UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

DIRECCIÓN DE POSGRADO, COOPERACIÓN Y RELACIONES INTERNACIONALES

TRABAJO DE TITULACIÓN PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL GRADO DE MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

METODOLOGÍA DE AUDITORIA INFORMÁTICA UTILIZANDO TÉCNICAS Y HERRAMIENTAS DE HACKING ÉTICO PARA LA EVALUACION DE VULNERABILIDADES EN LA SEGURIDAD INFORMÁTICA EN EMPRESAS DEL SECTOR METAL MECÁNICO DE MANABÍ.

Autor: ING. VERA CONFORME JACINTO DANIEL

Tutor:

ING. SENDON VARELA JUAN CARLOS Mgtr

Febrero de 2022

DECLARACIÓN EXPRESA

Declaro que la responsabilidad del contenido de este proyecto titulado metodología de auditoria informática utilizando técnicas y herramientas de hacking ético para la evaluación de vulnerabilidades en la seguridad informática en empresas del sector metal mecánico de Manabí, es de mi persona, a la vez que autorizo a la Universidad Laica "Eloy Alfaro" de Manabí, hacer uso completo o parcial del contenido de este trabajo de Maestría, con fines estrictamente académicos o de investigación.

El derecho que me corresponde como autor, con excepción de la presente autorización, seguirán vigentes a favor, de conformidad con lo establecido en los artículos 5, 6, 8, 19 y demás artículos pertinentes de la Ley de Propiedad Intelectual y su Reglamento.

Así mismo, autorizo a la Universidad Laica "Eloy Alfaro" de Manabí para que realice la digitalización y publicación del trabajo de titulación en el repositorio virtual, en conformidad a lo establecido en el Art. 144 de la Ley Orgánica de Educación Superior.

_____

Ing. Vera Conforme Jacinto Daniel

CERTIFICACIÓN DEL DIRECTOR DE TRABAJO DE TITULACIÓN

En calidad de director de Trabajo de Titulación nombrado por la Comisión Académica del Programa de Maestría en Tecnologías de la Información de la Universidad Laica "Eloy Alfaro" de Manabí.

CERTIFICO

Que he dirigido y analizado el trabajo de titulación: metodología de auditoria informática utilizando técnicas y herramientas de hacking ético para la evaluación de vulnerabilidades en la seguridad informática en empresas del sector metal mecánico de Manabí, elaborado por Ing. Jacinto Daniel Vera Conforme con Cédula Nacional de Identidad N°- C.I. 131217724-7 estudiante de la Maestría de Tecnología de la Información, presentado como requisito previo a la obtención del Título de Magister en Tecnologías de la Información**.**

El mismo que considero reúne los requisitos legales y méritos necesarios en el campo epistemológico, siendo apto para ser evaluado por parte del Tribunal Evaluador que se designe y aprueba con el fin de continuar el proceso de titulación determinado por la Universidad Laica "Eloy Alfaro" de Manabí.

_____

Ing. Juan Carlos Sendon Varela.

TRIBUNAL DE GRADUACIÓN

Nombres Firmas

Lector 1 _____

Lector 2 _____

Lector 3 _____

Calificación Trabajo de Graduación

Calificación Trabajo Escrito: _____

Calificación Sustentación de Proyecto de Posgrado: _____

Nota Final de Trabajo de Graduación _____

Lo certifica,

SECRETARIA DE DIRECCIÓN DE POSGRADO, COOPERACIÓN Y RELACIONES INTERNACIONALES

AGRADECIMIENTO

Agradezco el apoyo incondicional de mi esposa y toda mi familia en esta etapa de mi carrera profesional, Agradecer mi tutor por las enseñanzas y guías que me pudo brindar en la elaboración de este proyecto. A la empresa del Sector mecánico por darme la apertura para realizar este proyecto y finalmente agradecer a mis compañeros de esta maestría los cuales fueron parte importante en cada momento por su incansable motivación.

DEDICATORIA

Dedicada a mi amada esposa Cristina la cual ha estado a mi lado en incasables jornadas de trabajo dándome su apoyo y cariño para seguir adelante y a mis queridos padres, quienes siempre me han apoyado y nunca han cuestionado mis esfuerzos ni mi capacidad para motivarme a hacer cualquier cosa que me proponga. Ellos me han dado la motivación para enfrentar cualquier desafío que se me presente en la vida.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Durante los últimos años la información se ha convertido en el activo más importante para cualquier organización. Debido a los innumerables ataques informáticos y las distintas formas en la que se exponen los medios informáticos, se vuelve de suma importancia contar con estrategias de control y supervisión que brinden las debidas seguridades, las cuales permitan evidenciar el estado de la seguridad informática dentro de las empresas del sector metalmecánico de Manabí.

El enfoque de esta investigación tiene como objetivo el análisis de diversas metodologías para la realización de auditorías informáticas. Basándose inicialmente en revisiones bibliográfica para la gestión de la seguridad informática, se realizó un análisis comparativo de diversas metodologías con el fin de definir adecuadamente la que más se adapte a nuestra investigación. Para evaluar el estado actual de la seguridad informática se empleó una encuesta estructural, la misma que se aplicó a los diferentes jefes departamentales del área de informática de las empresas que conforman el sector metalmecánico con el objetivo de obtener datos sobre el nivel de la seguridad informática existente.

Como resultado del análisis se pudo determinar que la metodología OSSTMM es la adecuada para este trabajo, la misma que brinda una fácil implementación apoyándonos en el manual de metodologías abiertas de testeo usando las técnicas de hacking ético como herramienta para diagnosticar, encontrar, descubrir y mitigar vulnerabilidades informáticas, de esta forma poder activar mecanismo para prevenir ataques informáticos y garantizar la confiabilidad, disponibilidad e integridad de la información.

PALABRAS CLAVES

Seguridad informática, metodología, metalmecánico, auditoria.

ABSTRACT

During the last years, information has become the most important asset for any organization. Due to the innumerable computer attacks and the different ways in which computer media are exposed, it becomes extremely important to have control and supervision strategies that provide the necessary assurances, which allow to demonstrate the state of computer security within the companies in the metal-mechanic sector of Manabí.

The focus of this research is to analyze various methodologies for conducting computer audits. Initially based on bibliographic reviews for the management of computer security, a comparative analysis of various methodologies was carried out in order to adequately define the one that best suits our research. To evaluate the current state of computer security, a structural survey was used, which was applied to the different department heads of the computer science area of the companies that make up the metal-mechanic sector with the objective of obtaining data on the level of computer security. existing.

As a result of the analysis, it was possible to determine that the OSSTMM methodology is adequate for this work, the same one that provides an easy implementation based on the manual of open testing methodologies using ethical hacking techniques as a tool to diagnose, find, discover and mitigate. computer vulnerabilities, in this way to be able to activate a mechanism to prevent computer attacks and guarantee the reliability, availability and integrity of the information.

KEYWORDS

Computer security, methodology, metalworking, auditing.

INTRODUCCIÓN

En el contexto tecnológico, el uso del internet han logrado un desarrollo significativo en la estructura de comunicación global y han diversificado la forma de acceso a la información. Sumado a esto la evolución de las telecomunicaciones la cuales han cambió la forma de transmisión de datos, migrando de un entorno centralizado a un ambiente distribuido, conectando así redes internas y externas creando un solo entorno Chalen, (2010).

Desde el punto de vista industrial, el uso de la tecnología se proyecta como uno pilares fundamentales para la automatización de sus procesos abarcando distintas tecnologías como redes inalámbricas, computación distribuida y el internet de las cosas como lo detalla sus siglas en ingles Internet of Things (IoT), siendo así esta ultima la principal innovación para sector industrial, Gabalán, (2015).

El creciente uso de soluciones Informáticas en las distintas áreas de la industria metalmecánica ha impactado directamente en sus procesos y fomentan la transformación tecnológica de muchas industrias, sin embargo, así como avanza la tecnología avanza los riesgos de mantener la información protegida y esto requiere de niveles de seguridad adecuados para la mayor protección de su información, La preservación de estos atributos constituye el paradigma básico de la norma internacional y de toda la ciencia de la Seguridad de los Información CARISSIMI, (2018).

A nivel internacional la Organización de Estados Americanos, para hacer frente a las nuevas amenazas en materia de seguridad informática, se han creado algunas estrategias, con la intervención de la empresa pública, la academia y los organismos estatales, se crearon los centros CERT (Computer Emegency Response Team). Estos son

equipos de respuesta ante emergencias informáticas, con el objetivo de limitar el daño en sistemas de información y poder garantizar la continuidad de los servicios que soportan, S-CERT, (2019).

En el Ecuador se encuentra una filial de estos equipos, llamado EcuCERT que inició sus actividades en noviembre de 2013 donde su alcance se enmarca en el ámbito de la aplicación de la Ley Orgánica de Telecomunicaciones (LOT), teniendo como objetivo el apoyo en la prevención y resolución de incidentes de seguridad informática (ecucert, 2021).

En un estudio realizado por Sendón, (2020) a varias empresas del sector industrial pesquero del cantón Manta en Ecuador, manifiesta la problemática en cuanto a las técnicas y métodos que utilizan para garantizar la seguridad informática en dicho sector industrial, observándose que, a pesar del aumento de los eventos extraordinarios, no cuentan con un proceso de gestión de incidentes informáticos, según lo manifiesta el autor la problemática está originada por el bajo presupuesto asignado a la seguridad informática, la falta de comunicación entre mandos altos y un personal encargado del área tecnológica sin el conocimiento adecuado.

En la presente investigación se observarán diferentes tipos de metodologías existentes para la auditoria informática entre las más utilizadas tenemos Application Security Project (OWASP) Testing Guide, una de las más utilizadas para auditorias informáticas Open Source Security Testing Methodology Manual (OSSTMM), y otra de las metodologías viables para un proceso de auditoria Open Web, la cual es utilizada por la certificación Certified Ethical Hacking (CEH) según Juan Diego Muñoz, (2017). La

mismas que nos permitirá evidenciar los problemas existentes en la seguridad informática de las empresas del sector metalmecánico de Manabí.

En el presente documento mostraremos los aspectos generales para determinar una metodología de auditoria informática adecuada al sector empresarial en estudio, la misma que basándose en técnicas de Hacking Ético sea la responsable de evidenciar las principales falencias en materia de seguridad informática y falta de controles.

El primer capítulo presenta el marco teórico, que incluye todos los conceptos, fases y términos de la metodología para la auditoria informática propios del mundo de la informática segura, con el objetivo de hacer comprensible el contenido del presente trabajo.

En el segundo capítulo se desarrollará el diseño metodológico y se definirá el tipo de investigación y la metodología que más se adapte al sector empresarial en estudio, para lo cual se expondrán diversas metodologías de seguridad informática.

Se indica en el tercer y último capítulo se expondrán los resultados obtenidos una vez aplicada la metodología escogida y podremos evidenciar las vulnerabilidades en la seguridad informática de las empresas del sector metalmecánico de Manabí. Se publicará la evidencia que se recolectó a lo largo del proceso del despliegue de la metodología en auditoría informática

Realidad problemática

Internacional

A nivel mundial las organizaciones están constantemente expuestas a amenazas y diversos tipos de ataques informáticos que pueden ocurrir en cualquier momento, logrando afectar la información en su confidencialidad, integridad y disponibilidad, en los últimos tiempos se ha evidenciado un aumento significativo en incidentes en la seguridad informática afectando así a las organizaciones y el uso de su información.

Armstrong &Peiris, (2014), según lo manifestado por este autor la información en una organización es un activo circunstancial y el cual siempre está en constante crecimiento, de la misma manera crecen los riesgos de mantenerla de forma segura, los sistemas de información la gran mayoría de casos no son correctamente desarrollados para soportar ataques informáticos, dejando así un punto débil para su seguridad y resguardo. el autor resalta la importancia de realizar un proceso de auditoría informática de forma periódica, las auditorías en sistemas informáticos deben contar con los mecanismos y técnicas para prevenir algún inocente de este tipo.

Un estudio realizado en el 2020 por Kaspersky Lab, que es una de las empresas enfocadas en brindar software para gestionar de la seguridad informática, expone que en Latinoamérica gran porcentaje de las organizaciones se sienten alarmadas debido incremento de los ataques informáticos como se evidencia en la figura 1. La mayoría de los casos reportados son de phishing (método para engañar y hacer que un usuario comparta información confidencial haciéndose pasar por otra persona o institución), lo

que genera una gran preocupación para las instituciones que no cuentan con una política de seguridad informática.

Figura 1
Nivel de Vulnerabilidad a nivel de Latinoamérica.

Nota: Figura de referencia de la detención de phishing en latan
Fuente: Extraído del reporte anual de vulnerabilidades de la empresa Kaspersky.

Nacional

En ecuador diversas empresas y organizaciones han presentado amenazas de ataques informáticos según lo manifiesta Gutiérrez, (2021). Tomando uno de los más relevantes y actuales como el que se presentó en la empresa pública Corporación Nacional de Telecomunicaciones (CNT), en la que se suscitado una ataque informático por medio de un ransomware (software malicioso que encripta las información con el objetivo de pedir un pago por el rescate para volver acceder a su información) este ataque encripto gran parte de la información de esta entidad dejando limitadas sus operaciones,

estos ciberataques se realizan con la finalidad de que las instituciones desembolsen grandes sumas de dinero como rescate para así poder recuperar su información.

Local

Según lo publicado por la revista empresarial Ekos (2018), menciona que el segmento de la industria metalmecánica de Manabí cuya principal actividad es la fabricación de inmobiliarios de metal, requiere cambios esenciales en las estrategias de desarrollo y mejoramiento tecnológico. En consecuencia, al desarrollo de este sector Industrial de Manabí, se viene ejecutando proyectos a mediano y largo plazo para el mejoramiento de los recursos tecnológicos con el fin de priorizar la adaptación de nuevas tecnologías.

A pesar de que este sector ha realizado importantes inversiones en mejoramiento tecnológico aún existen falencias en su seguridad informática, tomando en consideración que no cuentan con una política de seguridad informática clara, lo que genera la falta de enfoque ante posibles ataques informáticos, exponiéndose a posibles vulnerabilidades de su información.

En la actualidad no existe disponible un estudio nacional en seguridad informática de la industria metalmecánica, por esta razón los indicadores del Ministerio de Industrias y Productividad (MIPRO) han clasificados la industrial como un sector sensible a problemas de carácter tecnológico los cuales pueden generar retrasos en sus procesos.

Formulación del problema

En Ecuador la falta de implementación de medidas de seguridad Informática a los sistemas de información ha hecho que el crecimiento de ataques informáticos esté en constante desarrollo, independientemente del tamaño de la industria, el análisis de seguridad informática en cualquiera de sus formas comienza a convertirse en una actividad necesaria.

La carencia de implementación de medidas de seguridad a incrementado significativamente los problemas de seguridad de la información, el no contar una estrategia para prevenir posibles vulnerabilidades en los sistemas de información representa un gran riesgo.

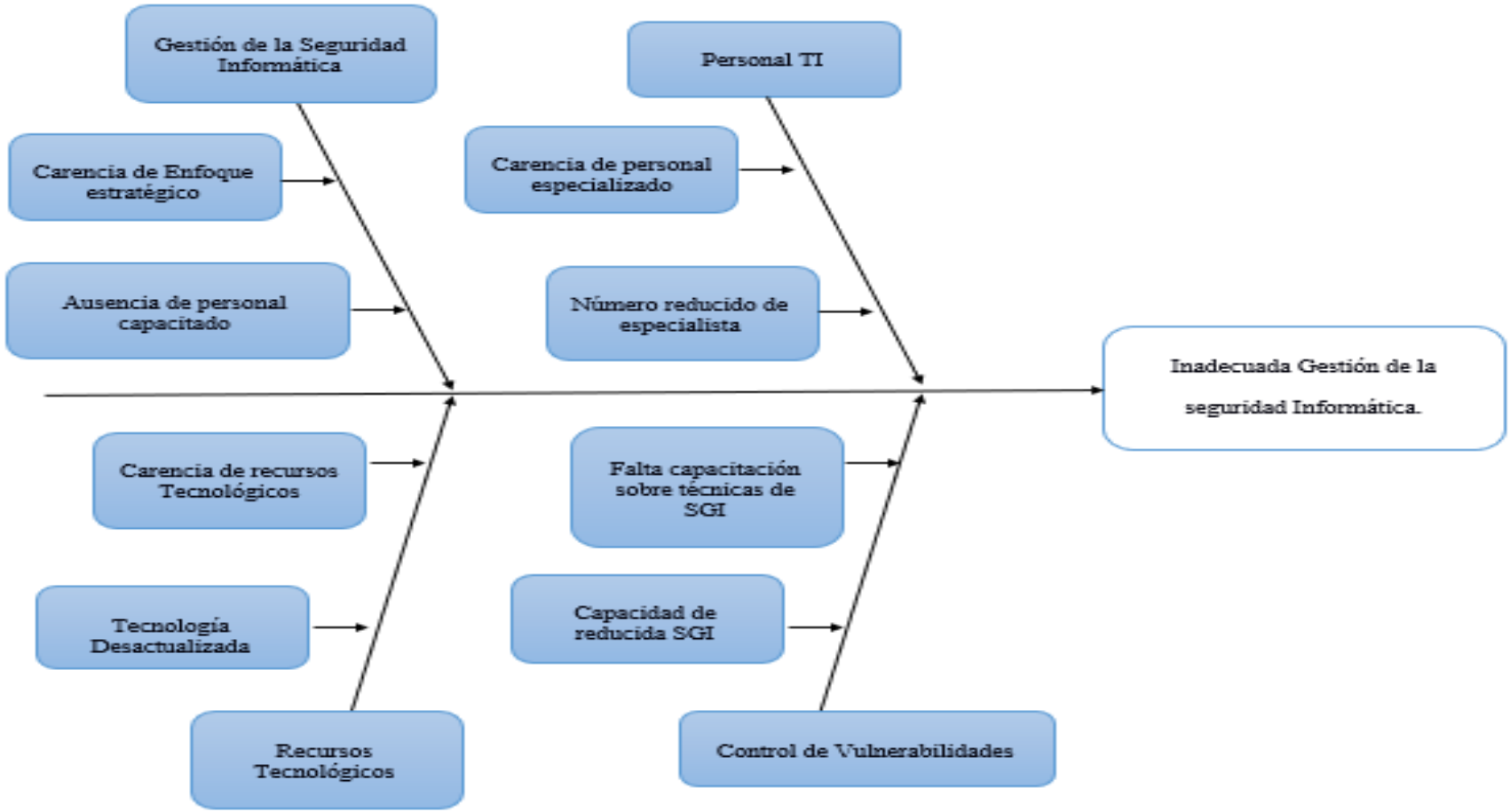
Ante esta problemática se debe efectuar una auditoria informática la misma que realizará el análisis de las metodologías para su aplicación en las empresas del sector metal mecánico, evaluando los tipos de auditoria informática, se consideró en esta investigación dos alternativas. la primera se muestra como un auditorio documental donde se realiza el proceso de verificación en la documentación que brindan cada una de las áreas, con el objetivo de evaluar el cumplimiento de las normativas de seguridad Informática. Por otro lado, la segunda propuesta está basada en la aplicación de una metodología en auditoria informática utilizando herramientas de hacking ético las cuales permitirán exponer las diferentes vulnerabilidades con respecto a la seguridad informática.

considerando lo mencionado anteriormente, se definió aplicar una metodología de auditora informática, la misma que faculte el uso de herramientas de hacking ético,

que nos permitirán detectar vulnerabilidades en la seguridad informática, con esto poder identificarlas, clasificarlas y establecer lineamientos para su mitigación.

Por lo tanto, el problema radica en última instancia en la falta de una adecuada evaluación de los procesos cuando se trata de sistemas de seguridad de la información, a esto se le suma el desconocimiento del estado de seguridad de la Informática, lo que impide tomar decisiones y acciones correctivas para asegurar la integridad de la información

Figura 2
Formulación del esquema de Problema



Nota: formada en base a la problemática existente
Fuente: Elaboración Propia
.

Justificación e importancia del estudio

Se justifica el desarrollo del presente proyecto, basándose en la Ley Orgánica de Protección de Datos Personales del ministerio de telecomunicaciones y de la sociedad de la información, la cual en su artículo 66 reconoce y garantizará a las personas naturales y jurídicas: "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección (TELECOMUNICACIONES, 2021).

Actualmente las empresas del sector metalmecánico se ven en la necesidad de realizar una auditoria informática porque desde el punto vista empresarial permitirá evidenciar las posibles falencias informáticas del su sector, razón por la cual se hace inevitable considerar las metodologías de auditoria informática para establecer la más acorde y aplicarla basándose en los aspectos tecnológicos con respecto a la metodología escogida, llegando a establecer procesos y generando reportes sobre las fortalezas y debilidades en seguridad informática.

En referencia a lo mencionado en el párrafo anterior, se justifica de forma practica la importancia que tienen los procesos de auditoria informática en la empresa, puesto que se proporcionará una mejor perspectiva del uso de la información, esto será de gran utilidad para el desarrollo de políticas de seguridad de la información, a su vez permitirá que se tomen acciones correctivas necesarias para mejoramiento continuo de las empresas del sector metalmecánico de Manabí.

La justificación teórica, de acuerdo con Calle (2020), los antecedentes previos a la investigación, se generará mediante los resultados obtenidos en la encuesta

estructurada que se realizó al personal del área de tecnología de la información de cada empresa del sector metalmecánico, y en base a esto poder definir una metodología que sea adoptable a los procesos administrativos y operativos de las empresas en estudio.

Abordando el ámbito Metodológico como un factor importante las metodologías de auditoria informática son claves en los procesos de las empresas del sector metalmecánico de Manabí. Por este motivo genera la necesidad de implementar un control metodológico para conocer, analizar y detectar vulnerabilidades en la seguridad informática y la cual contribuirá a un nuevo modelo de negocio para las empresas en varios sectores empresariales.

Objetivos

Objetivo General

Formular una evaluación de la seguridad informática utilizando una metodología de auditoria informática la cual permita el uso y aplicación de técnicas y herramientas de hacking ético en el sector Industrial metalmecánico.

Objetivos Específicos

- Efectuar un levantamiento de información vía encuesta para determinar el nivel actual de la seguridad informática dentro de del sector metalmecánico de Manabí.
- Establecer una revisión bibliográfica sobre las distintas metodologías de auditoria informática, así como de técnicas de hacking ético que permita la realización de un diagnóstico de vulnerabilidades informáticas en el sector metalmecánico de la provincia de Manabí.
- Realizar un análisis comparativo de las distintas metodologías de auditoría informáticas revisadas en la bibliografía, así como las técnicas de hacking ético que puedan ser utilizadas en la evaluación.
- Aplicar la metodología de auditoria informática evaluada, resultado del análisis comparativo, para determinar las principales vulnerabilidades en una empresa del sector metalmecánico.
- Proponer lineamientos basados en la metodología de auditoria informática para garantizar la seguridad informática en las empresas del sector metalmecánico.

CAPITULO I. MARCO TEÓRICO REFERENCIAL Y LEGAL

1.1 Introducción

En este capítulo se examinarán los conceptos relacionados con la seguridad de la información junto con sus principios fundamentales, elementos clave, términos y definiciones sobre los diferentes mecanismos de prevención, así como temas sobre la gestión de riesgos.

En los últimos años, la seguridad de la información se ha posicionado como un proceso indispensable y ha pasado de ser considerada por los ejecutivos de corporaciones y organizaciones multinacionales como una inversión.

La globalización ha creado un mundo digital donde la información es la actividad intangible más valiosa a la que estamos conectados. En algunos países, la transformación digital ocurrió rápidamente, mientras que en otros tomó más tiempo ASTUDILLO, (2017).

La información se ha convertido en una actividad crítica para el éxito y la supervivencia de cualquier organización en el mercado. Como resultado, el objetivo principal de las organizaciones es garantizar la seguridad de esta información y los sistemas que la procesan.

Para una adecuada gestión de la seguridad de la información, es necesario implementar un sistema que aborde esta tarea de manera metódica, documentada y metódica, con objetivos de seguridad claros y una evaluación precisa de los riesgos a los que está expuesta la información de la organización (ORREGO, 2010).

1.1.1 Antecedentes investigativos referenciales.

En el presente trabajo se ha revisado la bibliografía científica y técnica sobre la problemática establecida, basándose en los objetivos específicos los cuales permitirán realizar un análisis del contexto de la investigación y que sirven como sustento para el desarrollo del proyecto.

El conocimiento que tenemos ahora es parte de la acción que demuestra las implicaciones y efectos sobre los procesos cognitivos y prácticos relacionados con la búsqueda de información almacenada en las computadoras, así como el diseño de dichos sistemas y su papel en la sociedad Capurro R., (2007). El mismo autor cita una definición de la información como ciencia propuesta por Belver Griffith como el objetivo de la creación, recopilación, organización, interpretación, asignación, almacenamiento, recuperación, difusión, transformación y uso de la información (Griffith Belver, 1980).

Por otra parte, el Ingeniero Informático y doctor en Seguridad Informática José Alonso Cebrian más conocido con su seudónimo (chema alonso) plantea ante la RAE el termino *Hacker* con un significado diferente al estipulado con este organismo, Según chema alonso el termino define un amante de la tecnología que busca sus límites. Teniendo en cuenta a los *Hacker* que trabajan como especialistas en seguridad de la información y desarrollan herramientas para intentar fortalecer a los sistemas comerciales descubriendo los puntos débiles que debían fortalecerse en preparación para cuando llegaran los *Hacker* maliciosos o ciber criminales.

1.1.2 Teorías relacionadas al tema.

En un informe difundido por la empresa francesa de software Antidot, se afirma que en la actualidad, donde todo se mueve con mayor rapidez, la información supone un desafío estratégico para las empresas, sirviendo como recurso y actividad imprescindible para cualquier organización y clave para el negocio en la toma de decisiones, implementación de estrategias y transferencia tecnológica, permitiendo ventajas competitivas y maximizando el valor de todas las partes involucradas a través de estos procesos (Antidot, 2014).

Según López Santoyo, (2015), menciona que la seguridad de la información se refiere a una práctica de defensa de equipos informáticos, dispositivos electrónicos, sistemas informáticos, dispositivos móviles. La seguridad de la información permite identificar y eliminar las vulnerabilidades de la red, brindando a los usuarios la capacidad de defenderse contra cualquier ataque malicioso.

1.2 Auditoria

El contexto de auditoria proviene del latín “auditorius” el cual su significado es la persona que tiene la virtud de oír y revisar cuentas. En un proceso de auditoria informática se puede evaluar la eficacia y eficiencia de los procesos informáticos, equipos tecnológicos, controles, archivos y seguridad. Mediante esta práctica se realiza un proceso de acción la misma que permite la tomar decisiones para de esta forma corregir errores en caso de que existan o a su vez mejorar la forma de trabajo (Pérez, 2017).

1.2.1 Auditoria Informática

Aunque con frecuencia hablamos de "auditoría Informática", sería preferible utilizar el término" auditoría de tecnología de la información", bajo este concepto se describe como el conjunto de técnicas, actividades y procedimientos destinados a el análisis, evaluación, verificación y planificación sobre el control de la seguridad informática. La auditoría informática Comprende un examen metódico del sistema informático en institución donde se verificará la rentabilidad, seguridad y eficiencia (Gonzalo, 2017).

1.2.2 Tipos de Auditoria de seguridad informática.

Como lo menciona Muñoz Enrique, (2018) La auditoría informática para la seguridad de la información se ha dividido en varios tipos los cuales detallamos a continuación:

- **Auditoría Informática Interna:** Es la estructura organizativa que se realiza con recursos materiales y personas que pertenecen a la empresa o institución donde se aplica. El departamento que realiza estas acciones planifica, ejecuta y controla actividades que contribuyen fundamental a descubrir deficiencias o irregularidades dentro de la organización.
- **Auditoría Informática Externa:** tiene sus bases en la contratación de un servicio de consultora externa para llevar a cabo el proceso de auditoría Informática estructurado, Puesto que el servicio de consultaría no es parte de la organización, está mejor posicionado para emitir un juicio realista de las tareas que requieran correcciones o acción de mejora.

1.2.3. Fases o etapas de la Auditoría de Sistemas

Según Muñoz Enrique (2018), existen tres fases o etapas principales en una metodología de auditoría que puede ser utilizada para cualquier tipo de auditoría dentro del campo de los sistemas:

- **Planeación de la auditoría**: Esto incluye identificar el origen de la auditoría, realizar una visita preliminar al área a evaluar, establecer los objetivos de la auditoría y seleccionar los puntos de evaluación, Crear planes, programas y presupuestos para realizar la auditoría, elegir los métodos, herramientas, equipos y procedimientos requeridos para la auditoría y finalmente asignar los recursos y sistemas informáticos para la auditoría.
- **Ejecución de la auditoría**: Durante esta fase, las acciones previstas para la auditoría se llevan a cabo utilizando las herramientas e instrumentos elegidos durante la fase anterior. Además, los documentos de las desviaciones descubiertas son identificados y desarrollados para crear el decreto preliminar que se incluirá en el cuerpo de papeles de trabajo del auditor.
- **Dictamen de la auditora**: Las principales tareas a realizar en esta etapa son el análisis de la información y la elaboración de un informe sobre las situaciones detectadas que se registrará en un dictamen final y se presentará como informe de auditoría (Muñoz Razo, 2018).

1.2.4. Importancia de la auditoría de sistemas informáticos.

Dado que establece mecanismos que ayudan a lograr una mayor confianza en la información que se obtiene y procesa, la auditoría de los sistemas de información “es una práctica no sólo recomendable sino aceptada por todos los miembros de la organización” (GONZÁLEZ, 2019).

1.3 Seguridad de la información

Las instituciones o empresas independientemente de la actividad económica o productiva a la que se dediquen, basan su desarrollo en la información la misma que se considera como un activo de gran valor para la organización, debe protegerse adecuadamente debido a la exposición permanente de una gran variedad de amenazas y vulnerabilidades, colocando en riesgo la confidencialidad, integridad y disponibilidad de esta.

Debido a que la información puede adoptar diversas formas sea escrita, en papel, correo electrónico, almacenada digitalmente, transmitida mediante voz, video, medios electrónicos entre otros, también existen varias maneras por las que pueden ser sustraídas, robadas o modificadas gracias a la interconectividad de las redes (STRASSMANN, 2019).

Ruiz & López (2020), afirman en su página web que dentro de una organización, mantener la confidencialidad, integridad y disponibilidad de la información , así como de los sistemas involucrados en su manejo, constituye a las buenas prácticas en materia de seguridad de la información, es decir, asegurar la continuidad de las actividades de la organización mediante una rápida y oportuna reacción ante desastres, minimizando los

daños y maximizando el retorno de las inversiones y las oportunidades de negocios. Bajo estos tres parámetros se construye la seguridad de la información.

1.3.1 Confidencialidad de la información

El acceso a la información está contemplado en la constitución y detalla que únicamente a la persona que, en virtud propia o de un tercero, revele información registrada será condenado a prisión privada de uno a tres años de libertad. Este recurso solo está disponible para aquellos que tienen los permisos y privilegios propios para acceder a ella. El acceso no autorizado, el acceso clandestino, la fuga de información o la sustracción de la información están protegidos por la ley en su sección tercera Delitos contra la seguridad de los activos de los sistemas de información y comunicación del COIP (ASAMBLEA NACIONAL, 2014).

1.3.2 Integridad de los datos

La integridad de los datos dictamina que la cadena de información debe ser la misma en todo momento, es decir, no debe cambiarse ni eliminarse durante la transmisión o el almacenamiento de esta misma. Cuando la información se cambia, modifica o corrompe, sin variaciones del original, que se considera exacto y confiable (Fritz, 2016).

1.3.3 Disponibilidad

El termino de disponibilidad en la información tiene sus bases en tener acceso a las fuentes de información en cualquier momento, ya sea información o servicios, siempre deben estar listos y disponibles cuando los usuarios lo necesiten, Zambrano Carolina (2019).

1.3.4 Autenticidad

Significa asegurarse de que una entidad es quien dice ser o, en otras palabras, tener confianza en la fuente de información. Afecta la autenticidad de los dispositivos en la red de transporte de datos, como switches, enrutadores y destinos de origen y destino, debido a que actualmente existen ataques dirigidos a asegurar la identidad de estos dispositivos (Altamirano & Oré, 2017).

1.3.5 Trazabilidad

Consiste en determinar cuándo se requieren las acciones realizadas por los usuarios, así como cuándo se realizaron. Este concepto también incluye la capacidad del administrador de monitorear todo lo que sucede en la red en tiempo real para identificar usuarios o dispositivos que interfieren con el funcionamiento normal de la red, rastrear posibles atacantes y aprender de decisiones pasadas en la red (Pinzon Cepeda, 2010).

1.4. Metodología de Trabajo.

Una metodología se refiere al camino o grupo de acciones a seguir para lograr una meta que une una tarea que requiere habilidades y conocimientos particulares. Habrá varias metodologías dependiendo del tipo de seguridad que se persiga (defensiva u ofensiva). Dicho de otro modo, puede tener como objetivo la implementación segura de software, o puede ser una metodología de desarrollo segura, o puede tener como objetivo evaluar la confidencialidad, integridad y disponibilidad de los datos almacenados.

1.4.1 Metodología de Auditoría Informática.

Una metodología en auditoria informática hace referencia al conjunto de procedimientos para realizar un objetivo en concreto en la que se requiere habilidades y conocimientos específicos. Existen varios tipos de metodologías en función del tipo de seguridad que se necesite estas pueden ser (defensiva u ofensiva), es decir puede tener variar objetivo a medida que se despliega la metodología, (Pérez Merlos, 2019).

1.4.2 Necesidad de Metodologías.

Una estandarización de la industria Metalmecánica es absolutamente necesaria dada la importancia y el rápido crecimiento de la tecnología. De ahí que, es necesario procesos estandarizados de auditoría de la seguridad de la información, llevados a cabo por mecanismos de revisión y control dentro del sector industrial en estudio.

Es un desafío completar este trabajo sin una metodología porque hay muchas variables que deben tenerse en cuenta y muchas consideraciones al realizar un análisis de seguridad Informática. Son muchas las razones que hacen necesaria la existencia y uso de metodologías.

- Proporcionan un orden adecuado de las pruebas.
- Abarcar todas las diferentes pruebas que correspondan realizarse.
- Proporcionar en gran medida el desarrollo al analista.
- Los resultados se muestran de una forma más organizada y ordenada.
- Realización del proceso de una forma ética y legal.

1.4.3 Tipos de Metodologías de Auditoria Informática

Según lo ilustra Gonzalo (2017), existen dos tipos metodologías de Auditorias Informáticas y todas dependen de lo que se pretenda revisar o analizar, para ilustrar lo mencionado analizaremos los dos tipos metodologías mencionados a continuación:

Metodologías Generales: Las metodologías generales según CEPAL (2020), consienten en dar un informe sobre la fiabilidad de la información, el resultado de esta metodología es un informe estructurado donde se evidencian las vulnerabilidades encontradas. Es importante conocer que este tipo de auditoria informática tiene como material de trabajo procesos de encuestas o los checklist, cuestionarios, entre otras que permiten anotar observaciones que ayudan a conservar datos importantes de pruebas sobre hallazgos.

Metodologías Específicas: Las metodologías especificas se definen como aquellas que el auditor interno o externo "formula" para su uso, son más específicas y exhaustivas dependiendo donde se aplican en estas metodologías se pueden usar varias técnicas para evidenciar las vulnerabilidades informáticas, al igual que la anterior metodología se generan informes que permiten el registro de las acciones y sus observaciones.

1.5. Descripción conceptual de metodologías de auditoría informática.

Dado que el enfoque del presente trabajo es desarrollar una metodología de evaluación de la seguridad informática en el sector metalmecánico de Manabí, es importante comprender cómo se llevan a cabo las evaluaciones en cualquier área a través de un conjunto de acciones específicas y procedimientos metodológicos, similares a los

que se utilizan en la auditoría. Deben crearse previamente de acuerdo con las ideas y los saltos de línea que se presentan a continuación:

1.5.1. Metodología de Auditoría.

Una metodología de auditoría está enfocada a evaluar muchos aspectos sobre la eficacia y la productividad de las operaciones de una empresa u organización, este tipo de auditoria fomenta las actividades donde su prioridad se centra en las fases operativas. Un plan de auditoría servirá como guía para llevar a cabo diferentes pasos los cuales buscan la eficiencia, efectividad y economía en el empleo de los recursos humanos, financieros, ambientales, tecnológicos y de tiempo logrando así el cumplimiento de las atribuciones institucionales, (ISACA, 2011).

1.5.2. Metodologías de auditoría informática para seguridad de la información.

Según (International Organization for Standardization - ISO), la norma ISO/IEC 27001:2013 la cual especifica los requisitos generales diseñados para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza" con el fin de lograr:

- Establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización.
- la evaluación y gestión de los riesgos de seguridad de la información que se adaptan a las necesidades de la organización.

Las directrices proporcionadas por el estándar ISO/IEC 27002: 2013 brindan orientación para las normas de seguridad de la información organizacional y las prácticas de gestión de la seguridad de la información, incluida la selección, implementación y gestión de controles, teniendo en cuenta el entorno organizacional para el riesgo de seguridad de la información (Organización Internacional para la Estandarización, 2018).

1.6. Sistemas de información.

Comprender los conceptos de sistemas, tecnologías de la información y la comunicación es un requisito previo para participar en el proceso de una auditoría de las tecnologías de la información y la comunicación. El auditor podrá juzgar la naturaleza del problema y los riesgos que se encontrarán al planificar y llevar a cabo la auditoría una vez que haya adquirido una comprensión y familiaridad con el entorno informativo.

1.6.1. Características de los sistemas de información.

Si el objetivo principal de un sistema de información dentro de una organización tuviera que resumirse en una sola oración, se podría decir que la responsabilidad de este sistema es proporcionar información oportuna, precisa y en el formato adecuado a la persona que la necesita dentro .la organización, en el momento preciso en que esa persona necesita tener acceso a esta información.

Las organizaciones se beneficiarán de la información en la medida en que le facilitará la toma de decisiones, por lo que deberá cumplir una serie de requisitos, entre los que cabe destacar:

- **Exactitud**: dicta que la información debe ser independiente de errores y con alta precisión.

- **Completitud**: La información debe sustentar todos aquellos hechos que pudieran ser relevantes.
- **Economicidad**: El costo en que se debe incurrir para obtener la información debe ser menor que el beneficio proporcionado.
- **Confianza**: Para dar crédito a la información obtenida, se ha de garantizar tanto la calidad de los datos utilizados, como la de las fuentes de información.
- **Relevancia**: la información debe ser útil para tomar decisiones. En este sentido, en este contexto se debe evitar cualquier acción que sea innecesaria o que no agregue valor.
- **Nivel de detalle**: La información debe reflejar el nivel de detalle relevante para la decisión que se está tomando, debe contener la presentación y el formato adecuados para que sea sencillo y fácil de manejar.
- **Verificabilidad**: La información ha de poder ser verificada y justificada en todo momento.

1.6.2. Estructura de los sistemas de información.

Los componentes que conforman los sistemas de información son cinco de los cuales podemos citarlos como fundamentales en esta estructura: personas, actividades, datos, redes y tecnología, la existencia de una conexión entre los componentes internos de la organización y los sistemas de información forman la estructura que menciona el autor (Gómez Viertes, 2018).

1.6.3. Clasificación de los sistemas de información.

En general, las clasificaciones más extensas de los sistemas de información buscan agruparlos según su propósito. En una escala muy amplia, se puede decir que los dos propósitos fundamentales de los sistemas son los siguientes:

- **Soporte a las actividades operativas**: incluye a los sistemas de información para actividades más estructuradas (como contabilidad, ventas, adquisiciones y, en general, lo que se denomina "gestión corporativa "), así como sistemas que permiten una gestión de información menos estructurada, como aplicaciones ominosas y programas técnicos para funciones de ingeniería.
- **Soporte para las decisiones y el control de la gestión**: se puede proporcionar directamente desde las aplicaciones internas de gestión empresarial (mediante la extracción de datos de fuentes existentes) o mediante aplicaciones especializadas.

En los sistemas de información de gestión se pueden generar informes bajo demanda de forma periódica cuando se presenta una situación excepcional (posiblemente desencadenando el control por excepción en este caso). En estos informes, es posible comparar las metas previstas con los resultados reales de las distintas operaciones realizadas para cada área funcional o centro de responsabilidad (González Gallego, 2014).

1.7. Conclusiones concernientes al marco teórico en referencia al tema propuesto.

Una vez culminado este capítulo donde se investigó y analizo exhaustivamente cada uno de los temas que conforman el marco teórico para el desarrollo del proyecto planteado, se llega a lo siguiente:

- Como componente del proyecto de investigación, se examinaron proyectos, libros, artículos científicos y proyectos de otras universidades relacionados con el tema.
- La investigación del marco teórico permitió conocer detalles cruciales sobre el flujo de trabajo, las etapas y las mejores prácticas para el uso de la metodología que se utilizara.
- Los conceptos analizados basados en procesos metodológicos de seguridad de la información, serán de mucha relevancia para el proceso investigativo.

CAPITULO II. DISEÑO METODOLÓGICO

2.1. Investigación Científica.

Una de las cualidades esenciales del ser humano es la tendencia de comprender y explicar el mundo que le rodea y buscar el sentido de las cosas. La investigación científica consiste en una serie de etapas a través de las cuales se busca entender, verificar, corregir y aplicar el conocimiento, por medio de la aplicación del método científico procurando tener información importante y fidedigna (Rodriguez Moguel, 2015).

2.1.1 Tipo de investigación.

El presente trabajo refleja los requerimientos metodológicos de una investigación aplicada debido a que se caracteriza por emplear técnicas de auditoria para la seguridad informática de forma operativa con la que se busca atender necesidades prácticas de una metodología abierta, de esta manera poder aportar con nuevos hallazgos de vulnerabilidades y dale solución de forma satisfactoria, apoyándose en nueva estrategia la información obtenida puede ser valiosa y respetable para la teoría. La investigación que se lleva a cabo dirige sus esfuerzos a abordar las necesidades del sector metalmecánico de Manabí con respecto a la seguridad informática.

La investigación que se proyecta aplicar se centra en abordar la problemática antes expuesta las empresas del sector metalmecánico de Manabí y su posible solución. El proyecto actual tiene como objetivo la búsqueda, recuperación, análisis, crítica e interpretación de datos relevantes, para aportar soluciones integrales.

2.1.2. Alcance de la investigación

El método de investigación que se utilizara en este proyecto será cuantitativo a causa de evaluar la metodología de auditoría Informática que se adapte los resultados como métricas o RAV, esta investigación además pretende abarcar la mayoría de los ambientes tecnológico que tiene el sector metalmecánico de Manabí.

En esta investigación, auditará la seguridad de la información teniendo en cuenta la metodología escogida, con el objetivo de evaluar los riesgos para la seguridad de la información en las empresas del sector metalmecánico de Manabí. La población serán las empresas del sector metalmecánico, y para la exposición se recolectaron datos sobre la gestión de los departamentos de tecnología de la información de cada empresa. Los métodos de recolección de datos utilizados en este estudio fueron cuestionarios y entrevistas.

2.1.3. Métodos de investigación

En cuanto a las técnicas utilizadas para recopilar la información para esta investigación, se realizan las siguientes técnicas.

2.1.3.1. Analítico - Sintético.

Esta técnica examina eventos comenzando con la disección del objeto de estudio en cada una de sus partes constituyentes para el análisis individual, y luego combinando esas partes para un análisis holístico y comprensivo (síntesis), Bernal Torres C.A, (2006). Este método de ayuda para llevar a cabo la descomposición de los temas de estudio de metodología de auditoria informática utilizando técnicas y herramientas de hacking ético para la evaluación de vulnerabilidades en la seguridad informática en empresas del sector

metal mecánico de Manabí con el fin de analizarla y sintetizarla con base en información encontrada en diversos libros, resaltando la información pertinente para cada variable de estudio.

2.1.3.2. Inductivo - Deductivo.

Este método de inferencia está basado en la lógica y conectado al estudio de hechos particulares, arrojando conclusiones del más específico al más general de los hechos observados (inductivo) y del más general al más específico, basado en hechos observados en leyes o generales. reglas (deductivo). Ibáñez P. J. (2015). Esta metodología se utiliza en este capítulo, para realizar las inferencias relacionadas con el estudio de la metodología de auditoría informativa.

2.1.4. Herramienta de recolección de datos.

La recolección de datos para un proyecto de investigación cuantitativa es similar a medir o evaluar un grupo de datos que tiene en cuenta características numéricas, Orellana López & Sánchez Gómez, (2016). En el campo de la ciencia, la mayoría de las variables se miden con un alto grado de precisión.

Para el desarrollo de este proyecto se emplearon técnicas de investigación que arrojaron resultados que podrían ser utilizados para medir el valor de la solución con relación al problema, como lo observamos en la Tabla 1.

Tabla 1
Datos de investigación

TECNICAS	INSTRUMENTOS
Cuestionario	Formularios
Encuesta	Formularios
Entrevista	Formularios

Fuente: investigación propia

2.1.4.1. Cuestionario.

Es la principal herramienta de recolección de datos utilizada en técnicas de encuestas impresas o en línea, esta herramienta permite que la persona consultada llene por sí misma lo encuestado. Mendelsohn (2014). dicho instrumento de recolección de datos permite obtener la información de manera más amplia, las preguntas que componen el cuestionario ayudan a resolver dudas en referencia al tema de estudio.

2.1.4.2. Encuesta.

Es una metodología que hace uso de una colección de procedimientos de investigación estándar para recopilar y analizar una serie de datos de una muestra de casos que son representativos de una población teniendo en cuenta las respuestas de los sujetos de estudio. Aquiahuatl E.C. (2015). Las empresas del sector metalmecánico de Manabí donde se aplicará esta técnica que permitirá entrevistar al grupo de personas que laboran en el área de tecnología de la información, que servirá para sustentar inductivamente los hallazgos.

2.1.4.3. Entrevista.

Es una conversación que tiene un objetivo claro y está respaldada por ese objetivo. También tiene una dirección clara y se lleva a cabo con ese objetivo en mente (Figueroa C. M, 2012).

2.1.5. Revisión Bibliográfico.

El proceso para efectuar una revision bibliográfica se enfoca en examinar la documentación previa obtenida para realizar una investigación. La revisión bibliográfica justifica con base en autores las bases de las investigaciones. las bibliografias a revisar muestran un resumen de varios estudios y artículos que da una idea del actual estado de la investigación. En la revisión, un crítico de evaluación es realiza una valoración crítica de otras investigaciones sobre un tema definitivo.

2.1.5.1. Características de la revisión bibliográfica.

En la revisión de la literatura debe contar con características que nos permita conjugar con el tema de forma que podamos contar con un conocimiento acertado del tema en estudio. Las características se resumen en las siguientes fases.

- Seleccionar tema a investigar
- Organizar ideas.
- Búsqueda de información en bases de datos.
- Revisar, depurar y analizar los resultados
- Redactar la revisión bibliográfica.
- Publicar la revisión bibliográfica.

2.2. Plan de Muestreo.

2.2.1. Identificación de la población.

Es una agrupación de personas, cosas o medidas que tienen características comunes que se pueden ver en un lugar o tiempo específico. Se encuestó al personal del departamento de tecnología de la información de 9 empresas del sector metalmecánico de Manabí, Ecuador.

2.2.2. Identificación de la muestra.

Es un subconjunto exacto de la población hay varios tipos de museo, y el tipo elegido determinará la calidad. Debido a que nuestra población es tan pequeña, el museo no se utilizará en este documento. En su lugar, se utilizará toda la población. Esta herramienta se utilizó para que el gerente de tecnología de la información de la industria metalmecánica de Manabí tenga una mejor comprensión de las políticas de seguridad de la información.

En esta investigación se encuestó un total de 9 empresas pertenecientes al sector Metalmecánico de Manabí las cuales se encuentran catalogadas como industrias activas dentro de cámara de comercio de Manabí.

Esta investigación se centrar en el análisis de la población más que en la muestra obtenida, donde la población es casi idéntica a la de la muestra y comprende el 100 % de la población, hace plausible el plan propuesto.

1. **¿Las empresas del sector metalmecánico tiene políticas de seguridad de la información?**

En la empresa si existen políticas de seguridad, pero con un nivel bajo de incidencia.

2. **¿Dentro de la empresa se han socializado las políticas de seguridad de la información**?

Los medios de difusión para estas políticas se han realizado por medio de boletines y correo electrónico, en este caso las políticas de seguridad de la información se las comunica por el mismo medio desde la matriz.

3. **¿Cuenta la institución con los mecanismos que se utilizan en para evaluar el cumplimiento de las políticas de seguridad de la información?**

Actualmente no se tiene conocimiento de que exista un mecanismo para verificar si se están siguiendo las políticas de seguridad de la información.

4. **¿En la empresa se ha socializado de forma práctica las políticas de seguridad de la información con el resto del personal?**

No se ha realizado hasta el momento ningún tipo de socialización de políticas en la empresa.

5. **¿los problemas más frecuentes que se presentan con respecto a la seguridad de la información se producen de forma interna?**

Los problemas que se presentan con mayor frecuencia son la perdida de contraseñas debido a varios sistemas.

6. **¿**los **usuarios cuando tienen dificultad en el envío de información acuden a ustedes?**

Cuando no es considera como un problema complicado lo realizan por sí mismo y en cuanto ya es más complejo o los usuarios no tienen conocimiento del tema acuden al encargado de informática.

7. **¿los usuarios cuando tienen dificultad en el envío de información acuden a ustedes?**

Que los usuarios realicen por medio de la plataforma de correo electrónico empresarial que es una plataforma oficial.

8. **Dentro de la empresa se utiliza el correo institucional, personal para compartir información sea segura y no exista fugas y no sea utilizada por terceros.**

El método más recomendado para la difusión de información es el correo electrónico institucional, siempre que se tomen las debidas precauciones en todo momento.

2.3. Metodologías de trabajo.

Las diversas metodologías y técnicas de trabajo para este tipo de investigación son una suma de procedimientos que se deben cumplir con el propósito de realizar una implementación acorde objetivo propuesto. particularmente se debe realizar el análisis en las organizaciones para poder determinar la metodología adecuada para alcanzar las metas y objetivos.

2.3.1. Metodologías Abiertas para Auditoría de Seguridad Informática.

Según Maya y Jaramillo, (2015), el objetivo de una auditoría de seguridad es proporcionar elementos de juicio y acción para garantizar la eficacia, integridad y cumplimiento de las políticas implementadas. De acuerdo con el autor mencionado, una auditoría de seguridad de la información examina los procedimientos relacionados con la seguridad física y lógica al tiempo que garantiza la confidencialidad, integridad y accesibilidad de la información.

2.3.2. Revisión de Metodologías

Esta parte del capítulo repasaremos las metodologías de auditoría informática más utilizadas y conocidas en la actualidad.

- OSSTMM
- OWASP
- PTES

2.3.2.1. OSSTMM

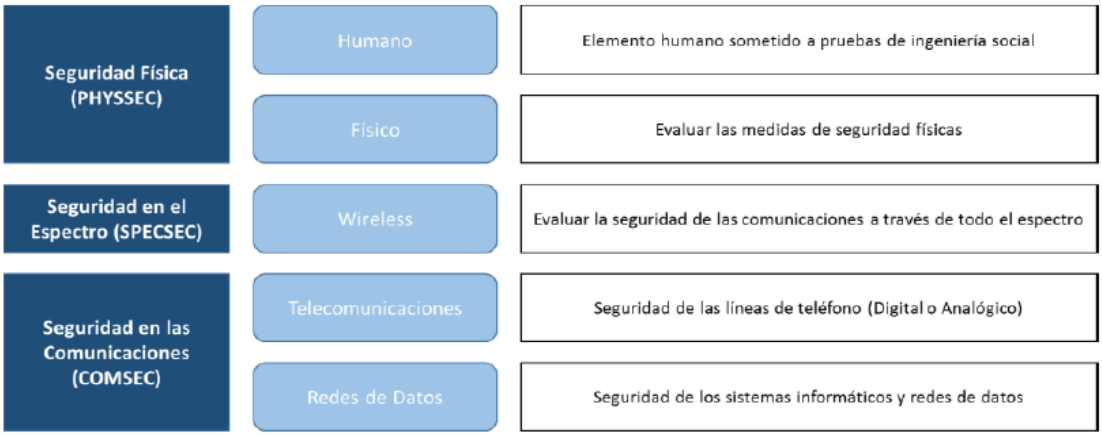
Esta metodología ha sido desarrollada por la organización ISECOM esta es una organización abierta y colaborativa, que fue fundada en enero de 2001 y se basa en la investigación en seguridad de la información. Su objetivo es dar a conocer la seguridad Informática, la investigación, la provisión de certificaciones y la integridad empresarial. Esta sistemática garantiza que sus proyectos y metodologías están libres de influencias comerciales. Las siglas con la que se representan es Institute for Security and Open Methodologies con traducción la cual sería Instituto de Seguridad y Metodologías Abiertas.

Una de sus principales ventajas es que tiene OSSTMM es una comprensión amplia del concepto de seguridad, en lugar de centrarse en áreas específicas que no están relacionadas con ella como lo hacen otras metodologías (ISECOM, 2020).

Esta metodología evalúa los siguientes puntos de la seguridad Informática los mismo que se evidenciamos en la figura 3:

- Factor Digital
- Factor Físico
- Factor Social
- Métricas
- Informes

Figura 3
Ámbitos de la metodología OSSTMM



Nota: clasificación de la metodología OSSTMM tomado del autor
Fuente: (Toth & Szneck, 2014).

Tipos de Herramientas de auditoría de la metodología OSSTMM

Hacking Ético Según Astudillo (2017), el hacking ético consiste en realizar pruebas de intrusión controlada en los sistemas informáticos para identificar vulnerabilidades con el objetivo de defenderlos de posibles ataques. De acuerdo con Jara . H, (2012), para realizar la práctica del hacking ético, el analista o auditor está al tanto de las pruebas que se realizarán donde se informará al personal con anticipación, pero desconoce el propósito para el cual está auditando. Están involucradas las siguientes fases de la piratería ética: recopilación de información, listado, análisis de vulnerabilidad, explotación y post-explotación.

Caja Negra. Benchimol. D. (2010), describió a este tipo de prueba como una "prueba intrusiva " donde el objetivo es acceder a un objetivo específico con privilegios mientras el equipo de seguridad de la organización no está informado, lo que reduce la capacidad de respuesta ante incidentes de seguridad.

Tándem. Esta prueba está destinada a evaluar los diversos controles de seguridad que están disponibles entre el auditor y el administrador. La verdadera naturaleza de la prueba es la minuciosidad de la observación del analista (Emiliani & R. Sierra, 2015). La protección de los controles que se encuentran en el momento de la auditoría de la información se prueba mediante un tipo de auditoría de esta naturaleza.

2.3.2.2. OWASP

La organización que desarrolla la metodología asociada a Open Web Application Security Project o, como se le conoce en español, Proyecto Abierto de Seguridad en Aplicaciones Web, se conoce con el nombre de OWASP.

La metodología tiene el mismo nombre que el proyecto ya que la auditoría de seguridad en aplicaciones web el cual su objetivo principal. El objetivo del método es hacer posible realizar una auditoría exhaustiva de una aplicación web (Foundation, 2020). Explicaremos los pasos y cómo se deben realizar.

Para aplicar la auditoría de la aplicación web, las pruebas se dividen en las siguientes categorías representada en el Figura 4:

Figura 4
cuadro de OWASP

Nota: Auditoría de Seguridad Web OWASP.
Fuente: https://www.tithink.com/es/2018/03/27/metodologia_owasp/

2.3.2.3. PTES

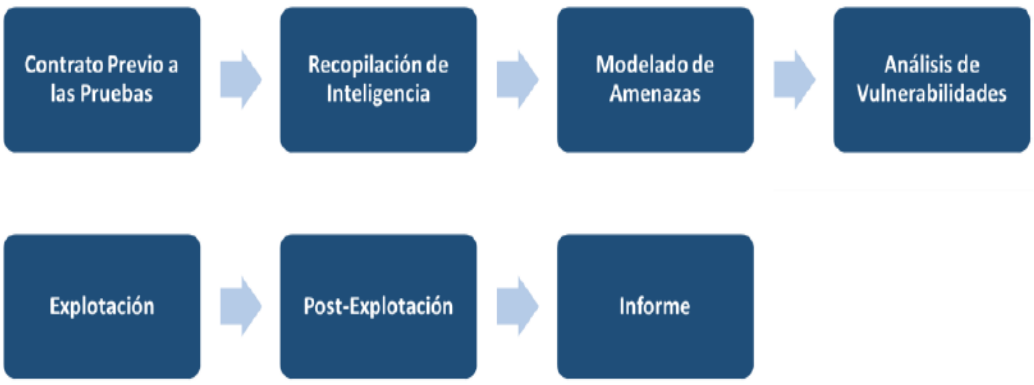
La Metodología PTES es el único proyecto que lleva a cabo su organización. La organización que comparte el mismo nombre que la metodología está formada por reconocidos expertos en el campo de la seguridad informática.

Los términos son equivalentes a Penetration Testing Execution Standard, o Estándar de Ejecución de Pruebas de Intrusión en español. El objetivo principal de esta metodología es llevar a cabo un procedimiento de pruebas de intrusión que cubra todo el proceso de principio a fin. Comenzando por establecer acuerdos y autorizaciones previas a las

pruebas que se realicen y al finalizar detallar cómo se debe elaborar el informe (Pentest Standard, 2016).

Las etapas de esta metodología son las siguientes que se representan en la figura 5:

Figura 5
Fases de la metodología PTES



Nota: Figura de muestra de la secuencia de la metodología PTES.
Fuente: http://www.pentest-standard.org/

2.3.3. Análisis comparativo de las metodologías OSSTMM, OWASP y PTES.

Las metodologías han sido comparadas en base a una serie de variables. la primera es la variedad de campos en los que se utiliza la metodología. Todas ellas abarban el ámbito digital de la seguridad Informática. Pero solo una de ellas cubre el ámbito físico, y la mitad de ellos cubre la ingeniería social.

El siguiente aspecto significativo por el cual se puede comparar una metodología es si tiene un manual técnico que describa cómo llevar a cabo las pruebas que requiere la metodología. Solo PTES y OWASP tienen pautas de prueba.

Es fundamental utilizar algún tipo de métrica al realizar las pruebas para poder evaluar el estado de seguridad de la informática de la organización; sin embargo, solo OSSTMM tiene capacidades métricas para realizar estas prácticas.

Una vez finalizada la auditoría, la parte del informe se vuelve igual de importante, si no más, porque no importa qué tan bien hecha haya sido la auditoría, no será posible transmitir la información al cliente de la manera adecuada si no se realiza correctamente la documentación. se evidencia que la metodología (OWASP) no determina sobre cómo deben redactarse los informes.

Con base a lo expuesto, las metodologías detalladas anteriormente se comparan en función de los factores de su aplicabilidad, siendo estos mismos que se detallan a continuación:

- **Factor Digital.** evalúa el factor digital de la seguridad informática.
- **Factor Físico.** Admite la valoración de la seguridad física de las instalaciones de la organización a auditarse.
- **Factor social**. Evalúa el complejo ámbito de ingeniera social.
- **Métricas. Evalúa**. mediante métricas la seguridad informática actual que presenta una organización.
- **Informes**. Al Culminar el proceso de auditoría es obligatorio la elaboración de un informe estructurado y parametrizado.
- **Guía técnica**. Permite seguir sistemáticamente los lineamientos necesarios para ejecutar la auditoría en una organización.

2.3.4. Criterios de selección para identificar las metodologías de auditoria.

Desde la perspectiva de López Santoyo (2015) se establece el siguiente cuadro comparativo para el análisis de cada una de las metodologías, en esta evaluación de metodologías se toman los siguientes aspectos de la seguridad de la información. ámbito digital, ámbito físico, ámbito social, guía técnica, métricas, informes, gestión de proyectos como se muestra en la tabla 2.

Tabla 2
Análisis comparativo de las metodologías de seguridad informática.

	OSSTMM	PTES	OWASP
AMBITO DIGITAL	cumple	cumple	cumple
AMBITO FISICO	cumple		
AMBITO SOCIAL	cumple		
GUIA TECNICA		cumple	cumple
METRICAS	cumple		
INFORMES	cumple	cumple	
GESTION DE PROYECTOS		cumple	

Nota: en esta tabla se muestra la comparación de las metodologías escogidas
Fuente: (López Santoyo, 2015).

2.3.5. Metodología Seleccionada.

Podemos determinar que la metodología OSSTMM la cual se eligió para llevar a cabo la aplicación de la guía. Consecutivamente se revelarán los beneficios y los inconvenientes que contribuyeron a la elección.

2.3.6. ¿Por qué la metodología OSSTMM ha sido elegida?

Con la tabla de comparación del capítulo anterior como guía, está claro que PTES y OSSTMM son las dos metodologías más completas.

El único sistema que cubre todas las áreas es OSSTMM, por lo que es la única forma de lograr el objetivo de realizar un análisis exhaustivo de todos los aspectos de la seguridad de la organización .Sin embargo , también incluye métricas y explica cómo completar los informes .Lo que falta es la fase de gestión del proyecto , que incluye la fase de acuerdo previo y la presentación de resultados .Como ya dijimos , esta es una tarea que no se ajusta al rol del analista , por lo que no es del todo mala .Si bien carece de una guía técnica sobre cómo realizar las pruebas que sugiere , ese es precisamente el objetivo del presente trabajo, algo que también falta en la literatura.

La metodología PTES, por otro lado, solo cubre la esfera digital en su aplicación, dejando poco espacio para un análisis de seguridad informática exhaustiva. No hay métricas disponibles para estimar el nivel de seguridad.

Estas conclusiones llevan a determinar que OSSTMM es el más adecuado. Los beneficios y desventajas de esta metodología.

2.4. Fases de la Metodología OSSTMM.

Cada fase de la metodología OSSTMM se alinea con las fases de Hacking Ético como el tipo de herramienta para el desarrollo de este estudio. Esta metodología tiene las siguientes fases.

2.4.1. Fase de Inducción.

El objetivo de esta fase es la recopilación de datos, incluida la cultura organizacional, las reglas, las normas y las políticas Internas son las que permiten establecer las limitaciones que auditor solicita. En esta fase de la metodología OSSTMM se aplica junto con la fase de recopilación de información, durante la cual utilizaremos herramientas de hacking ético, lo que da como resultado en:

- Se revisó el entorno de la empresa objeto de estudio, del sector metalmecánico de Manabí, su cultura organizacional y las políticas de seguridad de la información vigentes.
- El estudio de los detalles humanos incluyó la determinación de los tiempos en que el personal de TI está en el trabajo o activo dentro de la empresa.
- Se creó un listado de verificación en la que se determinó si se tenían controles para mitigar los ataques contra la seguridad de la información.

2.4.2. Fase Interacción.

En esta fase de las pruebas de seguridad de la información, se determina el alcance de las interacciones entre las actividades relacionadas con la información y las posibles

infracciones de seguridad. También se examina el acceso a aplicaciones y sistemas, así como los controles establecidos para los mismos.

- Se comprobó la visibilidad de los posibles objetivos de los ataques de seguridad.
- Se examinaron los puntos de acceso de la empresa del sector metalmecánico de Manabí en estudio, realizando un escaneo de los puertos abiertos.
- Se verificaron los controles que se utilizan para asegurar la confidencialidad, integridad y disponibilidad de la información.

2.4.3. Fase Investigación.

En la fase de investigación o descubrimiento, se realizan pruebas para determinar las fortalezas y debilidades del sistema de información de la organización. Los resultados permiten identificar las debilidades y fortalezas del sistema de información probado y apoyan el descubrimiento de la evidencia.

En esta fase se llevan a cabo muchas tareas, como comprobar interacciones entre procesos y exposiciones, así como analizar la información que se va descubriendo, también se evidencian las actividades del manejo de la información mal situadas o gestionadas. Además, se buscó información a la que se podía acceder libremente a través de los motores de búsqueda utilizando técnicas de hacking ético de Google para confirmar que no existían restricciones de red sobre ninguna información pertinente.

2.4.4. Fase Intervención.

Esta fase implica evaluar la efectividad de los controles, mapear el daño potencial de su uso inapropiado y revisar el proceso de auditoría para ver si se produjo un resultado confiable.

En esta fase el auditor se centra en los recursos necesarios para lograr los objetivos en la fase intermedia, que es la última etapa, estos recursos pueden intercambiarse, cambiarse, sobrecargarse o eliminarse como resultado de la penetración o interrupción del sistema.

- Con el cálculo del RAVs se revela la seguridad operativa de la empresa en estudio.
- Se desarrollan estrategias para disminuir las restricciones y fortalecer los controles.
- En esta etapa de la metodología OSSTMM se cuantifican los resultados obtenidos.

2.5. Estructura de OSSTMM.

El Manual Abierto de la Metodología para Seguridad OSSTMM, proporciona una hoja de ruta para realizar exámenes o auditorías para la seguridad Informática. esta metodología puede ser utilizada considerando estándares y normativas aplicadas a nivel mundial, la versión 3.0 de la metodología es ahora la versión vigente.

Basándonos en lo publicado por Navia, (2021) la metodología busca a cuantificar seguridad informática usando métricas cuantitativas. esta divide el área a ser examinada (“la seguridad operacional" u OpSec) en canales, cual son agrupado en tres clases como

se muestra en la tabla# en la misma que se menciona a breve rasgos los cinco canales que se toman en consideración por la metodología OSSTMM como se detalla en la tabla 3.

Tabla 3
Canales definidos en OSSTMM

Clase	Canal	Breve descripción
Seguridad Física (PHYSSEC)	Humano (HUMSEC)	comprende el factor humano de la comunicación.
	Físico	comprende los elementos tangibles, no electrónicos. Por lo general se lo toma como lo que es sí PHYSSEC.
Seguridad de espectro (SPECSEC)	Inalámbrico	comprende las comunicaciones mediante ondas electromagnéticas.
Seguridad de Comunicaciones (COMSEC)	Telecomunicaciones	muestra las redes de telecomunicaciones sobre líneas telefónicas.
	Redes de datos	conjuga los sistemas electrónicos y cableado que constituyen las redes de datos.

Nota: Estructura de OSSTMM

Las operaciones, Controles, y Limitaciones son los tres grupos de criterios usado a evaluar cada uno canal. Cada grupo entiende una porción de la operación y seguridad de un sistema o infraestructura, asi como una parte de sus defectos. Estos criterios y su forma de relación, son mostrado en Figura 6.

Figura 6
Mapeo de los criterios de Operación y Control con los de Limitaciones

Category		OpSec	Limitations
Operations		Visibility	Exposure
		Access	Vulnerability
		Trust	
Controls	Class A - Interactive	Authentication	Weakness
		Indemnification	
		Resilience	
		Subjugation	
		Continuity	
	Class B - Process	Non-Repudiation	Concern
		Confidentiality	
		Privacy	
		Integrity	
		Alarm	
			Anomalies

Nota: criterios de Operación y Control con los de Limitaciones
Fuente: http://revistas.utm.edu.ec/index.php/informaticaysistemas

los criterios mostrados en Figura 1 permitir para el cálculo de la RAV (Riesgo Evaluación Valor, Valor de Evaluación de Riesgos), cual es una escala para medición un potencial ataque superficie y es calculado como un cuantitativo saldo entre operaciones, controles, y limitaciones. los óptimo RAV valor debería ser cerca de 100%; un valor abajo esto indica seguridad defectos, y un valor arriba esto indica eso allí son más seguridad controles que son necesario.

CAPITULO III: RESULTADOS Y DISCUSIÓN

3.1. RESULTADOS

Tomando en consideración la metodología sugerida para este estudio, se realizaron procedimientos específicos que arrojaron resultados concluyentes en este estudio.

El principal problema con la recopilación de datos fue que se llevó a cabo de forma automática y en línea para garantizar la confidencialidad de la fuente de información. Debido a la situación anterior, las (9) empresas procedieron a llenar la información para su posterior análisis.

Si tomamos en cuenta los resultados de las herramientas utilizadas, podemos decir que los usuarios encuestados conocen que las empresas que conforman parte del sector metalmecánico de Manabí, donde se efectuaron estos procesos que cuenta con políticas de seguridad de la información, pero todos mencionan que la institución no les ha hecho conocer estas políticas y no se las ha proporcionado con capacitación para mantener la información segura.

3.1.1. Resultados del levantamiento de información vía encuesta.

mediante le proceso de levantamiento de la información él cual se realizó mediante aplicación de la encuesta al personal del departamento de tecnología, logrando definir las directrices necesarias para el avance de la investigación, a continuación, se muestran las preguntas que se realizaran en la encuesta.

1. **¿Las empresas del sector metalmecánico tiene políticas de seguridad de la información?**

   si ☐ no ☐

2. **¿Por qué medios se han socializado las políticas de seguridad de la información**?

   si ☐ no ☐

3. **¿Cuenta la institución con los mecanismos que se utilizan en para evaluar el cumplimiento de las políticas de seguridad de la información?**

   si ☐ no ☐

4. **¿En la empresa se ha socializado las políticas de seguridad de la información con el resto del personal?**

   si ☐ no ☐

5. **¿los problemas más frecuentes que se presentan con respecto a la seguridad de la información se producen generan de forma interna?**

   si ☐ no ☐

6. **¿los usuarios cuando tienen dificultad en el envío de información acuden a ustedes?**

   si ☐ no ☐

7. **¿las recomendaciones que Ud. da al personal al compartir información son tomadas en consideración?**

   si ☐ no ☐

8. **Dentro de la empresa se utiliza el correo institucional, personal para compartir información sea segura y no exista fugas y no sea utilizada por terceros.**

   si ☐ no ☐

3.1.2. Tabulación de los resultados de la encuesta.

Se destacan los siguientes resultados de la encuesta realizada tabulando el porcentaje de obtenido en cada una de las preguntas. El mismo que demuestra en la tabla 4.

Tabla 4
Tabulación de resultados de la encuesta realizada al personar de TI

	Preguntas	Resultados	Análisis
1	¿Conoce usted sobre políticas de seguridad de la información digital?	no 35% si 65%	Más de la mitad de los usuarios manifiestan tener conocimientos de las políticas de seguridad digital sin embargo no en su totalidad
2	¿Tiene conocimiento de las políticas de seguridad de la información?	no 40% si 60%	Más de la mitad de los usuarios que se aplicó la encuesta manifiestan conocer sobre las políticas de seguridad de la información
3	¿Conoce usted si la empresa tiene establecidas políticas de seguridad para el manejo de información digital?	no 60% si 40%	La mayoría de usuarios de la institución desconocen que se establece políticas de seguridad para el manejo de la información
4	¿En la empresa se ha socializado las políticas de seguridad de la información con el resto del personal?	no 60% si 40%	En su totalidad (60%) del personal encuestado que menciona no conoce las políticas de la institución con un (40%) de personal que si las conoce
5	¿Cuáles son los problemas más frecuentes que se presentan con respecto a la seguridad de la información y porque se producen?	no 90% si 10%	en su mayoría los usuarios coinciden que la falta de capacitación de como tener una información segura
6	¿Cuándo los usuarios tienen dificultad del envío de información acuden a ustedes?	no 95% si 5%	La mayor parte de los usuarios de las empresas mencionan que comparten la información por medio de correo institucional y correo personal casi la mitad utilizan grupos de trabajo en medios tradicionales
7	¿Cuáles son las recomendaciones que Ud. da al personal al compartir información ésta sea segura?	no 85% si 15%	La mayor parte de los usuarios desconocen que re realice un monitoreo de políticas, con un mínimo que si conocen que exista este control
8	Dentro de la empresa se utiliza el correo institucional, personal y grupos de trabajo a su criterio cual sería el más recomendable para compartir información sea segura y no exista fugas y no sea utilizada por terceros.	no 45% si 55%	La mayoría de los usuarios encuestados mencionan tomar precauciones cuando comparten información con otras personas

Nota**:** resultados obtenidos mediante la revisión de la encuesta realizada.

3.1.3. Resultados de la revisión bibliográfica.

La diferencia entre los autores que han abordado los temas que se tratan en la investigación donde se clasifica cada uno de los tipos de revisiones desde el punto vista tradicional.

Tabla 5
Clasificaciones de las revisiones bibliográficas

	Emiliani & R. Sierra. (2015)	Maya y Jaramillo, D. (2015).	Muñoz Enrique, F. I. (2018).	Muñoz Enrique, F. I. (2018).
Revisión tradicional o narrativa	cumple			
Revisión de la literatura		cumple	cumple	cumple
Revisión Sistemática	cumple	cumple	cumple	cumple
Revisión sistemática de la literatura				
meta análisis	cumple	cumple	cumple	cumple
revisión panorámica		cumple		
revisión de estudios mixtos		cumple		
revisión de mapeo sistemática		cumple		
revisión rápida			cumple	

Nota**:** resultados obtenidos mediante la revisión bibliográfica de varios autores.

3.2. Análisis de los resultados en fases

En los siguientes resultados de la auditoría de seguridad de la información realizada con la metodología OSSTMM se evidenciará cada una de sus faces en ejecución.

3.3. Fase de Inducción – Recolección de información

Las siguientes tabulaciones muestran los resultados obtenidos de las encuestas realizadas al personal administrativo de la empresa metalmecánica las cuales permitieron definir la factibilidad y viabilidad del proyecto, lo que se puede ver de forma detallada en la tabla 4.

Entorno Organizacional

- En el área de informática que forma parte de las empresas del sector metalmecánico de Manabí, se establecen y ponen en práctica políticas básicas de seguridad de la información. Los ejemplos incluyen listas de filtros de contenido de intranet, firewalls perimetrales, controles de acceso a repositorios externos y controles de acceso lógico.
- Debido a que no existen políticas implementadas para brindar protección tanto a la información como a la energía eléctrica, los planes de continuidad no se pueden definir de manera efectiva.
- La seguridad operativa de la organización no está adecuadamente respaldada por IPS, IDS o antivirus con licencia para la detección de amenazas potenciales.

3.4. Fase Interacción – Scanning y enumeración

En esta fase, se realizarán pruebas de interacción que incluyen tres técnicas y se utilizarán herramientas especializadas como NMAP, NESSUS, SCAN, y ETTERCAP para recopilar información sobre la cantidad de dispositivos conectados en general Veremos la justificación del uso de estas herramientas especializadas más adelante.

Aplicación de la Herramienta Especializada NESSUS:

Presentamos en primer lugar los resultados relacionados con la técnica de prueba de penetración en la que hemos utilizado la herramienta NESSUS ya que sirve para la detección de vulnerabilidades, más que todo porque efectúa un análisis a las vulnerabilidades de alto grado.

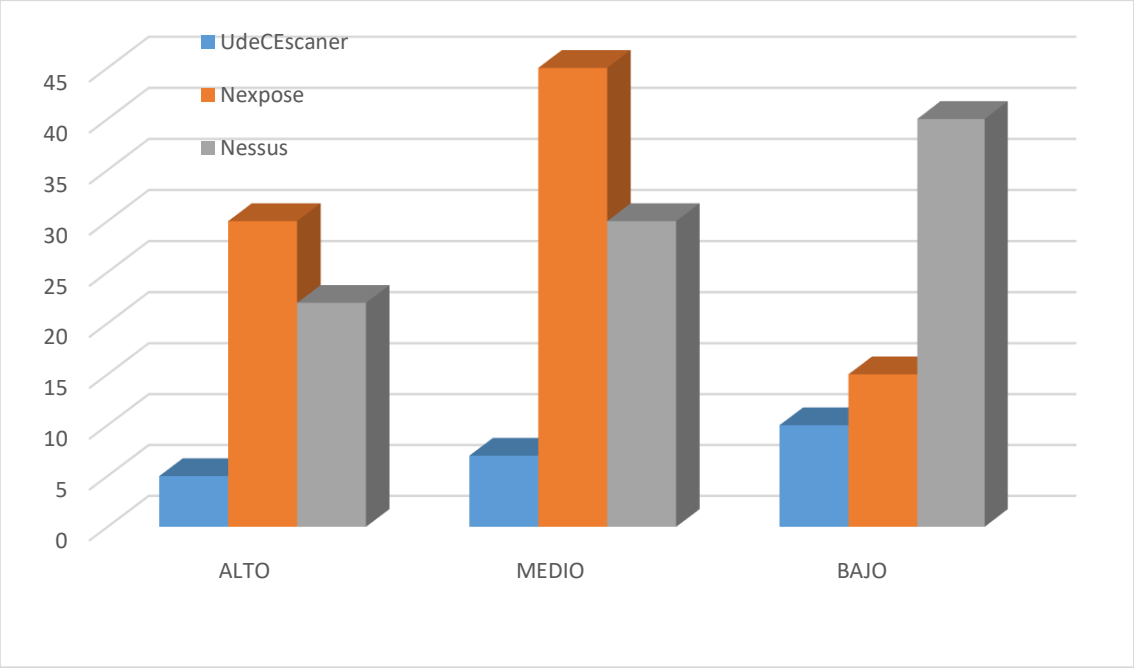
Justificación: Según David A. Franco (2013), el uso de la herramienta para auditoria informática en los laboratorios de pruebas de penetración (NESSUS, NEXPOSE y SCANER). Genera la creación de un mapa entre los niveles de seguridad el cual revela cada herramienta con una escala definida para poder comparar las herramientas, como se ve en las Tablas 6 y 7.

Tabla 6
Mapeo entre las escalas de severidad utilizada por las herramientas de evaluación

UdeCEscanner	Nexpose	Nessus	Nueva escala
Alto	Critico	Crítico, Alto	Alto
Medio	´Severo	Medio	Medio
Bajo	Moderado	Bajo, Info	Bajo

Nota: escala definida por los autores.

Tabla 7
Resultados para un laboratorio de pruebas de penetración



Notas: Resultados obtenidos en las pruebas de aplicaciones para auditoria informática

Como se observa en la Tabla 6, la herramienta que identificó más vulnerabilidades fue NESSUS, seguida de NEXPOSE y UDECESCANER. Debido a esto, en comparación con otras herramientas, la herramienta UDECESCANER presentó una cantidad muy pequeña de vulnerabilidades. Como se mencionó anteriormente, NESSUS descubrió vulnerabilidades de alta gravedad, que afectan principalmente a los servicios OpenSSH y servidores Apache debido al consumo de memoria y problemas de seguridad en la ejecución remota de código.

Las características de las herramientas de detección de vulnerabilidades se detallan en una comparación como se observa en la Tabla 8.

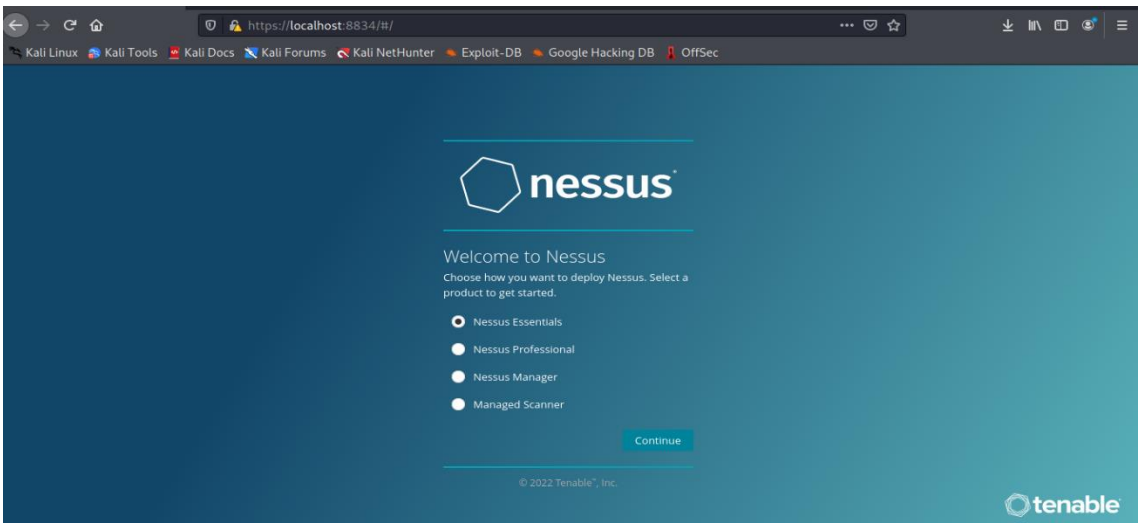
Tabla 8
Comparación de las herramientas y sus características para la detección de vulnerabilidades

Herramientas/Parámetros	**UdeCEscaner**	**Nexpose**	**Nessus**
Facilidad de uso	Alta	Alta	Alta
Requerimiento del sistema	Bajo	Alto	Medio
Facilidad de instalación	Simple	Compleja	Media
Interfaz amigable	Alto	Alto	Alto
Complejidad	Baja	Alto	Alto
Numero de Vulnerabilidades detectadas	80	195	305
Legibilidad del reporte final	Alta	Alta	Alta
Contenido del reporte	Medio	Alta	Medio
Velocidad de detecciones	Alta	Baja	Medio

Nota: Se muestra la comparación entre las características de las herramientas en estudio.

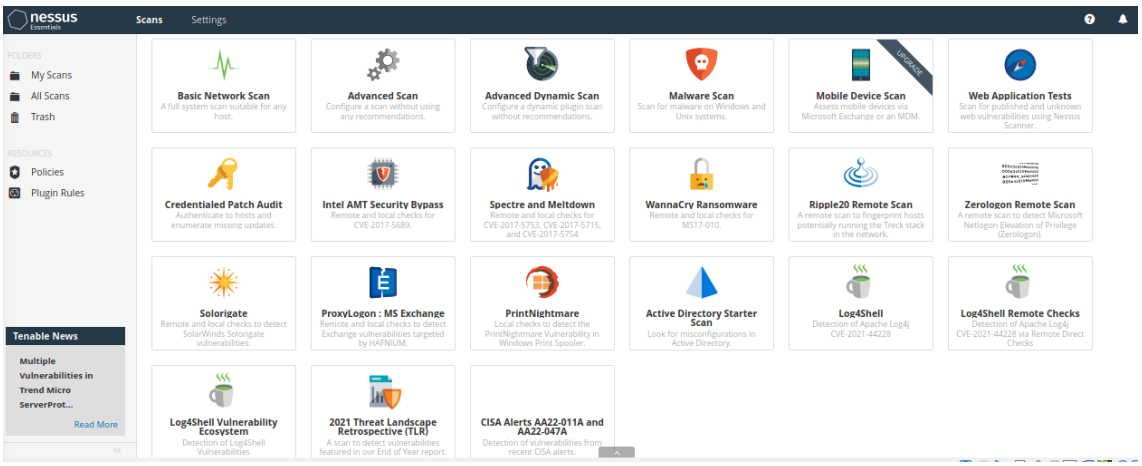
Hurtado & Mendao (2016) mencionan, que el uso de la herramienta NESSUS para ofrecer un reporte general a nivel de red o segmento de red, es una de las más completas ya que revisa las vulnerabilidades en cada capa del modelo OSI. Empecemos el proceso para la instalación en equipo auditor, como se puede ver en la figura 7.

Figura 7
Proceso Instalación y puesta en marcha de Nessus



Nota: Visualización de inicio de la herramienta Nessus.
Fuente: Elaborada en el proceso de instalación

Figura 8
Visualización de la herramienta de Nessus.



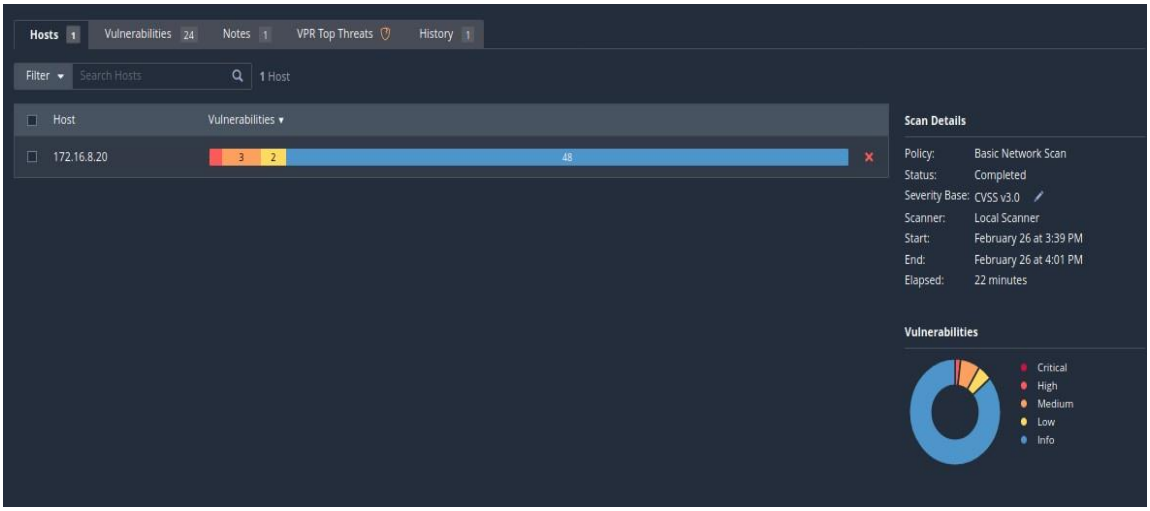
Nota: Visualización de inicio de la herramienta Nessus.
Fuente: Elaborada en el proceso de puesta en escena de la aplicación Nessus

Como se plantea en la presente investigación, se utilizará la herramienta NESSUS porque, a diferencia de otras herramientas, ofrece soluciones y es la que se utiliza con mayor frecuencia para detectar vulnerabilidades, configurar sistemas y garantizar la compatibilidad. Es por ello que este herramienta está siendo utilizada para evaluar las vulnerabilidades en la red de datos de las empresas Metalmecánica de Manabi.

los resultados del escaneo pueden ser visualizados como informes en varios formatos, Los resultados también pueden ser guardados en una base de conocimiento para referencia en futuros escaneo de vulnerabilidades.

Las pruebas de vulnerabilidad de Nessus se realizaron para determinar si podrían provocar que los servicios o los sistemas operativos se degradaran y fallaran. (pruebas no seguras) antes de escanear.

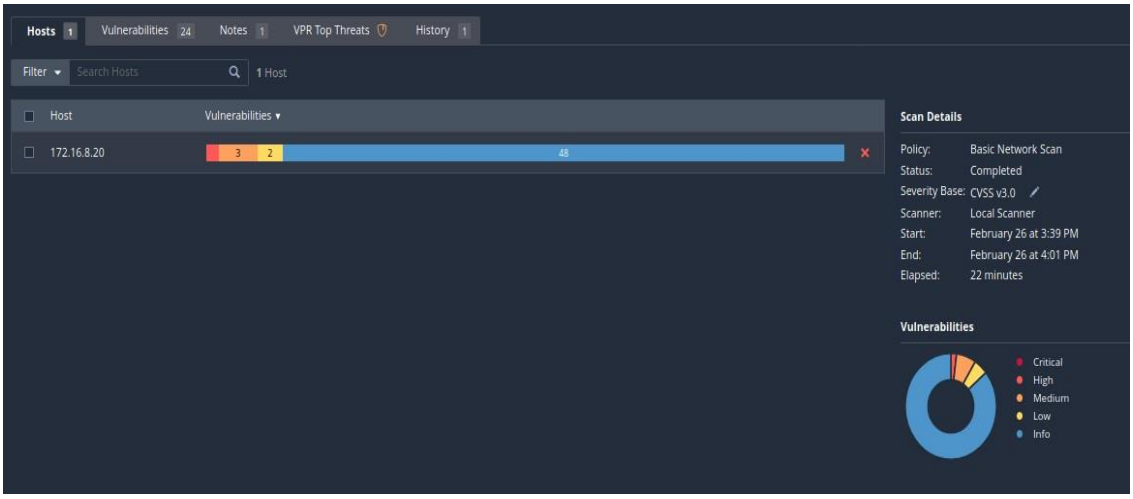
Figura 9
Resultados de escaneo en Nessus prueba 1



Nota: reporte de Nessus
Fuente: elaboración propia

Los resultados del escaneo se pueden ver en las Figuras 9 y 10 y se pueden exportar en una variedad de formatos. También se pueden guardar en una base de conocimiento para futuras exploraciones de vulnerabilidades. Las pruebas de vulnerabilidad realizadas en Nessus se efectuaron porque pueden inducir al deterioro y fallo de los sistemas operativos o servicios. (pruebas inciertas) antes de escanear.

Figura 10
Resultados de escaneo en Nessus prueba 2



Nota: reporte de Nessus
Fuente: elaboración propia

Uso de Herramienta Especializada NMAP:

En segundo lugar, se presentan los resultados relacionados con la técnica de prueba pasiva. Para esta técnica, usamos la herramienta NMAP porque es útil para escanear redes y verificar dispositivos remotos que ejecutan servicios. También podemos identificar procesos activos, sistemas operativos, la presencia de filtros o cortafuegos, entre otras cosas.

Justificación: Según Narváez Portillo (2015), se justifica el uso de las siguientes herramientas: NMAP, METASPLOIT, AIRCRACK.NG, BURPSUITE, HYDRA y WIRESHARK. En este resumen se menciona la herramienta NMAP la cual estaremos utilizando en esta investigación, junto con una descripción de su función, características, prueba objetivo y resultados obtenidos.

HERRAMIENTA AIRERACK-NG.

OBJETIVO

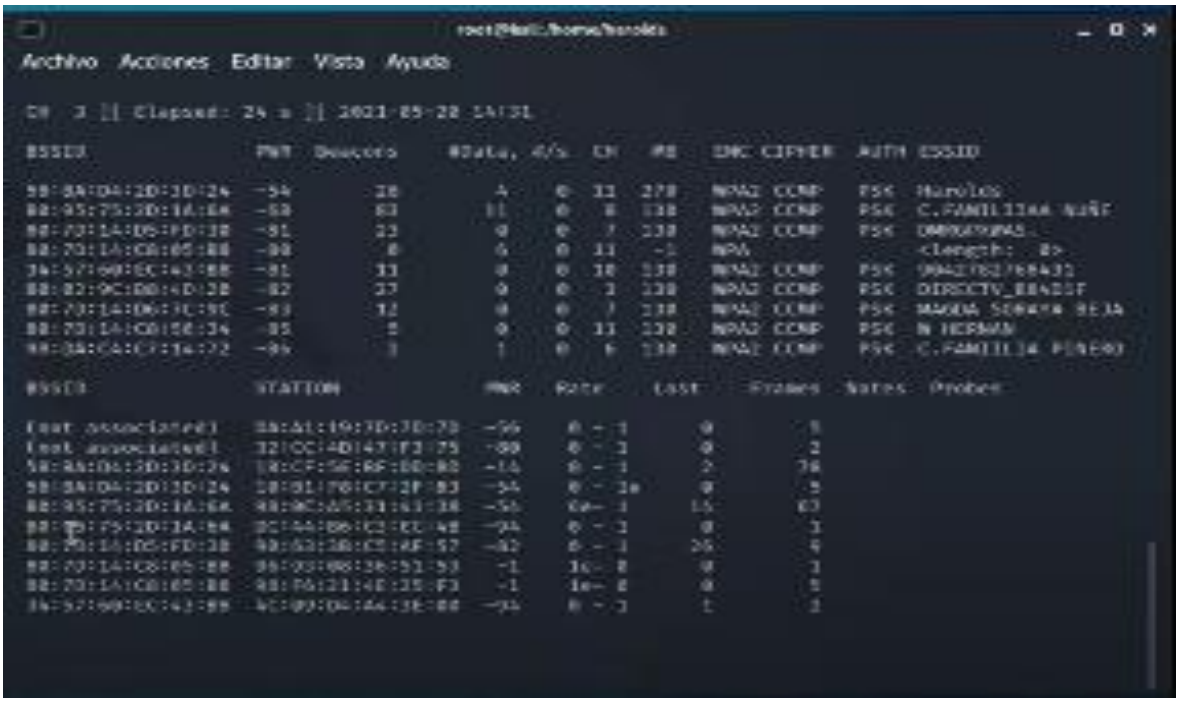
Probar el conjunto de herramientas Airerack-ng mediante su empleo en la tarea de descifrar la clave de la red inalámbrica WLAN: SSID-INDUMA

RESULTADOS

Se detectan las características de la red WLAN-SSID-INDUMA como: dirección MAC, canal por el cual transmite de la red, tipo de encriptación y tipo de cifrado, así como la actividad de autenticación y des autenticación entre el cliente y el punto de acceso y finalmente en el proceso de combinaciones para descifrarlo de clave con 5799644

registros, sin que la clave sea encontrada se concluye que la misma es fuerte y cumple con los estándares requeridos como visualizamos en la figura 11.

Figura 11
Resultados de herramienta en AIRERACK-NG.



Nota: Resultados de herramienta en AIRERACK-NG.
Fuente: elaboración propia

HERRAMIENTA BURPSUITE

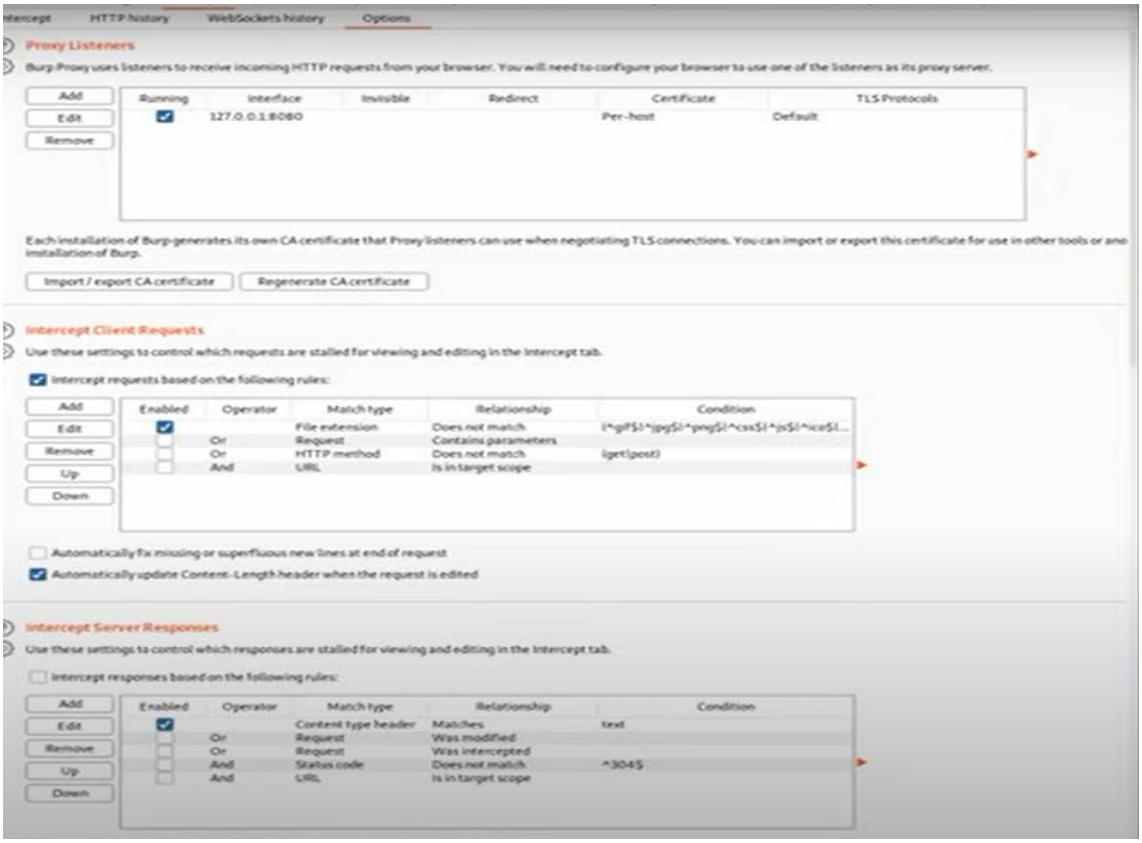
OBJETIVO

Interceptar una búsqueda dirigida a la página web del dominio de la empresa

RESULTADOS

se observa en la figura 12 interacción de la petición de ingreso a la página principal de la organización, así como la captura de la portada del sitio de la organización.

Figura 12
Resultados de herramienta en Burpsuite.



Nota: Resultados de herramienta en Burpsuite.
Fuente: elaboración propia

HERRAMIENTA HYDRA

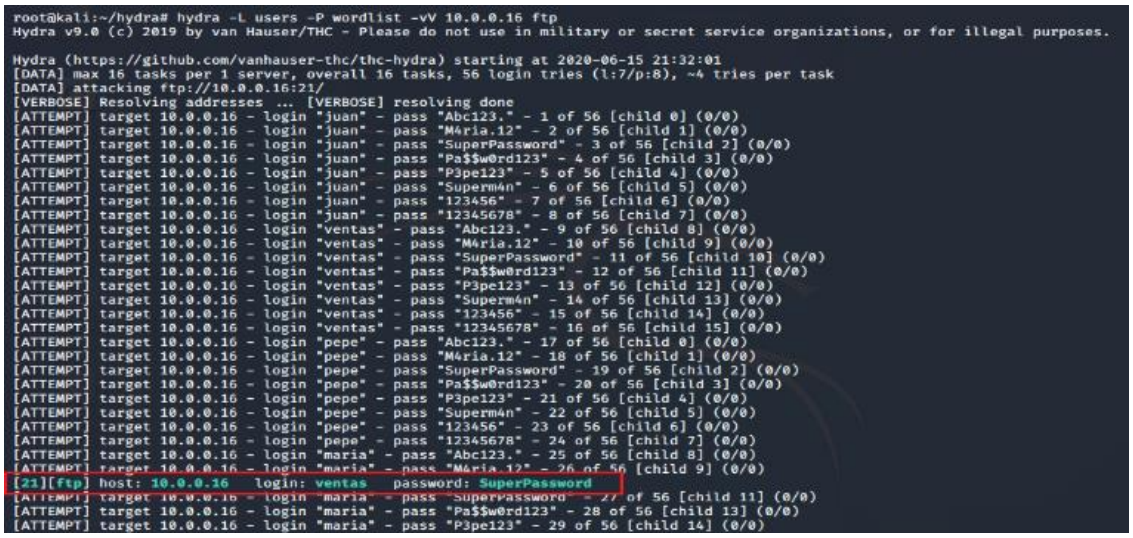
OBJETIVO

Verificar la contraseña de inicio de sesión de un equipo del área administrativa

RESULTADOS

Se obtiene tres opciones validas de para vulnerar contraseña como vemos en la figura 13.

Figura 13
herramienta en Hydra



HERRAMIENTA METASPLOIT

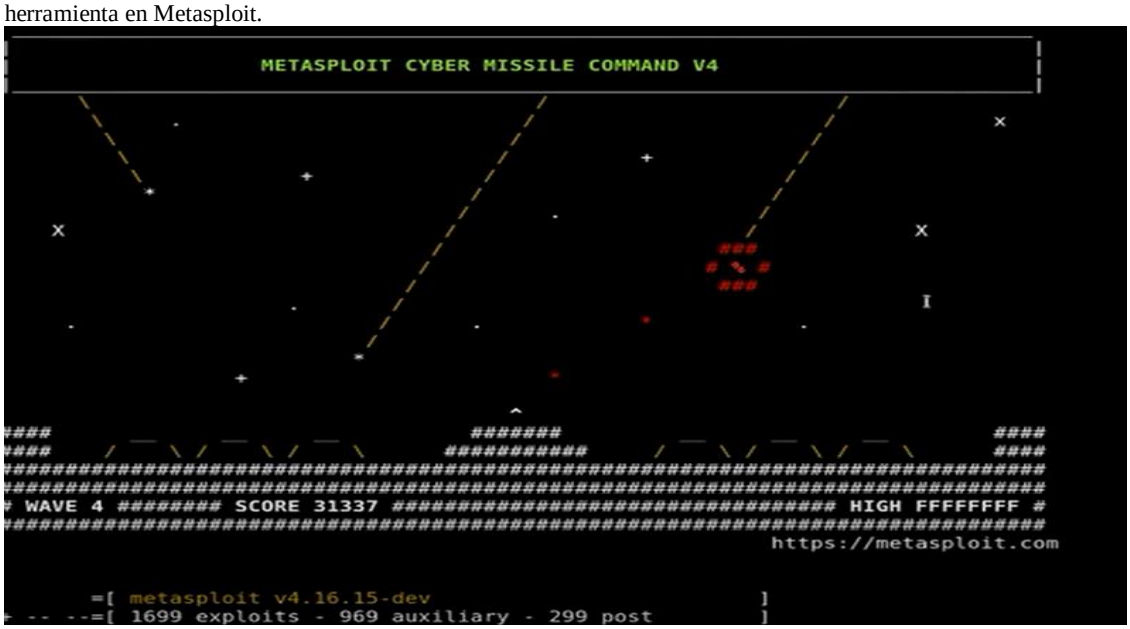
OBJETIVO

Realiza una explotación del sistema operativo Windows 10 de los ordenadores destinados para esta prueba.

RESULTADOS

se encuentran varias vulnerabilidades las cuales presenta con la posibilidad de ejecución remota dentro su sistema operativo potenciando un ataque de mayor alcance, parte de esta interacción la podemos observar en la figura 14.

Figura 14
herramienta en Metasploit.



Nota: Resultados de herramienta Metasploit
Fuente: elaboración propia

HERRAMIENTA WIRESHARK

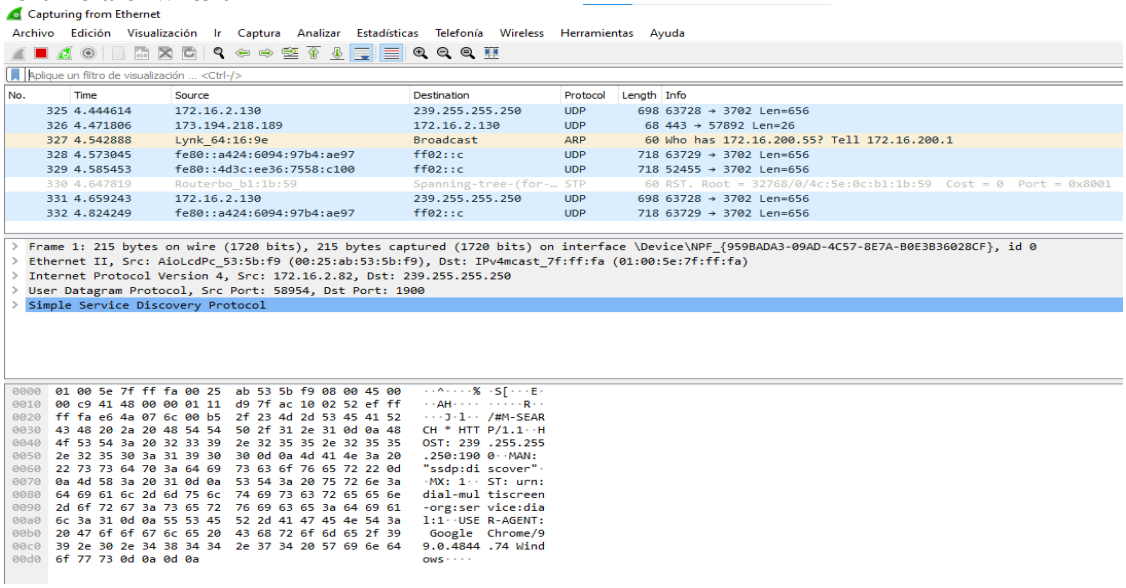
OBJETIVO

Observar el intercambio de paquetes durante un esquema de saludo de tres vías ejecutado entre dos vías.

RESULTADOS

Se observa en la figura 15 el intercambio de paquetes SYN, ACK entre dos direcciones, adicional se podrían descifrar paquetes de datos.

Figura 15
herramienta en Wireshark

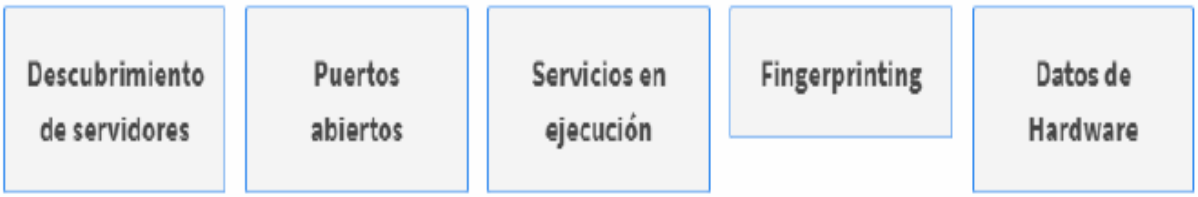


Nota: Resultados de herramienta en Wireshark
Fuente: elaboración propia.

Si bien existen herramientas que han visto un uso extensivo recientemente en la seguridad de la información, NMAP se destaca ya que se usa con frecuencia para el espionaje. Por ejemplo, los administradores de sistemas lo utilizan para encontrar posibles aplicaciones no autorizadas que se ejecutan en una red o servidor, que los intrusos pueden aprovechar y utilizar para encontrar posibles objetivos de ataque.

La herramienta NMAP tiene la característica automatizar procesos que realiza administrador de la red, la misma proporciona los servicios que se mencionar en la figura 16:

Figura 16
Características de la aplicación NMAP



Nota: Proceso en secuencia de la aplicación NMAP
Fuente: https://geekflare.com/es/nmap-vulnerability-scan/

Justificaciones Científicas:

R. Sri & M. Mohan (2020) según argumentan que la identificación de ataques está involucrada en todos los resultados de la comparación de varias herramientas, incluidas NMAP, NETCRAFT, ZENMAP, SPARTA, VIRUS TOTAL e IP TRACKING, y llega a la conclusión de que los ataques cibernéticos como los que se muestran en la Tabla 9 pueden ser posibles.

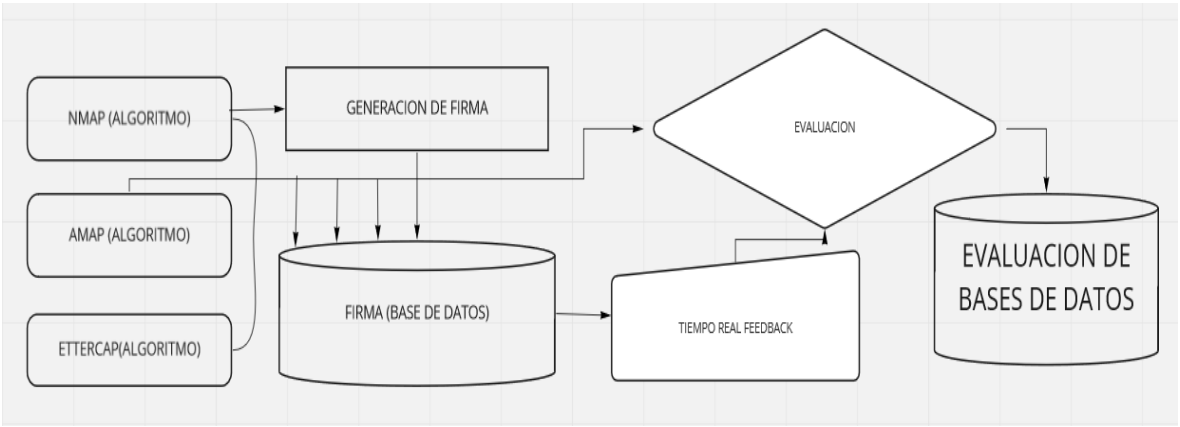
Tabla 9
Resultados de comparación de diferentes herramientas

Herramientas	Ataques
Sparta	rangos de ip EXAMINADOS, es posible un ataque de diccionario
Network Mapper (Nmap)	Encontró la fuente de otros hosts o nuevos ataques
Zenmap	detectar los ataques de phishing
Virus Total	Se pueden insertar diferentes programas maliciosos utilizando estas vulnerabilidades
IP tracking	Ataques DDoS

Nota: Conceptos obtenidos en la investigación.
Fuente: (R. Sri & M. Mohan, 2020)

Según Waheed Ali, Ghanem, & Baharí (2013), Justifica y realiza la comparación de los resultados mediante pruebas exhaustivas contra la precisión de la base de tres herramientas (NMAP, AMAP y ETTERCAP). La comparación involucró analizar la misma base de datos que se muestra en la Figura 17 donde una coincidencia con un algoritmo es los que se busca a través de cada una de sus etapas.

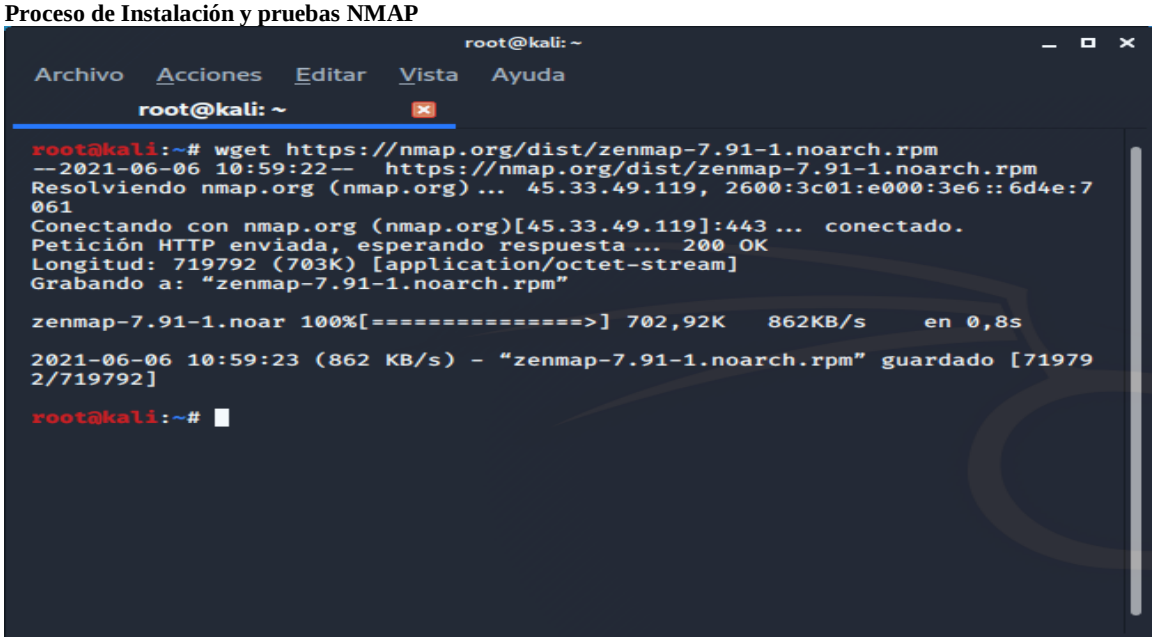
Figura 17
Estructura de la base de datos para evaluación del sistema



Nota: precisión de la base de 3 herramientas NMAP, AMAP, ETTERCAP.
Fuente: (Waheed Ali, Ghanem, & Baharí, 2013)

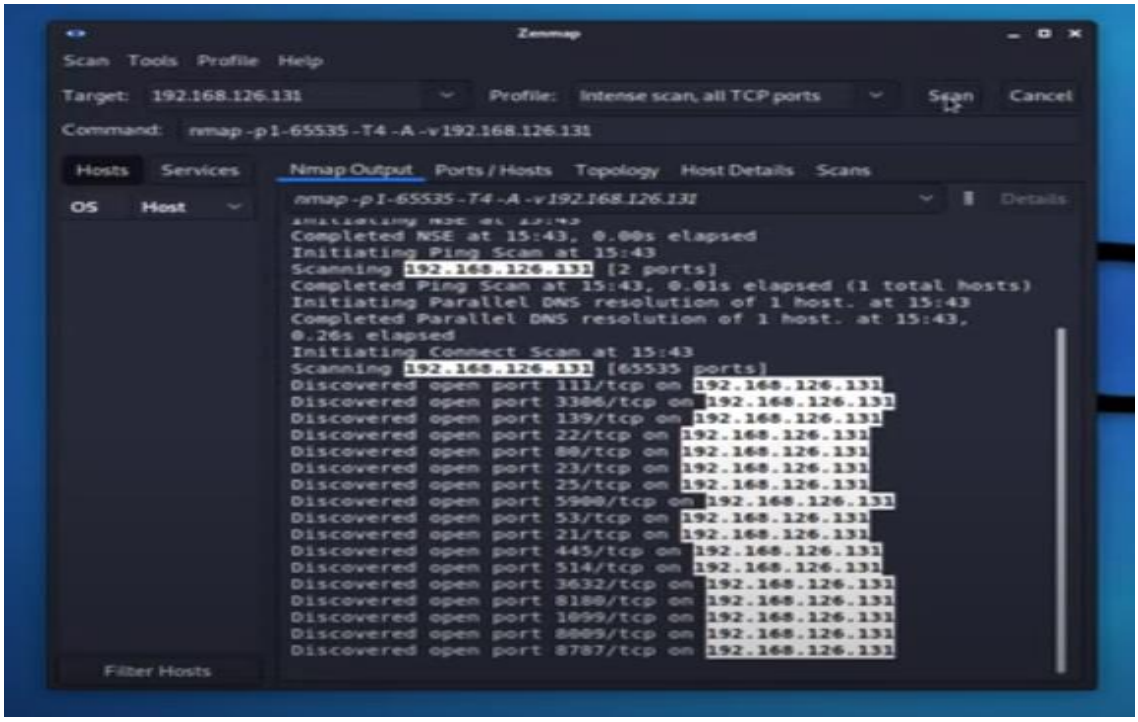
Según Bermeo, (2017) determina que NMAP es una potente herramienta que se utiliza para la detección y escaneo de redes herramienta que es de gran aporte para las auditorias de seguridad, permitiendo equilibrar los servicios que se ejecutan en el dispositivo, así como escaneo de puertos, scripts, redes, y explotando vulnerabilidades, como evidenciamos en la figura 18.

Figura 18
Proceso de Instalación y pruebas NMAP



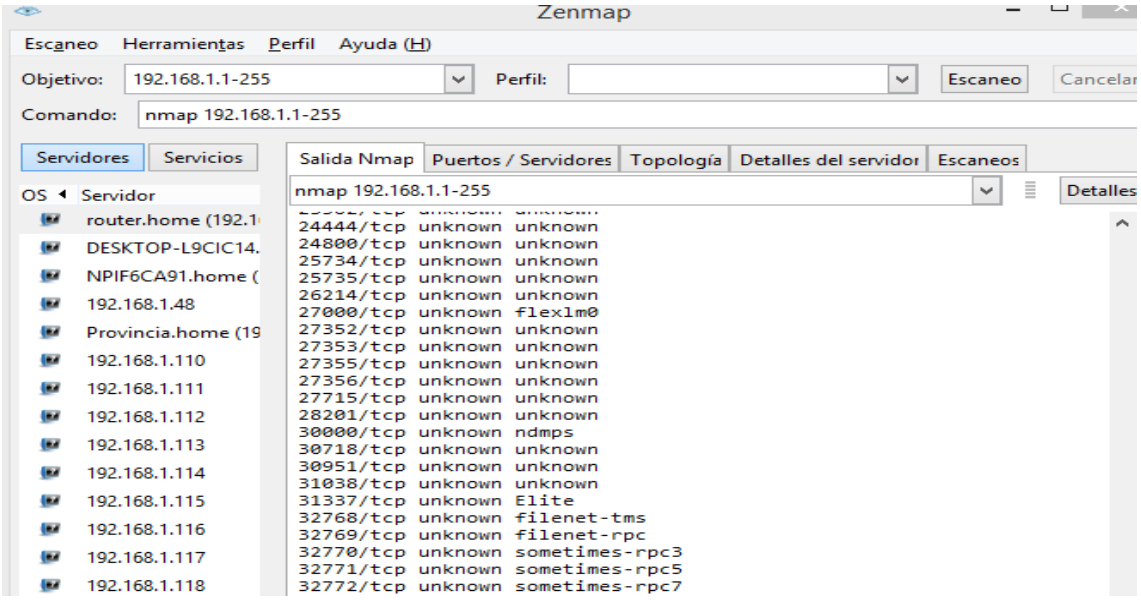
Nota: Instalación en el equipo auditor para Prueba Pasiva
Fuente: Elaboración Propia.

Figura 19
Prueba Pasiva de zenmap



Nota: muestra de la puesta en marcha de la herramienta.
Fuente: Elaboración Propia.

Figura 20
Uso de Herramienta NMAP para escaneo de puertos abiertos



Nota: vista de los puertos abiertos en las aplicaciones en red auditada
Fuente: Reporte Sistema.

Como se indicó en la investigación actual, se utilizará la herramienta NMAP. Esta herramienta se utiliza para escanear y permite evaluar los servicios que se están ejecutando de forma remota, identificar dispositivos activos, sistemas operativos, filtros o firewalls, entre otras cosas. Por ello, esta herramienta se utilizará para evaluar las vulnerabilidades en la red de datos de la empresa metalmecánica.

Uso de Herramienta Especializada ETTERCAP

En tercer lugar, discutiremos los resultados de la técnica de prueba Fuzztesting. Para esto, usamos la herramienta ETTERCAP, que es útil para ataques de intermediarios porque tiene un monitor de actividad de conexión, capacidades de filtrado de contenido y muchas otras características interesantes. Además, permite el protocolo activo y pasivo y la disección característica para analizar redes y hosts.

Justificación: Según Coteron Tene (2012). La justificación para el uso de las herramientas de hacking etixco CAIN & ABEL, ETTERCAP, TPCDUMP, WIRESHARK y CAPSA fue proporcionada por el hecho de que las alternativas fueron evaluadas en base a las propiedades de las herramientas utilizadas en este estudio, las cuales se muestran en la Tabla 10.

Tabla 10
Resultados en escala utilizando las herramientas ettercap

CRITERIO (b,d,g,i)	
ESCALA	INTERPRETACION
1	Malo
2	Regular
3	Buena
4	Muy Buena
5	Excelente

Nota: se muestra la escala de la herramienta para realizar la detección de vulnerabilidades
Fuente: (Coteron Tene, 2012)

Los resultados de los valores de esta investigación se muestran en la Tabla 10. Donde mostramos la escala para la identificación de vulnerabilidades en los hosts elegidos, para este proceso se requiere el uso de cualquiera de las tres herramientas (ETTERCAP, CAN & ABEL y WIRESHARK).

Justificación Científica: Según Sudhakar, R, & K, (2017), Justifica la utilización de las herramientas ETTERCAP, ARPWATH, WIRESHARK, ARPSPOOF, URLSNARF , NMAP -F y TPCDUMP para realizar un análisis comparativo de estas herramientas para la detección de invasión basada en ARP (protocolo para la resolución de DIRECCIÓN) , como se muestra en Tabla 11 y 12.

Tabla 11
Comandos y herramientas para realizar ataques controlados.

herramientas y comandos	Funciones o Propósitos
Ettercap	Escaneo de la red, ARP spoofing y Sniffing
ARPWATCH	Supervise la actividad de Ethernet (detección)
Wireshark	Sniffing (captura de paquetes)
Arpspoof - i eth0	ARP suplantación de identidad
Urlsnarf -i eth0	Snarfing la url
Namp -F or Nmap	Escaneo de puertos
TCP dump	Escuchar la red

Nota: Muestra de comandos y las Funciones para la prueba de envenenamiento de paquetes
Fuente: Sudhakar, R, & K, (2017)

Tabla 12
Tabulación de cumplimiento de la herramienta ettercap.

Parámetros	Esquema de criptografía	Servidor de validación de detección centralizado	Detección pasiva	Herramienta ettercap
Afinidad de problemas de agotamiento de ip	si	si	no	no
cumplir con el punto único de falla	no	no	si	si
alias de IP	si	si	no	no
Compatibilidad con versiones anteriores	no	si	si	si

Nota: Parámetros utilizados para detección con la herramienta de envenenamiento

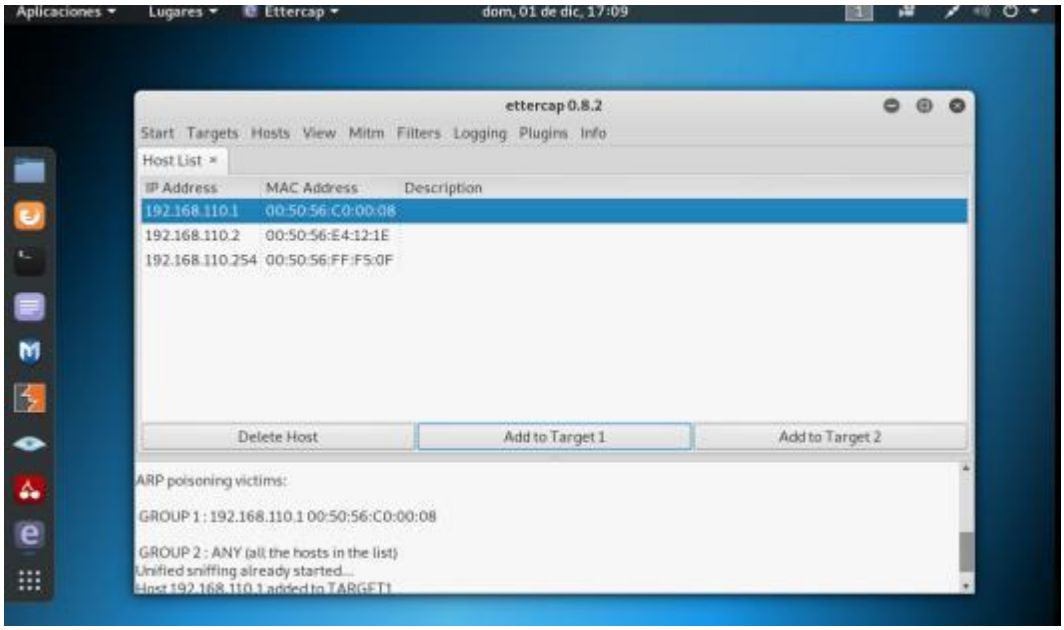
Como se señaló anteriormente, existen varias formas de realizar ataques basados en la debilidad e ineficiencia de la red de datos, como escuchar sin beneficios de cifrado sólido, donde otros pueden leer la información de un usuario a medida que avanza por el sistema. En cualquier caso, aquí es donde se comparan las herramientas de hacking etico que se utilizarán en esta investigación. Como se ha justificado, se utilizará la herramienta ETTERCAP ya que es útil para detectar invasiones.

En este proceso usamos un ataque conocido como "hombre en el medio" puede interceptar los paquetes usando la herramienta multiplataforma ETTERCAP, como se muestra en las Figuras 21 y 22. ETTERCAP lo usa para auditar redes que ya no soportan direcciones pasivas y activas de varios servicios o protocolo.

Figura 21
Proceso de Instalación de Ettercap

Nota: Instalación Herramienta para Prueba Fuzz Testing.

Figura 22
Proceso de ejecución de Ettercap

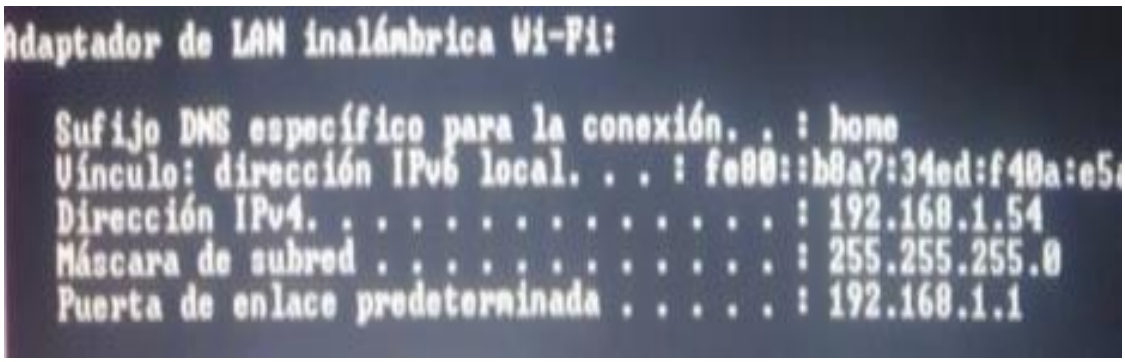


Nota: despliegue de la Herramienta Ettercap para Ataque de Hombre en medio

3.4.1. Intrusión

La herramienta de auditoría que se empleó para evaluar las técnicas de piratería ética fue una computadora de red local portátil con las características de red que se muestran en la Figura 23.

Figura 23
detalle de su conexiona a red que se utilizara para la evaluación de técnicas

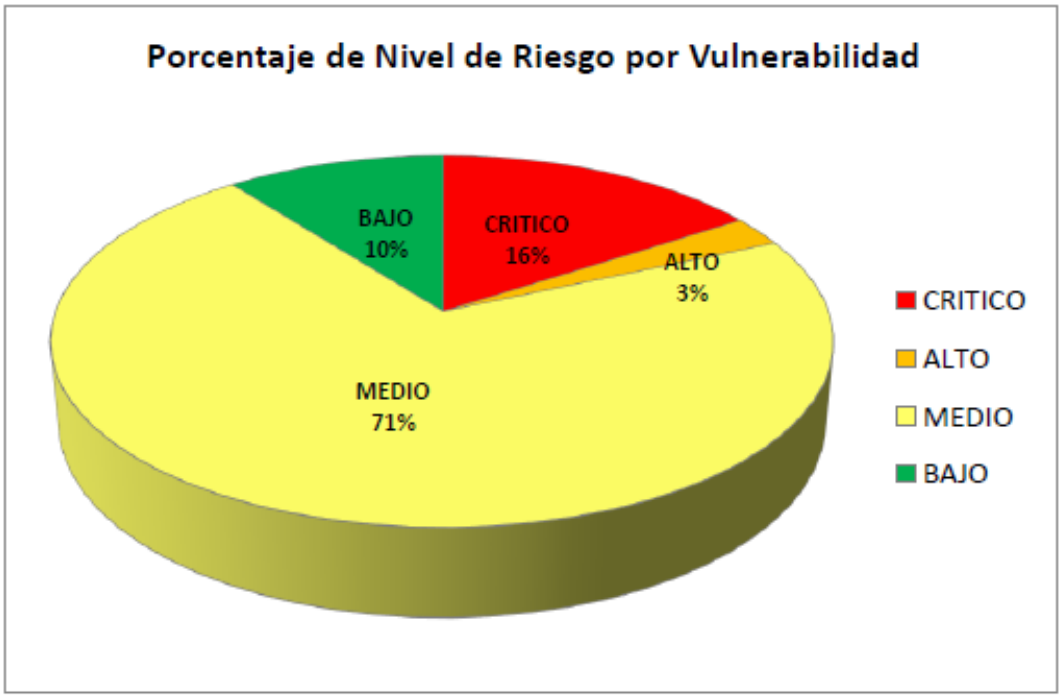


Nota: Detalle del equipo auditor para la evaluación de técnicas

3.4.2. Ganando Acceso y Escalando Privilegios.

Una descripción general de los niveles de vulnerabilidad descritos en los informes NESSUS y NMAP, serán los que nos permitan centrarnos más en el objetivo del estudio, como se muestra en la Tabla 12.

Tabla 5
Reporte por nivel de riesgo por vulnerabilidad



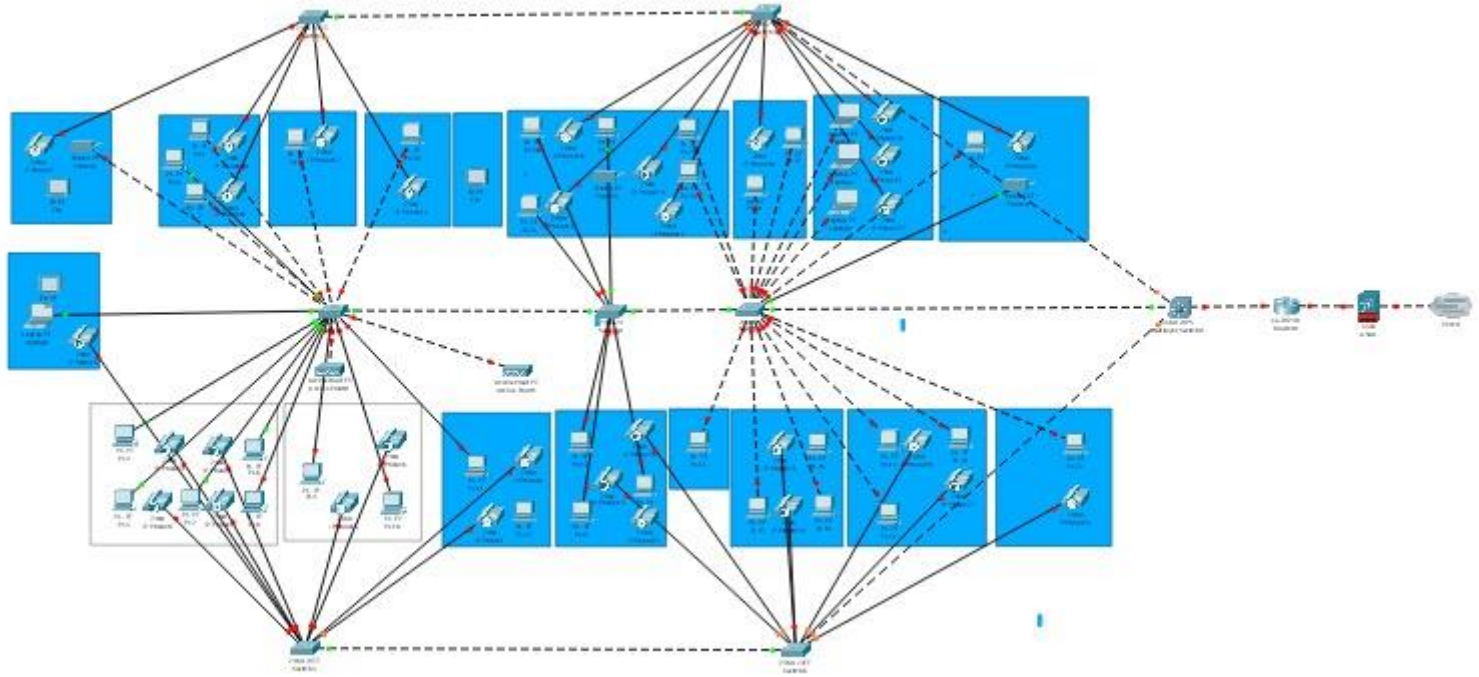
Nota: porcentaje del nivel de vulnerabilidades
Fuente: Tabulaciones resultados obtenidos en pruebas.

Cabe señalar que el informe identificó todos los niveles de riesgo de vulnerabilidad, lo que indica que el 71% de las vulnerabilidades se clasifican en las siguientes categorías de riesgo: medio, crítico, bajo y extremo.

3.4.3. Mapeo de la Red.

Se utiliza como modelo la estructura organizacional actual de una de las empresas del sector metalmecánico de Manabí, para evaluar las técnicas de hacking, en donde se mapea la red de datos utilizando las herramientas mencionadas.

Figura 24
Topología actual de red de datos

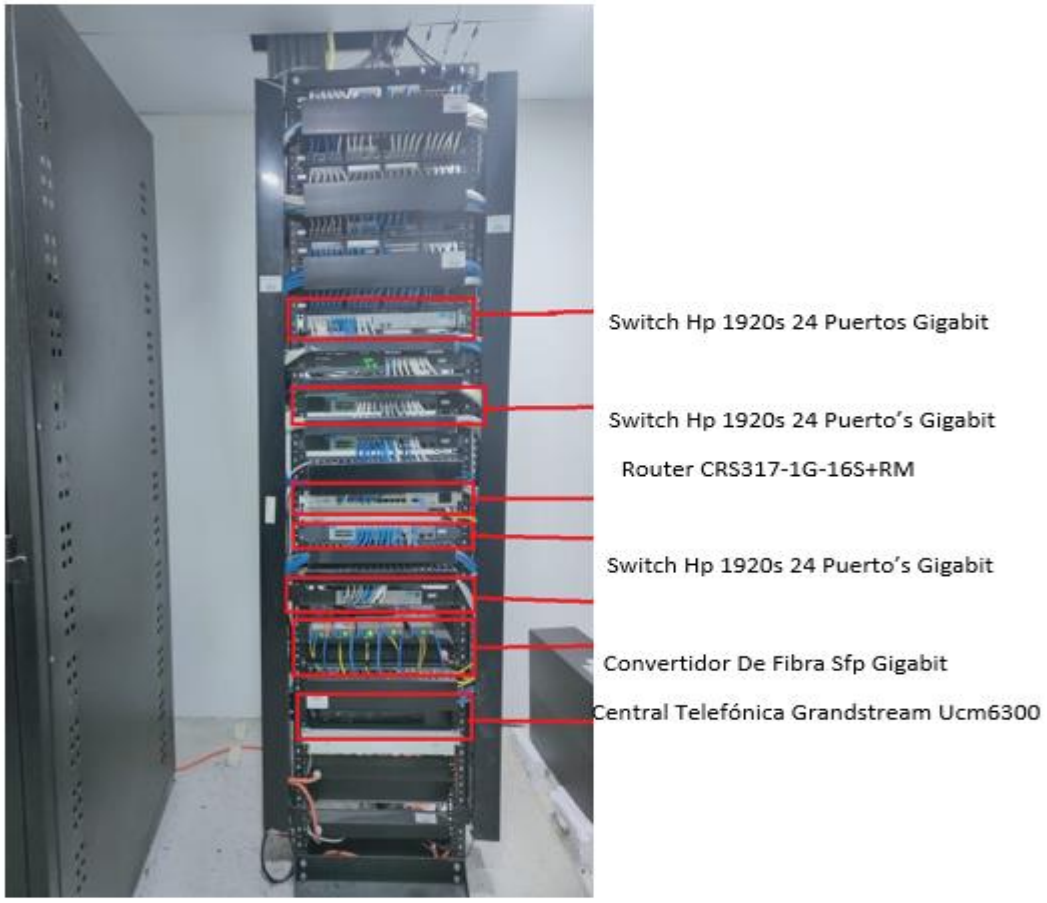


Nota: Estructura de red interna en análisis.
Fuente: Extrado de sistema packet tracer

Como se ve en la Figura 24, se indica un crecimiento proporcional de la red, ocurriendo la mayor parte de este crecimiento en el área administrativa. Esto conduce a un hacinamiento en el interruptor principal, lo que afecta la velocidad y la capacidad de los equipos conectados a esta red.

se observa en la figura 25 que el cableado CAT 6A de la marca AMP la cual cuenta con varias certificaciones.

Figura 25
Cableado Actual de la Red de datos



Nota: Estructura del rack interno de la empresa en análisis
Fuente: fotografía tomada para la investigación por el autor de este trabajo

3.4.4. Identificación de Vulnerabilidades

En esta fase para la evaluación de las 03 técnicas hemos realizado la identificación de las vulnerabilidades utilizando las principales herramientas como es NESSUS, NMAP y ETTERCAP.

3.4.5. Técnica de Prueba de Penetración

El proceso consistió en realizar un análisis activo del sistema a través del escaneo a fin de buscar posibles debilidades en la red de la empresa metalmecánica.

Escaneo de Vulnerabilidades detectadas con Nessus.

El escaneo de vulnerabilidades detectadas por host en la empresa objeto de estudio se ha realizo utilizando la herramienta NESSUS SCAN como parte de la técnica de penetración a continuación el detalle:

Tabla 14
Niveles de Vulnerabilidad Detectadas en la prueba de penetración

192.168.1.1			
PROTOCOLO	PUERTO	ESTADO	NIVEL VULNERABILIDAD
ssl certificate	935	abierto	medio
ssl auto certificate		abierto	medio
ip forwarding		abierto	medio
dhcp	6160	abierto	bajo
192.168.1.2			
PROTOCOLO	PUERTO	ESTADO	NIVEL VULNERABILIDAD
ms		abierto	critico
ms		abierto	medio
smb	233	abierto	medio
192.168.1.3			
PROTOCOLO	PUERTO	ESTADO	NIVEL VULNERABILIDAD
smb	233	abierto	medio
192.168.1.4			

PROTOCOLO	PUERTO	ESTADO	NIVEL VULNERABILIDAD
ssl	935	abierto	medio
ssl certificate		abierto	medio
ssl cipher		abierto	medio
smb	233	abierto	medio

192.168.1.5

PROTOCOLO	PUERTO	ESTADO	NIVEL VULNERABILIDAD
smb	233	abierto	medio

192.168.1.6

PROTOCOLO	PUERTO	ESTADO	NIVEL VULNERABILIDAD
smb	233	abierto	medio

192.168.1.7

PROTOCOLO	PUERTO	ESTADO	NIVEL VULNERABILIDAD
smb	233	abierto	medio

192.168.1.8

PROTOCOLO	PUERTO	ESTADO	NIVEL VULNERABILIDAD
ms		abierto	critico
microsoft rdp rce		abierto	critico
escritorio remoto		abierto	critico
ms		abierto	alto
ssl certificate	935	abierto	medio
ssl auto certificate		abierto	medio
microsoft security		abierto	medio
escritorio remoto		abierto	medio
smb		abierto	medio
ssl sin hash		abierto	medio
ssl cipher	233	abierto	medio
Terminal Network		abierto	medio
Terminal Encryption		abierto	medio
SSL	935	abierto	bajo
Terminal Services		abierto	Bajo

192.168.1.9

PROTOCOLO	PUERTO	ESTADO	NIVEL VULNERABILIDAD
ms		abierto	critico
escritorio remote		abierto	critico
ssl certificate	935	abierto	medio
ssl auto certificate		abierto	medio
microsoft security		abierto	medio
smb		abierto	medio
ssl sin hash		abierto	medio

ssl cipher	233	abierto	medio
ssl	935	abierto	bajo

Nota: Reporte de la verificación de vulnerabilidades
Fuente: Elaboración Propia

En este proceso ha sido posible documentar los resultados utilizando la herramienta especializada de Nessus creando asi un informe detallado por cada host a los que se le realizo la prueba de penetración.

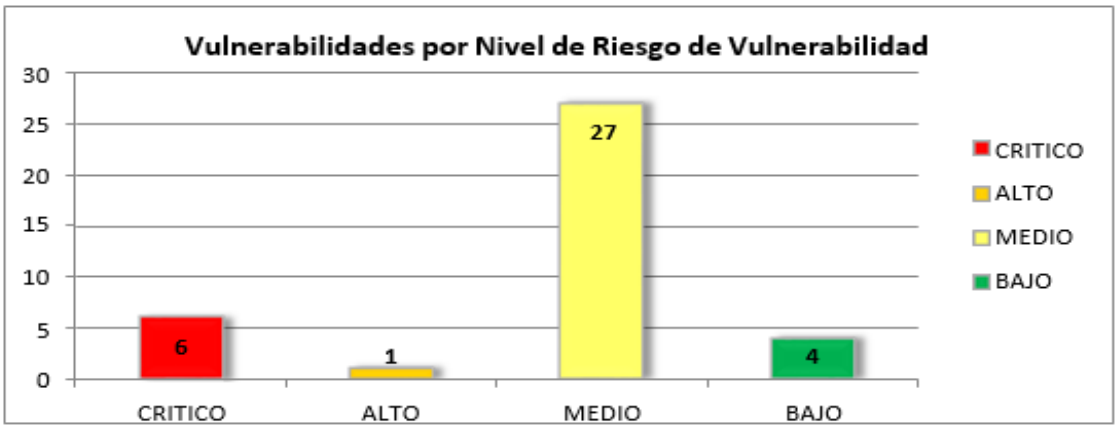
El siguiente es el resultado de las vulnerabilidades detectadas en el nivel de riesgo de la empresa de estudio.

Tabla 15
Resultados del escaneo de Vulnerabilidades en la prueba de Penetración

	RESULTADO DEL ESCANEO				
HOTS	**CRITICO**	**ALTO**	**MEDIO**	**BAJO**	**INFO**
192.168.1.1	0	0	3	1	23
192.168.1.3	0	0	0	0	4
192.168.1.4	1	0	2	0	22
192.168.1.5	0	0	0	0	5
192.168.1.6	0	0	4	0	23
192.168.1.7	0	0	1	0	27
192.168.1.8	0	0	1	0	13
192.168.1.9	0	0	1	0	12
192.168.1.10	3	1	9	2	40
192.168.1.11	2	0	6	1	36

Fuente: Elaboración Propia

Tabla 16
Detalle de la evaluación del riesgo por nivel de vulnerabilidad.



Fuente: Elaboración Propia

En la Tabla 16, observamos los tipos de niveles de vulnerabilidad descubiertos según el índice de cumplimiento de en red de la empresa en estudio, los que se define como: Cumplimiento alto del 3%, Cumplimiento medio del 71% y Cumplimiento mínimo del 10% En este caso, las vulnerabilidades en el nivel de cumplimiento crítico con el umbral del 16 % se consideran vulnerabilidades potenciales.

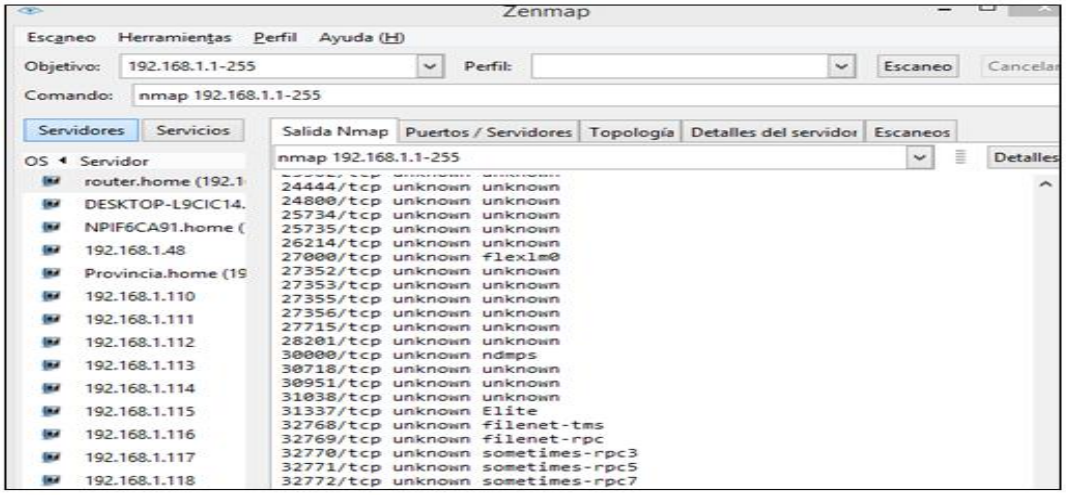
3.4.6. Técnica de Prueba Pasiva

El proceso involucró la realización de un análisis del tráfico de las comunicaciones descubriendo las vulnerabilidades a través de puertas abiertas.

Escaneo de Vulnerabilidades detectadas con NMAP.

Las direcciones IP que se escanearon en la red de la empresa de estudio se muestran en detalle en la Figura 26.

Figura 26
Escaneo de Vulnerabilidades en la Prueba Pasiva



Fuente: Reporte Nmap

Según Durand (2019) la herramienta NMAP es una de las herramientas más completas para la utilización del hacking ético. Para continuar, se completó el escaneo de

vulnerabilidades de direcciones IP utilizando la herramienta especializada NMAP, como se muestra en la Tabla 17 a continuación

Tabla 17
Escaneo de vulnerabilidades de puertos por protocolo en Prueba Pasiva

192.168.1.1				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**HERRAMIENTA**
80	TCP	OPEN	HTTP	NMAP
443	TCP	OPEN	HTTPS	NMAP
192.168.1.2				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**HERRAMIENTA**
80	TCP	OPEN	HTTP	NMAP
443	TCP	OPEN	HTTPS	NMAP
515	TCP	OPEN	PRINTER	NMAP
631	TCP	OPEN	IPP	NMAP
3910	TCP	OPEN	PRNREQUEST	NMAP
3911	TCP	OPEN	PRNSTATUS	NMAP
192.168.1.3				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**HERRAMIENTA**
135	TCP	OPEN	MSRPC	NMAP
139	TCP	OPEN	NETBIOS-SSN	NMAP
445	TCP	OPEN	MICROSOFT-DS	NMAP
3389	TCP	OPEN	MS-WBT-SERVER	NMAP
5040	TCP	OPEN	UNKNOWN	NMAP
5357	TCP	OPEN	WSDAPI	NMAP
192.168.1.4				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**HERRAMIENTA**
135	TCP	OPEN	MSRPC	NMAP
139	TCP	OPEN	NETBIOS-SSN	NMAP
445	TCP	OPEN	MICROSOFT-DS	NMAP
554	TCP	OPEN	RTSP	NMAP
2869	TCP	OPEN	ICSLAP	NMAP
2968	TCP	OPEN	ENPP	NMAP
192.168.1.5				
PUERTO	**PROTOCOLO**	**ESTADO**	**SERVICIO**	**HERRAMIENTA**
135	TCP	OPEN	MSRPC	NMAP
139	TCP	OPEN	NETBIOS-SSN	NMAP
445	TCP	OPEN	MICROSOFT-DS	NMAP
2968	TCP	OPEN	ENPP	NMAP
5040	TCP	OPEN	UNKNOWN	NMAP
5357	TCP	OPEN	WSDAPI	NMAP

192.168.1.6				
PUERTO	PROTOCOLO	ESTADO	SERVICIO	HERRAMIENTA
135	TCP	OPEN	MSRPC	NMAP
139	TCP	OPEN	NETBIOS-SSN	NMAP
445	TCP	OPEN	MICROSOFT-DS	NMAP
2968	TCP	OPEN	ENPP	NMAP
5357	TCP	OPEN	WSDAPI	NMAP
192.168.1.7				
PUERTO	PROTOCOLO	ESTADO	SERVICIO	HERRAMIENTA
135	TCP	OPEN	MSRPC	NMAP
139	TCP	OPEN	NETBIOS-SSN	NMAP
445	TCP	OPEN	MICROSOFT-DS	NMAP
554	TCP	OPEN	RTSP	NMAP
2869	TCP	OPEN	ICSLAP	NMAP
3389	TCP	OPEN	MS-WBT-SERVER	NMAP
5357	TCP	OPEN	WSDAPI	NMAP
192.168.1.8				
PUERTO	PROTOCOLO	ESTADO	SERVICIO	HERRAMIENTA
135	TCP	OPEN	MSRPC	NMAP
139	TCP	OPEN	NETBIOS-SSN	NMAP
445	TCP	OPEN	MICROSOFT-DS	NMAP
554	TCP	OPEN	RTSP	NMAP
192.168.1.9				
PUERTO	PROTOCOLO	ESTADO	SERVICIO	HERRAMIENTA
2869	TCP	OPEN	ICSLAP	NMAP
2968	TCP	OPEN	ENPP	NMAP
3389	TCP	OPEN	MS-WBT-SERVER	NMAP
5357	TCP	OPEN	WSDAPI	NMAP

Fuente: obtenidas según las métricas establecidas el autor (Durand, 2019)

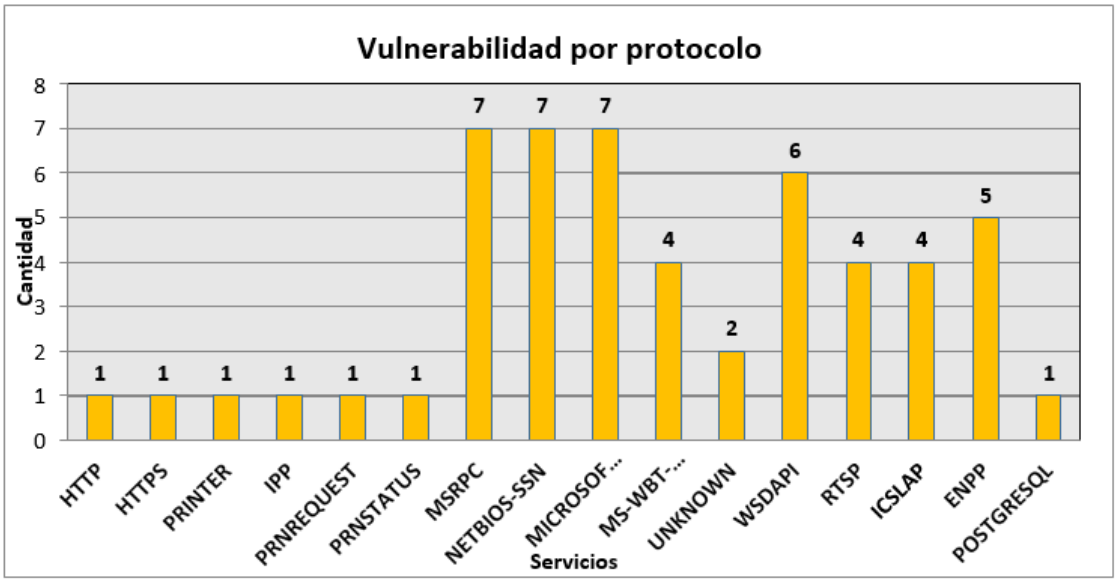
El siguiente es el resultado de tabular la información sobre las vulnerabilidades detectadas por protocolo dentro de la empresa.

Tabla 18
escaneo de puertos abiertos en la Prueba Pasiva

IP's	http	https	printer	prinrequest	prinstatus	MSRPC	netbios-SSN	microsotf-DS	SERVERQ	WSDAPI	RTSP	ICSLAP	ENPP	POSTGRESQL
192,168.1.1	1	1												
192.168.1.2			1	1	1									
192.168.1.3														
192.168.1.4						1	1	1	1	1				
192.168.1.5						1	1	1			1	1	1	
192.168.1.6						1	1	1		1			1	
192.168.1.7						1	1	1		1			1	
192.168.1.8						1	1	1	1	1	1	1		1
192.168.1.9						1	1	1	1	1	1	1	1	
192.168.1.10						1	1	1	1	1	1	1	1	

Fuente: Reporte NMAP

Tabla 19
Medición de las vulnerabilidades detectadas por protocolo en la Prueba Pasiva.



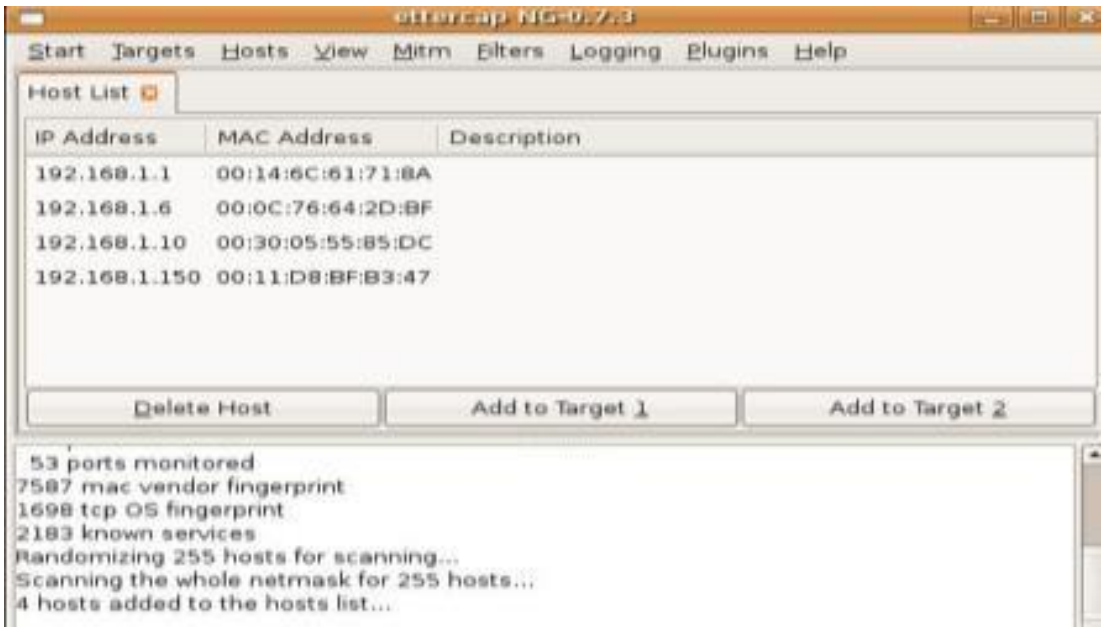
Fuente: elaboración propia

Como se puede observar en la Tabla 19, las vulnerabilidades fueron descubiertas en su mayoría por los protocolos abiertos de uso más frecuente en la red de datos, los mismos que se han clasificado ordinariamente.

3.4.7. Técnica de Prueba Fuzz testing o Caja Negra.

Es la técnica para evaluar e identificar los comportamientos que conducen a la violación del elemento de confidencialidad utilizando dispositivos conectados a la red , el proceso implica realizar un análisis de datos asíncronos o archivos relacionados con la evaluación.

Figura 27
Ataque tipo Man in the Middle en la Prueba de Fuzztesting



Nota: Prueba de Fuzztesting
Fuente: Extraído del reporte (elaboración propia)

Proceso de Ataque (Man in the Middle) detectados con ETTERCAP

Se enviaron un total de 100 archivos a cada dispositivo de red durante el desarrollo de la prueba MiTM.

Tabla 20
Muestra del Análisis de cada dispositivo en la Prueba Fuzz testing

IP	ARCH RECIBIDOS	ARCH ENVIADOS	%ARCH CORRUPTOS
192.168.1.1	97	100	3
192.168.1.2	80	100	20
192.168.1.3	81	100	19
192.168.1.4	90	100	10
192.168.1.5	94	100	6
192.168.1.6	86	100	14
192.168.1.7	94	100	6
192.168.1.8	86	100	14
192.168.1.9	96	100	4
192.168.1.10	88	100	12

Fuente: Elaboración propia

Tabla 21
Tabla de vulnerabilidad detectada por archivos en la prueba de Fuzztesting

Fuente: Elaboración propia

Como mostramos en la red de datos, una porción promedio de los archivos estan corruptos o fechados y se estima en un 10,8% del total de los expedientes examinados.

Resultados Generales - Scanning y enumeración

Todos los puntos interactivos que se descubrieron durante la evaluación de las redes humanas, físicas, inalámbricas y de datos se detallan en la Tabla 20. Se pudieron encontrar solo 5 puntos de confianza interactivos de un total de 146 puntos de acceso y visibilidad que podrían conducir a una brecha de seguridad de la información en algún momento. Dado que el 46,6% de las organizaciones en Ecuador, según el estudio de (ESET de 2017), formaron parte de alguna de estas redes maliciosas debido a la falta de buenas prácticas de seguridad de la información, los resultados anteriores pueden explicarse por una potencial botnet de dentro de las empresas del sector metalmecánico de Manabí. Por lo expuesto anteriormente, fue necesario examinar estrategias que permitan evidenciar el riesgo dentro de la empresa en estudio como vemos en la tabla 21.

Tabla 22
Fase de Interacción, Check list de verificación de seguridad informática y Nmap.

riesgo		confianza	acceso	visibilidades	total, porosidad
humano	seguridad física	1	8	2	11
físico	seguridad física	0	10	4	14
Wireless	seguridad en el espectro	0	12	3	15
redes de datos	seguridad en las comunicaciones	4	87	15	106
total		5	117	24	146

Nota: Tabla elaborada por los autores por medio de revisión bibliográfica de los contenidos necesarios.

Analizando los datos de la Tabla 23 y 24, que contabiliza los controles descubiertos durante la auditoría evaluativa con una de las herramientas de hacking ético, se observa que los controles de interacción, tipo A, suman 63 y afectan directamente la visibilidad, el acceso y la confianza (porosidad); en cambio, los controles de proceso, o tipo B, ascienden a 22, y dan seguridad frente a amenazas.

Tabla 23
Controles de seguridad cuantificados por canal humano, físico, Wireless, redes de datos.

	riesgo		AUTENTIFICACION	INDEMNIZACION	VISIBILIDADES	SUBYUGACION	CONTINUIDAD	TOTAL, CLASE A
humano	seguridad física	CONTROLES CLASE A (interaccion)	14	1	1	0	0	16
físico	seguridad física		0	3	0	0	15	18
Wireless	seguridad en el espectro		3	0	1	0	0	4
redes de datos	seguridad en las comunicaciones		14	1	0	2	8	25
	total		31	5	2	2	23	63

Nota: tabla elaborada mediante el Check list de verificación de seguridad informática y Nmap.

Tabla 24
Controles de seguridad cuantificados por canal humano, físico, Wireless, redes de datos

	riesgo		NO REPUDIO	CONFIDENCIALIDAD	PRIVACIDAD	INTEGRIDAD	ALARMA	TOTAL, CLASE B	TOTAL, POROSIDAD
humano	seguridad física	CONTROLES CLASE B (interaccion)	0	1	3	0	2	6	22
físico	seguridad física		0	0	0	0	1	1	19
Wireless	seguridad en el espectro		1	0	1	3	3	8	12
redes de datos	seguridad en las comunicaciones		1	3	1	1	1	7	32
	total		2	4	5	4	7	22	85

Nota: tabla elaborada mediante el Check list de verificación de seguridad informática y Nmap.

3.5. Fase de Investigación – Análisis de Vulnerabilidades.

Tabla 25
Fase Investigación – Limitaciones.

riesgo			exposicion	vulnerabilidad	debilidad	preocupacion	anomalias	total, limitaciones
humano	seguridad física	limitaciones	3	0	2	0	0	5
físico	seguridad física		1	1	2	2	0	6
Wireless	seguridad en el espectro		0	3	0	0	0	3
redes de datos	seguridad en las comunicaciones		3	14	2	1	0	20
total			7	18	6	3	0	34

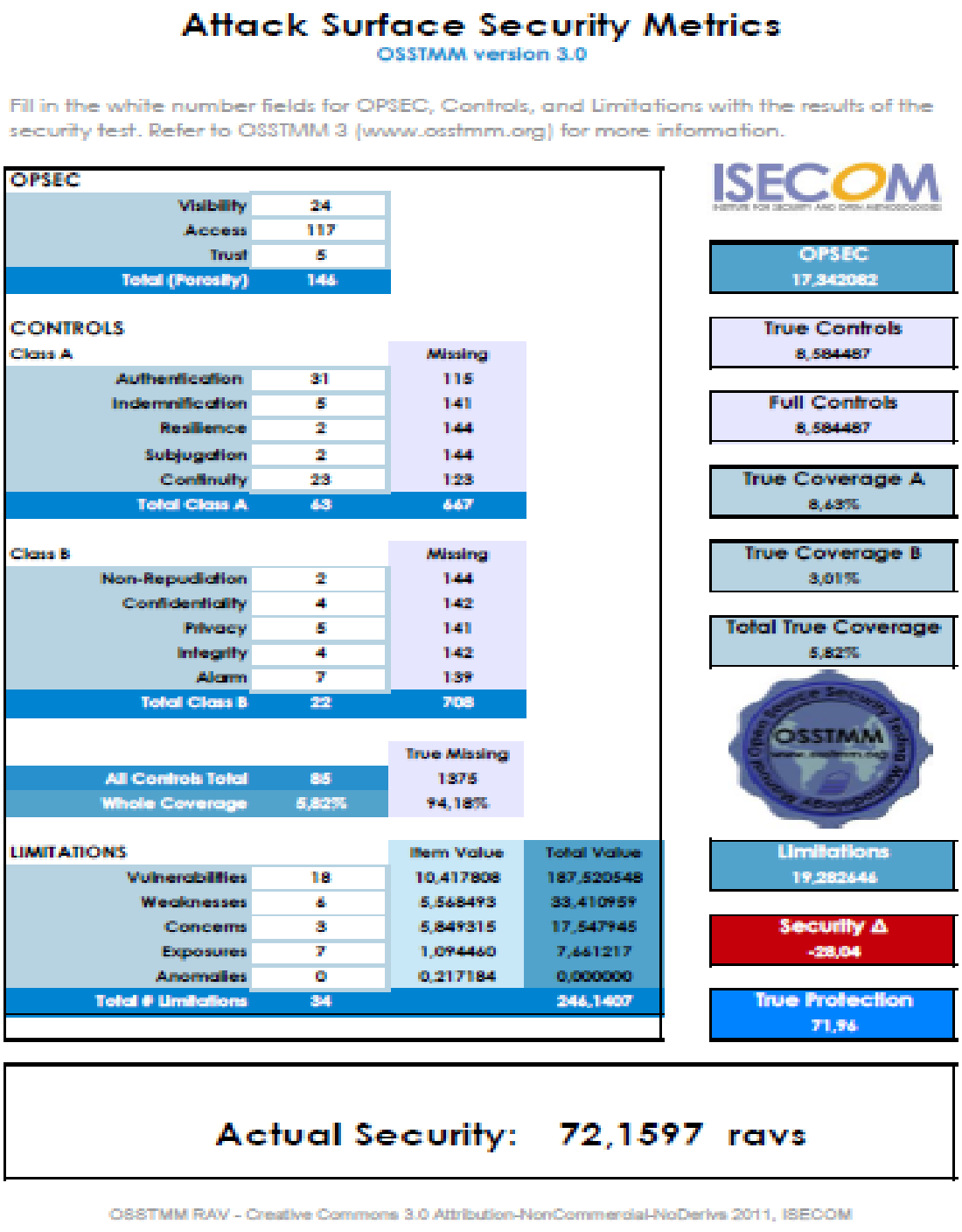
Nota: Check list de verificación de seguridad informática, Nessus.

En el cuadro anterior se cuantifican las limitaciones evidenciando un total de 34, de las cuales 18 son vulnerabilidades que afectan directamente la confiabilidad, integridad y accesibilidad de la información (ver tabla 25); en relación a esto, (Kaspersky., 2020), reporta que hay un aumento de malware infecciones en América Latina.

3.5.1. Resultado de la información obtenida modelado en la hoja electrónica, RAV.

Estos resultados los podemos evidenciar con mayor relevancia en la figura 28 la cual es extraída del reporte obtenido en la hoja electrónica RAV

Figura 28
Resultados finales del análisis de vulnerabilidades RAV, OSSTMM V3.0



Attack Surface Security Metrics

OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.

ISECOM

OPSEC

Visibility	24
Access	117
Trust	5
Total (Porosity)	146

CONTROLS

Class A		Missing
Authentication	31	115
Indemnification	5	141
Resilience	2	144
Subjugation	2	144
Continuity	23	123
Total Class A	63	667

Class B		Missing
Non-Repudiation	2	144
Confidentiality	4	142
Privacy	5	141
Integrity	4	142
Alarm	7	139
Total Class B	22	708

		True Missing
All Controls Total	85	1375
Whole Coverage	5,82%	94,18%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	18	10,417808	187,520548
Weaknesses	6	5,568493	33,410959
Concerns	3	5,849315	17,547945
Exposures	7	1,094460	7,661217
Anomalies	0	0,217184	0,000000
Total # Limitations	34		246,1407

OPSEC	17,342082
True Controls	8,584487
Full Controls	8,584487
True Coverage A	8,63%
True Coverage B	3,01%
Total True Coverage	5,82%
Limitations	19,282646
Security Δ	-28,04
True Protection	71,96

Actual Security: 72,1597 ravs

Fuente: Extraído del reporte OSSTMM (elaboración propia)
Nota: Documentación obtenida y modelada de acuerdo a la metodología implementada.

3.6. Fase de Intervención.

En esta fase se revela el estado de seguridad operativa de la empresa objeto del estudio del sector metalmecánico. Luego, los datos obtenidos se ingresan en la matriz de cálculo RAV, que es parte de la metodología OSSTMM, para producirlos resultados del estado de seguridad operativa del 72,15 % y una brecha de seguridad del 28,04 %.

3.6.1. Mitigación de las Vulnerabilidades

Esta parte de la fase de intervención evalúa las técnicas de Hacking Ético para desarrollar las pruebas de entrenamiento, donde se descubren las vulnerabilidades que coincidían con las ya clasificadas, y se procederá a mitigar las vulnerabilidades más críticas de la siguiente manera.

Técnica de Penetración: Vulnerabilidades clasificadas por Niveles

Vulnerabilidad Nivel Crítico:

Problema:

1. MS: el inicio de sesión para los sistemas operativos Microsoft Security. En concreto, "Certificado de Autenticidad del licenciamiento de Sistema Operativo se detectó que la licencia no original.
2. El servidor de escritorio remoto activado. Algún intruso puede acceder de manera local si se encuentra en la red y vulnerar la información de importancia para la empresa.

Medida de Mitigación:

1. Realizar un proceso de actualización y cambio de sistema operativo a la última versión que ofrece el fabricante Microsoft debido a que la actual

versión dejó de brindar soporte y se encuentra vulnerable ante cualquier ataque informático.

2. Creación de políticas y reglas en el firewall para habilitar escritorio remoto por puertos dentro de la red de trabajo.

Vulnerabilidades de Nivel Alto:

Problema:

1. MS: el proceso de autenticación en su login es de poca seguridad. Es decir, la forma de autenticación cuenta con una muy baja seguridad para su control de acceso.

Medida de Mitigación:

1. Inicialmente proceder actualización y cambio de sistema operativo que brinde mayor seguridad, dado que la versión que se utiliza es muy antigua dejó de brindar soporte de seguridad y se encuentra vulnerable ante un acceso no deseado.

Vulnerabilidades de Nivel Medio:

Problema:

1. SMB: servidor Zimbra plataforma que se encarga de la gestión de correo electrónico y no cuenta con un antispam que pueda el cual genera un alto riesgo en cada uno de los buzones.
2. SSL: (Cifrado Secure Socket Layer). El certificado de validación de la página no está habilitado de forma correcta el cual muestra la figura de sitio no seguro en algunos navegadores.

Medida de Mitigación:

1. Si se mantiene un servidor de correos Zimbra ya sea local o en la nube se debe conta con las medidas de protección antes virus y spam que se envían en los correos, mantener una buena política de acceso de archivos los cuales pueden incurrir en script que de entrada a múltiples accesos no identificados.

2. Cambiar el tipo de certificado ssl actualmente cuenta con un DV se recomienda cambiar a un certificado ssl EV el cual validara como una compañía valida y evitara caer en correos no deseados.

Técnica de Prueba Pasiva: Vulnerabilidades clasificadas por puertos o protocolos abiertos.

Problema:

1. Puertos Abiertos en aplicaciones no necesarias para la empresa:
2. Bajo control en el uso del Escritorio Remoto (RDP)
3. uso compartido de archivos en la red con poca seguridad
4. Direccionamiento IP segmentado solo en ciertas áreas.
5. Gestor de equipos de Impresión de documentos en red.

Medida de Mitigación:

6. Activación de puerto específico para el uso de escritorio remoto
7. Activar el certificado ssl EV para compañías
8. Desactivar la respuesta de broadcast de red.
9. Compartir solo las impresoras necesarias por puertos específicos.

Técnica de Prueba Fuzztesting o Caja Negra: Vulnerabilidades clasificadas por ataque de archivos

Problema:

1. El porcentaje de la media de archivos dañados en la red de datos asciende al 10,8% del total de archivos transferidos.

Medida de Mitigación:

1. Creación de cuentas de correo corporativas y envío de documentos a través de ellas.

En esta técnica de fuzztesting se trabajó con la herramienta especializada Ettercap, efectuando un ataque en las conexiones de la red en estudio, realizando el proceso de envenenamiento de archivos.

3.7. DISCUSIÓN

De acuerdo con los indicadores mostrados en esta investigación, se discuten los resultados obtenidos. El realizar la evaluación las auditorias informáticas para de esta forma desplegar las técnicas para descubrir las vulnerabilidades informáticas, puertas abiertas en sus sistemas de información y confianza de acuerdo con el índice de cumplimiento de la empresa, el cual se define a continuación.

Las herramientas utilizadas para las pruebas de penetración arrojaron los resultados de cumplimiento los cuales son: cumplimiento ALTO del 3%, cumplimiento

MEDIO del 71% y cumplimiento BAJO del 10% para este caso. Las vulnerabilidades en el nivel de cumplimiento CRTICO del 16 % se consideran vulnerabilidades potenciales.

Cabe recalcar que la funcionalidad de cada protocolo debe cumplirse siempre y cuando se esté utilizando y el estado cambie de LISTENER a ESTABLISHED, es decir el puerto este escuchando en la red, los mismos que han sido clasificados en una manera ordinaria.

Según (Hurtado & Mendao, 2016), la técnica de " caja noire " o "fuzztesting" menciona y detalla los elementos necesarios para realizar un ataque. En nuestro caso, hablaremos de los elementos mencionados por los investigadores porque ha sido posible realizar ataques el tipo "Man-in-the-Middle". Este tipo de ataque consiste en escuchar todo el tráfico generado por el objetivo o la víctima mientras está en línea.

Los hallazgos hacen referencia al nivel de riesgo descubierto, el reconocimiento de puntos de entrada y grado de confianza dado que las técnicas de Hacking Ético permitieron evaluar e identificar qué tan vulnerable es ingresar a una red de datos.

Según Patil, Jangra, Bhale , Raina, & Kulkarmi (2017), desarrollaron un análisis del proceso que constó de cuatro etapas en su investigación sobre la aplicación de la metodología OSSTMM utilizando herramientas etimológicas de hacking. Inducción (FASE 1), interacción (FASE 2), investigación (FASE 3) y su intervención final (FASE 4), Adicionalmente, se demostró la funcionalidad de las herramientas utilizadas en cada una de estas fases.

Como resultado, podemos comprobar que en este estudio pudimos usar una metodología de auditoria informática para evaluar técnicas de hacking ético para

identificar vulnerabilidades, la cual para determinar el estado de la seguridad informática. Y si estaba protegido de cualquier amenaza de intrusión.

3.7.1. Métricas para la evaluación de las Técnicas de las aplicadas.

Las siguientes métricas se que se aplicaron como estándares para futuras políticas de seguridad se plantearon con el fin de mejorar la seguridad de una red de datos en cualquier organización.

las métricas propuestas son fundamentales para realizar esta evaluación, las cuales se detallan en la Tabla 26.

Tabla 26
Métricas utilizadas para la evaluación de las Técnicas de las aplicadas.

Métricas usadas para evaluación de las Técnicas aplicadas.	prueba de penetración	prueba pasiva	fuzz testing
Vector de Acceso	Red Local	Red Local	Remoto
Complejidad de Acceso	Bajo	Bajo	Alto
Autenticación	simple	simple	simple
Impacto en el nivel riesgo	alto	Medio	alto
Impacto en el reconocimiento de puertos	alto	alto	alto
Impacto en la confidencialidad	bajo	bajo	alto
Facilidad de corrección	corrección	corrección	corrección
Facilidad Informe de vulnerabilidades	Identificada - corregida	Identificada - corregida	Identificada - corregida

Nota detalle de métricas usadas para la Evaluación de Técnicas de Hacking Ético.
Fuente: Elaboración Propia.

3.8. Participación científica

3.8.1 Información de la empresa del Sector metalmecánico para el estudio

Para esta investigación se tomó como muestra la empresa INDUSTRIAS MASTER INDUMASTER S.A, es una empresa del sector metal mecánico y comercial de la

provincia de Manabí, la cual se dedica a la fabricación y comercialización de muebles de hogar y oficina con tapizados de alta calidad, comprometidos a satisfacer las necesidades del cliente, Además, siguiendo los estándares internacionales cuidamos el medio ambiente y bienestar de nuestros trabajadores. gestionando su seguridad y salud.

La realización de proyectos de tecnologías de la información acoge un amplio espectro de su infraestructura informática la misma que cuenta con centro de datos donde se almacena y gestiona la información, el área tecnológica está en constante realización de proyectos los mismos que siguen en desarrollo actualmente como lo es su sistema ERP el mismo que cubre todas sus áreas que generan información, dicho sistema está desarrollado de forma web utilizando el lenguaje PHP con YII y su conectividad con la base de datos SQL Server, al igual que las demas funcionalidades tecnológicas con la que cuenta la empresa evidencia que cuenta con maquinaria con tecnología IOT tecnología que permite integrar los procesos industriales con los tecnológicos, como parte de resguardo de su información cuenta con un data center totalmente aislado de las demas áreas con un sistema de enfriamiento permanente el cual previene algún fallo en los procesos y con soporte energético para evitar perdida de comunicación en sus labores.

3.8.2. Métricas para el diagnóstico de vulnerabilidades

Las métricas planteadas para comenzar el análisis de las vulnerabilidades en la red de datos en la empresa en estudio. Se proporciona la siguiente en la siguiente explicación:

- **AV: VECTOR DE EXPLOTACION**: El objetivo se define como identificar y explotar vulnerabilidades de cualquier red.

- **AC: COMPLEJIDAD DE ACCESO:** dificultades que surgen al determinar la vulnerabilidad de una persona vulnerable o baja.
- **AU: AUTENTICACIÓN:** esto menciona que el usuario tenga los privilegios de acceso al objeto de diagnóstico.
- **NIVEL DE IMPACTO DE RIESGO: MUESTRA** los niveles de vulnerabilidades descubiertas (Alto = Crítico, Medio = Alto, Bajo = Normal).
- **RP: IMPACTO EN EL RECONOCIMIENTO DE PUERTOS:** muestra los niveles de riesgo en los puertos abiertos de forma innecesaria.
- **CI: IMPACTO DE LA CONFIDENCIALIDAD:** detalla la transmisión de datos en uno de comunicación segura.
- **FC: FACILIDAD DE SOLUCION:** detalla los niveles de complejidad para aplicar una solución al problema encontrado.
- **IV: INFORME DE VULNERABILIDAD:** muestra fiabilidad para la aplicación de una solución en un entorno existente, en tiempo real y para posteriores ataques.

Las matrices que se detallaron nos permiten establecer niveles de ataque y distinguir entre los varios tipos de ataques en tiempo real, con esto podremos encontrar soluciones adecuadas a la complejidad de la vulnerabilidad descubierta.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Se pudo obtener información acerca de cómo se gestiona la seguridad en las empresas del sector metalmecánico de Manabí, a través de la aplicación de una encuesta con la cual fue posible conocer el estado actual de las empresas que forman parte del sector metalmecánico de Manabí para la realización de una auditoría de la seguridad de la informática, dando como resultado del análisis los datos recabados a través de esta encuesta, se pudo notar que las empresas, a pesar de contar con personal calificado en el campo de tecnológico, no manejan de manera efectiva los aspectos de seguridad de la información en general.
- Basándose en la técnica de la revisión bibliográfica que se aplicó para este proyecto podemos concluir que la cuantificación de la bibliografía mejora el desarrollo del proyecto aportando asi datos y referencias de trabajos existentes fundamentados en el tema propuesto.
- Mediante el uso de la metodología OSSTMM y las pruebas de hacking ético, se realizó una auditoría de seguridad de la información en las empresas del sector metalmecánico de Manabí. Se establecieron métricas para medir la gravedad y el impacto de las vulnerabilidades descubiertas, siendo el principal hallazgo un valor de seguridad de 64,43%, o seguridad de la información moderadamente alta. Por lo que se sugiere mejorar los valores de evaluación de riesgo (RAV).
- Se evidenciaron las brechas que se generan en la seguridad de la información las cuales se cuantificaron como parte de la investigación utilizando la metodología OSSTMM utilizando las herramientas apropiadas para evaluar cada aspecto de la seguridad Informática. La cual de acuerdo a los componentes evaluados tienen un

alto riesgo de ser vulnerada y estar sujetos a violaciones de la seguridad de la información.

RECOMENDACIONES

- Realizar escaneos de vulnerabilidades continuos utilizando métodos y herramientas sofisticados que permiten la gestión de incidentes en seguridad de la información al tiempo que se establezcan responsabilidades y procedimientos preventivos para gestionar eventos y debilidades de manera oportuna.
- Se recomienda implementar las técnicas de hacking ético utilizadas en este en este estudio, ya que permitirán a al personal de tecnología aplicar, examinar y reducir el riesgo de vulnerabilidades.
- Se recomienda la actualización licencias de software, firewalls, la actualización de versiones de sistemas operativos, etc. para cada servicio es fundamental que se realicen actualizaciones para salvaguardar la integridad de la información de la institución.
- Se recomienda la compra de software para realizar análisis de vulnerabilidad continuos. Este software debe ofrecer líneas de comunicación de seguridad y confidencialidad para simular los ataques examinados y proponer mecanismos de mitigación, en caso de que sean lanzados por un atacante externo.

REFERENCIAS BIBLIOGRÁFICAS

Altamirano & Oré, J. R. (2017). Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías. *risti*, 114-128.

Antidot. (2014). *Linked Enterprise Data* (85-100 ed., Vol. Vol. 1). (H. S. Tassilo Pellegrini, Ed.) Heidelberg, Berlín , Alemania. doi:https://doi.org/10.1007/978-3-642-30274-9

Aquiahuatl E.C. ((2015)). *Metodología de la investigación interdisciplinaria: Tomo I Investigación monodisciplinaria.* Self published.

Armas, J. A. (2018). *Ciberseguridad: Como adoptar medidas para proteger sus activos de información.* (Vol. 4). Review of Global Management. Obtenido de https://doi.org/10.19083/rgm.v4i2.1127

Armstrong &Peiris. (2017). *Sistemas Informacion* (Vol. vol .1). Madrid, España.

ASAMBLEA NACIONAL. (2014). COIP., (pág. 144). QUITO.

ASTUDILLO, K. (2017). *HACKING ETICO 101* (Vol. vol 2). GUAYAQUIL, Ecuador: Babecube Inc.

Benchimol. D. ((2010)). *Redes Cisco.* Argentina: Gradi.

Bernal Torres C.A. ((2006)). *Metodología de la investigación: para administración, economía, humanidades y ciencias sociales.* Mexico: Pearson Educación.

Bestuzhev, D. (2021). Ecuador lidera la lista de países más vulnerados por los ciberataques. *primicias*.

Calle, J. (2020). *Fases de un ataque a un Sistema Informático.*

Capurro R., C. (2007). *Epistemología y ciencia de la información.* Caracas - Venezuela: Revista Venezolana de Información, Tecnología y Conocimiento.

CARISSIMI, L. (2018).

CEPAL. (18 de 12 de (2020)). *Gestión de datos de investigación.* Obtenido de https://biblioguias.cepal.org/gestion-de-datos-de-investigacion

Chalen, M. (2010).

CROWE. (2020). *crowe.com*. Obtenido de https://www.crowe.com/uy/services/ciberseguridad/owasp

ecucert. (2021). *ecucert.gob.ec*. Obtenido de www.ecucert.gob.ec

Ekos. ((2018)). INDUSTRIA METALMECANICA S.A. *Ekos*, https://www.ekosnegocios.com/empresa/inmetsur-industria-metalmecanica-sa. Obtenido de https://www.ekosnegocios.com/empresa/inmetsur-industria-metalmecanica-sa

Emiliani & R. Sierra. (2015). *Manual Metodológico para pruebas de seguridad OSSTMM 3 y Guía de Pruebas OWASP 4.* Obtenido de https://es.scribd.com/document/265102425/Resumen-de-Guias-OSSTMM-OTGv4. (Consultado 25-04-2017).

Figueroa C. M. (2012). *Persona y profesion; profesion y tecnicas de seleccion y orientación.* Madrid.

Foundation, O. (2020). *OWASP Testing Guide v4 Table of Contents*. Obtenido de https://wiki.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

Fritz, E. |. (2016). TECNOLOGIA DE LA INFORMACION. *XVIII Workshop de Investigadores en Ciencias de la Computación* (págs. 383-387). Argentina: Red de Universidades con Carreras en Informática (RedUNCI). Obtenido de https://www.tecnologias-informacion.com/integridaddatos.html

Gabalán, V. (2015).

GK. (22 de 07 de 2021). *gk.city*. Obtenido de https://gk.city/que-es/

Gómez Viertes, Á. (2018). *"Sistemas de Información, Herramientas Prácticas para la Gestión Empresarial".* Madrid, Madrid, España.: Editora RAMA.

González Gallego, R. E. (2014). *Diccionario de Computación y Electrónica. México D.F*. Mexico D.F.

GONZÁLEZ, M. A. (2019). *Auditoría Informática* . MADRID: Socio-Director de Informáticos Europeos Extertos (IEE) .

Gonzalo, A. R. (2017). Auditoría de seguridad informática ulizando la metodología OSSTMM v3. *Revista Maskana, Vol.8*, 307–315.

Griffith Belver. (1980). *Key papers in information science.* Obtenido de http://kantor.comminfo.rutgers.edu/619phd/readings/InformationScience.pd

Gutiérrez, A. (2021). *agcriminalistica*. Obtenido de agcriminalistica: https://agcriminalistica.com/

Ibáñez P. J. (2015). *Métodos, técnicas e instrumentos de la investigación criminológica.* Madrid: Editorial Dikynson.

ISACA. (2011). Enfoque Metodologico de la auditoria a las tecnologias de Informacion y Comunicacion. *XIV CONGRESO ANUAL DE INVESTIGACION*, 9-14.

ISECOM. (2020). *http://www.isecom.org/*. Obtenido de http://www.isecom.org/research/osstmm.html

Jara . H, J. (2012). *Ethical Hacking 2.0.* Buenos Aires: Fox Andina.

Juan Diego Muñoz, D. P. (2017). Metodología para seleccionar políticas de seguridad informática. *Maskana - Ciencias de la Computación*.

Kaspersky., L. (2020). *Karspersky daily*. Obtenido de https://latam.kaspersky.com/blog/

López Santoyo, R. ((2015)). *Propuesta de implementación de una metodología de auditoría de seguridad informática.* Madrid.: UAM. Departamento de Ingeniería Informática. Obtenido de http://hdl.handle.net/10486/668900

Maya y Jaramillo, D. ((2015)). *Seguridad Informática para el Gobierno Autónomo Descentralizado de Santa Ana de Cotacachi, basada en la norma NTP-ISO/IEC 17799:2007 y la metodología OSSTMM V2*. Obtenido de

http://repositorio.utn.edu.ec/bitstream/123456789/3774/2/04%20RED%20034%20Art%C3%ADculo%20Cient%C3%ADfico%20Espa%C3%B1ol.pdf. (Consultado 05-04-2017).

Ministerio Coordinador de la seguridad. (2014). *Seguridad Informatica en el Ecuador.*

Muñoz Enrique, F. I. (2018). LA AUDITORÍA INFORMÁTICA Y SUS DIVERSAS. *METODOAUDINF*.

Muñoz Razo, C. (2018). *Auditoría en sistemas computacionales.* Mexico: Printed in Mexico.

Navia, M. (2021). *Instrumento para la auditoría técnica de seguridad informática en pequeños* (Vol. Vol. 5 Núm. 2). Portoviejo, Manabi, Ecuador: revistas utm. doi:https://doi.org/10.33936/isrtic.v5i2.3952 | 2550-6730

Oñate, O. &. (2017). *Mejora en la red de la seguridad de la red en la universidad de Chimborazo.* Chimborazo.

Orellana López, D. M., & Sánchez Gómez, M. C. (2016). TÉCNICAS DE RECOLECCIÓN DE DATOS EN ENTORNOS VIRTUALES MÁS USADAS EN LA. *Revista de Investigación Educativa*, 205-222.

Organización Internacional para la Estandarización. (2018). *ISO / IEC 27001:2018.*

ORREGO, J. L. (2010). *SEGURIDAD EN SISTEMAS OPERATIVOS.*

Pentest Standard. (2016). Penetration Testing Execution Standard. *High Level Organization of the Standard*. Obtenido de http://www.pentest-standard.org/index.php/PTES_Technical_Guideline

Pérez Merlos, J. C. (2019). Las Metodologías de la Auditoría Informática y su relación con Buenas. *IDEAS EN CIENCIA DE LA INGENIERIA*, 42- 49.

Pérez, E. G. (1 de Agosto de 2017). *METODOLOGIAS DE AUDITORIA INFORMATICA*. Obtenido de https://silo.tips/download/metodologias-de-auditoria-informatica

Pinzon Cepeda, R. (2010). TRAZABILIDAD DE LA INFORMACION. *ReCiTeLA*, 6-9.

Rodriguez Moguel. (2015). *Metodologia de la Investigacion* (Vol. Vol. 5). Juarez.

Ruiz & López, S. A. ((2020)). *EL PORTAL DE ISO 27001 EN ESPAÑOL*. Obtenido de https://www.iso27000.es/sgsi.html#section2c

S-CERT. (2019). *S-CERT S-CERT@S-CERT.de*. Obtenido de https://www.s-cert.de/esp/#:~:text=CERT%20es%20una%20sigla%20inglesa,de%20las%20Cajas%20de%20Ahorros.

Sendón, V. J. ((2020)).

STRASSMANN, P. A. (2019). *"El arte de presupuestar: como justificar los fondos para Seguridad Informática".* Obtenido de https://nextvision.com/

TELECOMUNICACIONES, M. D. (2021). *ACUERDO MINISTERIAL 006-2021*. Obtenido de https://www.telecomunicaciones.gob.ec/:

https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

Zambrano Carolina. (agosto de 2019). Estudios de Disponibilidad Léxica en la Base de Datos Scielo y sus Aportes a Educación. *Citrevistas, vol.30*(no.4), 69-84. doi:ISSN 0718-0764

ANEXO 1

MEMORANDUM

ME-SIS-NA-103-2022

PARA: **ING. JORGE SIMBAÑA CEVALLOS**
DE: **ING. JACINTO DANIEL VERA CONFORME**
ASUNTO: SOLICITUD PARA DESARROLLO DE AUDITORIA INFORMATICA
FECHA: 11 DE ENERO DEL 2022

Mediante la presente se solicita a la empresa INDUSTRIA MASTER INDUMASTER S.A con ruc: 1390140858001, la autorización para la aplicación de una metodología de auditoria informática utilizando técnicas y herramientas de hacking ético para la evaluación de vulnerabilidades en la seguridad informática dentro de su institución, la misma que servirá para el mejoramiento de procesos de prevención ante ataque informáticos.

Esperando su aprobación me suscribo.

ATENTAMENTE:

Ing. Jacinto Daniel Vera Conforme

ANEXO 2

REPORTES NESSUS

REPORTES NMAP

REPORTES ETTHERCAP

My Basic Network Scan

Report generated by Nessus™ Tue, 03 Oct 2019 09:59:21 GMT-0500

TABLE OF CONTENIDO

Hosts Executive Summary

192.168.1.1

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	4

Vulnerabilities — Total: 27

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.8	50686	IP Forwarding Enabled
LOW	3.3	10663	DHCP Server Detection
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	11002	DNS Server Detection
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	42823	Non-compliant Strict Transport Security (STS)
INFO	N/A	11936	OS Identification
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported

192.168.1.2

INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forwa.J Secrecy Cipher Suites Supported
INFO	N/A	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	22964	Service Detection
INFO	N/A	42822	Strict Transport Security (STS) Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	10386	Web Server No 404 Error Code Check

192.168.1.3

CRITICAL	HIGH	MEDIUM	LOW	INFO
1	0	2	0	22

Vulnerabilities — Total: 25

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	12634	Authenticated Check : OS Name and Installed Package Enumeration
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	11414	IMAP Service Banner Retrieval
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection

192.168.1.4

CRITICAL	HIGH	MEDIUM	LOW	INFO
1	0	2	0	22

Vulnerabilities Total: 25

INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	18528	SMTP Server Connection Check
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

192.168.1.5

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	5

Vulnerabilities — Total: 5

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	19506	Nessus Scan Information

192.168.1. 6

0	0	4	0	23
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 27

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported

192.168.1.7

Vulnerabilities — Total: 25

INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	51891	SSL Session Resume Supported
INFO	N/A	104743	TLS Version 1.0 Protocol Detection
INFO	N/A	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	64814	Terminal Services Use SSL/TLS
INFO	N/A	10287	Traceroute Information
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10940	Windows Terminal Services Enabled

192.168.1.8

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	0	27

Vulnerabilities — Total: 28

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information

192.168.1.9

0	0	1	0	13
CRITICAL	HIGH	MEDIUM	LOW	INFO

ulnerabilities Total: 14

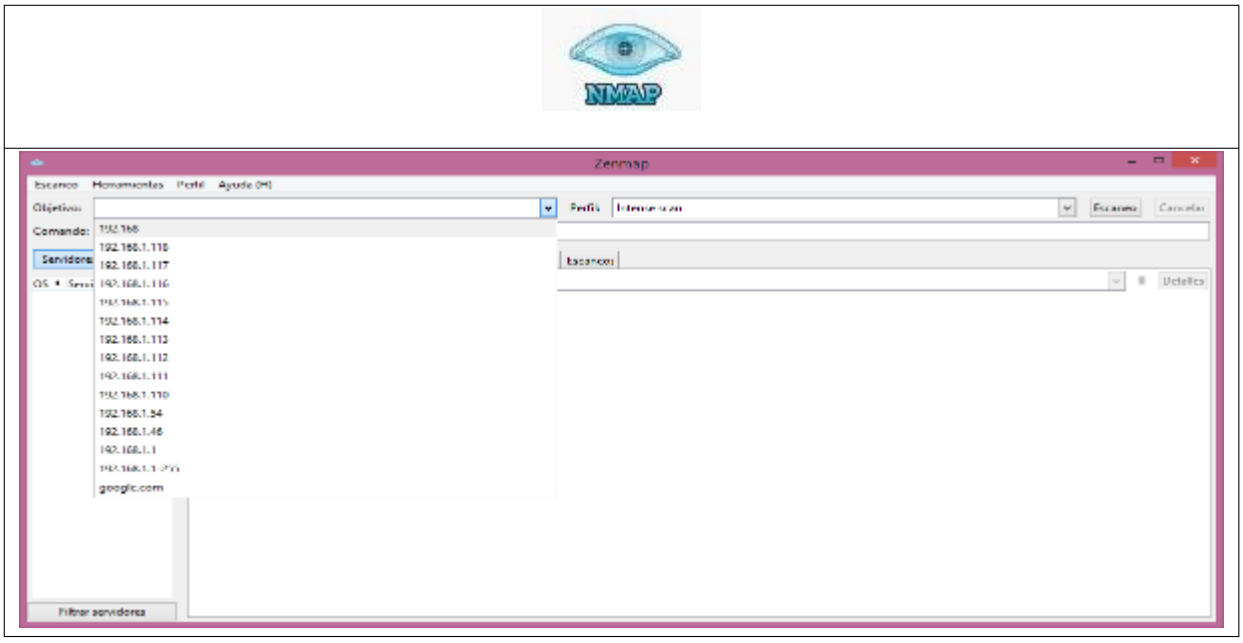
SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	10287	Traceroute Information
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

192.168.1.10

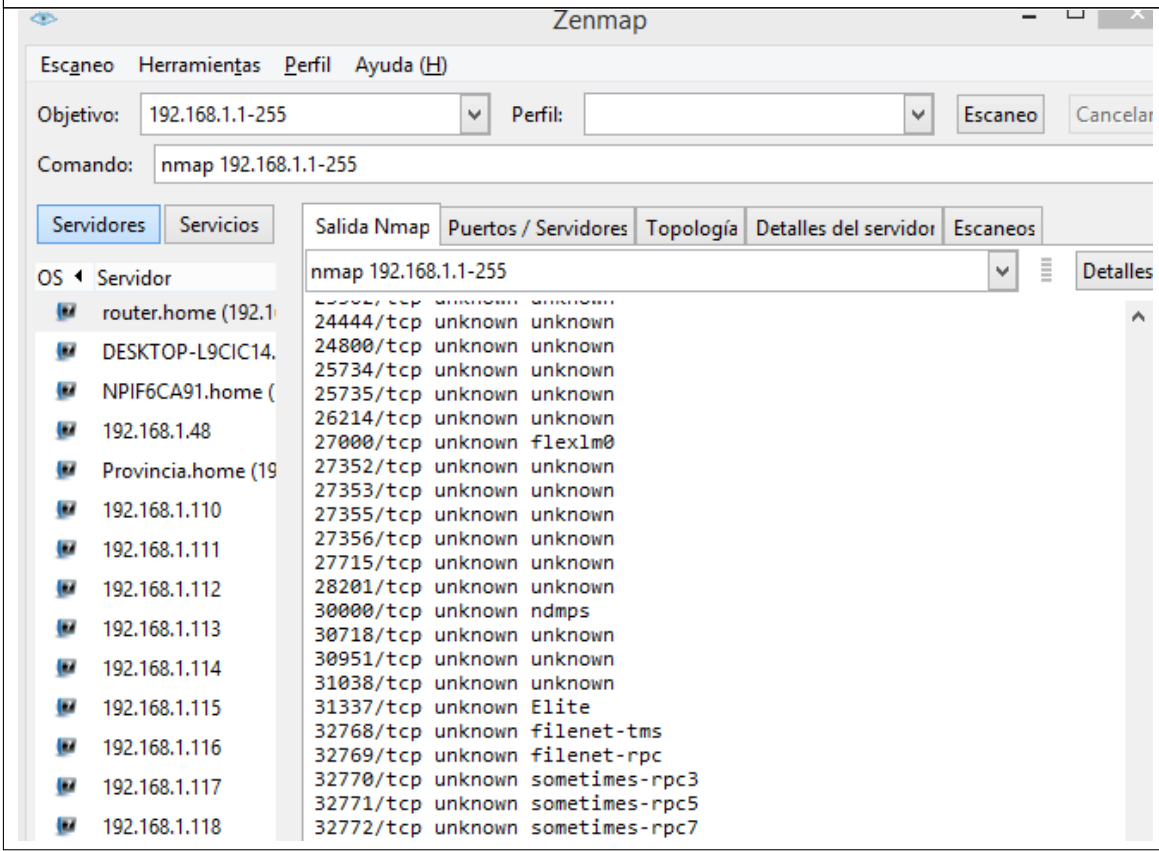
Vulnerabilities Total: 13

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	10287	Traceroute Information
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

REPORTES NMAP

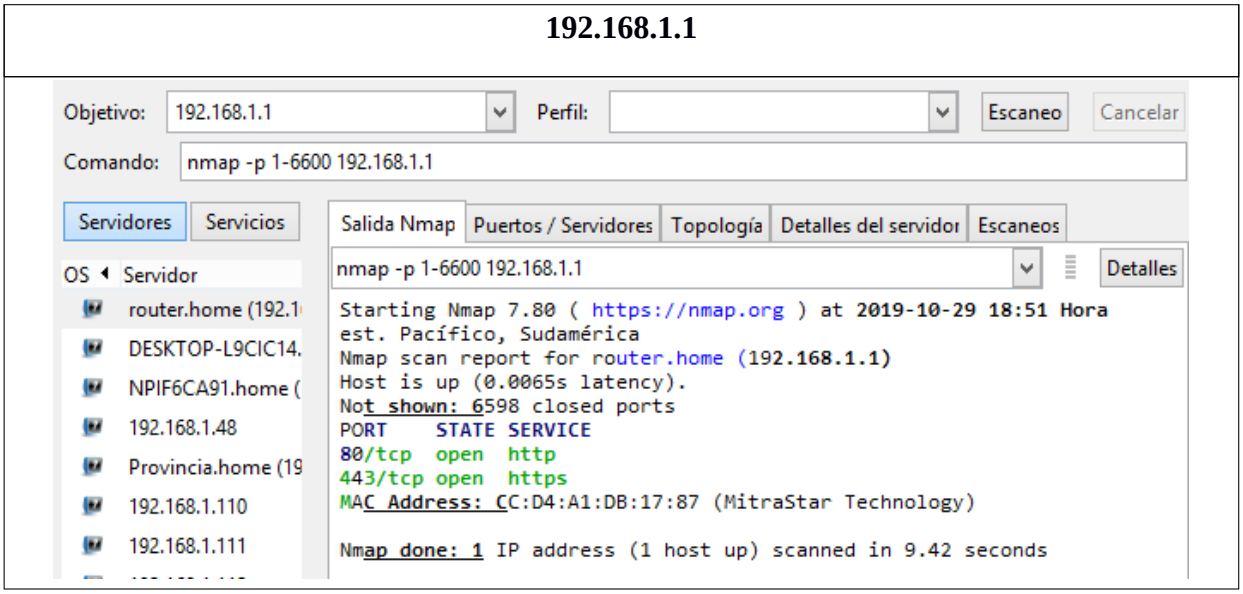


ESCANEO DE IPs EN LA RED DE DATOS

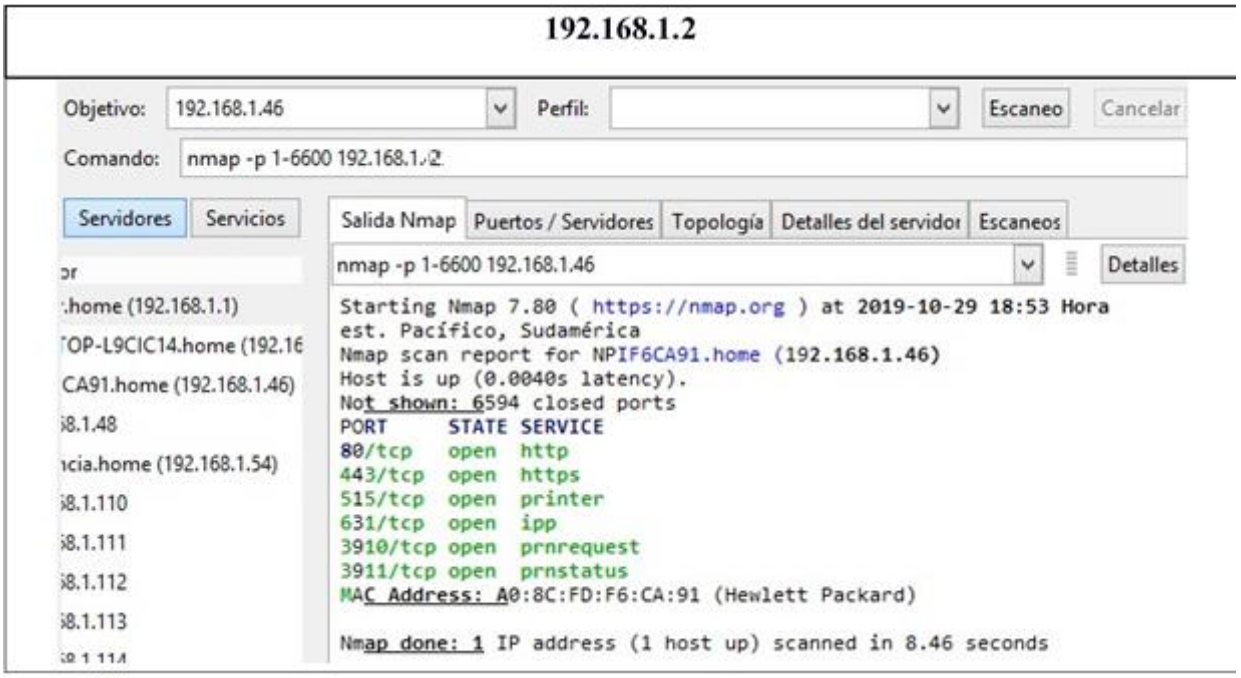


ESCANEO DE PUERTOS POR PC

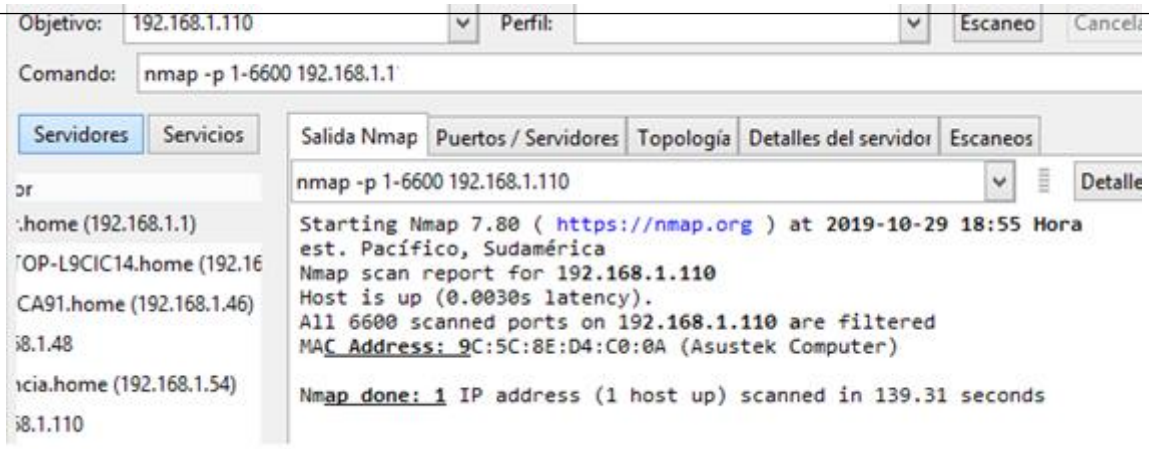
192.168.1.1



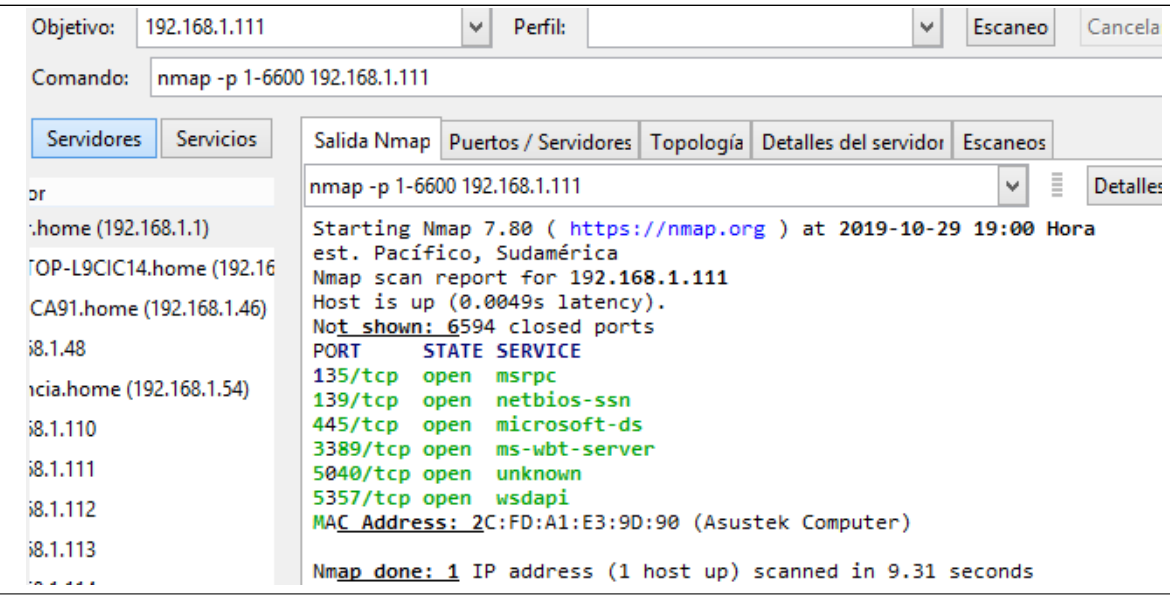
192.168.1.2



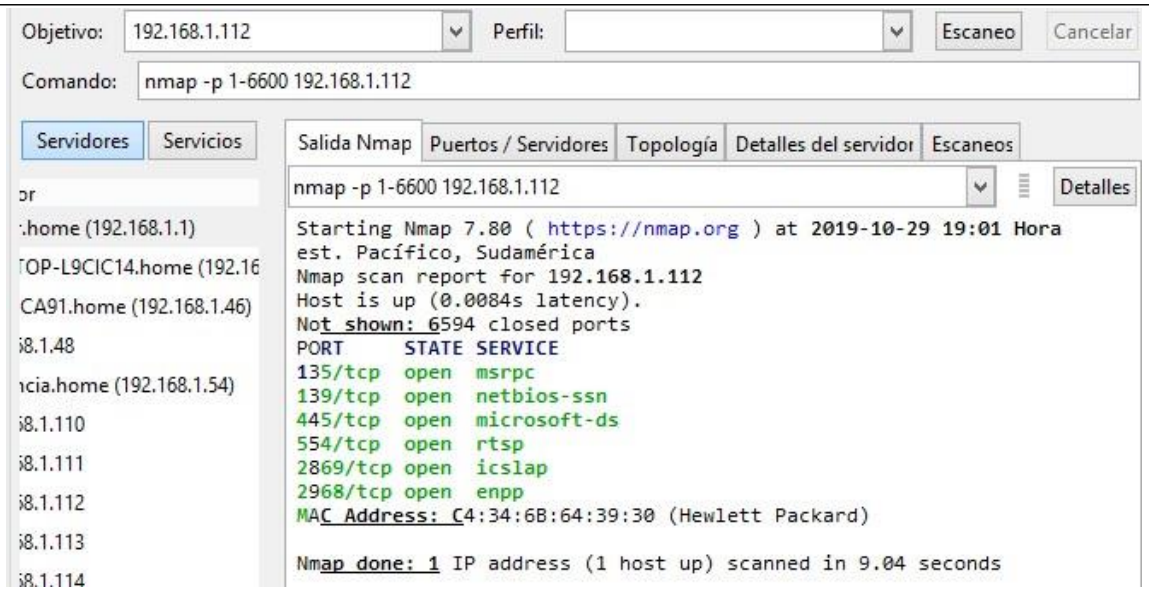
192.168.1.3



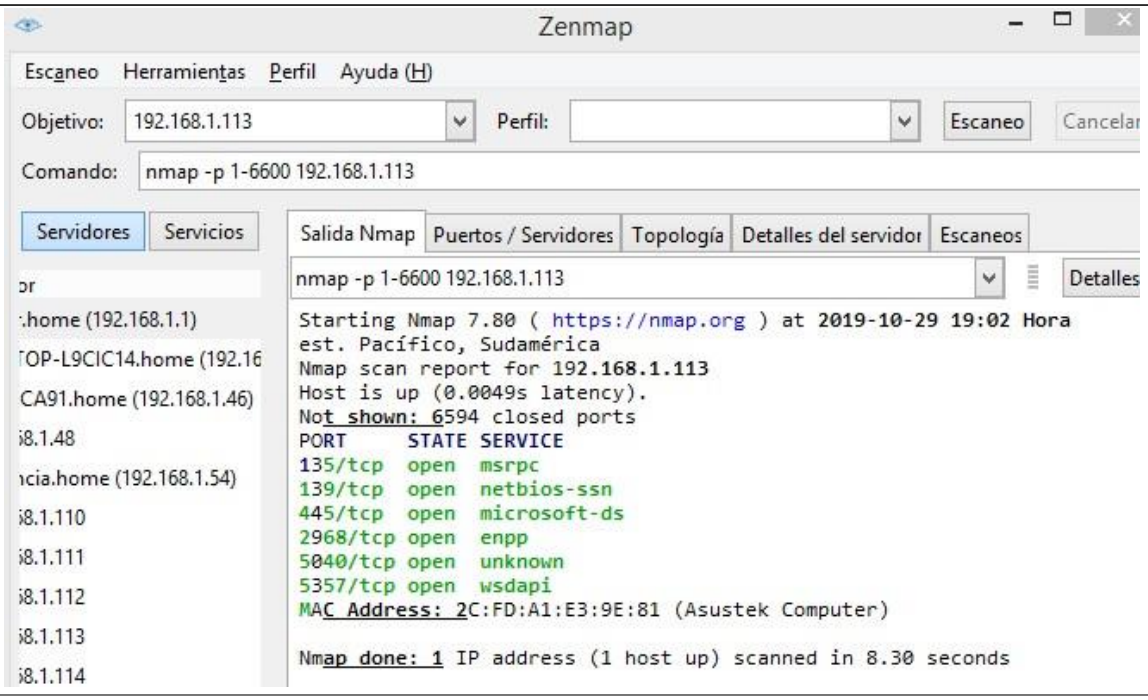
192.168.1.4



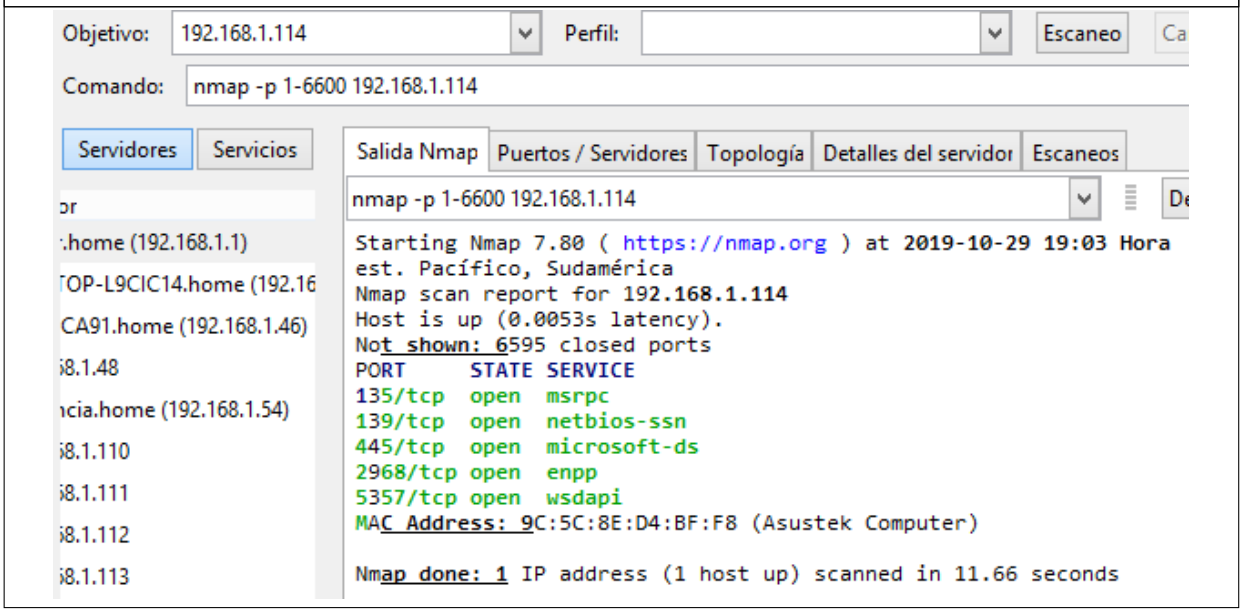
192.168.1.5



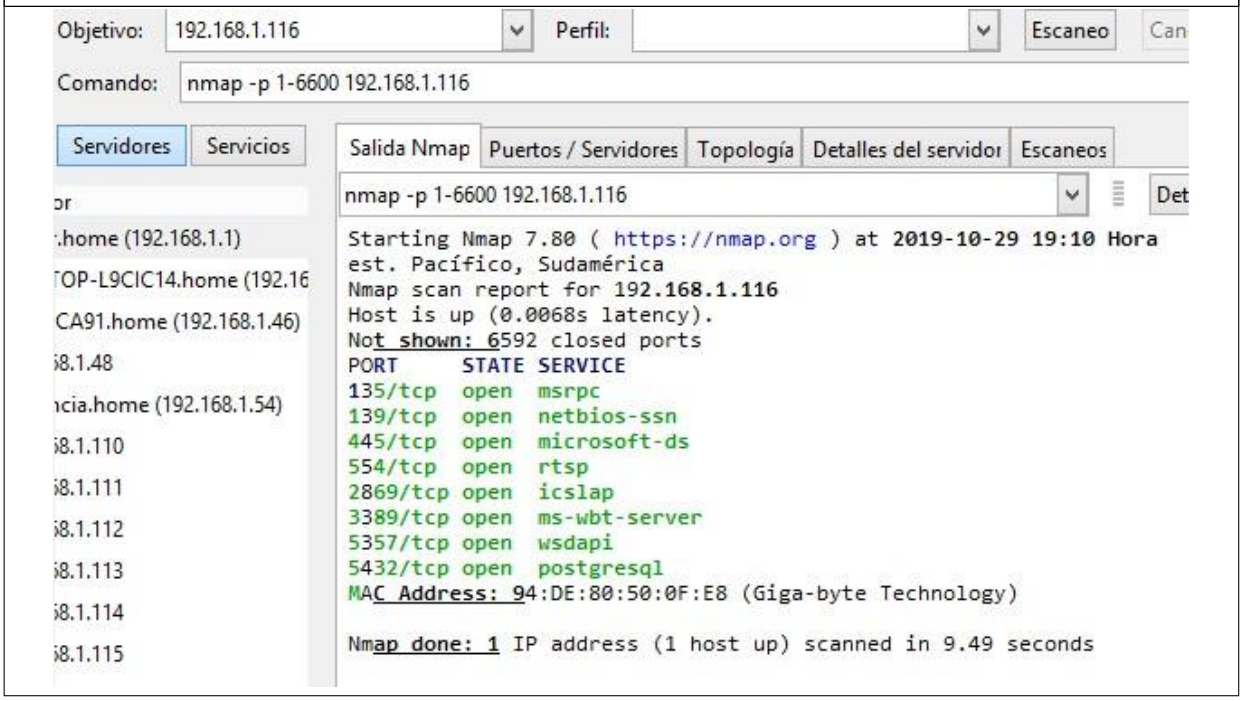
192.168.1.6



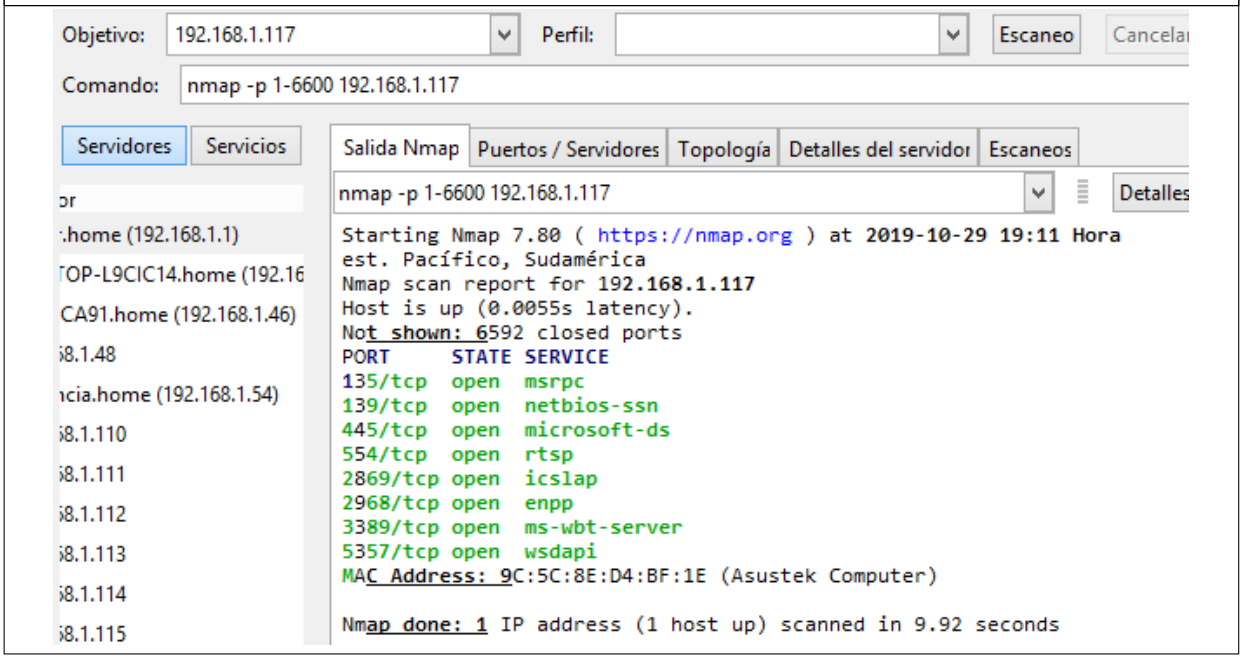
192.168.1.7



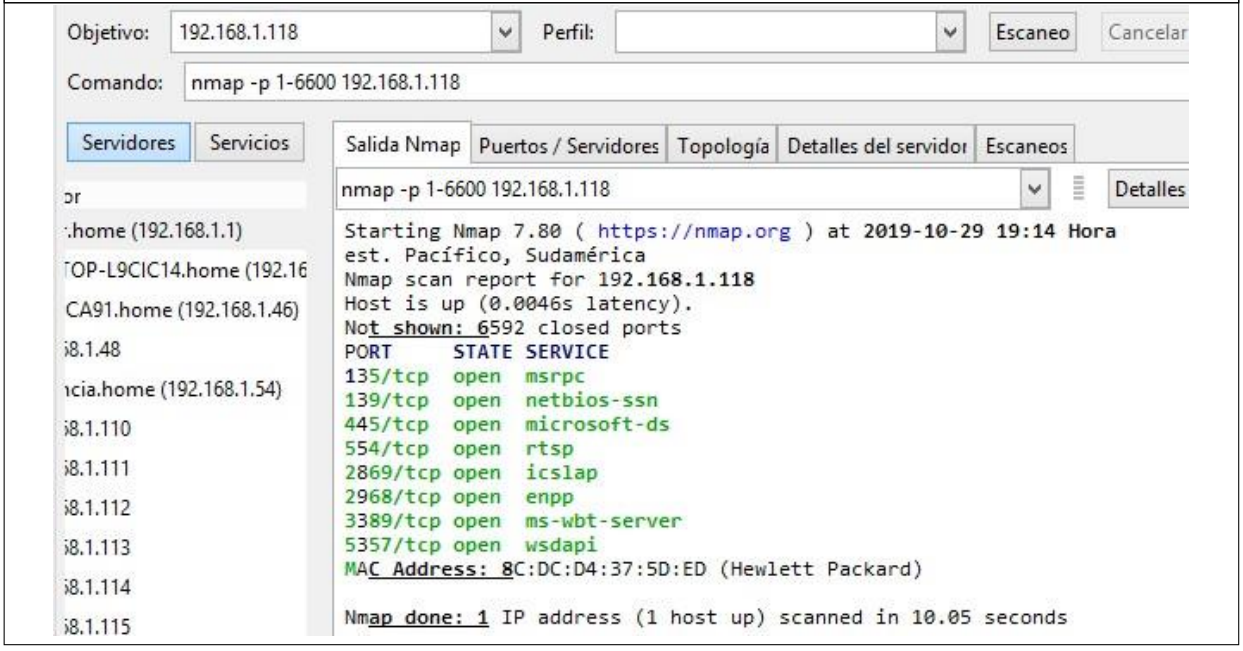
192.168.1.8

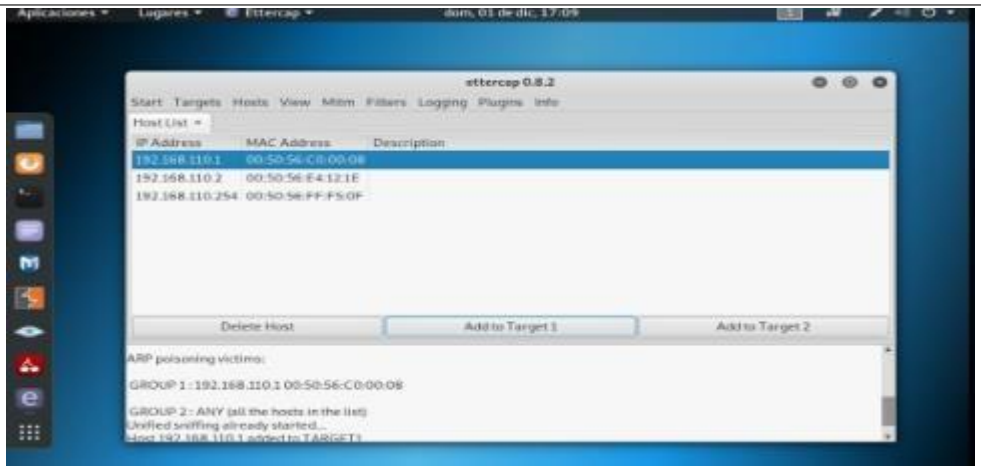


192.168.1.9



192.168.1.10





MAN IN THE MIDDLE