UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE INGENIERÍA ELECTRÓNICA

IMPLEMENTACIÓN DE PRUEBAS DE HACKEO ÉTICO PARA EVALUAR EL SISTEMA DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RHELEC INGENIERÍA CIA. LTDA

Trabajo de titulación previo a la obtención del
Título de Ingeniero Electrónico

AUTORES: Roberto Javier Chango Saavedra
Daniela Alexandra Gualpa Sarabia

TUTOR: Jhonny Javier Barrera Jaramillo

Quito-Ecuador

2023

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Nosotros, Roberto Javier Chango Saavedra con documento de identificación N° 1722817309 y Daniela Alexandra Gualpa Sarabia con documento de identificación Nº 1721393708; manifestamos que:

Somos los autores y responsables del presente trabajo; y, autorizamos a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 06 de marzo del año 2023

Atentamente,

Roberto Javier Chango Saavedra
1722817309

Daniela Alexandra Gualpa Sarabia
1721393708

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Nosotros, Roberto Javier Chango Saavedra con documento de identificación N° 1722817309 y Daniela Alexandra Gualpa Sarabia con documento de identificación Nº 1721393708, expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Proyecto Técnico : "Implementación de pruebas de Hackeo Ético para evaluar el sistema de seguridad informática en la empresa Rhelec Ingeniería Cía Ltda.", el cual ha sido desarrollado para optar por el título de Ingeniero Electrónico en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 06 de marzo del año 2023

Atentamente,

Roberto Javier Chango Saavedra
1722817309

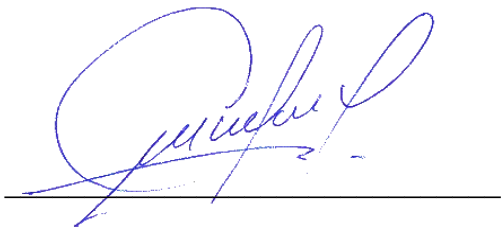
Daniela Alexandra Gualpa Sarabia
1721393708

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Jhonny Javier Barrera Jaramillo con documento de identificación N° 1400378475, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: IMPLEMENTACIÓN DE PRUEBAS DE HACKEO ÉTICO PARA EVALUAR EL SISTEMA DE SEGURIDAD INFORMÁTICA EN LA EMPRESA RHELEC INGENIERÍA CÍA LTDA., realizado por Roberto Javier Chango Saavedra con documento de identificación N° 1722817309 y por Daniela Alexandra Gualpa Sarabia con documento de identificación N° 1721393708, obteniendo como resultado final el trabajo de titulación bajo la opción Proyecto Técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 06 de marzo del año 2023

Atentamente,



Ing. Jhonny Javier Barrera Jaramillo, MsC

1400378475

DEDICATORIA

Al terminar esta etapa estudiantil, es mi deseo dedicar la presente tesis a mi Padre Juan, mi Madre Pilar y mi Hermana Elizabeth, quienes con su apoyo y amor incondicional han sido el pilar fundamental para la realización de este trabajo ya que juntos me inspiraron a la culminación de mi carrera y todo ese esfuerzo es dedicado a ellos.

Roberto

La presente tesis se lo dedico con todo mi amor y bondad a Dios, a mis padres Jaime Gualpa y Marlene Sarabia, cuyo esfuerzo, sacrificio y apoyo incondicional han sido primordiales en mi carrera profesional, sus buenos valores y principios me han hecho ser quien soy hoy.

Sus reglas y libertades me permitieron conocer lo bueno y lo malo de la vida, donde he podido tener una visión más clara de los triunfos y los deseos que anhelo obtener a partir de hoy.

A mí querido hijo Emiliano, por ser fuente principal de motivación e inspiración para poder culminar mis estudios, hijo mío hemos logrado un sueño más, a partir de hoy seguiré esforzándome para que la vida nos depare un futuro mejor.

A mis profesores y amigos por estar presente en cada triunfo y fracaso, compartiendo conocimiento, apoyo y ayuda que nos llevaran a tener una amistad duradera y cumplir muchos sueños más.

Daniela

AGRADECIMIENTOS

Con un profundo respeto agradezco a mis padres por su apoyo incondicional.

Un agradecimiento muy especial a mi tutor Ing. Jhonny quien, con su sabiduría, paciencia, apoyo y sus excelentes conocimientos contribuyeron para la realización de este trabajo, a cada uno de mis maestros que supieron brindarme valiosos conocimientos.

A mis más cercanos amigos, quienes formaron parte de esta etapa.

Finalmente quiero agradecer a la universidad Politécnica Salesiana, por brindarme un espacio como estudiante en tan prestigiosas instalaciones para obtener un estudio de calidad.

Roberto

Gracias a Dios por haberme permitido culminar la etapa final y haberme dado salud, fuerza e inteligencia para lograr mi objetivo de finalizar la carrera de Ingeniería Electrónica.

Agradezco a mis padres por darme la vida, educación, y total apoyo en todo lo que me he propuesto, gracias a mis hermanos, familiares por el apoyo incondicional.

Un cordial agradecimiento a nuestro tutor Ing. Jhonny, por permitirnos ser partícipes de este proyecto de titulación, por la confianza y el apoyo durante el desarrollo de este trabajo de investigación.

Gracias a mis profesores por tener la paciencia suficiente para transmitir sus conocimientos.

Gracias por creer en mí.

Daniela

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Rhelec Ingeniería, es una compañía que brinda asistencia en el campo de las Telecomunicaciones, la Ingeniería Eléctrica, y en servicios de Construcción, cumpliendo requisitos de calidad con sus usuarios y con la normativa permitida en materia de seguridad, salud y medio ambiente.

Actualmente esta compañía no aplica ninguna estrategia de seguridad para la administración de la información en su infraestructura tecnológica. Considerando, el alto uso de sus servicios de red, así como el intenso manejo de la información en sus diferentes áreas, se hace necesario diseñar y aplicar pruebas de penetración, teniendo como objetivo diagnosticar con precisión el estado de seguridad de la compañía a través de pruebas de ataque autorizadas y controladas para detectar vulnerabilidades que buscan aprovechar las debilidades percibidas en la línea base visible de la organización.

Para complementar las pruebas realizadas, se definirán estrategias tales como políticas de seguridad, reforzamiento de dispositivos hardening, con las respectivas actividades y procedimientos necesarios para garantizar que los recursos con sus respectivos activos de información estén protegidos.

PALABRAS CLAVES: Hardening, Hacking Ético, Metodologías y Análisis de Riesgos Informáticos, Seguridad Informática

ABSTRACT

Rhelec Ingeniería, is a company that provides assistance in the field of Telecommunications, Electrical Engineering, and Construction services, meeting quality requirements with its users and with the applicable regulations allowed in terms of safety, health and environment.

Currently this company does not apply any security strategy for the management of information in its technological infrastructure. Considering, the high use of its network services, as well as the intense information management in its different areas, it is necessary to design and apply penetration tests, aiming to accurately diagnose the security status of the company through authorized and controlled attack tests to detect vulnerabilities that seek to exploit the weaknesses perceived in the organization's visible baseline.

To complement the tests carried out, strategies such as security policies, reinforcement of hardening devices will be defined, with the respective activities and procedures necessary to ensure that the resources with their respective information assets are protected.

KEY WORDS: Hardening, Ethical Hacking, Methodologies and Computer Risk Analysis, Computer Security.

INTRODUCCIÓN

Hoy en día, muchas de las organizaciones públicas y privadas realizan procesos rutinarios que exigen la transferencia permanente de información valiosa sobre su infraestructura de red. De no ser controlados, estos procesos pueden tener y un alto riesgo de sufrir ataques como el robo, intercepción, duplicación o modificación de información e incluso ataques más agresivos que pueden producir incluso la interrupción total de sus procesos.

El presente trabajo de titulación, se concentra en la implementación de un conjunto de pruebas de hackeo ético para la detección de fallos y vulnerabilidades, además de emplear medidas y normativas de seguridad para regular el uso de sus activos de información, así como procesos de hardening para fortalecer la seguridad en sus dispositivos de hardware.

La documentación que respalda el siguiente trabajo, se divide en cuatro capítulos que se detallan a continuación.

En el capítulo uno se detalla los antecedentes, subdivididos en: planteamiento del problema, justificación, el desarrollo de objetivos tanto generales como específicos y el marco conceptual, donde se encuentran descritos los fundamentos teóricos más relevantes que conforman el proyecto.

En el capítulo dos se presenta un reconocimiento situacional en el cual se realiza una recopilación de información con respecto de la compañía a estudiar, en la cual se comprende la información más relevante como la ubicación, la misión y visión, los objetivos empresariales, etc.

Posteriormente, el tercer capítulo define el análisis de la metodología que se aplicó, la descripción y selección de herramientas que se utilizaron, la ejecución de las pruebas que se realizaron las cuales van de la mano con el reporte de vulnerabilidades y finalmente el análisis de riesgo de las mismas.

Finalmente, el capítulo 4 engloba las estrategias para mejorar las seguridades, donde se detallará los controles implementados, el análisis del equipamiento, la instalación y/o configuración de comandos y por último las pruebas realizadas con resultados positivos como la mejora en la operación, conectividad y desempeño de los cambios realizados.

CAPÍTULO 1

ANTECEDENTES

1.1 Planteamiento del Problema

Actualmente, muchas organizaciones cuentan con redes internas para transmitir mayores volúmenes de información digital, los desarrollos tecnológicos han hecho que estas instituciones sean parte de la evolución en el número de ataques de hackers a usuarios de Internet e Intranet en los últimos tres años. Las principales amenazas que asechan a las empresas ecuatorianas se concentran en ataques de ingeniería social y vulnerabilidades internas que provocan ataques como el robo de información confidencial, evidenciando que las empresas no han analizado e implementado recursos en el campo de la seguridad informática. La incipiente aplicación de pruebas de penetración de hackeo ético para el descubrimiento temprano de debilidades en los servicios de red privadas, es uno de los primordiales problemas que ponen en peligro la seguridad de las empresas. En el caso de la compañía Rhelec Ingeniería, no es la excepción, si bien se han implementado varios servicios de red y sus respectivos protocolos, sin embargo, hasta el momento nunca se h implementado herramientas para detectar vulnerabilidades existentes en su infraestructura. Rhelec Ingeniería cuenta con una intranet y sus respectivos equipamientos que no han sido sometidos a ninguna prueba técnica de "hacking ético" para detectar vulnerabilidades, dejando de lado la posibilidad de minimizar el nivel de riesgo de que su información sea modificada o a su vez robada en su totalidad.

1.2 Justificación

Con el aumento del consumo de los medios digitales y el acceso a los servicios de Internet, las organizaciones públicas y privadas del mundo actual se han visto en la obligación de ejecutar medidas de seguridad. Este proyecto define un conjunto de pruebas para la detección de brechas de seguridad existentes en la infraestructura de red tecnológica, a través de una estrategia metodológica de pruebas de hackeo ético sobre los activos tecnológicos de la empresa para detectar fallos y debilidades en su red interna. La importancia de este proyecto técnico considera el uso de las metodologías que permitan efectuar el proceso de identificación y recolección de datos para plantear medidas que

puedan hacer frente a las vulnerabilidades. El impacto del hacking ético y "Hardening", en este trabajo técnico tiene que ser determinante para minimizar los resultados de un posible acontecimiento de seguridad hacia la rotura de la Seguridad Informática de la empresa Rhelec Ingeniería. Los resultados permitirán identificar las fortalezas y debilidades encontradas en las brechas de seguridad.

1.3 Objetivos

1.3.1 Objetivo General.

Implementar una estrategia de fortalecimiento (hardening) del sistema de seguridad de la empresa Rhelec a partir de un conjunto de pruebas de hackeo ético para la detección de fallos y vulnerabilidades.

1.3.2 Objetivos Específicos.

- Determinar la línea base de la empresa Rhelec Ingeniería en el área de seguridad informática definiendo un estudio inicial de su infraestructura tecnológica
- Realizar un análisis comparativo sobre las metodologías y herramientas más importantes del hackeo ético existente en el mercado para el análisis de seguridades en empresas.
- Implementar un conjunto de pruebas de penetración sobre los activos tecnológicos en la empresa para la detección de vulnerabilidades en la misma
- Definir las recomendaciones y acciones correctivas para la seguridad informática a partir de los resultados obtenidos de las pruebas realizas.

1.4 Marco Conceptual

1.4.1 Seguridad Informática Guiada a Empresas.

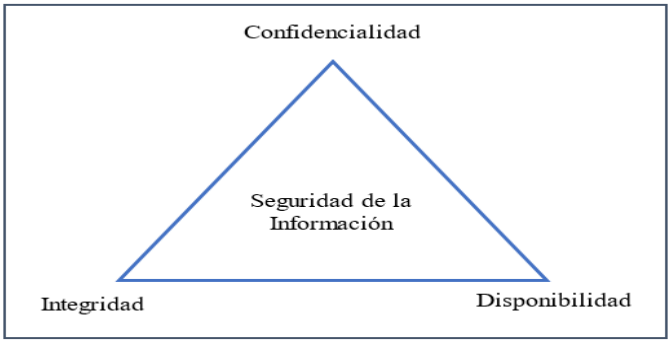
Es el procedimiento de evitar y descubrir el uso no lícito de redes informáticas e incluir evaluaciones y cuantificar los activos informáticos de una estructura, como datos, equipos y software. La seguridad informática es minimizar el riesgo, implementar medidas preventivas a través de políticas de seguridad y evitar cambiar o reemplazar la información almacenada. (Pacheco, 2018)

1.4.1.1 Principales Elementos que Cubren la Seguridad Informática.

Los elementos más relevantes de la seguridad informática denotan los tres pilares fundamentales, que se muestra en la Figura 1.1.

1. **Confidencialidad**: Usuarios autorizados que pueden acceder a la base de información
2. **Integridad:** Únicamente son los usuarios autorizados que pueden modificar las bases de datos necesarios.
3. **Disponibilidad:** Datos que deben estar aptos para el usuario cuando los necesite.

Figura 1.1 Triada C.I.A. Seguridad Informática

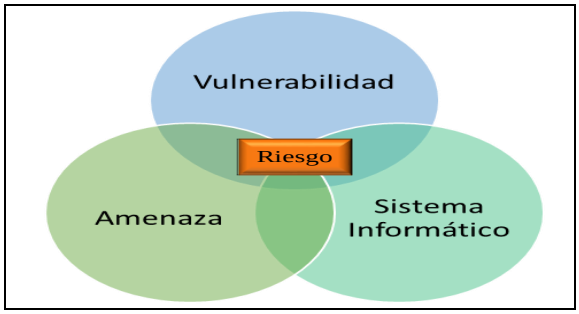


Fuente: Roberto Chango y Daniela Gualpa

1.4.2 Vulnerabilidad y Riesgo Informático.

El termino vulnerabilidad informática hace énfasis a las debilidades que se encuentran en los sistemas informáticos, ya que a través de la inseguridad un ciberdelincuente puede cometer cambios fraudulentos en las bases de datos que se encuentras en los sistemas de las organizaciones. (Mayorga, 2017). Según, (Juan, 2010) el riesgo se define como la probabilidad de que un incidente dañino ocurra cuando el haga efecto el impacto dentro de la organización.

Figura 1.2 Vulnerabilidades vs Amenazas de Riesgo Informático

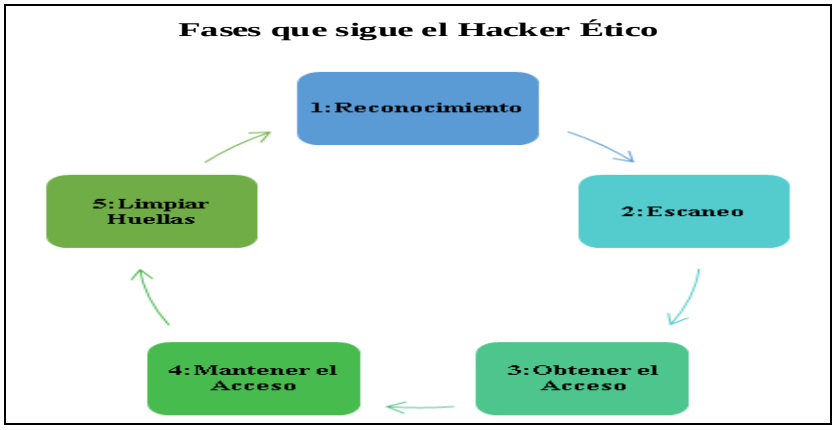


Fuente: Roberto Chango y Daniela Gualpa

1.4.3 Fases de Hacking Ético Guiada en Empresas.

Al momento de efectuar el hacking ético, es indispensable segmentar en cinco fases, estos ciclos son consideras a nivel mundial por reconocidos profesionales en Seguridad de la Información y Otorgado por la empresa EC-Council. (Tovar, 2020)

Figura 1.3 Fases de Hacking Ético



Fuente: Roberto Chango y Daniela Gualpa

(Fase 1) Reconocimiento: Fase inicial donde el profesional conocido como Hacker Ético investiga varias técnicas para encontrar el mayor número de datos de la organización que permite descubrir sospechas de ataques y vulnerabilidades dentro de un sistema operativo. (Fase 2): Escaneo: En esta fase es donde la exploración implica apoderarse de la información que fue recopilada en la fase anterior y examinar con el objetivó de detectar posibles ataques que permitan entrar en el sistema al momento de realizar un análisis de fallas de configuración o presencia de vulnerabilidades con el uso de metodologías y herramientas de Hacking Ético.

(Fase 3): Obtener Acceso: Esta es la fase donde el intruso ha conseguido acceder al sistema y se encarga de manipular la explotación de forma manual en las diversas vulnerabilidades encontradas en la fase de escaneo querrá mantener el acceso vulnerable para futuras explotaciones o ataques. (Fase 4): Manteniendo Acceso: En esta fase el Hacker Ético busca ampliar la variedad de herramientas, emplear archivos ocultos que permiten disponer de puertas traseras para el control de remoto de sistema manteniéndolo comprometido. (Fase 5): Limpiar Huellas: Después de haber realizado cada una de estas fases el Hacker Ético, genera un informe de evidencias de presencia dentro del sistema. También deberá cubrir las huellas para evitar el acceso comprometido a vulnerabilidades.

1.4.4 Tipos de Hackers.

1.4.4.1 Hacker Ético "White Hat".

Persona profesional en seguridad informática que posee conocimientos avanzados en tecnología, usa metodologías certificadas que mejoran los tiempos de respuesta ante vulnerabilidades en una fase de explotación dentro de la red (Burgos, 2019).

1.4.4.2 Ciberdelincuente "Black Hat".

Persona con habilidades y conocimientos en informática, tienen como objetivo infiltrar, romper y vulnerar las seguridades de los sistemas informáticos obteniendo información privilegiada, buscan tener un beneficio personal, económico y además lo hacen por emoción al espionaje.

1.4.5 Metodologías del Hacking Ético

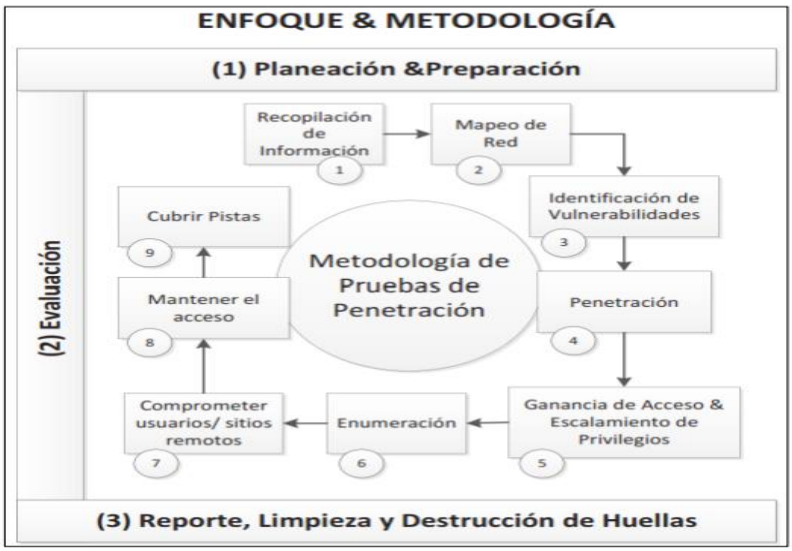
1.4.5.1 Metodología OSSTMM.

Esta norma OSSTMM mejor conocida como "Open Source Security Testing Methodology Manual", también identificada como una metodología en pruebas de seguridad de código abierto, según, (Olegario, 2021), "actualmente es uno de los estándares de referencia para los profesionales que realizan hacking ético", se guían a través de un grupo de procedimientos y métodos para ejecutar exploraciones dentro de los sistemas activos y pasivos de una organización, OSSTMM tiene varias etapas para inspeccionar la infraestructura de una red, aplicando el método de Hacking ético, también conocido como mapeo de seguridad.

1.4.5.2 Metodología ISSAF.

La metodología ISSAF es aplicable y cubre el análisis de seguridad en prácticamente cualquier entorno de cualquier entidad, independientemente de su tamaño. Esta metodología es compatible con el análisis del sistema en aparatos de red, sistemas de auditoria de bases de datos, sistemas operativos y aplicaciones. Otro elemento importante de ISSAF es la implementación de los requisitos normativos y las buenas prácticas. Este es un método específico para las pruebas de "pentesting". (Penagos, 2019). ISSAF debe cumplir 3 etapas para proteger la seguridad de la información en una organización y estas son: Planeación y preparación, Evaluación, Reporte y Borrar Huellas

Figura 1.4 Fases de la Metodología ISSAF



Fuente: (Penagos, 2019) Recuperado de ISSAFF

1.4.5.3 Metodología OWASP.

OWASP por sus siglas (Open Web Applicattion Project) es una idea global que tiene como finalidad ayudar a potenciar la seguridad del software en las aplicaciones, esta organización sin fines de lucro, además de mostrar la importancia de garantizar los criterios de seguridad en las aplicaciones, proporciona la información suficiente para gestionar los riesgos que implica conectar con los diferentes errores a nivel de código abierto, OWASP, determina un plan basado en un enfoque colaborativo donde cualquier profesional de la seguridad informática puede aportar su conocimiento,. (De Luz, 2021)

1.4.6 Herramientas para Hacking Ético.

1.4.6.1 Herramienta de Nmap.

Es un aplicativo de escaneo que identifica brechas de seguridad y análisis de red de código abierto. Nmap emplea paquetes IP "sin procesar" de una nueva forma para establecer qué computadoras están visibles en la red, los servicios (nombres y versiones de las aplicaciones) que ofrecen, los sistemas operativos (y sus versiones) que se desempeñen con el tipo de filtro de paquetes. Nmap se usa comúnmente para pruebas de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias como el inventario de la red, programar una actualización de servicio y monitorear el tiempo de apagado de una computadora o servicio. (Albacete, 2017)

1.4.6.2 Herramienta de Nessus.

Nessus es una herramienta profesional y con una alta popularidad a nivel mundial, ayuda a reducir la superficie de ataques de una organización y garantiza el cumplimento de los objetivos de detección de malware, detección de datos confidenciales, Nessus admite variedad de tecnologías que permiten escanear los sistemas operativos, dispositivos de red, Firewalls de última generación, servidores web e infraestructura crítica para detectar vulnerabilidades y amenazas. (Tenable, 2021)

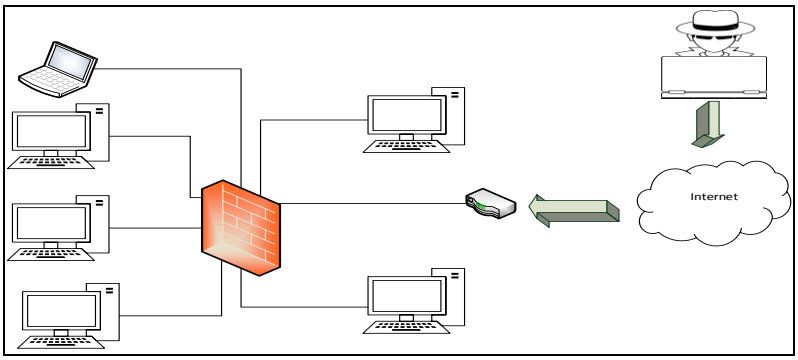
1.4.6.3 Herramienta de Metasploit.

Según (Ciberseguridad, 2021), Metasploit fue diseñado originalmente en el año de 2003 por HD Moore como una herramienta de red portátil basada en Perl . Además, esta herramienta es ideal para aprovechar el desarrollo y la mitigación de vulnerabilidades contra un dispositivo de red remota, te posibilita llevar a cabo testeos de seguridad, intentando y desarrollando tus propios exploits. Metasploit se creó inicialmente en un lenguaje de programación llamado Perl y se ha vuelto a escribir completamente en Ruby.

1.4.7 Hardening.

El Hardening es un conjunto de procesos de endurecimiento y/o robustez de la seguridad informática, su principal fin es proteger los activos tecnológicos de una organización, este proceso de configuración busca minimizar las vulnerabilidades, entorpecer al atacante y mejorar el tiempo de respuesta ante la presencia de amenazas de forma interna y/o externa en el software y hardware de un sistema operativo. (KIMAT, 2018). Eliminar usuarios, el cierre de puertos inutilizables, la eliminación de servicios innecesarios, son acciones para endurecer la red.

Figura 1.5 Esquema de Seguridad (Hardening)



Fuente: Roberto Chango y Daniela Gualpa

CAPÍTULO 2

ANÁLISIS SITUACIONAL

2.1 Información Empresarial

La compañía Rhelec Ingeniería. Inició sus procesos en el 2005, y ofrece una gama de servicios enfocados, en los sectores civil, eléctrico y de las telecomunicaciones. Su ámbito de operación principalmente se enfoca en proyectos de montaje estructural, construcción civil y mantenimiento eléctrico, garantizando la calidad y excelencia global de cada obra, adaptándose siempre a las necesidades del mercado y consiguiendo la satisfacción del cliente. (Rhelec, Ingenieria, 2021)

2.2. Línea de Negocio y Servicio de la Empresa

(Rhelec, Ingenieria, 2021), compañía que presta servicios en los sectores de Ingeniería Eléctrica, Telecomunicaciones y la Construcción, cumpliendo con los requisitos de las normativas legales adaptables en materia de seguridad, salud y medio ambiente. Siempre trabajando por la mejora continua en:

Servicios de mantenimiento y soporte de radio bases, equipamiento, transmisión, mantenimientos (Emergentes, Correctivos, Preventivos), convirtiéndose en un proveedor de servicios calificados con apoyo económico, salud ocupacional, seguridad laboral con cobertura 24/7 en todas las provincias de la Costa, Sierra, Oriente y Región Insular. La empresa se dedica al diseño de construcciones en: Administración y procesamiento de información, análisis de datos, KPI, SLA, mesa de gestión y operaciones 24/7, monitoreo de alarmas, Dashboards, Automatizados Qlik Sense, Network Operation Center.

2.3 Descripción de la Infraestructura Tecnológica

La topología de red con la que fue diseñada y se mantiene hasta la fecha en la empresa Rhelec Ingeniería es de tipo estrella utilizada por su eficiencia y simpleza. Para que la red de la empresa admita una amplia diversidad de aplicaciones y servicios, la arquitectura de red debe cumplir con las expectativas de los internautas en cuanto a tolerancia a deficiencias, escalabilidad, condición de servicio y confianza. En la siguiente

tabla se menciona los distintos dispositivos que existen en los distintos departamentos que conforma la empresa Rhelec.

Tabla 2.1. Dispositivos Activos y Pasivos de las diferentes áreas de la Empresa.

DISPOSITIVO ACTIVO	DISPOSITIVO PASIVO	ÁREA
2 computadoras	4 cable de red	CONSTRUCCIONES
2 teléfono IP	2 toma de datos RJ45	
1 Access Point	1 canaleta	
3 computadoras	6 cable de red	CONTABILIDAD
3 teléfono IP	3 toma de datos RJ45	
1 impresora	1 canaleta	
2 computadoras	4 cable de red	TALENTO HUMANO
2 teléfono IP	2 toma de datos RJ45	
1 impresora de red	1 canaleta	
2 computadoras	4 cable de red	BODEGA Y ACTIVOS
2 teléfono IP	2 toma de datos RJ45	
2 cámara IP	1 canaleta	
2 computadoras	4 cable de red	VEHÍCULOS
2 teléfono IP	2 toma de datos RJ45	
1 cámara IP	1 canaleta	
1 computadora	2 cable de red	RECEPCIÓN
1 teléfono IP	1 toma de datos RJ45	
1 impresora de red	1 canaleta	
1 computadora	2 cable de red	COMPRAS
1 teléfono IP	1 toma de datos RJ45	
1 cámara IP	1 canaleta	
1 computadora	2 cable de red	SISTEMAS
1 teléfono IP	1 toma de datos RJ45	
1 Access Point	1 canaleta	
1 computadora	2 cable de red	TALLER ELÉCTRICO
1 teléfono IP	1 toma de datos RJ45	
1 cámara IP	1 canaleta	
1 computadora	2 cable de red	SEGURIDAD INDUSTRIAL
1 teléfono IP	1 toma de datos RJ45	
1 cámara IP	1 canaleta	
1 computadora	2 cable de red	GUARDIANÍA
1 teléfono IP	1 toma de datos RJ45	
1 cámara IP	1 canaleta	
3 computadoras	30 cable de red	SERVIDORES
2 switch	1 toma de datos RJ45	
1 Router	3 rack	
1 modem	2 patch panel	
1 cámara IP	5 canaleta	

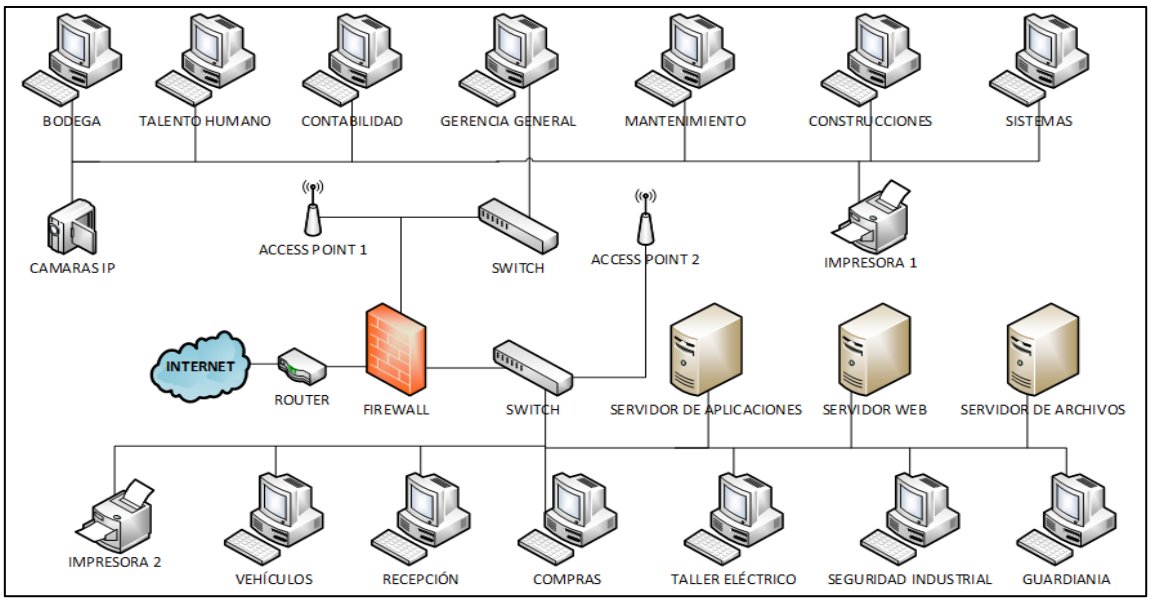
Fuente: Roberto Chango y Daniela Gualpa

Los servicios que existen en la red de la empresa son los siguientes:

- Servidores de: Archivos, Aplicaciones, Web.
- Servicio de WLAN, impresora de red, DHCP, Telefonía IP y cámaras IP.

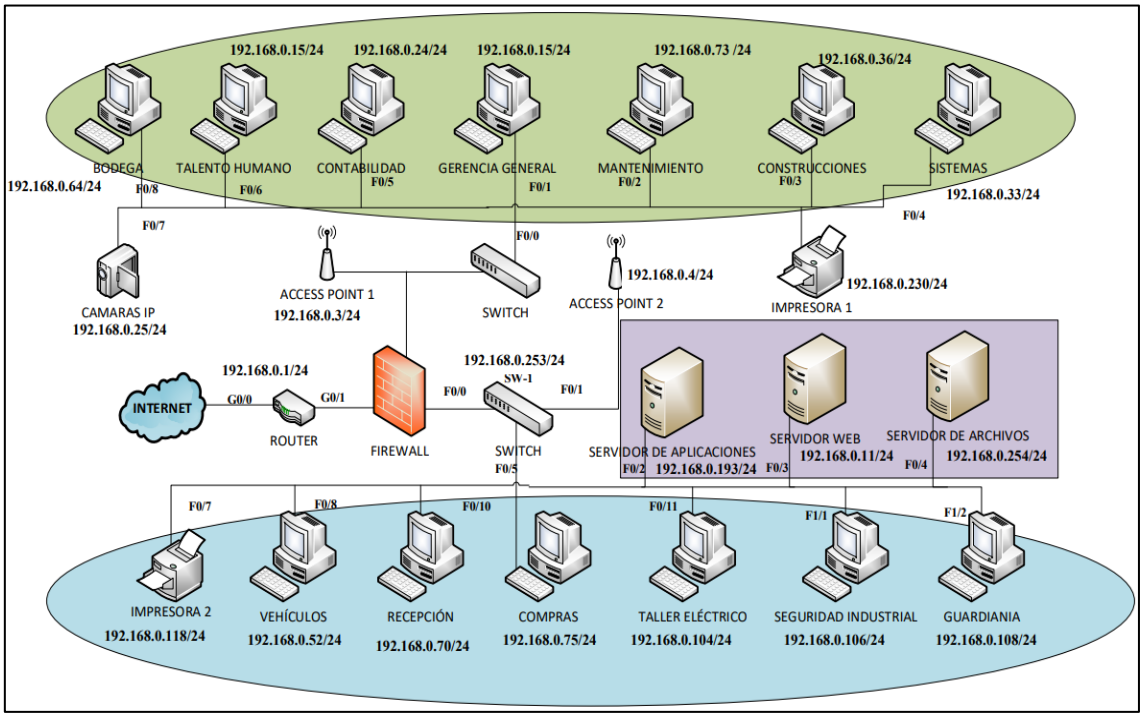
La empresa Rhelec Ingeniería cuenta con un enlace de acceso a internet por fibra óptica provisto por la empresa Fibramax con un ancho de banda de 20MB.En la figura 2.1 y figura 2.2 se ilustra cómo está conformada la topología física y lógica de la red empresa Rhelec Ingeniería.

Figura 2.1 Topología Física de la red de la empresa Rhelec Ingeniería CIA Ltda.



Fuente: Roberto Chango y Daniela Gualpa

Figura 2.2 Topología Lógica de la red de la empresa Rhelec Ingeniería.



Fuente: Roberto Chango y Daniela Gualpa

En la siguiente tabla se define el direccionamiento IP de red por áreas que conforma la topología de Red de la empresa Rhelec Ingeniería.

Tabla 2.2 Direccionamiento IP de dispositivos que se encuentran en la Empresa

EQUIPOS	DIRECCIÓN IP	MÁSCARA
Gerencia General	192.168.0.15	255.255.255.0
Construcciones 1	192.168.0.36	255.255.255.0
Construcciones 2	192.168.0.62	255.255.255.0
Mantenimiento 1	192.168.0.73	255.255.255.0
Mantenimiento 2	192.168.0.74	255.255.255.0
Mantenimiento 3	192.168.0.85	255.255.255.0
Mantenimiento 4	192.168.0.87	255.255.255.0
Mantenimiento 5	192.168.0.89	255.255.255.0
Contabilidad 1	192.168.0.24	255.255.255.0
Contabilidad 2	192.168.0.29	255.255.255.0
Talento Humano 1	192.168.0.40	255.255.255.0
Talento Humano 2	192.168.0.44	255.255.255.0
Vehículos 1	192.168.0.52	255.255.255.0
Vehículos 2	192.168.0.53	255.255.255.0
Bodega 1	192.168.0.64	255.255.255.0
Bodega 2	192.168.0.67	255.255.255.0
Recepción	192.168.0.70	255.255.255.0
Compras	192.168.0.75	255.255.255.0
Sistemas	192.168.0.33	255.255.255.0
Taller Eléctrico	192.168.0.104	255.255.255.0
Seguridad Industrial	192.168.0.14	255.255.255.0
Guardianía	192.168.0.16	255.255.255.0
Access Point Primario	192.168.0.4	255.255.255.0
Access Point Secundario	192.168.0.3	255.255.255.0
Servidor de archivos	192.168.0.254	255.255.255.0
Servidor de aplicaciones	192.168.0.193	255.255.255.0
Servidor web	192.168.0.11	255.255.255.0
Router	192.168.0.1	255.255.255.0
Switch	192.168.0.253	255.255.255.0
cámaras IP	192.168.0.25	255.255.255.0

Fuente: Roberto Chango y Daniela Gualpa

2.4 Descripción de la Problemática de la Empresa en Cuanto a Seguridades Informáticas.

Por medio de una encuesta realizada exclusivamente a los funcionarios del departamento de sistemas (Anexo 1), se pudo conocer que desde la fundación de la empresa Rhelec hasta la fecha actual, nunca se ha realizado ningún tipo de pruebas de

hackeo ético (pentesting). Las personas encargadas del área de sistemas no tienen el control sobre las operaciones de las áreas empresariales de la organización. Se detectó además que la red inalámbrica (WLAN) permite libre navegación sin ninguna restricción de acceso, lo cual la hace vulnerable y proclive al acceso a sitios no permitidos.

Ciertas preguntas que están generalmente realizadas a los departamentos de mantenimiento, contabilidad, bodega, recepción, vehículos y compras, se pudo detectar varias problemáticas que se mencionan a continuación:

- El departamento de bodega, recepción y compras, son las áreas más sensibles de la empresa en cuanto a seguridad informática, debido a que sus respectivos ordenadores de trabajo no tienen un sistema operativo actualizado. Actualmente están operando con Windows 7, y ya han dejado de ser efectivos, convirtiéndose en serios problemas de seguridad, por esta razón es urgente instalar actualizaciones de los SO para garantizar la seguridad. Hace poco tiempo, el departamento de bodega sufrió un incidente de seguridad informática debido a la descarga de archivos adjuntos con contenido malicioso enviados desde correos desconocidos. Por otra parte, algunas de las computadoras de esta área no cuentan con software antivirus.
- También, se logró observar que en algunos sistemas informáticos de la organización permiten escalar diferentes niveles de permisos para acceder a secciones de forma discrecional. Se requiere la reconfiguración de los permisos de estos sistemas en función de los perfiles de los usuarios y de esa manera se minimizan los riesgos de sufrir todo tipo de ataques.
- La mayoría de empleados de la compañía no son conscientes de la importancia de la seguridad de la información, y tampoco se ha definido programas de formación y/o capacitación para prevenir ataques de seguridad informática. En cuanto a las contraseñas que utilizan en sus computadoras de trabajo, no utilizan una combinación robusta entre números y caracteres. Algunos empleados incluso no utilizan contraseñas, se pudo observar que en distintos puestos de trabajos los usuarios tienen sus contraseñas escritas en un papel adhesivo pegado en las pantallas de su equipo.

2.5 Análisis de los Problemas Detectados

Gracias a la encuesta realizada al personal de la empresa se ha podido obtener varias evidencias acerca de la problemática de ciberseguridad antes mencionadas que

tiene actualmente la organización, para así determinar una línea base. Las distintas pruebas de penetración dentro de la red local de la empresa permitirán evaluar de manera objetiva los problemas detectados dentro del sistema de seguridad informático de la organización que permitan establecer estrategias de mejora en cuanto a fortalecimiento (hardening) en la seguridad de la misma.

Los problemas de ciberseguridad pueden poner en riesgo la información confidencial y la reputación de una empresa y tener un impacto financiero, en la imagen u operación muy significativa en cualquier negocio. Al momento de abrir y/o descargar archivos de correos electrónicos desconocidos puede tratarse de un ataque de phishing que es un método para obtener contraseñas. Este tipo de ofensiva funciona mediante el remitir correos electrónicos de phishing o sitios web falsos a usuarios ingenuos.

Los equipos que no tienen una constante actualización en su sistema son más propensos a recibir un ataque rasomware. Actualmente es importante que las organizaciones inviertan una parte de su presupuesto al departamento de seguridad de la información, a través de sistemas de ciberseguridad, tanto para la protección de los usuarios como para los datos informáticos confidenciales que existe dentro de la empresa. Muchas empresas nacionales e internacionales no se sienten completamente protegidas ante un ciberataque, ya sea porque son necesarias actualizaciones constantes de software o porque no brindan soporte técnico para mantener sus sistemas informáticos en óptimas condiciones. El parque tecnológico de una empresa, independientemente de su tamaño o tipo, puede ser vulnerable a cualquier ciberataque. En este sentido, una buena gestión de la indagación es fundamental para tomar medidas preventivas y correctivas necesarias.

CAPÍTULO 3

METODOLOGÍA
HACKING ÉTICO PARA LA DETECCIÓN DE VULNERABILIDADES

El presente capítulo se describe la implementación de un conjunto de pruebas de hackeo ético para el descubrimiento de amenazas y susceptibilidad en la infraestructura de la empresa Rhelec, conjuntamente con la metodología y herramientas para implementar dichas pruebas.

3.1 Tipo de Investigación

Se utilizarán métodos de investigación con un enfoque deductivo e inductivo para las estrategias de operaciones lógicas y a través de diversas técnicas y herramientas para describir hechos más detallados respecto a la seguridad informática y la ética del hacking.

3.1.1 Método Deductivo.

Se realizará un análisis de conceptos generales hacia los más específicos, para inferir en el descubrimiento de vulnerabilidades y su posterior explotación ayudarán a su identificación, determinar el estado actual de la seguridad en la empresa Rhelec y determinar los controles prácticos para contrarrestar amenazas potenciales que logren posibles atentados informáticos.

3.1.2 Método Inductivo.

De un supuesto general hasta conceptos específicos, se da pasó a la condición actual de seguridad de la organización para establecer los factores que se aplicaran para complementar o crear una estrategia de seguridad en la empresa Rhelec. Se pretende seleccionar los aplicativos de software adecuados para realizar las simulaciones propuestas en el proyecto. La documentación va de la mano con el desarrollo diario de cada fase presentada para este proyecto.

3.1.3 Planeación del Proyecto.

Teniendo en cuenta que los principales objetivos del plan son: Analizar las metodologías y herramientas más importantes del hackeo ético para detectar

vulnerabilidades de la infraestructura de la red física y lógica de la organización, se prevén las siguientes actividades:

3.1.4 Análisis Comparativo de Metodologías para Identificar Vulnerabilidades en la Seguridad Informática.

Para realizar este análisis, se seleccionaron varias metodologías como ISSAF, OSSTM, OWASP, PTES, principalmente por sus características de auditoria que tienen enfoques similares en cuanto a la evaluación de la seguridad informática, se procedió a investigar la información de cada una de ellas, las cuales se encuentran planteadas en el **subcapítulo (**1.4.5 Metodologías del Hacking Ético**).**

Estas metodologías seleccionadas proporcionan un modelo de propuesta para integrar diferentes mecanismos específicos para pruebas de pentesting con la capacidad de evaluar las diversas vulnerabilidades en el sistema informático **y** aplicaciones web. Para determinar la metodología adecuada a utilizar en la infraestructura empresarial de Rhelec, se detalla en la tabla 3.1 la comparación de los indicadores asegurándose que cumplan con garantizar el trabajo completo que proporciona un enfoque sistemático desde la planificación, evaluación y mejora continua

Tabla 3.1 Comparación de las Metodologías.

CARACTERÍSTICAS	METODOLOGÍAS			
INDICADOR	**ISSAF**	**OSSTM**	**OWASP**	**PTES**
Determina los pasos a seguir para una buena evaluación	**SI**	NO	NO	NO
Permite realizar estudios de seguridad en cualquier sistema informático	NO	NO	**SI**	NO
Contiene un modelo para realizar pruebas	**SI**	NO	NO	**SI**
Determina las áreas de alcance	**SI**	**NO**	**SI**	**NO**
Contiene muestras de pruebas y resultados	**SI**	**SI**	**SI**	**SI**
Define técnicas para la evaluación	**SI**	**NO**	**SI**	**NO**
Publicación de evaluaciones de riesgos	**SI**	**SI**	**SI**	**SI**
Herramientas recomendadas para cada prueba	**SI**	**NO**	**SI**	**NO**
Enumera y categoriza las vulnerabilidades que se han encontrado	**SI**	**NO**	**NO**	**NO**
Determina las dimensiones de seguridad a evaluar	**NO**	**SI**	**NO**	**SI**

Es un estándar	NO	SI	SI	NO
Creación de informes	SI	SI	SI	SI
Recomendaciones	SI	NO	NO	SI
Contiene referencias a documentos y enlaces	SI	NO	SI	NO
Envía reseñas de aplicaciones web	SI	NO	SI	NO
Envía acuerdo de confidencialidad	SI	SI	NO	NO
Mantiene actualizaciones	SI	SI	SI	NO

Fuente: (Zea, 2019) Recuperado de Comparaciones de Metodologias en aplicaciones web. Universidad Técnica de Machala

Luego de esta comparación, en la Tabla 3.1 se seleccionó la metodología ISSAF para las pruebas de hackeo ético porque nos permite abordar todos los aspectos relevantes que ofrece una propuesta viable y de alto valor para abordar áreas clave de la seguridad de la información en la empresa, mediante un modelo que se ajusta a los escenarios reales para las pruebas realizadas, además permite documentar los procesos de manera clara y consistente en este proyecto de tesis.

3.1.5 Metodología ISSAF para Realizar Hacking Ético.

Para el desarrollo de este proyecto, se optó por la metodología **ISSAF** de la **OISSG** (Open Information SystemsSecurity Group), misma que se basa en la evaluación y análisis de ciberseguridad y aplicaciones. Las directrices metodológicas se centran en las siguientes tres fases:

Figura 3.1 Fases Metodología ISSAF

Fuente: Roberto Chango y Daniela Gualpa

Fase 1 - Planeación y Preparación): Durante esta etapa el punto inicial es proceder con el intercambio de información con la organización para preparar y planificar los procesos de pruebas de Pentesting. Además se debe mencionar la persona responsable, las fechas y horas de las pruebas y otras evaluaciones.

Tabla 3.2 Plan de Auditoría Empresa Rhelec.

PLAN DE AUDITORÍA DE SEGURIDAD EN LA INFRAESTRUCTURA DE LA RED											
HACKING ÉTICO											
Empresa:	RHELEC INGENIERÍA CIA LTDA.	Departamentos									
No. Auditoría	1	Gerencia General	Mantenimiento	Construcción	Contabilidad	Talento Humano	Vehículos	Bodega	Recepción	Sistemas	Seguridad Industrial
Objetivo	Examinar vulnerabilidades de seguridad en las redes inalámbricas para implementar planes de acción que ayuden a mitigar las vulnerabilidades descubiertas										
Alcance	Verificar la condición actual de la estructura de la red.										
Metodología	ISSAF										
Estado y estimación del Proceso											
Se revisarán todas las medidas de seguridad de la red inalámbrica para el diagnóstico, por cada vulnerabilidad descubierta											
AUDITORES											
Auditor General:	Roberto Chango & Daniela Gualpa										

Fuente: Roberto Chango y Daniela Gualpa

Fase 2 - Evaluación: Durante esta etapa se aplicó la estructura del método ISSAF de hacking ético, que permitió identificar puntos de acceso e introducir un enfoque de múltiples capas, los procesos implementados son. Recopilación de datos, mapeo de red, identificación de servicios vulnerables en puertos abiertos, lista de vulnerabilidades descubiertas, evaluación de impacto y determinar las rutas de ataque.

Fase 3 - Reportes: Se preparará un informe de evaluación de seguridad de TI que detallará las vulnerabilidades identificadas e implementará las recomendaciones basado en controles de seguridad (Hardening)

3.2 Herramientas para Aplicar Hacking Ético

Para realizar hackeo ético mediante pruebas de pentesting se utilizará el sistema operativo especializado en herramientas de ciber seguridades Kali Linux que se aplica ampliamente en el desarrollo de auditorías informáticas. El dispositivo que se utilizará es una computadora portátil conectada a la trama local de la empresa con las siguientes características:

- Sistema operativo: Kali Linux 2022.1

- Procesador: Intel(R) Core (TM) i5-1035G1
- Ram: 12 GB

Las herramientas de Kali Linux que se utilizarán para las diferentes pruebas de penetración son de código libre y comercial. En la tabla 3.3 se definen los equipos seleccionados para las pruebas de pentesting según las áreas más sensibles identificadas anteriormente.

Tabla 3.3 Equipos seleccionados para las pruebas de pentesting

MÁQUINA	IP
Servidor de Archivos	192.168.0.254 /24
Servidor Web	192.168.0.11 /24
Servidor de Aplicaciones	192.168.0.193 /24
Access Point Primario	192.168.0.4 /24
Router de Internet	192.168.0.1 /24

Fuente: Roberto Chango y Daniela Gualpa

3.3 Diseño de Pruebas y Escenario para las Pruebas de Hackeo Ético

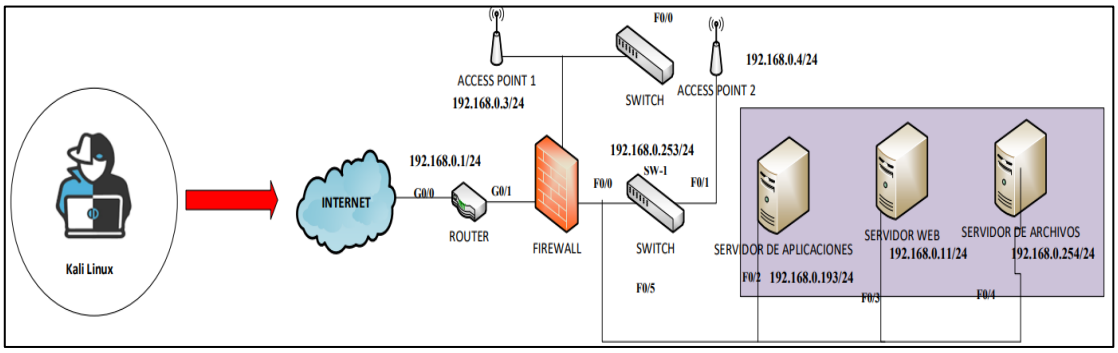
Para poder ejecutar las pruebas de pentesting, se realiza un diseño de las mismas, las cuales consta de lo siguiente:

- En primera instancia, se realizará una breve planeación de checklists de pruebas de red, como conectividad entre el host atacante y la host víctima, para no tener problema al momento de mapear los hosts y así asegurar la efectividad.
- Después, para examinar el reconocimiento de la trama local se utilizará la herramienta Nmap, la misma que permitirá obtener información valiosa acerca de los hosts que están conectados a la red tales como: su SO, los puertos abiertos, servicios y la versión que están ejecutando.
- Posteriormente, para el reconocimiento de vulnerabilidades se utilizará la herramienta Nessus, la cual servirá para descubrir esas vulnerabilidades encontradas por orden de criticidad y de forma gráfica. También da información de que exploits se pueden utilizar para romper la brecha de seguridad en las vulnerabilidades encontradas y soluciones para evitar las mismas.
- Finalmente, para la explotación de las vulnerabilidades se utilizará la herramienta de Metasploit, con el fin de contrarrestar las vulnerabilidades encontradas en los equipos que han sido víctimas de ataques utilizando códigos de explotación. Una

vez que la máquina víctima fue hackeada, los atacantes buscan escalar privilegios para mantener el acceso y analizar toda la información del equipo. Para terminar con las pruebas de pentesting, se eliminan las huellas del ataque para no generar inconvenientes en la máquina testeada.

Se diseña un escenario de pruebas que incluye: el atacante que se ejecuta en una laptop con una distribución Kali Linux, una WLAN, y los diferentes dispositivos que se van auditar, es decir:

Figura 3.2 Escenario de pruebas de pentesting



Fuente: Roberto Chango y Daniela Gualpa

3.4 Ejecución de Pruebas de Pentesting.

3.4.1 Hackeo Ético al Servidor de Archivos.

Para realizar el hackeo ético se escogió al servidor de archivos debido a que es el servidor que contiene el sistema operativo (Windows Server 2012) más antiguo existente en la empresa, por lo que se considera el servidor más vulnerable a ataques.

3.4.1.1 Fase de Reconocimiento.

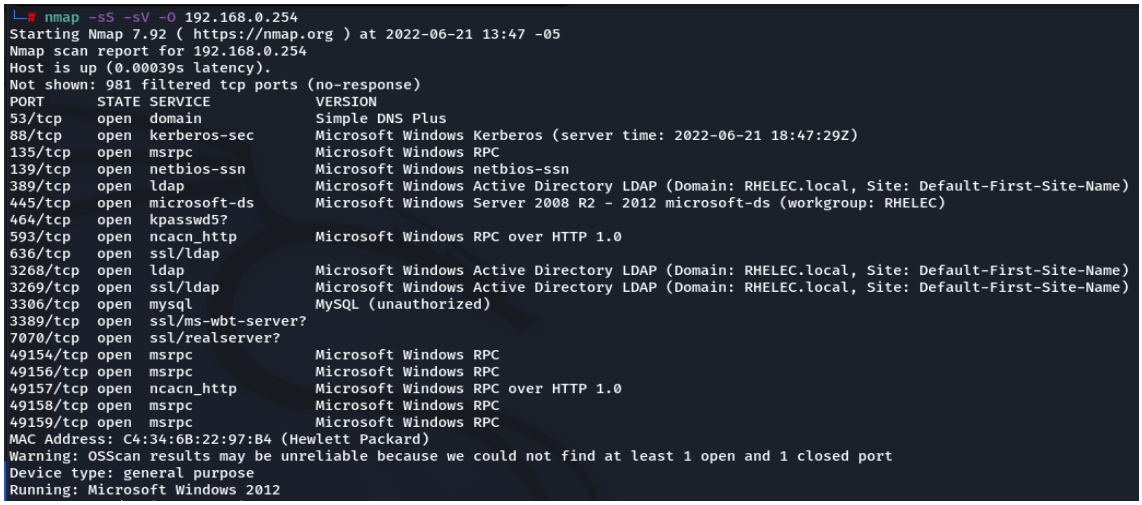
Las primeras pruebas de pentesting tiene como máquina objetivo al servidor de archivos de la empresa y su IP: 192.168.0.254. Para la actividad de reconocimiento y escaneo dirigida al mismo, se utiliza los siguientes comandos de Nmap descritos en la tabla 3.4.

Tabla 3.4. Auxiliares de comando para Nmap.

COMANDO	DESCRIPCIÓN
-sS	Para ser sigilosos en la red al momento de la ejecución de las pruebas
-sV	Identificación de la versión del servicio que está corriendo en el equipo
-O	Identificación del sistema operativo
-script vuln -p	Identificación de una vulnerabilidad en un puerto especifico

Fuente: Roberto Chango y Daniela Gualpa

Como se observa en la figura 3.3 se



recolecta información del escaneo de la máquina objetivo mediante la herramienta Nmap. Se utilizó el siguiente comando "Nmap -sS -sV -O 192.168.0.254/24", el cual sirve para mapear la IP del servidor de archivos de forma sigilosa para identificar los servicios y versiones de los puertos abiertos que existen en el servidor de archivos.

Figura 3.3 Resultado del escaneo de Nmap al servidor archivos

Fuente: Roberto Chango y Daniela Gualpa

Con la información recolectada en la figura 3.3, se determina que el servicio de archivos está corriendo en el puerto 445/tcp abierto con una versión de Windows Server 2012, por donde se llevará a cabo la explotación de esa brecha de seguridad.

3.4.1.2 Fase de Identificación de Vulnerabilidades.

Una vez identificado el puerto para atacar, se procede a consultar las debilidades del puerto seleccionado para el ataque, con la ayuda del comando "nmap -sS -sV -script vuln -p445 192.168.0.254", el cual sirve para identificar qué tan vulnerable es el puerto 445 para realizar una explotación por dicho puerto, tal como se observa en la figura 3.4.

Figura 3.4 Resultado del escaneo hacia el puerto 445 del servidor de archivos

```
└─# nmap -sS -sV -script vuln -p445 192.168.0.254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 13:47 -05
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.254
Host is up (0.00024s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: RHELEC)
MAC Address: C4:34:6B:22:97:B4 (Hewlett Packard)
Service Info: Host: SERVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
```

Fuente: Roberto Chango y Daniela Gualpa

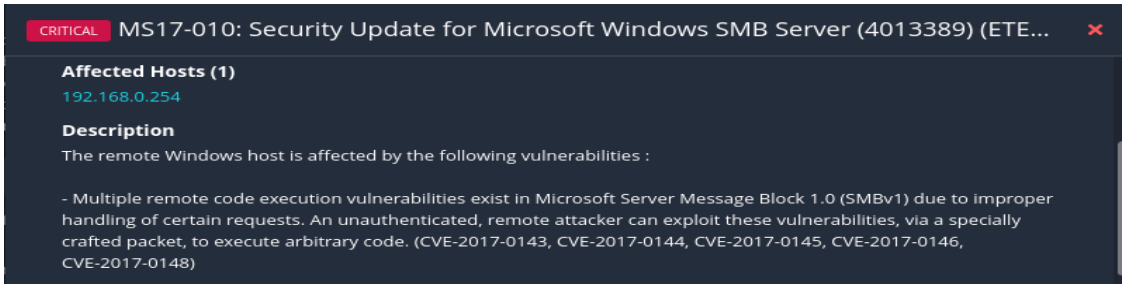
En la figura 3.4 detalla la información referente a una vulnerabilidad crítica en la brecha de seguridad del protocolo SMBv1 en el servidor de archivos, la cual puede ser ejecutado con un exploit referente a ms17_010 para explotar dicha vulnerabilidad. Para saber con precisión todas las vulnerabilidades existentes en todos los puertos del servidor de archivos, se utiliza la herramienta de Nessus para escanear las mismas y ponerlas en orden de criticidad de una forma gráfica tal como se muerta en la figura 3.5.

Figura 3.5 Resultado del escaneo al servidor de archivos con en Nessus.

Fuente: Roberto Chango y Daniela Gualpa

En la figura 3.6 se puede observar la vulnerabilidad crítica MS17-10 que corresponde a protocolos de Microsoft Server Message Block 1.0 (SMBv1), encontrado gracias a la herramienta Nessus, también se observa exploits que podrían utilizarse para explotar esa vulnerabilidad, en este caso se utilizara el exploit eternalblue posteriormente en la siguiente etapa.

Figura 3.6 Información de la vulnerabilidad crítica MS17-010



Fuente: Roberto Chango y Daniela Gualpa

3.4.1.3 Fase de Ataque y Penetración.

Una vez detectadas las vulnerabilidades a explotar, se inicializa la herramienta de metasploit framework para empezar con la fase de ataque y penetración al servidor de archivos. En la figura 3.7 se muestra la ejecución del comando "use auxiliary/scanner/smb/smb_ms17_010", el cual sirve para realizar un escaneo al protocolo "smb ms17-10" para saber qué tan vulnerable es el servidor con un exploit. Después se ejecuta el comando "set rhost 192.168.0.254" que sirve para setear la ip del servidor de archivos donde identifica que se va a realizar el escáner donde el host servidor de archivos tiene una alta probabilidad de ser explotado con el protocolo smb ms17-10. Finalmente se ejecuta el comando "run" para realizar el escáner al servidor de archivos.

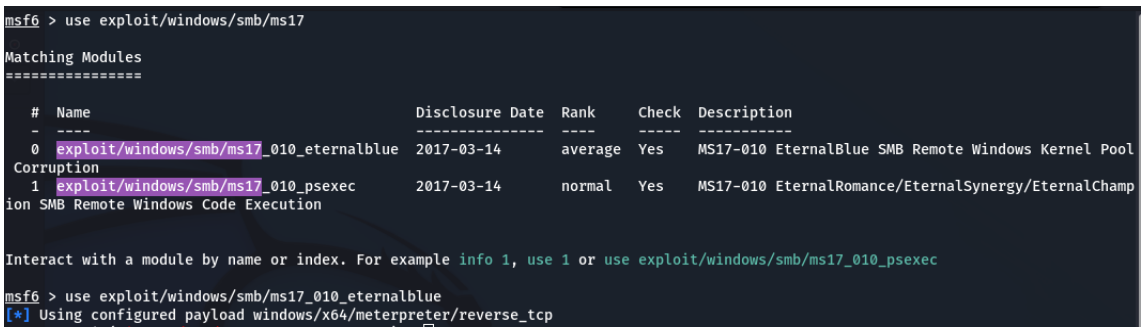
Figura 3.7 Resultado del escaneo para protocolo smb ms17-10 en metasploit

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                     Required  Description
   ----         ---------------                     --------  -----------
   CHECK_ARCH   true                                no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                               no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data  yes       List of named pipes to check
                /wordlists/named_pipes.txt
   RHOSTS                                           yes       The target host(s), see https://github.com/rapid7/metasploit-frame
                                                              work/wiki/Using-Metasploit
   RPORT        445                                 yes       The SMB service port (TCP)
   SMBDomain    .                                   no        The Windows domain to use for authentication
   SMBPass                                          no        The password for the specified username
   SMBUser                                          no        The username to authenticate as
   THREADS      1                                   yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhost 192.168.0.254
rhost => 192.168.0.254
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.0.254:445     - Host is likely VULNERABLE to MS17-010! - Windows Server 2012 R2 Essentials 9600 x64 (64-bit)
[*] 192.168.0.254:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Fuente: Roberto Chango y Daniela Gualpa

Una vez escaneado el protocolo smb ms17-10 en el servidor de archivos, en la figura 3.8, se ejecuta el comando "use exploit/windows/smb/ms17_010_eternalblue", el cual sirve para seleccionar el exploit de eternalblue recomendado para explotar esta vulnerabilidad que tiene un rango promedio de explotación para la brecha de seguridad encontrada mediante.

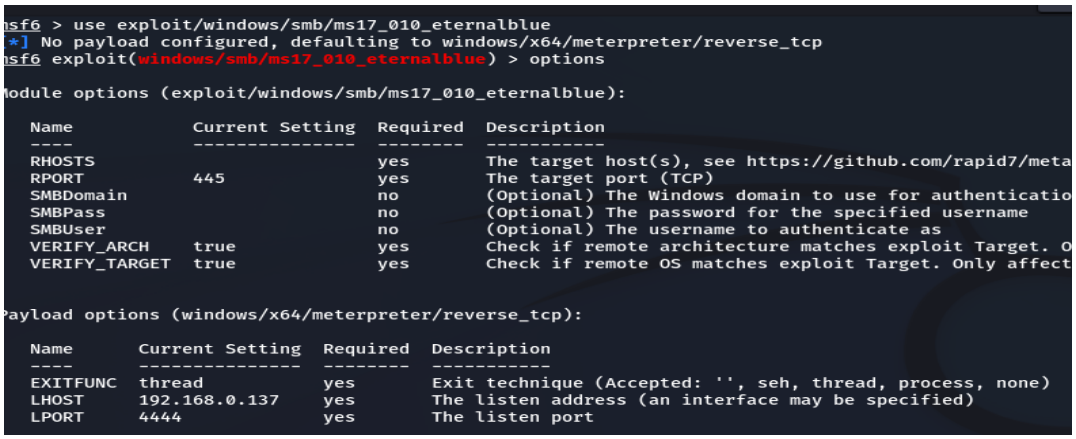
Figura 3.8 Resultado de la selección del exploit para el protocolo smb ms17-10



Fuente: Roberto Chango y Daniela Gualpa

Dentro del exploit eternalblue seleccionado, se escribe el comando “options” para saber los parámetros que deben ser seteados para llevar a cabo el ataque, como se muestra en la figura 3.9.

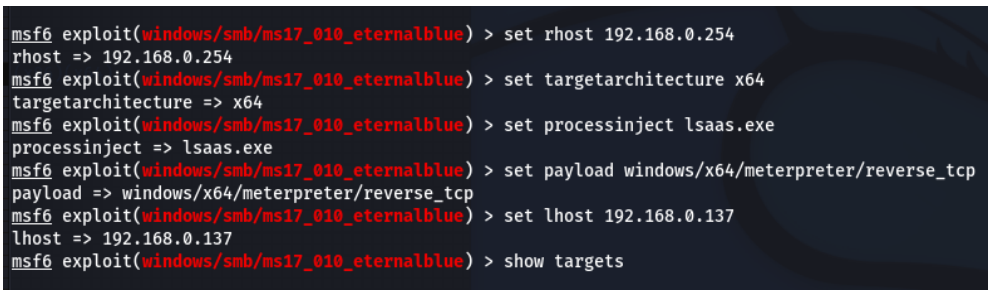
Figura 3.9 Resultado de opciones existente dentro del exploit eternalblue



Fuente: Roberto Chango y Daniela Gualpa

Se procede a setear los diferentes parámetros con los comandos mostrados en la figura 3.10 para que se lleve a cabo con éxito el ataque.

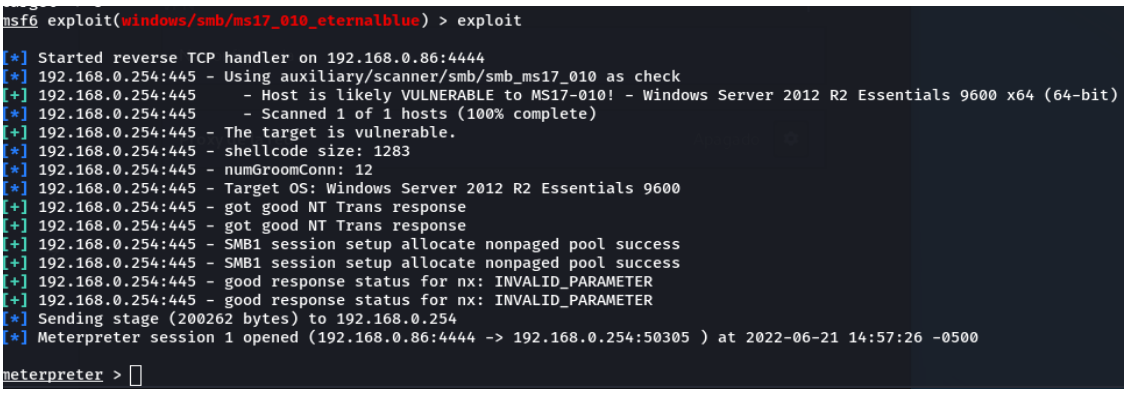
Figura 3.10 Comandos para setear los parámetros exploit eternalblue



Fuente: Roberto Chango y Daniela Gualpa

Finalmente, se digita el comando “exploit” para explotar la vulnerabilidad y asi obtener acceso al servidor de archivos mediante el payload meterpreter tal como se muestra en la figura 3.11.

Figura 3.11 Acceso al servidor de archivos mediante payload meterpreter

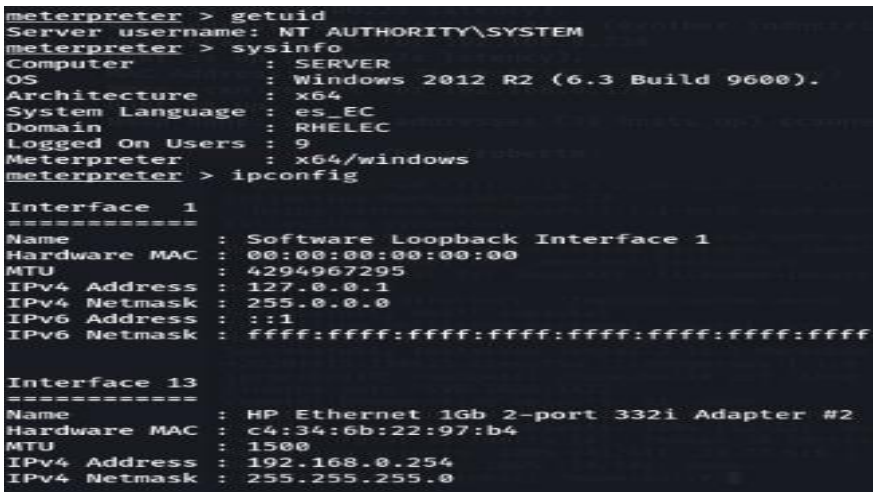


Fuente: Roberto Chango y Daniela Gualpa

3.4.1.4 Fase: Mantener Acceso.

Después de haber explotado la vulnerabilidad de la brecha de seguridad “ms17-10” y haber logrado tener acceso al servidor de archivos se mantiene el acceso, dentro de la shell meterpreter. Al tratarse de un proceso de hackeo ético se accedió a la información del servidor usando el comando “getuid” que muestra el privilegio de usuario que ganó el acceso al servidor. El comando “sysinfo” muestra informacion de la arquitectura del servidor, el comando “ipconfig” muestra las direcciones ip configuradas en las interfaces del servidor, como se observa en la figura 3.12.

Figura 3.12 Resultado de información del servidor de archivos en la consola meterpreter

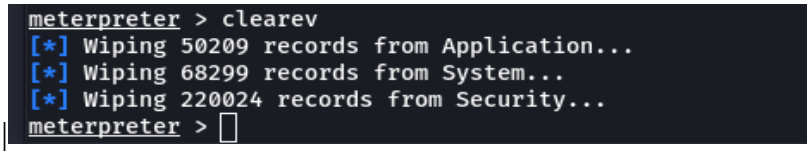


Fuente: Roberto Chango y Daniela Gualpa

3.4.1.5 Fase: Eliminar Huellas.

Posteriormente se procede a eliminar las huellas de evidencia que se pudo haber generado al momento de realizar las pruebas de las fases anteriores con el comando "clearev", tal como se observa en la figura 3.13, el cual es una herramienta propia de Metasploit.

Figura 3.13 Resultado de la fase de limpiar huellas

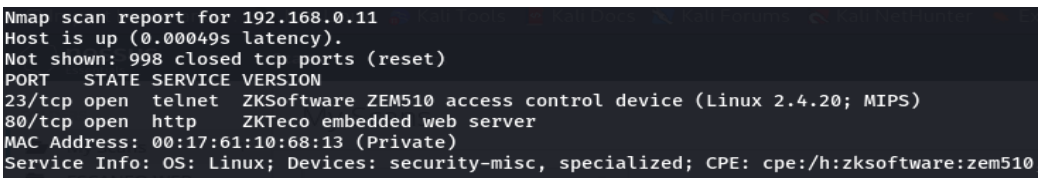


Fuente: Roberto Chango y Daniela Gualpa

3.4.2 Pruebas al Servidor Web.

La segunda prueba de pentesting tiene como máquina objetivo el servidor web de la empresa, tiene un sistema operativo Linux con IP: 192.168.0.11/24. Para la actividad de reconocimiento y escaneo dirigida al servidor, se utiliza el comando "nmap -sS -sV -O 192.168.0.11", el cual sirve para mapear la IP del servidor web de forma sigilosa para identificar los servicios y versiones de los puertos abiertos que existen en el servidor web, tal como se muestra en la figura 3.14.

Figura 3.14 Resultado del mapeo al servidor web con nmap



Fuente: Roberto Chango y Daniela Gualpa

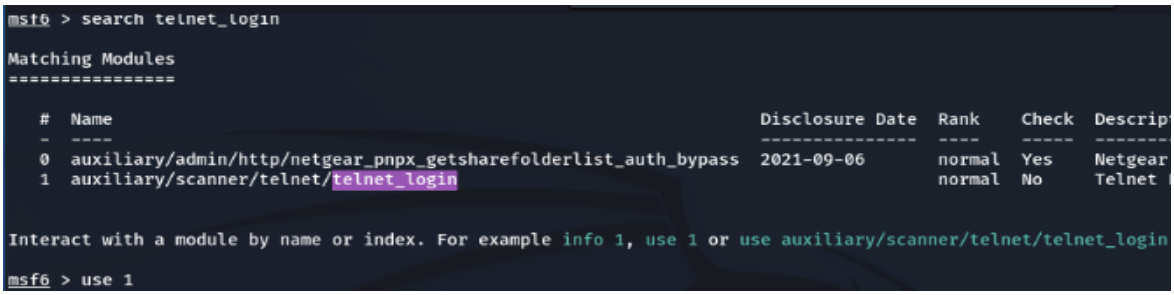
Con la herramienta Nessus se puede identificar una vulnerabilidad mediana que existe en el puerto 23/tcp/telnet tal como se muestra en la figura 3.15

Figura 3.15 Resultado del escaneo del puerto 23 del servicio telnet en Nessus

Fuente: Roberto Chango y Daniela Gualpa

En la herramienta Metasploit, se busca un exploit auxiliar de telnet login con el comando “search telnet login”, y se selecciona el número 1, tal como se muestra en la figura 3.16, el cual es usual para crear sesiones telnet y así poder entrar al servidor web de la empresa.

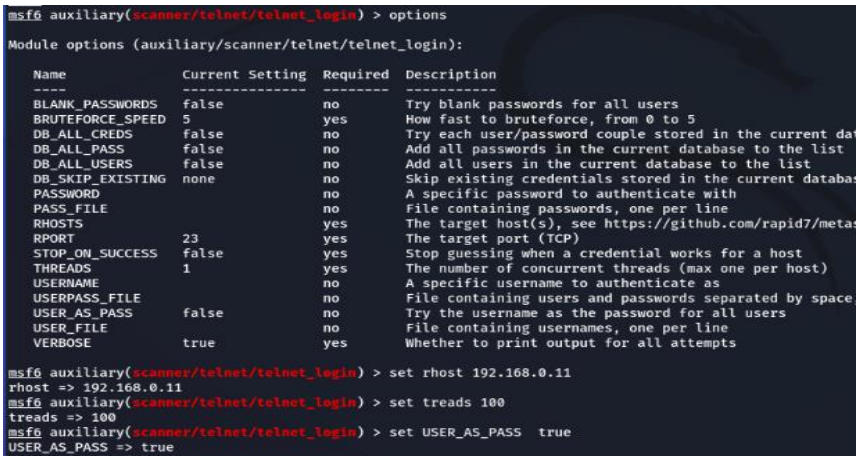
Figura 3.16 Resultado de la busqueda del auxiliar telnet login



Fuente: Roberto Chango y Daniela Gualpa

Una vez dentro del campo del auxiliar con el comando “options” se despliega los parámetros que deben ser setados, tal como se observa en la figura 3.17, para llevar a cabo el ataque.

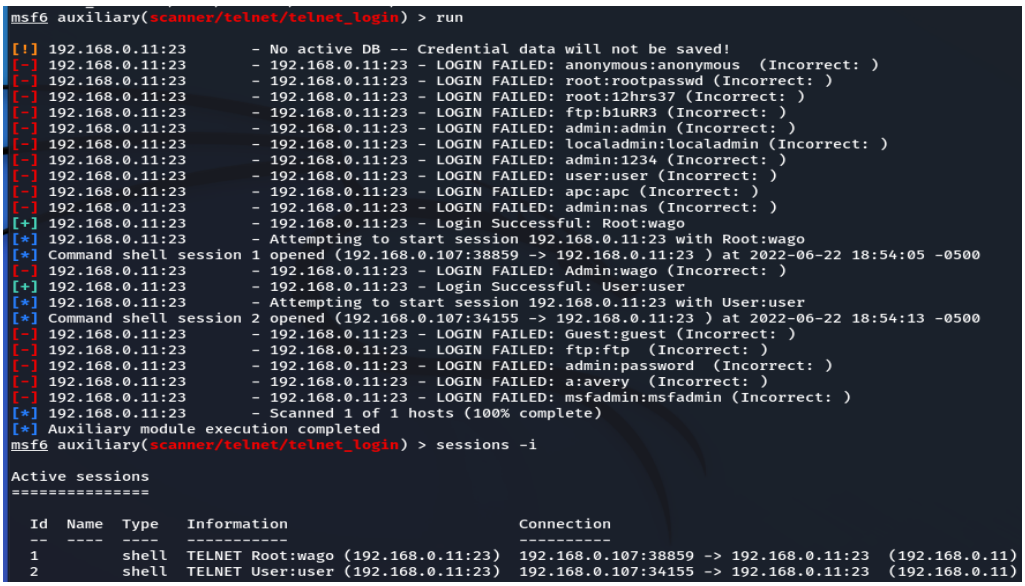
Figura 3.17 Resultado de las opciones de los parámetros del auxiliar telnet.



Fuente: Roberto Chango y Daniela Gualpa.

Una vez seteados los parámetros correspondientes, con el comando “run” se procede a ejecutar el ataque. Después se ejecuta el comando “sessions -i”, en cual sirve para definir las sesiones que se crearon sesiones de tipo Shell después de la explotación, tal como se observa en la figura 3.18, por medio de los cuales se podría tener acceso al servidor.

Figura 3.18 Resultado de las sesiones creada para acceder al servidor telnet.

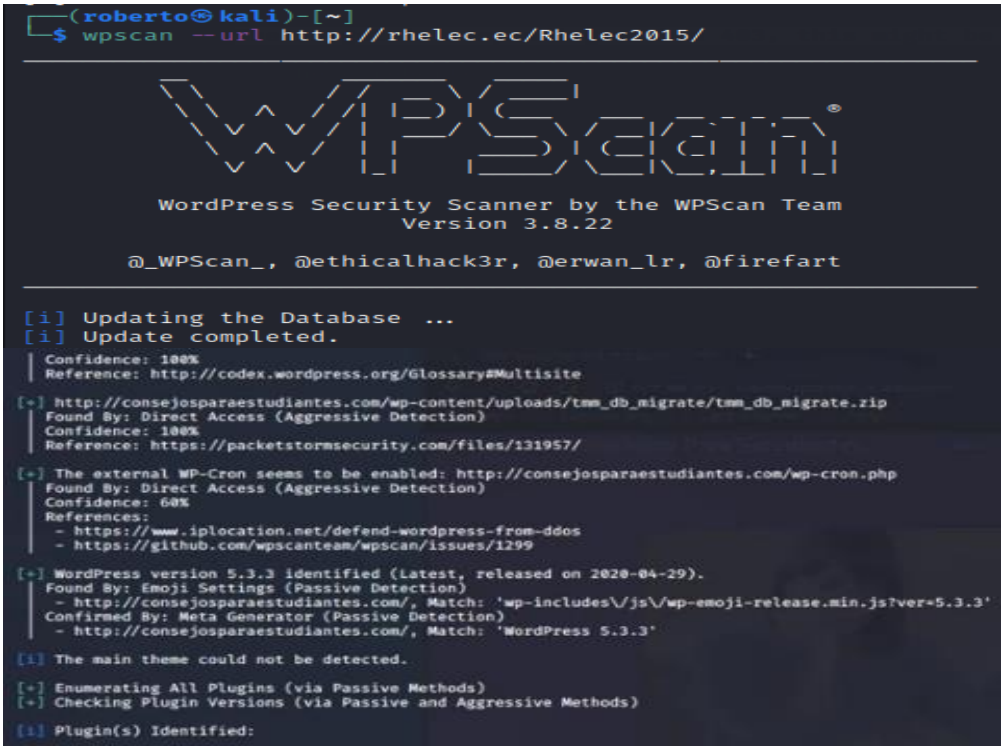


Fuente: Roberto Chango y Daniela Gualpa.

3.4.2.1 Pruebas a la Página Web.

La tercera prueba de pentesting tiene como objetivo la página web de la empresa, la cual tiene como dominio la url “www.rhelec.ec”. Para la actividad de reconocimiento y escaneo dirigida a la página web, se utiliza una herramienta el Kali Linux conocida como “WPScan”, con el comando “wpscan –url http://rhelec.ec/Rhelec.2015/”, el cual sirve para escanear las posibles vulnerabilidades que tiene la página web de una manera sigilosa, una vez terminado con el proceso correspondiente de escaneo hacia la página web, comienza a definir las vulnerabilidades encontradas en la misma, tal como se observa en la figura 3.19.

Figura 3.19 Resultado del escaneo a la página web de la empresa con WPScan.

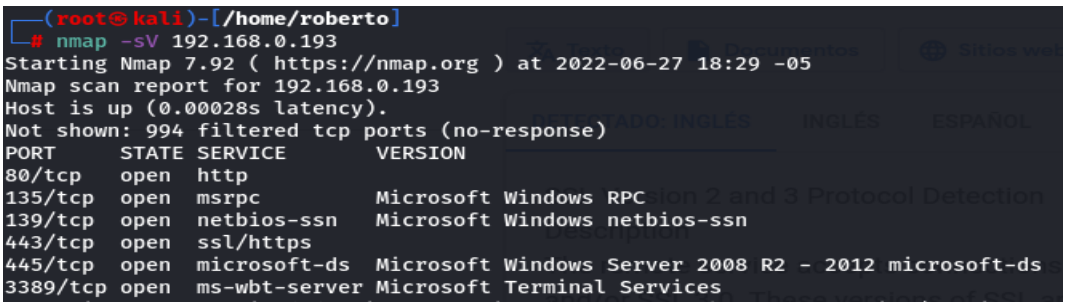


Fuente: Roberto Chango y Daniela Gualpa.

3.4.3 Pruebas al Servidor de Aplicaciones.

La cuarta prueba de pentesting tiene como máquina objetivo el servidor de aplicaciones de la empresa con IP: 192.168.0.193/24 y un sistema operativo Windows Server 2016. Para la actividad de reconocimiento y escaneo dirigida al servidor se utiliza el comando "nmap -Sv -O 192.168.0.193", el cual sirve para mapear la IP del servidor de aplicaciones de forma sigilosa para identificar los servicios y versiones de los puertos abiertos que existen en el servidor, tal como se muestra en la figura 3.20.

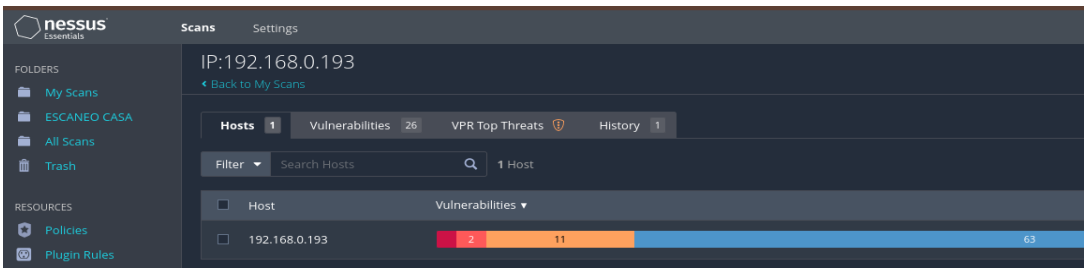
Figura 3.20 Resultado del mapeo al servidor de aplicaciones con Nmap.



Fuente: Roberto Chango y Daniela Gualpa.

Con la ayuda de la herramienta Nessus se categoriza las vulnerabilidades encontradas en el servidor de aplicaciones, tal como se muestra en la figura 3.21.

Figura 3.21 Vulnerabilidades encontradas en el servidor de aplicaciones en Nessus



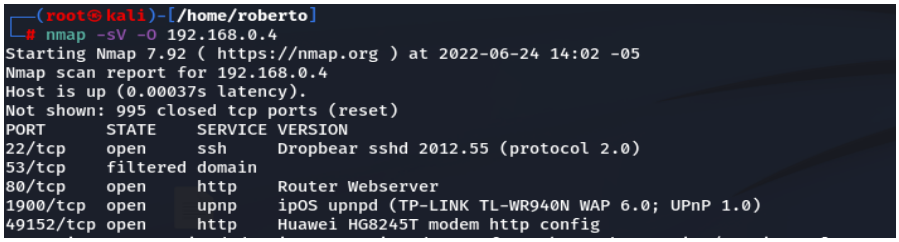
Fuente: Roberto Chango y Daniela Gualpa

3.4.4 Pruebas a la red WLAN.

3.4.4.1 Pruebas al Access Point Primario.

La quinta prueba de pentesting tiene como objetivo al Access Point primario de la empresa con IP: 192.168.0.4/24. Para la actividad de reconocimiento y escaneo dirigida al servidor, se utiliza el comando "nmap -sV -O 192.168.0.4", el cual sirve para mapear la IP del Access point de forma sigilosa para identificar los servicios y versiones de los puertos abiertos que existen en la red Wlan, tal como se muestra en la figura 3.22.

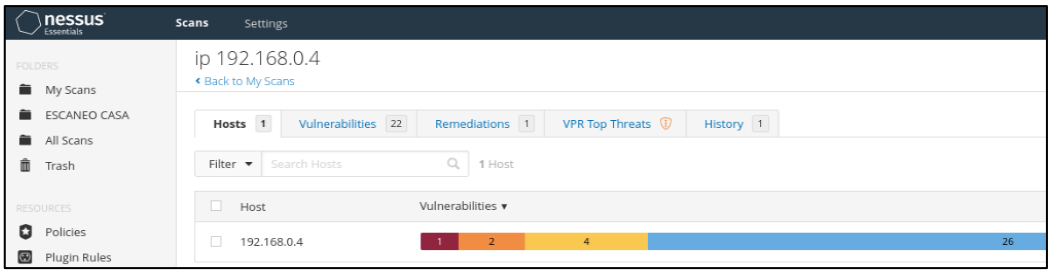
Figura 3.22 Resultado del escaneo al access point primario con Nmap.



Fuente: Roberto Chango y Daniela Gualpa

Con la herramienta Nessus se categoriza las vulnerabilidades encontradas en el access point primario, tal como se muestra en la figura 3.23.

Figura 3.23 Vulnerabilidades encontradas en el access point primario con Nessus.



Fuente: Roberto Chango y Daniela Gualpa

Por medio de la herramienta Nessus, se ha encontrado una vulnerabilidad alta en el puerto 22, tal como se muestra en la figura 3.24.

Figura 3.24 Vulnerabilidad crítica encontrada en el access point con Nessus.

Fuente: Roberto Chango y Daniela Gualpa

3.4.4.2 Pruebas al Router de Internet.

La séptima prueba de pentesting tiene como objetivo al Router de Internet de la empresa con IP: 192.168.0.1/24. Para esta prueba se utiliza una herramienta conocida en Kali Linux como “Fern WIFI Craker”, para auditar la red Wifi de la empresa, tal como se observa en la figura 3.25.

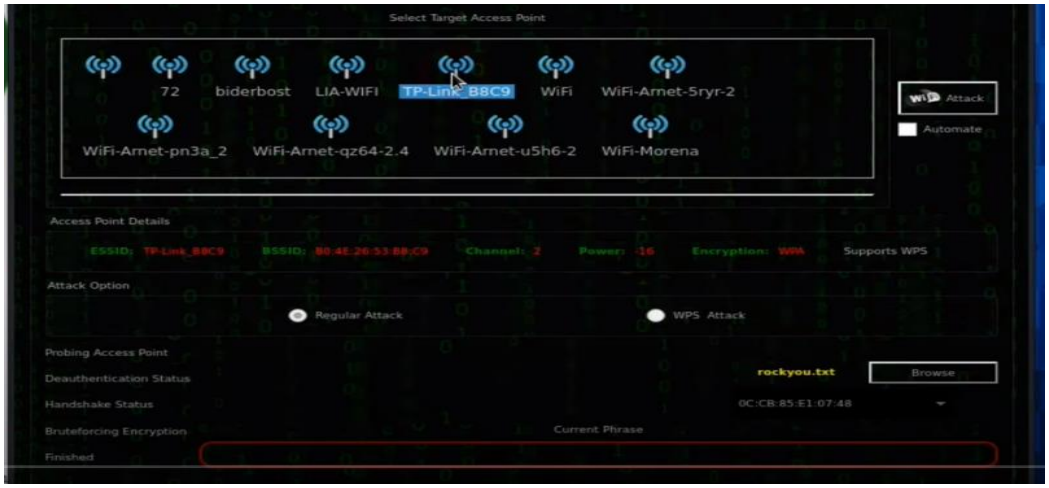
Figura 3.25 Interfaz de la herramienta Fern WIFI Craker.

Fuente: Roberto Chango y Daniela Gualpa

Al utilizar esta herramienta por medio de la interfaz “wlan0” automáticamente esta se coloca en modo monitor para proceder con el escaneo de la red wifi. En la figura 3.26 se define las redes wifi que encontro la herramienta anteriormente mencionada, la

red wifi sobre la que que se va a trabajar es TP-Link_RH correspondiente a la de la organización.

Figura 3.26 Redes Wifi encontradas con la herramienta Fern WIFI Craker.



Fuente: Roberto Chango y Daniela Gualpa

Esta herramienta contiene un archivo de texto con una enorme recopilación de contraseñas filtradas en diferentes brechas de seguridad a nivel mundial. Con la ayuda de este archivo se prueba las contraseñas contenidas en el mismo con la contraseña de la red wifi empresarial para hackear la red si la contraseña esta dentro de esa base de datos. Cuando la herramienta se está ejecutando. La conmutación de claves criptográficas que se realiza de forma que, en una etapa posterior, se pueda establecer una conexión de cifrado simétrico entre el servidor y el navegador del usuario. En la figura 3.27 se muestra el resultado de la contraseña encontrada al finalizar con la ejecución de la herramienta.

Figura 3.27 Resultado de la contraseña descifrada de la red wifi.

Fuente: Roberto Chango y Daniela Gualpa

3.5 Reporte de Vulnerabilidades Encontradas

3.5.1 Vulnerabilidades en Servidor de Archivos.

Con las pruebas de pentesting realizadas se logró detectar muchas vulnerabilidades referentes principalmente a puertos abiertos en el servidor de archivos con dirección IP: 192.168.0.254/24, las cuales se definen en la tabla 3.5.

Tabla 3.5 Vulnerabilidades en Servidor de Archivos

PUERTO	ESTADO	SERVICIO	VULNERABILIDAD
445/tcp	Abierto	Microsoft-ds	Critica
636/tcp	Abierto	Ssl/Ldap	Alta
3269/tcp	Abierto	Ssl/Ldap	Alta
3389/tcp	Abierto	Ssl	Alta
49156/tcp	Abierto	Msrpc	Media
49158/tcp	Abierto	Msrpc	Media
53/tcp	Abierto	Domain	Baja
593/tcp	Abierto	Ncacn_http	Baja

Fuente: Roberto Chango y Daniela Gualpa

Otra vulnerabilidad que se detectó fue la obsolescencia del sistema operativo (Windows Server 2012) que se encuentra instalado en el servidor de archivos.

3.5.2 Vulnerabilidades en Servidor Web.

Con la segunda prueba de pentesting realizada anteriormente se logró detectar algunas vulnerabilidades en el servidor web con dirección IP: 192.168.0.11/24, las cuales se definen en la tabla 3.6.

Tabla 3.6 Vulnerabilidades en Servidor Web

PUERTO	ESTADO	SERVICIO	VULNERABILIDAD
23/tcp	Abierto	Telnet	Alta
80/tcp	Abierto	Http	Baja

Fuente: Roberto Chango y Daniela Gualpa

En un tercer pentesting realizado al sitio web de la organización encontró una confiabilidad del 70% en cuanto a XML-RPC (Remote Procedure Call), protocolo de llamada a procedimiento remoto que usa XML para codificar datos y HTTP como protocolo de emisión de mensajes, esto se debe a que no se ha actualizado la página web y le hace falta plugin de seguridad para llegar una confiabilidad del 100%.

3.5.3 Vulnerabilidades en Servidor de Aplicaciones.

Gracias a la prueba de pentesting realizada, se logró detectar varias vulnerabilidades en el servicio de telnet con dirección IP: 192.168.0.11/24, mismas que se enumeran en la tabla 3.7.

Tabla 3.7 Vulnerabilidades en Servicio de Aplicaciones

PUERTO	ESTADO	SERVICIO	VULNERABILIDAD
443/tcp	Abierto	Ssl/https	Critica
445/tcp	Abierto	Microsoft-ds	Media
80/tcp	Abierto	Http	Media

Fuente: Roberto Chango y Daniela Gualpa

3.5.4 Vulnerabilidades en la red WLAN.

3.5.4.1 Vulnerabilidad en el Access Point Primario.

En la prueba de pentesting realizada anteriormente, se pudo detectar un conjunto de vulnerabilidades en el Access Point primario definidos en la tabla 3.8.

Tabla 3.8 Vulnerabilidades en Access Point Primario

PUERTO	ESTADO	SERVICIO	VULNERABILIDAD
22/tcp	Abierto	Ssh	Alta
1900/tcp	Abierto	Upnp	Media
53/tcp	Abierto	Domain	Baja

Fuente: Roberto Chango y Daniela Gualpa

3.5.4.2 Vulnerabilidad en el Router de Internet.

La prueba realizada anteriormente en el router de internet de la organización se detectó un bajo nivel de seguridad en cuanto al acceso wifi protegido (WPA). La contraseña de la red wifi fue descifrada fácilmente, ya que esta contenía solo números tal como se muestra en la figura 3.27.

3.6 Análisis de riesgo de las Vulnerabilidades Detectadas

3.6.1 Riesgos en Servidor de Archivos.

3.6.1.1 Vulnerabilidades de Microsoft Windows SMBv1.

El servidor de archivos tiene activado el SMBv1 (bloque de mensajes del servidor de Microsoft). El cual se ve amenazado por las siguientes vulnerabilidades encontradas:

- En la difusión de información en SMBv1 conforme al mal uso de los paquetes del mismo. Esta brecha de seguridad se puede vulnerar fácilmente mediante un paquete SMBv1 que puede ser diseñado específicamente para exponer información confidencial y valiosa de la organización.
- En la denegación de servicio en SMBv1 por el manejo incorrecto de las solicitudes del mismo. Esta vulnerabilidad se puede explotar con una solicitud SMB particularmente diseñada para detener el funcionamiento del servidor que este no responda, siendo esto muy perjudicial para un servidor que trabaja las 24 horas dentro de la empresa Rhelec Ingeniería.
- En la ejecución remota de comandos sobre SMBv1 debido al manejo incorrecto de los paquetes del mismo. Esta vulnerabilidad podría explotarse utilizando un paquete característico de SMBv1 especialmente diseñado para la ejecución de un código arbitrario hacia el servidor de la empresa.
- Autenticación de sesión nula SMB, que podría permitir una inicialización de sesión con una sesión cero, es decir, sin nombre de usuario ni contraseña y dependiendo de la configuración y estructuración de la misma, es posible que los piratas informáticos aprovechen este problema en particular de esta brecha de seguridad para obtener datos e información confidencial una vez obtenido acceso al servidor de la organización.

3.6.2 Riesgos en Servidor Web

3.6.2.1 Vulnerabilidad de Servicio Telnet sin cifrar

El servicio de Telnet remoto que utiliza la empresa se lleva a cabo un servicio telnet mediante un canal no cifrado. En la actualidad, no es muy recomendable utilizar Telnet a través de un canal no cifrado, porque los nombres de usuario, contraseñas y los comandos se envían en texto no encriptado. Esto facilita a los ciberdelincuentes remotos interceptar una sesión de telnet para así conseguir credenciales y otra información

corporativa confidencial de la empresa y así pueda alterar el tráfico intercambiado entre el cliente y el servidor. Por lo antes mencionado, es preferible usar SSH a que Telnet, porque telnet resguarda acreditación de escuchas ilícitas y puede transmitir flujos de datos adicionales, como por ejemplo sesiones X11.

3.6.3 Riesgos en Servidor de Aplicaciones.

3.6.3.1 Vulnerabilidad en el Protocolo SSL Versión 2 y Versión 3.

Este servicio remoto acepta conexiones cifradas en las versiones de SSL 2.0 y SSL 3.0, las mismas se ven afectadas por varias fallas, que incluyen:

- Un esquema de relleno inseguro con cifrados CBC.
- Esquemas inseguros de renegociación y reanudación de sesiones.
- Un atacante puede explotar estas fallas para realizar ataques de intermediario o para descifrar las comunicaciones de datos entre el servicio afectado y los clientes.

3.6.4 Riesgos en Red Wlan.

3.6.4.1 Riesgo en Access Point Primario.

3.6.4.1.1 Vulnerabilidad en Dropbear SSH Server.

En el Access Point primario se ejecuta una versión de Dropbear SSH antecedente a 2016.74, la cual es antigua y por eso se ve amenazado por las siguientes vulnerabilidades:

- Se detecta una falla en el enlace de formato debido a la manipulación inadecuada de los especificadores de formato de sucesión en los inicios de sesión de usuarios y argumentos de los hosts. Esta vulnerabilidad se puede explotar ejecutando un código arbitrario con privilegios de root.
- Se detectó una falencia en dropbear convert debido al mal manejo de archivos de claves en OpenSSH diseñados especialmente. Esta vulnerabilidad se puede explotar para ejecutar código arbitrario.
- Se encontró una falla en el dbclient al momento de manejar los argumentos -m o -c en las secuencias de comandos. Esta vulnerabilidad se puede explotar mediante un script que puede ser diseñado especialmente para correr un código arbitrario.

CAPÍTULO 4

ESTRATEGIAS PARA MEJORAR LAS SEGURIDADES

4.1 Controles a ser Implementados para Fortalecimiento (hardening)

4.1.1 Acciones para Vulnerabilidades en Servidor de Archivos.

Estas vulnerabilidades son consideradas las más críticas detectadas en las pruebas de pentesting, ya que estas permiten la activación remota de código si un ciberdelincuente envía textos configurados a un servidor Microsoft Server Message Block versión 1.0 (SMBv1). Este restablecimiento de seguridad es importante para todas las traducciones simultáneas de Microsoft Windows. Para contrarrestar estas vulnerabilidades se aplican las siguientes acciones mencionadas a continuación:

- Instalar la actualización del parche de seguridad correspondiente para el sistema operativo Windows Server 2018 (kb 4012213), el cual es posible descargar desde la página oficial de los parches de seguridad de Windows. Este corrige las vulnerabilidades mencionadas anteriormente al corregir esencialmente cómo SMBv1 maneja las solicitudes existentes.
- Deshabilitar el protocolo SMBv1 en los componentes de cliente y servidor en el sistema del servidor de archivos. Esta medida de seguridad lo recomienda la seguridad de Microsoft Windows.
- Crear políticas de seguridad (GPO) para establecer configuraciones o parámetros en la red de dominio y así establecer políticas.

4.1.2 Acciones para Vulnerabilidades en Servidor de Aplicaciones.

La vulnerabilidad critica del servidor de aplicaciones se da por el puerto abierto 443/tcp, esto se da debido a que acepta conexiones de SSL 2.0 y SSL 3.0, con esto un hacker de sombrero negro puede explotar esta vulnerabilidad para penetrar las comunicaciones de datos entre el servicio amenazado y los clientes. Este protocolo podría obviarse ya que no es necesario tener abierto el puerto 443 para este servicio, por lo que lo la acción a implementar es:

- Configurar el puerto 443 en las reglas de salida del Firewall de Windows para permitir la conexión a este puerto solo si la conexión es segura, caso contrario se denegaría el tráfico de datos por el puerto 443.
- La vulnerabilidad media detectada por el puerto 445 en cuanto a protocolo de SMBv1, la acción a implementar es:
- Deshabilitar el protocolo SMBv1 de las características de Windows para mitigar esta vulnerabilidad, ya que en Windows Server 2016 se puede utilizar las versiones superiores a este protocolo

4.2 Análisis del Equipamiento para el Fortalecimiento (hardening)

4.2.1 Equipamiento para Windows Server 2012.

Para el fortalecimiento (hardening) en el servidor de archivos de la empresa Rhelec Ingeniería es primordial el equipamiento de programa de actualización de parche de seguridad para el sistema operativo Windows Server creada por Microsoft para la vulnerabilidad del protocolo SMBv1 que contrarresta los exploits utilizados en contra del mismo, debido a que SMBv1 fue un gran éxito en su época, pero no fue desarrollado para el mundo conectado de hoy en día, que existe mucha más tecnología y facilidad para vulnerar protocolos antiguos, después de todo, han pasado varios años de la revolución de la información desde entonces. Microsoft ya depreció SMBv1 en la actualidad por lo que recomienda deshabilitar ese protocolo. Debido a su tecnología obsoleta, SMBv1 es muy inseguro. Tiene muchas vulnerabilidades las cuales pueden ser explotadas por algunos exploits desarrollados para el protocolo SMBv1 y muchos de estos permiten la ejecución de control remoto en una máquina objetivo.

Las Políticas de grupo son una herramienta importante porque brindan una forma agrupada de administrar y aplicar todos los tipos de configuraciones de sistemas operativos, aplicaciones y configuración de los usuarios respecto a Active Directory. Estas configuraciones ayudaran al mejor manejo de administración de usuarios en la empresa Rhelec Ingeniería. Los equipamientos para este fortalecimiento (hardening) a implementar en el servidor de archivos son herramientas de software que se instala y se configura para las brechas de seguridad encontradas anteriormente.

4.3 Instalación y Configuración de Hardening

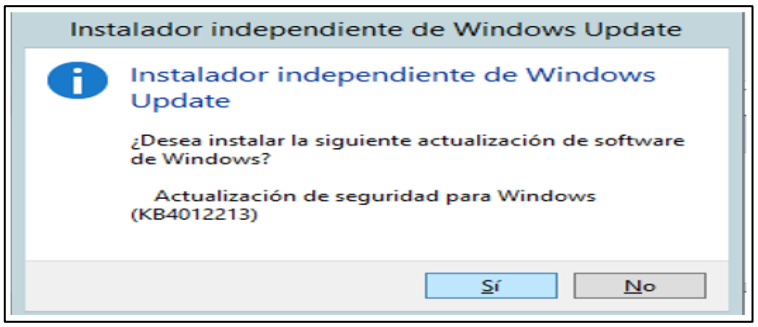
4.3.1 Hardening en servidor de archivos.

Una vez definida las diferentes acciones y herramientas a usar para mitigar la mayoría de vulnerabilidades encontradas en el servidor de archivos con sistema operativo Windows Server 2012, el siguiente paso es la implementación de la misma dentro del servidor de archivos

4.3.1.1 Parche de seguridad para Windows Server 2018 (KB 4012213).

Este parche de seguridad es uno de los tantos que ofrece Microsoft Windows para las distintas vulnerabilidades encontradas en los diferentes sistemas operativos, los cuales se pueden obtener de la página oficial de Microsoft. Para la instalación del parche de seguridad KB 4012213, una vez descargado el parche se ejecuta como cualquier otro programa de instalación, como se representa en la figura 4.1 y figura 4.2

Figura 4.1 Instalación del parche de seguridad KB 4012213



Fuente: Roberto Chango y Daniela Gualpa

Después de haber aceptado la instalacion, se ejecuta las actualizaciones correspondiestes al parche de seguirdad, para ser implementadas una vez que se reinicie el sistema haciendo desaparecer la vulnerabilidad critica MS17-010.

4.3.1.2 Inhabilitación de SMBv1.

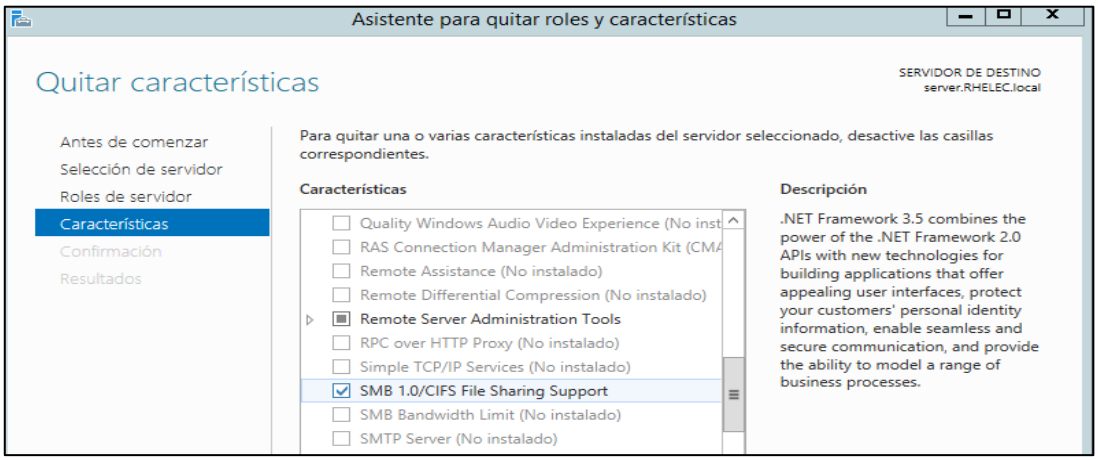
Para proceder a deshabilitar la opcion de soporte para compartir archivos, se procede a ingresar al administrador del servidor para posteiormente entrar al asistente de quitar roles y caracteristicas donde se selecciona el servidor de la empresa en este caso es “server.RHELEC.local” con IP:192.168.0.254/24, como se muestra en la figura 4.2.

Figura 4.2 Selección del servidor de archivos dentro del administrador del servidor

Fuente: Roberto Chango y Daniela Gualpa

Una vez seleccionado el servidor, se ingresa a caracterticas, se busca y se desmarca el casillero donde se enceuntra “SMB 1.0/CIFS File Sharing Support”, como se muestra en la figura 4.3

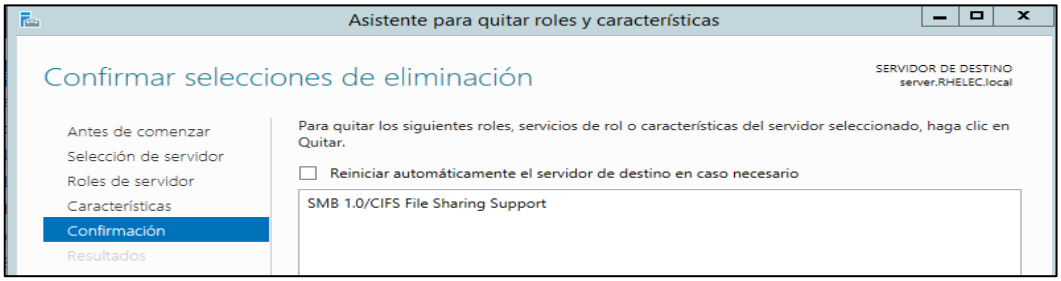
Figura 4.3 Inhabilitación de la caracteristica de SMB 1.0



Fuente: Roberto Chango y Daniela Gualpa

Finalmente, se confirma la Inhabilitación de SMB 1.0, para que al reiniciar el sistema, se apliquen los cambios y desaparezca otra vulnerabilidad alta del servidor.

Figura 4.4 Confirmación de deshabilitación de SMB 1.0

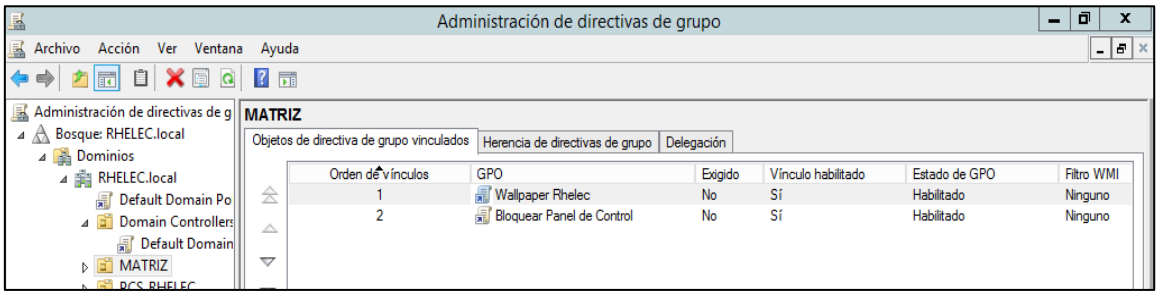


Fuente: Roberto Chango y Daniela Gualpa

4.3.1.3 Creación de Políticas de Grupo (GPO).

Las políticas de grupo serán de gran ayuda para administrar los diferentes usuarios organizacionales, para que estos no tengan privilegios de acceso dentro de la red empresarial. Para proceder con la creación de las GPOs se desglosa el bosque "RHELEC.local" para aplicar las políticas en el subdominio matriz, como se puede observar en la figura 4.5

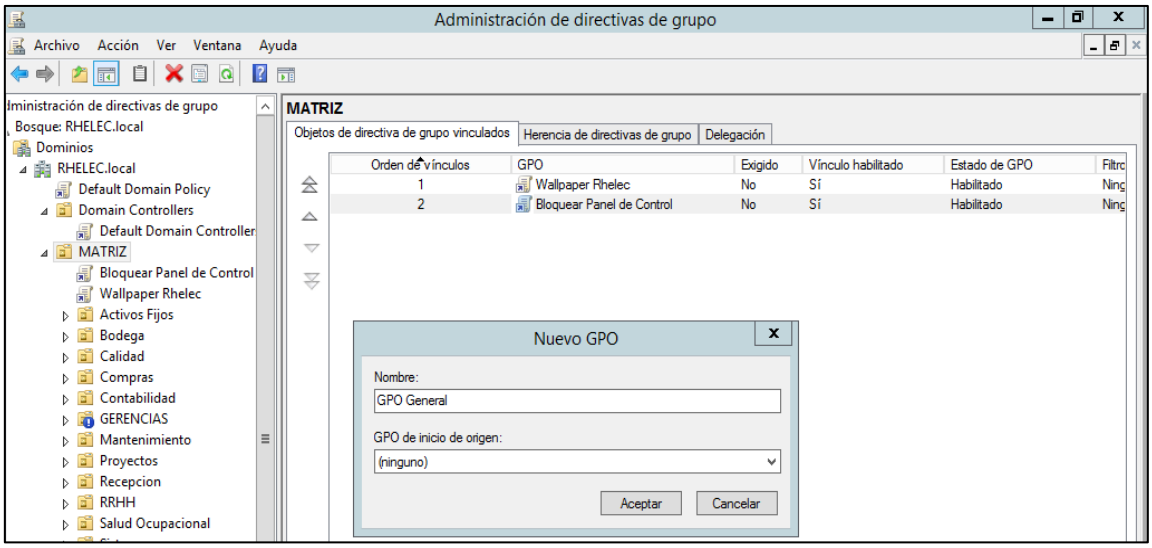
Figura 4.5 Selección de subdominio para las políticas GPOs



Fuente: Roberto Chango y Daniela Gualpa

Una vez selecionado el domino se crea una nueva GPO para que se pueda habilitar junto con las otras políticas ya existentes, como se observa en la figura 4.6.

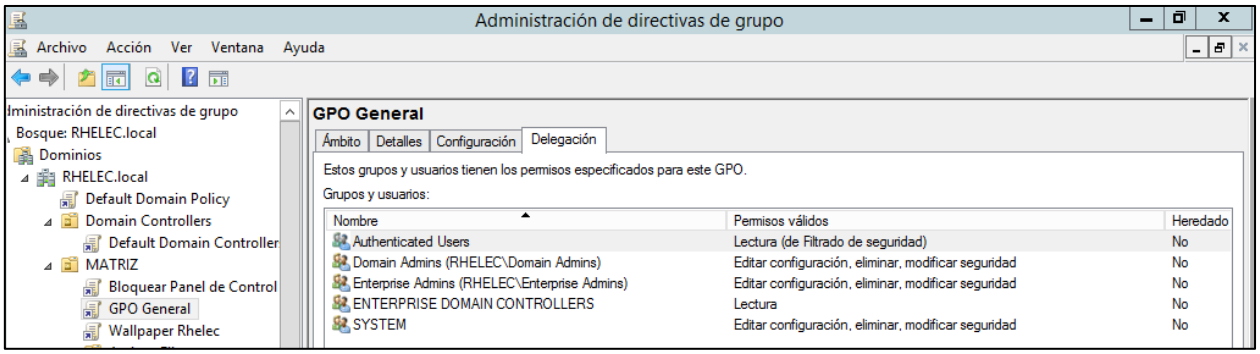
Figura 4.6 Creación de una nueva política GPO



Fuente: Roberto Chango y Daniela Gualpa

En la figura 4.7 se puede obser a que delegaciones nomas esta ligada esta nueva política GPO creada para la administración segura de usuarios.

Figura 4.7 Delegacion de la nueva política GPO

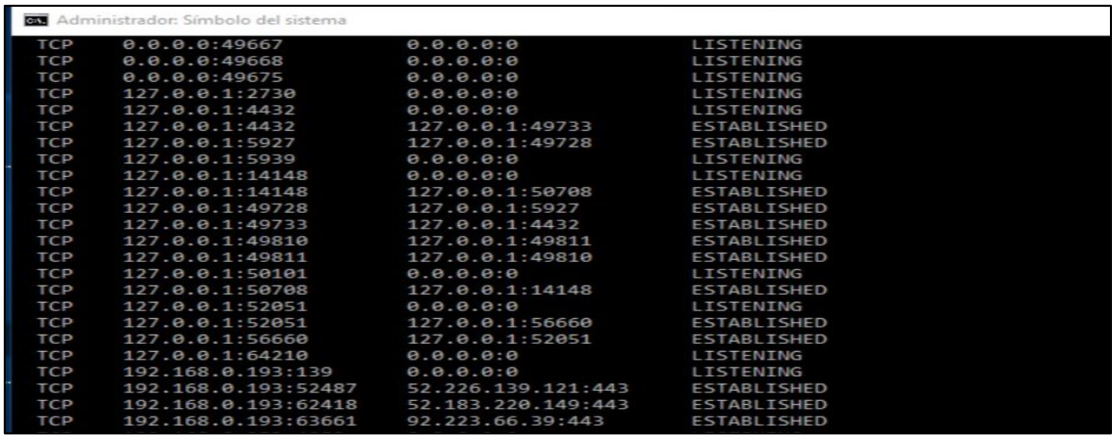


Fuente: Roberto Chango y Daniela Gualpa

4.3.1.4 Hardening en Servidor de Aplicaciones.

En el Servidor de archivos se encontró una vulnerabilidad crítica en el puerto 443, la cual se pudo evidenciar en el servidor haciendo una revisión para saber si el puerto 443 está abierta para alguna dirección IP. La prueba se lo realizó en el símbolo del sistema con el comando "netstat -an", como se puede apreciar en la figura 4.8

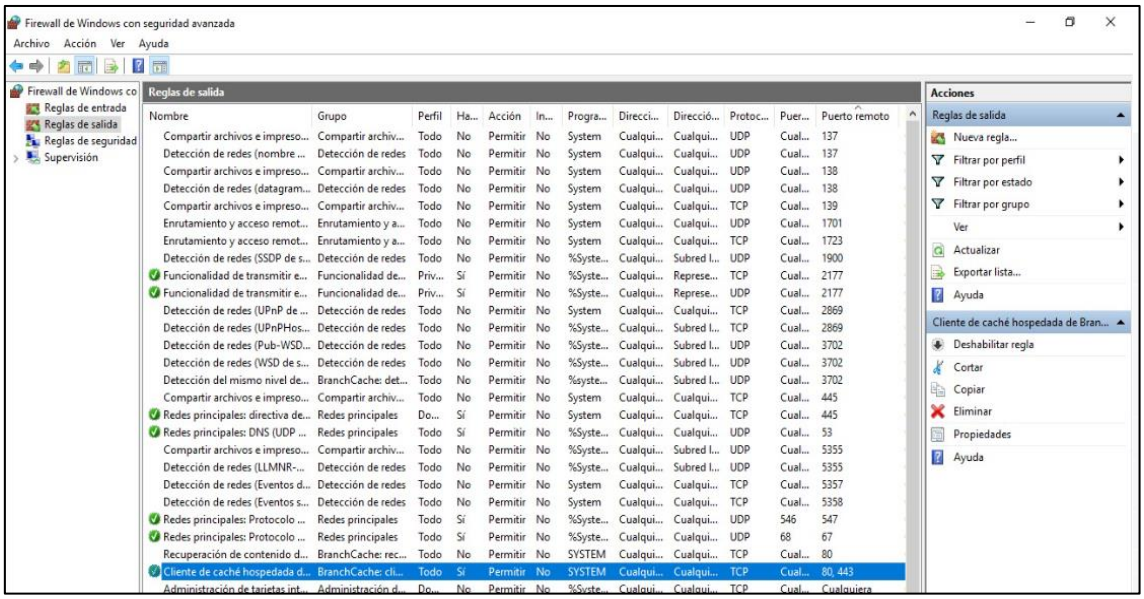
Figura 4.8 Ejecución del comando "netstat -an" para revision puerto 443



Fuente: Roberto Chango y Daniela Gualpa

Para dar solución a esta brecha de seguridad, se debe ir al Firewall de Windows para buscar en configuraciones avanzadas que regla de salida esta activada al acceso remoto del puerto 443, la cual se observa en la figura 4.9.

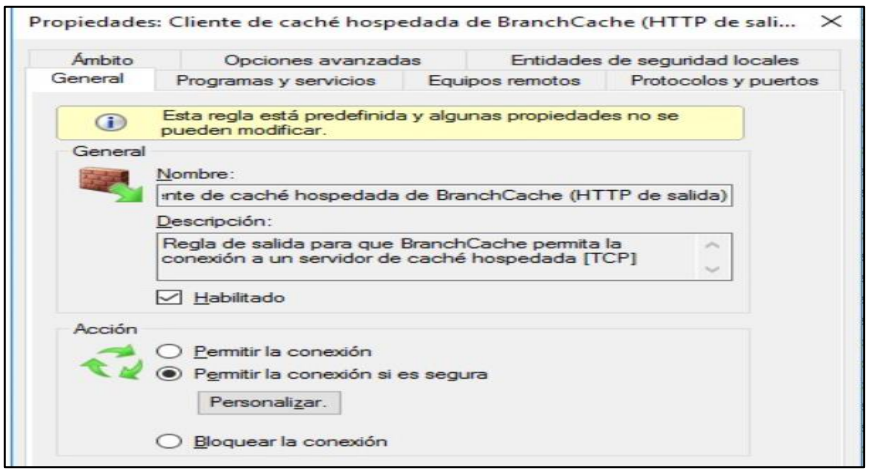
Figura 4.9 Selección del puerto remoto 80,443 en Firewall Windows



Fuente: Roberto Chango y Daniela Gualpa

Finalmente, para aplicar la solución a esta brecha de seguridad, en la opción propiedades de la regla de salida seleccionada anteriormente, se debe seleccionar en la opción permitir la conexión si es segura, tal como se muestra en la figura 4.10.

Figura 4.10 Selección de conexión segura para el puerto 443



Fuente: Roberto Chango y Daniela Gualpa

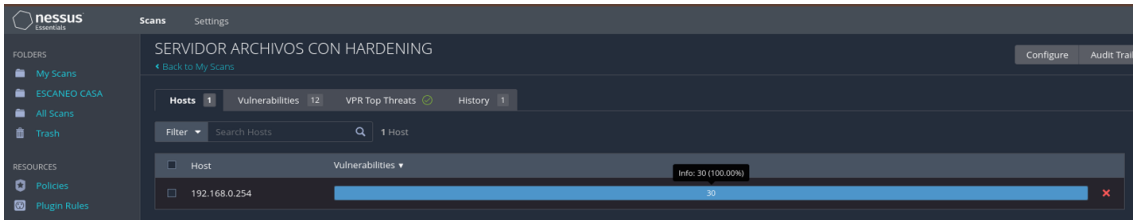
4.4. Pruebas Realizadas con la Implementacion del Hardening

4.4.1 Pruebas en Servidor de Archivos.

Despues de haber implementados las estrategias de fortalecimiento en el servidor de archivos, se realizó un nuevo escaneo de vulnerabilidades en el mismo, para observar el resultado en cuanto a la efectividad de los fortalecimientos. Mediante la herramienta

Nessus se realizó el escaneo del servidor con IP:192.168.0.254 y el resultado fue excelente ya que desparecieron en totalidad las vulnerabilidad que se habían detectado, tal como se puede observar en la figura 4.11.

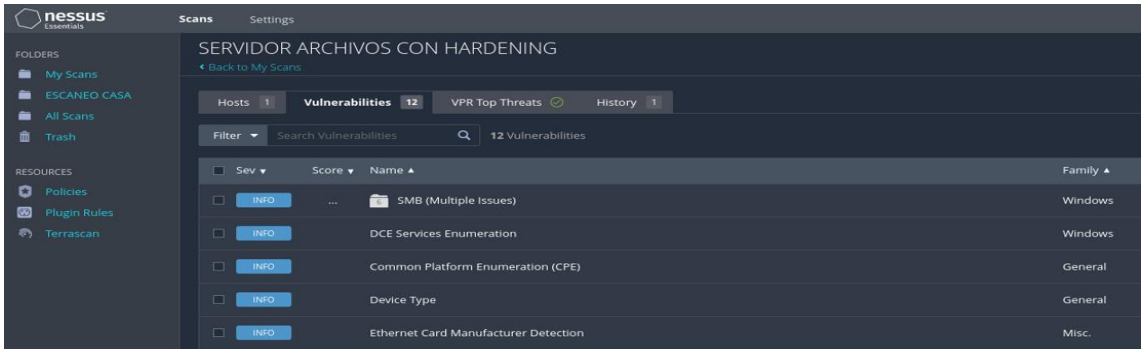
Figura 4.11 Escaneo del servidor con hardening en Nessus



Fuente: Roberto Chango y Daniela Gualpa

Una vez finalizado el escaneo al servidor de archivos, se definieron aquellas vulnerabilidades encontradas que no representan riesgo alguno, ya que tan solo son de muestra información, como se puede evidenciar en la figura 4.12.

Figura 4.12 Vulnerabilidades informativas encontradas en el servidor de archivos con hardening



Fuente: Roberto Chango y Daniela Gualpa

En la figura 4.13 se realiza el escaneo de vulnerabilidad puntual al puerto 445 del servidor de archivos, por el cual fue atacado, y claramente se puede evidenciar que por medio de las acciones de fortalecimiento han desaparecido las brechas de seguridad detectadas anteriormente.

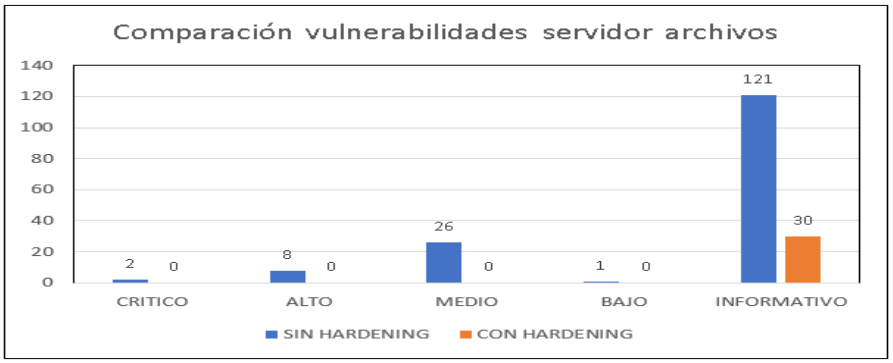
Figura 4.13 Escaneo del bulnerabilidad al puerto 445 en Nmap

```
┌──(root㉿kali)-[/home/roberto]
└─# nmap -sS -sV -script vuln -p445 192.168.0.254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-27 20:30 -05
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.254
Host is up (0.00038s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: RHELEC)
MAC Address: C4:34:6B:22:97:B4 (Hewlett Packard)
Service Info: Host: SERVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
```

Fuente: Roberto Chango y Daniela Gualpa

Como se puede evidenciar en la figura 4.14. Las pruebas realizadas después de haber implementado las estrategias de fortalecimiento, todas estas tuvieron un éxito rotundo ya que desaparecieron todas las vulnerabilidades encontradas anteriormente, lo cual se puede decir que fue un excelente fortalecimiento de casi al 100%.

Figura 4.14 Comparación de vulnerabilidades con y sin hardening en servidor archivos



Fuente: Roberto Chango y Daniela Gualpa

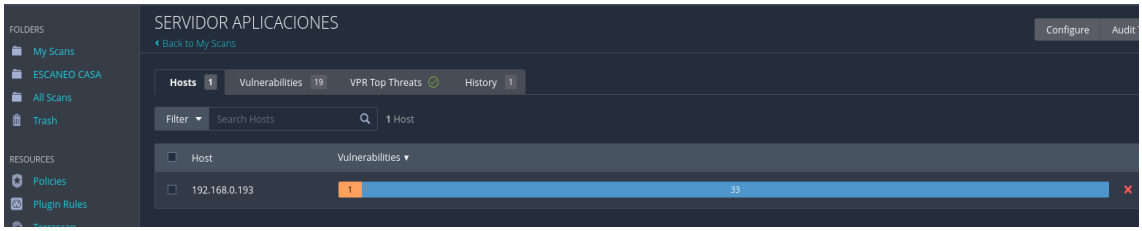
Con la implementación de las estrategias de fortalecimiento en el servidor de archivos se pudo afirmar que: Las vulnerabilidades críticas, altas, medianas y baja desaparecieron en su totalidad, lo cual es excelente gracias a las estrategias de fortalecimiento implementadas al servidor de archivos y las vulnerabilidades informativas se redujeron de 121 a 30, lo cual como su nombre lo indica solo son de uso informativo.

4.4.2 Pruebas en Servidor de Aplicaciones.

Después de haber implementados las estrategias de fortalecimiento en el servidor de aplicaciones, se empleo un nuevo escaneo de vulnerabilidades en el mismo, para observar el resultado de que tan efectivos fueron los fortalecimientos. Mediante la

herramiena Nessus se realizó el escaneo del servidor con IP:192.168.0.193 y es resultado fue demasiado bueno ya que desparecieron en su totalidad las vulnerabilidad criticas y mediana que se habian detectado anteirormente, tal como se puede observar en la figura 4.15.

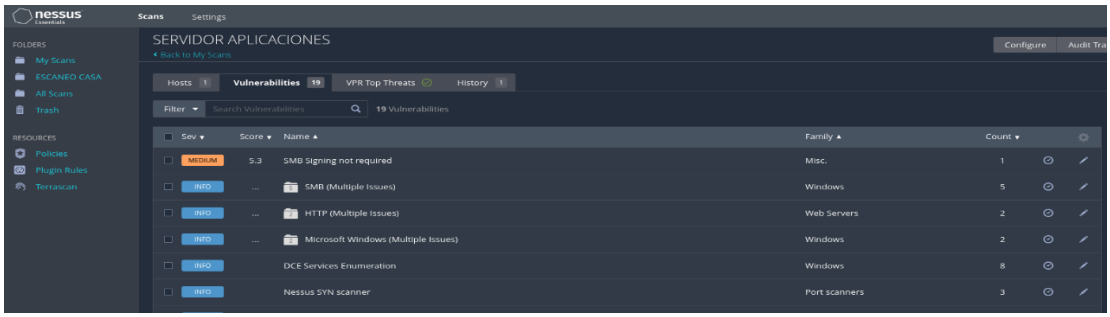
Figura 4.15 Escaneo del servidor con hardening en Nessus



Fuente: Roberto Chango y Daniela Gualpa

Una vez finalizado el escaneo al servidor de aplicaciones, se definieron las vulnerabilidades encontradas, las cuales se redujeron considerablemente, como se puede evidenciar en la figura 4.16.

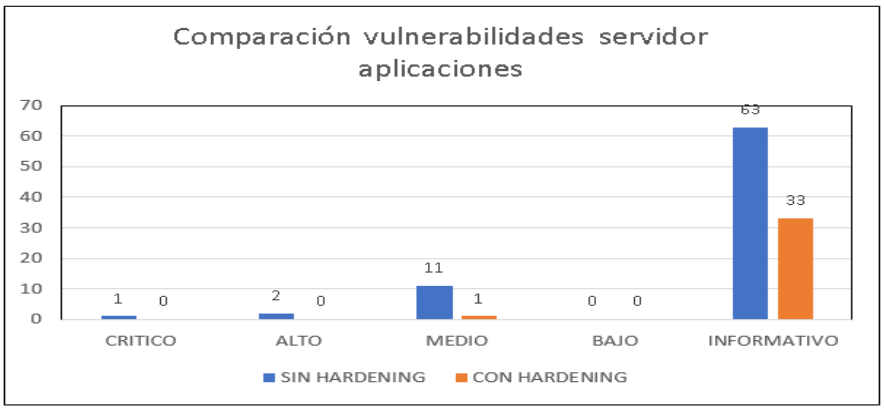
Figura 4.16 Vulnerabilidades encontradas en el servidor de aplicaciones con hardening



Fuente: Roberto Chango y Daniela Gualpa

En la figura 4.17 se evidencia la gran disminución de vulnerabilidades que hubo con la implementación de las estrategias antes mencionadas hacia el servidor de aplicaciones para mitigar las brechas de seguridad.

Figura 4.17 Comparación de vulnerabilidades con y sin hardening en servidor aplicaciones



Fuente: Roberto Chango y Daniela Gualpa

Con la implementación de las estrategias de fortalecimiento en el servidor de aplicaciones se pudo afirmar que:

- Una vulnerabilidad crítica que había desapareció totalmente.
- Las dos vulnerabilidades críticas que había desaparecieron totalmente.
- De las once vulnerabilidades se redujeron a 1, lo cual es bastante bien.
- Las 63 vulnerabilidades de información se redujeron a 33, lo cual solo son vulnerabilidades de información.

CONCLUSIONES

- En análisis situacional de seguridad realizado en Rhelec, permitió detectar la ausencia de estrategias de seguridad implementadas, determinando que la infraestructura se posee un alto nivel de vulnerabilidades y de riesgos para diversos tipos de ataques.

- Las pruebas de pentesting realizadas en los equipos más importantes de la empresa, permitieron detectar el alcance de los posibles ataques y su afectación al explotar las vulnerabilidades, además de las consecuencias en cuanto a no atender los riesgos latentes de estas debilidades.

- El diseño de un escenario de pruebas permitió simular ataques de hackeo utilizando fuerza bruta y de barrido puertos abiertos de los servidores, las cuales ayudaron a detectar diversas vulnerabilidades para posteriormente aplicar acciones correctivas en los dispositivos (Hardening).

- Las estrategias de fortalecimiento (hardening) en los servidores de archivos y aplicaciones resultaron exitosas, ya que se pudieron mitigar todos los riesgos de Alta severidad de estado crítico, y 11 riesgos de estado Medio que se redujeron a 1 sólo riesgo.

RECOMENDACIONES

- Este trabajo de investigación pudiera ser considerado como una guía para otras empresas que deseen incurrir en pruebas de testeo de la seguridad de la información, con el fin de mejorar sus controles para identificar vulnerabilidades mediante evaluaciones autorizadas.

- Dada la importancia de la seguridad, se sugiere mantener actualizado el hardware, y las aplicaciones, ya que por lo general cada nueva versión incluye correcciones de errores y otras funciones que permiten un funcionamiento adecuado del software,

- Las organizaciones deben preocuparse por escribir, aplicar y revisar sus políticas y procedimientos de seguridad de forma continua para reducir los riesgos de ciberataques y prevenir problemas futuros en sus operaciones.

- Es necesario considerar un programa de capacitación para los empleados en temas de seguridad y ciberseguridad incluyendo los principales riesgos a los que están expuestos sus activos, los ataques más comunes y las principales recomendaciones para evitar estos incidentes.

- Se sugiere crear un plan de pentesting periódico para detectar amenazas y vulnerabilidades a través de la metodología ISSAF, como parte de una estrategia para la implementación de acciones de mitigación de riesgos.

REFERENCIAS

Albacete, J. F. (2017). *Seguridad en equipos informáticos. IFCT0510.* IC Editorial. Recuperado el 17 de 05 de 2021, de https://books.google.at/books?id=N1YpEAAAQBAJ

Alberto, R. (19 de Septiembre de 2020). *TicsCamaraValencia*. Obtenido de de https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-el-hacking-etico/

Burgos, D. (2019). La importancia del Hacking Etico en el Sector Finaciero. *Universidad Piloto de Colombia*. Recuperado el Abril de 2021, de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2735/Trabajo%20de%20grado3049.pdf?sequence=1&isAllowed=y

Ciberseguridad. (Diciembre de 2021). *¿Qué es Metasploit Framework y cómo funciona?* Recuperado el Abril de 2021, de https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

De Luz, S. (2021). *OWASP ZAP, audita la seguridad de webs y evita vulnerabilidades.* Recuperado el 04 de 2022, de https://www.redeszone.net/tutoriales/seguridad/owasp-zap-auditar-seguridad-web

Iglesia, E. D. (15 de Noviembre de 2019). *Campusciberseguridad.com*. (C. I. Ciberseguridad, Editor) Recuperado el 18 de Abril de 2021, de https://www.campusciberseguridad.com/blog/item/133-tipos-de-hackers

Jorge, I. (2018). *Vista de análisis de los ciberataques realizados en América Latina.* Universidad Interbacional del Ecuador. INNOVA. Recuperado el 7 de Marzo de 2021, de https://revistas.uide.edu.ec/index.php/innova/article/view/837/1182

Juan, V. M. (2010). *Codejobs*. Recuperado el 16 de Abril de 2021, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X201000010000&Ing=es&nrm)iso

KIMAT. (2018). *Qué es el Hardening*. Recuperado el 2022, de https://www.kimat.mx/que-es-hardening-kimat/

Mayorga, F. (2017). *Analisis de vulnerabilidades y diseño de procesos correctivos de la pagina web de la Dirección de Educación a Distancia y Virtual de la Univerrsidad Técnica de Ambato.* Ambato. Recuperado el 04 de 2021, de Https://repositorio.uta.edu.ec/jsúi/handle/123456789/15531

Olegario, C. (2021). *EVALUACIÓN DE METODOLOGÍAS DE HACKING PARA EL DIAGNOSTICO DE VULNERABILIDADES.* Recuperado el 16 de Abril de 2021, de https://repositorio.uss.edu.pe/handle/20.500.12802/9148

Oñate O., M. C. (2017). *MEJORAS EN LA SEGURIDAD DE LA RED INALÁMBRICA DE LAUNIVERSIDAD NACIONAL DE CHIMBORAZO APLICANDO HACKING.* Riobamba. Recuperado el Abril de 2021, de http://dspace.unach.edu.ec/handle/51000/4170

Pacheco, J. (2018). *Desarrollo de una guía técina estandar para aplicar herramientas de Ethical Hacking en redes de datos, dirigido a PYMES.* Quito. Recuperado el 8 de marzo de 2021, de http://repositorio.puce.edu.ec/handle/22000/12612

Penagos. (2019). *Analisis de metodologias de Etichal Hacking para ña detecion de vulnerabilidades en las PYMES.* Tesis, UNAD. Recuperado el 02 de 2022

Peña, J. (2018). *Hacking Éticoo para analizar y evaluar la seguridad informática en la infraestructurade la empresa Playicaucho Industrial S.A.* Recuperado el 6 de Marzo de 2021, de http://repositorio.uta.edu.ec/handle/123456789/28102

Rhelec, Ingenieria. (08 de enero de 2021). *Rhelec Ingeniería.* (AINTELDATA, Editor, & Rhelec Ingeniería.) Recuperado el 18 de 06 de 2022, de http://rhelec.ec/Rhelec2015/

Tenable. (2021). *Escanner de Vulneravilidades Nessus*. Recuperado el Abril de 2021, de https://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/datasheets/NessusPro-(DS)-EsLa.pdf

Torres, D. (2021). *OpenWebinars.net*. Recuperado el 16 de 05 de 2021, de https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/

Tovar, L. (2020). *Hacking Ético para Mejorar la Segruidad en la Infraestructura Informatica del Grupo Electrodata* . Lima. Recuperado el 19 de Marzo de 2021, dehttps://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/3095/Luis%20Tovar_Trabajo%20de%20Suficiencia%20Profesional_Titulo%20Profesional_2020.pdf?sequence=1&isAllowed=y

Vega, G. (2017). Vulnerabilidades y Amenazas a Servicios Web de la Intranet de La Universidad Técnica de Babahoyo. *6*(1). Obtenido de https://www.3ciencias.com/articulos/articulo/vulnerabilidades-amanezas-los-servicios-web-la-intranet-la-universidad-tecnica-babahoyo/

Zara. (Diciembre de 2018). *Gray Hat Hacking*. Recuperado el 7 de Marzo de 2021, de de https://zarza.com/gray-hat-hacking-los- de-la-etica-ambigua/

Zea, M. &. (2019). *Comparaciones de Metodologias en aplicaciones web.* Universidad Técnica de Machala , Machala. Recuperado el mayo de 2022

ANEXOS

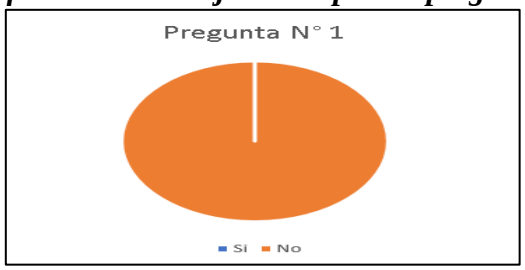
Anexo 1. Encuesta realizada a la empresa Rhelec Ingeniería.

ENCUESTA AL DEPARTAMENTO DE SISTEMAS

1. ¿Gestiona el uso seguro y correcto del correo electrónico empresarial y de las redes sociales en la organización?

a. Si b. No

Gráfico 1. Porcentaje de Respuesta pregunta 1



Fuente: Roberto Chango y Daniela Gualpa

Interpretación. – En este grafico el 100% representa, que el empleado no gestiona de manera adecuada el uso del correo electrónico y redes sociales de la organización, presentando gran riesgo en pérdidas informáticas.

2. ¿Controla la seguridad de los usuarios y de los datos empresariales que conforman las áreas o departamentos de la empresa?

a. Si b. Algunos c. No

Gráfico 2. Porcentaje de Respuesta pregunta 2

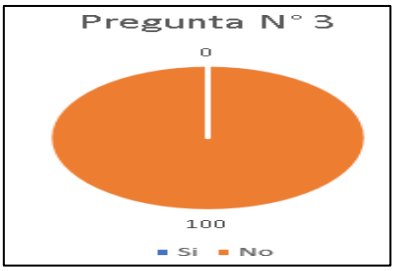
Fuente: Roberto Chango y Daniela Gualpa

Interpretación. - Se puede visualizar que el empleado en su mayoría no supervisa en algunas áreas o departamentos de la empresa, resultando así en consecuencias negativas por el descuido de las mismas como el robo de información.

3. ¿Cuentan con un plan de prevención de riesgos en cuanto a la seguridad de la información?

a. Si b. No

Gráfico 3. Porcentaje de Respuesta pregunta 3



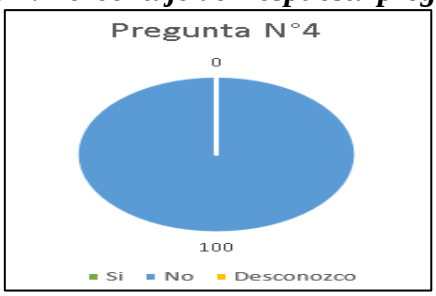
Fuente: Roberto Chango y Daniela Gualpa

Interpretación. - El 100% demuestra que el área de sistema no cuenta con un plan de prevención, por lo que la organización se encuentra altamente vulnerable a sufrir ataques.

4. ¿Alguna vez se ha realizado pruebas de hackeo ético (pentesting) en el sistema de seguridad informática en la empresa?

a. Si b. No c. Desconozco

Gráfico 4. Porcentaje de Respuesta pregunta 4.



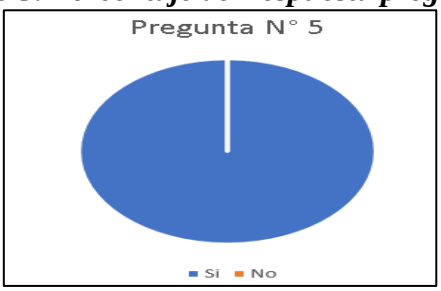
Fuente: Roberto Chango y Daniela Gualpa

Interpretación. -El 100 % indica que la persona encargada del área de sistemas nunca ha evaluado a través de pruebas de hacking ético la seguridad informática lo cual es una desventaja, ya que en la actualidad la organización está más propensa a ataques

5. ¿En la empresa existe algún manual de política de seguridad de la información?

a. Si b. No

Gráfico 5. Porcentaje de Respuesta pregunta 5.



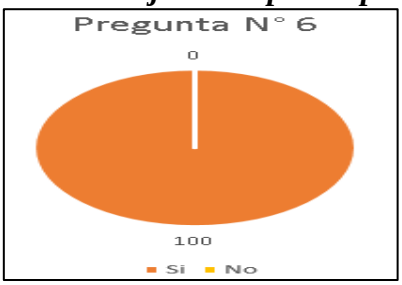
Fuente: Roberto Chango y Daniela Gualpa

Interpretación. -El 100 % indica que dentro de la empresa si existe un manual de política de seguridad informática, sin embargo, el desconocimiento de cómo aplicar las normas que se deben cumplir pone en desventaja al personal, ya que su manual es muy básico.

6. ¿En la red WLAN, la empresa tiene restricciones de acceso a sitios web sociales y de diversión?

a. Si b. No

Gráfico 6. Porcentaje de Respuesta pregunta 6.



Fuente: Roberto Chango y Daniela Gualpa

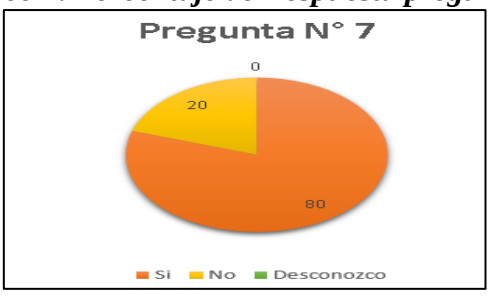
Interpretación. -El 100 % indica que la red Wlan no existe restricción de acceso a sitios de red ocio.

Encuesta realizada a las diferentes áreas de la empresa Rhelec

7. ¿Conoce usted si su computadora de trabajo tiene instalado un Software de Antivirus?

a. Si b. No c. Desconozco

Gráfico 7. Porcentaje de Respuesta pregunta 7.



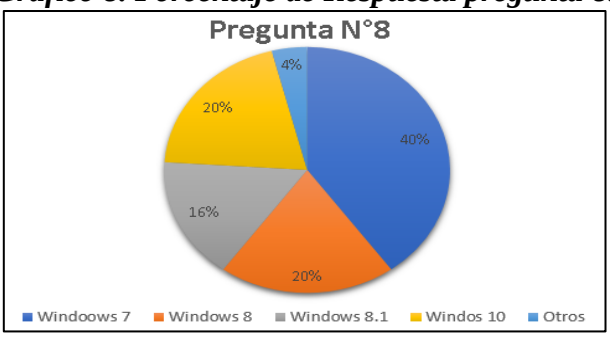
Fuente: Roberto Chango y Daniela Gualpa

Interpretación. -El 80% de los empleados de la empresa conocen sobre el software antivirus instalado en las computadoras de su trabajo y la importancia que tiene, mientras que el 20% al no conocer si su máquina de trabajo posee un software antivirus se vuelve más vulnerable ante cualquier tipo de virus.

8. ¿Qué versión de Windows tiene instalado en su computador de trabajo?

a. Windows 7 b. Windows 8 c. Windows 8.1 d. Windows 10 e. Otros

Gráfico 8. Porcentaje de Respuesta pregunta 8.



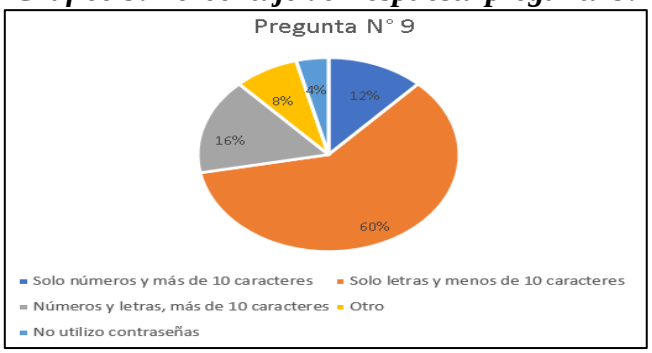
Fuente: Roberto Chango y Daniela Gualpa

Interpretación. -El 40% de los empleados tienen instalado el sistema operativo de Windows 7, en la actualidad se conoce que este sistema operativo cumplió su periodo de soporte lo que implica que ya no es un sistema seguro. Por lo que la empresa debe ya considerar instalar una actualización más nueva.

9. ¿Las contraseñas que utiliza en su computadora de trabajo tienen una mezcla entre números, letras y es de más de 10 caracteres aleatorios?

a. Solo números y más de 10 caracteres b. Solo letras y menos de 10 caracteres
c. Números y letras, más de 10 caracteres d. Otro e. No utilizo contraseñas.

Gráfico 9. Porcentaje de Respuesta pregunta 9.



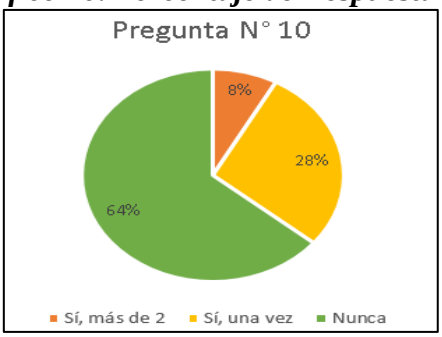
Fuente: Roberto Chango y Daniela Gualpa

Interpretación. -El 60% de los usuarios usa sus contraseñas solo letras y menos de 10 caracteres por lo que no se tiene contraseñas robustas y se puede hackear fácilmente por partes de terceros,

10. ¿En el último año ha sufrido algún incidente de seguridad informática en su computadora de trabajo (correos maliciosos, bloqueo de computadora, perdida de documentos y fallos de software)?

a. Sí, más de 2 b. Sí, una vez c. No, nunca

Gráfico 10. Porcentaje de Respuesta 10.



Fuente: Roberto Chango y Daniela Gualpa

Interpretación. -El 60% representa el impacto que sufrió hace varios meses atrás el área de recepción y bodega ya que a través de correo electrónico sus ordenadores están expuestos a infectar con archivos maliciosas que fueron enviados por este medio.