UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS DE LAS VULNERABILIDADES DE LA RED INFORMÁTICA MEDIANTE LA HERRAMIENTA OPENVAS DEL GAD DE VINCES

ESTUDIANTE:

VERÓNICA FERNANDA MUÑOZ AGUIRRE

TUTOR:

ING. CARLOS CEVALLOS MONAR

ABRIL - SEPTIEMBRE 2022

Resumen

Conforme ha pasado el tiempo han aumentado los casos de hackeo a sistemas de información y redes informáticas dado que poseen vulnerabilidades que son aprovechadas por delincuentes informáticos para lograr acceder a sistemas y apropiarse de información de las organizaciones. La presente investigación buscó determinar las vulnerabilidades de la red informática mediante la herramienta OpenVAS del GAD de la ciudad de Vinces, con dicha herramienta se realizó un escaneo el cual se ejecutó mediante el entorno gráfico GreenBone. El tipo de metodología con la que se desarrolló la investigación fue de tipo aplicada en conjunto con la metodología OSSTMM; mismas que se las aplicó a través de tres fases. La primera fase fue la valoración dónde se conoció los sistemas de la empresa y actividades que realiza, adicionalmente se realizó una entrevista al jefe de TICS para obtener información certera. La segunda fase fue la ejecución donde se realizó el escaneo de la red y la tercera fase que fue el informe el cual sirvió de apoyo para identificar las vulnerabilidades de la red.

Como resultado se determinaron las amenazas a las que está propensa la red y cuál era el nivel de impacto que estas tendrían, se llegó a la conclusión que en la red informática del GAD de la ciudad de Vinces existen varias vulnerabilidades y falencias; por ende sus sistemas no están totalmente seguros, incluso algunos equipos no están configurados adecuadamente por tal motivo se recomendó implementar software que mejoren la seguridad y gestionar de mejor manera la configuración de los equipos ya que representan un riesgo para la información que almacenan en ellos.

Palabras clave: vulnerabilidad, red informática, openvas, seguridad, amenazas.

Abstract

As time has passed, cases of hacking of information systems and computer networks have increased since they have vulnerabilities that are exploited by computer criminals to gain access to systems and appropriate information from organizations. The present investigation sought to determine the vulnerabilities of the computer network through the OpenVAS tool of the GAD of the city of Vinces, with this tool a scan was carried out, which was executed through the GreenBone graphic environment. The type of methodology with which the research was developed was applied in conjunction with the OSSTMM methodology; which were applied through three phases. The first phase was the assessment where the company's systems and activities carried out were known, in addition, an interview was conducted with the head of TICS to obtain accurate information. The second phase was the execution where the network scan was performed and the third phase was the report which served as support to identify network vulnerabilities.

As a result, the threats to which the network is prone were determined and what was the level of impact that these would have, it was concluded that in the computer network of the GAD of the city of Vinces there are several vulnerabilities and shortcomings; therefore their systems are not totally secure, even some equipment is not configured properly for this reason it was recommended to implement software that improves security and better manage the configuration of the equipment since they represent a risk for the information they store in them.

Keywords: vulnerability, computer network, openvas, security, threats.

Contenido

Planteamiento Del Problema 7

Justificación 9

Objetivos 10

Objetivo General: 10

Objetivos Específicos: 10

Líneas De Investigación 11

Marco Conceptual 12

Sistemas De Información 13

Funciones De Los Sistemas De Información 14

Red Informática 15

Tipos De Redes 16

Componentes De Una Red Informática 19

Vulnerabilidades Informáticas 20

Tipos De Vulnerabilidades Informáticas 20

Comunicación O Red: 20

Física: 21

Humana: 21

Emanaciones: 21

Hardware: 21

Software:..... 22

Naturales:..... 22

Amenazas..... 22

Riesgo..... 23

Seguridad Informática..... 23

Métodos De Seguridad Informática..... 24

Seguridad de Hardware:..... 24

Seguridad de Software:..... 25

Seguridad de red:..... 25

Evaluación De Vulnerabilidades..... 25

Escaneo De Red..... 26

OpenVAS..... 26

Marco Metodológico..... 27

Resultados..... 28

Discusión De Resultados..... 36

Conclusiones..... 38

Recomendaciones..... 39

Referencias..... 41

Anexos..... 43

Figura 1 *Ciclo de la Información* 14

Figura 2 *Resultado de Vulnerabilidades y Amenazas* 23

Figura 3 *Inicio del Escaneo en OpenVAS* 29

Figura 4 *Gráficos de los Resultados* 30

Figura 5 *Lista de Vulnerabilidades* 30

Figura 6 *Lista de Vulnerabilidades* 31

Figura 7 *Lista de Vulnerabilidades* 31

Figura 8 *Organigrama Funcional del GAD Vinces* 43

Figura 9 *Entrevista al Jefe del Dpto. de Sistemas* 44

Figura 10 *Proceso de Análisis de la Red* 44

Figura 11 *Iniciar OpenVAS* 44

Figura 12 *Inicializando OpenVAS* 44

Figura 13 *Interfaz Greenbone desde el Navegador* 44

Tabla 1 *Cantidad de Vulnerabilidades* 32

Tabla 2 *Vulnerabilidad Alta 1* 32

Tabla 3 Vulnerabilidad Alta 2 ..... *33*

Tabla 4 Vulnerabilidad Media 1 ..... *33*

Tabla 5 *Vulnerabilidad Media 2* 34

Tabla 6 *Vulnerabilidad Baja 1* 34

Tabla 7 *Vulnerabilidad Baja 2* 35

Tabla 8 *Análisis General De La Red* 37

Tabla 9 *Análisis Económico* 40

Planteamiento Del Problema

La era digital en la que se está viviendo ha generado a nivel mundial que las técnicas de cibercrimen se extiendan por intenciones lucrativas, los ataques a las redes informáticas cada vez son más comunes en organizaciones públicas sean éstas grandes o pequeñas. Las empresas pueden estar susceptibles a estas amenazas debido a que no se le da la importancia necesaria a la seguridad de la información y por tal motivo no se tiene el debido cuidado, ya sea de sus servidores, aplicaciones o software; por otro lado, también hay casos en los que los equipos o sistemas son de versiones muy antiguas.

Los ataques a las redes informáticas de una empresa pueden ser motivados por diversas causas y consisten en extorsiones por información previamente cautiva; hechos que causan que la empresa sea afectada al no poder hacer uso de su información. Se detienen las actividades laborales teniendo como consecuencia baja confiabilidad de parte de los usuarios, así como también la pérdida de recursos económicos.

En el Ecuador existen empresas que no hacen uso de sistemas de seguridad para proteger sus bases de datos de cualquier tipo de amenaza informática, ya sea por el costo de inversión que representa la implementación de estos sistemas para la empresa o simplemente no le dan mayor importancia. En otros casos hay situaciones en las que la institución hace uso de un software gratuito, sin embargo, estos no ofrecen garantía referente a la integridad de la información, ni soporte de parte del autor, siendo esta una desventaja.

Desde el año 2020 se presenta un significativo incremento en ataques a sistemas informáticos relacionados al sector público, los cuales han ocasionado situaciones tales como; sistemas colapsados, retención de base de datos, alteración y hurto de información, entre otras.

Tal es el caso como el que se presentó en la conocida empresa CNT (Corporación Nacional De Telecomunicación), institución que a mediados del mes de julio del 2021 fue víctima de un ataque informático (hackeo), en el cual invadieron parte de los equipos de la empresa, introduciendo virus de tipo ransomware a sus sistemas, cuyo resultado fue alteraciones de software y daños tanto en la red como en las bases de datos; viéndose interrumpidos varios de sus servicios tales como atención al cliente, facturaciones y recargas (Ortiz, 2021)

El Gobierno Autónomo Descentralizado Municipal del Cantón Vinces se localiza en las calle Sucre y 9 de octubre, es una institución pública de autonomía administrativa y financiera, se encarga de gestionar y ejecutar obras públicas, con los recursos públicos gestionados por ingresos propios y por parte del Estado, cuya finalidad es beneficiar a los habitantes que residen en este cantón, efectuando a cabalidad las competencias determinadas por el Código Orgánico de Organización Territorial, Autonomía y Descentralización en relación con la Constitución de la República del Ecuador.

El presente caso de estudio se plantea realizar Análisis de las vulnerabilidades de la red informática, mediante la herramienta OpenVAS en el GAD de Vinces, estableciendo como un elemento crítico incrementar la seguridad para proteger la información importante de esta institución pública, debido a que una red institucional no solo necesita tener enlazados a los usuarios, sino también preservar la información que se gestiona en ella.

Justificación

Existen diversos tipos de análisis que se pueden realizar a una red informática con el fin de evidenciar las incidencias de la red; cada uno está orientado a llevar a cabo análisis con distintas perspectivas, mediante el diagnóstico es posible mostrar la información recopilada ya sea mediante informes o gráficos; los mismos que sirven a los administradores del departamento de TICS, para tomar las medidas pertinentes y de esta manera se pueda prevenir intrusiones a la red preservado la integridad y disponibilidad de la información. Uno de estos métodos es el escaneo de la red se podría evidenciar las fragilidades informáticas y posibles amenazas de la misma; de esta manera se evitarán ataques o suplantaciones.

Dentro del GAD de la ciudad de Vinces, se gestiona la información de cada departamento y usuario; dicha información es de suma importancia para la institución por lo que en la mayoría de los casos se maneja de manera confidencial. El presente estudio de caso se enfocará en realizar un análisis a la red informática del GAD Municipal de la ciudad de Vinces, haciendo uso de la herramienta OpenVAS, la herramienta es utilizada para realizar escaneo de redes, teniendo como propósito analizar las amenazas y vulnerabilidades de las mismas; esto permite alertar al personal del departamento de sistemas acerca de las afectaciones que pueda ser objeto la red y dar a conocer los efectos informáticos que pueden provocar en los sistemas si no se ponen en marcha las debidas normas de seguridad.

En el presente caso de estudio, se categorizan diferentes temas de trabajos sobre las amenazas y vulnerabilidades de red del GAD de Vinces, así como también las medidas de seguridad para proporcionar un estudio de caso en el campo de interés. Como resultado, se obtienen nuevas ideas para los sistemas de seguridad de redes de esta institución pública, con lo cual se podrá ser más eficaz y eficiente con el uso de la información.

Objetivos

Objetivo General:

Determinar las vulnerabilidades de la red informática mediante la herramienta OpenVAS en el GAD de la ciudad de Vinces.

Objetivos Específicos:

- Aportar con conocimientos teóricos que permitan reflejar las estrategias de seguridad informática.
- Identificar las amenazas y vulnerabilidades existentes en la red informática del GAD de Vinces.
- Proponer mecanismos de seguridad para mitigar las vulnerabilidades y amenazas de la red informática en el GAD de la ciudad de Vinces.

Líneas De Investigación

El presente caso de estudio basa el desarrollo de su investigación bajo la orientación de la línea de investigación denominada “sistemas de información y comunicación, emprendimiento e innovación”; en conjunto con la sublínea de investigación “redes y tecnologías inteligentes de software y hardware”. Comprendiendo así, el proceso de recolección y gestión de información con la finalidad de que la investigación efectúe la política de supervisión de la institución.

Esta investigación se relaciona directamente con dichas líneas de investigación ya que al hablar de sistemas de información se refiere a la manipulación o administración de información mediante un grupo determinados de dispositivos computacionales. Además, a estos sistemas se los suele considerar seguros siempre y cuando ellos mantengan la disponibilidad e integridad de la información, para mantener estas características se realizan implementaciones de medidas de seguridad, así como también de softwares destinados a estas acciones.

En cuanto a la sublínea de investigación bajo la cual se rige este estudio, en relación a las redes informáticas podemos resaltar que estas estructuras tienen como objetivo transportar datos, compartir recursos e información y a su vez ofrecer un servicio; estos procesos son posible gracias a que los equipos que las componen se encuentran interconectados. Es necesario que la información que se transporta a través de la red sea siempre respaldada ya que es posible que la red sea vulnerable en ciertas áreas.

Es por esto que se determinó realizar la investigación en el GAD de la ciudad de Vinces, para la obtención de datos actualizados del estado de la red con la finalidad de identificar las amenazas existentes en la misma.

Marco Conceptual

El Gobierno autónomo descentralizado correspondiente a la municipalidad de la ciudad de Vinces inauguró sus funciones desde el año 1909. La edificación se encuentra actualmente ubicada en las calles Sucre S/N y 9 de octubre. Donde ofrece los servicios relacionados a catastros, ordenación territorial tales como es la legalización de predios, trámites relacionados al servicio de agua potable, entre otros.

Los sistemas con los que se tienen sistematizados los procesos del GAD de Vinces facilitan a los trabajadores designados de cada departamento el ingreso de datos a tiempo real. La red informática que se encuentra distribuida en el edificio es cableado simple, esta red está integrada por un servidor SQL Server 2008 el cual trabaja con motor de base de datos CentOS y un servidor Windows Server 2012 que trabaja con Postgres13. Además, cuenta con un total de 12 Switches incluido el principal y seis routers.

Entre los principales sistemas con los que se trabaja se encuentra el Sistema Nacional para la Administración de Tierras (SINAT) en conjunto con el Sistema Integral de Catastros (SIC) y el sistema de cobro de agua potable. Estos últimos almacenan importante información por lo que es necesario velar por la seguridad de la misma, motivo por el cual se hace uso de sistemas defensores como antivirus y firewalls como el ClearOS.

Existen varios escenarios por los cuales se puede ver afectada la integridad y disponibilidad de los datos de una organización y es por esto que se considera necesario aplicar los protocolos de seguridad correspondientes dado que cada vez se incrementan los ataques a red tales como el secuestro o robo de información.

Sistemas De Información

Al hacer referencia al término sistemas de información hablamos de un grupo de elementos informáticos, el cual debe tener una funcionalidad ordenada manteniendo como objetivo una correcta gestión de datos e información; por tanto, debe permitir que esta sea procesada fácilmente. Cada sistema de información está conformado por un conjunto de recursos interrelacionados que trabajan al mismo tiempo, colocados de manera estratégica en relación al propósito para el que es destinado; el cual puede ser recolectar información personal, procesar datos, ordenar documentos, entre otras funciones (editorial etece, 2021)

Un sistema de información tiene como principales objetivos la gestión y administración de los datos e información que almacena. Es importante que pueda recuperar siempre los datos y que además se tenga acceso a ellos con total seguridad.

Dentro de las organizaciones, los sistemas de información son vitales ya que comprenden una constante comunicación entre departamentos y las diversas actividades que se llevan a cabo dentro de las empresas, incluyendo la información que cada una de estas produce. A partir de los datos procesados se generan informes precisos, los grupos administrativos debaten sobre los resultados presentes en dichos informes y basándose en ellos proceden a realizar el proceso de toma de decisiones (Peiró, 2020)

Podemos deducir que los sistemas de información componen una parte fundamental dentro de las organizaciones, considerando que aportan confiabilidad e integridad en lo que se refiere a los datos, ya que son capaces de brindar soporte de la información captada durante las actividades. Es por esto que a la hora de decidir sobre la empresa se los considera de gran relevancia dado que facilitan la comunicación de la información y, además, permiten conocer los niveles de productividad de las organizaciones.

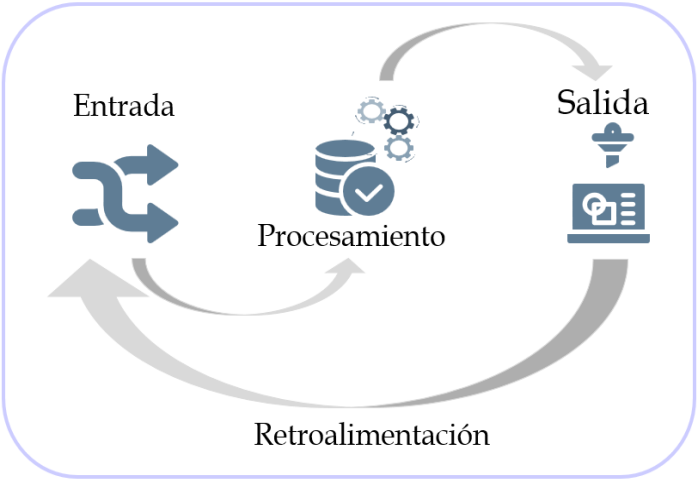
Funciones De Los Sistemas De Información

Cumplen con tres acciones importantes, a través de las cuales se genera información a manera de informes o estadísticas. La organización necesita dichos reportes para la toma de decisiones, administración de actividades, estudio de los inconvenientes que se presentan o para la innovación en productos y servicios. Las acciones son las siguientes:

- La entrada, que es el ingreso o captura de datos relevantes de la organización o del medio con el fin de que el sistema se encargue de procesarlos.
- El procesamiento, en esta acción lo que el sistema hace es transformar los datos de manera que las personas puedan entenderlos de una mejor manera.
- La salida, aquí la información que ha sido procesada anteriormente se transporta a los trabajadores o colaboradores que requieran emplearla.

Además, debemos incorporar un proceso de retroalimentación lo cual equivale al producto entregado a miembros de la institución encargados de la organización para que realicen sugerencias y de tal manera sea posible ejecutar las respectivas mejoras en el proceso de entrada (Laudon, 2018)

Figura 1 *Ciclo de la Información*



Red Informática

Según (Tintín-Perdomo et al., 2018), "Se denomina red informática a un grupo de elementos computacionales (hardware o software) que se encuentran interrelacionados, haciendo uso en tiempo simultáneo de recursos."

Dentro de las redes existen elementos tales como emisor, mensaje, canal y receptores. Gracias a estos elementos se realiza el flujo de datos ya que están en una constante compartición de la información. En cuanto a los emisores y receptores, los papeles de dichos participantes se van intercalando conforme son transportados los datos; es decir, quien en algún momento cumple el rol como emisor pasará a ser receptor y viceversa.

En general, las redes establecen comunicación entre los recursos mediante un conjunto sincronizado de dispositivos que se encargan de ejecutar la transmisión de ondas electromagnéticas; mismas que trasladan a manera de paquete los datos que se necesita compartir manteniendo así la comunicación entre procesos y departamentos de la entidad.

Al diseñar e implementar una red informática en una empresa u organización, se busca sistematizar los procesos que se desarrollan durante las actividades tales como registrar datos de los clientes, actualizar información o verificarla para dar respuestas a consultas de usuarios. Desde esta perspectiva lo que hace una red informática es aportar en varios aspectos como mejorar la eficacia de la entidad dado que se disminuye el tiempo de respuesta a clientes. Otra ventaja que se obtiene es que la información se almacena y clasifica mejor de tal manera que se facilita la búsqueda en el caso de querer encontrar un dato específico.

Adicionalmente, si los recursos de la red están correctamente distribuidos se evitan fallas en la misma y las actividades de los empleados no serán interrumpidas, con lo cual aumentará la productividad de la entidad.

Tipos De Redes

Existen diversas perspectivas desde las cuales se puede clasificar a las redes, entre las cuales se encuentra según su alcance geográfico, según su medio de propagación y según su topología, las cuales se describen a continuación:

Según su medio de propagación:

Hay de tipo alámbricas, donde la comunicación entre determinados recursos de la red es mediante cableado. Y de tipo inalámbricas, donde la comunicación entre los equipos es a través de ondas de señal.

Según su tamaño o alcance:

- **PAN**, estas siglas se traducen al español como “Red de área personal”. Esta se caracteriza por tener un alcance de escasos metros y se integra por dispositivos manipulados únicamente por un usuario.
- **WPAN**, estas siglas se traducen al español como “Red inalámbrica de área personal”. Tiene las mismas características que una red PAN con la diferencia que se propaga a través de medios inalámbricos.
- **LAN**, estas siglas se traducen al español como “Red de área local”. Los equipos interconectados que pertenecen a esta red se encuentran ubicados en un área reducida. Son las de menor alcance ya que tienen cobertura geográfica en un rango entre los 200 metros hasta 1 kilómetro.
- **WLAN**, estas siglas se traducen al español como “Red de área local inalámbrica”. Es como una red LAN, pero esta hace uso de recursos inalámbricos para establecer comunicación.

- **CAN**, estas siglas se traducen al español como “Red de área de campus”. Está compuesta por un conjunto de dispositivos tecnológicos de elevada velocidad y el espacio donde se interconectan las redes está delimitado geográficamente.
- **MAN**, estas siglas se traducen al español como “Red de área metropolitana”. Se caracteriza por la velocidad de ancho de banda y aunque se delimita su alcance, esta abarca más territorio en comparación con una red de campus.
- **WAN**, estas siglas se traducen al español como “Red de área amplia”. Estas redes son las que manejan las empresas proveedoras de internet (Lederkremer, 2019)

En la actualidad tienen un alto protagonismo en nuestro diario vivir, ya que las utilizamos en diversos ámbitos como por ejemplo el entorno en el que laboramos, en centros educativos, sin dejar de mencionar los espacios públicos. Definitivamente son de gran ayuda al momento de querer compartir recursos e información como por ejemplo si se requiere compartir un documento, enviar mails o simplemente mandar a imprimir. Son actividades sencillas, pero desde el punto de vista empresarial son de gran valor ya que esto influye en el desempeño de la empresa.

En el caso que una organización o empresa desee poner en marcha una red informática buscando mejorar el entorno laboral de sus colaboradores debe procurar aplicar una red con las características y recursos que vayan de acorde a sus necesidades. Para escoger el tipo de red adecuado se debe tomar en cuenta varios elementos, hay que fijarse en aspectos como la cantidad de ordenadores que requieren, el tipo de sistemas o aplicativos que se ejecutarán y a partir de esto escoger planes de internet de acorde al consumo de ancho de banda, decidir la calidad de ordenadores que se necesite y en la colocación estratégicas de los equipos.

Además, es indispensable conocer la infraestructura de la entidad. Se debe conocer con cuántos pisos cuenta, el número de departamentos y la forma en la que están distribuidos. A partir de este punto se puede realizar un diseño de cómo se distribuirá la red y cada uno de los equipos que van a integrarla; así podrían inclinarse por un tipo de red.

Según su topología física las redes pueden dispersarse de varias formas.

Limones (2021), menciona que pueden ser a manera de:

- **Bus:** Se comparten los datos mediante una sola vía de enlace a la que todos los equipos están conectados.
- **Anillo:** En esta red el grupo de computadores establecen conexión haciendo uso de un cable el cual se distribuye de forma circular dando aspecto de anillo.
- **Estrella:** Por lo contrario de las redes anteriores, aquí cada ordenador tiene su propia vía de comunicación.
- **Malla:** Cada ordenador está conectado al resto de ordenadores, es decir todos se comunican con todos.
- **Híbrida:** Hace referencia a la implementación de dos o más topologías simultáneamente.
- **Árbol:** Es lo que se conoce como árbol invertido ya que la comunicación se desplaza a todos los ordenadores de manera jerárquica e inicialmente desde la raíz.

Los dirigentes de empresas buscan constantemente estrategias para potenciar su productividad y sin duda las redes informáticas aportan en ello. Al igual que el disponer de lugares y recursos adecuados para los empleados ayuda su desenvolvimiento operacional. Cabe mencionar que también es importante que se tenga presente el costo económico que esto significa para la

empresa y por supuesto saber si sus dirigentes están dispuestos a realizar la inversión dado que esto puede influir en la calidad de equipos y en la cantidad de equipos que dispongan adquirir.

Componentes De Una Red Informática

Es de conocimiento que cuando iniciaron las redes, aplicarlas representaba un alto costo de inversión debido a los precios, a pesar de que no eran tan avanzadas como ahora, no eran capaces de almacenar datos a gran escala y a esto le sumamos las limitaciones que en ese entonces presentaban. Como ya se mencionó antes, para que una red informática trabaje de manera ideal debe estructurarse con los equipos tecnológicos que mejor convengan y para hacer que funcione debe contener elementos básicos.

De la parte correspondiente a hardware se puede mencionar tarjetas de conexión de red, estaciones de trabajo, servidores, puentes de conexión, routers, entre otras cosas. En lo relacionado a software podemos destacar elementos como aplicaciones de oficina, programas y sistemas manejadores de base de datos. Con el paso de los años la tecnología de los equipos ha aumentado por ende la innovación en ellos es continua es por esto que al adquirir ordenadores y otros dispositivos se debe considerar que tan actual es el modelo ya que se pueden presentar casos en los que sea necesario cambiar piezas y si el dispositivo ha sido descontinuado por sus fabricantes será imposible repararlo (Lederkremer, 2019)

Es imprescindible que las personas encargadas de administrar la red, conozcan a fondo el tipo de operaciones a las que se dedica la empresa para escoger equipos con viabilidad de acorde a estas. Una vez que haya consolidado la red en las instalaciones de la empresa los administradores deben poner en marcha las normas de seguridad correspondientes.

En cuanto al mantenimiento de la red, este puede realizarse de forma preventiva, consiste en el monitoreo de la red de forma periódica para detectar a tiempo los fallos y así velar por la estabilidad de los equipos.

También se puede realizar mantenimiento correctivo, el cual consiste en el reemplazo o reparación de alguna parte de la red que se haya roto. Y por último el mantenimiento predictivo, que como su nombre lo indica lo que hace es predecir posibles fallos desde perspectivas como la temperatura o corriente eléctrica (Uribe, 2022)

Vulnerabilidades Informáticas

Cuando nos referimos a una vulnerabilidad desde el punto de vista informático, se habla de errores o sistemas de información poco robustos y esto provoca que los sistemas de una empresa estén más propensos a cualquier tipo de amenaza cibernética. Evidentemente esto significa un obstáculo para mantener a salvo la información ya que afecta directamente la disponibilidad e integridad de los datos almacenados (INCIBE, 2017)

Tipos De Vulnerabilidades Informáticas

Las vulnerabilidades que podemos presenciar en una red informática o en algunos sistemas son de varios tipos. Las podemos clasificar según sus rasgos y se describen a continuación:

Comunicación O Red:

Este tipo de vulnerabilidad puede darse al tener los recursos informáticos ubicados en departamentos de fácil acceso y sin verificar el ingreso de personas autorizadas. En este caso, bastará que la persona que infringe los equipos tome el mandato de uno de ellos para posteriormente extenderse a toda la red informática (Segundo Galindo, 2017)

Física:

Cuando se presentan casos donde una persona sin importar si forma parte de la empresa o no, ingresa a los equipos de manera física y toma posesión del mando de estos sin autorización. Es común que estas vulnerabilidades sean aprovechadas por trabajadores de la misma entidad, ya que les resulta sencillo desplazarse entre las estaciones de trabajo y tienen el conocimiento del modelo de la red al igual que de los equipos informáticos de mayor relevancia para la empresa (Romero Castro et al., 2018)

Humana:

Estas vulnerabilidades tienen que ver con la configuración y parametrización. Cuando se presentan casos donde al realizar la instalación de los equipos y sistemas, se los deja funcionando con la configuración por defecto del fabricante; como por ejemplo aplicaciones de servidores, programas e incluidos firewalls. La actualización de sistemas, es otro aspecto que se debe tomar en cuenta debido a que existen empresas que no actualizan los sistemas y posiblemente hacen uso de una versión antigua la cual no es tan segura. Estas vulnerabilidades pueden prestarse para a la infiltración de código malicioso como las inyecciones de código en SQL, Cross Site Scripting, Denegación de servicios, entre otros (Restrepo Zuluaga, 2018)

Emanaciones:

Estas se dan cuando la red está susceptible a radiaciones electromagnéticas cuyo objetivo es decodificar o editar los datos que circulan a través de la red (Segundo Galindo, 2017)

Hardware:

Se las cataloga como la probabilidad de que algún elemento físico de la red llegue a presentar falencias, puede ser por funcionamiento o tiempo de vida útil. Esto puede significar una detención total o parcial de la red puesto que el tiempo para reemplazar el equipo puede tardar.

Software:

Estas vulnerabilidades hacen referencia a los errores conocidos como bugs, los cuales son fallos o defectos que se presentan en los sistemas, ocasionando interrupciones en el funcionamiento normal de estos (Restrepo Zuluaga, 2018)

Naturales:

Se considera una vulnerabilidad natural aquellos daños o pérdidas que son consecuencia de catástrofes naturales como incendios, lluvias o movimientos sísmicos. Mayormente tienen mayor impacto cuando la empresa no cuenta con medidas de prevención y tampoco se ha realizado una evaluación de la ubicación geográfica de la red (Segundo Galindo, 2017)

En ocasiones el administrador de la red no realiza una gestión correcta de los recursos, dejando ciertas áreas desprotegidas. Si nos fijamos en la cantidad de procesos y funciones sistematizadas que hoy en día hacen que las empresas lleven a cabo sus actividades normales, podemos decir que la mayoría de empresas dependen en un alto porcentaje del buen servicio de la red. A estas vulnerabilidades las relacionamos al hecho de ingreso sin autorización, hurto de perfiles de usuarios, infestación por medios extraíbles y el robo, modificación o eliminación de datos.

Sin duda una inadecuada gestión o fallo de la red de cualquier índole puede ser aprovechada por intrusos que buscan afectar a la empresa puesto que los empleados no podrían desempeñar con normalidad sus actividades, y para cualquier entidad este tipo de fallas no solo repercuten en la pérdida de tiempo sino también puede reflejarse en pérdidas económicas.

Amenazas

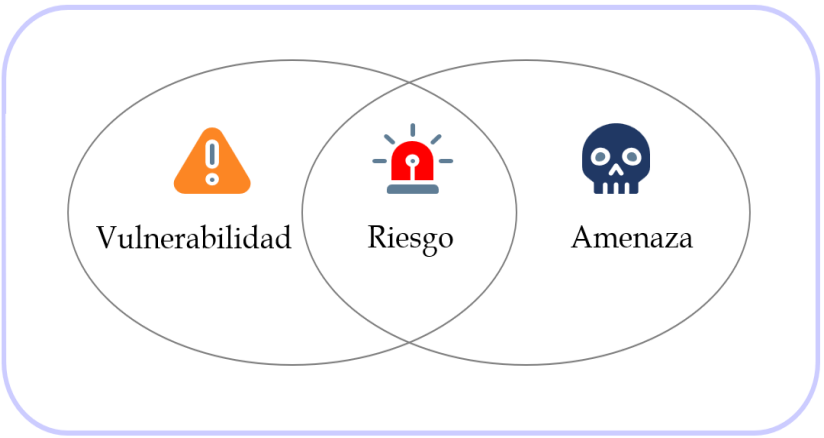
Las amenazas pueden estar presentes tanto en la parte interna como en la externa y son todas aquellas acciones que se realizan con el fin de quebrantar la seguridad de los sistemas de

información aprovechando las vulnerabilidades que estos presentan. A partir de estas amenazas pueden provenir los ataques como el robo y malware; acontecimientos físicos como catástrofes naturales o recalentamiento de equipo; y la negligencia en las decisiones como la mala administración de permisos a usuarios (INCIBE, 2017)

Riesgo

En informática se denomina riesgo a toda aquella posibilidad que una amenaza tiene de ejecutarse valiéndose de las vulnerabilidades de activos o conjunto de activos y que esto por ende atente contra la integridad de una organización o genere pérdidas en ella. Los riegos se pueden clasificar según el impacto que produjo: afectación en las operaciones, afectación a la reputación y afectaciones legales a la organización (Arévalo Moscoso et al., 2017)

Figura 2 *Resultado de Vulnerabilidades y Amenazas*



Seguridad Informática

Al hablar de seguridad informática, se debe entender que la seguridad informática se encarga del medio informático. La seguridad informática se define como la disciplina que se encarga de plantear y diseñar normas, procedimientos, métodos y técnicas con el fin de obtener un sistema de información seguro, confiable y sobre todo que tenga disponibilidad.

Actualmente la seguridad informática tiene como principal tarea minimizar riesgos, procurando mantener íntegra la información proveniente de las diversas áreas, puede ser de la entrada de datos, del medio que transporta la información, del hardware que se usa para transmitir y recibir información.

Métodos De Seguridad Informática

Existen diversos tipos de seguridad informática que una empresa debe tener en cuenta para evitar pérdida de datos. Con tantas cosas ocurriendo en Internet, se vuelve extremadamente necesario asegurar el contenido de nuestra red y nuestras comunicaciones ante posibles problemas de pérdida o interceptación de datos. La seguridad informática es la rama de la tecnología de la información que se ocupa de la protección de datos en una red, sus comunicaciones o una computadora independiente. (Universidad Internacional de Valencia, 2018)

Estos son tres diferentes tipos de seguridad informática:

Seguridad de Hardware:

Todo proceso informático tiene como base para su funcionamiento el uso de cualquier tipo de equipo físico o emulado, ya sea presencial o virtualizado, mediante el cual interactúa el usuario final. De tal manera, podemos deducir que la seguridad de hardware es un tipo de seguridad informática orientada a velar por la protección del equipo donde se abarca lo referente a la integridad del equipo, como de la información que almacena y la manera en esta se transmite. Entre los modelos de seguridad basados en hardware podemos mencionar la autenticación, biométrica, claves y módulos de plataformas de confianza y de seguridad hardware(viewnext, 2018)

Seguridad de Software:

Este tipo de seguridad está dirigida a implementar normas que ayuden a proteger los sistemas de inconvenientes en la ejecución de cualquier sistema o programa que haya sido instalado. Por tanto, se deduce que la seguridad de software es la puesta en marcha de buenas prácticas como el hacking ético, protección de datos y de programas y aplicaciones. La seguridad de software se utiliza para proteger el software contra ataques maliciosos de hackers y otros riesgos, de forma que nuestro software siga funcionando correctamente sin que afecten este tipo de riesgos potenciales (Universidad Internacional de Valencia, 2018)

Seguridad de red:

La seguridad de red se refiere a cualquier actividad diseñada para proteger la red. Tiene como finalidad predefinir filtros que mantengan a salvo los componentes de la red, datos almacenados e información transmitida, previo a que intrusos puedan ingresar al sistema. Este tipo de seguridad propone salvaguardar la información durante la transmisión o recepción, disminuyendo las posibilidades que ésta sea captada por atacantes. Entre las herramientas que se usan en este caso son Firewalls, Anti Spam y VPN (viewnext, 2018)

Evaluación De Vulnerabilidades

El proceso de evaluación de vulnerabilidades es aquel mediante el cual se busca señalar, clasificar y medir las vulnerabilidades. Por lo tanto, las evaluaciones de vulnerabilidades nos proporcionan información de los riesgos a los que se está expuestos facilitándonos la gestión de los mismos para luego iniciar procesos de mitigación. Existen métodos mediante los cuales se puede llevar a cabo una evaluación de vulnerabilidades, uno de ellos es el escaneo basado en red.

Escaneo De Red

Los escaneos basados en red combinan el descubrimiento de hosts y servicios con la enumeración de vulnerabilidades. En este tipo de evaluación se identificarán los distintos dispositivos que componen la red, determinando su importancia en el sistema y posibles vulnerabilidades. Una característica de este tipo de evaluación es el uso de la técnica del fingerprinting, mediante la cual se averigua el tipo y versión del dispositivo a partir de las respuestas que este proporciona, pudiendo luego buscar vulnerabilidades específicas para ese tipo de dispositivo (Borja Villora, 2018)

OpenVAS

OpenVAS (Open Vulnerability Assessment System – Sistema Abierto de Evaluación de Vulnerabilidades) Es una herramienta de código abierto que nos brinda varias opciones en lo relacionado al análisis de vulnerabilidades, ayudándonos a determinar las amenazas de la red y a partir de los resultados que nos brinda se efectúan operaciones con el fin de mejorar los niveles de seguridad de los sistemas (Altube Vera, 2020)

Esta herramienta prevendrá ante vulnerabilidades al identificar los errores de seguridad ya que ofrece características a través de su entorno gráfico Greenbone Security Desktop como: realizar un escaneo de forma simultánea en varios equipos, soporta el protocolo SSL, implementar escaneos programados, detener o reiniciar las tareas de escaneo en cualquier momento, administrar usuarios desde la consola, reportes claros y completos.

Esta herramienta clasificará las vulnerabilidades dependiendo del nivel de incidencia y riesgo que se encuentren presente: alto (75% -100%), medio (50%-74%) y bajo (menores o iguales al 49%).

Marco Metodológico

El tipo de investigación que se aplicó al presente caso de estudio es de tipo aplicada dado que es aquella que tiene como objetivo resolver problemas concretos y prácticos de la sociedad o las empresas. La investigación aplicada, por tanto, permite solucionar problemas reales.

Para el desarrollo de la investigación se tomó como referencia la metodología OSSTMM (Manual de Metodología de Pruebas de Seguridad de Código Abierto) que es una metodología para pruebas de seguridad, mantenida por el Instituto de Seguridad y Metodologías Abiertas (ISECOM). Esta metodología fue adaptada al perfil de la investigación y en este caso se segmenta en tres fases: valoración, ejecución e informe.

- **Fase 1:** Es la fase de valoración y consiste en tener conocimiento general de la entidad en cuestión y del departamento de TICS, al igual que tener noción de la ejecución del sistema informático.
- **Fase 2:** La fase de ejecución consiste en realizar evaluaciones mediante la ejecución de softwares para realizar pruebas y obtener evidencias. Además, en esta etapa se realiza la detección de las vulnerabilidades.
- **Fase 3:** La última fase es la del informe donde se muestra los resultados preliminares y las vulnerabilidades encontradas.

Con el fin de recaudar información confidencial y verídica acerca de las características de la red informática, se efectuó una entrevista al jefe del departamento de sistemas. Además, se hizo uso de fuentes bibliográficas con el objetivo de recopilar documentos y así tener un flujo concordante y ordenado de información correspondientes a las vulnerabilidades de red; está compuesta de varios sitios de información donde se incluyen libros electrónicos, tesis, artículos, revistas y sitios webs confiables correspondientes a publicaciones de los últimos cinco años.

Resultados

La metodología anteriormente presentada fue aplicada a la red informática del GAD de Vinces, obteniendo los siguientes resultados:

Fase 1. Valoración

Esta fase se enfocó en conocer las áreas de la institución, el organigrama de la empresa (Anexo 1), servicios que ofrece; así como lo referente al funcionamiento al área de sistemas de información donde se incluye arquitectura organizacional, operaciones, recursos tecnológicos, servicios y el ambiente laboral, donde se realizaron procedimientos tales como:

- Determinación del funcionamiento de la red de la entidad y como se encuentra distribuida de acuerdo a las estrategias operacionales de la misma; corroborando así su desempeño.
- Indagación sobre la gestión de la red, actualizaciones periódicas de los sistemas y respaldo de información a cargo de los integrantes del departamento de sistemas.
- Observación de los componentes físicos de la red y como se encuentran distribuidos en la edificación. Donde pudimos constatar que es posible que una persona puede acceder a ellos ya que no cuentan con filtros de seguridad necesarios.

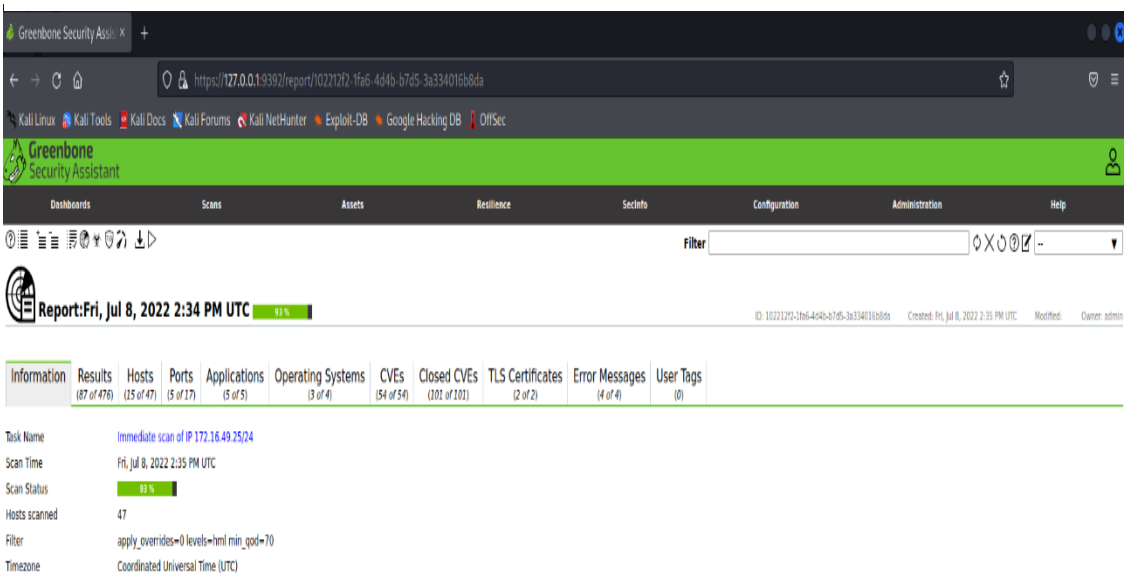
Esta fase se sustentó con la realización de una entrevista realizada al jefe del departamento de sistemas (Anexo 2); con la cual se obtuvo respuestas que sirvieron como parte de la valoración donde se constató que los administradores de la red realizan respaldo de la información diariamente, el mantenimiento a la red se realiza trimestralmente o dado el caso que se presenten fallas en algún equipo este se reemplaza. Además, las normas de seguridad no se aplican en su totalidad en la red y por ende los niveles de seguridad de la misma son bajos.

Fase 2. Ejecución

En esta fase se inicia el proceso de escaneo de la red informática para determinar las vulnerabilidades con la herramienta anteriormente propuesta OpenVAS, la cual nos permite realizar escaneo de toda la red mostrándonos las vulnerabilidades para prevenir posibles ataques informáticos.

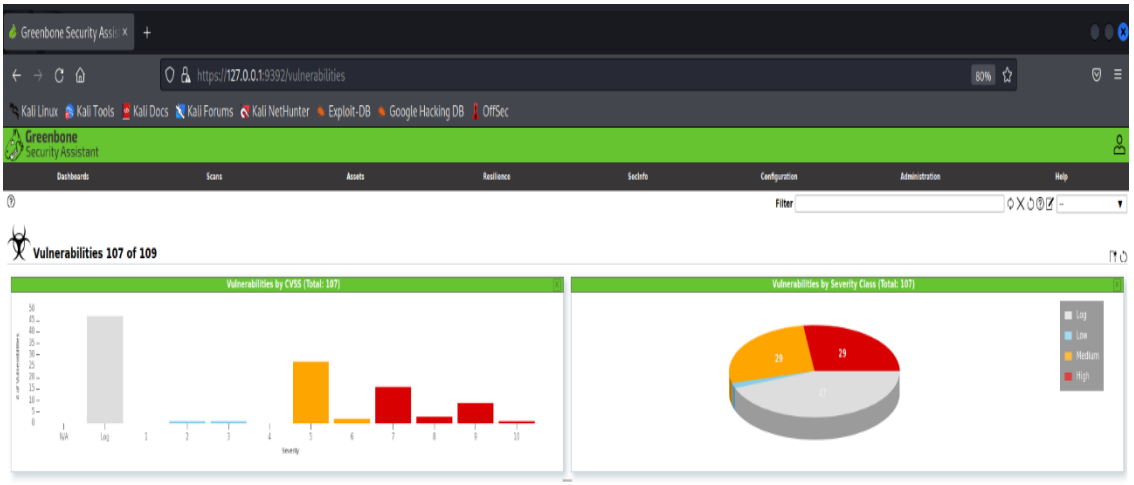
Una vez realizada la configuración correspondiente continuamos con el siguiente paso que fue ejecutar la tarea de escaneo de la red como se muestra en la Figura 3. El escaneo de vulnerabilidades en la red informática del GAD de la ciudad de Vinces, fue realizado el día 18 de Julio a las 14:30 pm y tuvo una duración de 10 minutos.

Figura 3 *Inicio del Escaneo en OpenVAS*



Concluida la etapa de escaneo fue posible observar y evidenciar las vulnerabilidades y amenazas. OpenVAS nos muestra gráficos a manera de barras y pastel como se puede observar en la Figura 4, donde podemos visualizarlas de forma general.

Figura 4 *Gráficos de los Resultados*



Fase 3. Informe

La herramienta OpenVAS también nos muestra un listado detallado de las deficiencias encontradas a través del análisis y estas a su vez se encuentran categorizadas según el nivel de riesgo como se muestra en las siguientes ilustraciones.

Figura 5 *Lista de Vulnerabilidades*

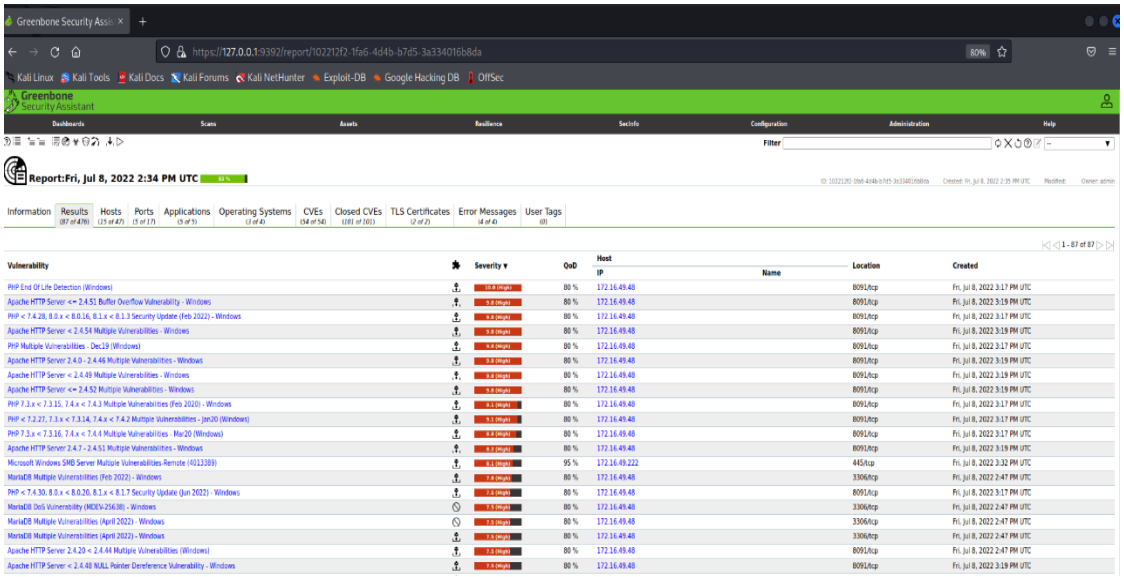


Figura 7 *Lista de Vulnerabilidades*

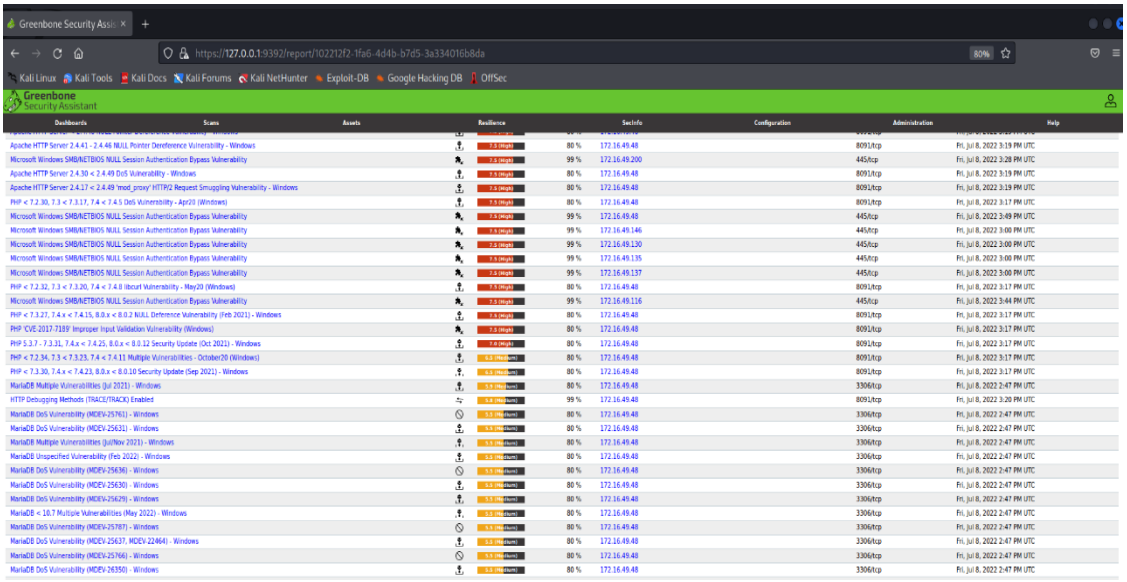
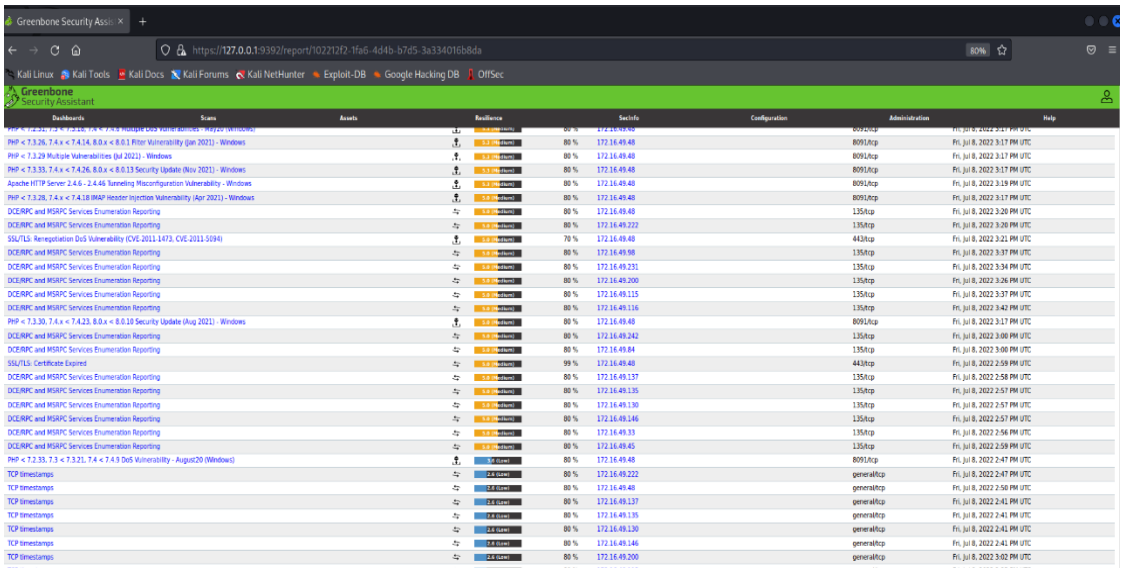


Figura 6 *Lista de Vulnerabilidades*



A continuación, se muestran en una tabla los resultados del análisis con los que se puede establecer la cantidad de vulnerabilidades presentes en la red informática de la GAD de Vinces.

Tabla 1 *Cantidad de Vulnerabilidades*

Escaneo con la herramienta OpenVAS	
Vulnerabilidades encontradas:	60
Información extra:	47
Total de vulnerabilidades	107
Tipo de análisis:	Avanzado
Vulnerabilidades	
Alta	29
Media	29
Baja	2

Detalles de las vulnerabilidades encontradas

Tabla 2 *Vulnerabilidad Alta 1*

Detalle de la vulnerabilidad	
Recursos afectados:	Apache HTTP Server
Versión instalada:	2.4.43
Impacto:	Alto
Detalle:	Se identificó que el servidor está propenso a una vulnerabilidad de desbordamiento de buffer. De forma remota un atacante puede realizar peticiones continuas al servidor que superan el límite de memoria y así causar un desbordamiento de buffer. Este desbordamiento provocaría que el sistema colapse, es decir puede volverse inestable, devolver información errónea o bloquearse. Se determinó la vulnerabilidad en el analizador multiparte mod_lua (r: parsebody () llamado desde Lua Scripts).
Recomendaciones:	Actualizar a la versión 2.4.52 o a una posterior.

Tabla 3 *Vulnerabilidad Alta 2*

Detalle de la vulnerabilidad	
Recursos afectados:	Apache HTTP Server (Múltiples Vulnerabilidades)
Versión instalada:	2.4.43
Impacto:	Alto
Detalle:	Se identificaron las siguientes vulnerabilidades: -Posible solicitud de contrabando -Leer más allá de los límites en mod_isapi -Leer más allá de los límites a través de ap_rwrite () -Denegación de servicio en mod_lua r:pparsebody -Divulgación de información en mod_lua con websockets Se determinó que existen vulnerabilidades en la seguridad de la información.
Recomendaciones:	Actualizar a la versión 2.4.54 o a una posterior.

Tabla 4 *Vulnerabilidad Media 1*

Detalle de la vulnerabilidad	
Recursos afectados:	MariaDB (Múltiples vulnerabilidades)
Versión instalada:	10.5.8
Impacto:	Medio
Detalle:	Se identificaron las siguientes vulnerabilidades: -La vulnerabilidad permite que un atacante con privilegios altos con acceso a la red a través de múltiples protocolos comprometa el servidor MariaDB. - La vulnerabilidad permite que un atacante no autenticado con acceso a la red a través de múltiples protocolos comprometa el servidor MariaDB. Se definió que el servidor está propenso a múltiples vulnerabilidades.
Recomendaciones:	Actualizar a la versión 10.5.12 o una posterior.

Tabla 5 *Vulnerabilidad Media 2*

Detalle de la vulnerabilidad	
Recursos afectados:	Apache HTTP Server (mala configuración)
Versión instalada:	2.4.43
Impacto:	Medio
Detalle:	Se identificó que el servidor tiene una vulnerabilidad por mala configuración de tunelización. Estaba configurado en una URL que estaba canalizando toda la conexión independientemente, lo que permitía que la solicitud posterior en la misma conexión pase sin que posiblemente se configurara la validación, autenticación o autorización de http. Se determinó que la URL no actualizada por el servidor proviene de Mod_proxy _wstunnel
Recomendaciones:	Actualizar la versión más actual 2.4.54

Tabla 6 *Vulnerabilidad Baja 1*

Detalle de la vulnerabilidad	
Recursos afectados:	PHP (vulnerabilidad de denegación de servicio)
Versión instalada:	7.3.12
Impacto:	Bajo
Detalle:	Se identificó que la función phar parse zipfile tenía una vulnerabilidad de uso posterior a la liberación debido al manejo incorrecto de la variable actual_aluas. Se estableció que hay una vulnerabilidad de denegación de servicio en la función phar_parse_zipfile.
Recomendaciones:	Actualizar la versión 7.3.21 o a una posterior.

Tabla 7 *Vulnerabilidad Baja 2*

Detalle de la vulnerabilidad	
Recursos afectados:	TCP (marcas de tiempo)
Versión instalada:	7.3.12
Impacto:	Bajo
Detalle:	Se identificó que el host remoto implementa marcas de tiempo TCP por lo tanto, el tiempo de actividad del host remoto se puede calcular. Se estableció que el host implementa por definición RFC1323VRFC7323
Recomendaciones:	Mitigación. En la configuración del sistema desactive las marcas de tiempo.

Discusión De Resultados

Como se pudo visualizar en las ilustraciones referentes a los resultados, la herramienta OpenVAS a través del proceso de escaneo nos mostró vulnerabilidades de impacto alto, medio y bajo. Se identificó un total de 107 vulnerabilidades mediante las cuales se puedo determinar que los sistemas informáticos que utiliza actualmente el GAD de la ciudad de Vinces tienen varias falencias lo cual reduce los niveles de seguridad.

La mayoría de estas vulnerabilidades están relacionadas a los servidores y los motores de bases de datos utilizados. Entre las principales amenazas que encontró OpenVAS se encuentra la detallada en la Tabla 2 la cual es de impacto alto y podemos deducir que, con el aprovechamiento de esta el servidor está susceptible a que se produzca un desbordamiento de buffer lo cual representaría un gran riesgo; sin embargo, esto se puede mitigar actualizando la versión de este.

La mala configuración es otra de las vulnerabilidades que se pudo evidenciar, tal como se muestra en la Tabla 5, una mala configuración de tunelización siendo esta de impacto medio. Esto provoca que, al existir solicitudes sucesivas a la misma conexión unas sean autenticadas o validadas y otras no. Otro caso de una configuración deficiente es el que se muestra en la Tabla 7, aunque es de impacto bajo permite que se puedan calcular el tiempo de actividad del host.

El jefe del departamento de sistemas del GAD de Vinces durante la entrevista comentó que no se aplican las normas de seguridad en su totalidad, por lo que se considera que los sistemas no están debidamente protegidos ya que no implementan ningún software ni hardware de detección de intrusos. El cuarto de equipos donde se encuentran ubicados los servidores, aunque cuenta con sistema de enfriamiento no está resguardado y los cables pertenecientes a la red no se encuentran organizados de manera ordenada.

Además, los software de seguridad que utilizan son únicamente los que vienen por defecto en los sistemas, como antivirus y firewall.

A continuación, se muestra un análisis general de la red informática:

Tabla 8 *Análisis General De La Red*

Análisis General De La Red	
Infraestructura	Se determinaron las siguientes vulnerabilidades: -No se gestionan de manera adecuada las normas de seguridad. -El cableado no está segmentado por departamentos. -El control de acceso a la entidad y cuarto de equipos no es del todo eficiente.
Programas/Aplicaciones	Se determinaron las siguientes vulnerabilidades: -Los software que se utilizan son únicamente los que vienen preinstalados. - No hay programas para la detección de intrusos. -No se ha gestionado de forma correcta las configuraciones.

Conclusiones

Con el desarrollo de la investigación realizada a la red informática del GAD de Vinces la cual fue analizada utilizando la herramienta OpenVAS se evidenció que existen varias vulnerabilidades y falencias en la red. Estas fallas pueden ser aprovechadas por hackers por lo que los equipos de almacenamiento del GAD están propensos a ingresos de intrusos y estos a su vez pueden sustraer, manipular o divulgar la información.

En la red informática no se aplican normas de seguridad suficientes tanto en sistemas como en equipos que forman parte de la red, considerando el tipo de actividades a la que se dedica la organización, tomando en cuenta la cantidad y la clase de información que tiene bajo su responsabilidad.

Respecto a software de seguridad, la entidad únicamente hace uso de aquellos que vienen por defecto en algunos sistemas, como firewalls y antivirus. También existen equipos que continúan con configuraciones de fábrica como los routers y existen otros en los que la configuración no fue realizada de la manera correcta.

En relación a la estructura de la red se constató que el cuarto de equipos no tiene las seguridades necesarias ya que no cuenta con ningún filtro de seguridad, motivo por el cual se encuentra susceptible a que personas ajenas a la organización puedan acceder a los servidores. Además, el cableado no se encuentra correctamente organizado ni segmentado por departamentos.

Recomendaciones

Una vez concluido el caso de estudio y evidenciadas las vulnerabilidades que presenta la red informática se le recomienda al director administrativo aplicar en la organización todas las normas de seguridad necesarias tanto en sistemas (software) como en equipos (hardware) con el fin de evitar la intromisión de extraños a la red y proteger la información que almacena en sus sistemas.

Cualquiera de las vulnerabilidades identificadas mediante la herramienta representa un riesgo para entidad por tal motivo se recomienda al director de sistemas contratar software que ayuden a reforzar la seguridad de la red, dado que es necesario precautelar la integridad de la información de manera que esta sea más confiable.

También se recomienda mantener los sistemas siempre actualizados y con los parches de seguridad más actuales ya que con cada actualización los desarrolladores buscan realizar mejoras al producto, como las correcciones de vulnerabilidad por lo cual los sistemas estarían menos susceptibles a las amenazas informáticas.

El administrador de la red informática debe gestionar las configuraciones de sistemas para evitar el ingreso de personas o elementos no autorizados, por lo cual se debe implementar un firewall de red que aporte a la administración, que mejore el proceso de monitoreo para de esta manera poder controlar el tráfico. En cuanto al departamento de equipos es recomendable colocar una cerradura biométrica para evitar el acceso de extraños al mismo.

Tomando en cuenta que los hackeos están en aumento se recomienda elaborar planes de contingencia ante posibles ataques informáticos o fallas en la red y así evitar que las actividades y la información de la organización se vean afectadas. Desde esta perspectiva también es importante controlar el ingreso de personas a la entidad para mantener a salvo los equipos.

En base a las recomendaciones planteadas se realizó un análisis económico, con el fin de presentar presupuestos de inversión que pueden significar para la empresa implementar estas soluciones.

Tabla 9 *Análisis Económico*

Recursos		
Nombre	**Descripción**	**Valor**
Firewall de red	Kaspersky	$425/ 1 año
Cerradura Biométrica	Marca Tuya Smart Modelo F2-21	$150,00

Referencias

Altube Vera, R. (2020). Qué es OpenVAS. *OpenWebinars*. https://openwebinars.net/blog/que-es-openvas/

Arévalo Moscoso, F. M., Cedillo Orellana, I. P., & Moscoso Bernal, S. A. (2017). Metodología Ágil para la Gestión de Riesgos Informáticos. *Killkana Técnica*, *1*(2), 31. https://doi.org/10.26871/killkana_tecnica.v1i2.81

Borja Villora, D. (2018). *Evaluación y gestión de vulnerabilidades: Cómo sobrevivir en el mundo de los ciberataques* [Universitat Politècnica de València]. https://riunet.upv.es/handle/10251/106947

editorial etece. (2021). *Sistema de Información - Concepto, tipos, elementos y ejemplos*. Concepto. https://concepto.de/sistema-de-informacion/

Segundo Galindo, J. (2017). *Propuesta de prevención de ataques informáticos de una red LAN, mediante el escaneo de vulnerabilidades* [Universidad Autónoma Del Estado de Mexico]. http://hdl.handle.net/20.500.11799/67650

INCIBE. (2017, marzo 20). *Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?* https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Laudon. (2018). Administración de los Sistemas de Información Capítulo 1-El reto de los sistemas de Información ¿Qué es un sistema de información? *Tecnología Laudon & Laudon.*, 1-65. https://www.emagister.com/uploads_user_home/Comunidad_Emagister_8601_laudon.pdf

Lederkremer, M. (2019). *Redes Informáticas* (1ra ed.). RedUsers. https://books.google.com.mx/books?id=7frADwAAQBAJ&hl=es&source=gbs_navlinks_s

Limones, E. (2021). *Topología de redes informáticas*. OpenWebinars.

Ortiz, S. (2021, julio 19). Hackers atacaron los sistemas informáticos de la CNT. *Expreso*. https://www.expreso.ec/actualidad/hackers-atacaron-sistemas-informaticos-cnt-108488.html

Peiró, R. (2020). *Sistema de información - Qué es, definición y concepto*. Economipedia. https://economipedia.com/definiciones/sistema-de-informacion.html

Restrepo Zuluaga, A. G. (2018). *VULNERABILIDADES EN REDES DE INTERNET ALAMBRICAS E INALAMBRICAS* [UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA]. https://repository.unad.edu.co/handle/10596/27729

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L., & Castillo Merino, M. A. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES: Vol. Volumen 46*.

Tintín-Perdomo, V. P., Caiza-Caizabuano, J. R., & Caicedo-Altamirano, F. S. (2018). Arquitectura de redes de información. Principios y conceptos. *Dominio de Las Ciencias*, *4*(2), 103. https://doi.org/10.23857/dc.v4i2.780

Universidad Internacional de Valencia. (2018). *Tres tipos de seguridad informática que debes conocer*. https://www.universidadviu.com/es/actualidad/nuestros-expertos/tres-tipos-de-seguridad-informatica-que-debes-conocer

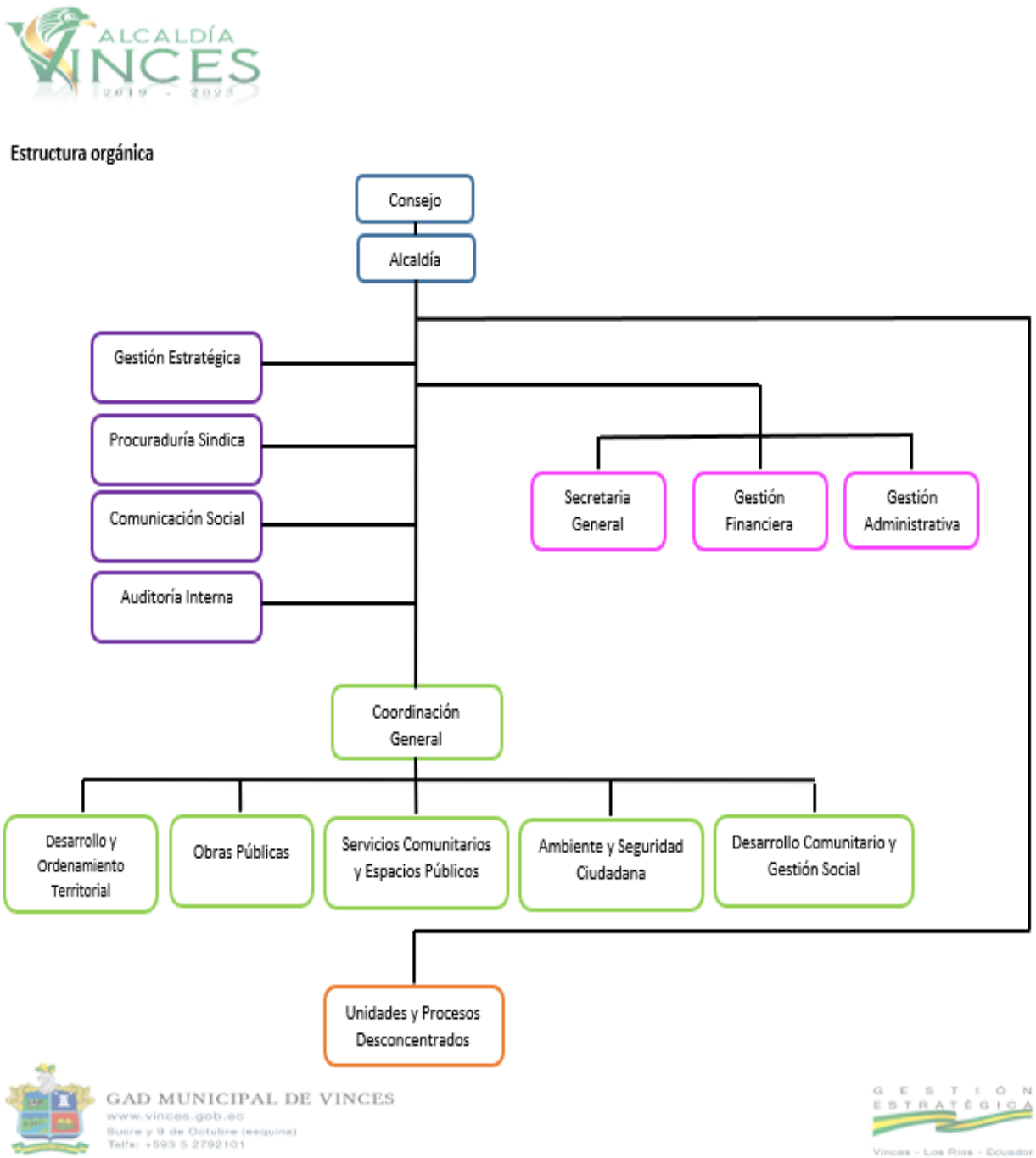
Uribe, I. (2022, marzo 9). *Mantenimiento industrial: correctivo, preventivo y predictivo*. Secmotic. https://secmotic.com/mantenimiento-industrial-correctivo-preventivo-y-predictivo/#gref

viewnext. (2018). *Tipos de seguridad informática – Viewnext*. CEAC. https://www.avansis.es/ciberseguridad/tipos-de-seguridad-informatica/

Anexos

Anexo 1.

Figura 8 *Organigrama Funcional del GAD Vinces*



Anexo 2.

Entrevista

Fecha: Julio, 18 de 2022

Entrevistado: Ing. Kleiner Navarro

Lugar: GAD Municipal de Vinces

Preguntas

1. **¿Cuál es el tipo de red?**

   Tenemos de tipo inalámbrica y red cableada. En la cableada existen dos categorías, la categoría 5E Y 6 A.

2. **¿Cuáles son los protocolos aplicados a la red?**

   Se utilizan de acuerdo a los estándares establecidos.

3. **¿Se realizan procesos de respaldo de la información?**

   Sí, se realiza todos los días.

4. **¿Cada qué tiempo se realizan mantenimientos a la red?**

   El mantenimiento se realiza trimestralmente.

5. **¿Qué acciones se toman al momento de que se presentan fallos en la red?**

   Dependiendo del tipo de falla, si la falla está relacionada con algún equipo se procede a realizar la suplantación. En el caso de algún sistema se trata de estabilizarlos.

6. **¿Se aplican normas de seguridad?**

   Sí, aunque no en su totalidad.

7. **¿En qué nivel considera usted que se encuentra el nivel de seguridad de la red?**

   Yo considero que se encuentra en un nivel medio de seguridad.

Anexo 3.

Figura 9 *Entrevista al Jefe del Dpto. de Sistemas*

Figura 10 *Proceso de Análisis de la Red*

Figura 11 *Cuarto de Servidores*

Anexo 4.

Ejecución de OpenVAS

Figura 11 *Iniciar OpenVAS*

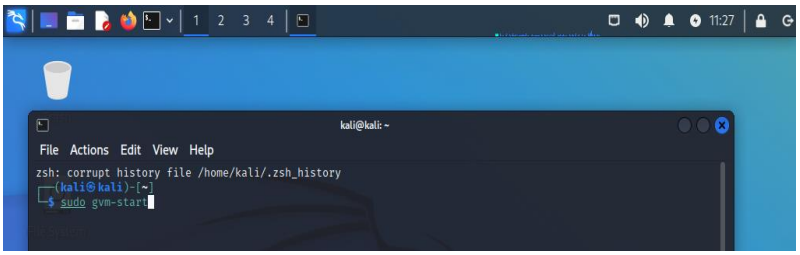


Figura 12 *Inicializando OpenVAS*

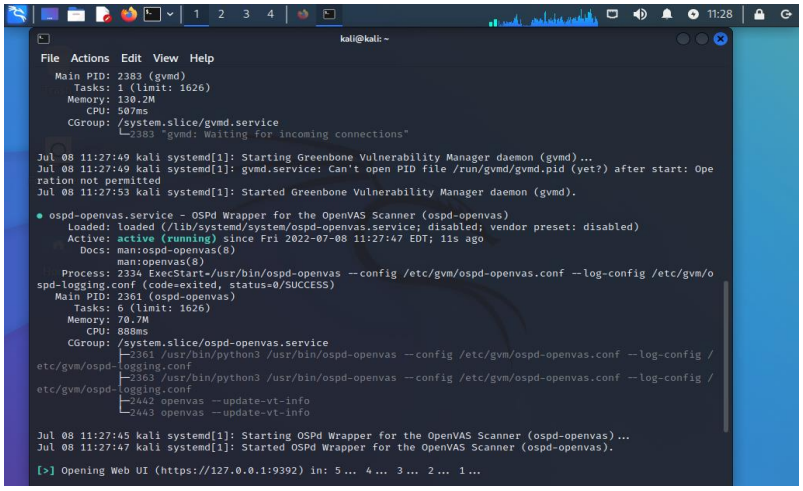
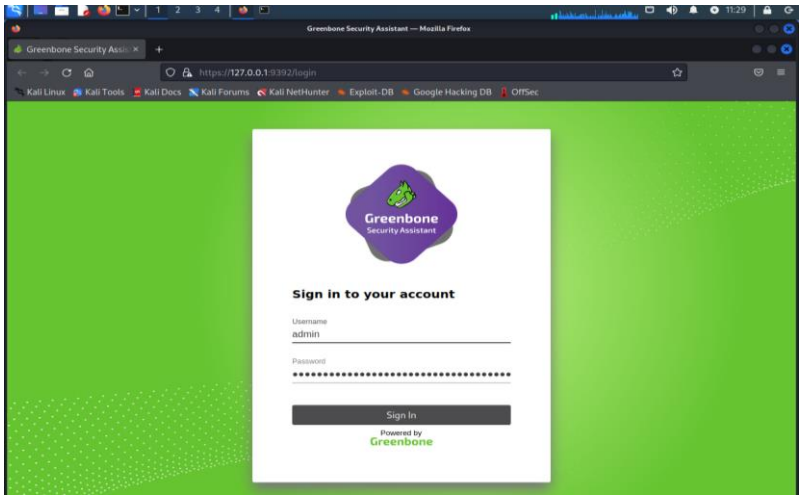


Figura 13 *Interfaz Greenbone desde el Navegador*



Anexo 5.

ALCALDÍA VINCES 2019 - 2023

Oficio No. 351-A-OF-GADMVINCES-JAMC-2022
Vinces, 7 de julio de 2022

Asunto: Contestación de oficio No. D-FAFI-UTB-0207-2022.

Licenciado
Eduardo Galeas Guijarro, MAE.
DECANO DE LA FACULTAD DE
ADMINISTRACIÓN, FINANZAS E INFORMÁTICA DE LA UTB
Babahoyo.-

De mis consideraciones:

Por medio del presente reciba usted un cordial saludo. Dando contestación a su oficio No. D-FAFI-UTB-0207-2022, de fecha 5 de julio del 2022, mediante el cual solicita el permiso respectivo para que la Srta. **MUÑOZ AGUIRRE VERÓNICA FERNANDA,** con C. I. No. 120713377-6, estudiante de la Carrera de Ingeniería en Sistemas, realice el caso de estudio titulado: "ANÁLISIS DE LAS VULNERABILIDADES DE LA RED INFORMÁTICA MEDIANTE LA HERRAMIENTA OPENVAS DEL GAD DE VINCES".

Al respecto, comunico a usted que su petición ha sido acogida favorablemente, por lo que la prenombrada estudiante podrá realizar la investigación del caso de estudio, bajo la supervisión del Ing. Kleiner Navarro Espinoza, coordinador de tecnología y de la información del GAD Municipal del Cantón Vinces.

Con sentimientos de distinguida consideración.

Atentamente,

JUAN ALFONSO MONTALVAN CEREZO

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE VINCES ALCALDÍA VINCES 2019 - 2023 ALCALDÍA

Sr. Alfonso Montalván Cerezo
ALCALDE DEL CANTÓN VINCES
JAMC/evll

RECIBIDO
DIRECCIÓN TÉCNICA DEPARTAMENTO
SECRETARÍA GENERAL
FECHA: 12/07/2022 HORA: 12:36

GAD MUNICIPAL DE VINCES
www.vinces.gob.ec
Sucre y 9 de Octubre (esquina)
Telfs: +593 5 2782101

ALCALDÍA
Vinces - Los Ríos - Ecuador

Anexo 6.

CERTIFICADO DE ANÁLISIS
magister

Análisis De Las Vulnerabilidades De La Red Informática Mediante La Herramienta OpenVAS Del Gad Vinces

2% Similitudes

1% Texto entre comillas
< 1% similitudes entre comillas
< 1% Idioma no reconocido

Nombre del documento: Análisis De Las Vulnerabilidades De La Red Informática Mediante La Herramienta OpenVAS Del Gad Vinces.docx
Tamaño del documento original: 1,44 Mo
Autor: Verónica Muñoz Aguirre

Depositante: Verónica Muñoz Aguirre
Fecha de depósito: 12/8/2022
Tipo de carga: url_submission
fecha de fin de análisis: 12/8/2022

Número de palabras: 7247
Número de caracteres: 46.682

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	Documento de otro usuario El documento proviene de otro grupo 4 fuentes similares	< 1%		Palabras idénticas : < 1% (64 palabras)
2	Documento de otro usuario El documento proviene de otro grupo 2 fuentes similares	< 1%		Palabras idénticas : < 1% (26 palabras)
3	CASO EDDER CASTILLO LEON.docx | CASO EDDER CASTILLO El documento proviene de mi grupo 8 fuentes similares	< 1%		Palabras idénticas : < 1% (23 palabras)

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	Documento de otro usuario El documento proviene de otro grupo	< 1%		Palabras idénticas : < 1% (36 palabras)
2	repositorio.upse.edu.ec https://repositorio.upse.edu.ec/bitstream/46000/5855/1/UPSE-TTI-2021-0016.pdf	< 1%		Palabras idénticas : < 1% (12 palabras)