UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

ABRIL 2022 – SEPTIEMBRE 2022

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

APLICACIÓN DE METODOLOGÍAS DE DETECCIÓN TEMPRANA DE VULNERABILIDADES EN LA RED DE LA EMPRESA INNOVACIÓN TECNOLÓGICA GARCÍA

ESTUDIANTE:

OCHOA ACOSTA JUAN GUILLERMO

TUTOR:

ING. HUGO GUERRERO TORRES, MGS

AÑO 2022

Contenido

PLANTEAMIENTO DEL PROBLEMA 3

OBJETIVOS 6

- **Objetivo principal** 6
- **Objetivos específicos** 6

LÍNEA DE INVESTIGACIÒN 7

MARCO CONCEPTUAL 8

MARCO METODOLÓGICO 16

RESULTADOS 18

DISCUSIÓN DE RESULTADOS 25

CONCLUSIONES 26

RECOMENDACIONES 28

Bibliografía 29

ANEXOS 30

PLANTEAMIENTO DEL PROBLEMA

La agilización de flujos y procesos se ha dado a través de la evolución de las redes y las tecnologías de la información y han permitido incrementar el tamaño y el flujo de la información, sin embargo, esto posibilita la aparición de nuevas amenazas y vulnerabilidades.

Las vulnerabilidades de seguridad son causadas por errores del personal siendo así buscadas o creadas directamente por las acciones de los delincuentes que buscan desestabilizar la organización.

La empresa Innovación Tecnológica García se dedica a la venta de equipos tecnológicos, realiza pagos y ventas vía internet en el cual los clientes registran datos e información personal de suma importancia que almacenan en su base de datos.

El sistema de compras en línea que posee la empresa, aunque demuestra funcionabilidad no es considerado seguro por muchos clientes lo que ha perjudicado en las ventas por este medio, es necesario visualizar a los clientes un entorno confiable en el cual estén seguros al momento de realizar sus compras. Esto lleva a la pregunta ¿qué tan seguro esta la información que ingresa a la empresa? lo que lleva a este caso de estudio.

La protección de la información es una tarea continua que requiere mucho esfuerzo a nivel técnico y tecnológico, ya que representa un impacto negativo en el nivel de funcionamiento y reputación de la empresa Innovación Tecnológica García.

Los problemas de seguridad en la empresa conllevan a la pérdida o robo de información,

por fuentes internas y/o externas. Esto puede perjudicar la imagen que se tiene de la empresa y perjudicar a los clientes que confiaron en ella.

JUSTIFICACIÓN

El presente proyecto tiene como finalidad la aplicación de metodologías de detección temprana de vulnerabilidades en la red de la empresa Innovación Tecnológica García.

Debido a las constantes amenazas que existen en la red de la empresa, se ha generado daños, como la exposición de información privada, el acceso no autorizado a datos, la infección de programas entre otros, siendo un problema que se da de manera cotidiana afectando así la seguridad de la empresa.

Por lo expuesto antes, el descubrimiento de las vulnerabilidades en la red se puede mejorar y así reforzar la seguridad evitando el filtrado de malware y los robos de información ya que toda empresa tiene información personal de los trabajadores como de los clientes de dicha empresa y en respuesta a estos eventos prioritarios y de seguridad implica una serie de decisiones e innovación y organización de la información.

Esta metodología nos ayudara a detectar fallas y verificar de quien o de donde se producen ya sea por fallas internas o externas, con el fin de corregir dichas falencias que se puedan producir en la empresa.

OBJETIVOS

- **Objetivo principal**

Aplicar una metodología para la detección temprana de vulnerabilidades en la red de la empresa de INNOVACIÓN TECNOLÓGICA GARCÍA.

- **Objetivos específicos**

• Análisis del estado actual de la infraestructura de red de la empresa INNOVACION TEGNOLOGICA GARCIA

• Análisis de metodologías que son factibles para la búsqueda de vulnerabilidades tempranas en la red de la empresa INNOVACION TEGNOLOGICA GARCIA

• Evaluar el estado de vulnerabilidades en la red de la empresa INNOVACION TEGNOLOGICA GARCIA.

LÍNEA DE INVESTIGACIÒN

En el presente caso de estudio, el cual tiene como propósito principal aplicar metodologías para encontrar vulnerabilidades en la red de la empresa INNOVACIÓN TECNOLÓGICA GARCÍA de la ciudad de Babahoyo tiene una relación muy directa con la línea de investigación de la carrera de ingeniería en sistemas de información, la cual es denominada “Sistemas de información y comunicación, emprendimiento e innovación”, ya que algo que se menciona en dicha línea de investigación, tiene que ver con los sistemas de información, los cuales durante su desarrollo, necesitan su respectivo análisis de requerimientos, con el propósito de poder asegurarse de que las actividades y funciones que llevará a cabo el futuro sistema, cumple o no con solucionar las problemáticas y las necesidades que se tienen actualmente en un lugar determinado, puede ser una empresa, una institución pública o privada, entre otras, pero debe solucionar una problemática, sino el sistemas de información por más atractivo que luzca, no servirá para nada, porque no ayuda en nada ni a nadie.

La sub línea de investigación de este caso de estudio es la de “Redes y tecnologías inteligentes de software y hardware.

MARCO CONCEPTUAL

La evolución de la tecnología de la información y comunicación (TIC), ha hecho que las personas tengan mayor accesibilidad a los sistemas informáticos, estos avances tecnológicos permiten que las personas tengan a su alcance cualquier tipo de información, pero todo esto ha causado que también crezca el riesgo vinculado con la seguridad. La seguridad informática apareció debido a la necesidad de dar soporte a esas nuevas tecnologías, la infraestructura de red al ser requerida por las empresas para permitir el acceso a la información y dar movilidad a las personas, necesitan ser tratadas de manera primordial, por cuanto deben cuidar la parte vital de toda empresa, como son sus datos. El uso de redes inalámbricas gana cada vez más usuarios y con ello el uso de herramientas y recursos tecnológicos, pero también aparecen nuevas vulnerabilidades y amenazas. (Servicio de deteccion temprana de vulnerabilidades basados en shodan, 2021).

La seguridad de la información es todo el conjunto de técnicas y acciones que se implementan para controlar y mantener la privacidad de la información y datos de la institución; y asegurarnos que esa información no salga del sistema de la empresa y caigan en las manos equivocadas. (AdminiberoBlogs, 2020)

Los adversarios desarrollan nuevas amenazas, debido al crecimiento del tráfico de Internet, logrando con ello que la expansión de la superficie de ataque crezca. A medida que eso sucede, los riesgos para las empresas son cada vez mayores, más de un tercio de las organizaciones que han sufrido un ataque perdió el 20 % de sus ingresos o más (Chuquitarco

Mario, 2017)**.**

En informática, se entiende por red (usualmente red informática o red de computadoras) a la interconexión de un numero determinado de computadores (o de redes a su vez) mediante dispositivos alámbricos o inalámbricos que, mediante impulsos eléctricos, ondas electromagnéticas u otros medios físicos les permiten enviar y recibir información en paquetes de datos, compartir sus recursos y actuar como un conjunto organizado. (Etecé, 2021)

Una red es un conjunto de dispositivos conectados entre sí por medios físicos que mediante cualquier medio de transporte de datos comparten información, recursos y servicios. Las redes de ordenadores están en todas partes: lo más normal es que en un domicilio haya un router (enrutador en castellano) inalámbrico que provee de internet por ejemplo a ordenadores, teléfonos y tabletas; seguramente en el centro de trabajo haya una red de cable por la que los equipos se comuniquen e incluso no es nada raro que haya establecimientos como librerías, cafeterías o centros comerciales que promocionen una conexión gratuita a internet. (Sanchez, 2014)

Vulnerabilidades

Según la empresa Ambit Building Solutions (Ambit S.A., 2020) , una vulnerabilidad es un fallo o debilidad de un sistema de información que pone en riesgo la seguridad de la misma. Se trata de un “agujero” que puede ser producido por un error de configuración, una carencia de procedimientos o un fallo de diseño. Los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas informáticos (por ejemplo, de los sistemas operativos) para poder entrar en los

mismos y realizar actividades ilegales, robar información sensible o interrumpir su funcionamiento.

Las empresas deben evitar ataques debido a estas vulnerabilidades, que pueden s er corregidas, en su mayoría, con la actualización del software o firmware.

Amenazas informáticas

Una amenaza informática es toda aquella acción que aprovecha una vulnerabilidad para atacar o invadir un sistema informático. Las amenazas informáticas para las empresas provienen en gran medida de ataques externos, aunque también existen amenazas internas (como robo de información o uso inadecuado de los sistemas). (Ambit S.A., 2020)

Tipos de Vulnerabilidades y Amenazas informáticas en la empresa

Son muchas las vulnerabilidades y amenazas informáticas a las que están expuestas las empresas en la actualidad. Por eso la inversión en ciberseguridad y sistema de protección ha experimentado un gran aumento en los últimos años, siendo los profesionales en ciberseguridad uno de los perfiles más buscados en el sector de la informática. (Ambit S.A., 2020)

A continuación, se indican las principales amenazas y vulnerabilidades a las que se exponen las empresas hoy en día:

Amenazas de Malware. Los programas maliciosos son una de las mayores ciber amenazas a la que se exponen las empresas. Dentro del malware existen distintos tipos de amenazas, siendo las principales.

Virus. Los virus informáticos son un software que se instalan en un dispositivo con el objetivo de ocasionar problemas en su funcionamiento. Para que un virus infecte un sistema es necesaria la intervención de un usuario (intencionada o inintencionadamente).

Gusanos. Es uno de los malware más comunes que infectan los equipos y sistemas de una empresa, ya que no requieren de la intervención del usuario ni de la modificación de algún archivo para poder infectar un equipo. El objetivo de los gusanos es el de replicarse e infectar el mayor número de dispositivos posibles utilizando la red para ello. Son una amenaza para las redes empresariales, porque un solo equipo infectado puede hacer que la red entera se vea afectada en un espacio corto de tiempo.

Troyanos. Los troyanos son programas que se instalan en un equipo y pasan desapercibidos para el usuario. Su objetivo es el de ir abriendo puertas para que otro tipo de software malicioso se instale.

Ransomware. El ransomware se ha convertido en el malware más temido en la actualidad por las empresas. Consiste en encriptar toda la información de la empresa, impidiendo el acceso a los datos y los sistemas y se pide un rescate para poder liberar la información (normalmente en criptomonedas como bitcoins).

Keyloggers. Se instalan a través de troyanos y se encargan de robar datos de acceso a plataformas web, sitios bancarios y similares.

Vulnerabilidades del sistema

Según (Ambit S.A., 2020) los sistemas y aplicaciones informáticos siempre tienen algún error en su diseño, estructura o código que genera alguna vulnerabilidad. Por muy pequeño que sea ese error, siempre podrá generar una amenaza sobre los sistemas y la información, siendo la puerta de entrada para recibir ataques externos o internos. Las principales vulnerabilidades suelen producirse en:

- Errores de configuración.
- Errores en la gestión de recursos.
- Errores en los sistemas de validación.
- Errores que permiten el acceso a directorios.
- Errores en la gestión y asignación de permisos.
- Amenazas de ataques de denegación de servicio

Un ataque de denegación de servicio distribuido (DDoS) se produce cuando un servidor recibe muchas peticiones de acceso, sobrecargando el sistema y haciendo que el servidor caiga o funcione de forma incorrecta (acceso lento o rebotando mensajes de errores). Para realizar este tipo de ataques se utilizan muchos ordenadores (bots) que de forma automatizada hacen peticiones a ese servidor. (Ambit S.A., 2020)

Se deben tomar medidas para prevenidr los ataques DDoS para evitar que el sistema quede inactivo perjudicando así al negocio o los procesos que ejecute la empresa.

Vulnerabilidades producidas por contraseñas

Utilizar contraseñas poco seguras genera vulnerabilidades en los sistemas, pues si son fácilmente descifrables pueden generar incursiones de terceros no autorizados que pueden robar, modificar o eliminar información, cambiar configuraciones si disponen de los privilegios apropiados, o incluso apagar equipos. (Ambit S.A., 2020)

Se debe generar contraseñas seguras para incrementar el nivel de ciberseguridad de las empresas

Vulnerabilidades producidas por usuarios

Una de las principales causas de los ataques informáticos está relacionada con un uso incorrecto o negligente por parte de un usuario. Una mala asignación de privilegios o permisos puede hacer que un usuario tenga acceso a opciones de administración o configuración para las que no está preparado, cometiendo errores que suponen una amenaza para la empresa. (Ambit S.A., 2020)

El error humano es otra causa de riesgos en ciberseguridad. El usuario siempre tiene el riesgo de cometer un error que pueda generar una vulnerabilidad que suponga una amenaza informática. Por eso en ciberseguridad se tiende a automatizar procesos críticos para minimizar o eliminar el factor de riesgo del error humano. (Ambit S.A., 2020)

Las malas prácticas o la falta de formación en ciberseguridad también generan vulnerabilidades, como la apertura de ficheros de dudosa procedencia, engaños por publicidad falsa, apertura de correos fraudulentos y similares. Estas acciones son una amenaza a sufrir

ataques como el phishing (suplantación de identidad) o similares. (Ambit S.A., 2020)

Otras amenazas informáticas

Existen muchas otras amenazas informáticas que afectan a las empresas como los ataques por Inyección SQL que afectan a servidores de bases de datos empresariales, red de equipos zombies (utilizando recursos de la empresa para actividades ilícitas), ataques MITM (man in the middle), etc. (Ambit S.A., 2020)

La ciberseguridad dentro de una empresa o negocio debe ser una actividad flexible y dinámica que se adapte continuamente a las nuevas amenazas.

Nessus Security Scanner es una herramienta licenciada bajo GPL que permite detectar las vulnerabilidades de un sistema. La principal característica de esta herramienta es que se basa en un modelo cliente/servidor, lo que permite tener el servidor desde el que se realiza e escaneo y desde los clientes conectarse al servidor para iniciar un escaneo, ver informes, etc. (Julio Gómez López, 2014)

Según (David A. Franco, 2012) En la metodología para la detección de vulnerabilidades en redes de datos, se tiene tres fases soportadas por herramientas de software, mediante las cuales se busca obtener las vulnerabilidades en los equipos de red (tanto cableada como inalámbrica) y servidores en las redes de datos objeto de estudio (en adelante: red objetivo). Esta metodología se diferencia de otras en la medida en que se soporta cada etapa en herramientas software. Por lo que en cada fase se puntualizan las acciones que se deben realizar y como se deben llevar a

cabo a través de las herramientas apropiadas. El esquema de la metodología para detección de vulnerabilidades en redes de datos, se presenta en la figura. Como puede verse en esta figura, la metodología propuesta costa de tres, las cuales se detallan a continuación.

Metodología para la detección de vulnerabilidades de datos

Figura1. Esquema de la metodología para la detección de vulnerabilidades en redes de datos. (https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642012000300014)

MARCO METODOLÓGICO

Tipo de investigación

En el presente caso de estudio se utilizó el método de investigación inductivo – deductivo el cual nos ayudara analizar las vulnerabilidades en la red en la empresa Innovación Tecnológica García.

Inductivo

La empresa Innovación Tecnológica García se maneja información importante de clientes y trabajadores en la cual se necesita investigar la seguridad de los datos ya que no se tenía en cuenta la seguridad de la red y sus dispositivos conectados a la misma.

Deductivo

Las principales causas de robos de información se deben a una mala configuración de la red y equipos, es por esto que se investigó a la empresa Innovación Tecnológica García con el fin de analizar la red, su topología e infraestructura y verificar los problemas presentados en esta empresa en torno a la seguridad de la red y corregir inmediatamente para evitar la pérdida de información.

Técnicas e instrumentos

La encuesta, realizando un formulario de preguntas objetivas dirigido al personal de la empresa Innovación Tecnológica García, con este formulario se pretende saber cuáles son las vulnerabilidades y la importancia de conocer y corregir los problemas que afecten directamente a

la red de la empresa.

1. **¿**Conoce usted si existen o no vulnerabilidades en la red de la empresa?
2. ¿Qué tan importantes son los datos que maneja la empresa?
3. ¿ha sufrido algún tipo de ataque en sus datos?
4. ¿cuenta con una metodología para detección de vulnerabilidades en la red?
5. ¿Qué sistema operativo utiliza en los dispositivos de la empresa?
6. ¿aparte de los dispositivos conectaos a la red hay otros dispositivos que no sean de la empresa?

Población. El personal que labora actualmente en la empresa, son 6 personas.

¿Cómo se utilizó la herramienta?

Se utilizo la herramienta Nessus empezando por acceder a la plataforma con usuario y contraseña, una vez cargado el programa procedemos a ingresar la ip que vamos a escanear (equipo conectado) empezando por analiza la topología de la red de la empresa luego se escanea los puertos abiertos y cerrados y damos iniciar a la aplicación Nessus para obtener el análisis de las vulnerabilidades

RESULTADOS

Tabulación de resultados.

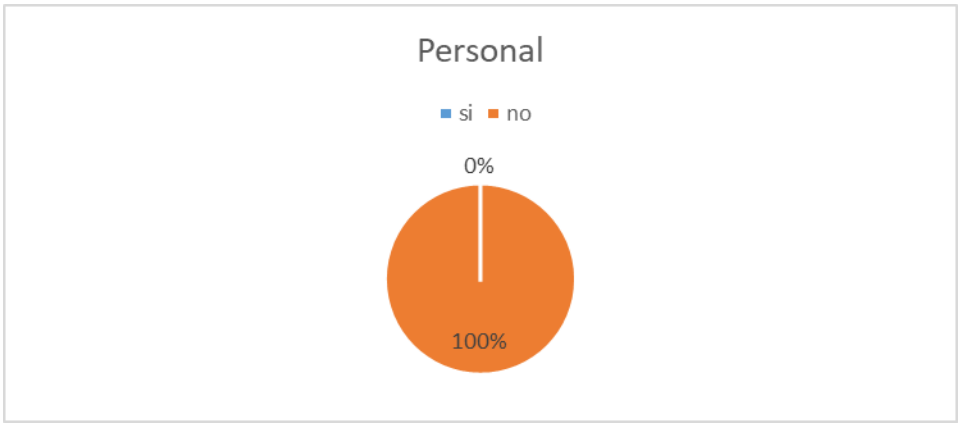
Pregunta 1. ¿Conoce usted si existen o no vulnerabilidades en la red de la empresa?

Tabla 1. Resultados de la pregunta 1

Respuesta	Valor	Porcentaje
Si	0	0 %
NO	6	100%

Fuente: Encuesta a empleados de la empresa
Elaborado por el autor

Ilustración 1 vulnerabilidad en la red



Fuente: Encuesta a empleados de la empresa
Elaborado por Juan Ochoa

Pregunta 2. ¿Qué tan importantes son los datos que maneja la empresa?

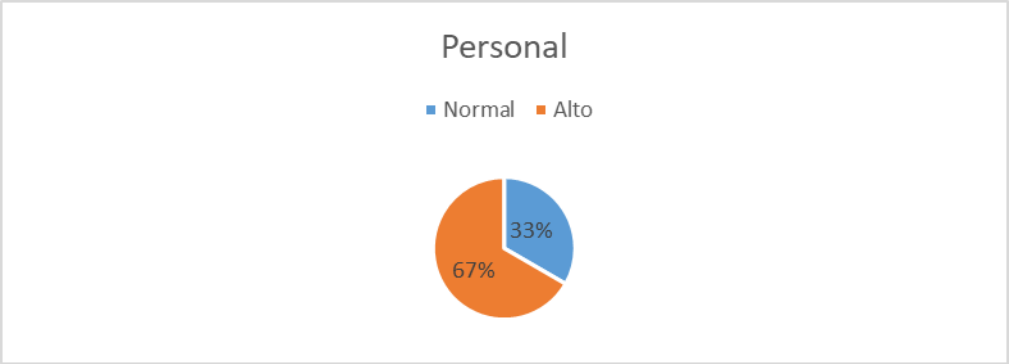
Tabla 2. Resultados de la pregunta 2

Respuesta	Valor	Porcentaje

NORMAL	2	33%
ALTO	4	67%

Fuente: Encuesta a empleados de la empresa
Elaborado por el autor

Ilustración 2 Datos de la empresa



Fuente: Encuesta a empleados de la empresa
Elaborado por Juan Ochoa

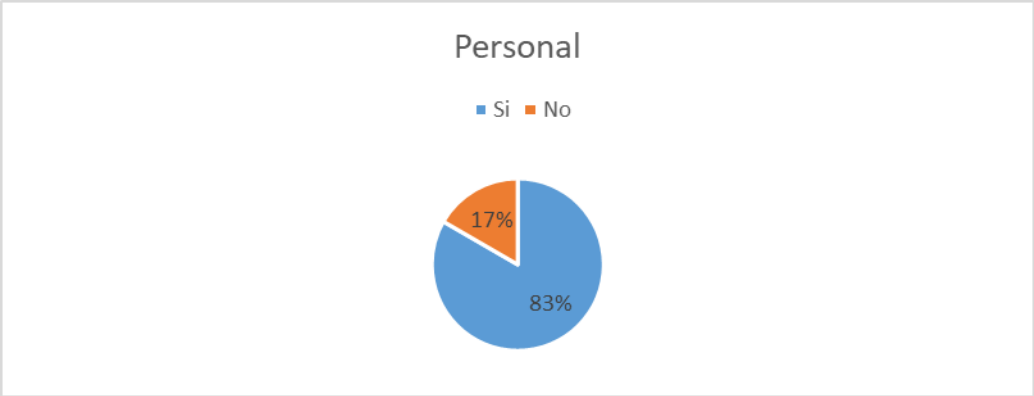
Pregunta 3. ¿ha sufrido algún tipo de ataque en sus datos?

Tabla 3. Resultados de la pregunta 3

Respuesta	Valor	Porcentaje
Si	5	83%
NO	1	17%

Fuente: Encuesta a empleados de la empresa
Elaborado por el autor

Ilustración 3 ataque de datos



Fuente: Encuesta a empleados de la empresa
Elaborado por Juan Ochoa

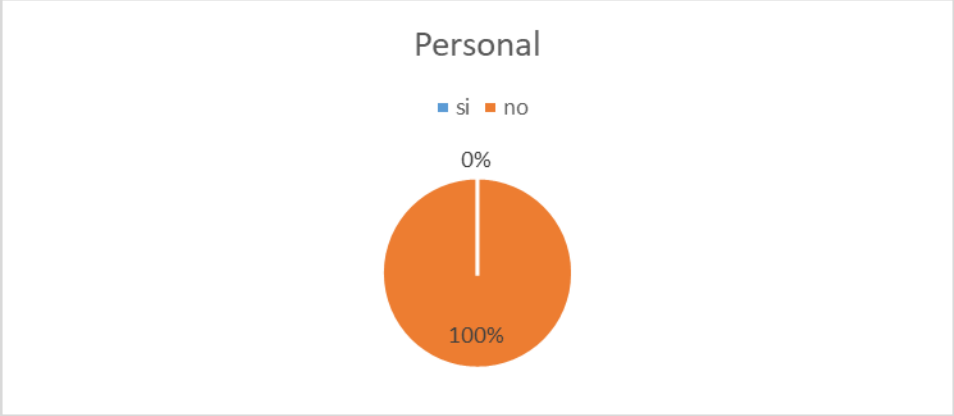
Pregunta 4. ¿cuenta con una metodología para detección de vulnerabilidades en la red?

Tabla 4. Resultados de la pregunta 4

Respuesta	Valor	Porcentaje
Si	0	0 %
NO	6	100%

Fuente: Encuesta a empleados de la empresa
Elaborado por el autor

Ilustración 4 metodología de ataque en la red



Fuente: Encuesta a empleados de la empresa
Elaborado por Juan Ochoa

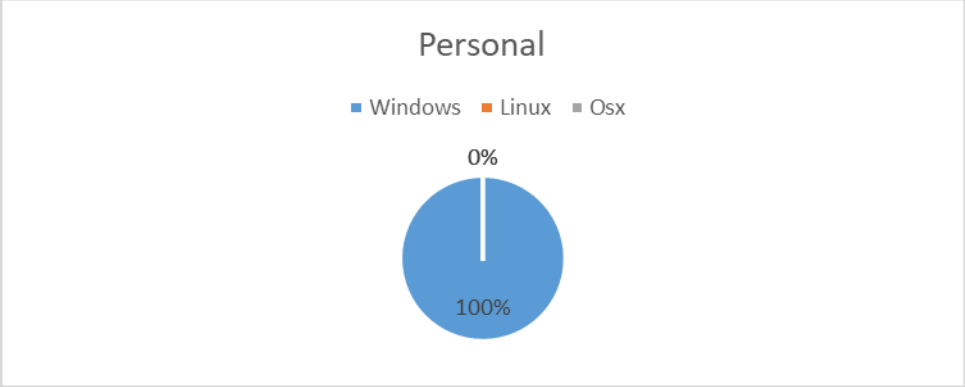
Pregunta 5. ¿Qué sistema operativo utiliza en los dispositivos de la empresa?

Tabla 5. Resultados de la pregunta 5

Respuesta	Valor	Porcentaje
Windows	6	100%
Linux	0	0%
Osx	0	0%

Fuente: Encuesta a empleados de la empresa
Elaborado por el autor

Ilustración 5 Sistemas operativos utilizados



Fuente: Encuesta a empleados de la empresa
Elaborado por Juan Ochoa

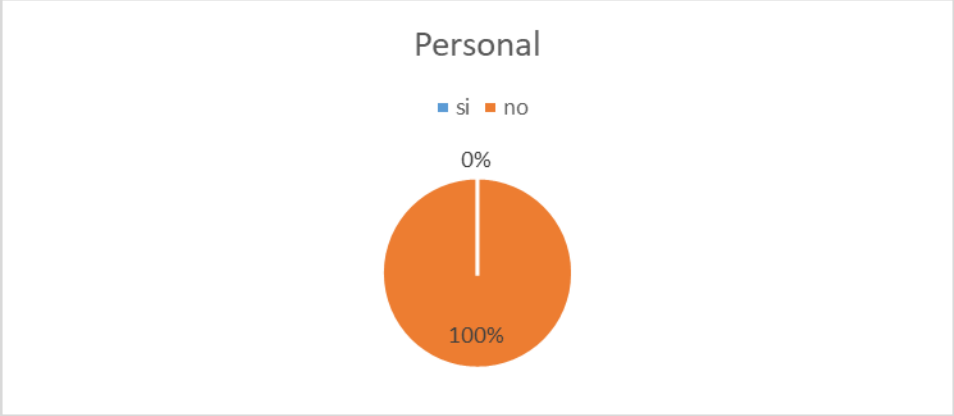
Pregunta 6. ¿aparte de los dispositivos conectaos a la red hay otros dispositivos que no sean de la empresa?

Tabla 6. Resultados de la pregunta 6

Respuesta	Valor	Porcentaje
Si	0	0 %
NO	6	100%

Fuente: Encuesta a empleados de la empresa
Elaborado por el autor

Ilustración 6 Otros dispositivos conectados a la red



Fuente: Encuesta a empleados de la empresa
Elaborado por Juan Ochoa

Listado de algunas vulnerabilidades

Tabla 7. Resultados de análisis de vulnerabilidades de la máquina principal

vulnerabilidades	**localización**	**nivel**	**Puerto**
Parche de licencia	Sistema operativo	Medio	445 tcp
No se requiere firma SMB	Base de datos	Bajo	445 tcp
Detección de servicio SMB de Microsoft Windows	Servidor	Bajo	139 tcp - smb
Enumeración de plataforma común (cpe)	Estructura	Bajo	N/A

Tabla 8 resultado de análisis de vulnerabilidades de maquina secundaria

vulnerabilidades	**localización**	**nivel**	**Puerto**
Parche de licencia	Sistema operativo	Medio	443 tcp
No se requiere firma SMB	Base de datos	Bajo	443 tcp
Detección de servicio SMB de Microsoft Windows	Servidor	Bajo	139 tcp - smb
Enumeración de plataforma común (cpe)	Estructura	Bajo	N/A

DISCUSIÓN DE RESULTADOS

Todos los empleados encuestados indican que desconocen si existen vulnerabilidades dentro de la red de la empresa lo que podría provocar problemas graves en el funcionamiento de la red.

El 33% del personal de la empresa maneja datos comunes y el otro 67% maneja datos muy importantes según los encuestados es decir que no saben la importancia de los datos que manejan.

La mayor parte del personal ha recibido o detectado que han sido atacados por malware o accesos no autorizados en la red de la empresa al no saber las consecuencias podría resultar algún problema en el futuro.

La empresa no cuenta con ninguna metodología para la detección de vulnerabilidades por lo que la misma no está protegida lo que provocaría un mal funcionamiento de los equipos conectados a la red.

Se detecto vulnerabilidades en la red con un ítem de grado medio el cual podría ocasionar algún fallo en los sistemas e información.

Gracias a la encuesta realizada al personal de la empresa Innovación Tecnológica García se puede concluir que todos los trabajadores han sido víctimas de ataques informáticos mediante la vulnerabilidad de la red ya que según la encuesta la información de la empresa es muy importante el cual se quiere evitar cualquier problema de filtración de malware a sus dispositivos

y poner en riesgo la información de la empresa.

CONCLUSIONES

Los empleados de la empresa desconocen la existencia de vulnerabilidades dentro de la red lo que conlleva a problemas futuros.

Se desconoce la importancia de los datos por parte del personal que labora en la empresa cosa que es fundamental para la empresa.

La empresa ha recibido ataques en su red por parte de terceros, solo unos pocos empleados conocían o sabían que estaban siendo atacados o tratando de vulnerar su seguridad, esto se debe a que no cuentan con metodologías de detección de vulnerabilidades.

Al aplicar esta metodología de detección temprana de vulnerabilidades a la empresa Innovación Tecnológica García seguirá mejorando su seguridad y manteniendo sus datos a salvo de algún ataque informático ya que con esta metodología su red estará más segura y podrá aplicar en periodos cortos este método para asegurar que todo está en buen estado y mejorando la fiabilidad de la empresa.

En el escaneo de puertos se detectaron los equipos que están conectados a la red de la empresa Innovación Tecnológica García y por último es el escaneo de vulnerabilidades donde se detecta cada fallo en los equipos conectados a la red. (foto 1,2,3 de anexos)

Al concluir como resultado encontramos fallas comunes como una advertencia de un problema de Microsoft ya que no se cuenta con una verificación de Microsoft para el sistema

operativo que se está utilizando en el equipo, esta es la alerta más común que notificó la herramienta Nessus y como ya se sabe nos da una corrección a dicho problema de vulnerabilidad. Con este resultado podemos observar que la mayor vulnerabilidad que tenemos en estos equipos es utilizar licencias piratas o no activar el sistema operativo en uso para este tipo de procesos que se lleva acabo, como es el ingreso de datos personales como son, las tarjetas de crédito y muchos más el cual nos estamos poniendo en riesgos para donde podemos ser víctimas de ataques y robo de información y salir muy perjudicados tanto la empresa como el cliente. La empresa procedió a comprar licencias originales para evitar estos fallos de vulnerabilidad y así como también aplicar esta metodología cada cierto tiempo para mejorar su seguridad y evitar ataques informáticos.

RECOMENDACIONES

Capacitar al personal en la detección y monitoreo de posibles vulnerabilidades dentro de la red de la empresa, lo que ayudará a que se mantenga segura.

Informar a todo el personal que labora actualmente en la empresa que todos los datos que se ingresan son muy importantes ya que desconocían de esta información.

Se recomienda acoger la información de las metodologías de detección temprana de vulnerabilidades en la red, la información recabada con las herramientas utilizadas que ayudaron a determinar y evidenciar las vulnerabilidades en la red de la empresa Innovación Tecnológica García.

Utilizar esta metodología para detectar vulnerabilidades con la finalidad de prevenir posibles amenazas y riesgos de seguridad además de asegurar y fortalecer la seguridad de la red de la empresa logrando ser más fiable para sus clientes.

También utilizar licencias ya sea de sistema operativo como también de antivirus, configurar el firewall y capacitar al personal que labora en la empresa para evitar cualquier fallo por parte de ellos para que la empresa pueda ser mucho más fiable para sus clientes.

Bibliografía

AdminiberoBlogs. (10 de julio de 2020). *Ibero*. Obtenido de https://blog.posgrados.ibero.mx/seguridad-de-la-informacion/

Ambit S.A. (10 de 11 de 2020). *Ambist building solutions together S.A.* Obtenido de https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

Arrieta, E. (20 de febreo de 2018). *diferenciador*. Obtenido de diferenciador: https://www.diferenciador.com/diferencia-entre-metodo-inductivo-y-deductivo/

Chuquitarco Mario, R. M. (15 de diciembre de 2017). Diagnóstico de las vulnerabilidades en redes inalámbricas en el Ecuador. *Revista de la Universidad Internacional del Ecuador.*, 12.

David A. Franco, J. L. (2012). Metodología para la Detección de Vulnerabilidades en Redes de Datos. *SCIELO*, 5.

Etecé, E. (5 de Agosto de 2021). *Editorial Etecé*. Obtenido de https://concepto.de/red-2/

Julio Gómez López, M. A. (2014). *Hackers Aprende a atacar y a defenderte.* España: RA-MA, S.A. .

Sanchez, E. G. (2014). *Redes e Internet.* Marpadal Interactive Madia.

Satelite. (2022). *Tendencias de ciberseguridad para el 2022 en Ecuador.* Quito: Powered by InMarketing.

Servicio de deteccion temprana de vulnerabilidades basados en shodan, 123 (universidad de las fuerzas armadas 22 de noviembre de 2021).

ANEXOS

Encuesta dirigida al jefe y empleados de la empresa Innovación Tecnológica García

1.- ¿Conoce usted si existen o no vulnerabilidades en la red de la empresa?

2.- ¿Qué tan importantes son los datos que maneja la empresa?

3.- ¿ha sufrido algún tipo de ataque en sus datos?

4.- ¿cuenta con una metodología para detección de vulnerabilidades en la red?

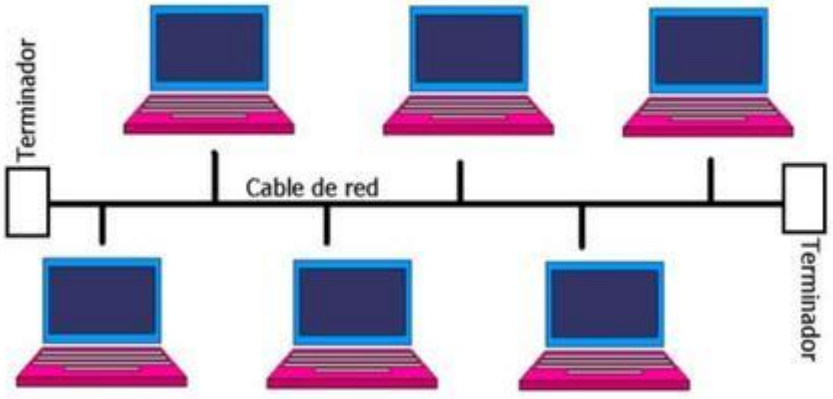
5.- ¿Qué sistema operativo utiliza en los dispositivos de la empresa?

6.- ¿aparte de los dispositivos conectaos a la red hay otros dispositivos que no sean de la empresa?

Resultado de análisis

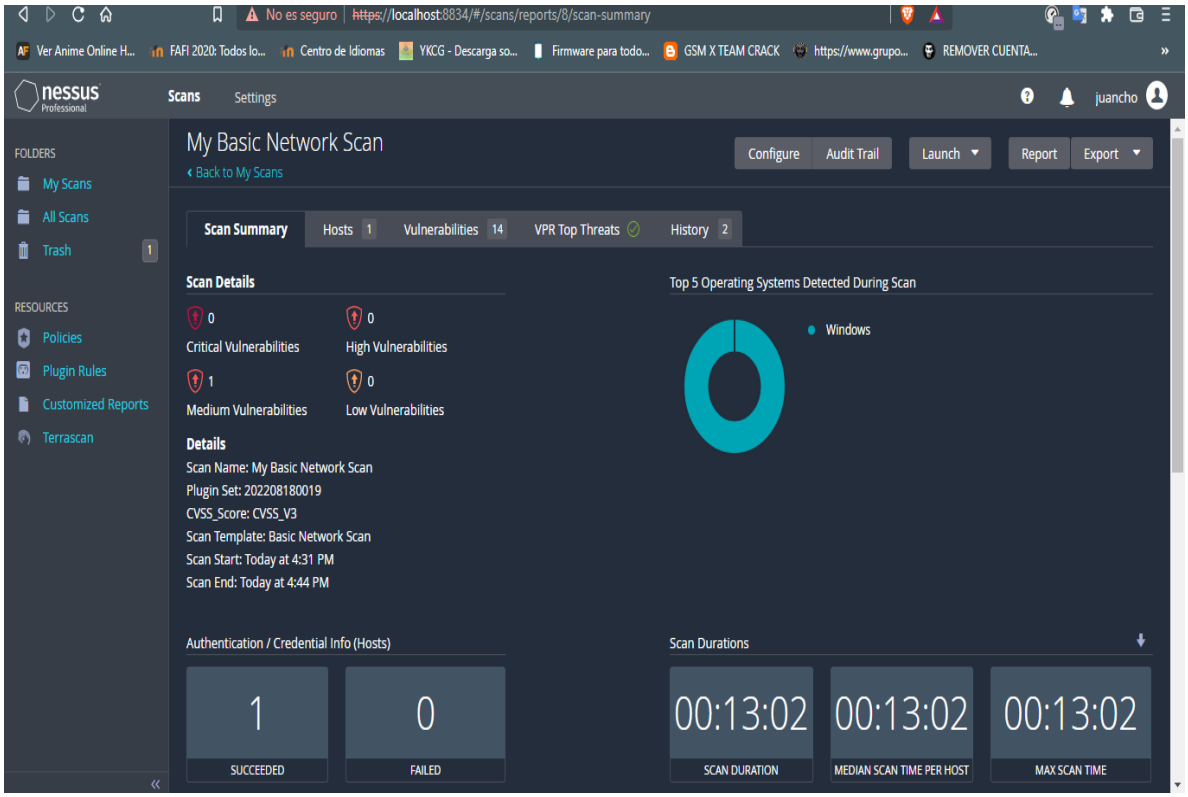
Topología de la red

Ilustración 7 topología de la red tipo bus



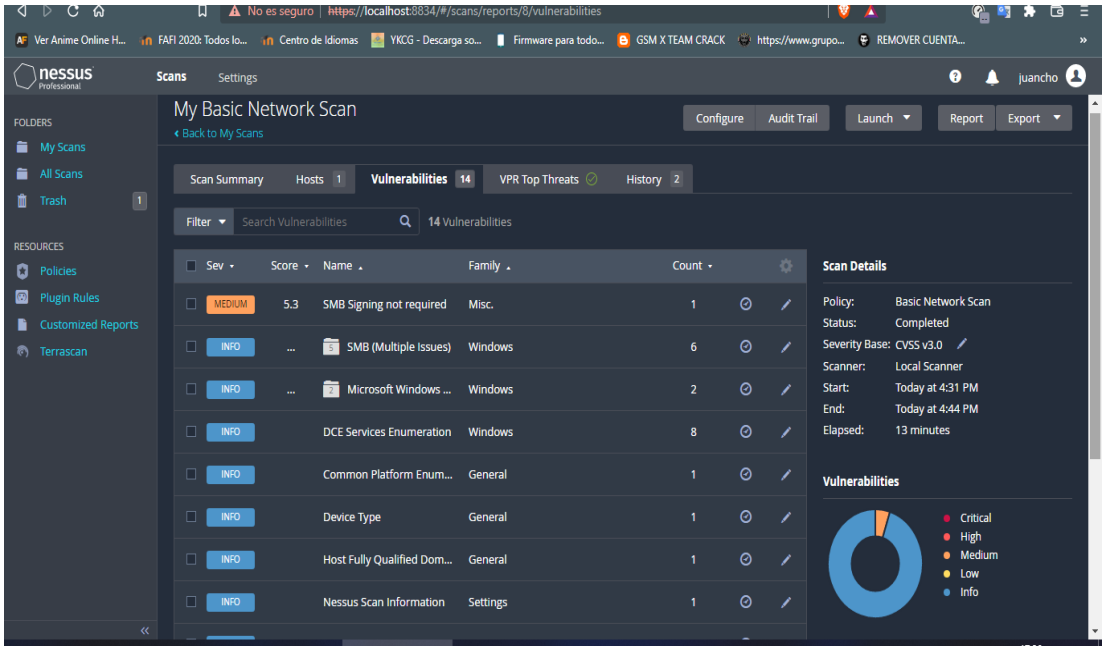
http://new-prestige.weebly.com/topologiacutea-de-bus.html

Ilustración 8 Resultado de la aplicación nessus



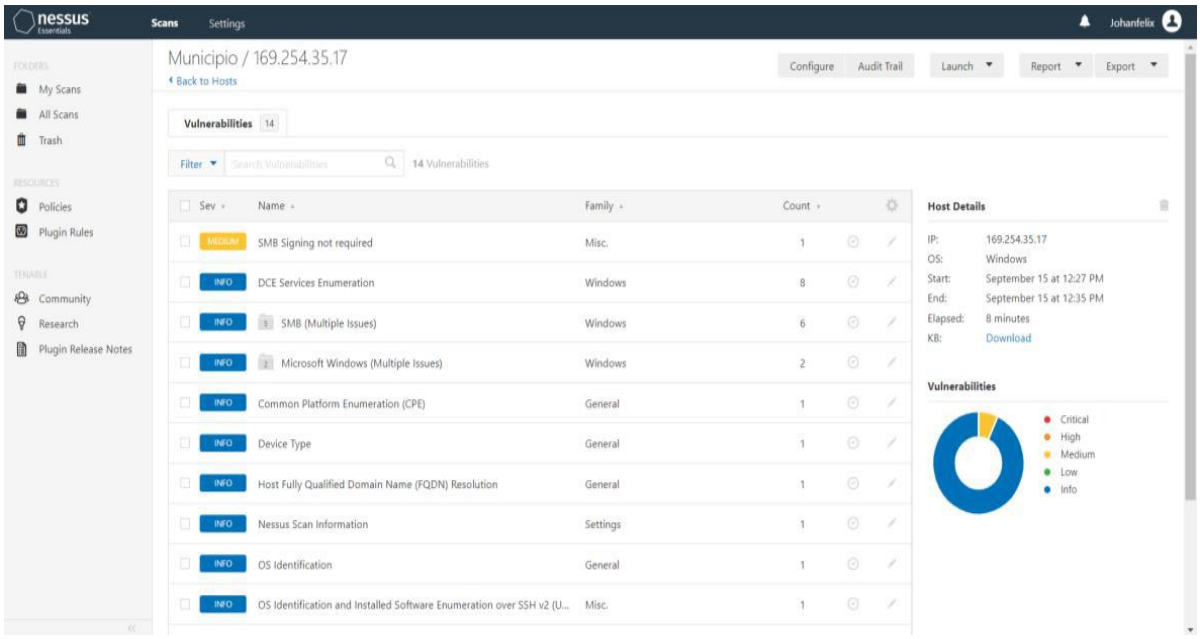
Elaborado por Juan Ochoa

Ilustración 9 Vulnerabilidad de grado medio encontrada



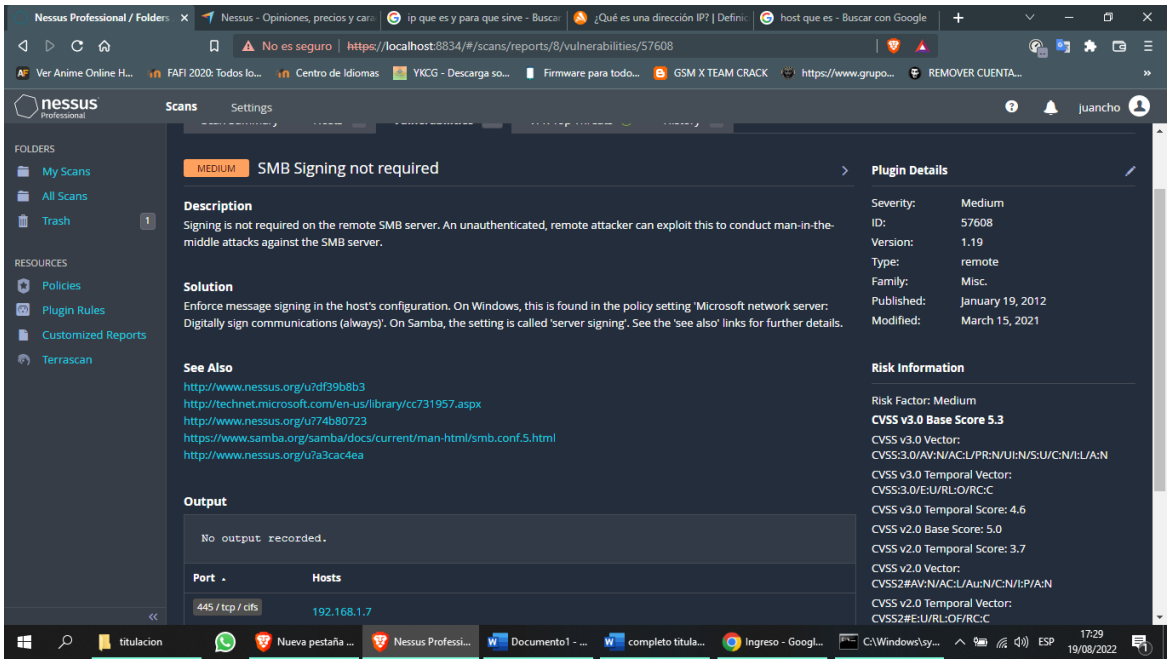
Elaborado por Juan Ochoa

Ilustración 10 Vulnerabilidad de grado medio encontrada en otro equipo



Elaborado por Juan Ochoa

Ilustración 11 Consejos para solucionar la vulnerabilidad



Elaborado por Juan Ochoa

Ilustración 12 certificado anti plagio

Elaborado por juan ochoa