos y seguridada de información*. 31.

Mogollon, K. (2022). *Importancia del Sistema de Gestión de Seguridad de la Información (SGSI) y su incidencia en materia de control interno*.

Nguyen, L., Simmons, A., Tran, H., & Tran, T. (2023). *Security Testing of a Smart Home Management System using Formal Method and Gray-box Testing*. https://doi.org/10.21203/rs.3.rs-3326022/v1

Nuñez, C. (2021). *Penetration testing: auditoría profesional | Enhanced Reader*.

Nur, S., Johari, H., Adnan, R., & Tajjudin, M. (2020). *JOURNAL OF ELECTRICAL AND ELECTRONIC SYSTEMS RESEARCH Application of IMC-PID Controller with Integer-order Filter and Fractional-order Filter for Steam Distillation Essential Oil Extraction Process*.

Ortega-Garcés, D. (2023). *Análisis de metodologías para pruebas de penetración y usabilidad para PYMES*. 1–13.

Rodríguez, A. (2020). Herramientas fundamentales para el hacking ético Fundamental Tools for Ethical Hacking. In *Revista Cubana de Informática Médica* (Issue 1).

Scariot, N. (2022). ¿Qué es ser hacker? *Journal of Economic Perspectives*, *2*(1), 1–4.

Sekhon, A., Ji, Y., Dwyer, M., & Qi, Y. (2022). *White-box Testing of NLP models with Mask Neuron Coverage*.

Singh, G. (2022). Kali Linux. In *Nature* (Vol. 388, pp. 539–547).

Túqueres, O. (2021). *Análisis de vulnerabilidad en la infraestructura tecnológica de la organización Uniscan en el área funcional de frontera de la empresa. 669*.

Universo, E. (2020). *Los delitos informáticos crecen en Ecuador; cada clic en la web deja su rastro | Informes | Noticias | El Universo*.

Zafra, J. (2017). Introducción al pentesting. *Universitat de Barcelona*, 1–65.

Zhou, S., Liu, J., Hou, D., Zhong, X., & Zhang, Y. (2021). Autonomous penetration

testing based on improved deep q-network. *Applied Sciences (Switzerland), 11*(19). https://doi.org/10.3390/app11198823

Anexos

Anexo A. Encuesta personal Masternet

Evaluación del uso de la red

Evaluador: Ing. Diego Silva

Empresa: Masternet

DATOS		
PREGUNTAS PARA CONOCER EL DIAGNOSTICO DEL USO DE LA RED		
NO	Descripción	Observación
1.-	¿El uso de la red es adecuado?	Respuesta de opción múltiple
2.-	¿Los niveles de operatividad son los óptimos de los dispositivos?	Respuesta de opción múltiple
3.-	¿Han recibido ataques a la red?	Respuesta de opción múltiple
4.-	¿Tienen sistema de recuperación de fallas?	Respuesta de opción múltiple

Nota: Elaboración propia

Evaluación estado de la red

DATOS		
PREGUNTAS PARA CONOCER EL DIAGNOSTICO MANTENIMIENTO DE LA RED		
NO	Descripción	Observación
1.-	¿Utilizan equipos especializado con frecuencia para verificar su funcionamiento?	Respuesta de opción múltiple
2.-	¿Reciben manteamiento adecuado?	Respuesta de opción múltiple
3.-	¿Los estados de conexión con los demás elementos de la red son los óptimos?	Respuesta de opción múltiple
4.-	¿Utilizan dispositivos de seguridad si hubiere ataques?	Respuesta de opción múltiple

Nota: Elaboración propia