IDENTIFICACIÓN DE LAS DIFERENTES VULNERABILIDADES DE LA RED LAN DE PLANTA ENSAMBLADORA Y EL ALMACÉN DE PEREIRA DE LA COMPAÑÍA SUZUKI MOTOR DE COLOMBIA S.A, MEDIANTE LA METODOLOGÍA PENETRATION TESTING EXECUTION STANDARD

JAIME ALBERTO MOSQUERA MOSQUERA.
JULIÁN ANDRÉS RUIZ JARAMILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
DOSQUEBRADAS
2021

IDENTIFICACIÓN DE LAS DIFERENTES VULNERABILIDADES DE LA RED LAN DE PLANTA ENSAMBLADORA Y EL ALMACÉN DE PEREIRA DE LA COMPAÑÍA SUZUKI MOTOR DE COLOMBIA S.A, MEDIANTE LA METODOLOGÍA PENETRATION TESTING EXECUTION STANDARD.

JAIME ALBERTO MOSQUERA MOSQUERA.
JULIÁN ANDRÉS RUIZ JARAMILLO.

Proyecto de Grado – Proyecto Aplicado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMÁTICA

TUTOR
EDUARD ANTONIO MANTILLA TORRES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
DOSQUEBRADAS
2021

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Dosquebradas, Fecha sustentación

DEDICATORIA

A Dios

Por haberme permitido llegar hasta este punto y haberme dado salud para lograr nuestros objetivos, además de su infinita bondad y amor.

A mis Padres

Por haberme apoyado en todo momento, por sus concejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada por su amor.

Jaime Alberto Mosquera Mosquera

Mi proyecto de grado se lo dedico principalmente a Dios, que sin él nada sería posible, pues es él quien nos brinda la vida y la sabiduría para realizar cualquier acto en la vida.

y como no dedicar este importante logro a todas las personas que me rodean en mi vida cotidiana, familiares y amigos, que son quienes nos dan fuerza y animo en los momentos que desfallecemos.

Julián Andrés Ruiz Jaramillo

AGRADECIMIENTOS

Agradezco en primer lugar a DIOS, ya que con EL todo y sin EL nada…. por iluminarme y fortalecer mi espíritu para emprender este camino hacia el éxito.

También a mis padres por el constante apoyo por siempre haberme dado su fuerza y apoyo incondicional que me ha ayudado y llevado hasta donde estoy ahora.

Jaime Alberto Mosquera Mosquera

Agradezco A mi madre, mi abuela y mi hermana que siempre han estado en todo momento bueno y malo a mi lado, que son mi inspiración y ganas de salir adelante siempre.

Julián Andrés Ruiz Jaramillo

Agradecemos a Suzuki Motor de Colombia S.A. por permitirnos y darnos la oportunidad de realizar nuestro proyecto de grado de especialización en seguridad informática en la compañía, por siempre contar con la disposición de facilitar las actividades desarrolladas en el trascurso del proyecto para unos buenos resultados que beneficien a la compañía.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

AMENAZA: Se refiere a un incidente generado por una persona o software que puede generar daño a la información de un sistema informático, dispositivos o la totalidad de una red informática.

ANTIVIRUS: Software que brinda protección a los equipos informáticos, el cual impide el acceso de virus y archivos maliciosos.

CAJA BLANCA: Las pruebas de tipo caja blanca se utilizan cuando se cuenta con la información de la organización a la cual se va a realizar la auditoria.

CAJA GRIS: Las pruebas de tipo caja gris se utiliza en el caso de contar con información parcial de la organización a la cual se va a realizar la auditoria.

CAJA NEGRA: Las pruebas de tipo caja negra se utiliza en caso de no contar con ningún tipo de información de la organización a la cual se va a realizar la auditoria.

CONFIDENCIALIDAD: Es la protección que se le brinda a la información para evitar que personas o procesos tengan acceso a información de una organización sin estar autorizados.

CONTRASEÑA: Son palabras compuestas de letras mayúsculas, minúsculas, caracteres especiales y números con el fin de proteger los accesos a plataformas y herramientas.

DISPONIBILIDAD: Es la capacidad que se brinda de contar siempre con los servicios disponibles independiente de los incidentes que se puedan presentar.

FIREWALL: Un firewall es un dispositivo o elemento que protege, monitorea y restringe el tráfico de red, puede controlar el tráfico tanto entrante como saliente, mediante reglas previamente configuradas.

HACKER: Son personas que se dedican a realizar actividades de intrusión en diferentes sistemas informáticos, buscan las debilidades de los sistemas e intentan repararlos o sabotearlos.
Los hackers se dividen en diferentes ramas dependiendo de la labor que desarrollen.
Un hacker es considerado como un experto tecnológico superando por mucho los conocimientos en seguridad informática de una persona del común o ingeniero.

HACKER ÉTICO: Persona que se dedica a encontrar vulnerabilidades en los entornos informáticos, estas personas son contratadas por las organizaciones con

el fin de encontrar fallas y vulnerabilidades con el fin de fortalecer y mejorar la seguridad de una organización.

INGENIERÍA SOCIAL: Técnica mediante la cual una persona engaña con información falsa a otra persona para robar su información personal.

INTEGRIDAD: Es conservar la información con exactitud como fue generada, evitando manipulación y alteración por personas o procesos que no estén autorizados.

NESSUS: Herramienta de análisis y escaneos de vulnerabilidades más usada por la comunidad de hacking ético, realiza escaneos de red para detección de amenazas en las configuraciones y prevención de estas, desarrollado por Tenable.

NEXPOSE: herramienta para el análisis de vulnerabilidades, desarrollado por Rapid7, es uno de los softwares más completos para realizar escaneos de red y de host.

PENTEST: Pruebas de intrusión realizada por especialistas de seguridad informática con el fin de hallar o identificar vulnerabilidades en redes corporativas.

PTES: Penetration Testing Execution Standard, es un estándar para la ejecución de pruebas de penetración**.**

PISHING: Herramienta mediante la cual se sustrae información personal bancaria con el fin de robar, se realiza a través de correos electrónicos o llamadas telefónicas.

RED LAN: de la palabra en ingles Local Área Network, la cual traduce red de área local, esta red se denomina local debido a que se encuentra en infraestructuras como empresas, hogares y comprende los equipos que se sitúan dentro del sitio.

SPAM: Son correos electrónicos que contienen información no desea en las bandejas de entrada, normalmente presentan información publicitaria, pero también presentan contenidos de dudosa reputación.

VIRUS: programa que se replica con facilidad en los archivos y equipos, son altamente contagiosos, con el propósito de robar información, disminuir su rendimiento, estos virus no pueden dañar el equipo como tal, pero si son bastante molestos pues pueden hacer que los controladores fallen.

VULNERABILIDAD: Es un fallo en un sistema de información la cual puede ser explotada por un delincuente informático para lograr obtener acceso no autorizado y realizar acciones que inapropiadas para afectar la información o su funcionamiento.

RESUMEN

El siguiente trabajo tiene como propósito realizar un pentest o prueba de concepto con el fin de diagnosticar el estado de la infraestructura tecnológica de la compañía Suzuki Motor de Colombia S.A y específicamente a la red LAN de la planta ensambladora ubicada en el corregimiento de Cerritos perteneciente al municipio de Pereira, de igual manera se aplicará este pentest o prueba de concepto al almacén Pereira.

El proyecto aplicado tuvo una duración de diez (10) meses, la metodología que se utilizó para las pruebas de pentesting fueron de tipo caja blanca, basados en la metodología PTES, empleando diferentes herramientas se logró obtener información valiosa sobre las vulnerabilidades y brechas de seguridad en la red LAN.

PALABRAS CLAVES: Amenazas, Herramientas, PTES, Pentest, Red LAN, Vulnerabilidades.

ABSTRACT

The following work aims to perform a pentest or proof of concept in order to diagnose the state of the technological infrastructure of the company Suzuki Motor de Colombia SA and specifically to the LAN network of the assembly plant located in the village of Cerritos belonging to the municipality of Pereira, in the same way this pentest or proof of concept will be applied to the Pereira warehouse.

The applied project had a duration of ten (10) months, the methodology that was used for the pentesting tests were white box type, based on the PTES methodology, using different tools it was possible to obtain valuable information about vulnerabilities and security gaps in the LAN network.

KEYWORDS: LAN Network, Pentest, PTES, Threats, Tools, Vulnerabilities

INTRODUCCIÓN

La seguridad informática se ha convertido en una de las ramas más importantes de los departamentos de TI y de las organizaciones en general, esta diciplina viene teniendo gran auge en nivel mundial debido a las buenas prácticas y mejoras que ofrece a las infraestructuras tecnológicas de las diferentes organizaciones, sin importar su tamaño o geolocalización, es por esto que se requiere personal certificado y capacitado en estas prácticas, pues la seguridad de la información de cada organización depende de ello.

El uso de diferentes herramientas de pentest sobre las redes de datos organizaciones se ha convertido en una necesidad, ya que a través de estas se mueve diariamente información de alto valor, siendo estas herramientas de gran ayuda para conocer el estado de seguridad con que cuenta la organización, permitiendo de este modo realizar correcciones necesarias para mitigar los efectos adversos que puede presentar la intrusión de personas mal intencionadas a las redes corporativas.

El presente proyecto busca establecer e identificar las diferentes vulnerabilidades de la red LAN de planta ensambladora y el almacén de Pereira de la compañía Suzuki Motor de Colombia S.A., mediante diferentes herramientas de pentesting y empleando la metodología PTES, teniendo en cuenta la identificación de vulnerabilidades en las dos sucursales de la empresa, el objetivo es realizar un despliegue a nivel nacional de correcciones masivas las cuales permitirían la mejora de la infraestructura tecnológica a nivel general.

Se presenta un informe técnico y ejecutivo con el análisis de las vulnerabilidades encontradas y de las posibles soluciones, con el fin de mitigar las vulnerabilidades y riesgos encontrados durante el Pentest realizado a la red LAN de la planta ensambladora y el almacén Pereira, con el fin de que la compañía mejore considerablemente los niveles la de seguridad en sus sistemas informacionales.

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Actualmente la compañía Suzuki Motor de Colombia S.A cuenta con varios almacenes a nivel nacional, estos almacenes se encargan de la venta y prestación de servicios a las motocicletas vendidas de la marca, los almacenes cuentan con un cuarto de infraestructura de telecomunicaciones RACK, los cuales albergan los dispositivos de conexión utilizados para generar comunicación con el punto principal por medio de una conexión Multiprotocol Label Switching (MPLS); esta conexión se realiza hacia el punto principal que se encuentra ubicado en el corregimiento de Cerritos, de la ciudad de Pereira.

La sede más cercana al punto principal es el almacén ubicado en la ciudad de Pereira sobre el cual se realizan las pruebas piloto a nivel de configuración de red y nuevos dispositivos de seguridad, antes de iniciar una implementación masiva a nivel nacional.

La planta ensambladora de Suzuki Motor de Colombia S.A, es el punto principal de la organización donde se despliega toda la infraestructura tecnológica a los diferentes almacenes a nivel nacional, la cual brinda una conexión tipo LAN extendida mediante canales MPLS que permite la comunicación directa entre los almacenes y la planta ensambladora.

La infraestructura tecnológica de la compañía Suzuki Motor de Colombia S.A cuenta con 680 equipos de cómputo entre equipos de escritorio y laptops, 250 teléfonos de voz IP, 72 Access Point Meraki ubicados en los almacenes, 40 Access Point Hewlett-Packard y servidores con diversos sistemas operativos como Linux Centos 6 y 7, Windows Server versión 2008 R2 y Windows Server 2012 que brindan diferentes tipos de servicios para el desarrollo de las actividades de la organización. Sin embargo, a pesar de contar con una infraestructura de comunicaciones bien organizada y de buena capacidad, se presenta un problema repetitivo en la red desde hace aproximadamente un año, la falla consiste en una saturación de red LAN con énfasis en las horas pico, se evidencia lentitud en las respuestas, fallas en la navegación y consulta de los aplicativos de uso general de la compañía. Esta situación genera inconvenientes y malestar entre los usuarios tanto de los almacenes, como de la planta ensambladora, el desarrollo de las operaciones diarias de la organización se ven entorpecidas por las situaciones antes mencionadas.

Para mitigar las deficiencias de la infraestructura, es necesario realizar una revisión y monitoreo de los activos de información de la compañía, en la cual se validará si se presentan vulnerabilidades que puedan ser explotadas, provocando perdidas de información y mal funcionamiento de los dispositivos.

1.2 FORMULACIÓN DEL PROBLEMA

Se evidencia la necesidad de generar mejoras constantes en la infraestructura tecnológica de la compañía Suzuki Motor de Colombia S. A, aumentando los tiempos de respuesta en la Red LAN, para que los miembros de la empresa se sientan a gusto con los diferentes servicios prestados por las herramientas tecnológicas proporcionadas por la administración. Por lo anteriormente argumentado surge la necesidad de validar el funcionamiento de la red LAN de la planta ensambladora y el almacén Pereira, con el propósito de revisar a fondo y descubrir las vulnerabilidades presentes. Basado en estas premisas el presente proyecto aplicado pretende explicar:

¿Cómo la evaluación de seguridad de la infraestructura tecnológica permitirá minimizar el impacto y probabilidad de ocurrencia de vulnerabilidades, amenazas y riesgos en los sistemas informáticos de la compañía Suzuki Motor de Colombia S.A.?

2 JUSTIFICACIÓN

Mediante un análisis detallado de la infraestructura tecnológica de la red LAN de Planta Ensambladora y el almacén de Pereira, se busca identificar las diferentes vulnerabilidades mediante pruebas de testing, estas pruebas servirán para conocer el estado actual de la infraestructura y su nivel de seguridad.

La realización de este pentest o prueba de concepto permitirá obtener información valiosa para la compañía y específicamente al área de T.I de Suzuki Motor de Colombia S. A con el fin de mitigar o eliminar vulnerabilidades mejorando considerablemente la seguridad y el funcionamiento de su infraestructura tecnológica.

Los resultados obtenidos del análisis realizado a la red LAN serán suministrados mediante un informe detallado al jefe del Departamento de Sistemas de Suzuki Motor de Colombia S. A para dar a conocer las vulnerabilidades existentes y la manera de solucionarlas.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Evaluar la infraestructura tecnológica de la red LAN de Planta Ensambladora y el almacén de Pereira de la compañía Suzuki Motor de Colombia S.A. mediante herramientas de pentesting basados en la metodología Penetration Testing Execution Standard (PTES)

3.2 OBJETIVOS ESPECÍFICOS

- Analizar la infraestructura tecnológica de la red LAN de Planta Ensambladora y el almacén de Pereira de la compañía Suzuki Motor de Colombia S.A., para identificar las posibles vulnerabilidades que presenta la red LAN, apoyados en la metodología PTES.

- Seleccionar las herramientas de pentesting de red que permitan ejecutar las pruebas tipo caja blanca para la identificación de las vulnerabilidades en la red LAN de Planta Ensambladora y el almacén de Pereira de la compañía Suzuki Motor de Colombia S.A, teniendo en cuenta las herramientas que propone la metodología PTES.

- Elaborar la documentación sobre los resultados obtenidos al hacer las diferentes pruebas de seguridad a la red LAN de Planta Ensambladora y almacén de Pereira de la compañía Suzuki Motor de Colombia S.A.

- Establecer recomendaciones a partir de los resultados obtenidos en el pentest que permitan mitigar el riesgo frente a una amenaza en la red LAN de la Planta Ensambladora y del almacén Pereira de la compañía Suzuki Motor de Colombia S.A.

4 MARCO REFERENCIAL

4.1 MARCO CONCEPTUAL

A continuación, se definirán conceptos claves relacionados con la seguridad informática, que serán usados en el presente proyecto aplicado de grado.

4.1.1 Vulnerabilidad informática:

Cuando se hace referencia a una vulnerabilidad informática, hablamos de una debilidad en un sistema o entorno informático el cual puede ser aprovechado por un atacante

"es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos"[1].

4.1.2 Amenaza informática:

Es un evento pasado o hipotético que puede generar daño en los entornos informáticos, permitiendo fuga, robo y manipulación de la información.

"Es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas"[2].

4.1.3 Infraestructura informática:

Es el conjunto de herramientas tanto de hardware como de software que tiene una organización y con los cuales realiza sus procesos, este término incluye la configuraciones y estructura de red, esta "consiste en un conjunto de dispositivos físicos y aplicaciones de software que se requieren para operar toda la empresa. Sin embargo, la infraestructura de TI también es un conjunto de servicios a lo largo

[1] Incibe. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [Sitio WEB]. Incibe. [Consulta: 3, octubre, 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

[2] Incibe. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [Sitio WEB]. Incibe. [Consulta: 3, octubre, 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

y ancho de la empresa, presupuestados por la administración y que abarcan capacidades tanto humanas como técnicas"[3].

4.1.4 Delito informático:

Se refiere a la acción antijuridica sobre la Ley 1273 de 2009 denominada "de la protección de la información y de los datos" establecida por el gobierno de Colombia para la protección de los sistemas que utilicen tecnologías de información y comunicaciones. Según lo define la Policía Nacional Colombiana en su sitio web "Los delitos informáticos son conductas en que el o los delincuentes se valen de programas informáticos para cometer delitos como implantación de virus, suplantación de sitios web, estafas, violación de derechos de autor, piratería"[4].

4.1.5 Riesgo informático:

La probabilidad de que una vulnerabilidad pueda ser explotada o un evento nocivo ocurra afectando la organización, "Se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado. El riesgo puede ser mitigado mediante políticas de seguridad y continuidad del negocio que suelen prever posibles ataques y proponen soluciones de actuación ante situaciones cuyo riesgo pueda ser elevado"[5].

[3] Universidad Nacional de Salta. UNIDAD 1: Introducción a la Informática Hardware y Software. [Sitio WEB]. Seminario de Informática. [Consulta: 23 marzo 2021]. Disponible en: https://economicas.unsa.edu.ar/sigeco/archivos/semi_material/U1-DT-IntroduccionalaInformatica.pdf

[4] Policía Nacional de Colombia. [Sitio web] [Citado 23 de marzo 2021]. Disponible en: [https://www.policia.gov.co/denuncia-virtual/delitos-informaticos#:~:text=Los%20delitos%20inform%C3%A1ticos%20son%20conductas,(Normatividad%20sobre%20delitos%20inform%C3%A1ticos)].

[5] Incibe. Glosario de términos de ciberseguridad. [Sitio web] [Citado 23 de marzo de 2021]. Disponible en: [https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf]

4.2 MARCO TEÓRICO

4.2.1 Seguridad Informática en las organizaciones: Dado el crecimiento de los delitos informáticos en Colombia, las diferentes organizaciones se han visto con la necesidad de realizar mejoras a la seguridad de sus infraestructuras tecnológicas con el fin de evitar que se comentan actos ilícitos en contra de los recursos informáticos, como es acceso no autorizado a los sistemas informáticos atentando contra los pilares de la información permitiendo la alteración, filtración, secuestro o perdida de la información.

Partiendo del hecho que ningún entorno informático o infraestructura es segura en un 100 %, es importante que a las organizaciones se apliquen análisis de riesgos con el fin de detectar posibles vulnerabilidades y brechas de seguridad, un análisis de riesgo "es el estudio de las causas de las posibles amenazas, y los daños y consecuencias que éstas puedan producir"[6].

Teniendo en cuenta que la seguridad informática en las organizaciones se ha convertido en una necesidad básica y fundamental para cada organización, debemos indicar que "la seguridad Informática abarca procedimientos meticulosos destinados a proteger contra intrusos externos e internos los activos de infraestructura tecnología (Hardware, Software, redes de datos y sistemas de información) con que cuentan las empresas y son utilizados diariamente para almacenar, transmitir y procesar la información"[7].

Además, se podrá indicar que la seguridad informática como diciplina se encarga de establecer técnicas y procedimientos enfocados en brindar condiciones seguras y favorables para los ambientes informáticos tanto en empresas como a personas del común.
La seguridad informática se basa en 3 pilares esenciales, los cuales se deben cumplir para que el entorno informático cuente con los estándares mínimos de seguridad.

- Confidencialidad: Las organizaciones son responsables de establecer controles que permitan garantizar la confidencialidad de su información, para la cual las empresas se deben apoyar en estándares nacionales o internaciones que les permitan establecer técnicas de control para los sistemas de información, logrando de esa manera que personas o programas

[6] GOMEZ. Análisis de Riesgo. (Sitio web) (citado 23 de marzo 2021). Disponible en: (https://www.monografias.com/trabajos83/analisis-riesgo/analisis-riesgo.shtml)

[7] PALACIOS PALACIOS Jeysser. Análisis de vulnerabilidades de la infraestructura tecnológica en la dependencia de formación profesional integral del SENA regional Guainía, para el diseño de una propuesta de aseguramiento de la información basada en la metodología Magerit. Guainia; Unad. P 15

no autorizados puedan tener acceso a la información catalogada como confidencial por la organización.

> Esto involucra un monitoreo del manejo de claves, del control del personal que tienen acceso quienes deben firmar compromisos de confidencialidad con su contratante. La confidencialidad es uno de los factores de mayor riesgo y más complejos de asegurar ya que la información es manejada por el eslabón más débil de la cadena, el usuario, quien, por error, omisión o con conocimiento de causa puede dejar expuesta la información vulnerando la organización[8].

Cualidad y seguridad de un entorno informático sobre la información de una organización de no permite que personas o programas no autorizados puedan consultar o hacer uso de la misma.

- Integridad: Cualidad de la información, haciendo referencia a que la información sea confiable, que no presente modificaciones o sea incorrecta debido a alteraciones de usuarios o programas no autorizados en un entorno informático.
  Conservar la integridad de la información es sumamente importante pues de esto depende el funcionamiento correcto de cada proceso de una organización, es por esto por lo que se puede llegar a decir que es el pilar más importante de la información.

- Disponibilidad: Busca generar entornos informáticos que puedan garantizar a los usuarios el acceso de manera constante independientemente de los incidentes que se puedan presentar, la organización debe contar con planes de recuperación de desastres ya sean naturales o ataques informáticos,

  Pues bien, se debe tener en cuenta que hay factores que pueden afectar este pilar como lo indica Ricardo Alfredo López

  > Se debe analizar desde los factores de riesgo físico que puedan llegar a impedir el acceso a la información como son robos, fallos eléctricos, riesgos por desastres naturales, ataques de denegación de servicios, ataques terroristas, asonadas, y demás factores que impidan el acceso a la información, como también factores de riesgo Lógico como son malware, secuestradores de información, ransomware, escalamiento de privilegios y destrucción de la data.[9]

[8] ALFREDO LÓPEZ Ricardo. Sistema de Gestión de la Seguridad Informática. Bogotá: Areandina. 2017. P. 11.
[9] ALFREDO LÓPEZ Ricardo. Sistema de Gestión de la Seguridad Informática. Bogotá: Areandina. 2017. P. 11.

Metodologías de Intrusión y testing

En la actualidad existen diferentes tipos de metodologías de intrusión y testing las cuales se pueden aplicar en cualquier tipo de compañía, permitiendo que las organizaciones puedan identificar diferentes vulnerabilidades en su Sistema de Gestión de Seguridad de la Información (SGSI), estando estos acoplados y ajustados a estándares de alta calidad, permitiendo que los niveles de seguridad sean aceptables para confrontar las amenazas existentes en los entornos web y ambientes digitales, como indica el ingeniero Juan Carlos Briceño "Para realizar un análisis de riesgos completo, es necesario conocer muy bien la infraestructura de la empresa, entender el corazón del negocio que maneja, y comenzar de manera ordenada a recolectar información, organizarla y analizarla, con el fin de identificar las amenazas, los riesgos, las causas, los controles utilizados, y en general todo lo concerniente a los activos de información de esta"[10], permitiendo de esta manera que se puedan aplicar las metodologías de intrusión y testing acorde a la necesidad y la infraestructura de la organización.

Ataques Informáticos

Un ataque informático es todo aquel intento organizado con el fin de vulnerar los sistemas informáticos y ocasionar daños a las infraestructuras tecnológicas tanto de las compañías como de las personas del común.

Los ataques informáticos a raíz de la pandemia generada por el virus COVID-19, se han incrementado, ocasionando esto grandes inconvenientes y perdidas para las compañías a nivel nacional.
Como informa el artículo en el periódico EL TIEMPO en el año 2019"De acuerdo con un estudio realizado por el Mintic, la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), se revela que en Colombia más del 60% de las organizaciones encuestadas incurrieron en costos cercanos al millón de pesos por daños relacionados con ciberataques, mientras que el 20% gastaron entre 1 y 15 millones de pesos, el 15% entre 15 y 235 millones y el 5% presentó valores desaforados de hasta 4.000 millones de pesos, como consecuencia de incidentes de vulneración tecnológica"[11]

[10] BRICEÑO Juan Carlos. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE SEGURIDAD INFORMÁTICA DE LA EMPRESA KAPPA10 LTDA. (Sitio web) (citado 23 de marzo 2021). Bogotá. Disponible en: (https://repository.unad.edu.co/bitstream/handle/10596/27822/%20%09jcbricenoo.pdf?sequence=1&isAllowed=y) P 25

[11] El Tiempo. Empresas que pierden hasta $4.000 millones por ciberataques. (sitio web). (citado el 27 de marzo de 2021). Disponible en: https://www.eltiempo.com/economia/existen-empresas-que-pierden-hasta-4-000-millones-por-ciberataques-392246

Según el Centro de Atención Inmediata virtual de la policía nacional[12] en el año 2020 se presentó un incremento en la ciberdelincuencia de más del 96% en comparación con el año 2019, representando esto un alto índice de ataques informáticos no solo en las compañías colombianas, sino también en las personas del común, por lo tanto, se está generando una gran demanda en el campo de la seguridad informática con el fin de fortalecer y proteger las organizaciones de estos ataques, que lo único que representan para las mismas son pérdidas económicas.

[12] POLICÍA NACIONAL, Balance Cibercrimen 2020, Bogotá. 2020, No 45. p 1.

4.2 ANTECEDENTES O ESTADO ACTUAL

De acuerdo a las búsquedas realizadas, referente a trabajos aplicados o proyectos relacionados sobre identificaciones de vulnerabilidades en redes corporativas o empresariales, se encuentra el trabajo desarrollado por VIVER RAMÍREZ Aydee Mercedes quien realizo su proyecto aplicado de especialización sobre la identificación de vulnerabilidades de la red LAN del buque oceanográfico de la autoridad colombiana a través de las herramientas de pruebas de pentesting, en este trabajo se maneja test de escaneos de vulnerabilidades en los sistemas de información de un buque de la armada AR Libertad que esta asignado a tareas en la aguas de jurisdicción correspondientes a Colombia en el océano pacifico.

Este proyecto surge debido al alto grado de valor que tiene la información que recolecta este buque, debido a que los datos son de interés tanto institucional, nacional e internacional, sin embargo, se evidencia la poca seguridad y la falta de medidas de protección, dejando estos datos expuestos, con lo que se puede presentar ataques de intrusión, permitiendo así que la información sea vulnerada en su totalidad.

Título del trabajo Aplicado: Identificación de vulnerabilidades de la red LAN del buque oceanográfico de la autoridad colombiana a través de las herramientas de pruebas de pentesting[13].

Autor: VIVER RAMÍREZ, Aydee Mercedes

Obtenido de: https://repository.unad.edu.co/bitstream/handle/10596/12425/46646702.pdf?sequence=1&isAllowed=y

Dentro de los referentes conceptuales del análisis relacionado con vulnerabilidades en redes corporativas o empresariales se encuentra el proyecto de grado de los Especialistas de Seguridad informática MONTOYA SALAZAR, Yeny Patricia, VANEGAS, Andrés Ferney, quienes ejecutan un análisis de vulnerabilidades a los sistemas informáticos del departamento de policía del Caquetá, donde se evalúa la infraestructura tecnológica de esta entidad con el fin de detectar las vulnerabilidades existentes, debido a que la información que manejan es de alto valor, ya que es información necesaria para los procedimientos que ejercen otras instituciones gubernamentales.

[13] VIVER RAMÍREZ, Aydee Mercedes. Identificación de vulnerabilidades de la red LAN del buque oceanográfico de la autoridad colombiana a través de las herramientas de pruebas de pentesting. (Sitio web) (citado 17 de mayo 2021). Cali. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/12425/46646702.pdf?sequence=1&isAllowed=y

Debido a que la Policía considera que el segundo activo más importante es la información que se recopila, se exige un manejo adecuado a la misma, esto conlleva a la necesidad de realizar análisis y encontrar las vulnerabilidades para mitigarlas y/o corregirlas dado el caso.

Título del trabajo aplicado: Análisis de vulnerabilidades en el sistema de seguridad físico e informático del departamento de policía Caquetá[14].

Autor: MONTOYA SALAZAR, Yeny Patricia, VANEGAS, Andrés Ferney.

Obtenido de: https://repository.unad.edu.co/jspui/bitstream/10596/25972/1/%20%09ypmontoyas.pdf

En un tercer trabajo relacionado con el tema de identificación de vulnerabilidades en redes corporativas o empresariales, se encuentra el proyecto de grado del especialista de seguridad informática VALDERRAMA GUARDIA, Jhon Edinson, que se refiere, a la necesidad de realizar un pentest a la alcaldía de Cantón San Pablo, debido a que se presentan graves pérdidas de información y daños de la misma, el objetivo de este pentest es presentar una mejora sobre la Confidencialidad, disponibilidad e integralidad de la información que maneja dicha alcaldía, pues es ahí donde se manejan todos los temas relacionados del municipio, finalizado este pentest se pretende poder dar una solución o mitigación a la vulnerabilidades encontradas mejorando ostensiblemente la seguridad de la información.

Título del trabajo aplicado: Pentesting “prueba de penetración” para la identificación de vulnerabilidades en la red de computadoras en la alcaldía del municipio de Cantón del San Pablo, departamento del Chocó[15].

Autor: VALDERRAMA GUARDIA, Jhon Edinson.

Obtenido de: https://repository.unad.edu.co/bitstream/handle/10596/18049/1077436201.pdf?sequence=1&isAllowed=y

[14] MONTOYA SALAZAR, Yeny Patricia, VANEGAS, Andrés Ferney. Análisis de vulnerabilidades en el sistema de seguridad físico e informático del departamento de policía Caquetá. (Sitio web) (citado 17 de mayo 2021). Florencia. Disponible en: https://repository.unad.edu.co/jspui/bitstream/10596/25972/1/%20%09ypmontoyas.pdf

[15] VALDERRAMA GUARDIA, Jhon Edinson. Pentesting “prueba de penetración” para la identificación de vulnerabilidades en la red de computadoras en la alcaldía del municipio de Cantón del San Pablo, departamento del Chocó. (Sitio web) (citado 17 de mayo 2021). Cantón del San Pablo. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/18049/1077436201.pdf?sequence=1&isAllowed=y

4.3 MARCO LEGAL

Dada la incursión y utilización de tecnologías en los diferentes sectores del país, se ve la necesidad de promover una ley que cobije y proteja a las organizaciones y población en general de los accesos fraudulentos y robos de información en los diferentes entornos informáticos, es por eso que en el congreso de la república de Colombia se promulga la ley 1273 del 2009, con el fin de castigar las personas o grupos que quebranten o incumplan los artículos que la componen, con penas de prisión las cuales se encuentran entre los treinta y seis (36) a noventa y seis (96) meses y multas económicas las cuales están entre 100 a 1.000 salarios mínimos legales mensuales vigentes.

4.3.1 Ley 1273 del 2009[16]

Artículo 1° Adiciónese el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPITULO I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Artículo 269A: Acceso abusivo a un sistema informático.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos

Artículo 269D: Daño Informático.

Artículo 269E: Uso de software malicioso.

Artículo 269F: Violación de datos personales.

Artículo 269G: Suplantación de sitios web para capturar datos

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la

[16] Ley 1273 de 2009 Nivel Nacional. [Sitio Web]. Propiedad de la Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá D.C. [Consulta: 19 de abril 2021]. Disponible en: http://https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva:

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
- Por servidor público en ejercicio de sus funciones.
- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- Obteniendo provecho para sí o para un tercero.
- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
- Utilizando como instrumento a un tercero de buena fe.
- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO II

De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes.

Artículo 269J: Transferencia no consentida de activos.

Las penas que genera el incumplimiento de cada artículo de esta ley están entre cuarenta y ocho (48) meses de prisión y un máximo de noventa y seis (96) Meses de prisión, y multas de entre cien (100) y mil (1000) salarios mínimos legales vigentes.

4.3.2 Ley estatutaria 1581 de 2012

Mediante la ley 1581 de 2012 se establece la disposición general para la protección de datos personales registrados en cualquier base de datos que puedan ser susceptibles de manipulación por entidades públicas o privadas.
Dado que la compañía Suzuki Motor conserva en sus bases de datos información susceptibles de sus clientes y al tener algún tipo de vulnerabilidad en su infraestructura tecnológica, estos datos se pueden ver expuestos adulteración, perdida o accesos no autorizados, lo cual puede generar multas económicas por parte de los entes reguladores.

La ley 1581 establece en el titulo VI deberes de los responsables del tratamiento y encargados del tratamiento, el artículo 17 que corresponde a deberes de los responsables del tratamiento en el caso del presente trabajo aplican los siguientes literales:

“d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;

n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.”[17]

Las organizaciones que incumplan la presente ley y procedimientos correspondientes estarán expuestos a sanciones por parte de la Superintendencia de Industria y Comercio a los responsables del tratamiento y encargados del tratamiento de los datos, mediante los siguientes literales se establecen los tipos de sanciones y multas.

“a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;

b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;

[17] Ley estatutaria 1581 de 2012 [Sitio Web]. Función pública. [Consulta: 22 de junio 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;

d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;"[18]

[18] Ley estatutaria 1581 de 2012 [Sitio Web]. Función pública. [Consulta: 22 de junio 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

5 DISEÑO METODOLÓGICO

El diseño metodológico para la elaboración del proyecto de grado aplicado se realizará mediante la metodología cuantitativa debido a que con esta metodología se puede cuantificar, hacer el uso de gráficos estadísticos para demostrar las incidencias encontradas, agrupándolas y de este modo dar un mejor entendimiento de la situación y como indica BARRANTES ECHAVARRÍA Rodrigo en su libro Investigación: un camino al conocimiento en la página 118, “el plan de trabajo dentro del enfoque cuantitativo es completo, estructurado, minucioso, detallado, cronogramado, e inclusive debe contener los instrumentos de recolección de la información”[19].

Es por esto por lo que se decidió que la mejor opción para realizar el pentest requerido para el desarrollo del proyecto aplicado en la red LAN de la compañía Suzuki motor de Colombia S.A y el almacén Pereira, es el estándar Penetration Testing Execution Standard (PTES), ya que ofrece una metodología estandarizada de procesos, los cuales se pueden aplicar a la necesidad actual, cabe resaltar que se tomara en cuenta las partes necesarias y que apliquen al proyecto que se llevara a cabo.

5.1 METODOLOGÍA PTES

El trabajo aplicado a la compañía Suzuki Motor de Colombia S.A, específicamente a la planta ensambladora y el almacén de Pereira, se basará en el desarrollo de la guía Metodológica PTES, el cual tiene como base siete sesiones principales, las cuales pueden ser o no aplicables a este proyecto de grado, permitiendo llevar de una manera controlada y establecida el desarrollo de toda la actividad.

Las siete sesiones a desarrollar son las siguientes:

5.1.1 Interacciones previas:
Se acordará con el Departamento de Sistemas de la compañía Suzuki Motor de Colombia S. A, el nivel de profundidad que tendrán las pruebas de intrusión y de concepto, el cuándo, el cómo de la realización de la actividad y su alcance en general.

5.1.2 Recolección de información:
Se buscará recopilar la información necesaria para la realización del pentest o

[19] BARRANTES ECHAVARRÍA Rodrigo. Investigación: Un camino al conocimiento. Ed 2. 2013 p 118

prueba de concepto, los activos de información que serán objetivos de análisis, se realizará una recolección de información de 3 niveles, lo cual permitirá definir la duración, las limitantes de las pruebas y las posibles vulnerabilidades que podemos usar en un futuro.

5.1.3 Modelado de amenazas:
Durante este proceso, se analiza la infraestructura de la compañía Suzuki Motor de Colombia S. A, específicamente la planta ensambladora y el almacén Pereira los planes de contingencia con que se cuentan, los activos humanos, activos informáticos, básicamente se planeara y se verificara por donde se puede generar las vulnerabilidades, centrados en dos elementos claves como los activos y los atacantes.

5.1.4 Análisis de vulnerabilidades:
El análisis pretende realizar las pruebas de vulnerabilidades a los activos de información establecidos por el Departamento de Sistemas de la compañía Suzuki Motor de Colombia S.A., indicando el grado de profundidad a realizar en las pruebas y dando cumplimiento a lo pactado con la organización, para la realización de un análisis profundo y completo se pretende realizar la aplicación de los subprocesos del análisis de vulnerabilidad que están conformados por pruebas, activos, pasivos, validación e investigación.

5.1.5 Explotación:
En esta etapa se realiza la explotación de las vulnerabilidades halladas con el fin de ser aprovechadas y realizar ingresos a los sistemas de la compañía, esta no será considerada pues el objetivo no es vulnerar o aprovecharse de las brechas de seguridad encontradas, ya que se pueden ver afectados los diferentes procesos de la compañía.

5.1.6 Post explotación:
Una vez realizada la explotación, se realizará la permanecía en la red y se continúa revisando información interna, mediante el acceso obtenido, pero al no realizar la fase o etapa de explotación, esta tampoco será tenida en cuenta para ejecutar sobre Suzuki Motor de Colombia S.A. con el fin de no generar afectaciones a los procesos cotidianos desarrollados.

5.1.7 Informe:
Finalizados los pentest se hará entrega a la compañía Suzuki Motor de Colombia S. A los detalles e informes con las vulnerabilidades encontradas, el nivel de seguridad con que se cuenta, se entregara los informes en un lenguaje comprensible para que

las personas interesadas de la compañía puedan comprender e interpretar los resultados obtenidos.

Según lo indicado en las siete sesiones, para el desarrollo del proyecto aplicado a la compañía Suzuki Motor de Colombia en su planta principal y almacén de Pereira, solo se tendrán en cuenta cinco sesiones:

- Interacciones previas
- Recolección de Información
- Modelado de amenazas
- Análisis de vulnerabilidades
- Informe

Se decide no tener en cuentas dos sesiones que son:

- Explotación
- Post Explotación

Debido a que la ejecución de estas dos sesiones puede generar inconvenientes en la compañía Suzuki Motor de Colombia S.A y el correcto funcionamiento de los diferentes activos de información ocasionando una alteración en la operación de la compañía.

6 DESARROLLO DE LOS OBJETIVOS

6.1 ANÁLISIS DE LA INFRAESTRUCTURA TECNOLOGÍA.

El análisis de la infraestructura tecnología con la que cuenta Suzuki Motor de Colombia S. A, se realizará con la modalidad de auditoria o pentest denominado caja blanca, por parte del Departamento de TI y con aprobación de la administración, se suministró la información de la infraestructura tecnológica que componen los sitios denominados Planta ensambladora y almacén Pereira, que son los objetos de estudio de este proyecto aplicado.

Partiendo del uso de metodología PTES se da inicio con la fase de Compromiso Previo, donde se realiza una reunión con la jefe del departamento de Sistemas y el coordinador de desarrollo tecnológico de la compañía Suzuki Motor de Colombia S.A, en la cual se estable el alcance de la prueba de penetración, donde se acuerda cuantos activos de información serán permitidos para la realización de la actividad, fecha de inicio de la actividad y fecha de finalización de esta, horarios en los que se permitirá la realización de las pruebas, se establecen las IP de los activos de información que se permite por parte de la compañía para estas pruebas, estas IP deben estar ocultas para evitar dar a conocer información de la segmentación de la red, se define que solo se realizara sobre IP de activos de información internos.

En la reunión se establece que la línea de comunicación directa y el contacto de emergencia, será con la jefe del departamento de sistemas, donde se establece que la información a comunicar se va a manejar vía correo electrónico y vía telefónica para mantener al tanto del progreso de las actividades y de las pruebas de penetración realizadas, se define que se entregara como resultado las evidencias de los pentest realizados y que estos no serán suministrados a ningún otra persona debido a que son catalogados como información confidencial y de alto riesgo para la compañía.

6.1.1 Especificación de Rangos de IP planta ensambladora.

Mediante el acuerdo establecido con el jefe del departamento de sistemas se decide que se trabajara sobre diez activos de información en la planta ensambladora, siendo este acuerdo parte de la fase 2 de la metodología PTES recopilación de inteligencia o información, con la se definen los objetivos de la auditoria y por lo cual se estable el levantamiento de requerimientos de las IP a analizar, como se muestra en el cuadro 1. Levantamiento de requerimientos.

El pentest a realizar es de caja blanca debido a conocimiento propio sobre los activos informáticos y de la conformación de la infraestructura tecnológica a analizar de la compañía.

Cuadro 1. Levantamiento de requerimientos

FORMATO DE LEVANTAMIENTO DE REQUERIMIENTOS PARA PENTEST

Nombre de la Compañía:	Suzuki Motor de Colombia S.A.	FECHA	15/04/2021
Nombre de contacto en la compañía:	Yorlen Álzate Peláez		
Nombre del contacto que realiza la actividad:	Julian Andrés Ruiz Jaramillo		
Nombre del contacto que realiza la actividad:	Jaime Alberto Mosquera Mosquera		

No.	OBJETIVO AUDITAR	IP	ESCENARIO	TIPO DE AUDITORIA
1	Servidores	192.XXX.YYY.Z43	LAN	Caja Blanca
2	Servidores	192.XXX.YYY.Z21	LAN	Caja Blanca
3	Servidores	192.XXX.YYY.Z23	LAN	Caja Blanca
4	Servidores	192.XXX.YYY.Z46	LAN	Caja Blanca
5	Servidores	192.XXX.YYY.Z49	LAN	Caja Blanca
6	Servidores	192.XXX.YYY.Z19	LAN	Caja Blanca
7	Servidores	192.XXX.YYY.Z44	LAN	Caja Blanca
8	Servidores	192.XXX.YYY.Z51	LAN	Caja Blanca
9	Equipos	192.XXX.YYY.Z48	LAN	Caja Blanca
10	Equipos	192.XXX.YYY.Z03	LAN	Caja Blanca

Fuente: MOSQUERA Jaime Alberto, RUIZ Julián Andrés

Habiendo establecido los activos de información a trabajar en la planta ensambladora de la compañía Suzuki Motor de Colombia S.A, se procede a definir los activos de información y las IP a auditar en el almacén Pereira.

Bajo la información suministrada por parte del departamento de TI, se procede a realizar el diagrama de topología de la red LAN del punto de planta ensambladora al igual que del almacén Pereira, el objetivo de diagramar la red LAN es poder

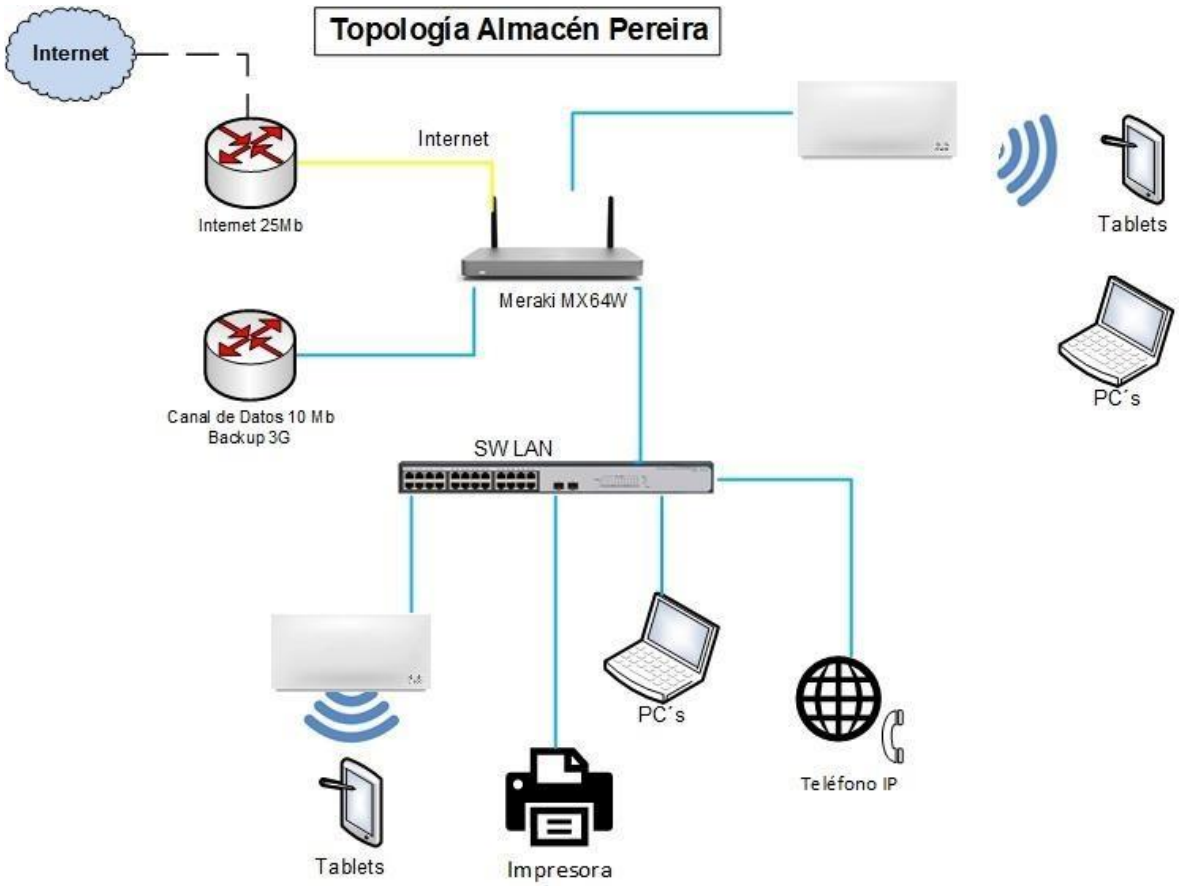
identificar los activos que componen esta infraestructura e identificar posibles vulnerabilidades en dichos activos de información de Suzuki Motor de Colombia S.A.

6.1.2 Infraestructura tecnológica Almacén Pereira

La infraestructura de red que se representa en la figura 1, del almacén Pereira tiene el objetivo una mayor identificación de los siguientes activos que hace parte de la red de datos.

- 1 Swicht HP de 24 puertos
- 1 firewall UTM
- 2 AP Wi-Fi
- 1 impresora
- 12 computadores
- 9 teléfonos IP
- 4 tabletas Samsung Galaxy

Figura 1. Topología Almacén Pereira



Fuente: MOSQUERA Jaime Alberto, RUIZ Julián Andrés

Con la identificación de los activos que componen la infraestructura tecnológica de la sede Pereira, se podrá dar paso a la búsqueda de información más detallada de cada uno de los activos identificados que permita conocer información como sistema operativo, IP, Marca, modelo, entre otros, información que resultará útil para la realización del pentest.

Telefonía IP Almacén Pereira

Cuadro 2. Segmento Telefonía IP

MARCA	MODELO	IP
Grandstream	GXP	192.YYY.XXX.Z3
Grandstream	GXP	192.YYY.XXX.Z2
Grandstream	GXP	192.YYY.XXX.Z1
Grandstream	GXP	192.YYY.XXX.Z0

Grandstream	GXP	192.YYY.XXX.Z9
Grandstream	GXP	192.YYY.XXX.Z8
Grandstream	GXP	192.YYY.XXX.Z7
Grandstream	GXP	192.YYY.XXX.Z6
Grandstream	GXP	192.YYY.XXX.Z5

Fuente: MOSQUERA Jaime Alberto, RUIZ Julián Andrés

Posterior a la identificación de cada uno de los teléfonos IP y sus segmentos que conforman la infraestructura se procede con la identificación de los equipos de cómputo como se muestran en el Cuadro 3.

Cuadro 3. Segmento PC

EQUIPO	SISTEMA OPERATIVO	FABRICANTE	MODELO	IP
Equipo1	Microsoft Windows 7 Professional	LENOVO	10B7006GLS	192.XXX.YYY.Z5
Equipo2	Microsoft Windows 10 Pro	HP	HP ProBook 440 G5	192.XXX.YYY.Z1
Equipo3	Microsoft Windows 10 Pro	HP	HP ProBook 440 G5	192.XXX.YYY.Z61
Equipo4	Microsoft Windows 7 Professional	Hewlett-Packard	HP ProBook 430 G2	192.XXX.YYY.Z48
Equipo5	Microsoft Windows 7 Professional	LENOVO	10B70029LS	192.XXX.YYY.Z28
Equipo6	Microsoft Windows 7 Professional	LENOVO	10B7006FLS	192.XXX.YYY.Z3
Equipo7	Microsoft Windows 7 Professional	LENOVO	10B70029LS	192.XXX.YYY.Z82
Equipo8	Microsoft Windows 7 Professional	Hewlett-Packard	HP ProBook 430 G2	192.XXX.YYY.Z54
Equipo9	Microsoft Windows 10 Pro	HP	HP ProDesk 400 G4 SFF	192.XXX.YYY.Z83
Equipo10	Microsoft Windows 10 Pro	LENOVO	10AUA03800	192.XXX.YYY.Z2
Equipo11	Microsoft Windows 7 Professional	LENOVO	10B70029LS	192.XXX.YYY.Z6
Equipo12	Microsoft Windows 10 Pro	HP	HP ProBook 440 G3	192.XXX.YYY.Z51
Equipo13	Microsoft Windows 7 Professional	Hewlett-Packard	HP ProBook 430 G2	192.XXX.YYY.Z15
Equipo14	Microsoft Windows 7 Professional	Hewlett-Packard	HP ProBook 430 G2	192.XXX.YYY.Z53

Equipo15	Microsoft Windows 7 Professional	LENOVO	10B70029LS	192.XXX.YYY.Z08
Equipo16	Microsoft Windows 7 Professional	LENOVO	10B70029LS	192.XXX.YYY.Z4

Fuente: MOSQUERA Jaime Alberto, RUIZ Julián Andrés

6.1.3 Infraestructura tecnológica planta ensambladora.

La infraestructura tecnológica de la planta ensambladora de Suzuki Motor de Colombia S.A es demasiado robusta por lo que se acordó con el jefe del Departamento de Sistemas el escaneo de vulnerabilidades sobre cierta cantidad de activos, es importante aclarar que hay activos considerados de alto impacto en los procesos diarios organizacionales, por lo que se consideró prudente evitar realizar el análisis sobre los mismos, con el fin de no entorpecer la continuidad del negocio.

En base a lo acordado con el jefe del área de T.I se obtuvo la aprobación del escaneo de vulnerabilidades sobre los siguientes activos de información, que se encuentran en el cuadro 4. Activos planta ensambladora, sobre el cual se estipulan los diferentes dispositivos y alcance del pentest a realizar, como se indicó anteriormente.

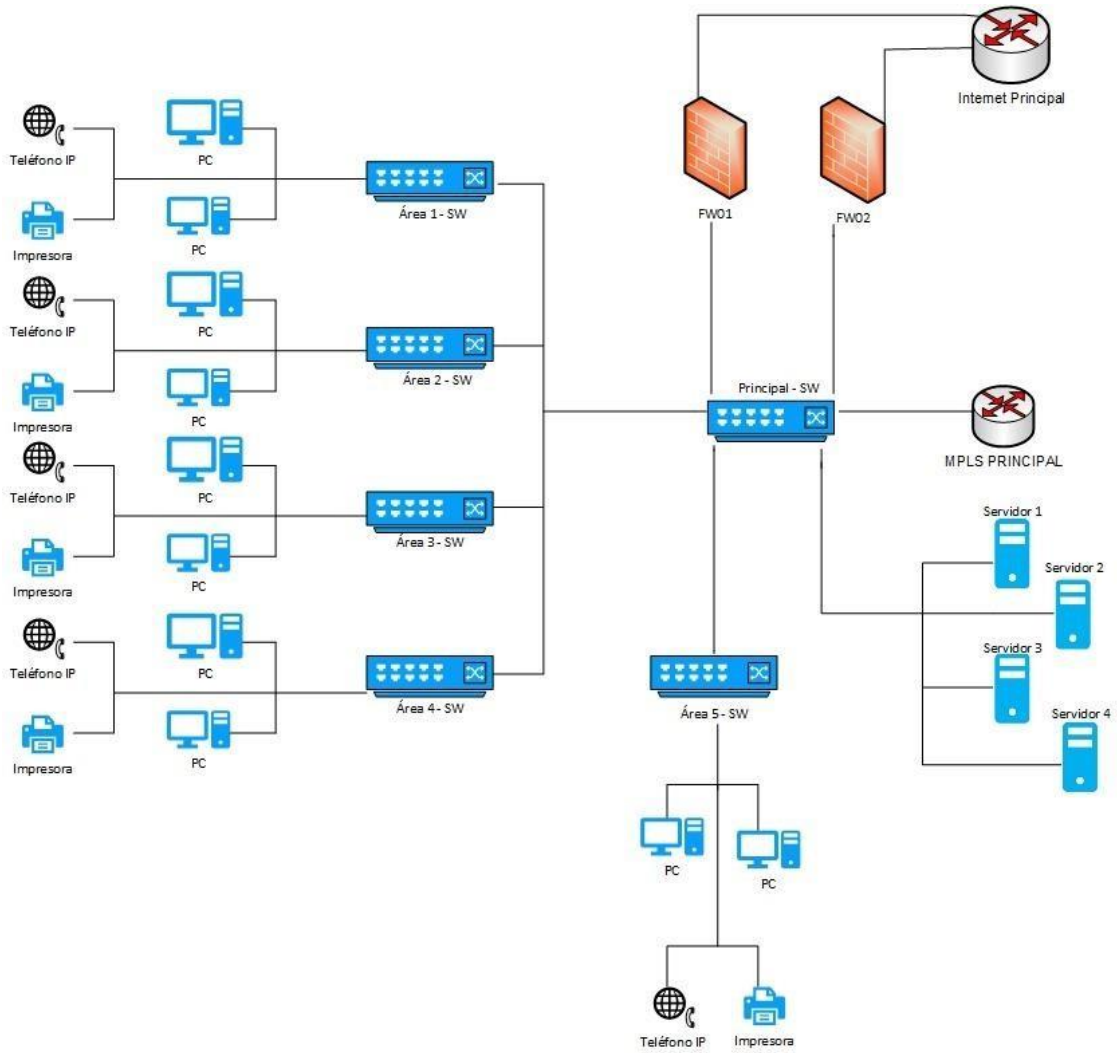
Cuadro 4. Activos Planta Ensambladora

No.	OBJETIVO AUDITAR	IP	ESCENARIO	TIPO DE AUDITORIA
1	Servidores	192.XXX.YYY.Z43	LAN	Caja Blanca
2	Servidores	192.XXX.YYY.Z21	LAN	Caja Blanca
3	Servidores	192.XXX.YYY.Z23	LAN	Caja Blanca
4	Servidores	192.XXX.YYY.Z46	LAN	Caja Blanca
5	Servidores	192.XXX.YYY.Z49	LAN	Caja Blanca
6	Servidores	192.XXX.YYY.Z19	LAN	Caja Blanca
7	Servidores	192.XXX.YYY.Z44	LAN	Caja Blanca
8	Servidores	192.XXX.YYY.Z51	LAN	Caja Blanca
9	Equipos	192.XXX.YYY.Z48	LAN	Caja Blanca
10	Equipos	192.XXX.YYY.Z03	LAN	Caja Blanca

Fuente: MOSQUERA Jaime Alberto, RUIZ Julián Andrés

Mediante el diagrama de red datos indicado en la figura 2 de planta ensambladora de Suzuki motor de Colombia se busca tener una mayor compresión del entorno de red y su conexión entre dispositivos.

Figura 2. Topología Planta



Fuente: MOSQUERA Jaime Alberto, RUIZ Julián Andrés

Se define que se podrá realizar los diferentes pentest en horario comercial, preferiblemente en el horario comprendido entre las 12:00 PM y las 2:00 PM los lunes, martes, miércoles y jueves, también se acuerda que el límite de tiempo para esta actividad será de la duración del proyecto aplicado que están realizando los Ingenieros Jaime Alberto Mosquera y Julian Andrés Ruiz, quienes son colaboradores del Departamento de sistemas.

Con la identificación de los activos que componen la infraestructura tecnológica de la planta ensambladora, se podrá dar paso a la búsqueda de información más detallada de cada uno de los activos identificados que permita conocer información como sistema operativo, IP, Marca, modelo, entre otros, información que resultará útil para la realización del pentest.

6.1.4 Agentes de amenaza

Según el estudio realizado a la infraestructura tecnológica de la compañía Suzuki Motor de Colombia S.A y tomando en cuenta la fase de modelado de amenazas de la metodología aplicada PTES y mediante un análisis del entorno competitivo del mercado en el que se encuentra, se pueden llegar a presentar amenazas tanto internas como externas debido a que Suzuki Motor como compañía tiene una presencia destacada a nivel nacional en el ámbito de fabricación y venta de motocicletas.

Es por eso, que se puede indicar que los agentes de amenaza a nivel interno pueden ser:

- Empleados: se pueden tomar como una amenaza a la seguridad de los activos de información por varias causas, como lo son:

    - Desconocimiento de manejo de tecnologías.
    - Espionaje, filtrado y venta de información.
    - Vandalización de Información importante.

- Administradores de Red y sistemas informáticos: estos agentes o actores pueden considerarse amenaza debido a un mal manejo y configuración de los sistemas informáticos de la compañía, permitiendo acceso a personas mal intencionadas.

- Programadores: Pueden ser considerados amenazas debido a mal uso de las herramientas con las que desarrollan aplicaciones o software, dejando puertas traseras para el ataque de hackers o ciberdelincuentes.

- Ingenieros y técnicos de soporte: Estos agentes se pueden tornar en una amenaza considerable, debido a malas prácticas en las instalaciones de software y la no actualización de sistemas operativos de equipos, dejando vulnerabilidades considerables y de fácil acceso a los hackers y ciberdelincuentes.

A nivel externo se pueden considerar varios agentes de amenaza para la compañía Suzuki Motor de Colombia S.A

- Competidores: se pueden considerar como una amenaza debido a que, pueden generar ataques con el fin de conocer información clasificada sobre planos y ensamble de motocicletas, robo de información financiera.

- Ciberdelincuencia: estos agentes se pueden tomar como una amenaza importante debido a la gran cantidad de personas y organizaciones delincuenciales cuyo objetivo es atacar cibernéticamente las organizaciones y lucrarse económicamente por medio de la penetración de los sistemas informáticos.

6.2 HERRAMIENTAS DE PENTESTING

Para las pruebas de tipo caja blanca que se realizaran para la identificación de vulnerabilidades en la red LAN de la planta ensambladora y almacén Pereira de Suzuki Motor de Colombia S.A, se ha decidido trabajar con 2 equipos de cómputo que tendrán a su vez dos máquinas virtuales con Sistema Operativo Kali Linux 2.1 y se utilizaran 3 herramientas de análisis de vulnerabilidades y de escaneo de puertos, estas herramientitas fueron seleccionadas mediante el documento de web denominado PTES Technical Guidelines, donde se muestran herramientas comerciales y de open source las cuales pueden ser utilizadas por decisión del auditor para realizar las pruebas de penetración, en este caso se seleccionan por experiencia de trabajo y conocimiento de uso, como lo son:

- Nessus
- Nexpose
- Nmap

6.2.1 Kali Linux 2.1

Actualmente se encuentra en su versión 2.1, es un sistema operativo GNU/Linux, su enfoque y uso principal es para realizar pentest o auditorias de infraestructuras tecnológicas, es un sistema operativo open source, se encuentra soportada por la organización Offensive Security.

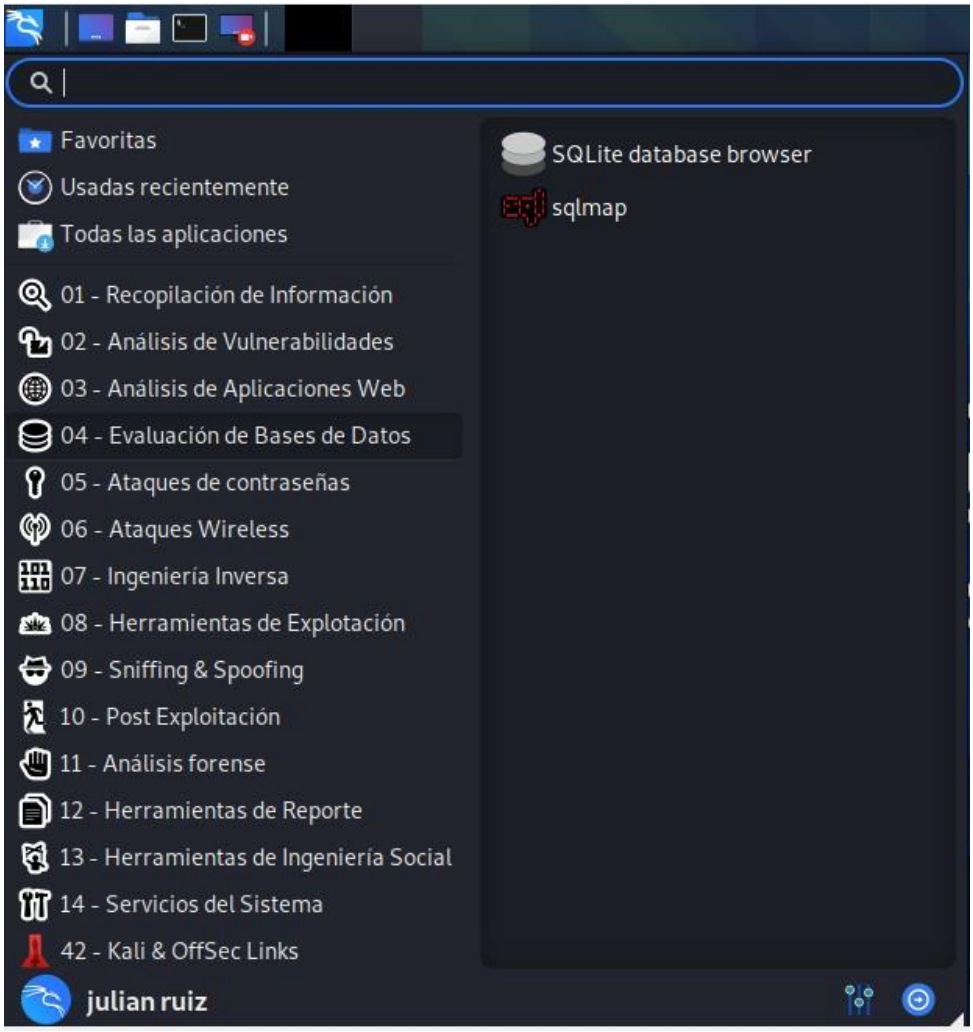
Basado en la distribución Debian, este sistema contiene más de 600 herramientas para realizar escaneos de vulnerabilidades.

algunas de las características de Kali Linux son:

- Árbol GIT Open Source
- Soporte a dispositivos inalámbricos
- Kernerl personalizados
- Paquetes y repositorio firmados con GPG
- Soporta múltiples lenguajes
- Personalizable

En la figura 3 se muestra el menú de aplicaciones Kali-Linux y los grupos de aplicaciones que contiene este sistema operativo.

Figura 3. Menú Principal Kali Linux



Fuente: MOSQUERA Jaime Alberto, RUIZ Julián Andrés

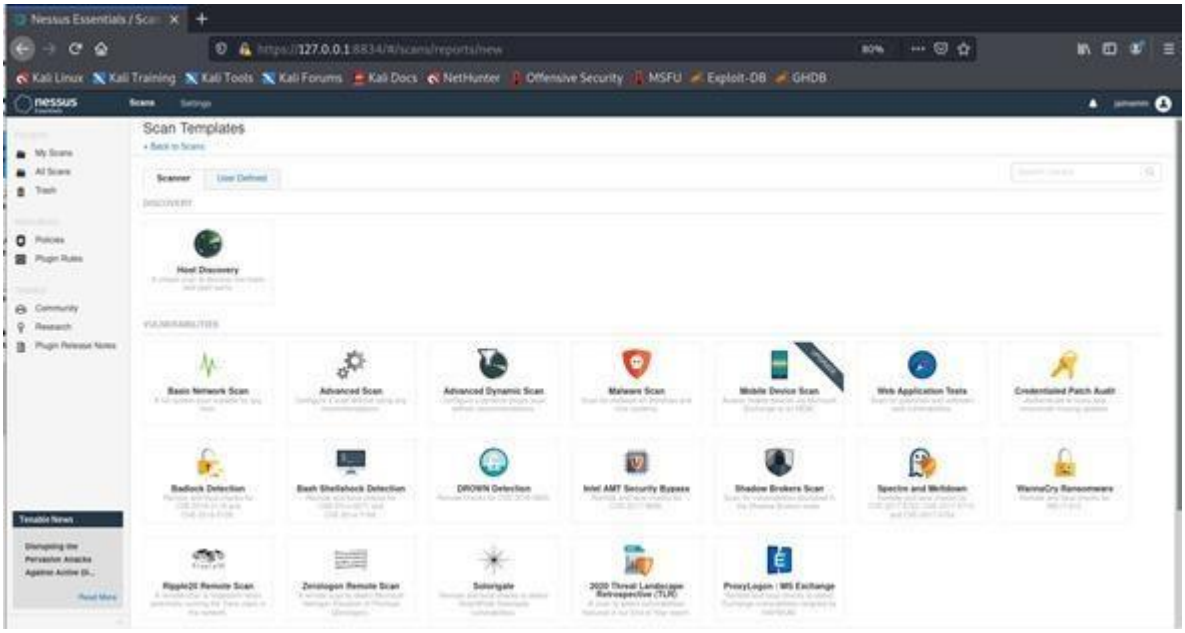
6.2.2 Nessus

Es una herramienta para la aplicación de análisis de seguridad automatizado-el cual realiza pruebas y descubrimiento de vulnerabilidades de seguridad conocidos, Nessus cuenta con una serie de características que brinda un aplicativo seguro, potente, actualizado y de fácil utilización para los profesionales de la seguridad de la información, está cuenta con licencia de pago para su versión Pro y también posee una versión Essentials para cual permite realizar escaneos en entornos hasta 16 IP sin ningún tipo de pago es un tipo de licencia temporal.

Nessus posee una serie de escaneos y complementos como se evidencia en la figura 4, que permiten realizar diferentes tipos de análisis dependiendo de la

infraestructura a auditar, permite realizar escaneos a diferentes sistemas operativos, bases de datos y entornos web, entre más complementos se utilicen más completo va a resultar el escaneo realizado por lo cual el tiempo del análisis va a ser mayor.

Figura 4. Entorno Nessus



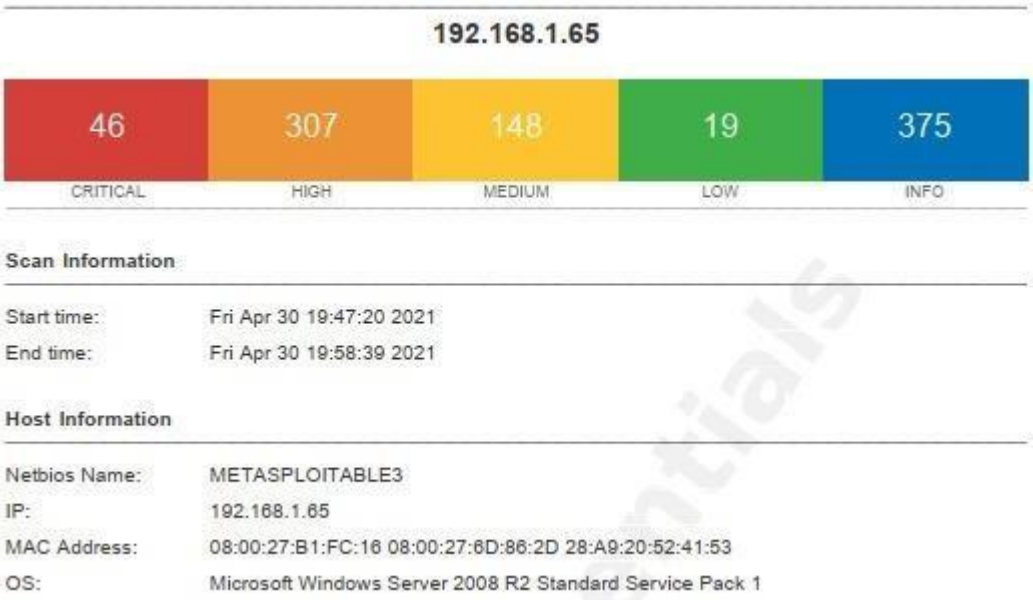
Fuente: MOSQUERA Jaime Alberto, RUIZ Julián Andrés

Una vez finalizado el escaneo Nessus generara un reporte con las diferentes vulnerabilidades identificadas del entorno auditado y estas vulnerabilidades serán catalogas en cinco (5) categorías:

- Critical
- High
- Medium
- Low
- Info

La figura 5, muestra la parte inicial del reporte generado por Nessus después del escaneo donde realiza la identificación del dispositivo auditado, su IP y la versión del sistema operativo, por lo general este tipo de reportes son muy extensos y se deben validar muy bien los resultados.

Figura 5. Reporte vulnerabilidades Nessus



Fuente: MOSQUERA Jaime Alberto, RUIZ Julián Andrés

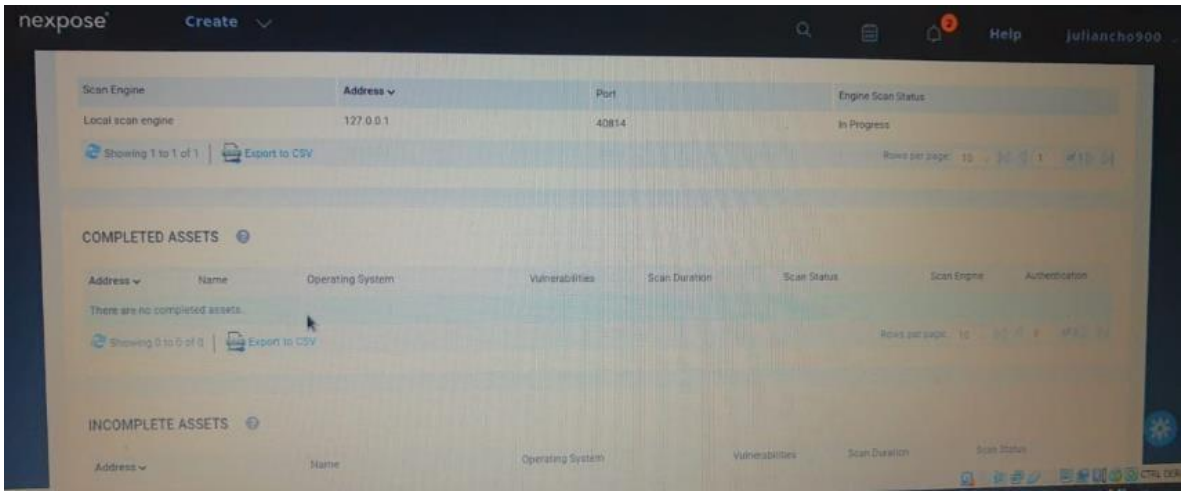
También los reportes generados por la herramienta indican la descripción completa de la vulnerabilidad, la solución que se debe aplicar para corregir la vulnerabilidad hallada y la identificación y valoración del CVSS para una búsqueda más profunda sobre la vulnerabilidad en bases de datos públicas.

6.2.3 Nexpose

Nexpose es una herramienta para la realización de pruebas de intrusión y testing, esta herramienta fue desarrollada por la compañía Rapid7, ella se puede integrar con el framework MetaSploit para convertirla en una herramienta que permita realizar análisis más robustos en busca de vulnerabilidades.

Nexpose permite realizar varios tipos de análisis y escaneos de vulnerabilidades, adicionalmente genera informes en tiempo real de los riesgos que se van presentando en la infraestructura tecnológica de la compañía, los análisis que se pueden realizar en diferentes formas y profundidades, con el fin de encontrar mayores vulnerabilidades.

Figura 6. Consola Nexpose



Fuente: Fuente: MOSQUERA Jaime Alberto, RUIZ Julián Andrés

Esta herramienta al finalizar el proceso de escaneo genera un informe sobre las vulnerabilidades halladas, nos entrega código Common Vulnerabilities and Exposures (CVE), para la consulta en bases de datos publicas donde podemos encontrar una posible solución o mitigaciones de la misma, en algunos casos el mismo informe entrega unos links para ejecutar la solución a la vulnerabilidad encontrada.

Los informes nos presentan la severidad de las vulnerabilidades y las agrupa gráficamente como se muestra en la figura 6. Severidad de la vulnerabilidad, estas vulnerabilidades se agrupan en tres (3) categorías:

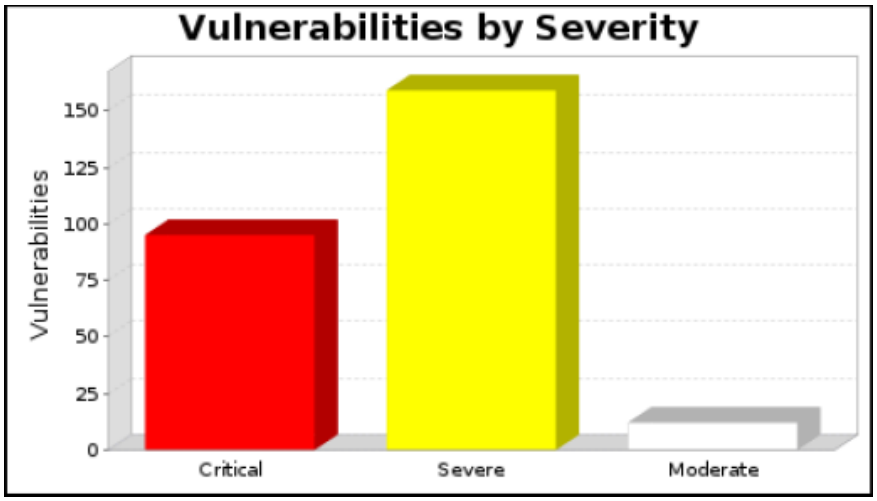
- Criticas
  Las vulnerabilidades críticas son aquellas que pueden poner el sistema en un riesgo alto y que pueden ser fácilmente explotadas por personas mal intencionadas, estas se deben corregir de forma inmediata para evitar que sean usadas para violentar los sistemas.

- Severas
  Este tipo de vulnerabilidades son menos críticas, de igual manera se deben de tratar, aunque estas no ponen el sistema en una situación de riesgo inmediato, si deben será tratadas de manera rápida y oportuna por que se pueden convertir en críticas, lo cual afectaría bastante la infraestructura tecnológica.

- Moderadas
  Son vulnerabilidades que se hallan durante el escaneo, las cuales no están exponiendo la infraestructura, se deben tratar, dado que en un futuro se

pueden convertir en vulnerabilidades criticas o severas, aunque estas dan un poco más tiempo para ser solucionadas.

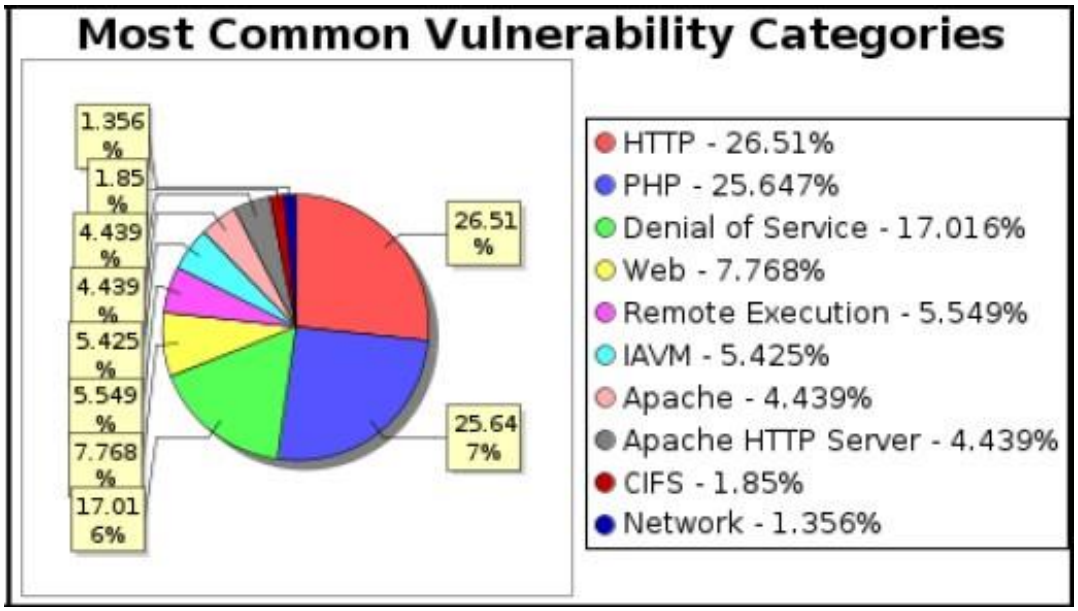
Figura 7. Severidad de las vulnerabilidades



Fuente: MOSQUERA Jaime Alberto, RUIZ Julián Andrés

De igual forma en el informe, se entrega un reporte detallado de las vulnerabilidades agrupadas por categorías, representadas en un gráfico circular, donde se indican en porcentajes esta información, como se muestra en la figura 7. Categorías De vulnerabilidades.

Figura 8. Categorías De vulnerabilidades



Fuente: MOSQUERA Jaime Alberto, RUIZ Julián Andrés

6.2.4 Nmap

Nmap (Network Mapper) es una herramienta de código abierto la cual permite realizar exploración de vulnerabilidades e identificación de redes en los host, esta herramienta es multiplataforma compatible con Windows, macOS y Linux, Nmap es utilizado para la identificación de dispositivos, que estén realizan uso de la red; Puede ser una red privada o una red pública, el objetivo es descubrir los host disponibles detectar que puertos se encuentran abiertos y que servicios se encuentran funcionando por dichos puertos, también permite conocer el sistema operativo utilizado por estos host.

Nmap permite realizar un mapeo de red con el cual se pueden identificar los diferentes dispositivos como servidores, router, computadores, teléfonos IP, switch que se encuentren conectados, también mediante escaneos a los dispositivos identificados se puede identificar la versión de sistema operativo con la que cuenta el dispositivo, adicionalmente Nmap identifica los puertos abiertos y establece los diferentes servicios que corren por estos puertos, esta información es muy valiosa para un atacante o auditor que está realizando un escaneo, Para esta herramienta se puede utilizar el entorno grafico Zenmap, el cual permite que se descarguen los informes, comparación entre los informes generados, al igual que permite ver las topologías de red.

6.3 PRUEBAS DE SEGURIDAD EN LA RED LAN

Basados en la fase cuatro (4) de la metodología PTES denominada análisis de vulnerabilidades, se procede a la realización y ejecución de las pruebas de seguridad tipo caja blanca, sobre los activos de información establecidos en la fase inicial “compromiso previo” con el personal del departamento de Sistemas de Suzuki Motor de Colombia de acuerdo al anexo A denominado Formato_Levantamiento_Requerimientos, con el objetivo de identificar las diferentes vulnerabilidades existentes en la red LAN de la compañía que puedan ser utilizadas por atacantes informáticos malintencionados para obtener información confidencial, privilegiada o acceso a los sistemas internos de la compañía sin autorización.

Para la realización de búsqueda de vulnerabilidades se utilizaron las herramientas de Nessus, Nexpose y Nmap sobre los activos de información tanto de la planta ensambladora como en el almacén Pereira.

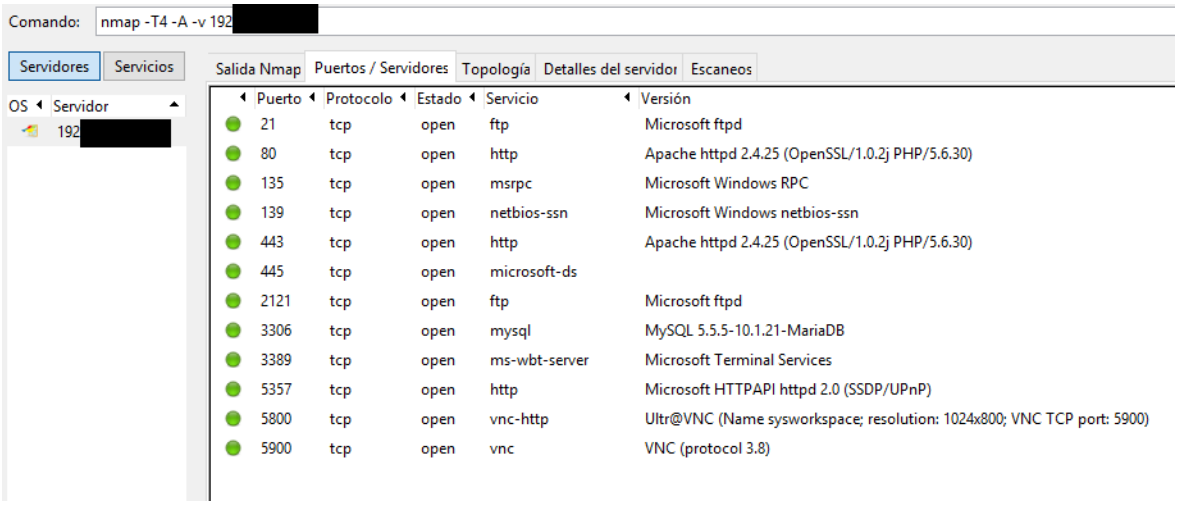
6.3.1 Escaneo de puertos con herramienta NMAP.

La primera herramienta por utilizar será Nmap con el fin de evidenciar que puertos se encuentran abiertos, el escaneo inicial se realiza sobre los 10 activos informáticos de la planta ensambladora, mostrando el estado de los puertos, servicios que se relacionan y se ejecutan sobre esos puertos, de igual forma las versiones de estos servicios.

Servidor 192.XXX.YYY.Z23

Se procede a realizar un procedimiento de escaneo con la herramienta Nmap sobre el servidor 192.XXX.YYY.Z23 donde se logra evidenciar diferentes cantidades de puertos en estado **Open** sobre los cuales se ejecutan diferentes servicios relacionados con las funciones que presta el servidor, en la figura 9 se visualiza la identificación de servicios como el Protocolo de Transferencia de Ficheros (FTP), MYSQL (Sistema de Gestión de Bases de Datos), Virtual Network Computing (VNC), entre otros.

Figura 9. Escaneo Nmap 192.XXX.YYY.Z23

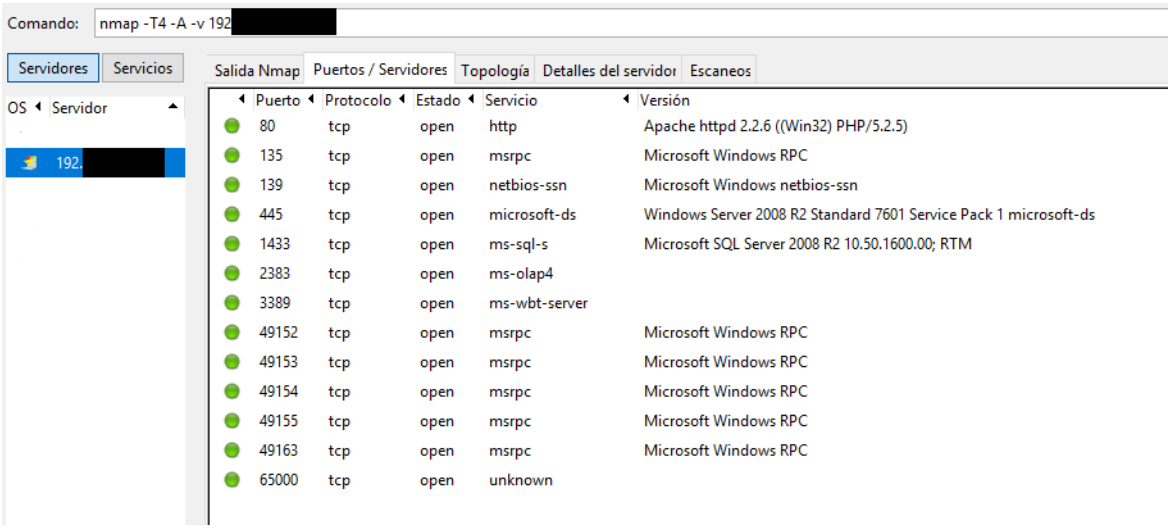


Fuente: Nmap

Servidor 192.XXX.YYY.Z49

Se realiza escaneo intensivo con la herramienta Nmap sobre el host con el objetivo de identificar los diferentes puertos que se encuentren en estado open y sus servicios que se ejecutan en ellos, se evidencia en la figura 10 que existe un total de trece (13) puertos en estado **open**, el puerto 80 está siendo utilizado por el software Apache 2.2.6, el puerto 135 se ejecuta el programador de tareas y MSDTC y sobre el puerto 1433 se está ejecutando el SQL Server 2008 R2.

Figura 10. Escaneo Nmap 192.XXX.YYY.Z49

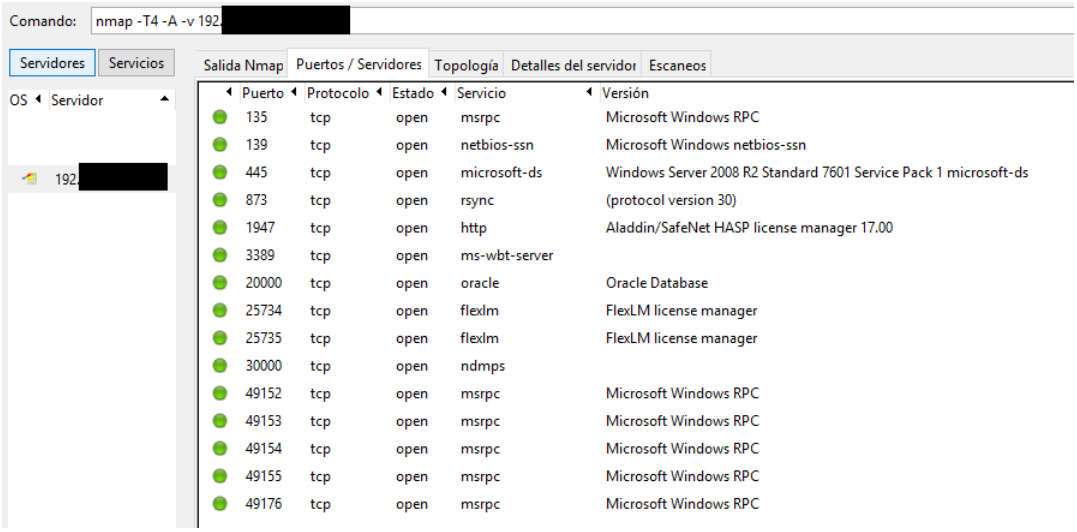


Fuente: Nmap

Servidor 192.XXX.YYY.Z19

Se procede con la ejecución del escaneo utilizando la herramienta Nmap sobre el host 192.XXX.YYY.Z19 con el objetivo de identificar los puertos en estado open y los diferentes servicios que se ejecutan en ellos. Sobre la figura 11 se evidencian quince (15) puertos con estado open en los cuales se ejecutan diferentes servicios, sobre el puerto 139 se ejecuta el protocolo netbios, el puerto 1947 se utiliza para el software SafeNet con el servicio Hasp, el puerto 20000 es utilizado por Oracle Database y los puertos 25734 y 25735 se utilizan servicios de FlexLM para la administración de licencias.

Figura 11. Escaneo Nmap 192.XXX.YYY.Z19

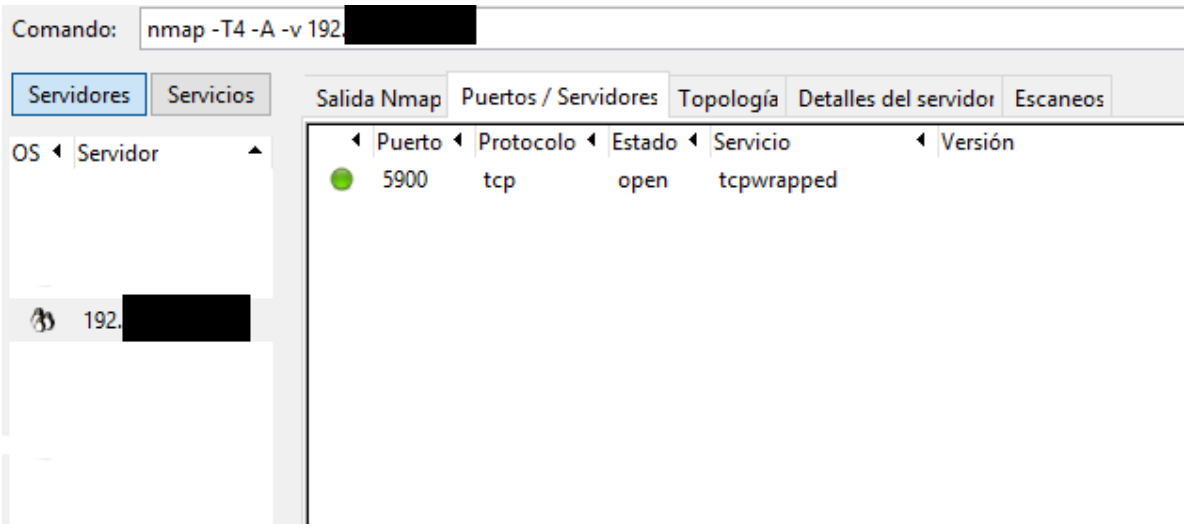


Fuente: Nmap

Servidor 192.XXX.YYY.Z48

Se procede con la realización del escaneo con la herramienta Nmap sobre el host, la configuración de seguridad del host dificulta la identificación de los puertos que se encuentran en estado open y los servicios que se ejecutan sobre ellos, en la figura 12 se evidencia únicamente el puerto 5900 el cual corresponde al servicio TCP Wrapped el cual se encarga de realizar filtros en el acceso a la red.

Figura 12. Escaneo Nmap 192.XXX.YYY.Z48

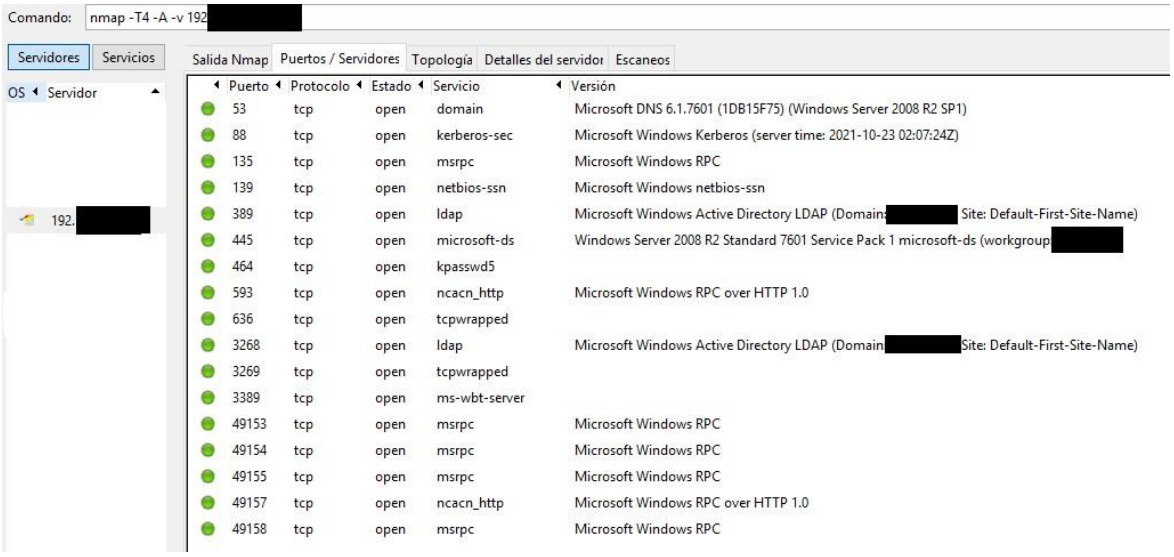


Fuente: Nmap.

Servidor 192.XXX.YYY.Z43

Se procede con la ejecución del escaneo intensivo con la herramienta Nmap sobre el host para lograr identificar los diferentes puertos que se encuentran en estado open y los servicios que se ejecutan en ellos, en la figura 13 se evidencia diecisiete (17) puertos en estado open, de los cuales se identifican servicios importantes como el puerto 53 ofrece el servicio Sistema de Nombres de Dominio (DNS), el puerto 389 y 3268 donde se identifica el servicio de active directorio y Protocolo Ligero de Acceso a Directorios (LDAP) y el puerto 88 donde se ejecuta el servicio de Kerberos.

Figura 13. Escaneo Nmap 192.XXX.YYY.Z43

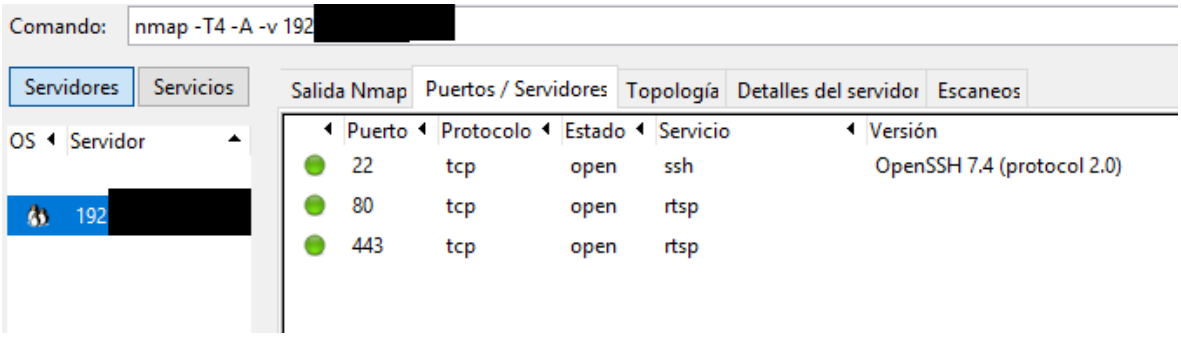


Fuente: Nmap

Servidor 192.XXX.YYY.Z44

Se procede con la ejecución del escaneo intensivo con la herramienta Nmap sobre el host para la identificación de los puertos y servicios en estado open, en la figura 14 se evidencian tres (3) puertos, el puerto 80 y 443 pertenecen a servicios web y el puerto 22 corresponde a servicio Secure Shell (ssh).

Figura 14. Escaneo Nmap 192.XXX.YYY.Z44

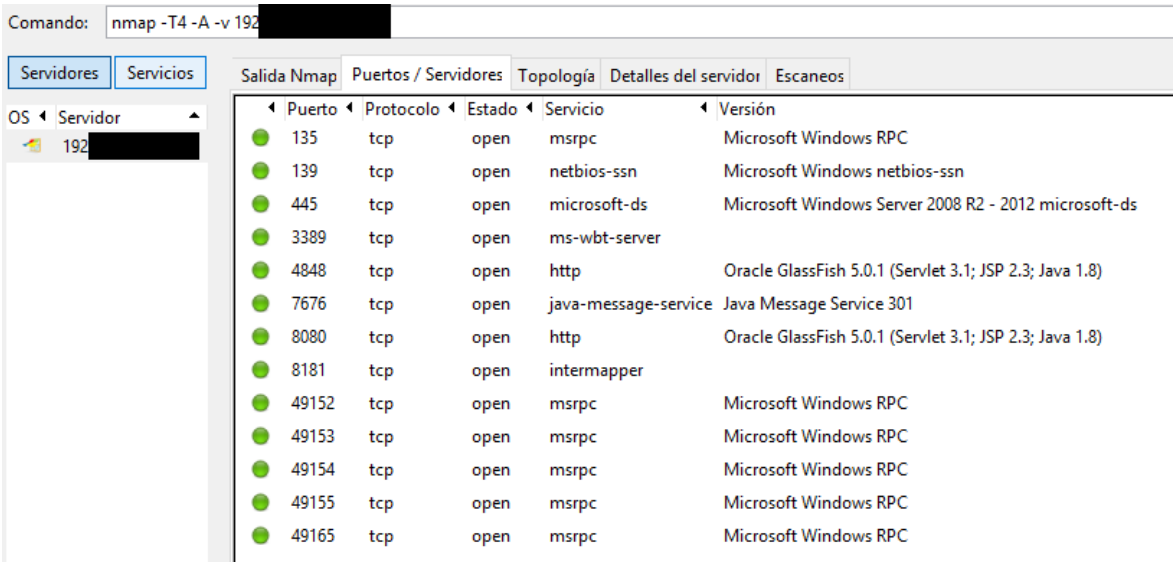


Fuente: Nmap

Servidor 192.XXX.YYY.Z51

Se realiza escaneo intensivo mediante la herramienta Nmap para lograr identificar los puertos y servicios en estado open del host, en la figura 15 se evidencia trece (13) puertos con estado open en los cuales se ejecutan diferentes procesos como en los puertos 4848 y 8080 donde se ejecutan los servicios de Oracle Glass Fish, el puerto 7676 se ejecuta servicio de Java y sobre el puerto 139 se ejecuta el NetBios.

Figura 15. Escaneo Nmap 192.XXX.YYY.Z51

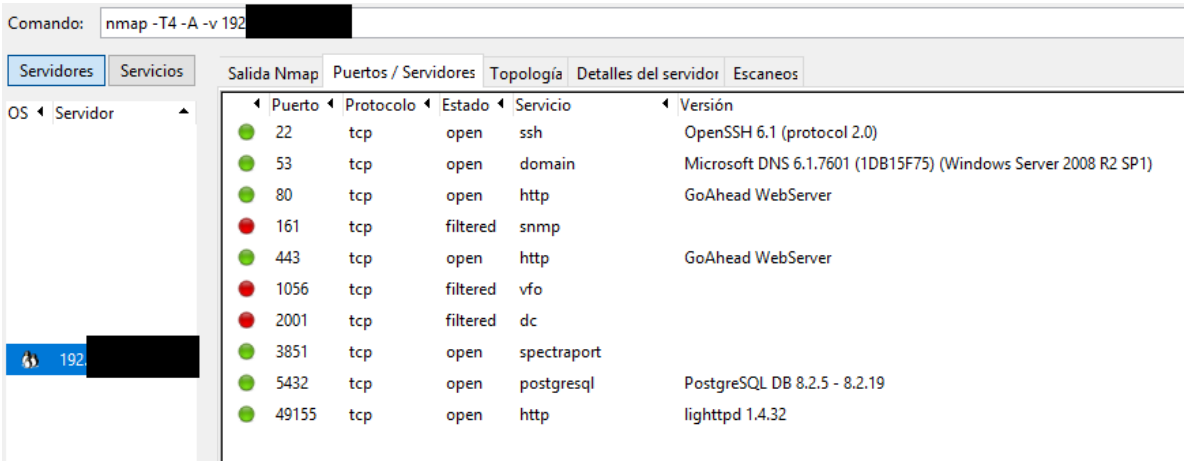


Fuente: Nmap

Servidor 192.XXX.YYY.Z21

Se ejecuta escaneo intensivo con la herramienta Nmap sobre el host con el objetivo de la identificación de los puertos en estado open y los servicios que se ejecutan en ella, en la figura 16 se identifican siete (7) puertos en estado open y tres (3) en estado close, de los puertos en estado open se identifica servicio en puerto 22 correspondiente a SSH, puerto 53 que corresponde a DNS y el puerto 5432 donde se ejecuta PostgreSQL.

Figura 16. Escaneo Nmap 192.XXX.YYY.Z21

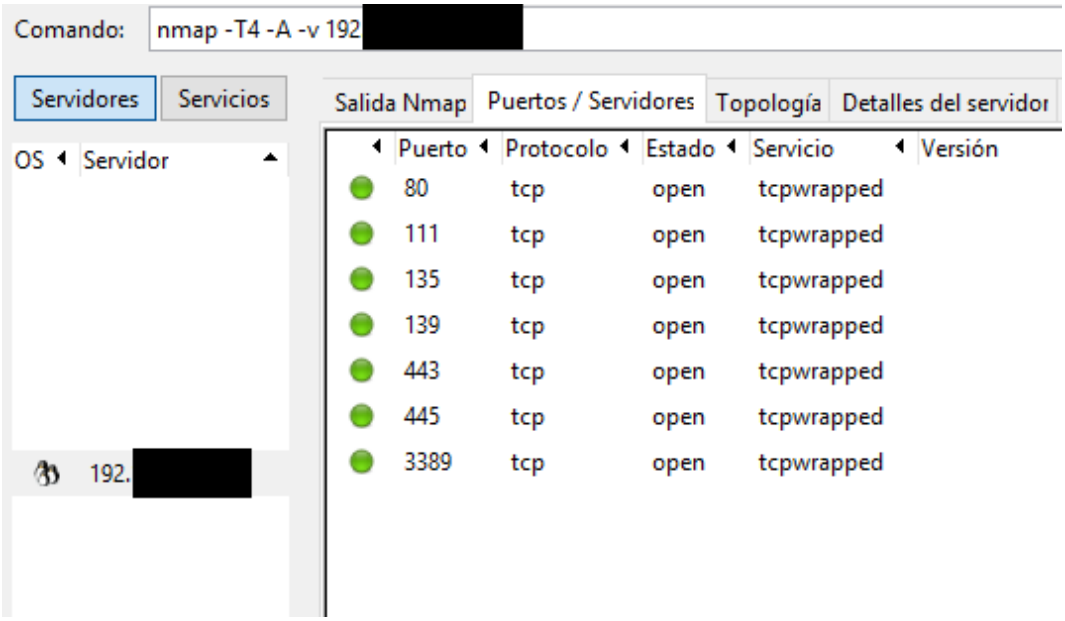


Fuente: Nmap

Servidor 192.XXX.YYY.Z46

Se procede con la ejecución del escaneo intensivo con la herramienta Nmap sobre el host para la identificación de los puertos en estado open y sus servicios relacionados, en la figura 17 se evidencia que existen siete (7) puertos abiertos pero debido a la configuración de seguridad no es posible la identificación de los servicios que se están ejecutando sobre dichos puertos.

Figura 17. Escaneo Nmap 192.XXX.YYY.Z46

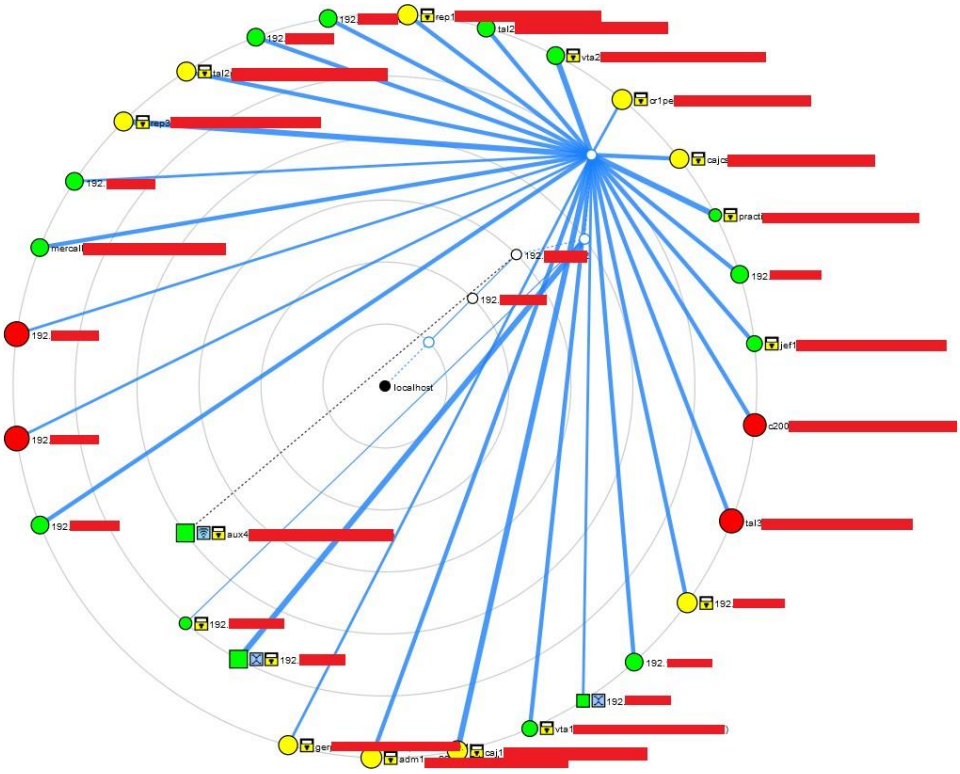


Fuente: Nmap

De igual manera se realiza la ejecución de la herramienta Nmap sobre la infraestructura tecnológica del almacén Pereira con el fin de identificar que puertos se encuentran abiertos en los activos de información del almacén, identificar los diferentes hosts que se encuentran conectados y servicios en estado open.

Una vez finalizada la revisión con la herramienta Nmap, nos permite visualizar mediante un diagrama generado los diferentes hosts a los cuales se le realizaron escaneos para la identificación de puertos y servicios que se encuentran en estado abiertos, en la figura 18 se evidencias dichos hosts conectados a la red del almacén de Pereira de Suzuki Motor de Colombia.

Figura 18. Topología de red escaneada almacén Pereira



Fuente: Nmap

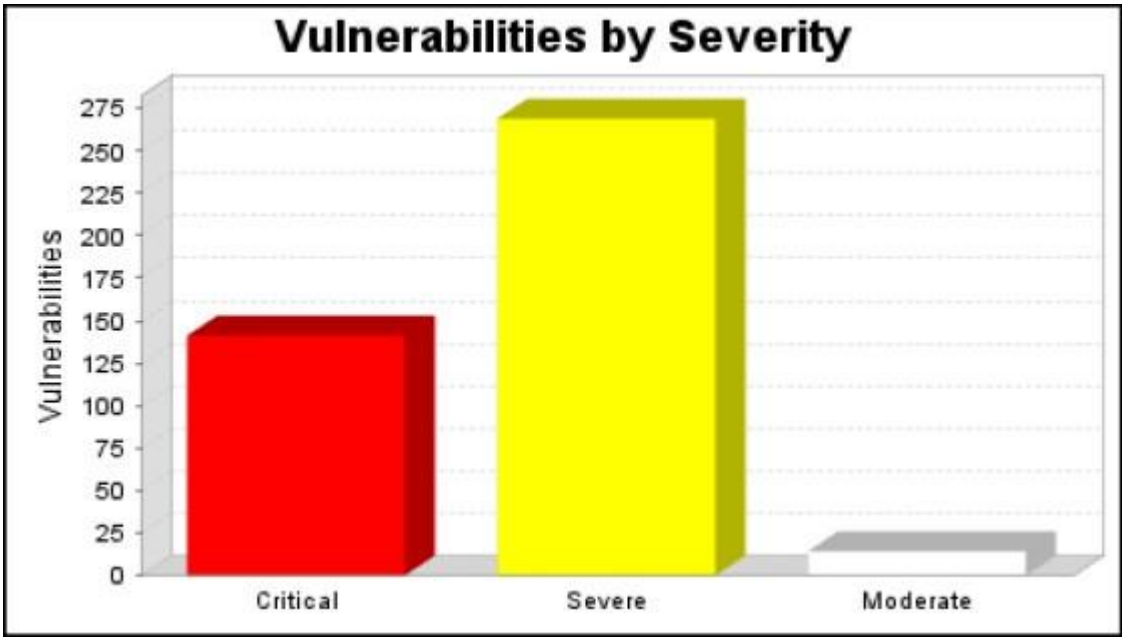
6.3.2 Auditoria de activos con la herramienta Nexpose.

Mediante el uso de la herramienta especializada en auditorias y pruebas de penetración Nexpose se realiza el escaneo de vulnerabilidades, con la opción Full Auditoria, la cual permite realizar un análisis profundo, permitiendo que en el análisis

realizado en dos (2) servidores de la planta ensamblado de Suzuki Motor de Colombia se puedan evidenciar algunas vulnerabilidades las cuales se debe revisar con detenimiento para dar solución o mitigar las vulnerabilidades halladas.

El primer análisis se realiza sobre el servidor con IP 192.XXX.YYY.Z49, donde se logra encontrar y evidenciar 424 vulnerabilidades totales las cuales pueden ser explotadas fácilmente por cualquier hacker o persona mal intencionada, 141 vulnerabilidades de estas son consideradas críticas estas son las que se requiere solucionar con mayor urgencia, 269 vulnerabilidades severas y 14 vulnerabilidades moderadas, como se evidencia en la Figura 19. Vulnerabilidades servidor 192.XXX.YYY.Z49

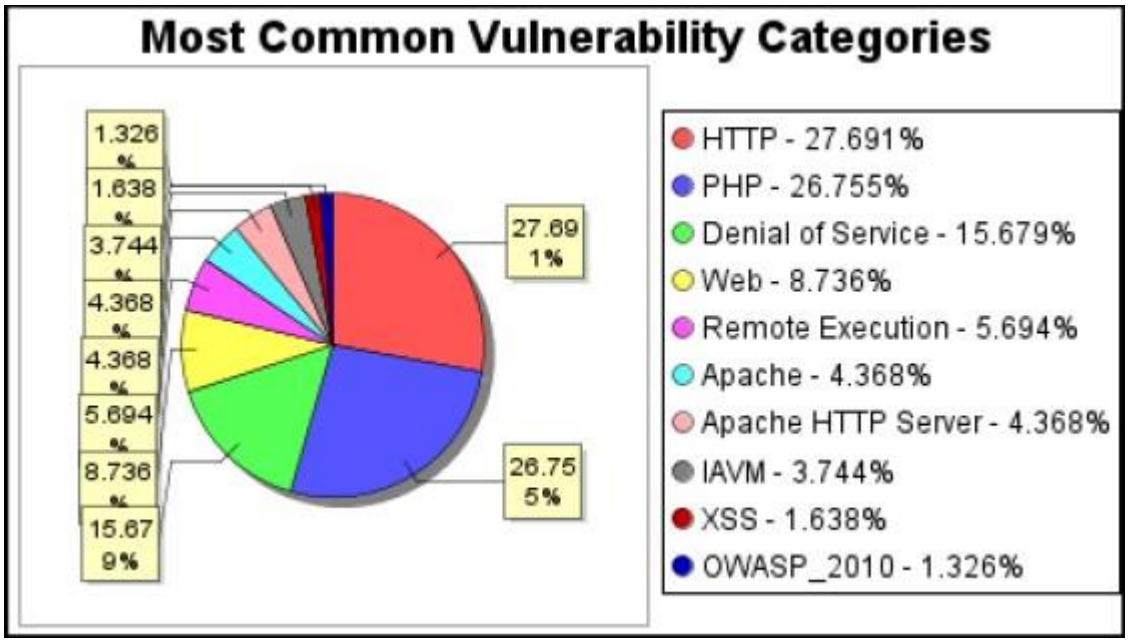
Figura 19. Vulnerabilidades servidor 192.XXX.YYY.Z49



Fuente: Nexpose

En este análisis también se evidencia los servicios que están más afectados y que cuentan con mayores vulnerabilidades, lo cual puede indicar con mayor facilidad las medidas correctivas a tomar, sobre estos servicios, permitiendo mejorar la seguridad, como se evidencia en la figura 20. Categorías de Vulnerabilidades más comunes.

Figura 20. Categorías de Vulnerabilidades más comunes.



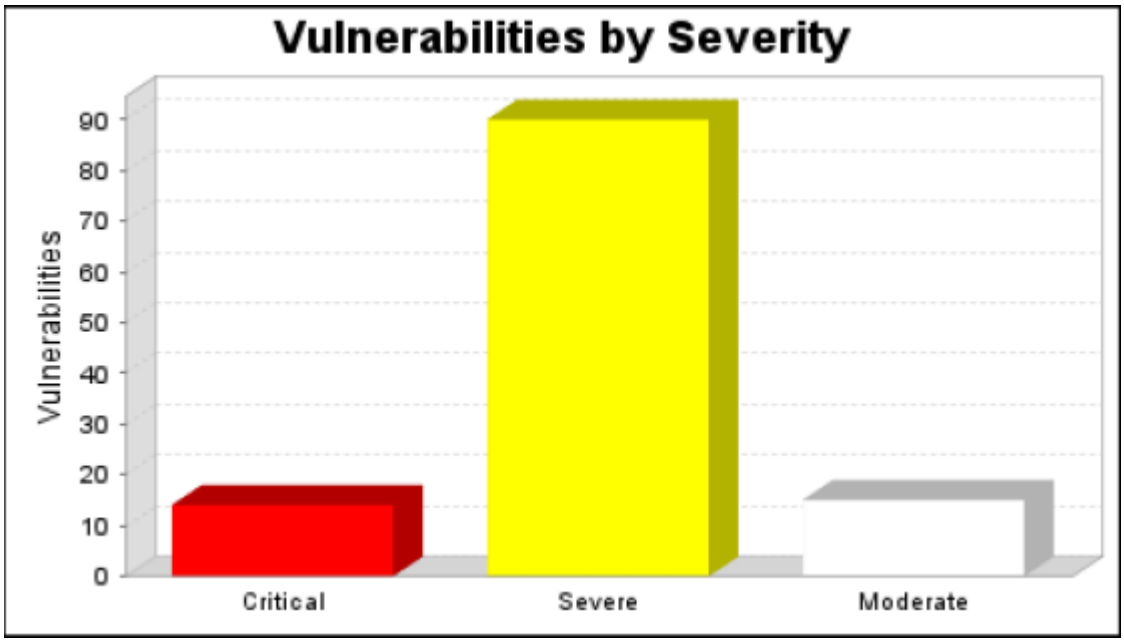
Fuente: Nexpose

Finalizado la auditoria sobre el servidor 192.XXX.YYY.Z49, se procede a realizar el análisis y auditoria de un segundo servidor con IP 192.XXX.YYY.Z23, de igual manera se realizar mediante la opción de Full auditoria, permitiendo esto un análisis y escaneo profundo de cada uno de los servicios que están instalados y se ejecutan sobre este.

En el análisis realizado se evidencian un total de 119 vulnerabilidades, entre las que se encuentran 14 vulnerabilidades críticas, las cuales se deben tratar de mitigar en la mayor brevedad posible, ya que estas pueden otorgar acceso fácilmente a personas mal intencionadas y estas tomar control de los sistemas informáticos de la compañía, 90 vulnerabilidades son consideradas críticas, también se debe realizar una revisión inmediata de estas vulnerabilidades, ya que pueden permitir exploits afectando el normal desarrollo de las actividades corporativas.

Finalmente se evidencian 15 vulnerabilidades moderadas, que deben ser revisadas, pero estas no representan un riesgo alto, debido a que no ponen en riesgo ni la infraestructura, ni la información ya que dichas vulnerabilidades no pueden ser explotadas por los atacantes, pero esto no significa que no se deba prestar atención, dado que con el paso del tiempo se pueden tornar en vulnerabilidades severas o críticas, todo esto se puede evidenciar en la figura 21. Vulnerabilidades Servidor 192.XXX.YYY.Z23.

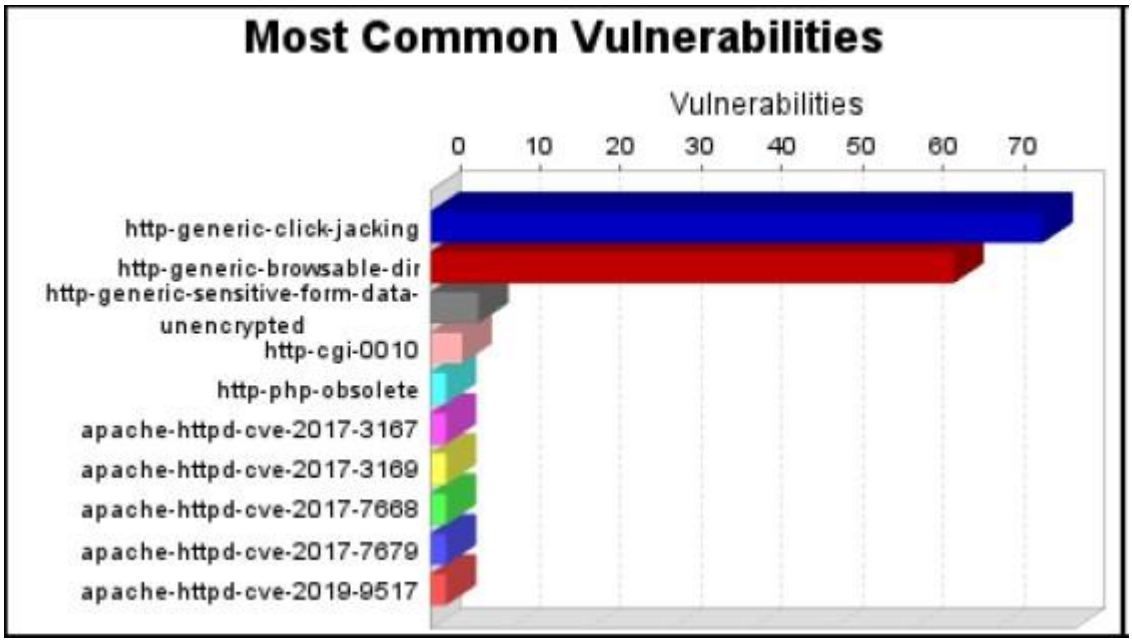
Figura 21. Vulnerabilidades Servidor 192.XXX.YYY.Z23



Fuente: Nexpose

En los informes obtenidos de la auditoría realizada sobre el servidor 192.XXX.YYY.Z23 podemos evidenciar las vulnerabilidades más comunes y detallar cuantas existen por cada las vulnerabilidades halladas, se puede evidenciar que se tiene mayor índice de vulnerabilidades sobre http-generic-click-jacking con un total de 76 apariciones, como se puede evidenciar en la Figura 22. Vulnerabilidades más comunes.

Figura 22. Vulnerabilidades más comunes

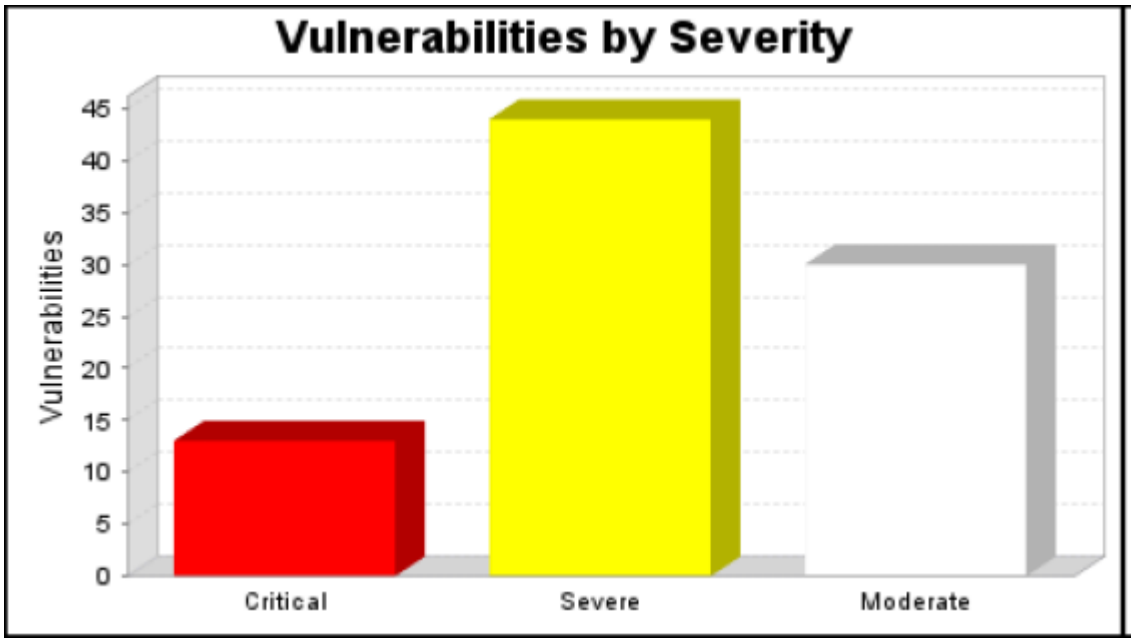


Fuente: Nexpose

Finalizado el proceso de escáner de los dos (2) servidores de planta ensambladora de Suzuki Motor de Colombia S.A, se procede a continuar la auditoria sobre la infraestructura tecnológica del almacén Pereira, con el fin de evidenciar que vulnerabilidades se hallan en esta sede y posterior a los hallazgos hacer una propuesta para mitigar y/o solucionar los problemas encontrados, permitiendo así una mejoría de seguridad en la infraestructura tecnológica de este almacén y de la misma forma poder replicar estas en otras sedes a nivel nacional.

El análisis inicial se realiza sobre 6 equipos de cómputo, lo cual permitió hallar mediante la opción denominada auditoria completa con el fin de realizar un análisis más profundo y detallado, con lo cual se logró evidenciar 87 vulnerabilidades, 13 de estas son vulnerabilidades críticas, que como se ha indicado anteriormente se deben de validar con prontitud ya que estas pueden ser explotadas muy fácilmente por cualquier atacante y conseguir acceder a la red corporativa y extraer información o apoderarse de los equipos, adicional se detectaron 44 vulnerabilidades severas las cuales se deben validar, estas son un poco menos graves puesto que no son de tan fácil explotación, pero se deben atender porque con el transcurso del tiempo se van a convertir en críticas y por ende se tendrían los sistemas en riesgo alto de ataque y finalmente se hallan 30 vulnerabilidades moderadas, las cuales no son tan urgentes pues no representan un riesgo significativo, lo cual no quiere decir que no se deben de validar, para su posterior mitigación, lo mencionado anteriormente se puede evidenciar en la figura 23. Vulnerabilidades Almacén Pereira.

Figura 23. Vulnerabilidades almacén Pereira

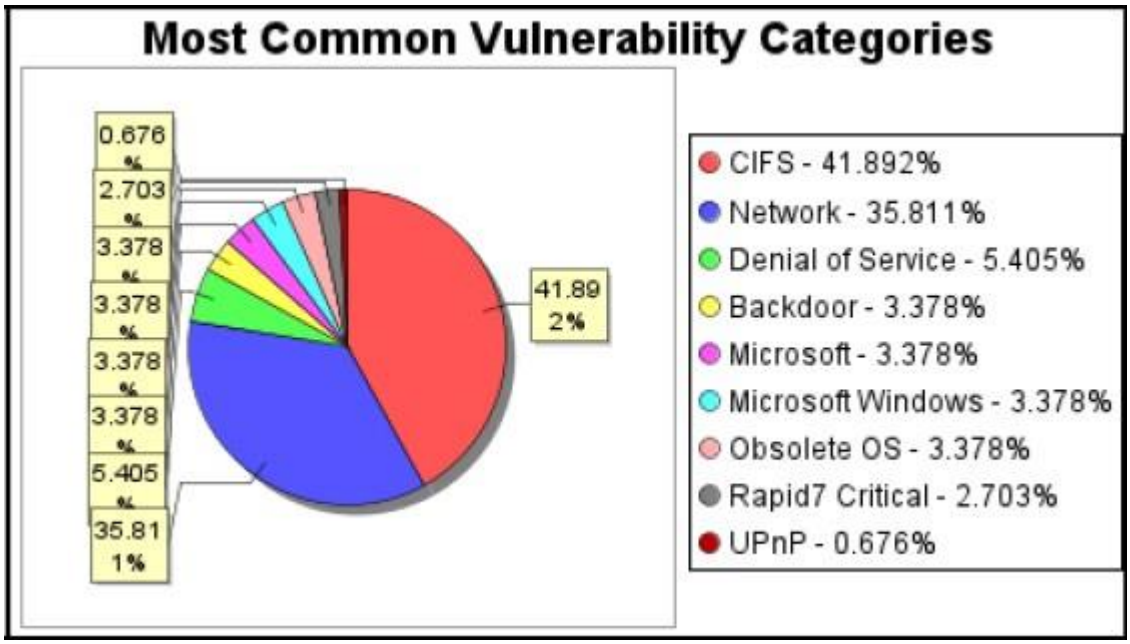


Fuente: Nexpose

Entre las categorías de vulnerabilidades detectadas por el análisis realizado con la herramienta Nexpose, se evidencia que el porcentaje más alto corresponde Common Internet File System (CIFS), que evidencia la situación de archivos que se encuentran compartidos sin ninguna protección, permitiendo que cualquier persona o ente malintencionado, secuestre información de los equipos, adicional a esto se logra detectar vulnerabilidades relacionadas con la red LAN y sistemas operativos obsoletos, lo cual indica que se presentan equipos sin actualizaciones, al igual que algunos software, esto permitiría la apertura de puertas trasera a atacantes, lo que se indica se puede evidenciar en la Figura 24. Categorías vulnerabilidades almacén Pereira.

Las vulnerabilidades encontradas en las pruebas realizadas es importante validarlas y en lo posible tratar de mitigarlas en el menor tiempo posible, debido a su gravedad pueden representar un riesgo no solo para el almacén, sino para la LAN extendida de Suzuki Motor de Colombia S.A

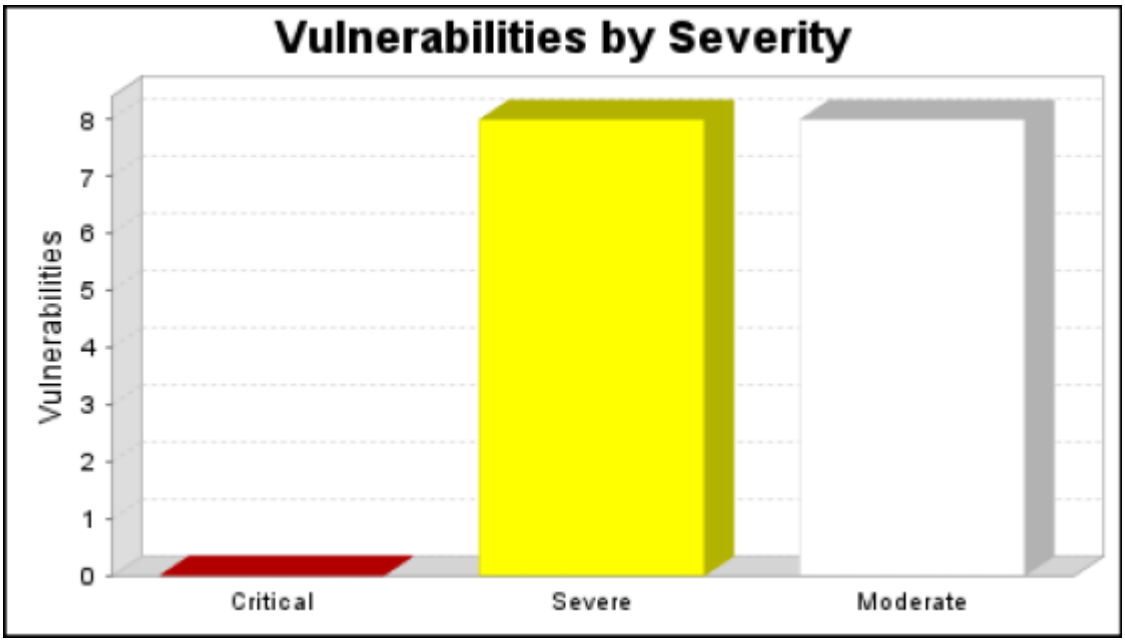
Figura 24. Categorías vulnerabilidades almacén Pereira



Fuente: Nexpose

Posterior a este análisis se realiza una auditoria sobre la telefonía IP del almacén Pereira donde se pueden evidenciar una serie de vulnerabilidades, que posiblemente afectaran el funcionamiento adecuado de las comunicaciones.
Se encuentran un total de 16 vulnerabilidades, 8 de estas consideradas severas y 8 más moderadas como se muestra en la Figura 25. Vulnerabilidades VoIP almacén Pereira.

Figura 25. Vulnerabilidades VoIP almacén Pereira

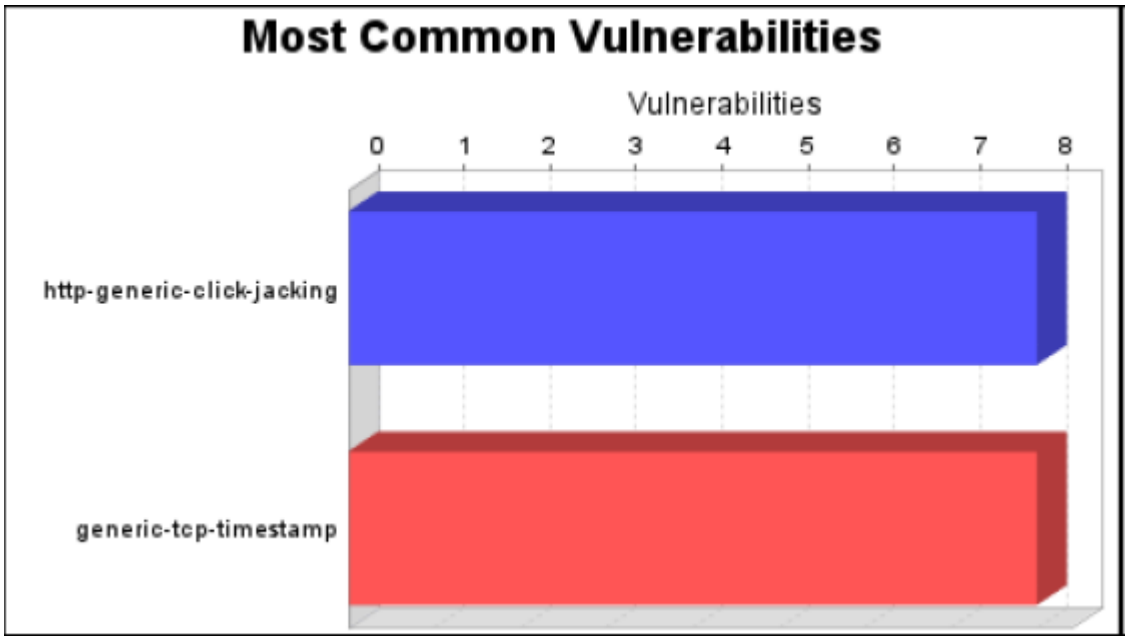


Fuente: Nexpose

Al realizar el análisis sobre los dispositivos se encuentra que todos tienen vulnerabilidades y que pueden otorgar información a atacantes, para su posterior explotación en otros sectores de la red.

Como información importante se evidencia que las vulnerabilidades más comunes están relacionadas con click-jacking y tcp-timestamp, vulnerabilidades que pueden permitir que se acceda a información mediante captura de datos de autenticación lo que puede ayudar a los atacantes a realizar actividades ilícitas por medio de esta información, como se evidencia en la figura 26. Vulnerabilidades más comunes VoIP

Figura 26. Vulnerabilidades más comunes VoIP



Fuente: Nexpose

6.3.3 Auditoria a activos con la herramienta Nessus en Planta ensambladora.

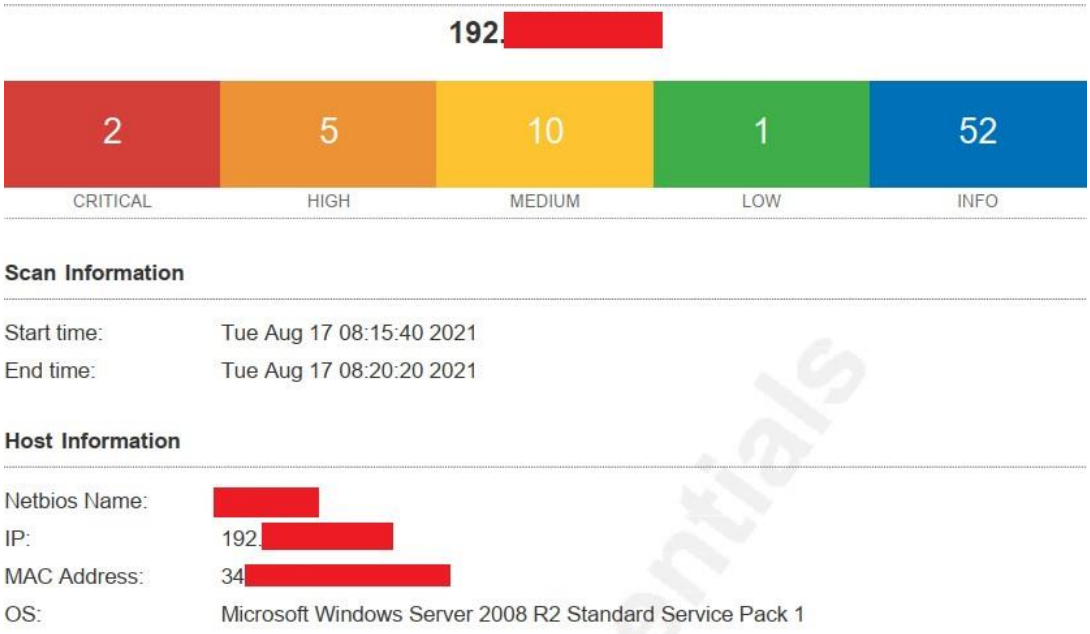
Para el análisis de vulnerabilidades de los diferentes activos de información de planta ensambladora de Suzuki Motor de Colombia se utiliza la herramienta Nessus la cual cuenta con el índice de falsos positivos más bajos de la industria de la seguridad informática, también cuenta con más de 45000 CVE lo que permite una correcta identificación de las vulnerabilidades.

Se presenta el resultado de los seis (6) escaneos realizados con la herramienta Nessus sobre los activos de información de planta dentro de la red interna de la organización, se evidencian vulnerabilidades en los hosts auditados.

Servidor 192.XXX.YYY.Z19

Se configura la herramienta de Nessus para realizar un proceso de escaneo sin afectación o caída del servicio del host auditado, una vez finalizados el escaneo los resultados son 18 vulnerabilidades totales las cuales se dividen en dos (2) criticas, cinco (5) altas, diez (10) medias y una (1) baja, también se identifican 52 vulnerabilidades informativas sobre estas vulnerabilidades informativas no es necesario realizar ninguna gestión, en la figura 27 se evidencia las vulnerabilidades halladas.

Figura 27. Escaneo Nessus 192.XXX.YYY.Z19

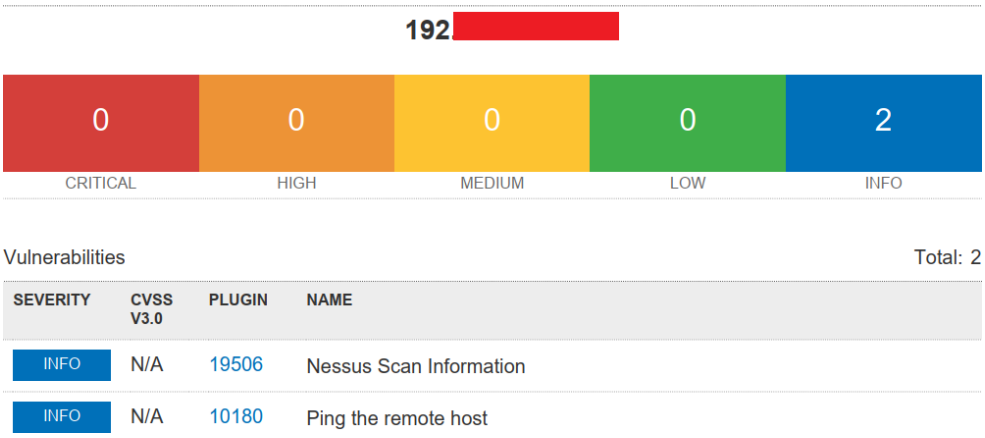


Fuente: Nessus

Servidor 192.XXX.YYY.Z48

Se realiza la configuración sobre la herramienta Nessus para la identificación de las vulnerabilidades del host, debido a la configuración de seguridad con la que cuenta dicho host este no permite la realización del análisis de las vulnerabilidades ya que es bloqueado por el antivirus instalado en el dispositivo, en la figura 28 se evidencia que no se identifican vulnerabilidades.

Figura 28. Escaneo Nessus 192.XXX.YYY.Z48

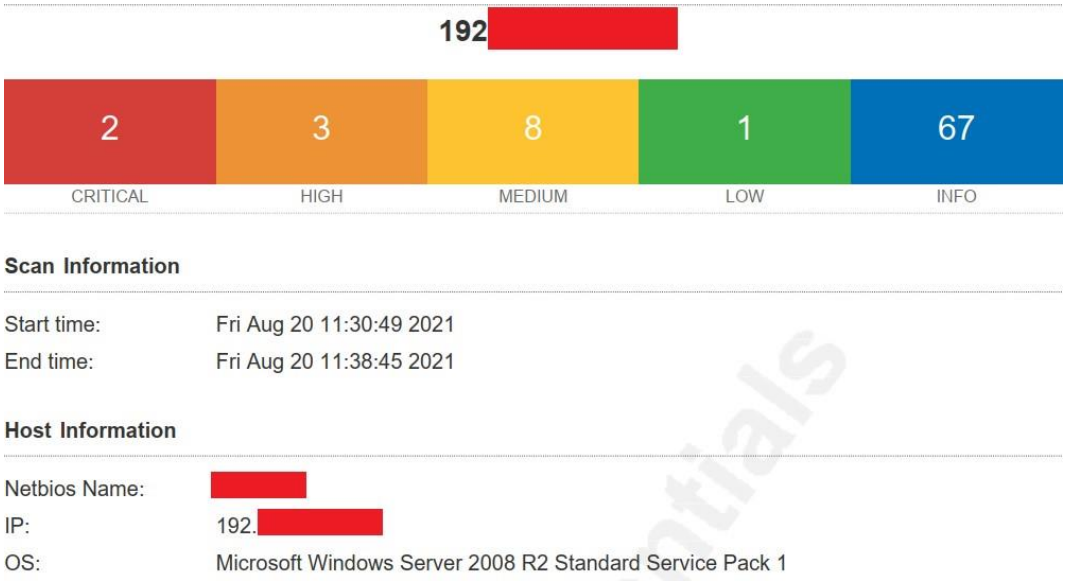


Fuente: Nessus

Servidor 192.XXX.YYY.Z43

Se procede a la configuración del escaneo profundo mediante la herramienta Nessus para la identificación de las vulnerabilidades existentes en el host a auditar, en la figura 29 se evidencia el hallazgo de 14 vulnerabilidades en total de las cuales dos (2) son críticas, tres (3) son altas, ocho (8) son medias y una (1) baja, todas estas vulnerabilidades requieren atención con el objetivo se eliminarlas o mitigar su impacto en el dispositivo.

Figura 29. Escaneo Nessus 192.XXX.YYY.Z43

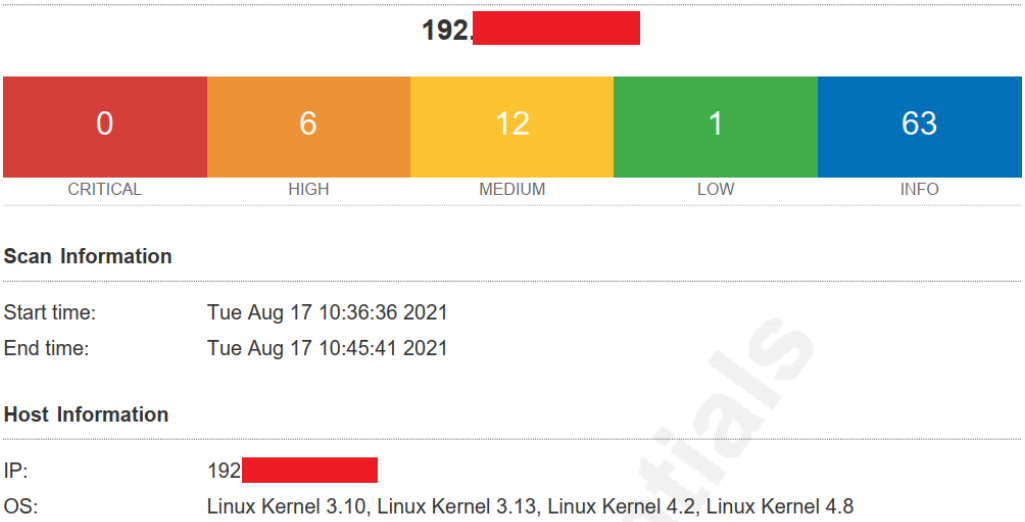


Fuente: Nessus

Servidor 192.XXX.YYY.Z44

Se lleva a cabo la configuración del escaneo para identificar las vulnerabilidades del host, en la figura 30 se evidencia los resultados del escaneo donde se identifican 19 vulnerabilidades las cuales se deben gestionar para mitigarlas o eliminarlas y evitar posibles explotaciones sobre estas, también se identifican 63 vulnerabilidades de tipo informativo sobre las cuales no es necesario la realización de alguna acción.

Figura 30. Escaneo Nessus 192.XXX.YYY.Z44

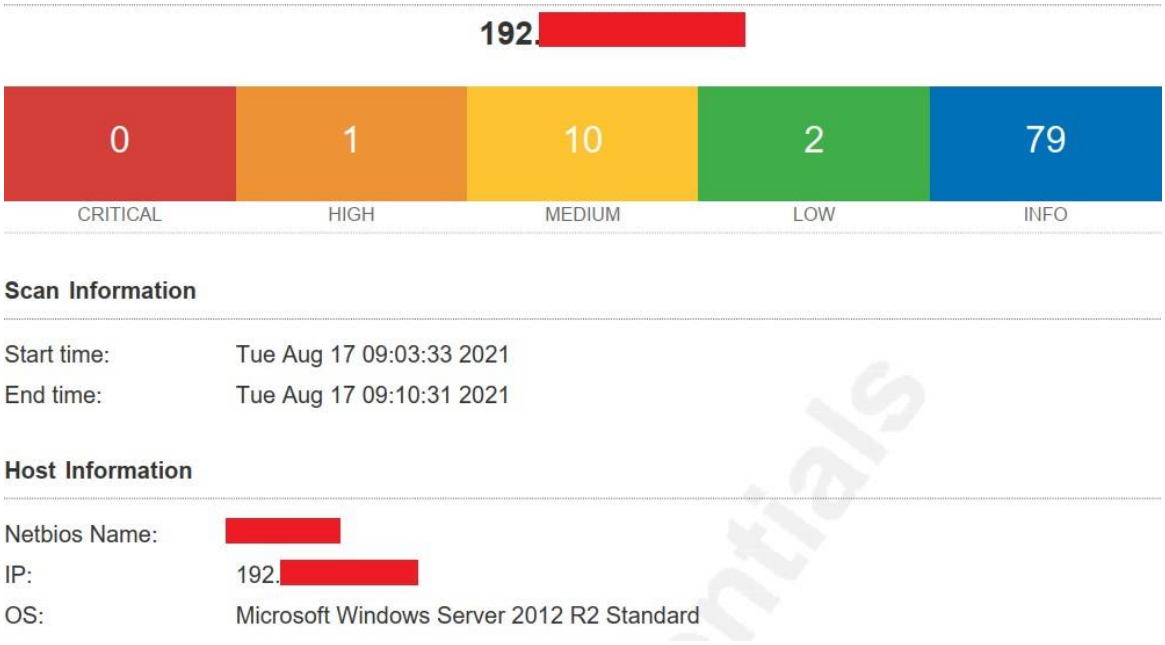


Fuente: Nessus

Servidor 192.XXX.YYY.Z51

Se realiza la configuración del tipo de escaneo a realizar sobre el host para la identificación de las vulnerabilidades con las que cuenta el servidor, sobre la figura 31 se identifican 14 vulnerabilidades las cuales deben ser gestionadas con el objetivo de mitigar o eliminar la vulnerabilidad para evitar que sean explotadas por atacantes ya sean internos o externos y puedan colocar en riesgo la información o servicios.

Figura 31. Escaneo 192.XXX.YYY.Z51

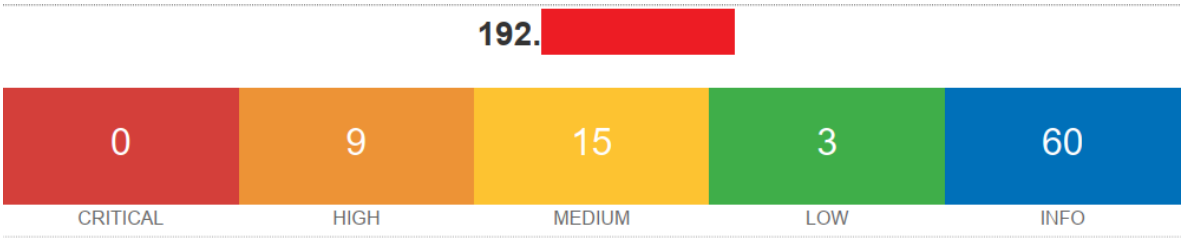


Fuente: Nessus

Servidor 192.XXX.YYY.Z21

Se realiza la configuración del escaneo de vulnerabilidades sobre la herramienta de Nessus con el objetivo de auditar el host y lograr identificar las vulnerabilidades que contiene, en la figura 32 se identifican 27 vulnerabilidades en total las cuales se dividen en nueve (9) vulnerabilidades altas, quince (15) vulnerabilidades medias y tres (3) vulnerabilidades bajas, estas vulnerabilidades se dejen mitigar o eliminar para evitar que sean aprovechas por atacantes y puedan generar afectaciones a la información o servicios que presta el host.

Figura 32. Escaneo Nessus 192.XXX.YYY.Z21



Scan Information

Start time:	Sun Oct 24 09:21:00 2021
End time:	Sun Oct 24 09:26:22 2021

Host Information

IP:	192.
OS:	Linux Kernel 2.6

Fuente: Nessus

6.4 RECOMENDACIONES A PARTIR DE LOS RESULTADOS OBTENIDOS EN EL PENTEST

La compañía Suzuki Motor de Colombia S.A. debe validar las diferentes vulnerabilidades halladas y presentadas en el informe técnico sobre los activos de información revisados con el objetivo de corregir o eliminar dichas vulnerabilidades las cuales pueden ser explotadas por personas malintencionadas afectando el funcionamiento y generando un riesgo para la organización y su información.

Se debe establecer un procedimiento o control para la realización de actualizaciones sobre los diferentes sistemas operativos y software que utiliza la organización con el objetivo de contar siempre con sistemas operativos y software actualizados para evitar posibles vulnerabilidades que puedan afectar el dispositivo o la información almacenada en él.

En la configuración de los servidores se debe emplear técnicas de hardening como el fortalecimiento del firewall, los accesos remotos sean seguros, bloquear puertos de red que no sea necesarios o que no se estén utilizando. Estas técnicas se realizan con el objetivo de robustecer la seguridad del dispositivo y los diferentes procesos realizados en dicho servidor.

Se debe realizar actualización en los sistemas operativos de los equipos de cómputo que se encuentran en las instalaciones del almacén Pereira, puesto que se evidencia sistemas operativos obsoletos, los cuales actualmente no cuentan con soporte por parte del fabricante.

Adicional a esta situación se presenta que los sistemas operativos que, si tienen soporte, no cuentan con parches de seguridad actuales, abriendo esto una puerta de ingreso a posibles vulnerabilidades y afectaciones tanto a la red del almacén y de la planta ensambladora de la compañía Suzuki Motor de Colombia S.A.

Restringir el uso de aplicativos de control remoto como VNC, debido a que se cuenta con una versión obsoleta, que puede generar inconvenientes de accesos no autorizados a los equipos y otorgar control un total del activo de información, existen herramientas con mayor grado de protección como ISL Light para realizar conexiones remotas en caso de que sea necesario brindar soporte remoto.

Se debe realizar verificación sobre documentos o archivos compartidos en la infraestructura del almacén Pereira, debido a que estos archivos no se encuentran protegidos por contraseñas y permite el acceso a cualquier tipo de usuario y/o invitado que esté conectado a esta red, permitiendo el control total de estos archivos.

Realizar la inactivación del servicio UPnP-HTTPU en los activos de información del almacén Pereira, debido a que este servicio está expuesto y puede generar

respuestas a solicitudes realizadas 30 veces mayores, generando alto flujo en la red, lo cual conllevaría a denegación de servicios.

Se debe realizar la validación de logueo en los equipos de VoIP debido a que estos presentan una vulnerabilidad asociada al usuario y contraseña, poco seguras, adicional a esto se evidencia la falta de actualización de los sistemas operativos de los teléfonos del almacén Pereira de la compañía Suzuki Motor de Colombia S.A.

Realizar la activación del protocolo de red SMB o activarlo en los equipos, para que el acceso a los recursos compartidos creados entre equipos solicite conexión mediante contraseña, debido a que cualquier intruso que pueda acceder a la red corporativa tendría acceso a dichos documentos, permitiendo el robo de información.

Se debe realizar validaciones y revisiones sobre los puertos que se tienen activos debido a que se logra evidenciar que varios de estos puertos contienen vulnerabilidades, ya que presentan configuraciones erróneas o falta de técnicas endurecimiento, adicional sobre estos puertos se ejecutan aplicaciones desactualizadas u obsoletas y pueden permitir la extracción de información a personas malintencionadas y con fines delictivos.

Se debe realizar validaciones sobre los servicios que están instalados en algunos servidores, pues se cuentan con versiones obsoletas de software, que permiten la fácil explotación de vulnerabilidades, la extracción de información o apoderamiento de los servicios de la infraestructura tecnológica de la empresa Suzuki Motor de Colombia S.A, lo cual puede generar pérdidas económicas y afectación de sus servicios a nivel nacional.

Realizar revisión de los certificados de seguridad SSL correspondientes a los servidores con sistema operativo Windows y Linux, debido a que se encuentran certificados inválidos y expirados lo cual genera vulnerabilidades que pueden ser aprovechadas por los atacantes con el objetivo de robo de información.

7 CONCLUSIONES

A partir de la finalización del proyecto aplicado sobre la compañía Suzuki Motor de Colombia S.A, partiendo del desarrollo de los objetivos específicos planteados y logrando desarrollar el objetivo general del presente proyecto, se pueden establecer una serie de recomendaciones, las cuales pueden ser de gran utilidad para mejorar la seguridad de la infraestructura tecnológica de la compañía, donde podemos concluir que:

Los análisis de infraestructura tecnológicas, en este caso la de la compañía Suzuki Motor de Colombia S.A mediante pentest, son totalmente necesarias pues estas auditorias, permiten conocer el grado de vulnerabilidad y de seguridad en el que se encuentra una organización, permitiendo que se pueda mejorar considerablemente la protección de cada uno de sus activos y por supuesto dando un alto índice de protección sobre su información.

Existen muchos tipos de herramientas para la realización de auditorías o pentest sobre las diferentes infraestructuras tecnológicas, la elección de una herramienta se debe basar sobre el conocimiento de uso de la herramienta y de igual manera se debe buscar que supla las necesidades presentadas en el pentest o auditoria que se pretende realizar., puesto que cada una de estas herramientas tiene un enfoque o especialidad y no todas sirven para lo mismo.

La seguridad informática es un factor sumamente importante para la empresa Suzuki Motor de Colombia S.A., por lo cual se debe contar con estrategias y metodologías para el manejo de la seguridad de la información las cuales brinden protección a los activos de información de la organización de posibles pérdidas de información o de ataques informáticos.

Las herramientas de escaneo de pentesting o de auditorías de seguridad, son un factor fundamental en el desarrollo e identificación de las vulnerabilidades de los activos de información de Suzuki Motor de Colombia S.A., ya que por medio de dichas herramientas se identifican las vulnerabilidades con las que cuentan los diferentes activos de información con el objetivo de mitigar o eliminar estas brechas de seguridad.

8 RECOMENDACIONES

Finalizado el desarrollo del proyecto aplicado en la compañía Suzuki Motor de Colombia S.A. se establecen una serie de recomendaciones basadas en los resultados obtenidos de la ejecución del pentest sobre la infraestructura tecnológica de la compañía.

Una vez realizado el análisis a la infraestructura tecnológica de la compañía Suzuki Motor de Colombia S.A. en planta ensambladora y almacén Pereira, se identifican diferentes tipos de vulnerabilidades que afectan los activos de información de la compañía debió a que actualmente cuentan con sistemas obsoletos y aplicaciones no actualizadas, por lo cual se recomienda al departamento de Sistemas de Suzuki realizar las siguientes recomendaciones para mejorar la seguridad de la infraestructura tecnológica de la compañía y mitigar las vulnerabilidades.

- Establecer un servidor de actualizaciones que permita actualizar de manera masiva los diferentes sistemas operativos y software utilizados por la compañía para el desarrollo de sus actividades.

- Establecer configuraciones de seguridad por medio del antivirus empleado por la compañía, para no permitir que los activos de información puedan ser escaneados con herramientas como Nmap, Nessus, Nexpose entre otras que permitan a un atacante conocer la información y vulnerabilidades del activo de información.

- Implementar algún estándar o norma enfocado a la seguridad de la información que ayude al departamento de TI a generar mejores prácticas, lo cual permite estandarizar múltiples procesos permitiendo a su vez el mejoramiento de la seguridad informática y funcionamiento de TI en Suzuki Motor de Colombia S.A

- Realizar la actualización o migración de los diferentes servidores que cuentan con sistema operativo Windows Server 2008 R2 Standard ya que es un sistema operativo obsoleto y no recibe actualizaciones de seguridad por parte del fabricante lo cual lo convierte en una vulnerabilidad critica.

- Establecer configuraciones de seguridad en los servidores con sistema operativo Windows y Linux para que no sea accesibles desde cualquier IP interna por medio del Remote Desktop Protocol (RDP).

- Implementar servicio de auditorías de logs para los diferentes servidores con los que cuenta la compañía, con el objetivo de identificar y monitorear en tiempo real los cambios o alertas que se puedan generar por parte de los

usuarios o los administradores del sistema, centralizando de manera adecuada dicha información para ser consultada de manera ágil.

- Realizar la utilización de técnicas de hardening en los diferentes activos de información de la compañía para contar con dispositivos más seguros y de difícil acceso para los atacantes, es por eso, por lo que se recomienda inhabilitar protocolo de conexiones remotas a los equipos, mejorar la seguridad de los archivos compartidos por medio de un servicio de file server, lo cual permite establecer accesos por medio usuarios y contraseñas seguras.

- Se recomienda la restricción de acceso a usuarios a configuraciones generales de los equipos de cómputo del almacén Pereira.
  Generar copias de seguridad de la información de los equipos y para equipos de alto valor informativo generar copias completas tanto en Sistema Operativo como información en general.

- Realizar el cifrado de discos en equipos portátiles, debido a que estos equipos son frecuentemente extraviados y algunos casos hurtados, al contar con el cifrado de discos la confidencialidad de la información de la compañía no se verá afectada.

- Realizar pruebas de penetración o auditorías a la infraestructura tecnológica de la compañía de manera frecuente para identificar posibles vulnerabilidades existente que puedan afectar la seguridad y la información de la compañía.

Para un buen desarrollo de pruebas de pentesting tanto en la infraestructura tecnológica de Suzuki Motor de Colombia S.A, como en las infraestructuras tecnológicas de cualquier organización deben estar acompañadas de una buena selección de herramientas para la identificación de las diferentes vulnerabilidades, esto apoyado en la metodología que se base para la realización de estas; Ya que las diferentes metodologías indican o proponen que herramientas usar, basadas en el objetivo a auditar, el tipo de sistema operativo y el alcance del pentest, no obstante y teniendo en cuenta que un factor importante para el uso de las herramientas de pentesting, es tener algún conocimiento previo ya que esto permite sacar el mayor provecho y obtener mejores resultados.

Es importante contar con buena documentación de las herramientas que se van a utilizar y a su vez que herramientas complementan a otras, logrando desarrollar pruebas con mayor profundidad e identificación del máximo de vulnerabilidades en las infraestructuras tecnológicas, pues esto permite que se desarrolle de una manera más amplia las recomendaciones y documentación pertinente para resolver o mitigar cada una de estas vulnerabilidades, lo que conlleva que la empresa Suzuki

Motor de Colombia S.A que solicito las pruebas pueda fortalecer la seguridad de su infraestructura tecnológica.

Los resultados obtenidos en las pruebas de pentest que se realizan sobre la compañía Suzuki Motor de Colombia S.A y sobre cualquier otra infraestructura deben estar acompañados de una buena documentación, tanto técnica para el personal del área de T.I donde se indiquen los tipos de vulnerabilidades, su código CVE, posibles formas de mitigar o resolver dicha vulnerabilidad, como un informe de tipo ejecutivo el cual se debe presentar para las personas que no están relacionadas a las áreas técnicas, este debe contener un lenguaje comprensible, fluido y de fácil entendimiento para las personas que los están leyendo, de este modo se pueda generar aceptación sobre los temas que se están tratando e indicando.

BIBLIOGRAFÍA

ÁLVAREZ LOZANO Michael David, CORREA MESA Miguel Ángel. análisis de las vulnerabilidades de la infraestructura tecnológica mediante testing de caja blanca, bajo la norma ISO 27005 en la compañía caracol radio, nodo principal Bogotá. [En línea]. Proyecto de grado. Universidad Cooperativa de Colombia, 2020. [Consulta: 23 de marzo 2021]. Disponible en: https://repository.ucc.edu.co/bitstream/20.500.12494/16502/1/2020_Analisis_Vulnerabilidades_Infraestructura.pdf

BRICEÑO OSORIO, Juan Carlos. Análisis de riesgos de los sistemas de seguridad informática de la empresa KAPPA10 LTDA. [en línea]. Proyecto de grado. Universidad Nacional Abierta y a Distancia – UNAD, 2018. [Consultado 17 de marzo de 2021]. Disponible en https://repository.unad.edu.co/bitstream/handle/10596/27822/%20%09jcbricenoo.pdf?sequence=1&isAllowed=y

CAO AVELLANEDA Javier. La importancia del análisis del riesgo dentro del SGSI. [Sitio Web]. Seguridad de la información Blogspot. [Consulta: 23 de marzo 2021]. Disponible en: http://seguridad-de-la-informacion.blogspot.com/2008/10/la-importancia-del-anlisis-del-riesgo.html

CAUTÍN GARCÍA, Carlos Andrés. Análisis de vulnerabilidades mediante pruebas de penetración avanzada pentesting al sitio web oficial de la alcaldía del municipio de Quibdó –Chocó. [en línea]. Proyecto de grado. Universidad Nacional Abierta y a Distancia – UNAD, 2019. [Consultado 17 de marzo de 2021]. Disponible en https://repository.unad.edu.co/bitstream/handle/10596/26950/%20%09cacouting.pdf?sequence=1&isAllowed=y

Centro Cibernético Policial. Balance Cibercrimen 2020. [Sitio Web]. Centro Cibernético Policial. [Consulta: 27 de marzo de 2021]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

Cero Uno Software. 7 conceptos básicos de Seguridad Informática. [Sitio WEB]. Cero Uno Software. [Consulta: 20, marzo,2020]. Disponible en: https://cerounosoftware.com.mx/2016/08/17/7-conceptos-b%C3%A1sicos-de-seguridad-inform%C3%A1tica/

Definición ABC. Definición de Hacker. [Sitio WEB]. Guillem Alsina González. [Consulta: 11, febrero,2020]. Disponible en: https://www.definicionabc.com/tecnologia/hacker-2.php

DOMÈNECH ONCINS Meritxell. Tipologías de hacker: White/Gray/Black Hat Hacker. [Sitio WEB]. Iniseg. [Consulta: 20, marzo, 2021]. Disponible en: https://www.iniseg.es/blog/ciberseguridad/tipologias-de-hacker-whitegrayblack-hat-hacker/

Ecured. Ataque informático. [Sitio WEB]. Ecured enciclopedia cubana. [Consulta: 27, marzo, 2021]. Disponible en: https://www.ecured.cu/Ataque_inform%C3%A1tico

El Tiempo. Empresas que pierden hasta $4.000 millones por ciberataques. [Sitio WEB]. [Consulta: 27, marzo, 2021]. Disponible en: https://www.eltiempo.com/economia/existen-empresas-que-pierden-hasta-4-000-millones-por-ciberataques-392246

Firma-e. Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad. [Sitio Web]. Firma-e. [Consulta: 16 de marzo de 2021]. Disponible en: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

GOMEZ. Análisis de Riesgo. [Sitio Web]. Monografias.com. [Consulta: 23 de marzo 2021]. Disponible en: https://www.monografias.com/trabajos83/analisis-riesgo/analisis-riesgo.shtml

Google Books. Seguridad de la información redes, informática y sistemas de información. [Sitio WEB]. Javier Areitio. [Consulta: 9, febrero,2021]. Disponible en: https://books.google.es/books?hl=es&lr=&id=_z2GcBD3deYC&oi=fnd&pg=IA1&dq=seguridad+de+la+informaci%C3%B3n&ots=wtiltJDYNh&sig=0aOOL3xPEFqIpWjeQMSIAcmgxjU#v=onepage&q=seguridad%20de%20la%20informaci%C3%B3n&f=false

Incibe. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [Sitio WEB]. Incibe. [Consulta: 3, octubre, 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Ley 1273 de 2009 Nivel Nacional. [Sitio Web]. Propiedad de la Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá D.C. [Consulta: 19 de abril 2021]. Disponible en: http://https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Ionos. LAN — Red de área local: la tecnología de un vistazo. [Sitio Web]. Ionos. [Consulta: 16 de marzo de 2021]. Disponible en: https://www.ionos.es/digitalguide/servidores/know-how/lan/

Netec. ¿Qué es seguridad informática? | Netec Global Knowledge. [Sitio WEB]. Netec. [consulta: 10, marzo, 2021] . Disponible en: ¿Qué es seguridad informática? | Netec Global Knowledge

Normas ISO. ISO 27001 Seguridad de la Información. [Sitio WEB]. Normas ISO. [Consulta: 5, marzo,2021]. Disponible en: https://www.normas-iso.com/iso-27001/

Ostec. Pentest: ¿qué es y cuáles son los principales tipos?. [Sitio Web]. Ostec. [Consulta: 15 de marzo de 2021]. Disponible en: https://ostec.blog/es/seguridad-perimetral/pentest-concepto-tipos/

PALACIOS PALACIOS Jeysser Aurelio. Análisis de vulnerabilidades de la infraestructura tecnológica en la dependencia de formación profesional integral del SENA regional Guainía, para el diseño de una propuesta de aseguramiento de la información basada en la metodología Magerit. [En línea]. Proyecto de grado. Universidad Nacional Abierta y a Distancia – UNAD, 2020. [Consulta: 23 de marzo 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/36525/japalaciospa.pdf?sequence=1&isAllowed=y

PTES. PTES Technical Guidelines - The Penetration Testing Execution Standard. [Sitio WEB]. Relik. [Consulta: 26, febrero,2021]. Disponible en: http://www.pentest-standard.org/index.php/Main_Page

Rapid7. Nexpose Vulnerability Scanner. [Sitio WEB]. Nexpose. [Consulta: 28, febrero, 2021]. Disponible en: https://www.rapid7.com/products/nexpose/

Raydes. Metodologías Existentes. [Sitio WEB]. Alonso Caballero. [Consulta: 10, marzo, 2021]. Disponible en: http://www.reydes.com/d/?q=Metodologias_Existentes

SARMIENTO ACOSTA, William Andrés. RODRÍGUEZ VÁSQUEZ, Elkin German. Análisis de vulnerabilidades de la infraestructura tecnológica en la dependencia de formación profesional integral del SENA regional Guainía, para el diseño de una propuesta de aseguramiento de la información basada en la metodología Magerit. [en línea]. Proyecto de grado. Universidad Católica de Colombia, 2019. [Consultado 17 de marzo de 2021]. Disponible en https://repository.ucatolica.edu.co/bitstream/10983/23377/1/Trabajo%20de%20Grado%20Seg.%20de%20la%20Informacion%20Final.pdf

Tenable. Nessus Professional Trial Guide. [Sitio Web]. Tenable. [Consulta: 15 de marzo de 2021]. Disponible en: https://docs.tenable.com/other/nessus/NessusTrialGuide.pdf

Tools Ietf. RFC 2828 - Internet Security Glossary. [Sitio Web]. Tools Ietf. [Consulta: 19 de abril de 2021]. Disponible en: https://tools.ietf.org/html/rfc2828

TORRES Cesar. La importancia de realizar un análisis de riesgo en las empresas. [En línea]. Universidad Piloto de Colombia, 2020. [Consulta: 23 de marzo 2021]. Disponible en: http://polux.unipiloto.edu.co:8080/00003266.pdf

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Revista Especializada en Ingeniería. Metodologías Para el Análisis de Riesgos en los SGSI; Bogotá: UNAD. [Sitio Web]. [Consultado 20 marzo de 2020]. Disponible en: https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

ANEXOS

Anexo A. Formato_Levantamiento_Requerimientos

FORMATO DE LEVANTAMIENTO DE REQUERIMIENTOS PARA PENTEST

Nombre de la Compañía:	Suzuki Motor de Colombia S.A.	FECHA	15/04/2021
Nombre de contacto en la compañía:	Yorlen Álzate Peláez		
Nombre del contacto que realiza la actividad:	Julian Andrés Ruiz Jaramillo		
Nombre del contacto que realiza la actividad:	Jaime Alberto Mosquera Mosquera		

No.	OBJETIVO AUDITAR	IP	ESCENARIO	TIPO DE AUDITORIA
1	Servidores	192.XXX.YYY.Z43	LAN	Caja Blanca
2	Servidores	192.XXX.YYY.Z21	LAN	Caja Blanca
3	Servidores	192.XXX.YYY.Z23	LAN	Caja Blanca
4	Servidores	192.XXX.YYY.Z46	LAN	Caja Blanca
5	Servidores	192.XXX.YYY.Z49	LAN	Caja Blanca
6	Servidores	192.XXX.YYY.Z19	LAN	Caja Blanca
7	Servidores	192.XXX.YYY.Z44	LAN	Caja Blanca
8	Servidores	192.XXX.YYY.Z51	LAN	Caja Blanca
9	Equipos	192.XXX.YYY.Z48	LAN	Caja Blanca
10	Equipos	192.XXX.YYY.Z03	LAN	Caja Blanca

Anexo B. Formato RAE

Fecha de Realización:	26/10/2021
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Infraestructura tecnológica y seguridad en redes
Título:	Identificación de las diferentes vulnerabilidades de la red LAN de planta ensambladora y el almacén de Pereira de la compañía Suzuki Motor de Colombia S.A, mediante la metodología Penetration Testing Execution Standard
Autor(es):	Mosquera Mosquera Jaime Alberto Ruiz Jaramillo Julián Andrés
Palabras Claves:	Herramientas, PTES, Pentest, Red LAN, Vulnerabilidades.
Descripción:	El proyecto aplicado tuvo como propósito realizar un pentest o prueba de concepto con el fin de diagnosticar el estado de la infraestructura tecnológica de la compañía Suzuki Motor de Colombia S.A y específicamente a la red LAN de la planta ensambladora ubicada en el corregimiento de Cerritos perteneciente al municipio de Pereira, de igual manera se aplicará este pentest o prueba de concepto al almacén Pereira. El proyecto aplicado tuvo una duración de diez (10) meses, la metodología que se utilizó para las pruebas de pentesting fueron de tipo caja blanca, basados en la metodología PTES, puesto que se conocía con antelación la infraestructura e información de la compañía Suzuki Motor de Colombia S.A. mediante el uso de varias herramientas se logró realizar estas pruebas obteniendo información valiosa sobre las vulnerabilidades y brechas de seguridad en la red LAN. Se presentó un informe técnico y ejecutivo con el análisis de las vulnerabilidades encontradas y de las posibles soluciones, con el fin de mitigar las vulnerabilidades y riesgos encontrados durante el estudio y auditoría

	realizada a la red LAN de la planta ensambladora y el almacén Pereira, con el fin de que la compañía mejore considerablemente la seguridad y su funcionamiento de red.

Fuentes bibliográficas destacadas:

PTES. PTES Technical Guidelines - The Penetration Testing Execution Standard. [Sitio WEB]. Relik. [Consulta: 26, febrero,2021]. Disponible en: http://www.pentest-standard.org/index.php/Main_Page

Normas ISO. ISO 27001 Seguridad de la Información. [Sitio WEB]. Normas ISO. [Consulta: 5, marzo,2021]. Disponible en: https://www.normas-iso.com/iso-27001/

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Revista Especializada en Ingeniería. Metodologías Para el Análisis de Riesgos en los SGSI; Bogotá: UNAD. [Sitio Web]. [Consultado 20 marzo de 2020]. Disponible en: https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

Firma-e. Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad. [Sitio Web]. Firma-e. [Consulta: 16 de marzo de 2021]. Disponible en: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

Google Books. Seguridad de la información redes, informática y sistemas de información. [Sitio WEB]. Javier Areitio. [Consulta: 9, febrero,2021]. Disponible en: https://books.google.es/books?hl=es&lr=&id=_z2GcBD3deYC&oi=fnd&pg=IA1&dq=seguridad+de+la+informaci%C3%B3n&ots=wtiltJDYNh&sig=0aOOL3xPEFqIpWjeQMSIAcmgxjU#v=onepage&q=seguridad%20de%20la%20informaci%C3%B3n&f=false

Incibe. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [Sitio WEB]. Incibe. [Consulta: 3, octubre, 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Ley 1273 de 2009 Nivel Nacional. [Sitio Web]. Propiedad de la Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá D.C. [Consulta: 19 de abril 2021]. Disponible en: http://https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Contenido del documento:	OBJETIVO GENERAL Evaluar la infraestructura tecnológica de la red LAN de Planta Ensambladora y el almacén de

	Pereira de la compañía Suzuki Motor de Colombia S.A. mediante herramientas de pentesting basados en la metodología Penetration Testing Execution Standard (PTES), con el fin de identificar las diferentes vulnerabilidades de la red LAN. OBJETIVOS ESPECÍFICOS Analizar la infraestructura tecnológica de la red LAN de Planta Ensambladora y el almacén de Pereira de la compañía Suzuki Motor de Colombia S.A., para identificar las posibles vulnerabilidades que presenta la red LAN, apoyados en la metodología PTES. Seleccionar las herramientas de pentesting de red que permitan ejecutar las pruebas tipo caja blanca para la identificación de las vulnerabilidades en la red LAN de Planta Ensambladora y el almacén de Pereira de la compañía Suzuki Motor de Colombia S.A, teniendo en cuenta las herramientas que propone la metodología PTES. Elaborar la documentación sobre los resultados obtenidos al hacer las diferentes pruebas de seguridad a la red LAN de Planta Ensambladora y almacén de Pereira de la compañía Suzuki Motor de Colombia S.A. Establecer recomendaciones a partir de los resultados obtenidos en el pentest que permitan mitigar el riesgo frente a una amenaza en la red LAN de la Planta Ensambladora y del almacén Pereira de la compañía Suzuki Motor de Colombia S.A.
Marco Metodológico:	El diseño metodológico para la realización del proyecto de grado aplicado está basado en la metodología cuantitativa debido que se pretende analizar una situación aportando evidencia física sobre la investigación efectuada en la infraestructura tecnológica de la compañía Suzuki Motor de Colombia S.A., es

	por eso por lo que se decidió hacer uso de una metodología modular para la realización de los pentest como lo es: Metodología PTES El trabajo aplicado a la compañía Suzuki Motor de Colombia S.A, específicamente a la planta ensambladora y el almacén de Pereira, se basará en el desarrollo de la guía Metodológica PTES, el cual tiene como base siete (7) sesiones principales, las cuales pueden ser o no aplicables a este proyecto de grado, permitiendo llevar de una manera controlada y establecida el desarrollo de toda la actividad. Las siete (7) sesiones Interacciones previas Recolección de información Modelado de amenazas Análisis de vulnerabilidades Explotación Post explotación Informe Según lo indicado en las siete (7) sesiones, para el desarrollo del proyecto aplicado a la compañía Suzuki Motor de Colombia en su planta principal y almacén de Pereira, solo se tendrán en cuenta cinco (5) sesiones: Interacciones previas Recolección de Información Modelado de amenazas Análisis de vulnerabilidades Informe Se decide no tener en cuentas dos (2) sesiones que son: Explotación Post Explotación

	Debido a que la ejecución de estas dos sesiones puede generar inconvenientes en la compañía Suzuki Motor de Colombia S.A y el correcto funcionamiento de los diferentes activos de información ocasionando una alteración en la operación de la compañía.
Conceptos adquiridos:	Planes de contingencia y respuesta ante incidentes de ciberseguridad. Establecer mínimos privilegios en los sistemas de información para prevenir la modificación o fuga de información. Realizar pruebas de vulnerabilidades constantes a la infraestructura tecnológica. Auditoria de logs permite registrar los diferentes movimientos en generados en los sistemas informáticos por los usuarios o por extraños.
Conclusiones:	A partir de la finalización del proyecto aplicado sobre la compañía Suzuki Motor de Colombia S.A, partiendo del desarrollo de los objetivos específicos planteados y logrando desarrollar el objetivo general del presente proyecto, se pueden establecer una serie de recomendaciones, las cuales pueden ser de gran utilidad para mejorar la seguridad de la infraestructura tecnológica de la compañía, donde podemos concluir que: Los análisis de infraestructura tecnológicas, en este caso la de la compañía Suzuki Motor de Colombia S.A mediante pentest, son totalmente necesarias pues estas auditorias, permiten conocer el grado de vulnerabilidad y de seguridad en el que se encuentra una organización, permitiendo que se pueda mejorar considerablemente la protección de cada uno de sus activos y por supuesto dando un alto índice de protección sobre su información. Existen muchos tipos de herramientas para la realización de auditorías o pentest sobre las diferentes infraestructuras tecnológicas, la elección de una herramienta se debe basar

	sobre el conocimiento de uso de la herramienta y de igual manera se debe buscar que subsane las necesidades presentadas en el pentest o auditoria que se pretende realizar, puesto que cada una de estas herramientas tiene un enfoque o especialidad y no todas sirven para lo mismo. La seguridad informática es un factor sumamente importante para la empresa Suzuki Motor de Colombia S.A., por lo cual se debe contar con estrategias y metodologías para el manejo de la seguridad de la información las cuales brinden protección a los activos de información de la organización de posibles pérdidas de información o de ataques informáticos. Las herramientas de escaneo de pentesting o de auditorías de seguridad, son un factor fundamental en el desarrollo e identificación de las vulnerabilidades de los activos de información de Suzuki Motor de Colombia S.A., ya que por medio de dichas herramientas se identifican las vulnerabilidades con las que cuentan los diferentes activos de información con el objetivo de mitigar o eliminar estas brechas de seguridad.