UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS

TEMA:

ANÁLISIS DE LAS VULNERABILIDADES DE LA RED LAN DEL DISTRITO DE EDUCACIÓN 12D02 PUEBLOVIEJO-URDANETA.

EGRESADO:

CLARA ISABEL VILLALVA QUIÑONES

TUTOR:

ING. IVÁN RUÍZ

AÑO

2021

RESUMEN

El presente estudio de caso habla acerca de las vulnerabilidades de la Red LAN del distrito de Educación 12D02 Puebloviejo- Urdaneta, lo cual nos va a permitir conocer en qué condiciones o estado se encuentra la red LAN de dicha Entidad, ya que en ella se almacena toda la información de los estudiantes actuales y de los que ya han culminado alguna determinada etapa educativa, además también almacena información de las Instituciones Educativas que han sido cerradas. Para la recolección de información acerca del estado de la red LAN se utilizaron las siguientes herramientas: entrevista realizada a encargado del área de las TIC´S del distrito de Educación 12D02 Puebloviejo-Urdaneta.

Gracias a la utilización de la herramienta de análisis de riesgos Nessus se logró evidenciar ciertas anomalías estructurales en la instalación de la red. Se notó que los switch se encuentran cerca de la entrada a la vista de todos, y además los cables de red se encuentran dispersos y también a la vista de todos. Esto puede provocar que los equipos se averíen por el polvo y que haya intermitencias de transmisión por la posición de los cables. Se recomienda reinstalar estos equipos en un rack cerrado y estructurar los cables en canaletas.

Durante los escaneos con las herramientas de análisis de vulnerabilidad seleccionadas se encontraron ciertos puestos abiertos de ciertos terminales de la red de los conjuntos y con vulnerabilidades de severidad alta, medias y bajas. Aun cuando estas vulnerabilidades encontradas no representan en el presente un problema critico en la organización, se propone ejercer las medidas pertinentes para conservar a la red segura de futuros ataques o errores en la administración de los procesos de la red.

Palabras claves: LAN, Vulnerabilidades, Distrito, red.

ABSTRACT

The present case study talks about the vulnerabilities of the LAN network of the district of Education 12D02 Puebloviejo- Urdaneta, which will allow us to know in which conditions or state is the LAN network of this Entity, since in it is stored all the information of the current students and of those that have already culminated some certain educational stage, in addition it also stores information of the educational Institutions that have been closed. The following tools were used to collect information about the state of the LAN: an interview with the person in charge of the system area; a survey of users, in this case those who work in or use the LAN of Education District 12D02 Puebloviejo-Urdaneta.

Thanks to the use of the Nessus risk analysis tool, it was possible to identify certain structural anomalies in the network installation. It was noted that the switches are located near the entrance in plain sight, and the network cables are scattered and in plain sight. This can cause the equipment to break down due to dust and intermittent transmission due to the position of the cables. It is recommended to reinstall this equipment in an enclosed rack and to structure the cables in cable ducts.

During the scans with the selected vulnerability analysis tools, certain open positions of certain terminals of the network of the assemblies were found with vulnerabilities of high, medium, and low severity. Although these vulnerabilities found do not represent a critical problem in the organization at present, it is proposed to take appropriate measures to keep the network safe from future attacks or errors in the administration of network processes.

Keywords: LAN, Vulnerabilities, District, red.

INTRODUCCIÓN

La tecnología, las redes informáticas y especialmente el Internet han avanzado en los últimos tiempos, el uso de Internet por parte de las instituciones tanto públicas como privadas se ha convertido en equipo para el desarrollo de sus actividades, lo que pone en vulnerabilidad la información que alojan en la red. Es de suma importancia el internet, en la actualidad es una necesidad, pero no todo es transparente y seguro, es aquí donde surgen las vulnerabilidades y donde se expone la información en la red que finalmente se convierten en potenciales riesgos.

Mediante el análisis de las vulnerabilidades se puede obtener la descripción del estado actual en el que se encuentra la red LAN del Distrito de Educación 12D02 Puebloviejo- Urdaneta a nivel de seguridad esto permitirá resguardar la información confidencial de las instituciones educativas que conforman dicha entidad.

El propósito del Distrito de Educación 12D02 Puebloviejo-Urdaneta es almacenar la información de las Instituciones Educativas existentes y de las que ya no se encuentran laborando con eficiencia y eficacia para de esta manera dar una óptima respuesta a los procesos que se gestionan en esta institución.

La línea de investigación del presente estudio de caso se basa en los Sistemas de Información y Comunicación, Emprendimiento e INNOVACIÓN y teniendo como sublinea de investigación las Redes y Tecnologías Inteligentes de Software y Hardware.

Para la recolección de información se llevaron a cabo entrevistas a los administrativos para poder conocer el estado de la Red LAN que utilizan, para determinar las vulnerabilidades de la misma. Dando un enfoque descriptivo, debido a que se logran comprender los procesos realizados en la red local y cualitativamente los datos obtenidos mediante la herramienta de estudio empleada.

DESARROLLO

El Distrito de Educación 12D02 Puebloviejo-Urdaneta perteneciente a la Provincia de los Ríos, es una entidad pública, la cual está conformada por 75 Instituciones educativas con una población estudiantil de 18.241 estudiantes entre los Cantones Puebloviejo y Urdaneta; tiene como objetivo asegurar la excelencia en la calidad educativa, el derecho al acceso a la educación de estudiantes con escasos recursos y de capacidades especiales, consolidando las instituciones educativas con docentes; dotándolos de los textos escolares, vestimenta, colación escolar, y manteniendo el compromiso con las Unidades de Apoyo a la Inclusión para el progreso en las condiciones escolares en la educación. (Llanes, 2020)

Se define a las amenazas como un mecanismo o tarea preparada para infringir y vulnerar el equilibrio de los activos informáticos. Estos riesgos nacen desde que exista una vulnerabilidad que pueda ser explotada, no es necesario que la igualdad de una red sea plenamente vulnerable, basta con que exista una pequeña grieta que permita el filtrado de información privada, también se puede piratear mediante ingeniería social, esto se debe al reciente incremento de ataques de este tipo por la falta de instrucción y concientización elemental en los usuarios, además un motivo bastante importante es el beneficio que pueden obtener con la información robada todo estas razones han llevado al crecimiento de esta clase de ataques en los últimos años.

La problemática actual es que presenta un bajo cumplimiento de las medidas de seguridad informática ya que no se garantiza la seguridad de la red. Debido a la ausencia de conocimientos de los administradores y la mala gestión de la aplicación de los recursos se han evidenciado algunas vulnerabilidades como caídas del sistema, ataques informáticos, y en ciertos casos los discos duros de respaldos sufren daños y estos factores ocasiona que se pierda información muy importante para la institución.

El Distrito de Educación 12D02 se encuentra dividido en varios departamentos como: Atención Ciudadana, Sistema de Gestión Docente, Unidad Distrital de Planificación, Departamento de Consejería Estudiantil, Departamento Administración Escolar, División Distrital Administrativa y Financiera. Por lo que la demanda de información es alta y gran parte de ella viaja por la red siendo vulnerable ya que no cuentan con sistemas de seguridad para resguardar la información.

Se evidencio que existe la falta de medidas de seguridad en las redes lo cual es un problema que está creciendo considerablemente, debido a que hay un mayor número de atacantes y además al descuido gracias a sus administradores, por lo cual se pone en peligro la integridad y confidencialidad de la información de la organización, la misma puede quedar expuesta a usuarios no autorizados o modificada a través de un experto.

Los usuarios del Distrito de Educación actualmente son considerados el eslabón más débil, debido a que estos navegan por internet, sin saber que pueden ser víctimas de ataques originados por malware, piratas informáticos o espectadores, subestimando el impacto que puede tener el riesgo de alto nivel. Los ataques suelen provenir en la mayoría de la red interna, donde usuarios externos pretenden entrar ilegítimamente a los sistemas informáticos ya sea para cambiar, remover o extraer la información e influir en el manejo de los servicios, es por esto que los administradores tienen que conocer la conducta usual del tráfico de la red, hacer uso de herramientas que los apoyen a la detección de intrusos y probables ataques para lograr tomar las medidas pertinentes.

Menciona (Janine Kremling, 2017) que la información pertenece a los activos más relevantes de la organización. Para una organización, la información es importante y debería protegerse correctamente, además la estabilidad se basa en una combinación de sistemas, operaciones y controles internos para asegurar la totalidad y confidencialidad de los datos y los

métodos de operación en una organización. El valor de la información para las empresas radica en que es un recurso importante que se lo utiliza en el desarrollo de sus operaciones diarias y estratégicamente para identificar altos niveles de competencia.

En la historia de las redes se ha mencionado que la tecnología ha ido avanzando de forma sorprendente, surgiendo la necesidad de recolectar, procesar y repartir información, con el pasar del tiempo además ha ido cambiando la manera de transmisión de esta, comenzando con cartas, redes telefónicas, radio y televisión, hasta llegar a esta época donde hay las redes informáticas. En empresas con una cantidad enorme de oficinas en sitios distantes la necesidad de mover y compartir recursos nació, puesto que este proceso les llevaba mucho tiempo, una vez que en verdad ellos requerían entrar a dichos recursos con un solo tecleo. Una red de Pc's ofrece a los usuarios oportunidades diversas en temas de programa, tanto información como programas. Es necesario compartir información, esa que se genera por los clientes: día con día y, que es el motivo de ser de las Pc's. Estima que la evolución se ha hecho en los últimos 10 años y corresponde en mucho, al desarrollo de novedosas corrientes en la administración de los Servicios Informáticos, el surgimiento de nuevos productos y tecnologías y a las novedosas utilidades que la computación y las redes muestran a la sociedad, las organizaciones y las instituciones generalmente. Se reflejan que la utilización exhaustiva de las redes de Pc's en todos los centros de enseñanza preeminente en el territorio está sentando las bases para poder hacer cambios cualitativos en lo demás de los procesos. (Ceruzzi, 2019)

Según Alegas (2011) una red es un conjunto de redes interconectadas a escala global. Puede definirse como un sistema de red informática global. Se conoce que las redes forman parte de Internet cambian ampliamente en propósito y tamaño. Hay redes públicas y privadas; local, regional e internacional; instituciones, educación, universidades, dedicadas a la investigación, entretenimiento. Los datos se emiten de manera fragmentada en paquetes: pueden ser como piezas de un rompecabezas que se juntan a medida que llegan a su ubicación. Aquello explica

que una vez que navegas por la web las páginas se vayan visualizando de manera fragmentada, comúnmente primero el escrito y después las imágenes. La finalidad elemental es trasmitir información, realizando que todos los programas, datos y conjuntos se encuentren a la mano para la red que lo solicite, sin que importe el sitio donde esté el recurso y el cliente. Su meta es conceder una alta confiabilidad, al disponer de fuentes alternativas de abastecimiento. Los diversos archivos podrían repetirse en diversas máquinas, de forma que si se pierde los datos de una los podría restaurar la copia. La existencia de diversas CPU supone que, si una de ellas deja de funcionar, las demás tienen la posibilidad de ser capaces de encargarse de su trabajo, aun cuando se tenga un rendimiento universal menor.

Una red de área local (LAN) es una red informática que conecta las computadoras en un área subjetivamente pequeña y predeterminad. Sobre todo, tienen la posibilidad de conectar entre ellas por medio de líneas telefónicas y ondas de radio, permitiendo compartir bases de datos, programas y periféricos como podría ser un módem, una impresora, un escáner, entre otros; poniendo a nuestra disposición otros medios de comunicación como tienen la posibilidad de ser la correspondencia electrónica y el chat. Cabe destacar que una red de área local ofrece ahorros fundamentales, tanto en términos de dinero, ya que no es necesario comprar muchos dispositivos y consume menos papel, y en un acceso al internet se puede usar una exclusiva conexión telefónica compartida por diversas computadoras conectados en red; como de tiempo, debido a que se consigue administración de la información y del trabajo. (Paraninfo, 2014)

Una red de área amplia (WAN) es una red de telefonía y conexión privada que conecta varias redes de área local. En una organización puede integrar conexiones corporativas, sucursales, instalaciones de localización, servicios en la nube y otras instalaciones. Comúnmente, se usa un enrutador u otro dispositivo multifunción para conectar una red de área local a una red de área extensa. Además permiten a los usuarios compartir entradas con aplicaciones, servicios y recursos centralizados. (Llamas, 2015)

Una red de área metropolitana (MAN) es un tipo de red intermedia, que encierra más o menos la medida de una localidad, situada en medio de las redes locales, que conectan Pc's en un radio bastante limitado, y las redes globales, que conectan computadoras de todo el mundo o de regiones bastante extensas. Se aplican para compartir información entre redes de centros públicos o privados de una misma localidad. Además, su capacidad es totalmente superior al de la red general, otorgando una velocidad de conexión mucho más rápida que la WAN y cercana a la LAN, al utilizar los mismos protocolos y procedimientos de conexión.

Una red de área personal (PAN) es conocida como una configuración elemental la llamada configuración básica personal, que está formada por dispositivos ubicados en el entorno personal y local de un usuario, así sea en la vivienda, trabajo, coche, parque, supermercado, entre otros. Esta configuración le posibilita al cliente implantar una comunicación con dichos dispositivos en el momento que sea de forma inmediata y eficaz.

La topología de red es un plano físico o lógico de la red para el intercambio de datos. En otros términos, es la revolución del diseño, tanto física como lógicamente. El término de red se puede conceptualizar como un "grupo de nodos interconectados". Un nodo es la intersección de una curva en un punto específico. Un nodo en particular depende del tipo de red en cuestión. Los recursos esenciales de una red son el servidor, los terminales, los dispositivos de red y el medio de comunicación.

Topologías más comunes.

Red de anillo es una topología que permite a los nodos conectarse directa, creando una única ruta continua. Además, tiene la característica de poseer un receptor y un transmisor lo que le permite realizar el oficio repetidor, posibilitando que la información llegue al siguiente recurso del anillo. Se conoce que, si el nodo principal se queda sin servicio por daños o cualquier otro motivo, la conexión en el anillo se pierde. (Carrascosa, 2019)

Red Bus-Estrella es una topología caracterizada por el hecho de que todos sus nodos están conectados a un controlador central. Cada transacción pasa por el nodo central, que representa la gestión y mantiene el control de cada comunicación. (Carrascosa, 2019)

Red de Estrella es una topología considera una de las principales. en la cual las estaciones están enlazadas de forma inmediata a un punto central y cada una de las transmisiones se hacen claramente por medio de este recurso. Esta red es conocida por tener un nodo central activo que tiene las características para prevenir errores. (Carrascosa, 2019)

Topologías Mesh es una topología basada en una combinación de más de una topología, por ejemplo, un bus combinado con una estrella es común en lugares donde tienen redes de bus y luego lo extienden a estrella. Además, es muy complicado detectar su conexión por parte del servicio técnico para repararlos. (Carrascosa, 2019)

Red Malla es una topología en la que hay inmunidad contra fallas de cable y congestión y puede dirigir el tráfico a rutas alternativas en caso de que un nodo esté inactivo u ocupado sumando ventajas a la tecnología tokens ring, aun con vínculos redundantes. Por políticas de redundancia, que realizan a la estabilidad informática, añadiendo cableado estructurado, con mucho sitio en las patcheras, para lograr continuar creciendo o meter cambios de localización de los grupos consumidores sin inconvenientes, con ella evitaremos probables acosos. (Carrascosa, 2019)

Explica (Castillo, 2019) que las redes de datos son fundamentos diseñados para transmitir información a través del intercambio de datos. Lo que hace que este tipo de red sea diferente de otras formas de comunicación, como una red de audio, es que está configurada para transmitir solo datos. Esto contrasta con una red de audio o voz, que se usa comúnmente tanto para comunicaciones de voz como para transmisión de datos, como el envío de facsímil. Además, son considerados recursos imprescindibles en una organización, pues favorecen a que

haya una mejor y más inmediata comunicación entre los empleados y se logre manejar un más grande número de datos para obtener la información elemental.

Capa de aplicación	Técnicas de aplicación que ofrece redes
Capa de presentación	Organización el módulo de información
Capa de sesión	Gestión de terminales de practicas
Capa de transporte	Suministrar servicios de identificación y error
Capa de red	Gestión de conexión por medio de la red
Capa de enlace de datos	Suministrar servicio de envío de datos
Capa física	Propiedades de la red

Tabla 1. Modelo de interconexión de sistema de capas OSI
Elaborado por: Clara Villalva.

Capa de aplicación: la como función identificar los recurso de conexión, además permite al usuario usar la capa de transportar para poder transferir y recibir información de los datos de los equipos tecnológicos. (García, 2015)

Capa de presentación: Tiene como funcionalidad elemental encargarse del formato en que se va a enseñar la información comprende la distribución de los recursos del grado de aplicación, decidir la semántica de las fórmulas empleadas para interpretar la información, descifrando el formato de aplicación de red. (García, 2015)

Capa de sesión: esta capa propicia a los usuarios de equipos diversos tiene la propiedad de entablar sesiones entre ellos. Una sesión favorece el transporte usual de datos, como lo hace la capa, sin embargo, otorga servicios modernizados que son útiles en varias aplicaciones. (Miguel, 2019)

Capa de transporte: Tiene como meta es suministrar a los usuarios un servicio eficaz que normalmente son procedimientos desarrollado por la capa de aplicación. Para poder hacer este objetivo, la capa de transporte usa los servicios proporcionados por la capa de red. El recuso de la capa tendrá la capacidad de transferir los datos el cual se lo conoce con el nombre de

entidad de transporte, además participar estar en el centro del programa, en un proceso separado, en un paquete de biblioteca o en la tarjeta de red. (Miguel, 2019)

Capa de red: Es aquella que identifica a los equipos mediante direcciones IP, es decir da los medios funcionales y se asegura de que tenga un destino de la misma red o mediante redes externas. La unidad de protocolo de datos popular como PDU se denomina paquete. Uno de los principales dispositivos que trabaja al nivel de la capa3 es el equipo Router que es usualmente uno de los más utilizados. Esta capa además nos permite hacer la fragmentación. (campos, 2017)

Capa de Enlace de Datos: su característica principal es reconocer las interfaces de los equipos por direcciones, de esta misma forma mantiene una cola que hace la función de control de errores o CRC. La unidad de protocolo de datos de la capa de enlace de datos se denomina trama o frame. (campos, 2017)

Capa Física: La función fundamental es identificar especificaciones eléctricas y físicas de los dispositivos en bits para la comunicación. La unidad de protocolo de datos popular como PDU en la capa física se denomina byte (Andrew, 2017)

La seguridad de redes se basa en prácticas adoptadas para prevenir y monitorear la entrada no autorizada, el mal uso, la modificación o el rechazo de una red informática y sus recursos disponibles. La estabilidad de la red está vinculada con el permiso para ingresar datos en la red, que es controlado por el administrador de la red. Cabe destacar que los individuos escogen o se les asignan un usuario y contraseña el cual les permitirá iniciar sesión y acceder a la debida información y a programas, también se conoce que cubre una diversidad de redes de Pc's, tanto públicas como privadas, que se utilizan en trabajos diarios; hacer transacciones y comunicaciones entre organizaciones, agencias gubernamentales y personas. Además tiene la

posibilidad de ser privadas, como en una organización, y otras que tienen la posibilidad de estar abiertas al público. (Pérez, 2020)

En cuanto a la seguridad, se consideraron tres aspectos importantes:

- Confidencialidad: Se refiere al servicio de seguridad que garantiza que la información no pueda estar disponible o detectada por procesos no autorizados.
- Disponibilidad: Se refiere a un sistema seguro que siempre está listo para poner información, hardware y software a disposición de los usuarios.
- Integridad: Se refiere al requerimiento de seguridad que asegura que la información sea creada, modificada y eliminada.

Según (Veiga, 2020) actualmente no se tiene en cuenta la seguridad física a la hora de diseñar diagramas de red, sin embargo, este es un punto muy importante porque permite la aplicación de barreras físicas y métodos de control, como medidas preventivas y medidas contra amenazas. A información y recursos confidenciales, o al uso de mecanismos para controlar el ingreso de objetos u otros elementos para proteger los sistemas tangibles de la organización.

Seguridad lógica incluye aplicaciones de barreras y/o métodos que protegen el acceso de datos y solamente se posibilite entrar a ellos a los individuos autorizadas para realizarlo. Hay varios controles para la estabilidad lógica como se puede evidenciar en la estabilidad Informática: sus Implicancias e Implementación" empero se ha considerado los próximos:

- El control de acceso se implementa cuando se usa el control en cualquier servicio de red para retener toda la información y proteger los datos confidenciales del acceso no autorizado.
- Listas de control de acceso ACL's su meta es filtrar el tráfico, permitir o denegar el tráfico de la red según las diferentes condiciones establecidas en los equipos de la red.
- Restricciones a los servicios se e refieren a las restricciones que siguen los límites de distribución de la aplicación o que están preestablecidas por un administrador.

Explica (Valdivia, 2015) que el ataque de denegación de servicios es un ataque por medio del cual se restringe el ancho de banda de la víctima mediante un consumo persistente de este o se ataca su sistema computacional consumiendo y agotando los recursos de un equipo, en el MiKrotik puede provocar incremento desmesurado del consumo de CPU, principalmente no existe una solución perfecta para defender contra ataques de denegación de servicio.

Indica (PALACIOS, 2020) que un cortafuego es un sistema situado entre dos redes, este sirve como un filtro que controla cada una de las comunicaciones que pasan de una red a la otra por medio de él y en funcionalidad de lo cual el cliente ocupe posibilita o deniega su paso, salvaguardando de esta forma la red de intromisiones indeseadas. Su funcionalidad es, ser una sólida barrera entre la red local y la red exterior. Este preserva separada la red interna de diversos tipos de redes externas. Es el delegado de defender una red confiable.

Explica (Navarrete, 2018) que una amenaza, de acuerdo con la seguridad informática, podría ser cualquier cosa que aproveche una vulnerabilidad para violar la estabilidad y alterar, borrar, afectar objetos u objetos de interés. La seguridad de la red está formada de elementos de hardware y programa diseñados para defender los datos y la información que se procesan en la red. Además, dichos elementos otorgan medidas preventivas configuradas para defender la infraestructura de la red y sus datos contra la entrada no autorizado, la modificación de datos, la corrupción y la divulgación inadecuada. En última instancia, la estabilidad de la red está diseñada para producir un ámbito seguro donde los usuarios de Pc’s, programas de programa y aplicaciones móviles tienen la posibilidad de hacer ocupaciones informáticas o digitales sin vulnerabilidades de red.

Las principales amenazas las podemos clasificar en:

CATEGORÍA	DESCRIPCIÓN
Interrupción.	Disponibilidad de una parte o total del sistema.
Intercepción.	Confidencialidad.
Modificación.	Ataque contra la integridad.
Fabricación.	Autenticidad.

Tabla 2. Amenazas de seguridad de la información.
Elaborado por: Clara Villalva.

AMENAZAS FÍSICAS	AMENAZAS LÓGICAS
➢ Desastres naturales. ➢ Fallos en los suministros ➢ Robos de información.	➢ Pérdida de datos. ➢ Virus informáticos, malware. ➢ Ataques e intrusiones a la red.

Tabla 3. Amenazas físicas y lógicas de una red
Elaborado por: Clara Villalva.

Indica (Vieites, 2018) que un ataque informático es una acción causada por un individuo con el fin causar inconvenientes a un sistema informático o red. Esta clase de ataque se crea ya que dichos delincuentes encuentran una vulnerabilidad en el programa o hardware, para obtener una virtud, principalmente financiera. Es por esa razón por lo cual están afectando de manera negativa la estabilidad de los sistemas involucrados y después les quitan los activos de la organización. El problema de los virus informáticos podría ser importante teniendo presente que un virus puede perjudicar o remover datos del equipo, utilizar el programa de correspondencia electrónico para propagarse a otros grupos o inclusive borrar todo el contenido.

Los sistemas informáticos usan diversos elementos, a partir de electricidad para dar ingesta de alimentos a los conjuntos hasta el programa de programa ejecutado por medio del sistema operativo que emplea la red. La forma que se podría minimizar los peligros de que la

información sea extraída por medio de la red es aplicando reglas que resguarden la información. La regla ISO27001 tiene como objetivo gestionar la estabilidad de la información que posibilita asegurar que los riegos de estabilidad sean conocidos por las empresas de forma eficiente. (Urbina, 2016)

Según (ciberseguridad. Blog, 2018) el escaneo de puertos es una de las técnicas de reconocimiento más reconocidas que usan los atacantes para encontrar los servicios expuestos a probables ataques. Cada una de las máquinas conectadas a una red de área local (LAN) o Internet ejecuta varios servicios que escuchan en puertos conocidos y no tan conocidos. Un escaneo de puertos ayuda al agresor a ubicar qué puertos permanecen accesibles, fundamentalmente, un escaneo de puertos se basa en remitir un mensaje a cada puerto, uno a uno. El tipo de contestación recibida sugiere si el puerto está a la escucha y, por consiguiente, puede probarse más detalladamente para identificar agotamiento.

Metodologías utilizadas en este caso de estudio:

Cabe destacar que la línea de investigación utilizada en este caso de estudio es la de sistemas de información y comunicación, emprendimiento e innovación, donde la sub línea de investigación es la de redes y tecnologías inteligentes de software y hardware, en donde se utilizó como instrumento de investigación es la entrevista la misma que permitió recolectar información muy importante sobre el Distrito de Educación 12d02 Puebloviejo, para asi poder comprender mejor los problemas que se han presentado la red.

En esta investigación se empleó el método descriptivo, cuyo objetivo es analizar la información recolectada para predecir los comportamientos de los elementos activos de información. Con este método se logró observar irregularidades que presenta la red de conexión, con el fin de ofrecer una propuesta referencial como guía hacia los usuarios de la red para tratar de conservar la seguridad de la información.

Una vez concluido el respectivo análisis de vulnerabilidades en la red del Distrito de Educación 12D02 Pueblovieljo-Urdaneta, se pudo conocer cuáles son las vulnerabilidades que presenta en la red y con el fin sugerir acciones necesarias para la correcta seguridad de la información que se maneja la institución.

En el análisis de los riesgos se realiza una predicción de lo que puede suceder en el futuro si no se toman las medidas necesarias en cuanto a las amenazas detectadas en la identificación de los riesgos, basándose en hechos estadísticos, con el objetivo de terminar el impacto, y tomando alternativas de solución.

Como primer punto es importante reconocer y valorar los activos, los cuales recursos que contribuyen al desarrollo de actividades de la institución.

Activos de hardware	**Activos de software**	**Activo de información**
Portátil	Sistema educativo.	Licencia de Windows server
Disco duro externos	Base de datos	Unidades USB
Router	Antivirus	Documentos en papeles
Servidores	Sistema operativo	Licencia OEM Profesional
Equipos de escritorio	Correo electrónico	Licencia suite Adobe desing
Cableado estructurado	Navegadores	Licencia de Oracle data base
Fibra óptica	Página web institucional	
Web site	Sistema de información humano	
Disco duro de servidores	Sistema de información administrativo	
Firewall físico	Red de docentes investigadores	
Impresora		
Ups unidad almacenamiento		
Switches		

Tabla 4. Activos de la institución
Elaborado por: Clara Villalva.

Continuación de indica el proceso de análisis de riesgo de la red LAN del Distrito de Educación 12D02 Puebloviejo – Urdaneta:

Para la realización del escaneo de los puertos se utilizó Nessus, herramienta que se utiliza para identificar las vulnerabilidades en una red.

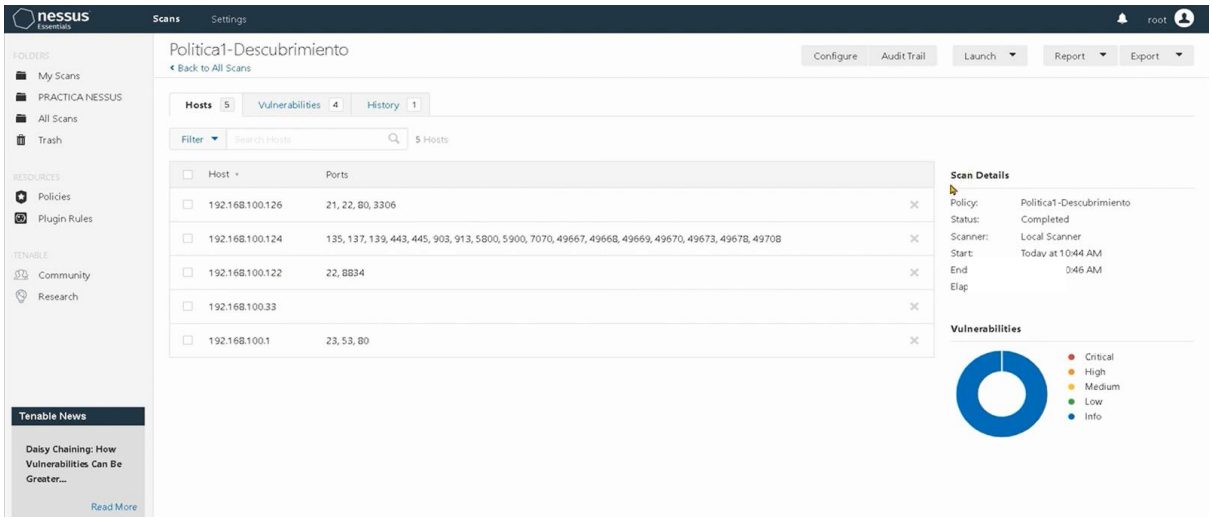


Ilustración 1. Ips encontradas una vez ejecutado el escaneo de Nessus
Elaborado por: Clara Villalva.

Se encontró un rango alto de vulnerabilidad en los siguientes host: 192.168.100.126, 192.168.100.124, 192.11268.100.122, 192.168.100.33,192.168.100.1 los cuales fueron identificados, el fin de este escaneo es verificar si existen puertos abiertos con vulnerabilidades.

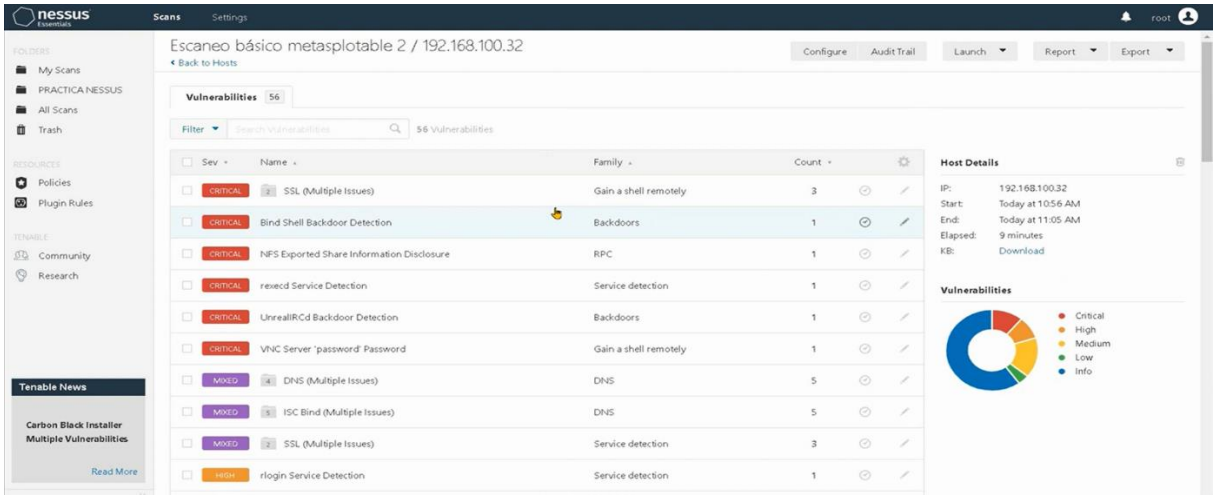


Ilustración 2. Niveles de vulnerabilidad
Elaborado por: Clara Villalva.

Nessus nos muestra la existencia de vulnerabilidades en la red, además los hosts escaneados con sus respectivos niveles de vulnerabilidad.

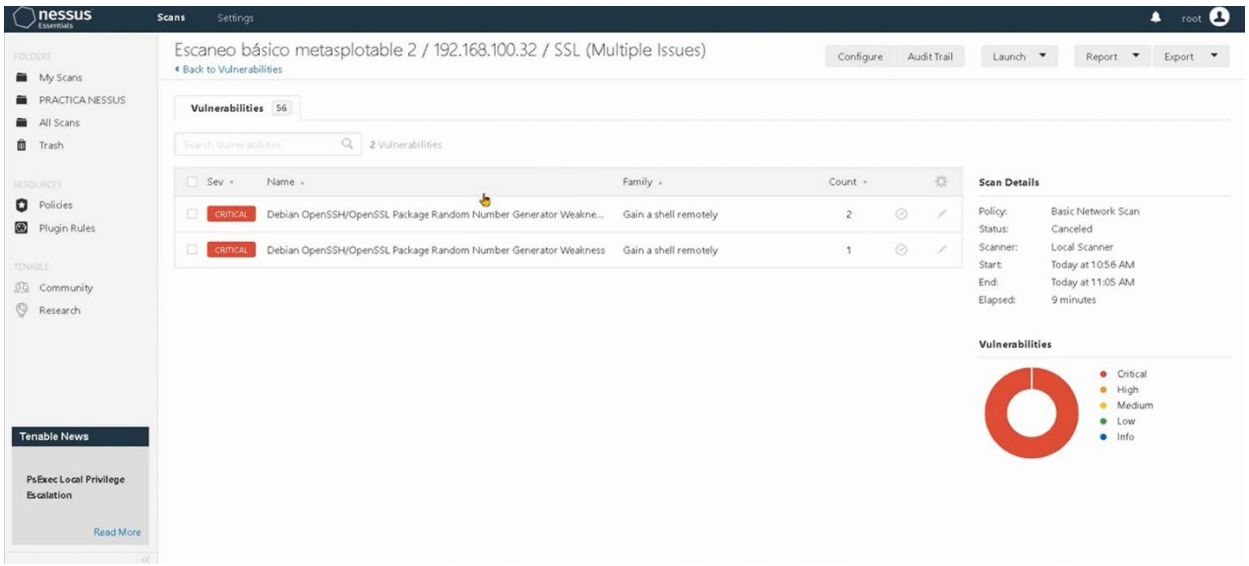


Ilustración 3. Vulnerabilidades encontradas
Elaborado por: Clara Villalva.

Aquí podemos apreciar las vulnerabilidades encontradas en el escaneo y estas se encuentran especificadas por escala de riesgo.

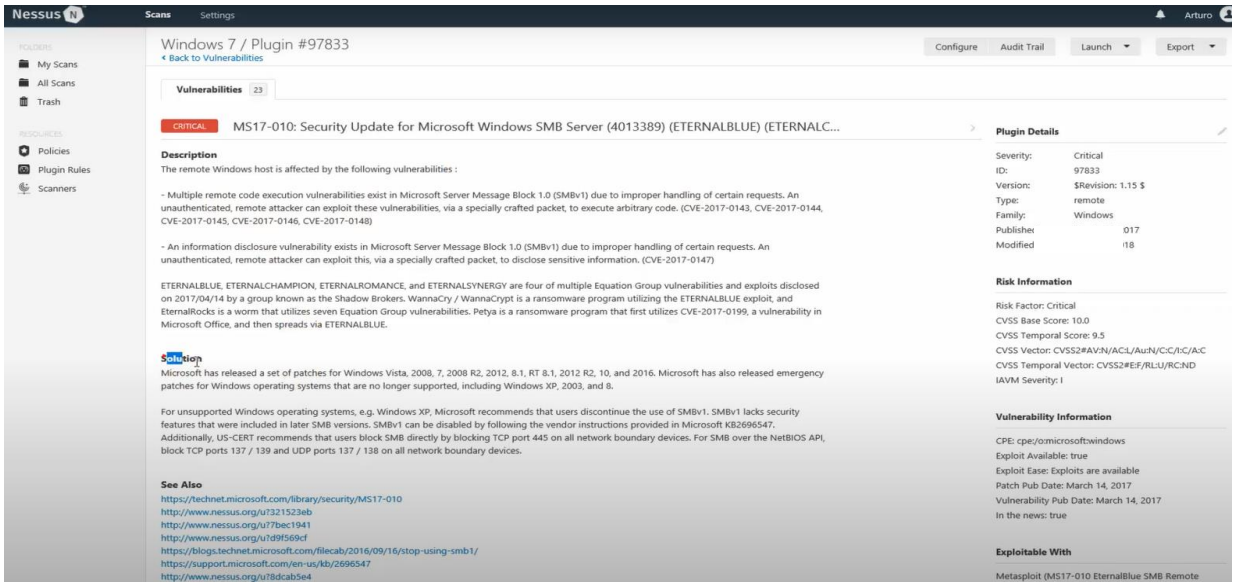
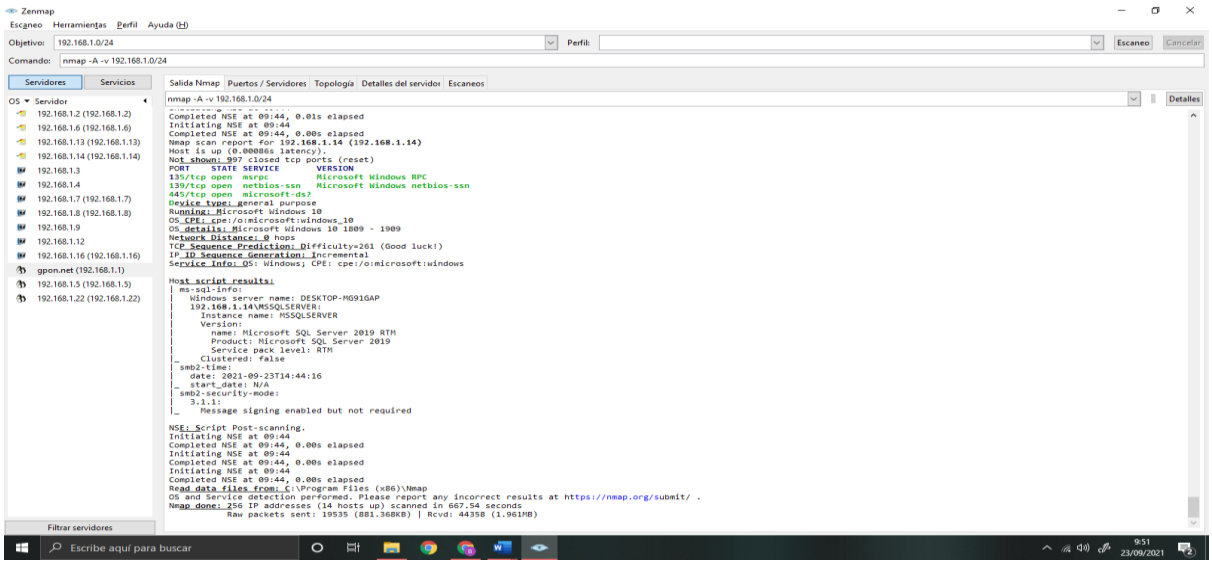


Ilustración 4. Posibles soluciones a vulnerabilidades
Elaborado por: Clara Villalva.

Nessus es una herramienta muy buena porque nos ofrece la posible solución a la vulnerabilidad a través reportes que se pueden imprimir en diferentes formatos.



Ilustracion 5. Nmap muestra la finalizacion del respectivo escaneo
Elaborado por: Clara Villalva.

En Zenmap primero lo que hacemos es dar un rango de Ip y después seleccionamos el tipo de escaneo que este caso es el escaneo intenso y muestra la información organizada de todas las ip y el estado de los puertos.

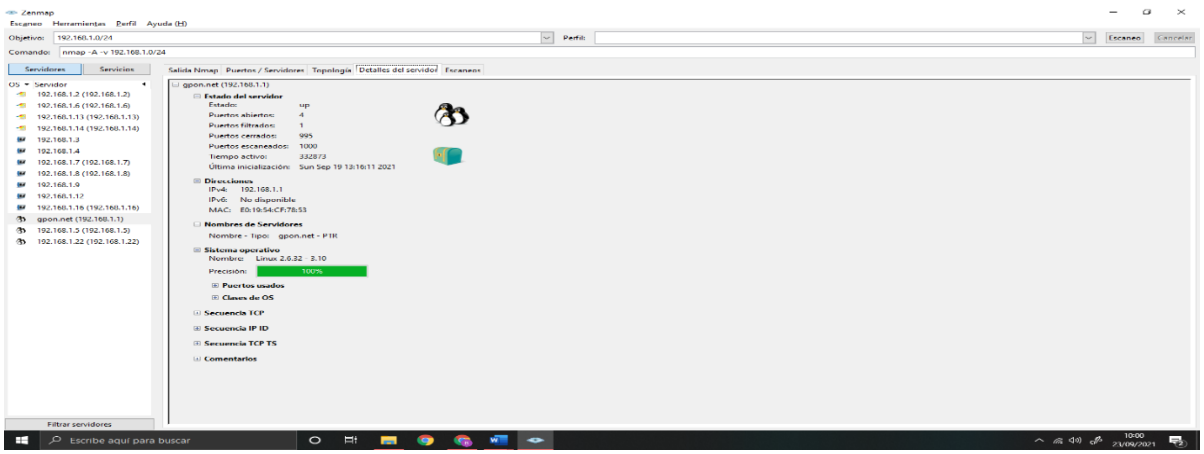


Ilustración 6. Detalles del servidor
Elaborado por: Clara Villalva.

Se puede observar un informe detallado como tipo de sistema que usa el pc y cada uno de los terminales testeados por el Nmap.

Como resultado del escaneo con Zenmap y Nessus se pudo evidenciar la existencia de amenazas y vulnerabilidades en la transmisión de datos de la red, luego gestionar los probables peligros que logren atentar con la estabilidad de los datos que usan por medio de la red de la organización. El escaneo tuvo una duración de alrededor de 30 min, donde la herramienta escogida otorgó un informe detallados de las amenazas y vulnerabilidades existentes en la red.

En la categorización de las vulnerabilidades se ha podido constatar que hay vulnerabilidades de severidad crítica, lo cual comprueba de que la red posee riesgos elevados de ser vulnerada, no obstante, sí existen están con prioridad alta, media y baja. Estas se muestran gracias a la mala configuración de los grupos de red y al mal funcionamiento de protocolos de red específicos.

El reporte muestra todas las vulnerabilidades encontradas y con sus respectivas resoluciones, es por esa razón que se sugiere hacer los cambios sugeridos por la herramienta Nessus, para que en el futuro puedan prevenir estos problemas, tomando las medidas pertinentes y que no logren perjudicar a la seguridad de la información, que se maneja la institución.

CONCLUSIÓN

Dada la investigación realizada se concluye que el Distrito de Educación 12D02 Puebloviejo-Urdaneta no cuenta con políticas para manejar la red, existen fallas en la instalación y configuración de la Red LAN, que, aun cuando sean de prioridad baja, se tienen que arreglar para que en el futuro no existan inconvenientes en lo referente a la seguridad de la información, así como en la transmisión de la misma a los diferentes nodos y terminales de la red.

Gracias a la utilización de las herramientas de análisis de riesgos Zenmap y Nessus se logró evidenciar que existen puertos abiertos en la Red. Aun cuando estas vulnerabilidades encontradas no representan un problema critico en la red, se propone ejercer las medidas pertinentes para conservar a la red segura de futuros ataques o errores en la administración de los procesos de la red.

Se notó que los switch se encuentran cerca de la entrada a la vista de todos, y además los cables de la red se encuentran dispersos. Esto puede provocar que los equipos se averíen por el polvo y que haya intermitencias de transmisión por la posición de los cables.

RECOMENDACIONES

- Se propone llevar a cabo medidas preventivas mediante un plan de seguridad estratégico que permita controlar y proteger la red de ataques informáticos y de otras vulnerabilidades, con el fin de defender todos los activos de información del Distrito de Educación 12D02 Puebloviejo-Urdaneta en todo tiempo.
- Se recomienda reinstalar estos equipos en un rack cerrado y estructurar los cables en canaletas.
- Se sugiere llevar a cabo una política y métodos de administración de seguridad tanto del personal que trabaja en el Distrito de Educación 12D02 Puebloviejo-Urdaneta como de los usuarios independientes con el objetivo prevenir pérdidas de información.
- Impulsar el uso de estándares de seguridad informático a todos los usuarios del Distrito de Educación 12D02 Puebloviejo-Urdaneta, con el fin emplear políticas fundamentadas valores éticos para conformar usuarios responsables en la utilización de la informática para salvaguardar los datos importantes almacenados en la red.

BIBLIOGRAFÍAS

Andrew. (2017). Redes de computadoras. Salvador. Obtenido de https://books.google.com.ec/books?id=WWD-4oF9hjEC&pg=PA326&dq=redes++capa+de+fisica&hl=es&sa=X&ved=2ahUKEwiQh5acnf3yAhUUHzQIHaJqAs8Q6AF6BAgJEAI#v=onepage&q=redes%20%20capa%20de%20fisica&f=false

Campos, L. (2017). Sistemas distribuidos: Arquitectura y aplicaciones. España.

Carrascosa, J. M. (2019). Instalaciones de telefonía digital y redes de datos (ICTVE). España. Obtenido de https://books.google.com.ec/books?id=hJmeDwAAQBAJ&pg=PA55&dq=topologia:+red+de+anillo,+red+bus+estrella,++red+estrella,+topologia+mesh,&hl=es&sa=X&ved=2ahUKEwijrLutzIvzAhX2TjABHQJ-DSYQ6AF6BAgJEAI#v=onepage&q=topologia%3A%20red%20de%20anillo%2C%20red%20bus

Castillo, C. M. (2019). Redes de datos y su cableado (FPB Instalaciones de telecomunicaciones). Madrid. Obtenido de https://books.google.com.ec/books?id=x1ekDwAAQBAJ&printsec=frontcover&dq=redes+de+datos&hl=es-419&sa=X&redir_esc=y#v=onepage&q=redes%20de%20datos&f=false

Ceruzzi, P. E. (2019). Breve historia de la computación. Mexico. Obtenido de https://books.google.com.ec/books?id=eBSGDwAAQBAJ&printsec=frontcover&dq=HISTORIA+DE+LAS+REDES+DE+COMPUTADORAS&hl=es&sa=X&ved=2ahUKEwii1ua_k4vzAhWERTABHbYTA-44ChDoAXoECAUQAg#v=onepage&q=HISTORIA%20DE%20LAS%20REDES%20DE%20COMPUTADORAS&f=false

Ciberseguridad, I. N. (20 de 3 de 2017). INCIBE. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

García, A. B. (2015). Modelo de programación web y bases de datos. Madrid. Obtenido de https://books.google.com.ec/books?id=Q1lWDwAAQBAJ&pg=PA101&dq=capa+de+aplicacion&hl=es&sa=X&ved=2ahUKEwiRtqCKmP3yAhUbFVkFHVq1CV84ChDoAXoECAMQAg#v=onepage&q=capa%20de%20aplicacion&f=false

Janine Kremling, . M. (2017). informacion y Cybersecurity. New York. Obtenido de https://books.google.com.ec/books?id=a9QpDwAAQBAJ&printsec=frontcover#v=onepage&q&f=false

Llamas, R. T. (2015). Instalación y configuración de los nodos de una red de área local. España. Obtenido de https://books.google.com.ec/books?id=PX5XDwAAQBAJ&pg=PA14&dq=Una+red+de+%C3%A1rea+amplia+(WAN)&hl=es&sa=X&ved=2ahUKEwiN6Py3o4rzAhUsSjABHajuAi4Q6AF6BAgCEAI#v=onepage&q=Una%20red%20de%20%C3%A1rea%20amplia%20(WAN)&f=false

Llanes, D. N. (2020). Informe de Redeccion de cuentas Distriti de Educacion 12D02 Puebloviejo-Urdaneta. Enero- Diciembre 2020. Obtenido de archivo pdf: https://educacion.gob.ec/wp-content/uploads/downloads/2021/05/12D02.pdf

Miguel. (2019). Redes Informáticas. Mexico. Obtenido de https://books.google.com.ec/books?id=7frADwAAQBAJ&pg=PA37&dq=redes++capa+de+sesion&hl=es&sa=X&ved=2ahUKEwiDqZjInP3yAhXTIDQIHWDFCroQ6AF6BAgFEAI#v=onepage&q=redes%20%20capa%20de%20sesion&f=false

Navarrete, S. V. (2018). EL ANÁLISIS DE VULNERABILIDADES. España. Obtenido de https://books.google.com.ec/books?id=5Z9yDwAAQBAJ&printsec=frontcover&dq=definicion+de+amenaza+en+red&hl=es&sa=X&ved=2ahUKEwi6j6HRkIvzAhWVVTABHdNrC94Q6AF6BAgLEAI#v=onepage&q&f=false

PALACIOS. (2020). Seguridad informática. Madrid. Obtenido de https://books.google.com.ec/books?id=UCjnDwAAQBAJ&pg=PA209&dq=definicion+de+cortafuego+o+firewall&hl=es&sa=X&ved=2ahUKEwiGs47-j4vzAhXMQjABHZr6ACwQ6AF6BAgFEAI#v=onepage&q=definicion%20de%20cortafuego%20o%20firewall&f=false

Pérez, A. (2020). La seguridad de las redes. Reino Unido. Obtenido de https://books.google.com.ec/books?id=tbzTDwAAQBAJ&printsec=frontcover&dq=seguridad+de+redes&hl=es-419&sa=X&redir_esc=y#v=onepage&q=seguridad%20de%20redes&f=false

Valdivia. (2015). Redes telemáticas. Mexico. Obtenido de https://books.google.com.ec/books?id=xbz-CAAAQBAJ&pg=PA142&dq=Ataque+de+denegaci%C3%B3n+de+servicios+en+la+red&hl=es&sa=

X&ved=2ahUKEwjAgNr31f3yAhXMElkFHT14BGQQ6AF6BAgIEAI#v=onepage&q=Ataque%20de%20denegaci%C3%B3n%20de%20servicios%20en%20la%20red&f=false

Veiga, J. M. (2020). Seguridad física y lógica de un sistema de información. Madrid. Obtenido de https://books.google.com.ec/books?id=tGnKDwAAQBAJ&pg=PA72&dq=seguridad+fisica+redes&hl=es-419&sa=X&ved=2ahUKEwinmIjP3ojzAhV9QjABHTeuACEQ6AF6BAgHEAI#v=onepage&q=seguridad%20fisica%20redes&f=false

ANEXOS

ANEXO I

Solicitud emitida a la Directora Distrital del distrito de Educación 12D02 Puebloviejo-Urdaneta por parte de la Decana de la F.A.F.I.

UNIVERSIDAD TECNICA DE BABAHOYO
FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA
DECANATO

Babahoyo, agosto 27 de 2021
D-FAFI-UTB-095-UT-2021

Master
Mirian Aguilar Limones
DISTRITO DE EDUCACION 12D02 PUEBLOVIEJO - URDANETA
En su despacho.-

De mis consideraciones:

La Universidad Técnica de Babahoyo y la Facultad de Administración, Finanzas e Informática (FAFI), con la finalidad de formar profesionales altamente capacitados busca prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

La señorita **VILLALVA QUIÑONEZ CLARA ISABEL**, con cédula de identidad No. **120735510-6** Estudiante de la Carrera de Ingeniería en Sistemas, matriculado en el proceso de titulación en el periodo Junio 2021 – Octubre 2021, trabajo de titulación modalidad Estudio de Caso para la obtención del grado académico profesional universitario de tercer nivel como **INGENIERO EN SISTEMAS.** El Estudio de Caso: **ANÁLISIS DE LAS VULNERABILIDADES DE LA RED LAN DEL DISTRITO DE EDUCACIÓN 12D02 PUEBLOVIEJO – URDANETA.**

En virtud de lo antes manifestado, solicito a usted, si es posible se sirva autorizar el permiso respectivo para que se realice el estudio de caso en la institución de su acertada dirección.

Atentamente,

Ing. Gina Carrasco Echeverria, MAE
DECANA DE LA FAFI

Recibido
Ministerio de Educación
SECRETARIA

Av. Universitaria Km 2 ½ vía Montalvo. Teléfono (05) 2572024 e-mail: decanatofafi@utb.edu.ec	Elaborado por: Carla Salvatierra Contreras	Revisado por: Ing. Gina Carrasco Echeverria, MAE

ANEXO II

ENTREVISTA

Tema: Análisis de las vulnerabilidades de la red LAN del Distrito de Educación 12D02 Puebloviejo – Urdaneta.

Dirigida: Encargado del departamento de las TIC'S - Licenciado Luis Aguay Balladares.

Objetivo: Determinar las vulnerabilidades de la red LAN del distrito de educación 12D02 Puebloviejo – Urdaneta

1. ¿Dónde se encentra ubicada la red LAN de la institución?

La red LAN del Distrito de Educación 12D02 se encuentra ubicada en la oficina central.

2. Con que frecuencia se le da mantenimiento a la Red LAN?

Cada 6 meses.

3. ¿La red LAN con qué frecuencia sufre caídas?

Repentinamente lo que en ocasiones ha provocado en ciertos casos pérdida de información.

4. ¿Considera que el Distrito de Educación presenta un bajo cumplimiento en las medidas de seguridad?

La verdad que si ya que han sufrido ataques informáticos donde se ha visto información comprometida.

5. ¿Cuál es el esquema estándar de la red LAN que se maneja la institución?

Tcp/Ip

6. ¿Cuáles son los servidores implementados?

En la actualidad contamos con la maquina central que ejerce la función del servidor. Todo en la organización se maneja de manera descentralizada, toda la información está en los diferentes terminales.

7. ¿Cuál es el proveedor de servicios de internet?

En la actualidad nuestro distribuidor es CNT. Ellos nos entregan internet con fibra óptica por medio de un conversor nosotros mismos nos encargamos de repartir el internet a los diferentes departamentos.

8. ¿Actualmente usan algún software adicional?

No, solo utilizamos el paquete de Microsoft Office hay desarrollo nuestras actividades.

9. ¿Se está alquilando equipo adicional para atender la solicitud?

No, solo trabajamos con los recursos tecnológicos que forman parte de la institución.

10. ¿La red posee algún tipo de mecanismo para resguardar la información que circula en ella?

No, cada funcionario se encarga de resguardar la información.

ANEXO III

Autorización emitida por la Directora Distrital del distrito de Educación 12D02 Puebloviejo- Urdaneta para la realización del caso de estudio en dicha institución.

República del Ecuador

Ministerio de Educación

Oficio N° MINEDUC-CZ5-DD12D02-035-2021-OF

Urdaneta, 14 de septiembre del 2021

Ingeniera
Gina Carrasco Echeverría
DECANA DE LA FAFI.
En su despacho.-

De mi consideración

En contestación al oficio N° D-FAFI-UTB-095-UT-2021, de fecha 27/08/2021, suscrita por usted, donde solicita permiso para que VILLALVA QUIÑONEZ CLARA ISABEL, estudiante de la carrera Ingeniería en Sistema realice el análisis de las vulnerabilidades de la red LAN del Distrito de Educación 12D02 Puebloviejo Urdaneta.

En virtud a lo expuesto esta Dependencia Publica, autoriza el permiso a la estudiante VILLALVA QUIÑONEZ CLARA ISABEL, a realizar el análisis de las vulnerabilidades de la red LAN del Distrito de Educación 12D02 Puebloviejo Urdaneta previo la obtención del título Ingeniera en Sistema.

Particular que comunico a usted para los fines pertinentes.

Atentamente,

Firmado electrónicamente por:
MIRIAN SHIRLEY AGUILAR LIMONES

MSc. Mirian Aguilar Limones
DIRECTORA DISTRITAL
DIRECCIÓN DISTRITAL 12D02 PUEBLOVIEJO URDANETA

Gobierno del Encuentro | Juntos lo logramos

ANEXO IV

Autorización para la realización del caso de estudio

Entrevista al encargado del departamento de las TIC'S