UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

AUDITORÍA INFORMÁTICA MEDIANTE LA METODOLOGÍA OSSTMM V3, PARA LA GESTIÓN DE LA SEGURIDAD EN LA COOPERATIVA DE TRANSPORTES FLOTA PELILEO

Trabajo de Titulación Modalidad: Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos

ÁREA: Seguridad informática.

LÍNEA DE INVESTIGACIÓN: Sistemas administradores de recursos.

AUTOR: Juan Carlos Carrazco Medina.

TUTOR: Ing. Dennis Vinicio Chicaiza Castillo, Mg.

Ambato - Ecuador

junio – 2023

APROBACIÓN DEL TUTOR

En calidad de Tutor del Trabajo de Titulación con el tema: AUDITORÍA INFORMÁTICA MEDIANTE LA METODOLOGÍA OSSTMM V3, PARA LA GESTIÓN DE LA SEGURIDAD EN LA COOPERATIVA DE TRANSPORTES FLOTA PELILEO, desarrollado bajo la modalidad Proyecto de Investigación por el señor Juan Carlos Carrazco Medina, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 de Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, junio 2023

_____

Ing. Dennis Vinicio Chicaiza Castillo, Mg.
TUTOR

AUTORÍA

El presente Proyecto de Titulación: AUDITORÍA INFORMÁTICA MEDIANTE LA METODOLOGÍA OSSTMM V3, PARA LA GESTIÓN DE LA SEGURIDAD EN LA COOPERATIVA DE TRANSPORTES FLOTA PELILEO, es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, junio 2023

Firmado electrónicamente por:
JUAN CARLOS CARRAZCO MEDINA

Juan Carlos Carrazco Medina
C.C 180469979-9
AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, junio 2023

Juan Carlos Carrazco Medina
C.C 180469979-9
AUTOR

APROBACIÓN TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por el señor Juan Carlos Carrazco Medina estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado AUDITORÍA INFORMÁTICA MEDIANTE LA METODOLOGÍA OSSTMMM V3, PARA LA GESTIÓN DE LA SEGURIDAD EN LA COOPERATIVA DE TRANSPORTES FLOTA PELIELO, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidenta de tribunal.

Ing. Elsa Pilar Urrutia Urrutia, Mg.
PRESIDENTA DEL TRIBUNAL

Ing. Víctor Guachimbosa
PROFESOR CALIFICADOR

Ing. Julio Balarezo
PROFESOR CALIFICADOR

DEDICATORIA

El presente proyecto de investigación se lo dedico a mis padres Juan y Carmen por ser un pilar importante en mi vida, a mis hermanos por su apoyo incondicional.

A mi esposa por su apoyo en cada momento y a mi hija Katheryn quien es mi inspiración para seguir cumpliendo metas.

Juan Carlos Carrazco Medina

AGRADECIMIENTO

Agradezco a Dios por guiar mi camino**,** a mis padres que gracias a su comprensión y apoyo me han permitido cumplir mis metas**.**

A mi tutor, el Ingeniero Dennis Chicaiza, por su apoyo brindado.

A los docentes de la carrera de Sistemas por compartir sus conocimientos en todo este tiempo como estudiante.

A la Cooperativa de Transportes Flota Pelileo por su apoyo para la realización del presente proyecto de investigación.

Juan Carlos Carrazco Medina

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

El presente proyecto de investigación está dirigida a la Cooperativa de Transportes Flota Pelileo, que tiene como objetivo realizar una auditoria informática para determinar vulnerabilidades e incidentes que involucren la fuga o pérdida de información, siendo esto de vital importancia para la continuidad de los servicios que presta la empresa.

Para ello se utiliza la metodología OSSTMM ya que presenta una planificación de ejecución y verificación de la seguridad en entornos informáticos, cada una de las secciones de la metodología proporciona módulos de ayuda para el desarrollo del análisis de seguridad, se toma la Sección Seguridad de la Información y los módulos: Revisión de la Inteligencia Competitiva, Revisión de la Privacidad y Recolección de Documentos, Sección Seguridad de las Tecnologías de Internet y los módulos: Sondeo de la Red, Identificación de Servicios y Sistemas, Búsqueda y Verificación de Vulnerabilidades. Con los resultados obtenidos de este análisis se establecerá medidas de seguridad que nos permitan minimizar riesgos en la operatividad evitando así la fuga de información lo que puede desencadenar en daños incalculables para la Cooperativa de Transportes Flota Pelileo.

Palabras clave: TI, metodología, OSSTMM, evaluación, políticas.

ABSTRACT

This research project is aimed at the Cooperativa de Transportes Flota Pelileo, whose objective is to carry out a computer audit to determine vulnerabilities and incidents that involve the leakage or loss of information, this being of vital importance for the continuity of the services it provides. the company.

For this, the OSSTMM methodology is used since it presents a planning of execution and verification of security in computer environments, each of the sections of the methodology provides help modules for the development of security analysis, the Security Section of the Information and modules: Competitive Intelligence Review, Privacy Review and Document Collection, Internet Technology Security Section and modules: Network Survey, Identification of Services and Systems, Search and Vulnerability Verification. With the results obtained from this analysis, security measures will be established that allow us to minimize risks in the operation, thus avoiding the leakage of information, which can trigger incalculable damage for the Cooperativa de Transportes Flota Pelileo.

Keywords: IT, methodology, OSSTMM, evaluation, politics.

CAPÍTULO I

MARCO TEÓRICO

1.1 Tema de investigación

AUDITORÍA INFORMÁTICA MEDIANTE LA METODOLOGÍA OSSTMM V3, PARA LA GESTIÓN DE LA SEGURIDAD EN LA COOPERATIVA DE TRANSPORTES FLOTA PELILEO

1.2 Antecedentes investigativos

Revisando la investigación bibliográfica en algunas universidades del Ecuador se han encontrados trabajos que servirán de apoyo en el trabajo de investigación:

En la Universidad Politécnica Salesiana, Fabricio Zavala en su proyecto "Diseño e Implementación de Seguridades en la Red de Datos de la Planta Central del Ministerio de Educación y Cultura del Ecuador, aplicando la tecnología OSSTMM" en el año 2010 recomienda que, para mantener un nivel alto de seguridad hay que estar constantemente investigando nuevas herramientas de seguridad y analizar los resultados, además un elemento fundamental son las políticas de seguridad planteadas, las mismas que se deben cumplir a cabalidad sin excepción alguna ya que solo basta uno que no cumpla para que la seguridad quede vulnerada. Las conexiones remotas no deben realizarse como administradores deben realizarse como usuarios de conexión y una vez ingresado darse privilegios [1].

En la Universidad Técnica de Ambato, Gloria Huilca en su proyecto "Hacking Ético para

detectar vulnerabilidades en los servicios de la intranet del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos" en el año 2012. Menciona que, "el objetivo principal de la aplicación de hacking ético es descubrir las deficiencias relativas a seguridad y las vulnerabilidades de los sistemas informáticos, analizarlas, calibrar su grado de riesgo y peligrosidad, y recomendar las posibles soluciones más apropiadas para cada una de ellas. Recomienda considerar la importancia y sensibilidad de la información y servicios críticos de la intranet por lo que es necesario establecer políticas de seguridad dentro de la institución" [2].

En la Universidad Técnica de Ambato, Christian Miranda Silva en su proyecto "Auditoría de redes, aplicando la metodología OSSTMM V3, para el Ministerio de Inclusión Económica y Social" en el año 2019 concluye que "el buen ejercicio de una empresa obedece a la eficiencia de su red y sus sistemas informáticos; una empresa puede tener gente de primera, pero si posee una red propensa a fallos, vulnerable e inestable y si no hay un equilibrio entre estas dos cosas, la empresa nunca podría brindar un servicio de calidad" [3].

En la Universidad Técnica de Ambato, Joel Allaica Caranqui en su proyecto "Auditoría de la Seguridad Informática siguiendo la metodología OPEN SOURCE SECURITY TESTING METHODOLOGYMANUAL (OSSTMM) para la empresa MEGAPROFER S.A" en el año 2020 recomienda "mejorar las políticas de contingencia de seguridad informática planteadas con fin de mantener el óptimo funcionamiento de sus servicios y ayuden al cumplimiento de las metas empresariales. Estas deben ser actualizadas constantemente basado en la evolución de la tecnología" [4].

1.2.1 Contextualización del problema

"A nivel mundial la auditoria informática juega un papel relevante ya que permite mostrar el estado en el que se encuentra la protección de la información y de los activos dentro de

las organizaciones. Además, involucra la identificación, análisis y evaluación de debilidades en las medidas de seguridad que han sido aplicadas, así como de los componentes tecnológicos de la empresa" [5].

"En el caso específico de las redes, la auditora está relacionada con un método o un conjunto de ellos para verificar el cumplimiento de los requisitos de seguridad" [5]. Es necesario verificar que se cumplan los requisitos de seguridad dentro de una colección de dispositivos interconectados como pueden ser routers, switches, hubs, computadoras y dispositivos móviles, entre otros.

"En cuanto a nivel nacional en Ecuador en la Universidad Central del Ecuador el diseño y aplicación del procedimiento de auditora ha permitido comprobar la vulnerabilidad desde el punto de vista práctico, en cuanto a la madurez de las capacidades de los procesos clasificados como primarios en la seguridad de las redes LAN arrojando resultados desfavorables. Se demostró que su aplicación contribuyo a la realización de recomendaciones necesarias para el mejoramiento de la seguridad de la red LAN de los laboratorios de computadoras de la Facultad de Ingeniería Ciencias Físicas y Matemática de la Universidad" [6].

Al realizar evaluaciones de auditoría en seguridad de las redes LAN tanto como en laboratorios de computadoras o empresas completas, se despierta el interés del personal administrativo, lo cual es favorable porque se genera un ambiente de conciencia para seguir con las normas establecidas.

La Cooperativa de Transportes Flota Pelileo tiene como misión ser líder y trabajar día a día para alcanzar un nivel de calidad que agregue valor y seguir contribuyendo con la sociedad en el servicio de boletería y encomiendas.

El gerente de la Cooperativa de Transportes Flota Pelileo se encuentra interesado en conocer los posibles ataques hacia la Cooperativa, por motivo de que la información diariamente es manipulada de suma importancia y en el mayor de los casos confidencial, la cual no le gustaría perder o en el peor de los casos que se divulgue, así que le gustaría saber qué medidas debería tomar, por lo cual la Cooperativa necesita una auditoria para detectar posibles vulnerabilidades que pueda tener la red y de esta manera determinar las medidas necesarias a tomar para evitar algún tipo de ataque y mejorar la eficiencia de la red.

1.2.2 Fundamentación teórica

Auditoría

"Es la revisión independiente de alguna o algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre la racionabilidad de sus resultados y el cumplimiento de sus operaciones" [7].

Auditoria Informática

"Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo. El propósito fundamental es elevar el uso adecuado de los sistemas para el correcto ingreso de los datos,

el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa" [7].

Seguridad

"Protección de los bienes personales y del negocio, a través del uso de controles de seguridad que restringen y gestionan el movimiento de personas y equipos" [8].

Auditoría de Seguridad Informática

"Una auditoría de seguridad informática es una evaluación de los sistemas informáticos cuyo fin es detectar errores y fallas mediante un informe detallado que se entrega al responsable en el que se describe:

- Equipos instalados, servidores, programas, sistemas operativos.
- Procedimientos instalados
- Análisis de Seguridad en los equipos y en la red
- Análisis de la eficiencia de los Sistemas y Programas informáticos
- Vulnerabilidades que pudieran presentarse en una revisión de las estaciones de trabajo, redes de comunicaciones, servidores" [9].

Pruebas de Penetración (PenTest)

"Una prueba de penetración es una operación cuyo propósito es evaluar la seguridad de alguna infraestructura de TI al explotar sus debilidades y vulnerabilidades del mismo

modo que lo haría algún hacker mediante los sistemas operativos, servicios, aplicaciones, configuraciones inapropiadas o comportamiento del usuario final" [10].

Escáner de Vulnerabilidades

"Herramientas de análisis para los equipos de toda la red. Determinan servicios que se están ejecutando en un equipo remoto" [11].

Herramientas de análisis

NMAP: "Es un explorador de redes y puertos orientado a las auditorias de seguridad" [12].

Maltego: "Es una herramienta de código abierto creado por Paterva para el análisis y la visualización de las conexiones de datos, utiliza un sistema de entidades sobre las cuales se pueden realizar transformaciones y así obtener mayor información de la misma (dispositivos, DNS, servidores de correo, ips, tecnologías aplicadas, documentos, números telefónicos, correos, etc.)" [13].

Buscador web de Google: "Buscador web de Google, es el primer producto de la empresa Google Inc. y producto estrella de ´esta. En ´él se pueden realizar búsquedas de webs por la W.W.W. a base de un algoritmo exclusivo. Es el buscador más utilizado por la clasificación de páginas web que realiza y sus opciones de búsqueda avanzada" [14].

VisualRoute: "Esta herramienta permite de una manera gráfica localizar los sitios por donde fluye una información hasta llegar a un destino. Es útil para localizar por donde pasa la información y desde donde se inicia a partir de una dirección web o una IP. Con

esta herramienta podemos localizar el servidor de una web, lo que nos permite por tanto investigar si es fiable o no. Además, permite realizar ping, tracer routers y realizar Whois" [15].

TheHarvester: "El objetivo de este programa es reunir a los correos electrónicos, subdominios, hosts, nombres de empleados de diferentes fuentes públicas, como los motores de búsqueda, los servidores de base de datos informáticas. Esta herramienta está diseñada para ayudar a los probadores de penetración en las primeras etapas de la prueba de penetración a fin de comprender la huella de cliente en el Internet.

También es útil para cualquier persona que quiere saber lo que un atacante puede ver sobre su organización" [16].

OpenVAS: "El Sistema de Evaluación de Vulnerabilidad abierto (OpenVAS) es un marco de diversos servicios y herramientas que ofrecen una solución completa y potente de análisis de vulnerabilidades y gestión de vulnerabilidades" [17].

Nessus: "Es un analizador de seguridad de redes potente y fácil de usar, con una amplia base de datos de plugins que se actualiza a diario. Nessus es creado por Tenable Network Security Inc., el cual mejora permanentemente el motor Nessus, diseña plugins para el analizador y directivas de auditoria" [18].

Vega: "Vega es un escáner de vulnerabilidades de código abierto y gratuito. Según sus propias palabras, Vega puede usarse "para pruebas rápidas y un proxy interceptor para inspección táctica. El escáner Vega encuentra XSS (cross.site scripting), inyección de SQL y otras vulnerabilidades. Vega se puede extender usando un poderoso API en el lenguaje de la web: JavaScrip" 19].

“VEGA incluye un escáner automatizado para ejecutar verificaciones rápidas además de un proxy de interpretación para la inspección táctica. El escáner de VEGA encuentra XSS (cross-site scripting), inyección de SQL y otras vulnerabilidades [20].

Metasploit Framework: “Es un framework desarrollada en Perl y Ruby en su mayor parte, que provee información acerca de debilidades o vulnerabilidades de seguridad informática y ayuda a la ejecución de pruebas de penetración, está desarrollado en lenguaje de programación Ruby y es software libre, también cuenta con interfaces las cuales se pueden utilizar para la explotación de vulnerabilidades” [21].

Hping3: “Es un software orientado a la auditoria de la pila TCP / IP, para descubrir la política cortafuegos, para escanear los puertos TCP de diferentes modos, para transferir archivos a través de un servidor de seguridad y muchas otras cosas” [22].

Hydra: “Es un software que permite realizar rápidos ataques de diccionario contra varios protocolos en los que incluyen telnet, ftp, http, https, smb, ssh, varias bases de datos, y mucho más” [23].

Iptables: “Es la entrada de seguridad en una serie de servicios de firewall y administración de sistemas Linux, iptables es un producto de seguridad de uso generalizado mediante reglas” [24].

Sslstrip: “Es un programa para sistemas operativos linux capaz de descifrar trafico https que viaja a través de una red” [25].

Medusa: “Es otro cracker de contraseñas en línea para servicios de red. Tiene Las características de ser veloz, masivamente paralelo y modular. Actualmentete, cuenta con módulos para los siguientes servicios: CVS, FTP, HTTP, IMAP, MS-SQL, NCP

(NetWare), PcAnywhere, POP3, PostgresSQL, rexec, Rlogin, rsh, SMB, SMTP (VRFY), SNMP, SSHv2, SVN, Telnet, VmAuthd, VNC y un módulo envoltorio genérico" [26].

"Medusa está destinada a ser una fuerza bruta de inicio de sesión rápida, masivamente paralela, modular. El objetivo es admitir tantos servicios que permitan la autenticación remota como sea posible" [11].

Kali Linux: "Es un Sistema Operativo orientado a la auditoria y seguridad informática en general. Distribución avanzada para Pruebas de Penetración, Hacking Ético y evaluaciones de la seguridad de la red" [27].

Hacking Ético: "Disciplina la cual está orientada a la búsqueda de vulnerabilidades ya sea en la red y aplicaciones para usarlas a beneficio de la misma empresa" [11].

Políticas: "Las políticas son instrucciones gerenciales que trazan una dirección predeterminada o describen la manera de manejar un problema o situación.

Se puede definir también como planteamientos de alto nivel que transmiten a los trabajadores la orientación que necesitan para tomar decisiones presentes y futuras.

Otro concepto que se puede dar, son requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas dentro, y en algunos casos fuera, de la organización. Las políticas también pueden considerarse como reglas de negocio" [28].

Contingencia: "La contingencia es el modo de ser de lo que puede suceder o no, especialmente de un problema que se plantea de forma imprevista" [29].

Plan de Contingencia: "Un plan de contingencias es un instrumento de gestión inmediata de las Tecnologías de la Información y las Comunicaciones en relación al soporte y el desempeño" [30].

Metodología: "Es un conjunto de procedimientos racionales utilizados para alcanzar una gama de objetivos que rigen una investigación científica, una exposición doctrinal o tareas que requieran habilidades, conocimientos o cuidados específicos" [31].

En la actualidad existen varias metodologías que permiten el desarrollo de una auditoría informática entre ellas Octave, ITIL, OSSTMM, etc.

OSSTM (Manual de la Metodología Abierta de Testeo de Seguridad)

"OSSTMM es una metodología estandarizada para una verificación y medición exhaustivas del estado operativo y de seguridad actual. En realidad, es una gran cantidad de charlas académicas para decir que el OSSTMM lo ayudará a realizar una prueba de seguridad de acuerdo con una receta que le permite no solo ejecutar la mejor prueba posible que puede generar de la manera más eficiente (ahorrando tiempo ahorra dinero), pero eso también le da números que representan de manera realista su nivel actual de seguridad" [32].

Secciones y Módulos de OSSTMM

Está formada por 6 ítems los cuales comprenden todo el sistema actual, estas son:

1. **Seguridad de la Información**

En esta sección se revisa la privacidad de los empleados mediante la recolección de información en internet, esta información es analizada en busca de datos que puedan considerarse como privados y no deberían estar expuestos al exterior.

- **Revisión de la Inteligencia Competitiva:** información recolectada a partir de la presencia en Internet.
- **Revisión de la Privacidad:** punto de vista legal y ético del
- almacenamiento, transmisión y control de los datos basados en la privacidad del empleado.
- **Recolección de Documentos:** en este módulo es importante la verificación de la información obtenida y perteneciente a varios niveles de lo que se considera seguridad de la información.

2. **Seguridad de los Procesos**

Esta sección realiza pruebas en las cuales se pueda tener algún acceso o privilegio mediante el uso de equipos de comunicación y la información de la sección anterior.

- **El testeo de solicitud:** Busca obtener privilegios de acceso a una empresa y sus activos mediante preguntas al personal de acceso, a través de diversos métodos teniendo como principal la ingeniería social. La Ingeniería Social tiene un papel fundamental en una gran cantidad de ciberataques, más allá de lo grande, pequeño o sofisticado que sea el crimen. Tal es el punto que siempre se ha mantenido como "una constante a lo largo de toda la historia de la seguridad de Internet".

- **El testeo de seguridad dirigida:** Es la detección de puntos de accesos privilegiados de una organización a través del teléfono, e-mail. Chat, etc. Convirtiéndose en otra rama de la ingeniería social por ende tienen gran relación con los módulos anteriores, la principal diferencia es que para este caso en cuestión

el atacante se hace pasar por otro individuo.

- **El testeo de las personas confiables:** Es un método el cual busca obtener acceso a la empresa a través de personas de confianza tales como un empleado o socio o alguna persona interna, con el fin de recabar información. Este aparato evidencia si existe algún camino o privilegio libre mediante la utilización de equipos de comunicación sumadas los datos recolectados del aparato anterior.

3. **Seguridad de las Tecnologías de Internet**

Esta sección identifica los servicios de los servidores en cuestión y aplicaciones de internet en busca de vulnerabilidades para luego de detectarlas proceder a explotarlas y generar su posible solución. También se realiza pruebas dirigidas en lo referente a peticiones de internet y sistemas de detección de intrusos

- **Sondeo de la Red:** introducción a los sistemas a estudiar, se encuentra el número de sistemas alcanzables que deben ser analizados sin exceder los límites legales.

- **Identificación de Servicios y Sistemas:** prueba invasiva de los servicios y puertos del sistema en los niveles de transporte y red.

- **Búsqueda y Verificación de Vulnerabilidades:** se identifica y verifica las debilidades, errores de configuración y vulnerabilidades en un servidor o en una red.

4. **Seguridad en las comunicaciones.**

Esta sección realiza pruebas en los dispositivos de comunicación como son VoIP, FAX, Correo de voz, PBX.

5. **Seguridad inalámbrica.**

Se evalúan dispositivos que ofrecen comunicación sin cables, el objetivo es buscar configuraciones por defecto o comunicaciones inalámbricas inadecuadas.

6. **Seguridad Física.**

Esta sección evalúa la seguridad física de la institución como son los controles de acceso, monitoreo mediante cámaras de seguridad, respuesta de alarmas ante amenazas o catástrofes.

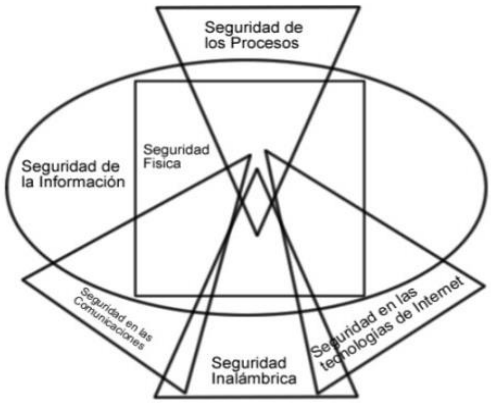


Figura 1: Mapa de seguridad OSSTMM

Fuente: Metodología OSSTMM

Ventajas de OSSTM

- Se integra y toma en consideración todos los estándares de seguridad de la información.
- Ofrece una calidad incuestionable de resultados.

Desventajas de OSSTM

- No hace referencia a que tipos de objetivos son ligados para cada test de penetración.
- No permite combinar su metodología con otra.

Ámbito y alcance de OSSTM

"El ámbito de aplicación de OSSTMM está orientado hacia cualquier tipo organización, independientemente del tamaño, tecnología o medidas de seguridad. La aplicabilidad de la metodología engloba cualquier entorno donde se requieran aspectos de seguridad, ya sea la seguridad física, la de los procesos, la de las comunicaciones y la del espectro electromagnético índice" [13].

1.3 Objetivos

1.3.1 Objetivo General

Implementar una Auditoria de la Seguridad Informática para la Cooperativa de Transportes Flota Pelileo mediante la Metodología OSSTMM V3.

1.3.2 Objetivos Específicos

- Realizar el análisis situacional del área de Tecnologías de la Información de la Cooperativa de Transportes Flota Pelileo.
- Realizar un análisis, planificado y metódico de los mecanismos de protección internos y externos para la seguridad de la red de la Cooperativa de Transportes Flota Pelileo.

- Identificar las vulnerabilidades de los servidores de la red informática que puedan ser explotadas por intrusos malintencionados.
- Elaborar un escenario para la simulación de ataques programados al servidor de la red informática para explotar las vulnerabilidades que puedan ser utilizadas por los intrusos malintencionados.
- Determinar políticas de contingencia de seguridad informática que mejore la integridad, confiabilidad y disponibilidad de la información

CAPÍTULO II

METODOLOGÍA

2.1 Materiales

- Entrevista
- Encuesta
- Observación

2.2 Métodos

Modalidad de la investigación

Investigación de campo

La presente modalidad es considerada ya que se acudió a la Cooperativa de Transportes Flota Pelileo y se realizó el conocimiento de la situación actual, recolectando información, por medio de técnicas e instrumentos para el propósito. Las técnicas utilizadas fueron: entrevista, encuesta y la observación.

Investigación bibliográfica y documental

Se realizó una investigación bibliográfica y documental obteniendo información valiosa para el sustento del presente proyecto, también se recurrió a fuentes obtenidas de libros, artículos, tesis desarrolladas en Universidades, con el objetivo de profundizar enfoques con respecto al tema que sirvió en el proceso de la investigación**.**

2.3 Población y muestra (en caso de requerir)

Para el presente proyecto de investigación no se requiere de población y muestra, se realizó entrevista al encargado de la TI y una encuesta al personal de la Cooperativa de Transporte Flota Pelileo.

2.4 Recolección de Información

Para conocer la situación actual de la Cooperativa de Transportes Flota Pelileo se acudió a las instalaciones de la misma donde se utilizó los métodos de la observación, la entrevista al encargado de la TI y una encuesta realizada a gerencia, presidencia, departamento contable y 17 oficinas de la Cooperativa de Transporte Flota Pelileo, obteniendo información precisa, clara, también se hará uso de proyectos de investigación, para así poder cumplir con los objetivos planeados.

2.5 Procesamiento y Análisis de Datos

Una vez terminada el proceso de recolección de información mediante la observación entrevista y encuesta se procederá con el análisis de los resultados.

El procesamiento de datos se lo efectuara utilizando una herramienta informática a fin de organizarlo a través de gráficos de tal forma que permita observar el nivel de importancia que tiene la realización esta auditoría de red.

CAPÍTULO III

RESULTADOS Y DISCUSIÓN

3.1 Desarrollo de la propuesta

Entrevista

Fue aplicada al encargado de la TI.

Objetivo: Conocer la situación actual de la Cooperativa y así descubrir los problemas que presenta.

1. **¿Cuentan con algún tipo de servidor?**

Sí, tenemos un solo servidor que es utilizado para el sistema de facturación para boletería y encomiendas de la Cooperativa de Transportes Flota Pelileo.

2. **¿Las instalaciones de cableado y oficinas fueron diseñadas para su funcionamiento?**

No, solo son adaptaciones.

3. **¿Se cuenta con un inventario de todos los equipos que integran la red informática?**

No existe ningún tipo de documentación, manuales.

4. **¿Cada cuánto tiempo se brinda mantenimiento preventivo a los equipos informáticos?**

Cada que los equipos presentan fallos ya que no se cuenta con ninguna planificación de mantenimiento.

5. **¿La habitación del servidor cuenta con un sistema de refrigeración?**

No, el espacio donde está el servidor es inadecuado en cuanto a temperatura y espacio.

6. **¿Qué sistemas informáticos tiene bajo su cargo o responsabilidad?**

El área de Sistemas es responsable del mantenimiento de equipos, soporte al personal.

7. **¿Se tienen instalado programa antivirus corporativo en la Cooperativa con sus respectivas licencias?**

No posee ningún tipo de antivirus.

8. **¿Se identifican los tipos de usuarios, sus responsabilidades, permisos y restricciones?**

No, las responsabilidades, permisos y restricciones no son asignados de manera específica.

9. **¿Se tienen instalados aplicaciones en cada equipo con sus respectivas licencias?**

No, solo se utiliza piratas.

10. **¿El sistema operativo que se maneja se revisa y actualiza el Software Instalado frecuentemente?**

No, ya que el sistema operativo es pirata.

Encuesta

Fue aplicada a 20 personas de la Cooperativa de Transportes Flota Pelileo.

Objetivo: Conocer la situación actual de la Cooperativa y así detectar los problemas que presenta.

1. **¿Se cuentan con algún tipo de control de entradas y salidas del personal de la Empresa?**

Tabla 1: Pregunta No. 1

Ítems	Frecuencia	Porcentaje
Si	0	0%
No	20	100%
Total	20	100%

Elaborado por: El investigador.

Fuente: Cooperativa de Transportes Flota Pelileo.

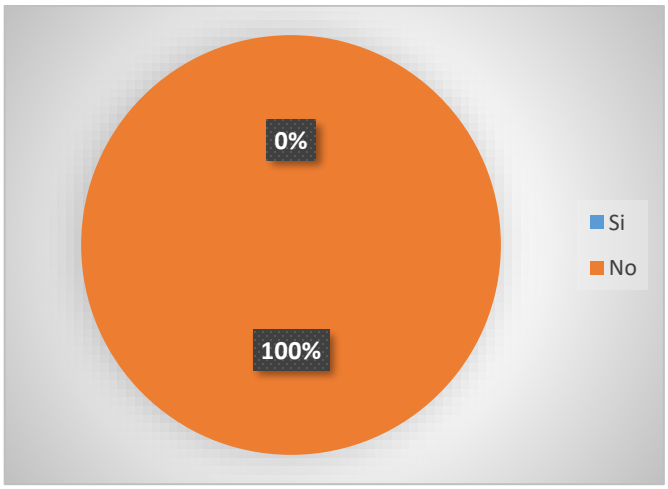


Figura 2: Pregunta 1 de la encuesta.

Elaborado por: El Investigador

Análisis: El 100 % de encuestados menciona que no cuentan con ningún tipo de software que controle las salidas y entradas del personal. Este tipo de controles es beneficioso para la Cooperativa ya que tiene una función de seguridad, con esto se controlaría quién ha tenido acceso a las instalaciones a lo largo de la jornada.

2. **¿Sus contraseñas están compuestas de una combinación de: números, letras mayúsculas, minúsculas y caracteres especiales?**

Tabla 2: Pregunta No. 2

Ítems	Frecuencia	Porcentaje
Si	8	40%
No	12	60%
Total	20	100%

Elaborado por: El investigador.

Fuente: Cooperativa de Transportes Flota Pelileo.

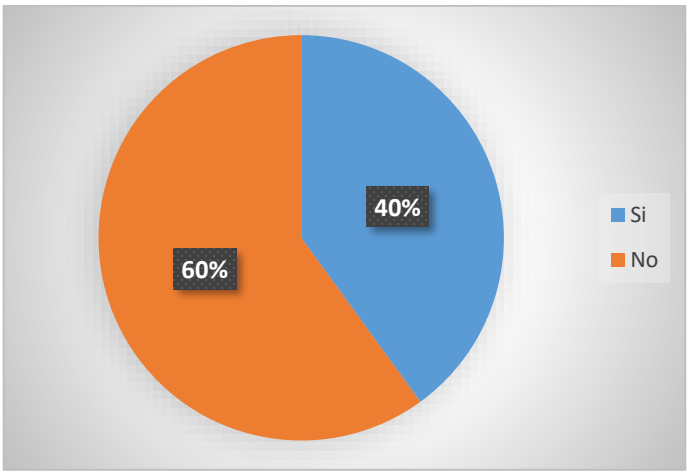


Figura 3: Pregunta 2 de la encuesta.

Elaborado por: El Investigador

Análisis: El 60 % de los encuestados cumplen con todos los parámetros, mientras que el 40% indica que no sigue este parámetro para las contraseñas, esto es muy importante ya que una contraseña segura ayuda a preservar la privacidad de los datos.

3. **¿Su equipo de trabajo cuenta con internet? de ser el caso ¿cómo califica el servicio?**

Tabla 3: Pregunta No. 3

Ítems	**Frecuencia**	**Porcentaje**
No cuenta		
Bueno	4	20%
Excelente	16	80%
Total	**20**	**100%**

Elaborado por: El investigador.

Fuente: Cooperativa de Transportes Flota Pelileo.

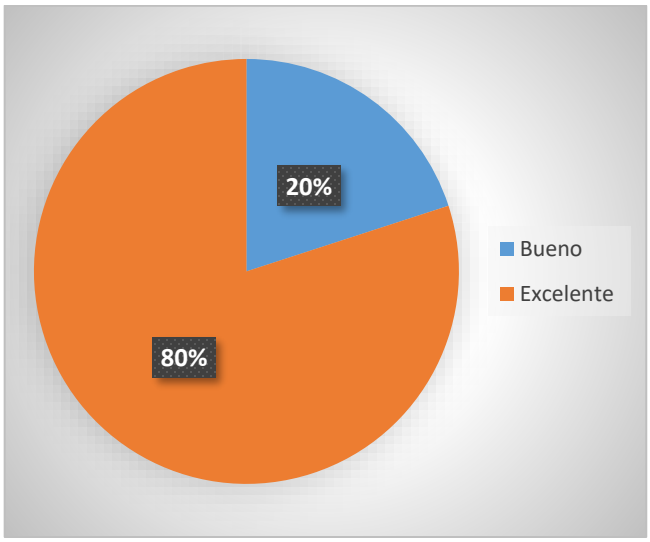


Figura 4: Pregunta 3 de la encuesta.

Elaborado por: El Investigador

Análisis: El 100% de los encuestados cuentan con acceso a internet, el 80% calificando el servicio como excelente y el 20% como Regular.

4. ¿Se han conectado remotamente a su equipo de trabajo de la Cooperativa?

Tabla 4: Pregunta No. 4

Ítems	Frecuencia	Porcentaje
Si	20	100%
No	0	0%
Total	20	100%

Elaborado por: El investigador.

Fuente: Cooperativa de Transportes Flota Pelileo.

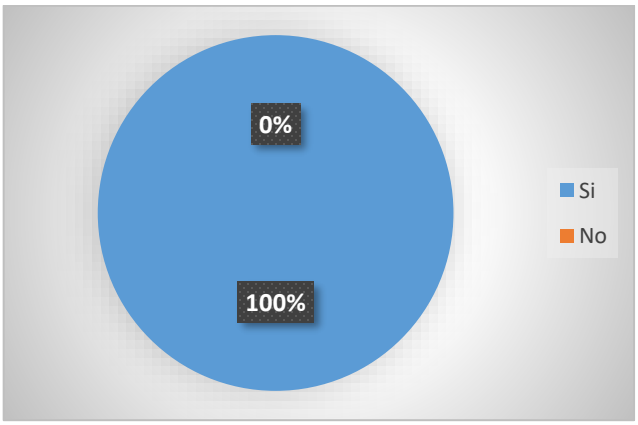


Figura 5: Pregunta 4 de la encuesta.

Elaborado por: El Investigador

Análisis: El 100% de los encuestados se han conectado remotamente. Las conexiones se lo están realizando por aplicaciones que utilizan los sistemas de criptografía reduciendo así el riesgo de la comunicación sea interceptada y terceros puedan ver lo que se está trasmitiendo

5. **¿Su usuario y contraseña, la tiene guardada en?**

Tabla 5: Pregunta No. 5

Ítems	**Frecuencia**	**Porcentaje**
Celular	5	25%
Papel	5	25%
Memoria	10	50%
Total	20	100%

Elaborado por: El investigador.

Fuente: Cooperativa de Transportes Flota Pelileo.

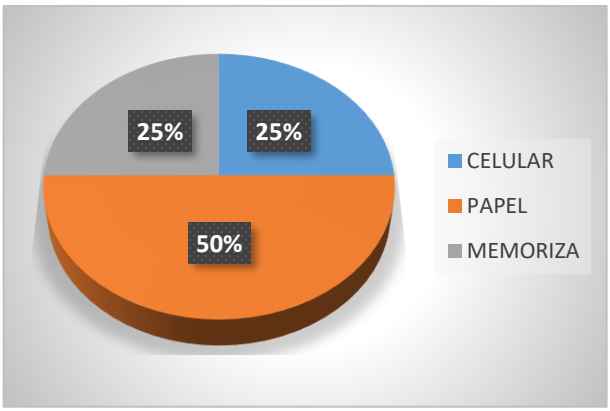


Figura 6: Pregunta 5 de la encuesta.

Elaborado por: El Investigador

Análisis: El 50% de los encuestados menciona que su usuario y contraseña se memorizan, el 25% lo tienen en el celular y el 25% tienen escrito en un papel, siendo esto un peligro ya que terceras personas pueden acceder a información de la Cooperativa como personal.

6. ¿Conoce sobre Políticas de Seguridad Informática?

Tabla 6: Pregunta No. 6

Ítems	Frecuencia	Porcentaje
Si	3	15%
No	17	85%
Total	20	100%

Elaborado por: El investigador.

Fuente: Cooperativa de Transportes Flota Pelileo.

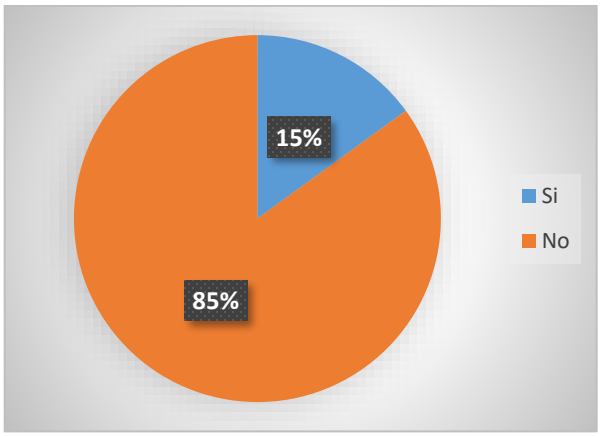


Figura 7: Pregunta 6 de la encuesta.

Elaborado por: El Investigador

Análisis: El 85 % de encuestados no conoce sobre políticas de seguridad informática y el 15% menciona conocer sobre este tema, por lo que se recomienda que se capacite al personal sobre estos temas, para evitar el mal uso de la tecnología.

7. ¿Conoce usted sobre los "ataques informáticos", y las maneras de evitarlos?

Tabla 7: Pregunta No. 7

Ítems	Frecuencia	Porcentaje
Si	3	15%
No	17	85%
Total	20	100%

Elaborado por: El investigador.

Fuente: Cooperativa de Transportes Flota Pelileo.

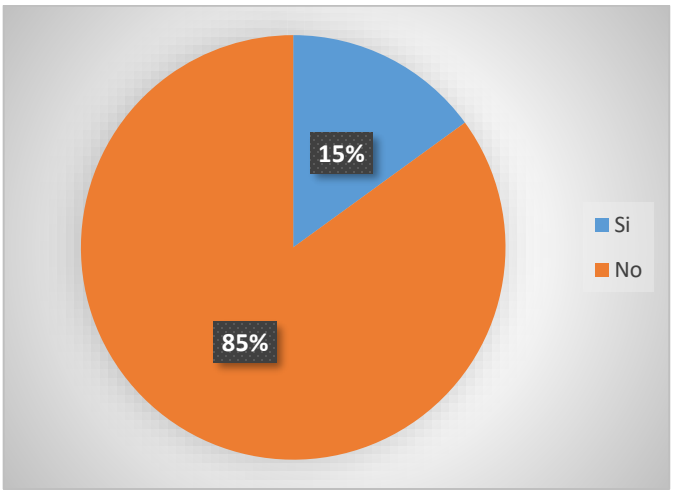


Figura 8: Pregunta 7 de la encuesta.

Elaborado por: El Investigador

Análisis: El 85% de los encuestados manifiesta que no conoce sobre ataques informáticos y las maneras de evitarlos, y el 15% conoce sobre esto, siendo esto perjudicial ya que pone en riesgo la información de la Cooperativa.

8. ¿Se tienen instalado programa antivirus en su equipo?

Tabla 8: Pregunta No. 8

Ítems	Frecuencia	Porcentaje
Si	0	0%
No	20	100%
Total	20	100%

Elaborado por: El investigador.

Fuente: Cooperativa de Transportes Flota Pelileo.

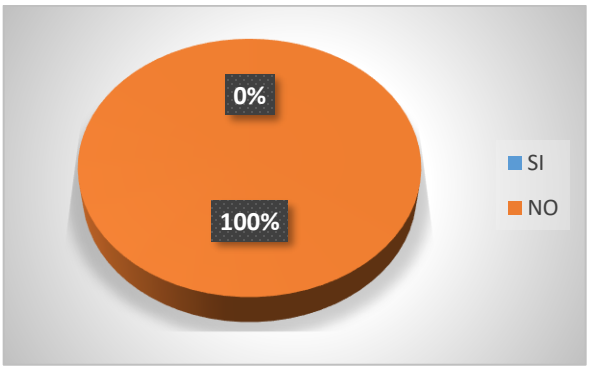


Figura 9: Pregunta 8 de la encuesta.

Elaborado por: El investigador.

Análisis: El 100% de los encuestados no tiene en sus equipos instalados antivirus, esto se corregir para cerrar la puerta a una posible infiltración de información.

9. **¿Usted está de acuerdo que se debe realizar una auditoría informática para para conocer las debilidades y desarrollar acciones con la gestión de la información?**

Tabla 9: Pregunta No. 9

Ítems	Frecuencia	Porcentaje
Si	0	0%
No	20	100%
Total	20	100%

Elaborado por: El investigador.

Fuente: Cooperativa de Transportes Flota Pelileo.

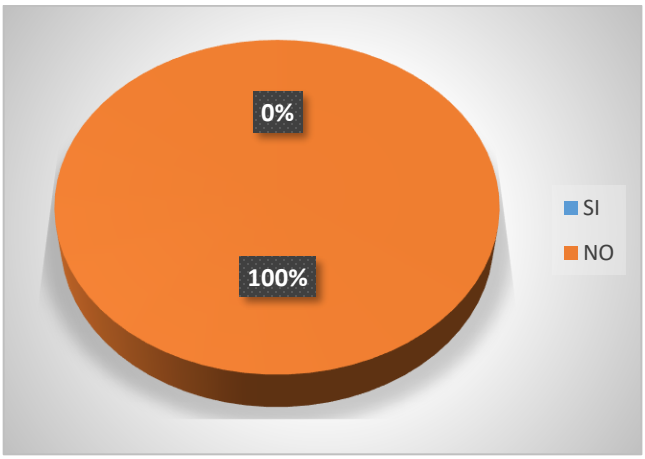


Figura 10: Pregunta 9 de la encuesta.

Elaborado por: El investigador.

Análisis: El 100% de los encuestados están de acuerdo en que se debe realizar una auditoría a la Cooperativa de Transportes, ya que, con los resultados obtenidos, se tomara decisiones en beneficio de la misma.

3.2 Análisis de la situación actual de la Cooperativa de Transportes Flota Pelileo

Historia

La Cooperativa de Transporte Flota Pelileo nace por la iniciativa visionaria de un grupo de transportistas originarios de la ciudad de Pelileo ubicada en la Provincia de Tungurahua, siendo su día de fundación el 24 de Agosto de 1959, convirtiéndose así en una empresa de viajes interprovincial que conecta una parte de la región interandina con otras provincias y regiones de Ecuador, posicionándose como una cooperativa de mucha tradición y de uso común de locales y turistas que deciden realizar viajes por vía terrestre desde y hacia esta localidad.

Entre las principales rutas que recorren las unidades de esta empresa de transporte, se encuentran localidades como Ambato, Guayaquil, Quito, Tena, Puyo, Coca y Milagro, realizando frecuencias directas entre todas estas ciudades del país meridional y teniendo horarios recurrentes de salidas y llegadas de un bus por cada hora, normalmente.

Misión

Ser una organización cooperativa que realiza en forma permanente el servicio interprovincial e intercantonal de transporte de pasajeros, turistas y encomiendas, desde y hacia diferentes ciudades que tiene sus rutas y frecuencias y viceversa, con unidades motorizadas en perfectas condiciones mecánicas, con confort y seguridad manteniendo como principios la **IGUALDAD, SOLIDARIDAD, COMPAÑERISMO Y DEMOCRACIA.**

Visión

Ser una operadora sin fines de lucro, líder de transporte de pasajeros, competitiva por excelencia a nivel nacional y que pone al servicio de la ciudadanía, modernos unidades cómodas, seguras y confortables, para un servicio óptimo a la comunidad, cumpliendo con los principios constitucionales del BUEN VIVIR.

Para los trámites ante el organismo provincial de tránsito la Cooperativa tomara el nombre de OPERADORA DE TRANSPORTE.

Valores Corporativos

Los valores de la cooperativa son los pilares más importantes de cualquier organización. Con ellos en realidad se define a sí misma, porque los valores de una cooperativa son los valores de sus miembros, y en especial los de sus dirigentes.

- **Lealtad:** Cumplir las responsabilidades individuales para fortalecer la imagen institucional.
- **Responsabilidad:** Desarrollar con efectividad las tareas encomendadas.
- **Honestidad:** Emprender actuaciones bajo criterios de discernimiento ético en la gestión institucional.
- **Respeto:** Comprender y valorar la libertad de pensamiento y los derechos inherentes a cada persona.
- **Eficiencia:** Se entregan resultados de calidad en base a la planificación institucional.
- **Compromiso:** Demostrar vocación de servicio y sentido de pertenencia frente a la entidad, ejerciendo el liderazgo necesario para dar cumplimiento a los objetivos de la organización, respetando el medio ambiente.
- **Competitividad:** Aplicar la cultura de calidad en el servicio, ofreciendo una amplia cobertura, que permita responder efectivamente frente a las exigencias del mercado dentro de un mundo globalizado.
- **Solidaridad:** Cooperación permanente y continua en el desarrollo en los procesos de la organización y en las relaciones interpersonales con clientes y usuarios.

Políticas Generales

- Realizar todo trabajo con excelencia.
- Brindar trato justo y esmerado a todos los clientes, en sus solicitudes y reclamos considerando que el fin de la empresa es el servicio a la comunidad.
- Todos los integrantes de la empresa deben mantener un comportamiento ético.
- Desterrar toda forma de paternalismo y favoritismo, cumpliendo la reglamentación

vigente.

- Los puestos de trabajo en la empresa son de carácter poli-funcional; ningún trabajador podrá negarse a cumplir una actividad para la que esté debidamente capacitado.
- Impulsar el desarrollo de la capacidad y personalidad de los recursos humanos mediante acciones sistemáticas de formación.
- Todas las actividades son susceptibles de delegación, tanto en la acción como en su responsabilidad implícita.
- Realizar evaluaciones periódicas, permanentes a todos los procesos de la organización.
- Mantener una sesión mensual documentada de trabajo de cada unidad, a fin de coordinar y evaluar planes y programas, definir prioridades y plantear soluciones.

Políticas de Servicio

- Servicio de transporte de pasajeros.
- Seguro de pasajeros.
- Servicio de encomiendas.
- Brindar un buen trato al cliente.
- Refrigerio al cliente.
- Unidades confortables y que disponga de buenos equipos de video y música.

Objetivos

1. Buscar el continuo mejoramiento del transporte interprovincial e intercantonal de pasajeros dentro de la cooperativa, para lo cual sus directivos realizaran evaluaciones periódicas del sistema de trabajo de sus unidades, personal, administrativos, choferes, con el fin de mejorar el servicio a nuestros usuarios de

acuerdo con el Contrato de Operación emitido a la institución.

2. Vigilar que los vehículos de los cooperados que son parte de la Cooperativa se encuentran en buen estado mecánico y de presentación, reuniendo siempre las condiciones de seguridad para brindar un servicio de calidad.

3. Establecer y poner en práctica el servicio de asistencia social, jurídica y médica, estos dos últimos a través de convenios institucionales, con el fin de auxiliar a sus miembros en caso de accidente o calamidad domestica debidamente comprobados, para lo cual sus directivos establecerán un fondo de asistencia social dentro de la planeación estratégica y presupuesto anual de la Cooperativa.

4. Crear una caja de ahorro y crédito del "Buen Vivir", a fin que la organización realice préstamos a sus asociados para realizar los arreglos y reparaciones de los vehículos que forman parte del parque automotor de la Cooperativa, como también cubrir las necesidades.

Atribuciones y deberes

1. Planificar y evaluar el funcionamiento de la cooperativa.
2. Aprobar políticas institucionales y metodologías de trabajo.
3. Proponer a la asamblea reformas al estatuto social y reglamentos que sean de su compromiso.
4. Dictar los reglamentos de administración y organización internos, no asignados a la Asamblea General;
5. Aceptar o rechazar las solicitudes de ingreso o retiro de socio;
6. Sancionar a los socios de acuerdo con las causas y el procedimiento establecidos en el Reglamento Interno. La sanción con suspensión de derechos, no incluye el derecho al trabajo. La presentación del recurso de apelación, ante la Asamblea

General, suspende de aplicación de la sanción;

7. Designar Presidente, Vicepresidente y Secretario del Consejo de Administración; y comisiones o comités espaciales y removerlos cuando inobservaren la normativa legal y reglamentaria;
8. Nombrar al Gerente y Gerenta subrogante y fijar su retribución económica;
9. Fijar el monto y forma de las cauciones, determinando los obligados a rendirlas;
10. Autorizar la adquisición de bienes muebles y servicios, en la cuantía que fije el Reglamento Interno;
11. Aprobar el plan estratégico, el plan operativo anual y su presupuesto y someterlo a conocimiento de la Asamblea General;
12. Resolver la afiliación o desafiliación a organismos representativa o económica;
13. Conocer y resolver sobre los informes mensuales del Gerente;
14. Resolver la apertura y cierre de oficinas operativas de la cooperativa e informar a la Asamblea General;
15. Autorizar el otorgamiento de poderes por parte del Gerente;
16. Informar sus resoluciones al Consejo de Vigilancia.
17. Aprobar los programas de educación, capacitación y bienestar social de la cooperativa con sus respectivos presupuestos.
18. Señalar el número y valor mínimos de certificado de aportación que deban tener los socios ya autorizar su transferencia, que sólo podrá hacerse entre socios o a favor de la Cooperativa.
19. Fijar el monto de las cuotas ordinarias y extraordinarias para gastos de administración u otras actividades, así como el monto de multas por inasistencia injustificada a la Asamblea General.
20. Cumplir y hacer cumplir los principios de valores y principios del cooperativismo.

Estructura Organizacional de la Cooperativa de Transporte Flota Pelileo.

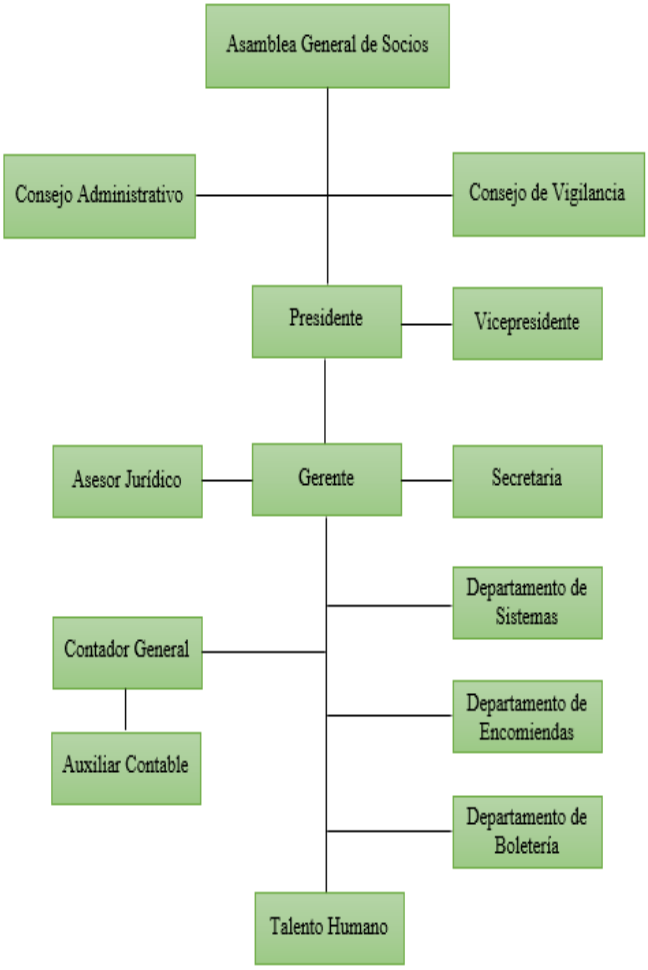


Figura 111: Organigrama de la Cooperativa de Transportes Flota Pelileo.

Elaborado por: El investigador.

Fuente: Cooperativa de Transportes Flota Pelileo.

Software detallado por departamento

Tabla 10: Resumen de Software

	Software		
Departamento	**Nombre**	**Versión**	**Tipo**
Gerencia	Windows	7 Pro 64-bits	Sistema Operativo
	Microsoft Word	2010 64-bits	Ofimática
	Anydesk	6.2.3	Acceso Remoto
Secretaria	Windows	7 Pro 64-bits	Sistema Operativo
	Microsoft Word	2010 64-bits	Ofimática
	Anydesk	6.2.3	Acceso Remoto
Gerencia Contabilidad	Windows	7 Pro 64-bits	Sistema Operativo
	Microsoft Word	2010 64-bits	Ofimática
	Anydesk	6.2.3	Acceso Remoto
Auxiliar Contable	Windows	7 Pro 64-bits	Sistema Operativo
	Microsoft Word	2010 64-bits	Ofimática
	Anydesk	6.2.3	Acceso Remoto
Sistemas	Windows	7 Pro 64-bits	Sistema Operativo
	Microsoft Word	2010 64-bits	Ofimática
	Anydesk	6.2.3	Acceso Remoto
	Windows	7 Pro 64-bits	Sistema Operativo

Boletería y Encomiendas	Microsoft Word	2010 64-bits	Ofimática
	Anydesk	6.2.3	Acceso Remoto
Talento Humano	Windows	7 Pro 64-bits	Sistema Operativo
	Microsoft Word	2010 64-bits	Ofimática
	Anydesk	6.2.3	Acceso Remoto

Elaborado por: El Investigador.

Fuente: Cooperativa de Transportes Flota Pelileo.

Recursos de Hardware

Se detalla las características de las computadoras de la Cooperativa de Transporte Flota Pelileo por departamento.

Tabla 11: Resumen de Hardware.

	Hardware			
Departamento	**Componente**	**Marca**	**Accesorios**	**Impresora**
Gerencia	Monitor	LG	Teclado, Mouse	No
	Procesador	Intel	Teclado, Mouse	
	RAM	4 GB	Teclado, Mouse	
	Disco Duro	500 GB	Teclado, Mouse	

Secretaria	Monitor	Samsung	Teclado, Mouse	Si
	Procesador	Intel	Teclado, Mouse	
	RAM	4 GB	Teclado, Mouse	
	Disco Duro	500 GB	Teclado, Mouse	
Contabilidad	Monitor	LG	Teclado, Mouse	Si
	Procesador	Intel	Teclado, Mouse	
	RAM	8 GB	Teclado, Mouse	
	Disco Duro	1 TB	Teclado, Mouse	
Auxiliar Contabilidad	Monitor	LG	Teclado, Mouse	Si (comparte con el Departamento de Contabilidad)
	Procesador	Intel	Teclado, Mouse	
	RAM	4 GB	Teclado, Mouse	
	Disco Duro	500 GB	Teclado, Mouse	
Sistemas	Monitor	LG	Teclado, Mouse	No
	Procesador	Intel	Teclado, Mouse	
	RAM	8 GB	Teclado, Mouse	
	Disco Duro	1 TB	Teclado, Mouse	
Boletería y Encomiendas	Monitor	LG	Teclado, Mouse	Si
	Procesador	Intel	Teclado, Mouse	
	RAM	8 GB	Teclado, Mouse	

	Disco Duro	500 GB	Teclado, Mouse	
Talento Humano	Monitor	LG	Teclado, Mouse	Si
	Procesador	Intel	Teclado, Mouse	
	RAM	4 GB	Teclado, Mouse	
	Disco Duro	500 GB	Teclado, Mouse	

Elaborado por: El Investigador.

Fuente: Cooperativa de Transportes Flota Pelileo.

Descripción del Servidor

Tabla 12: Resumen de Software del Servidor.

SOFTWARE		
Nombre	**Versión**	**Tipo**
Windows Server	2012 R2 Standard	Sistema Operativo Servidores
Microsoft Office	2010	Ofimática

Elaborado por: El investigador.

Fuente: Cooperativa de Transportes Flota Pelileo.

Tabla 7: Resumen de Hardware del Servidor.

HARDWARE		
Cantidad	**Componente**	**Marca**
1	Servidor	HP
	Capacidad	3 Discos
	RAM	32 GB
	Configuración	RAID 3

Elaborado por: El investigador.

Fuente: Cooperativa de Transportes Flota Pelileo.

Topología de la Red

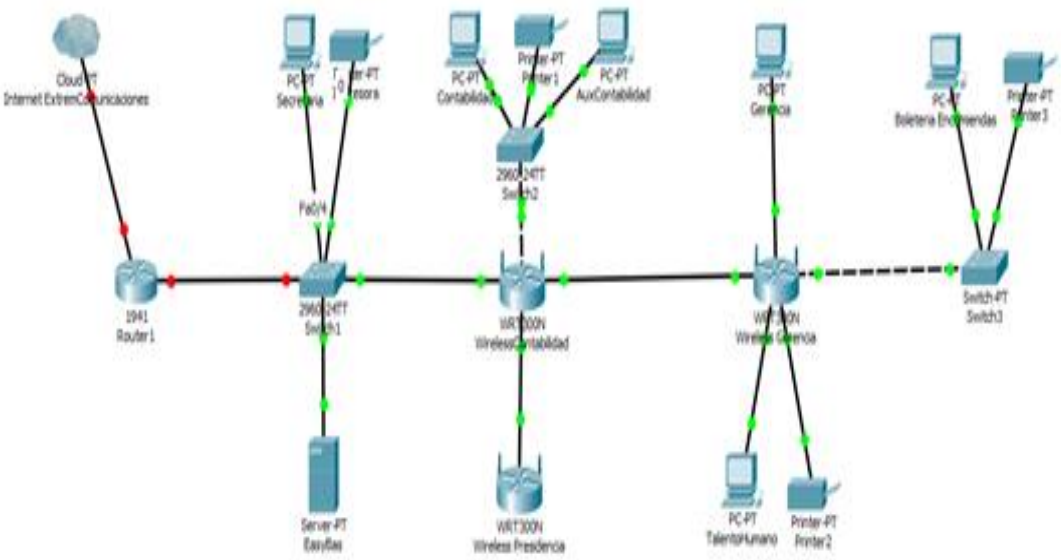


Figura 12: Topología de red de la Cooperativa de Transportes Flota Pelileo

Elaborado por: El investigador

Fuente: Cooperativa de Transportes Flota Pelileo.

Detección de problemas

- El espacio destinado para esta área de TI es pequeño, no cuenta con un ambiente ventilado para el correcto funcionamiento del servidor.
- No tienen UPS para prevenir descargas eléctricas.
- Para todos los procesos respecto a tecnología solo se cuenta con una sola persona lo cual provoca deficiencia al dar servicio técnico.
- El Sistema Operativo de todos los equipos de la Cooperativa no cuenta con licencias, se debe analizar su adquisición, también no cuenta con antivirus, provocando que las máquinas sean vulnerables a cualquier situación como virus, computadores lentos, etc.
- No cuenta con ningún tipo de políticas en cuanto a tecnología.

3.3 Análisis de las estrategias y herramientas necesarias para la ejecución de las Pruebas de Penetración y Hacking Ético

Tabla 8: Tipos de Análisis y Detección de Vulnerabilidades

Tipo	Carcterística	Aplicable al proyecto	Observación
Análisis de Vulnerabilidades	Tiene un objetivo definido	Si	Tiene como objetivo detectar vulnerabilidades en partes específicas
	Tiene en cuenta el entorno de seguridad actúa	Si	Aplica vulnerabilidades y fallos conocidos
	Trata de comprometer los sistemas objetivos	No	Solo lista las vulnerabilidades detectadas
	Explota las vulnerabilidades	No	No explota las vulnerabilidades
Test de Penetración	Tiene un objetivo definido	Si	Aplica vulnerabilidades y fallos conocidos
	Tiene en cuenta el entorno de seguridad actual	Si	Aplica vulnerabilidades y fallos conocidos
	Trata de comprometer los sistemas objetivos	Si	Lista y trata de comprometer los sistemas objetivos
	Explota las vulnerabilidades	Si	Explota las vulnerabilidades en un entorno real y virtual (simular un ataque real)
Hacking Ético	Tiene un objetivo definido	No	Toda la Infraestructura Tecnológica es su objetivo
	Tiene en cuenta el entorno de seguridad actual	No	Actúa como un atacante real
	Trata de comprometer los sistemas objetivos	Si	Su análisis es más complejo y profundo al comprometer los sistemas objetivos
	Explota las vulnerabilidades	Si	Explota las vulnerabilidades de manera directa y pura

Elaborado por: El Investigador.

Se puede observar en la tabla 14, que el Test de Penetración es la mejor opción para el presente proyecto ya que se orienta al servidor de la Cooperativa de Transportes Flota Pelileo.

Herramientas de reconocimiento

Tabla 9: Herramientas de reconocimiento

Característica	Maltego	The Harvester	Anubis	Foca	Uniscan	Visual Route
Costo	Versión libre y de paga	Versión libre	Versión libre y de paga	Versión libre y de paga	Versión libre	Versión libre y de paga
Plataforma	Windows, Mac, Linux.	Linux	Windows	Windows XP, 7, Server, Vista (32/64 bits),	Linux	Windows XP \ 2003 \ Vista \ 7, Mac OS X
Actualización / Soporte	Si	Si	No	Si	Si	Si
Facilidad de Manejo	Medio	Medio	Fácil	Fácil	Medio	Fácil

Elaborado por: El Investigador.

De acuerdo al análisis de las herramientas de reconocimiento tabla 15, Maltego, The Harverster y Uniscan cuentan con sus versiones libres y constante actualización, Se eligió la herramienta Maltego con su versión de prueba limitada por 30 días.

Herramientas de sondeo de puertos

Tabla 10: Herramientas de sondeo de puertos.

Característica	SuperScan 4	SuperScan 6	Nmap
Costo	Versión libre y de paga	Versión libre y de paga	Gratuito
Plataforma	Windows	Windows	Linux, Mac OS X, Windows y UNIX
Actualización / Soporte	Si	Si	Si
Facilidad de Manejo	Fácil	Fácil	Medio

Elaborado por: El Investigador.

Mediante el análisis de sondeo de puertos de la tabla 16, NMAP es el más eficaz porque cuenta con diferentes funciones y scripts para explorar las redes de computadoras, incluyendo la detección de equipos y sistemas operativos.

Herramientas de detección de vulnerabilidades

Tabla 11: Herramientas de detección de vulnerabilidades.

Característica	OpenVAS	Nessus	Vega	Nexpose
Costo	Versión libre	Versión libre y de paga	Versión libre	Versión libre
Plataforma	Centos, Debian, Fedora, OpenSuse, RedHat, Ubuntu, Windows	Microsoft Windows, Mac OS X, Linux, FreeBSD	Linux, OS X y Windows	MS Windows Server 2003 SP2 / Server 2003 R2, Red Hat Enterprise, Ubuntu LTS, SuSE Linux
Actualización / Soporte	Si	Si	Si	Si
Facilidad de Manejo	Fácil	Fácil	Fácil	Fácil

Elaborado por: El Investigador.

Mediante la tabla 17, herramientas de detección de vulnerabilidades por su versión libre se elige Nessus y Vega siendo las más accionadas en cuanto al número de direcciones ip a analizar, actualización y la generación de reportes.

Herramientas de explotación

Tabla 12: Herramientas de explotación.

Característica	Metasploit	Hping3	Hydra	Ettercap
Costo	Versión libre y de paga	Versión libre	Versión libre	Versión libre
Plataforma	Windows 64-Bit, Linux: 64/32 Bits	GNU/linux, FreeBSD, NetBSD, OpenBSD, Solaris y Mac OS X.	Linux	Linux / Windows
Actualización / Soporte	Si	Si	Si	Si
Facilidad de Manejo	Medio	Fácil	Fácil	Fácil

Elaborado por: El Investigador.

Según el análisis de la tabla 18, el Sistema Operativo Kali Linux diseñado principalmente para la Auditoría y Seguridad Informática en general, trae preinstalados más de 600 programas incluyendo Metasploit (software de pruebas de penetración), Ettercap (un sniffer), Hydra (crackeador de passwords) entre otras herramientas, Hydra fue seleccionada para utilizar en el presente proyecto.

3.4 Identificación de vulnerabilidades en el servidor que puedan ser explotadas por intrusos malintencionado

Para el cumplimiento de los módulos de las secciones en mención, se utiliza las herramientas informáticas ya estudiadas y seleccionadas.

Sección Seguridad de la Información

Módulo de Revisión de la Inteligencia Competitiva

El objetivo de este módulo es, conseguir toda la información posible de la organización que se va a auditar, esto se lo realiza de manera pasiva porque no se tiene un contacto directo con la institución auditar.

Mediante la herramienta Maltego se investiga las relaciones existentes que tiene un determinado dominio en este caso flotapelileo.com.ec

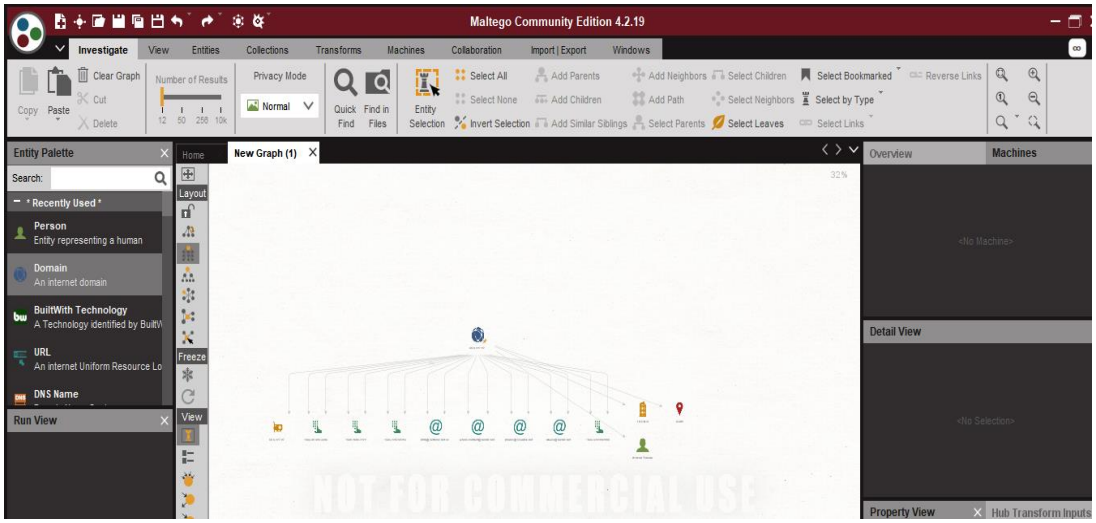


Figura 13: Maltego transformación del dominio

En la figura 13, se puede observar las transformaciones DNS aplicando a un tipo Domain nombrado flotapelileo.com, se muestra un servidor web relacionado as flechas muestran

que hay conexión entre el objeto principal(padres) y los objetos secundarios(hijos), las estrellas amarillas reflejan que el objeto provee servicios web.

Resultados de Maltego

Tabla 13: Lista de Servidores

Dirección	IP Pública	Servicio
www.flotapelileo.com.ec	45.6.227.87	DNS Name

Elaborado por: El Investigador.

El buscador de Google, es más provechoso siempre que se lo utilice de forma que se pueda filtrar información y reducir los resultados al máximo, esto se lo realiza mediante la utilización de sus operadores, esta técnica se la denomina “Google Hacking”

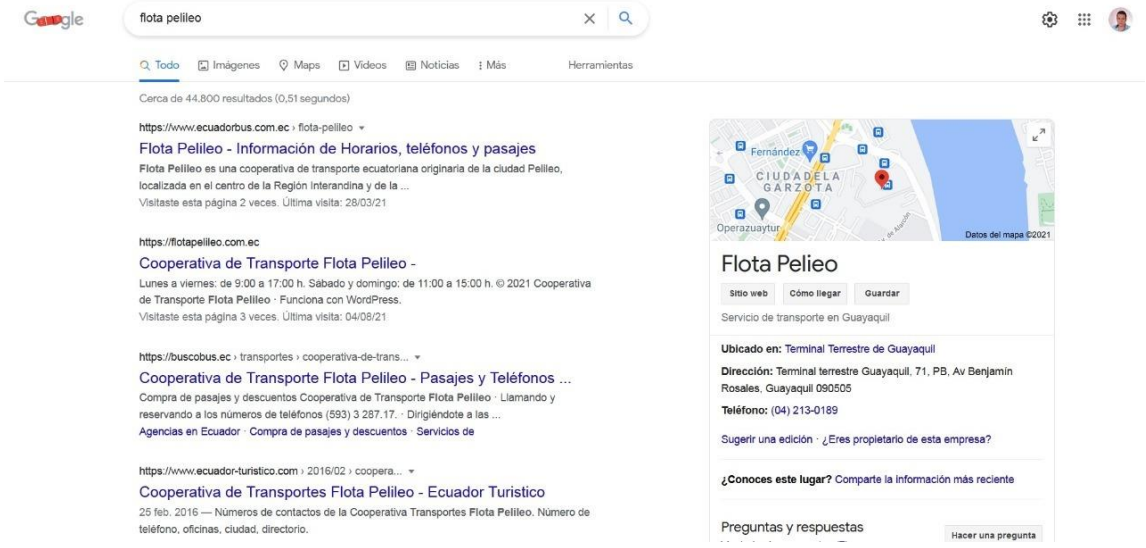


Figura 14: Búsqueda en Google

En la figura 14, se observa la búsqueda de “Flota Pelileo” en el buscador de google, el resultado es de más de tres mil resultados, el número de resultados se lo puede reducir mediante “Google Hacking”. Buscando información en la base de datos NIC (Network Information Center); “NIC es la autoridad que delega los nombres de dominio a quienes los solicitan. Cada país en el mundo cuenta con una autoridad que registra los nombres bajo su jurisdicción. Por autoridad no nos referimos a una dependencia de un gobierno, muchos NIC´s en el mundo son operados por universidades o compañías privadas”[34].

En el navegador de preferencia se ingresa a la dirección https://nic.ec/ y se digita el dominio en investigación, en este caso flotapelileo.com.ec

Figura 15: Consulta de Flota Pelileo en NIC.

En la figura 15, se observa el resultado de la consulta del dominio flotapelileo.com.ec en la base de datos NIC, se aprecian que los datos que obtengo como resultado es solamente con propósito informativo, no revela datos de personas naturales o empleados de la

Institución ya que de esa manera se podría utilizar la información para un ataque de Ingeniería Social.

Módulo de Revisión de la Privacidad

En este módulo se explora que los datos de los empleados considerados como privados no sean expuestos ante todo el mundo, de igual forma la confidencialidad con la cual se manipula la distribución de información a los empleados.

Uno de los principios básicos de Seguridad Informática es la Confidencialidad la cual se define en, la no divulgación de información de manera no autorizada.

La información de instituciones públicas es transparente y están obligadas a difundirla mediante un portal o sitio web, esto permite acceder a nombres de autoridades, directores y demás empleados, en caso de la Cooperativa flotapelileo.com.ec.

La web de la Cooperativa de Transportes Flota Pelileo, proporciona la siguiente tabla de Autoridades.

Tabla 14: Autoridades de la Cooperativa de Transportes Flota Pelileo

Cargo	Nombres del encargado
Presidente	Dennis Barahona
Gerente	Ing. Patricio Toctaquiza

Elaborado por: El Investigador.

Módulo de Recolección de Documentos

En este punto se procesa toda la información recolectada anteriormente para extraer datos importantes de cada uno de los documentos tales como nombres de usuarios, empleados claves de la institución, correos electrónicos, entre otros.

Se obtuvo documentos publicados en internet como:

- Nombres completos de varios empleados y autoridades pertenecientes a la Cooperativa.
- Datos personales como cédula, dirección de domicilio, fechas de nacimiento, entre otros.
- Informes de Auditorías internas de gastos.

Mediante un análisis de los metadatos de los documentos obtenidos se puede definir nombres de usuarios relacionados con la Cooperativa. Los datos personales pueden ser usados para la aplicación de Ingeniería Social, robo de información mediante phishing, creación de diccionario de datos, entre otros.

Como auditor me dieron acceso solo a algunos equipos de la Cooperativa de los cuales pude extraer la siguiente información:

Tabla 15: Hardware de la Cooperativa de Transportes Flota Pelileo.

Departamento	Cantidad	Componente	Marca
Gerencia	1	Monitor	LG
	1	Procesador	Intel
	1	RAM	4 GB
	1	Disco Duro	500 GB
Secretaria	1	Monitor	LG
	1	Procesador	Intel
	1	RAM	4 GB
	1	Disco Duro	500 GB
Contabilidad	1	Monitor	LG
	1	Procesador	Intel
	1	RAM	8 GB
	1	Disco Duro	1 TB
Auxiliar Contabilidad	1	Monitor	LG
	1	Procesador	Intel
	1	RAM	4 GB
	1	Disco Duro	500 GB
Sistemas	1	Monitor	LG

	1	Procesador	Intel
	1	RAM	8 GB
	1	Disco Duro	500 GB
Boletería y Encomiendas	1	Monitor	LG
	1	Procesador	Intel
	1	RAM	4 GB
	1	Disco Duro	500 GB
Talento Humano	1	Monitor	LG
	1	Procesador	Intel
	1	RAM	4 GB
	1	Disco Duro	500 GB

Elaborado por: El Investigador

Sección Seguridad de los Procesos

Testeo de Solicitud

Se obtuvo información, mediante una llamada telefónica, logrando un resultado positivo puesto que la persona que contesto la llamada, facilito los datos responsables del encargado de sistemas.

Realizado el testeo de solicitud se puede concluir que la secretaria que toma las llamas no tiene cuidado suficiente en revelar información.

Testeo de Sugerencia Dirigida

Se realizó, la prueba mediante la suplantación de identidad física, Pedro que se ha identificado como pariente del encargado de sistemas ha comentado a la secretaria que ha sido enviado para que le faciliten cierta información, la misma lo ha dejado pasar al departamento de sistemas.

Realizado el testeo de sugerencia dirigida se concluye que el personal de la Cooperativa, no tiene el conocimiento adecuado para evitar que personas mal intencionadas puedan acceder a las instalaciones, así como a la información que se maneja en dicho departamento.

Testeo de las Personas Confiables

Para realizar el testeo, se solicitó a un familiar de uno de los colaboradores de la Cooperativa de Transportes Flota Pelileo, el mismo que tenía como objetivo recabar información sobre los aplicativos que se manejan y el servidor donde se ejecutan, indicando que es para un trabajo universitario.

El cual obtuvo una respuesta negativa, ya que para dicha actividad previamente se debía entregar una solicitud autorizada por la Cooperativa donde se detalle la información que se necesita y mediante un análisis se verifica si es factible o no brindar la información solicitada.

Realizado el testeo de personas confiables se concluye que el personal encargado del departamento de sistemas tiene el conocimiento adecuado para evitar que personas mal intencionadas puedan acceder a la información que se maneja.

Seguridad en las Tecnologías de Internet

Sondeo de Red

Se obtiene las direcciones ip a auditar por parte de la Cooperativa y se hace un reconocimiento de la red institucional de manera detallada, cabe mencionar que existe información confidencial a la cual el auditor no tiene acceso.

Tabla 16: Redes internas de la Cooperativa de Transportes Flota Pelileo

Red	Mascara	Observación
192.168.100.1	225.225.225.0	Secretaria
192.168.0.1	225.225.225.0	Gerencia
192.168.0.2	225.225.225.0	Presidencia

Elaborado por: El Investigador

Lista de servidores de la Cooperativa

Tabla 17: Servidor de la Cooperativa de Transportes Flota Pelileo

Número	Dirección	Nombre
1	45.6.227.87	flotapelileo.com.ec

Elaborado por: El Investigador

Identificación de Servicios y Sistemas

En esta sección ejecuta un sondeo de puertos en el servidor para descubrir que servicios se están ejecutando actualmente.

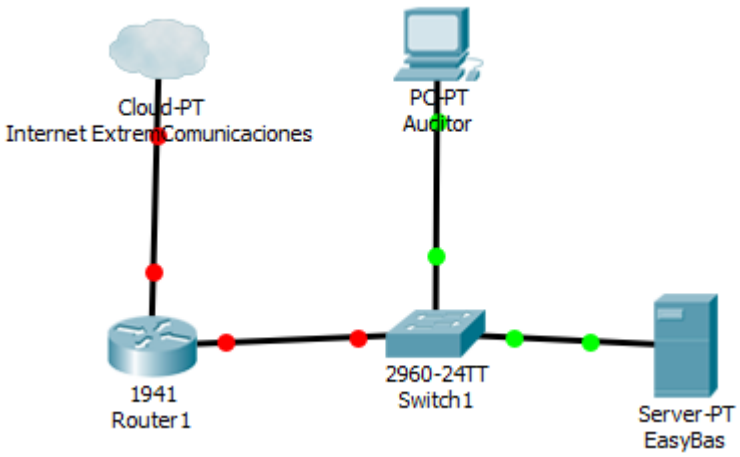


Figura 16: Escenario real del servidor

Elaborado por: El Investigador

En la figura 16, se muestra el escenario real para el sondeo de puertos.

Se utiliza la herramienta NMAP con su interfaz Zenmap para realizar los respectivos

sondeos de puertos y servicios a cada uno de los equipos en cuestión.

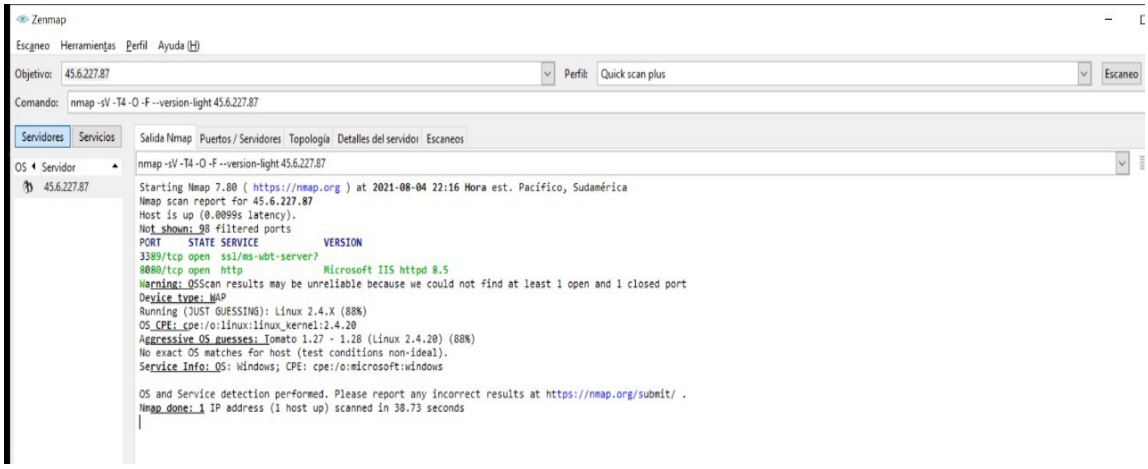


Figura 17: Sondeo de puertos con nmap

Servidor flotapelileo.com.ec

Tabla 18: Nmap a flotapelileo.com.ec

Puerto	Protocolo	Servicio	Detalle
3039	tcp	ssl/ms-wbt-server?	
8080	tcp	http	Microsoft IIS httpd 8.5

Elaborado por: El Investigador

Búsqueda y Verificación de Vulnerabilidades

En esta sección se indagan los posibles fallos, errores o vulnerabilidades de sistemas operativos, esto se lo realiza mediante el sondeo de vulnerabilidades, luego se explota

(pruebas de penetración) los fallos que se hayan detectado en el objetivo.

Para realizar lo mencionado se utilizan los programas de escaneo de vulnerabilidades Nessus y Vega, para la verificación, un framework de explotación el cual incluye herramientas de reconocimiento, escaneo, análisis y explotación de vulnerabilidades.

Escaneo de vulnerabilidades con NESSUS

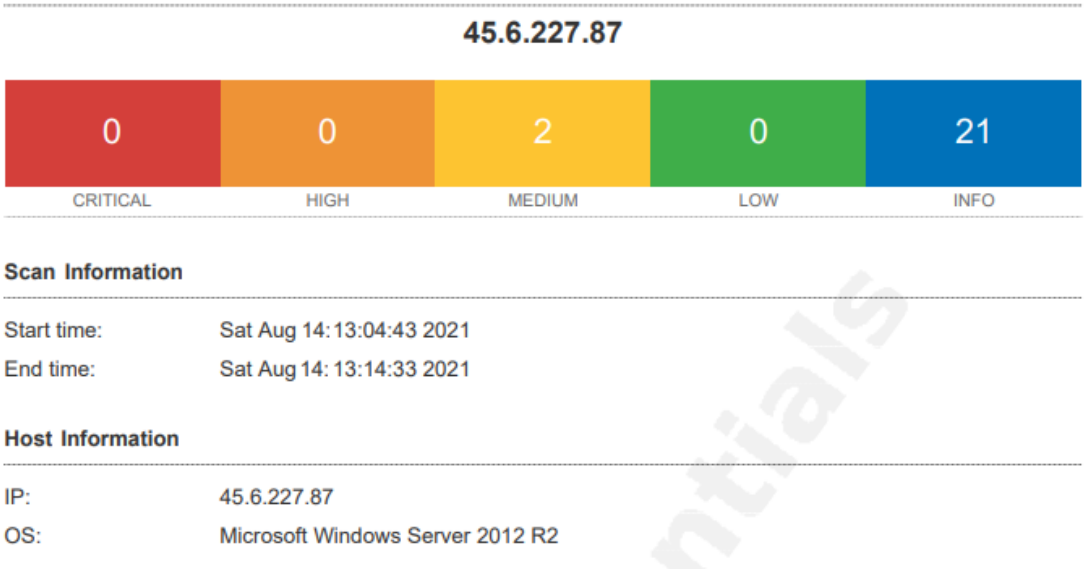


Figura 18: Escaneo de Vulnerabilidades con Nessus

Como se observa en la figura 18, tiene 2 vulnerabilidades de nivel medio y 21 de información. A continuación, se detalla las vulnerabilidades encontradas:

Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Nivel de riesgo

Medio

Conclusión

Los servicios de Terminal Server remotos no utilizan únicamente la autenticación de nivel de red.

Terminal Services Encryption Level is Medium or Low

Nivel de riesgo

Medio

Conclusión

El host remoto está utilizando una criptografía débil.

Escaneo de puertos con Nessus

Mediante este escaneo es posible determinar qué puertos TCP están abiertos.

Este complemento es un escáner de puerto SYN 'medio abierto'. Las exploraciones SYN son menos intrusivas que las exploraciones TCP (conexión completa) contra servicios rotos, pero pueden causar problemas para cortafuegos menos robustos y también dejar conexiones sin cerrar en el objetivo remoto, si la red está cargada.

Tabla 19: Puerto escaneados con Nessus

Puerto	Nivel de riesgo
53/tcp	Ninguno
3389/tcp	Ninguno
8080/www	Ninguno

Información de escaneo de Nessus

Este complemento muestra información sobre el análisis de Nessus.

Detalla para cada host probado, información sobre el escaneo en sí:

- La versión del conjunto de complementos.
- El tipo de escáner (Nessus o Nessus Home).
- La versión del motor Nessus.
- Los escáneres de puertos utilizados.
- El rango de puertos escaneado.
- El tiempo de ida y vuelta del ping
- Si es posible realizar comprobaciones de gestión de parches con credenciales o de terceros.
- Si la visualización de parches reemplazados está habilitada
- La fecha del escaneo.
- La duración del escaneo.
- El número de hosts escaneados en paralelo.
- El número de comprobaciones realizadas en paralelo.

```
Information about this scan :

Nessus version : 8.15.1
Nessus build : 20272
Plugin feed version : 202108280517
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : es8-x86-64
Scan type : Normal
Scan name : My Basic Network Scan
Scan policy used : Basic Network Scan
Scanner IP : 172.17.0.3
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 103.575 ms
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/8/28 13:04 UTC
Scan duration : 563 sec
```

Figura 19: Información del escaneo con Nessus

Identificación de S.O.

Usando una combinación de sondas remotas (por ejemplo, TCP / IP, SMB, HTTP, NTP, SNMP, etc.), es posible adivinar el nombre del sistema operativo remoto en uso. A veces también es posible adivinar la versión del sistema operativo sistema.

```
Remote operating system : Microsoft Windows Server 2012 R2
Confidence level : 75
Method : HTTP

The remote host is running Microsoft Windows Server 2012 R2
```

Figura 20: Identificación de S.O.

Conclusión

Es posible adivinar el sistema operativo remoto.

Detección de proxy de interceptación / NAT inversa

Descripción

Reverse NAT es una tecnología que permite que varias computadoras ofrezcan servicios públicos en diferentes puertos a través del mismo Dirección IP.

Según los resultados de las huellas dactilares del sistema operativo, parece que diferentes sistemas operativos están escuchando en diferentes controles remotos puertos.

También puede indicar la presencia de un proxy interceptor, un equilibrador de carga o un tráfico moldeador.

```
+ On the following port(s) :
 - 3050 (19 hops away)
 - 8080 (19 hops away)
 - 3389 (19 hops away)

The operating system was identified as :

Microsoft Windows Vista
Microsoft Windows Vista

+ On the following port(s) :
 - 53 (15 hops away)

The operating system was identified as :

Linux Kernel 2.6
```

Figura 21: Detección de proxy de interceptación / NAT inversa

Conclusión

La dirección IP remota parece conectarse a diferentes hosts a través de NAT inversa, o hay un proxy interceptor en el camino.

Los servicios de terminal utilizan SSL / TLS

Descripción

Los servicios de Terminal Server remotos están configurados para usar SSL / TLS.

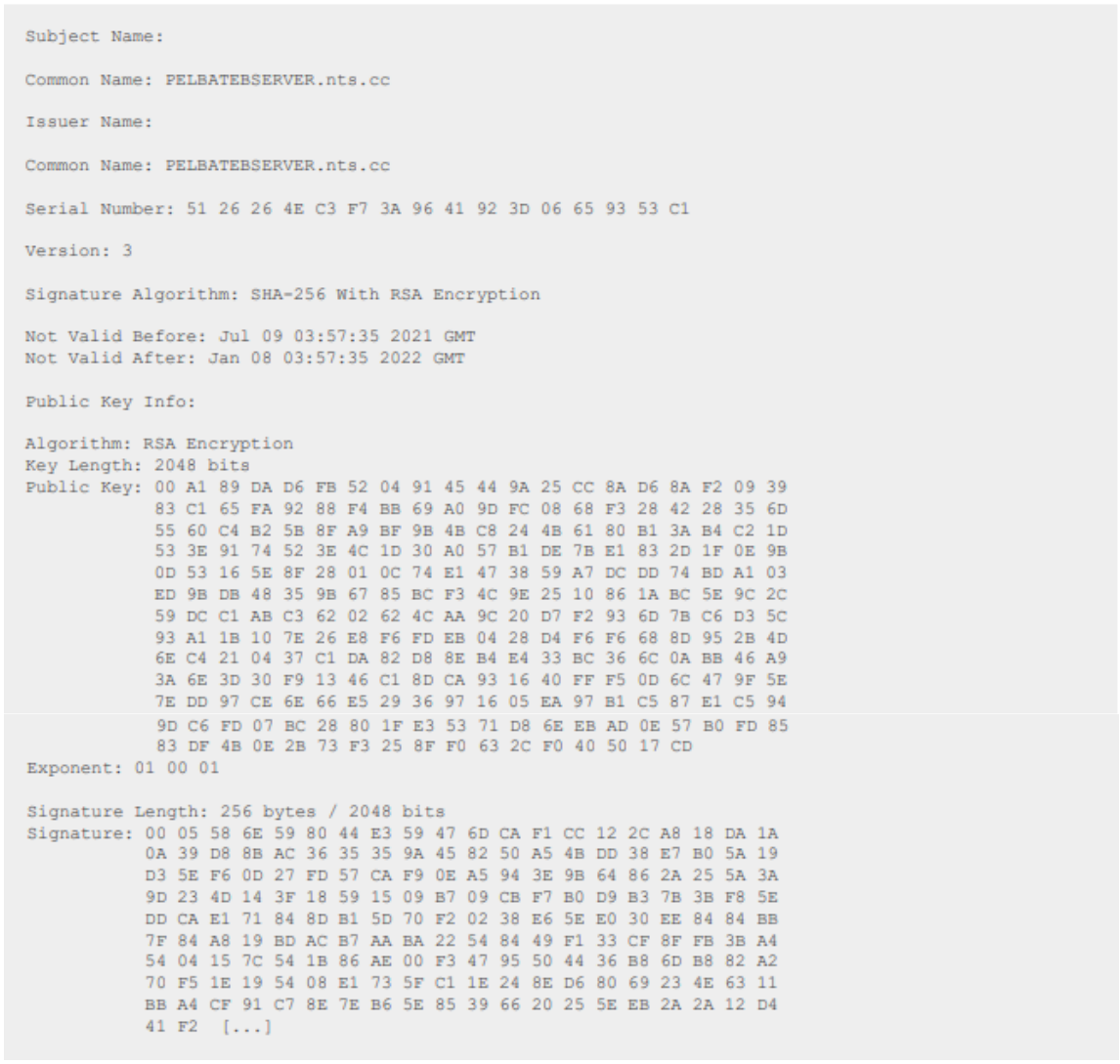


Figura 22: Servicios SSL / TLS

Escaneo de vulnerabilidades con VEGA

La herramienta VEGA contiene 3 ventanas con opciones diferentes la una es Website View, que es en donde muestra la URL que se está analizando. La opción Scan Alerts que muestra las vulnerabilidades encontradas según el riesgo de cada una, y Scan Alert Summary que muestra el resumen del proceso final cuando ha terminado de ejecutar la herramienta el debido análisis lo muestra según su categoría y riesgo. Para iniciar y usar

el escáner VEGA se lanza un escaneo por defecto pinchando en el icono de "New Scan".

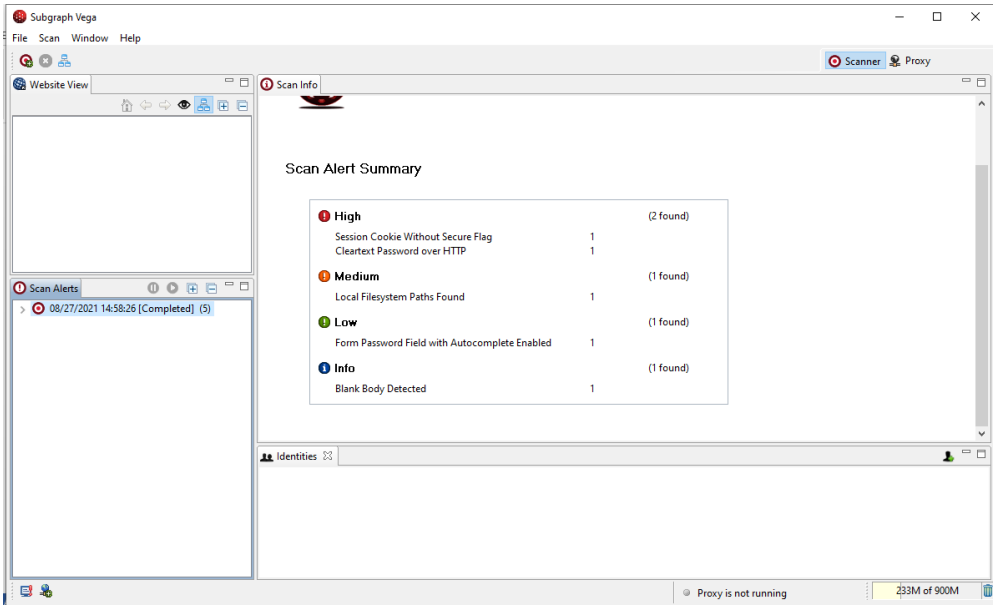


Figura 23: Escaneo con Vega

Como se observa en la figura 23, Vega está escaneando las vulnerabilidades que tiene el servidor de la Cooperativa.

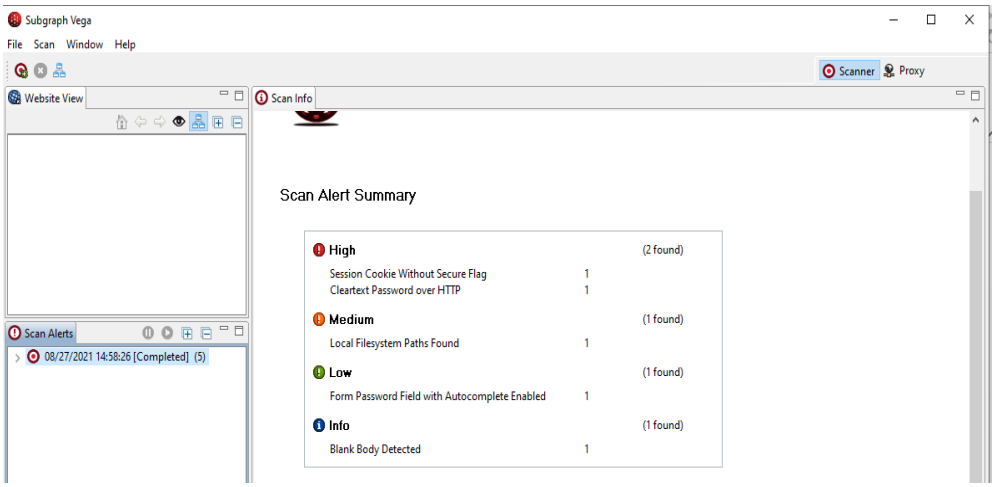


Figura 24: Detección de Vulnerabilidades con Vega

Como se observa en la figura 24, Vega encontró 4 vulnerabilidades; 1 vulnerabilidad alta, 1 vulnerabilidad media, 1 vulnerabilidad baja y 1 de información.

Las mismas que se detallan a continuación:

Cleartext Password over HTTP

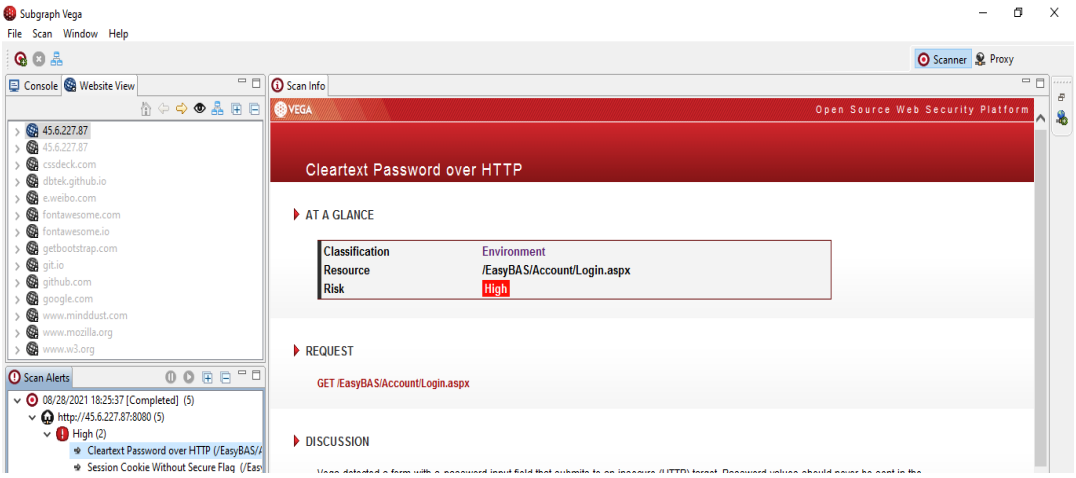


Figura 25: Contraseña de texto sin cifrar a través de HTTP

Contenido del recurso

GET /EasyBAS/Account/Login.aspx

Discusión

- Vega detectó un formulario con un campo de entrada de contraseña que se envía a un objetivo inseguro (HTTP).
- Los valores de las contraseñas nunca deben enviarse de forma clara a través de canales inseguros. Esta vulnerabilidad podría resultar en la divulgación no autorizada de contraseñas a atacantes de red pasivos.

Session Cookie Without Secure Flag

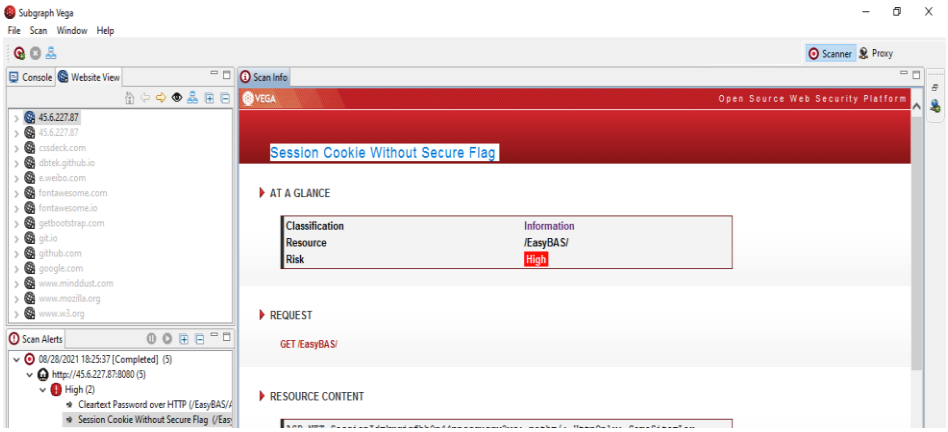


Figura 26: Cookie de sesión

Solicitud

GET /EasyBAS/

Contenido de Recursos

ASP.NET_SessionId=krqjgfhh0p44pnscguggy3wc; path=/; HttpOnly; SameSite=Lax

Discusión

Vega ha detectado que es posible que se haya configurado una cookie de sesión conocida sin el indicador de seguridad.

Local Filesystem Paths Found

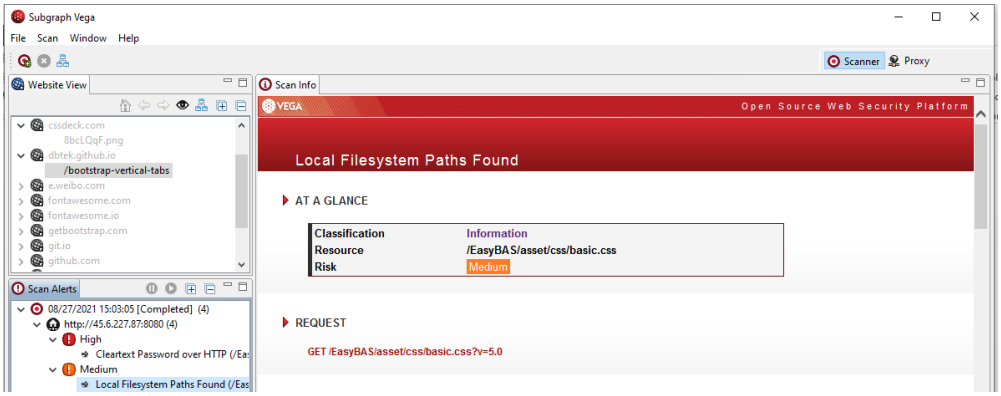


Figura 27: Rutas del sistema

Solicitud

GET /EasyBAS/asset/css/basic.css?v=5.0

Contenido de recursos

/media/items/

Discusión

Vega ha detectado una posible ruta absoluta del sistema de archivos (es decir, una que no es relativa a la raíz web). Esta información es sensible, ya que puede revelar cosas sobre el entorno del servidor a un atacante. Conocer el diseño del sistema de archivos puede aumentar las posibilidades de éxito de los ataques ciegos. Las rutas completas del sistema se encuentran muy a menudo en la salida de error. Esta salida nunca debe enviarse a clientes en sistemas de producción. Debe ser redirigido a otro canal de salida (como un registro de errores) para que los desarrolladores y administradores del sistema lo analicen.

Form Password Field with Autocomplete Enabled

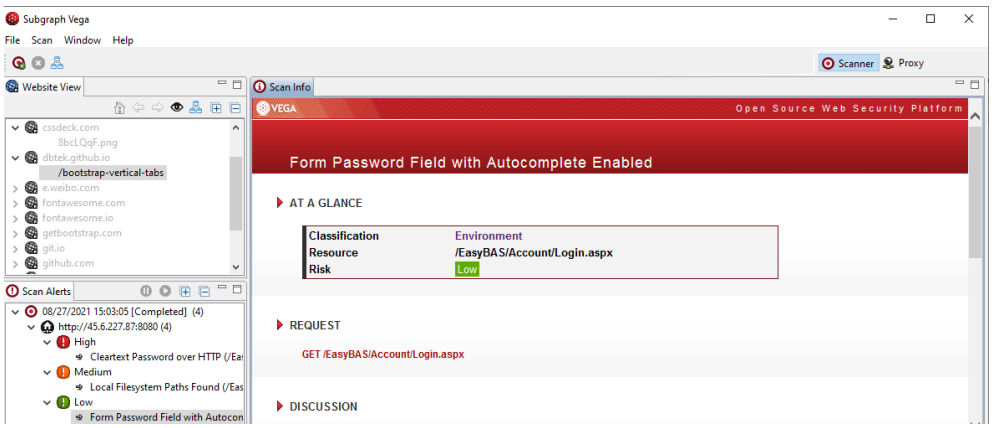


Figura 28: Entrada de contraseña

Solicitud

GET /EasyBAS/Account/Login.aspx

Discusión

Vega detectó un formulario que incluía un campo de entrada de contraseña. El atributo de autocompletar no estaba desactivado. Esto puede resultar en que algunos navegadores almacenen valores ingresados por los usuarios localmente, donde pueden ser recuperados por terceros.

Blank Body Detected

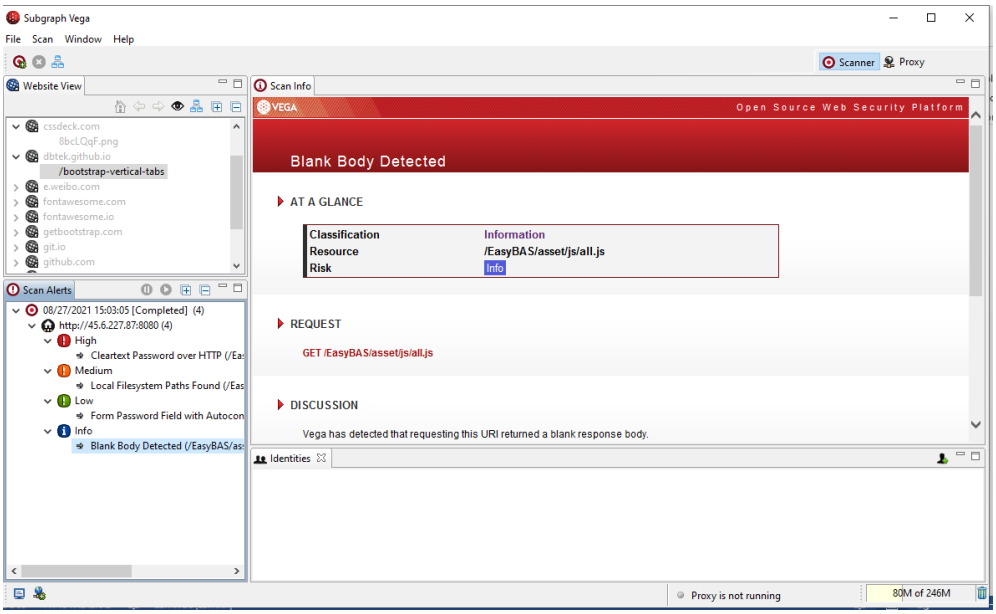


Figura 259: Cuerpo de respuesta en blanco

Solicitud

GET /EasyBAS/asset/js/all.js

Discusión

Vega ha detectado que al solicitar este URI se devuelve un cuerpo de respuesta en blanco.

3.5 Realización de Pruebas de Penetración

Una vez terminada la etapa de identificación de vulnerabilidades se procede con la explotación de las mismas, con el objetivo de explotar de manera exitosa y obtener acceso no autorizado a recursos o servicios del sistema vulnerable.

Ataque de Denegación de Servicios (DoS) mediante SlowHTTPTest

Los ataques "Slow HTTP" en aplicaciones web se basan en que el protocolo HTTP, por diseño, solicita que las peticiones que le llegan sean completas antes de que puedan ser procesadas. Si una petición HTTP no es completa o si el ratio de transferencia es muy bajo el servidor mantiene sus recursos ocupados esperando a que lleguen el resto de datos. Si el servidor mantiene muchos recursos en uso podría producirse una denegación de servicio (DoS)

SlowHTTPTest es una herramienta altamente configurable que simula algunos ataques de denegación de servicio de la capa de aplicación al prolongar las conexiones HTTP de diferentes maneras.

Es utilizado para buscar vulnerabilidades DoS en el servidor web, o simplemente para averiguar cuántas conexiones simultáneas puede manejar. SlowHTTPTest funciona en la

mayoría de las plataformas Linux, OS X y Cygwin, un entorno similar a Unix y una interfaz de línea de comandos para Microsoft Windows, y viene con un Dockerfile para facilitar aún más las cosas.

Para nuestro caso utilizamos slowhttptest que se instalara en Kali Linux mediante el siguiente comando: apt-get install slowhttptest

slowhttptest -c 500 -H -g -o ./output_file -i 10 -r 200 -t GET -u http://45.6.227.87 :8080/EasyBAS -x 24 -p 2

El comando se describe a continuación:

- **c:** Especifica el número objetivo de conexiones que se establecerán durante la prueba (en este ejemplo, 500, normalmente con 200 deberían ser suficientes para colgar un servidor que no tiene protección contra este ataque).
- **H:** Inicia slowhttptest en modo SlowLoris, enviando solicitudes HTTP sin terminar.
- **g:** Obliga a slowhttptest a generar archivos CSV y HTML cuando finaliza la prueba con la marca de tiempo en el nombre del archivo.
- **o:** Especifica el nombre del archivo personalizado, efectivo con -g.
- **i:** Especifica el intervalo entre los datos de seguimiento para las pruebas Slowrois y Slow POST (en segundos).
- **r:** Especifica la velocidad de conexión (por segundo).
- **t:** Especifica el verbo que se utilizará en la solicitud HTTP (POST, GET, etc.).
- **u:** Especifica la URL o IP del servidor que desea atacar.
- **x:** Inicia slowhttptest en modo de lectura lenta, leyendo las respuestas HTTP lentamente.
- **p:** Especifica el intervalo para esperar la respuesta HTTP en la conexión de prueba,

antes de marcar el servidor como DoSed (en segundos).

Ahora, ejecutamos el comando con el servidor de destino:

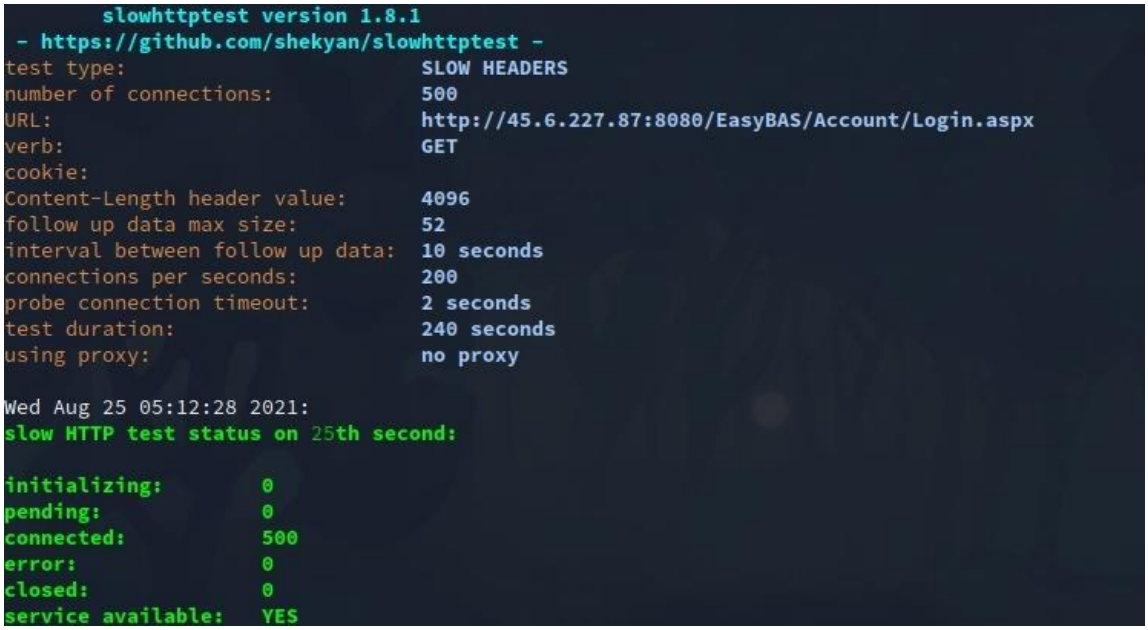


Figura 30: Ataque de Denegación de Servicios (DoS) mediante SlowHTTPTest

En la figura 30, se puede ver, que con 500 conexiones, el servidor no se bloquea en absoluto porque tenemos protección contra este tipo de ataques. El servicio disponible será siempre SÍ si se puede alcanzar el objetivo. La salida generada en HTML creada por nuestras opciones, será la siguiente:

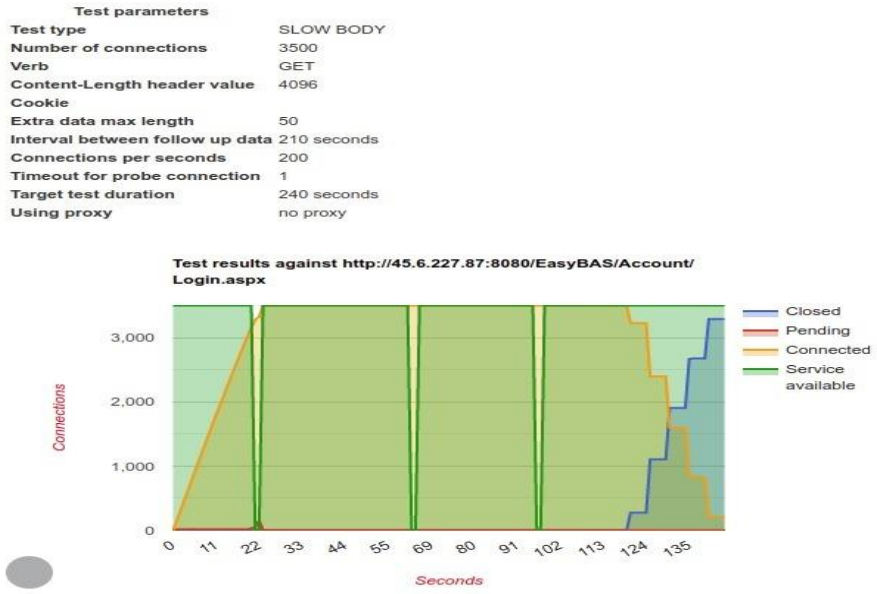


Figura 31: Resultados de SLOW BODY

Ahora desactivamos la protección contra ataques HTTP lentos en el servidor.

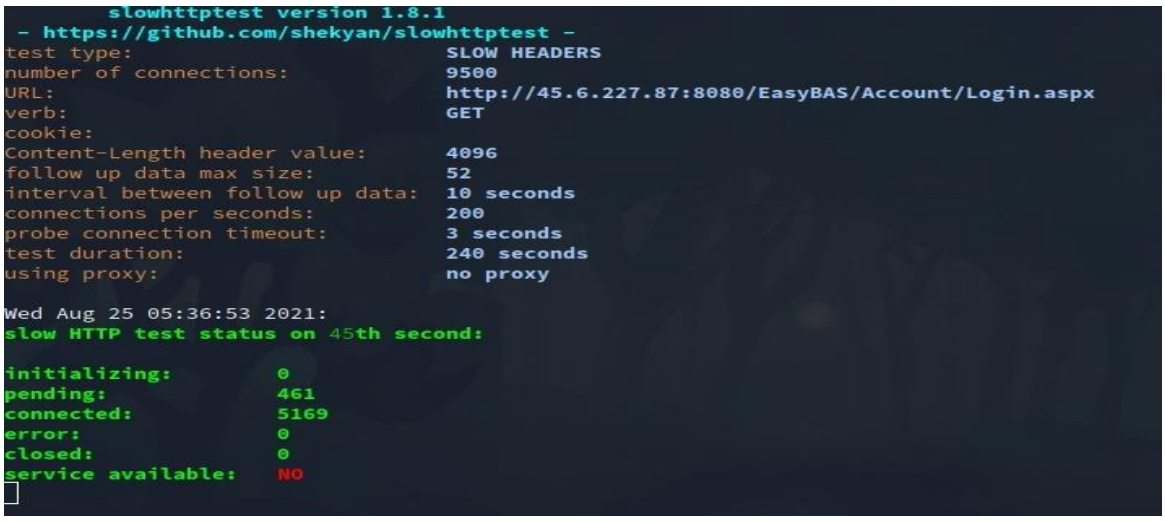


Figura 32: Servicio no accesible

En la figura 32, observamos que la salida es diferente y el sitio web en el servidor de destino no es accesible.

Figura 33: Servicio no disponible

En la figura 33, se observa que el servicio ya no está disponible.

Ataque por fuerza bruta

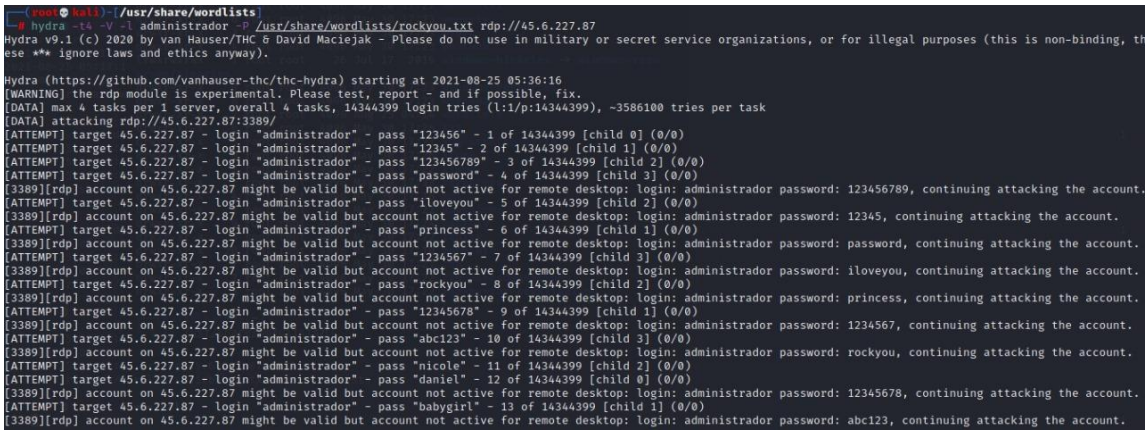
Un ataque de fuerza bruta ocurre cuando el atacante emplea determinadas técnicas para probar combinaciones de contraseñas con el objetivo de descubrir las credenciales de una potencial víctima y así lograr acceso a una cuenta o sistema. Existen diferentes tipos de ataque de fuerza bruta, como el "credential stuffing", el ataque de diccionario, el ataque de fuerza bruta inverso o el ataque de password spraying. Generalmente, los ataques de fuerza bruta tienen mayor éxito en los casos en los que se utilizan contraseñas débiles o relativamente fáciles de predecir.

Hydra

Es una de las aplicaciones más conocidas y utilizadas en hacking ético (y por piratas informáticos) para crackear contraseñas y conseguir acceder de forma no autorizada a redes y sistemas. Esta aplicación es totalmente gratuita y de código abierto y cuenta de base con más de 30 protocolos compatibles (sistemas operativos, webs, bases de datos, etc) donde intentar conseguir el acceso no autorizado crackeando y rompiendo contraseñas.

El comando se describe a continuación:

- **t:** Ejecutar TAREAS número de conexiones en paralelo (por host, predeterminado: 16)
- **V:** modo detallado / mostrar inicio de sesión + pase para cada intento / modo de depuración
- **l:** Indica el usuario del parámetro
- p**:** Esta opción indica una sola palabra que será utilizada como usuario.



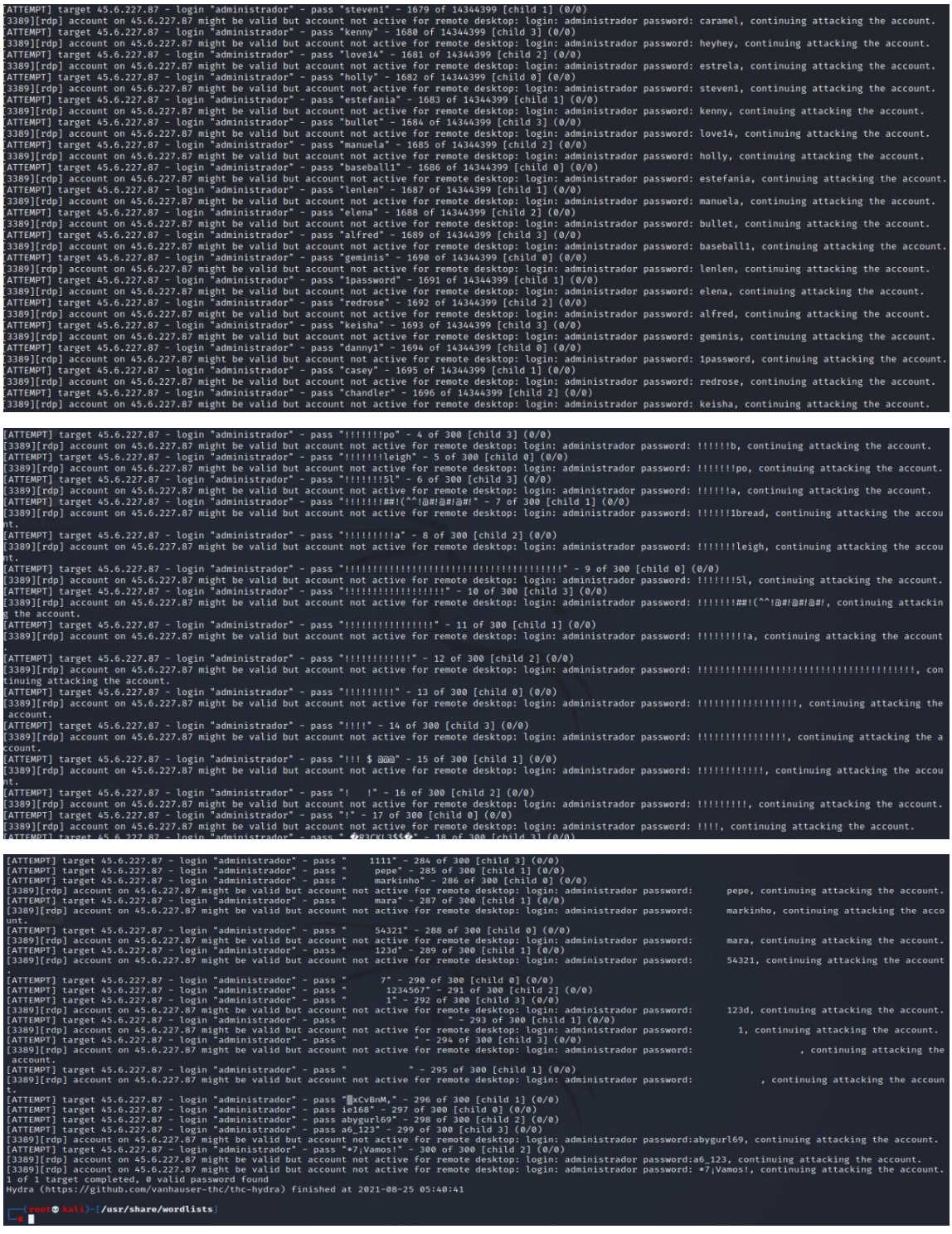


Figura 34: Ataque de fuerza bruta con Hydra

En figura 34, se observa que se tuvo éxito ya que se obtuvo las credenciales.

Una vez que se detectó vulnerabilidades se sugiere políticas de contingencia.

3.6 Elaboración de Políticas de Contingencia de Seguridad Informática que resguarde los activos informáticos de la Cooperativa de Transportes Flota Pelileo

Las Políticas de Contingencia de Seguridad Informática que se detallan tienen como objetivo ayudar a eliminar o reducir vulnerabilidades detectadas para proteger la Información junto con todos los activos de la Red Informática de la Cooperativa.

Política ante el mal uso de activos informáticos
• El personal de la Cooperativa debe comprometerse con la misma y de ser el caso firmar un compromiso de confidencialidad y el uso adecuado de los activos informáticos. • En caso de descubrir el mal uso de los recursos informáticos será reportado al departamento de Gerencia y de Sistemas para tomar medidas correctivas de manera inmediata. • La Gerencia conjuntamente con el Departamento de Sistemas debe planificar reuniones en las cuales se den a conocer las nuevas amenazas en lo que a Seguridad Informática se refiere.

Política ante el uso de dispositivos externos
• Queda prohibido el uso de dispositivos tecnológicos externos a la Cooperativa. • Para la utilización de dispositivos especiales se deberá pedir autorización con su respectiva justificación al Departamento correspondiente, y al departamento de TI siendo responsable del uso. • Se deberá informar al personal que los dispositivos ajenos a la Cooperativa como son discos externos, flash pueden ser transmisores de código malicioso como virus.

Política de administración de contraseñas
• Es responsabilidad del usuario garantizar la fortaleza de sus contraseñas. • Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos. Las contraseñas deben tener un mínimo de ocho (8) caracteres deben conformarse por al menos una letra mayúscula, una letra minúscula, un número y un carácter especial (+-*/@#$ %&). No debe contener caracteres especiales (vocales tildadas, ni eñes, ni espacios). • Evitar que la contraseña contenga: nombres de familiares, mascotas, fechas especiales, lugares visitados, secuencias como 123456, etc. • Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, deberá cambiarlo inmediatamente e informar al departamento de TI. • Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

Política para la confidencialidad de la información
• Está prohibido divulgar información fundamental de la Cooperativa por cualquier medio. • La información de la Cooperativa bajo ningún concepto podrá copiarse o distribuirse en cuentas de correo o almacenamiento remoto de índole personal.

Políticas de seguridad física y ambiental
• El Servidor debe contar con sistema de protección contra incendios, control de temperatura (aire acondicionado) permanente a una temperatura no superior a 22 grados centígrados y un sistema eléctrico de respaldo (UPS). • Los equipos que hacen parte de la infraestructura tecnológica, tales como servidor, estaciones de trabajo, cableado, UPS, dispositivos de almacenamiento, entre otros, deben estar protegidos y ubicados en sitios libres de amenazas como robo, incendio, inundaciones, humedad, agentes biológicos, explosiones, vandalismo y terrorismo. • El personal por ningún motivo puede reubicar los equipos de cómputo o de telecomunicaciones, ni retirar sellos de estos sin la autorización del personal de TI, debiéndose solicitar a la misma en caso de requerir este servicio. • Mientras se manipula el equipo de cómputo, no se deberán consumir alimentos ni ingerir líquidos. • El personal o funcionario deberá reportar de forma inmediata al departamento TI, cuando se presente algún evento como choques eléctricos, caídas, golpes o peligro de incendio.

Política de seguridad de área restringida
• Para acceder al servidor, el ingreso a las mismas debe ser con la autorización o vigilancia del encargado del departamento de sistemas. • El área donde se almacena la información importante deberá estar ubicado en un lugar que no esté expuesto a riesgos físicos y acceso al público.

Política de uso de software
• El personal no puede instalar ningún software que no esté autorizado por el departamento de TI y de ser el caso de debe pedir autorización con la debida justificación para su instalación. • Se restringe la instalación de software de dudosa procedencia por los riesgos que traen consigo en el caso que lo hicieran.

Política para el uso de redes
• Las redes fijas o móviles facilitadas por la Cooperativa de Transportes Flota Pelileo serán utilizadas dentro del ámbito laboral, es decir, bajo ningún concepto se accederá a páginas de contenido pornográfico, redes sociales personales, etc. • El departamento de sistemas con los directivos de la Cooperativa estipularan los estándares de los contenidos para uso laboral y administrativo en el caso de detectarse un mal uso de la red para fines recreacionales o ilícitos, para lo cual la TI debe notificar a Talento Humano para proceder a las sanciones respectivas. • El personal no puede intentar probar fallas de la Seguridad Informática, en caso de requerir estas pruebas deben ser aprobadas y controladas por departamento TI. • No se debe intencionalmente escribir, generar, compilar, copiar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño, acceso a las computadoras, redes o información de la Cooperativa.

Política ante Sistemas desactualizados
• Instalar un sistema que garantice la protección y estabilidad del servicio. • Aplicar constantemente los parches de seguridad que se publica por parte de los fabricantes y desarrolladores después del lanzamiento del producto.

Política ante Software desactualizado
• Decretar responsables que verifique las nuevas actualizaciones vulnerabilidades que se presenten en el software de uso cotidiano. • Las aplicaciones utilizadas en la Cooperativa se deben actualizar a sus versiones estables con sus respectivos parches de seguridad instalados, estén conectados a la red o no. • Verificar las actualizaciones del sistema operativo y los navegadores instalados.

Política ante certificados de seguridad caducados
• Todos los aplicativos Web deben contar con un certificado de seguridad (SSL) los mismos debe estar activos y actualizados. • El acceso a páginas sin un certificado SSL debe ser a través de una Red Privada Virtual(VPN).

Política de seguridad de equipos
• El Departamento de Sistemas deberá llevar un inventario actualizado de los recursos tecnológicos de software, hardware, licencias. • El encargado de TI debe verificar el cumplimiento sobre el cambio de contraseñas y administración de contraseña en el servidor, el cumplimento de la política debe ser registrado. • El mantenimiento lógico preventivo a los equipos de cómputo se debe realizar cada 6 meses y mantenimiento físico preventivo mínimo una vez por año, incluyendo el cableado estructurado. • Todos los equipos de cómputo deben tener instalado un Antivirus con su respectiva licencia.

Política ante pérdida de información
• Uno de los respaldos se debe almacenar en un sitio externo a la Cooperativa de una forma comprimida (recomendación). • Todos los sistemas de aplicaciones que manejen información sensible de la Cooperativa deben generar registros de bitácoras donde conste cambio y eliminación de información. • El encargado de TI con el Gerente debe examinar, desarrollar y mantener plan estratégico, planes de acción y planes de contingencia política.

Política ante configuraciones por defecto
• Para toda transferencia de archivos al servidor se deben usar protocolos de seguridad (SFTP, FTPS, SFTP). Además, es recomendable revisar las políticas de seguridad de los productos, logs de incidencias y realizar un monitoreo frecuentemente de las alertas. • Para realizar la configuración de un nuevo dispositivo o un sistema operativo de manera manual dejando activos exclusivamente los servicios que se vayan a utilizar y eliminar las configuraciones por defecto. • Configurar las aplicaciones y los servicios de red mediante un hardening del sistema operativo o servicio. • Proteger la cuenta de administrador mediante la creación y asignación de usuarios y roles.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- En la Cooperativa de Transportes Flota Pelileo no se ha ejecutado auditorías de seguridad informática para la detección de vulnerabilidades, no cuenta con herramientas que faciliten el análisis, detección y explotación de vulnerabilidades con esto puedo concluir que proyecto es favorable mediante la investigación de lo mencionado.

- Para realizar el presente proyecto de investigación se utilizó software libre evitando gastos extras, las herramientas utilizadas pueden ser recomendadas para dar un seguimiento al análisis y detección de vulnerabilidades dentro de la Cooperativa.

- Se ha cumplido con los objetivos del presente proyecto de investigación mediante el desarrollo del mismo, con el estudio y aplicación de herramientas de seguridad informática para la detección y explotación de vulnerabilidades facilitando como resultado Políticas de Contingencia de Seguridad Informática que deben ser aplicadas para eliminar o reducir vulnerabilidades existentes.

- La metodología OSSTMM v3 fue escogida de manera apropiada, ya que las secciones y módulos aplicados permitieron conseguir los resultados esperados en la detección de vulnerabilidades existentes en el servidor de la Cooperativa y así poder dar una propuesta de solución.

- Los servicios de Terminal Server remotos no están configurados para utilizar únicamente la autenticación de nivel de red (NLA). NLA utiliza el Protocolo de

proveedor de soporte de seguridad de credenciales (CredSSP) para realizar una autenticación sólida del servidor a través de Mecanismos TLS / SSL o Kerberos, que protegen contra ataques man-in-the-middle. Además de mejorar autenticación, NLA también ayuda a proteger la computadora remota de usuarios y software malintencionados al completar autenticación de usuario antes de que se establezca una conexión RDP completa.

- El servicio de Terminal Services remoto no está configurado para utilizar criptografía sólida.

- El uso de criptografía débil con este servicio puede permitir que un atacante espíe más las comunicaciones, fácilmente y obtener capturas de pantalla y / o pulsaciones de teclas.

- La herramienta Vega ha detectado un formulario que puede provocar el envío de una contraseña a través de un canal inseguro, esto podría resultar en la divulgación de contraseñas a los espías de la red.

- Las cookies pueden estar expuestas a intrusos de la red, las cookies de sesión son credenciales de autenticación; los atacantes que los obtienen pueden obtener acceso no autorizado a las aplicaciones web afectadas.

- Vega ha detectado lo que pueden ser rutas absolutas del sistema de archivos en el contenido escaneado, la divulgación de estas rutas revela información sobre el diseño del sistema de archivos, esta información puede ser sensible, su divulgación puede aumentar las posibilidades de éxito de otros ataques.

- Se puede almacenar un valor de contraseña en el sistema de archivos local del cliente, las contraseñas almacenadas localmente pueden ser recuperadas por otros usuarios o códigos maliciosos.

4.2 Recomendaciones

- Se sugiere mantener constantes capacitaciones en cuanto a la seguridad informática y ejecutar evaluaciones del correcto funcionamiento de los recursos informáticos para establecer las mejores prácticas relacionadas a reducir vulnerabilidades y errores de usuario final.

- Se recomienda al encargado de TI, optar por la metodología OSSTMM como referencia para el análisis de la seguridad, ya que la metodología presenta un proceso de evaluación de debilidades de una serie de áreas que refleja los niveles de seguridad presentes en la infraestructura a ser auditada, permite valorar los riesgos, vulnerabilidades que se puedan explotar y el impacto de una explotación real finalizando con un reporte incluyendo soluciones a los problemas de seguridad descubiertos.

- Se recomienda al Gerente conjuntamente con el encargado de TI utilizar y dar un seguimiento correcto a las Políticas de Contingencia de Seguridad Informática recomendadas con el objetivo de eliminar o reducir las vulnerabilidades detectadas, garantizado la integridad de la información junto con los activos de red informática.

- Habilite la autenticación de nivel de red (NLA) en el servidor RDP remoto. Esto generalmente se hace en el 'Remoto' pestaña de la configuración de 'Sistema' en Windows.

- Cambie el nivel de cifrado RDP a uno de High o FIPS Compliant.

- Las contraseñas nunca deben enviarse en texto sin cifrar. El formulario debe enviarse a un destino HTTPS.

- Al crear la cookie en el código, establezca el indicador de seguridad en verdadero.

- Las rutas absolutas se encuentran a menudo en la salida de error, Tanto los administradores del sistema como los desarrolladores deben ser conscientes, ya que el problema puede deberse a un error de la aplicación o una mala configuración del servidor, La salida de error que contiene información confidencial, como rutas absolutas del sistema, no debe enviarse a clientes remotos en servidores de producción, Esta salida debe enviarse a otro flujo de salida, como un registro de errores.

- La declaración del formulario debe tener un atributo de autocompletar con su valor establecido en "off".

BIBLIOGRAFÍA

[1] E. F. Zavala Vela et al., “Diseño e implementación de seguridades en la red de datos de la planta central del ministerio de educación y cultura del ecuador, aplicando la tecnología osstmm (open source security testing methodology manual); y, creación de políticas de seguridad mínimas para las subsecretarías, direcciones provinciales y cantonales de educación,” 2010.

[2] G. N. Huilca Chicaiza, “Hacking ético para detectar vulnerabilidades en los servicios de la intranet del gobierno autónomo descentralizado municipal del cantón cevallos.” [en línea]. Disponible en: http://repo.uta.edu.ec/handle/123456789/2900

[3] F. Miranda Silva “Auditoría de redes, aplicando la metodología OSSTMM V3, para el Ministerio de Inclusión Económica y Social” [en línea]. Disponible en https://repositorio.uta.edu.ec/bitstream/123456789/31313/1/t1716si.pdf

[4] J. F. Allaica Caranqui “Auditoría de la Seguridad Informática siguiendo la metodología OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL (OSSTMM) para la empresa MEGAPROFER S.A “[en línea]. Disponible en: https://repositorio.uta.edu.ec/bitstream/123456789/31313/1/t1716si.pdf

[5] M. Pilamunga, “Procedimiento de Auditoria para la Seguridad de las Redes LAN en los Laboratorios de Computadoras de la Escuela de Ciencias de la Facultad de Ingeniería Ciencias Físicas Y Matemática de la Universidad Central Del Ecuador,” Master's thesis, UNIVERSIDAD CENTRAL DEL ECUADOR, 2016.

[6] M. n. Mendoza, “Conoce los tipos de auditorías de redes y que puede revisar cada

una.” url: https://www.welivesecurity.com/laes/2015/04/20/auditorias-de-redes/, APR 2015.

[7] C. M. Razo, Auditoría en sistemas computacionales. Pearson Educación, 2002.

[8] M. T. ASSOCIATE, “Student study guide.” [en línea]. Disponible en: ftp://ftp.certiport.com/Marketing/Mta/docs/.

[9] A. Bahamontes, “Auditoría de seguridad informática,” antpji.com, 2013

[10] V. D. Casares, “Metodologías avanzadas de pen-test.” [en línea]. Disponible en: http://archivos.usuaria.org.ar/segurinfo2014/uruguay/agenda.html

[11] C. Tori, Hacking Ético. Mastroianni Impresiones, 2008.

[12] nmap.org, “Guía de referencia de nmap.” [en línea]. Disponible en: https://nmap.org/man/es/.

[13] D. Bradbury, “Computer fraud and security.” [en línea]. Disponible en: http://www.sciencedirect.com/science/article/pii/S1361372311701014, 2011.

[14] G. Inc, “Ayuda google.” [en línea]. Disponible en: https://support.google.com/vault/answer/2474474?hl=es, 2021.

[15] seguridadpublica.es, “Visualroute herramienta de ping, whois y traceroute.” [en línea]. Disponible en: http://www.seguridadpublica.es/2012/12/visualrouteherramienta-de-ping-whois-y-traceroute/, 2021.

[16] theharvester, “theharvester information gathering.” [en línea]. Disponible en:

https://code.google.com/p/theharvester/.

[17]] openvas.org, “El escáner de vulnerabilidades más avanzado del mundo open source.” [en línea]. Disponible en: http://www.openvas.org/about.html, 2021

[18] tenable network security, “Guía de instalación y configuración de nessus 5.0.” [en línea]. Disponible en: http://static.tenable.com/documentation, 2021.

[19] R. Svensson, From Hacking to Report Writing: An Introduction to Security and Penetration Testing. Apress.

[20] R. Ghaznavi-Zadeh, Kali Linux: Hacking Tools Introduction. Primedia Elaunch LLC.

[21] inforensicsuex, “Tests de penetración. explotación de vulnerabilidades con metasploit framework.” [en línea]. Disponible en: https://inforensicsuex.wordpress.com/2021/07/15/, 2021.

[22] sectools.org, “Thc hydra.” [en línea]. Disponible en: http://sectools.org/tool/hydra, 2015.

[23] J. Elks, “Man in the middle attack: Focus on sslstrip,” 2011

[24] L. Allen, T. Heriyanto, and S. Ali, Kali Linux â Assuring Security by Penetration Testing. Community experience distilled, Packt Publishing.

[25] https://www.kali.org/, “Kali linux.” [en línea]. Disponible en: https://www.kali.org/, 2021.

[26] C. Charles Cresson Wood, CISA, Políticas de Seguridad Informática - Mejores Prácticas Internacionales. Profesional, NetIQ, Inc., 1233 West Loop South 1800, Houston, TX 77027, 2002.

[27] R. Audi, The Cambridge Dictionary of Philosophy (2nd Edition). Cambridge University Press, 1999.

[28] C. O. S.A., "Itil Â® - gestión de servicios ti." [en línea]. Disponible en: http://itil.osiatis.es/, 2011.

[29] M. EYSSAUTIER De la Mora, "Metodología de la investigación: desarrollo de la inteligencia," México, Ecafsa, 2002.

[30] E. E. de Excelencia, "Gestión de riesgos iso 9001 plan de contingencias." [En línea]. Disponible en: https://www.escuelaeuropeaexcelencia.com/2016/09/gestion-de-riesgosplan-contingencia/ , Sep 2016. [Accedido: 30-junio-2021].

[31] F. Gutiérrez Benito et al., "Laboratorio virtualizado de seguridad informática con kali linux," 2014.

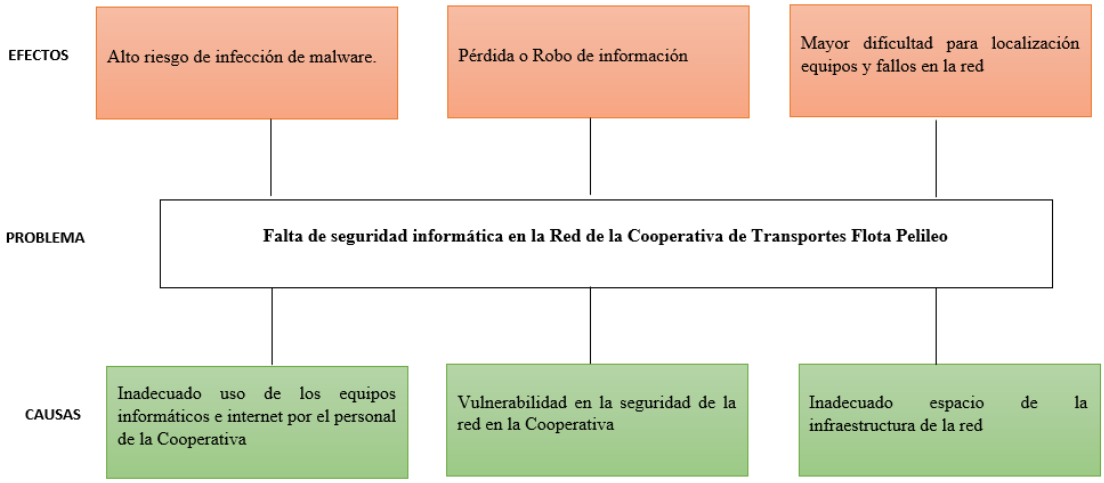
[32] D. Hoffman, D. Prabhakar, and P. Strooper, "Testing iptables," in Proceedings of the 2003 conference of the Centre for Advanced Studies on Collaborative research, pp. 80–91, IBM Press, 2003.

[33] J. Elks, "Man in the middle attack: Focus on sslstrip," 2011.

[34] uServers Comunicaciones, "Â¿ qué es el nic ?." [en línea]. Disponible en: http://web.uservers.net/ayuda/soluciones/dominios, 2015.

ANEXOS

Anexo 1: Árbol del problema



Anexo 1: Árbol del Problema
Elaborado por el investigador

Anexo 2: Ubicación de la matriz de la Cooperativa de Transportes Flota Pelileo

Anexo 2: Cantón Pelileo, Calle García Moreno y Montalvo.