*NETWORK ANALYZER*

*Gabriela Lara*

*Facultad de Ingeniería de Sistemas e Informática*

*UPB Bucaramanga*

*Bucaramanga, Colombia*

*gabriela.lara.2019@upb.edu.co*

*Silvia Coy*

*Facultad de Ingeniería de Sistemas e Informática*

*UPB Bucaramanga*

*Bucaramanga, Colombia*

*silvia.coy.2019@upb.edu.co*

*Camilo Gómez*

*Facultad de Ingeniería de Sistemas e Informática*

*UPB Bucaramanga*

*Bucaramanga, Colombia*

*camilo.gomez.2019@upb.edu.co*

I. INTRODUCCIÓN

Entre los principales recursos de infraestructura que se implementaron está el internet, el cual se ha utilizado para aplicar el esquema de teletrabajo y educación con apoyo de medios virtuales en instituciones y empresas, por tal motivo, se incrementó el volumen de tráfico de datos, lo cual no se tenía previsto, provocando problemas de conexión que afectan negativamente el desarrollo de las actividades por este medio. Por consiguiente, es preciso optimizar el uso del ancho de banda con el que cuenta cada residencia con el fin de evitar afectaciones, para ello se debe conocer detalladamente los servicios consumidos de cada hogar.

Teniendo en cuenta lo mencionado, a través de este proyecto se busca detectar el tráfico de información referente a los servicios de red de un hogar, y visualizar está en un tablero de control web, asimismo generar reportes de manera grafica donde se evidencie las estadísticas más relevantes de los datos recolectados.

II. ESTADO DEL ARTE

Esta sección Javier Salinas, [1] en 2013, en su tesis, presentó la construcción e implementación de una red IP virtualizada que implementa mecanismos de mitigación que induce los ataques, identifica su funcionamiento y elige el método más eficaz para mitigarlo.

Dominguez, Maya, Peluffo y Crisanto, [2] en 2016, en su artículo plantea un escenario de red donde implementa una red LAN con direccionamiento IP de clase C para realizar una prueba de concepto.

Javier de la paz Garcillan, [3] en 2019, presento la implementación de un sniffer de prime con BITSCOPE, el cual implanta una solución que permite escuchar en un canal de transmisión de mensajes PRIME, e interceptar la transmisión, leerla y poder obtener los bits a la salida de cada uno de los bloques de la cadena del receptor que desee, hasta la interpretación final del mensaje. todo esto por medio de una manera open-source y con una alternativa de hardware económica como lo es el procesador digital de señal y muestreador BitScope.

Erick Danilo Lara Hidalgo, [4] en 2020, desarrollo un aplicativo para caracterizar tramas 802.11 en redes inalámbricas utilizando software libre, que permite obtener parámetros determinados de forma automatizada del proceso de caracterización de redes inalámbricas en tiempo real, permitiendo escoger una característica determinada del tráfico de red y que esta sea desplegada dentro de una interfaz gráfica, comparando estas características obtenidas con características del sniffer Wireshark [4].

A. Pallavi y H. Patel [5] en 2012, Existen muchas herramientas disponibles para capturar el tráfico de red, pero algunas de estas herramientas solo capturan el tráfico de red sin analizarlo, por lo cual se necesitan utilizar otras herramientas para obtener las características del tráfico, estas pueden requerir de mucha memoria y solo tener la capacidad de rastrear paquetes IP o solo capturar paquetes tcp.

U. Banerjee, A. Vashishtha y M. Saxena [6] en 2010, Wireshark cuenta con muchas variaciones de filtrado como el filtrado basado en el tamaño del paquete, filtrado basado en los protocolos utilizados, filtrado de subcadenas, etc. Por lo tanto, con el uso adecuado de los comandos de filtrado y utilidades complementarias, Wireshark puede convertirse en un software de detección muy completo.

III. MARCO CONCEPTUAL

1. *Bases de datos*

Una base de datos es un conjunto organizado de datos o información estructurada, normalmente almacenados electrónicamente en un sistema de computadora. Generalmente una base de datos es controlada por un sistema gestor de base de datos (DBMS). Los datos y el DBMS, junto con aplicaciones conectadas a estos, se consideran un sistema de base datos, que a su vez es una base de datos. Las bases de datos se modelan comúnmente en filas y columnas en una seria de tablas para el procesamiento y consulta de datos eficiente, y que, con ello se pueda acceder, modificar, actualizar, controlar y organizar los datos.

Cabe resaltar que el lenguaje utilizado en casi todas las bases de datos es SQL, un lenguaje de programación usado para consultar, manipular, definir y proporcionar un control de acceso a los datos almacenados [7].

El concepto de base de datos es fundamental, para la creación de la base de datos, ajustes de desempeño de la base de datos, replicación y seguridad de esta, todo esto para el correcto desarrollo del proyecto.

1. *Ancho de banda*

Es el volumen de información que se puede enviar y recibir, es decir, transmitir a través de una conexión en un tiempo determinado, también conocido como tasa de transferencia de datos [8]. En otras palabras, es la medida de datos y recursos de comunicación disponible o consumida en una red de comunicación [9]. El ancho de banda se mide bits por segundo, sin embargo, es expresado frecuentemente en múltiplos como megabits por segundo (Mbps). Por otro lado, cuando se hace referencia al ancho de banda consumido en una red, indica la cantidad media de datos que se han transmitido exitosamente en una comunicación, denominado Throughput o Goodput [10].

En el proyecto se pretende realizar el análisis la cantidad de ancho de banda que consume un dispositivo en una red local. Esta información resulta útil al momento de realizar un análisis para determinar si es necesario aumentar el ancho de banda de un hogar.

1. *Direccionamiento IP*

El direccionamiento IP se considera una parte importante para los protocolos de capa de red ya que le asignan una dirección a cada red o dispositivo en internet que permite identificarlos y transmitir datos entre ellos [11]. La gestión de asignación automática de una dirección IP es realizada mediante los sistemas de direccionamiento conocidos como protocolos de internet [12], los cuales se encargan de entregar datagramas entre hosts de una red [13].

Los protocolos de internet actualmente utilizan dos versiones de IP para realizar esta labor mediante la conmutación de paquetes, las cuales son las direcciones IPv4 e IPv6. Principalmente se utilizaba el protocolo IPv4, sin embargo, con el aumento de redes y conexiones se agotaron más rápido de lo que se había previsto, lo que generó que la asignación se limitara, por esta razón optaron por adaptar una nueva versión denominada IPv6, la cual supera la capacidad de direccionamiento de IPv4 [14]. Estas direcciones son representadas en patrones binarios dado que las redes solo las interpretan en esta representación numérica, sin embargo, son expresadas en el sistema decimal para mayor comprensión [15].

Debido a que el direccionamiento IP permite identificar en internet una red o dispositivo, se emplean para conocer los detalles de los servicios de red consumido en cada uno de ellos, así como la cantidad de peticiones realizadas a una dirección IP determinada. También, es importante añadir que dentro del panorama de consumo se debe identificar el protocolo de internet utilizado.

1. *TCP/IP*

Los protocolos son conjuntos de normas para formatos de mensaje y procedimientos que permiten el intercambio de información entre máquinas y programas, para la correcta interpretación de estos mensajes las maquinas involucradas deben seguir las normas.

TCP/IP es un conjunto de protocolos que pueden interpretarse en forma de capas o niveles [16].

A continuación, se puede observar las capas del protocolo de TCP/IP, iniciando desde la parte superior son: capa de aplicación, capa de transporte, capa de red, capa de interfaz de red y hardware:

Gráfico, Gráfico de cajas y bigotes

Descripción generada automáticamente

Fig. 1. Conjunto de protocolos TCP/IP [16].

TCP/IP define como mover la información desde un remitente hasta un destinatario. Primeramente, los programas envían mensajes o corrientes de datos a uno de los de los protocolos de la capa de transporte de Internet, UDP (User Datagram Protocol) o TCP (Transmission Control Protocolo). Estos protocolos reciben la información de la aplicación, la dividen en partes pequeñas las cuales son llamadas paquetes, seguidamente añaden una dirección de destino, y después pasan los paquetes a la siguiente capa de protocolo, la capa de red de Internet.

En la capa de red de internet coloca el paquete en un datagrama de IP (Internet Protocol), pone la cabecera y la cola de datagrama, decide donde enviar el datagrama (directamente a un destino o a una pasarela) y traslada el datagrama a la capa de interfaz de red.

Finalmente, en la capa de interfaz de red acepta los datagramas IP y los transmite como tramas por medio de un hardware de red especifico [16]. Este Concepto es importante, para comprender y realizar la captura de los protocolos TCP y UDP, para el análisis que planteo en el proyecto.

1. *Redes de Datos*

Las redes de datos son infraestructuras que fueron creadas para poder transmitir información a través del intercambio de datos. En otras palabras, son estructuras con un fin especifico, cuya base es la conmutación de paquetes y que atienden a una clasificación exclusiva, teniendo en cuenta la distancia que puede cubrir su estructura física y el tamaño de esta [17].

Algunos de los elementos principales de las redes de datos son [17]:

* Hubs: Dispositivos para centralizar el cableado de una red, teniendo como objetivo la amplificación de señales, el cual es un proceso importante en el intercambio de datos.
* Patch Panels: Dispositivos de red eficaces y flexibles para mantener organizados centros de datos, estos son necesarios para disponer de un cableado organizado, necesario para el correcto funcionamiento.
* Servidores: Son sistemas que proporcionan recursos, datos, servicios o programas a través de una red, estos son los encargados de administrar la información y todo el proceso.
* Cables: Son de tipo horizontal, estos suelen elementos fundamentales de las redes de datos.

Tenemos en cuenta este concepto para el proyecto, debido a la importancia de la infraestructura de red, análisis de protocolos y servicios HTTP, FTP, DNS, SMTP, POP que se implementaran en servidores independientes.

1. *Sniffer*

Un sniffer es un programa que permite analizar el tráfico en una red de computadoras, y detectar problemas que existan en ellas. Este también puede ser usado para capturar, lícitamente o no, los datos que son transmitidos en la red. [18] el sniffer cuenta con una característica conocida como el "análisis del protocolo", que les permite "descifrar" el tráfico del ordenador debido a que los paquetes de datos de una red están dados en código binario.

Los sniffer cuentan con varias ventajas como lo podrían ser:

* Control del tráfico en la red
* Verificar el comportamiento de los usuarios de la red
* Recolección de datos para la generación de gráficas y estadísticas.
* Analizar los servicios que son más consumidos por los usuarios de una red.

Existen 2 tipos de sniffer, los cuales son: los hosts que se caracterizan por supervisar el tráfico de datos que hay en un computador. Mientras que los de red se deben instalar en un punto de acceso, el cual permita verificar el comportamiento de esta [19]. Este concepto nos permitirá conocer las acciones que se pueden realizar con un sniffer y la importancia de este.

1. *Lenguaje Unificado Modelado o UML*

Es un lenguaje estandarizado que permite desarrollar el modelado de un sistema o producto de software, donde se detalla todas las partes que lo componen mediante uno o varios diagramas [20]. Dicha herramienta de modelado proporciona técnicas sencillas, las cuales describen los límites, la estructura y el comportamiento del sistema gracias a su relación con el análisis y diseño orientado a objetos [21]. El modelado UML abarca diferentes tipos de diagramas que contribuirán a presentar en diferentes perspectivas el sistema de información. Algunos de los diagramas incluidos son el diagrama de clases, de casos de uso, de estados, de componentes, entre otros [22].

1. *Agile Inception*

Es una metodología de desarrollo ágil que adopta un modo de trabajo de acuerdo con las condiciones del proyecto, lo que permite gestionar su desarrollo de forma flexible y eficaz [23]. Se establecen una serie de actividades encaminadas a cumplir con el propósito y las expectativas del proyecto, las cuales generalmente se planifican entre un periodo de tres a seis meses, donde todas las personas que participaran en el proyecto pueden brindar su opinión al resto del equipo, lo que contribuye a una buena realización de la documentación y, por ende, permite que el proyecto se realice con más entendimiento [24].

1. *Scrum*

Es un marco de trabajo ágil en el que se aplican un conjunto de normas para organizar a un equipo de trabajo a través de diferentes roles. En scrum se realizan entregas parciales y regulares del producto, priorizando las entregas que más aporten al proyecto [25]. En el desarrollo del proyecto se despliegan una serie de roles, los cuales son:

* Scrum máster: persona lidera al equipo guiándolo para que cumplan las reglas y procesos de la metodología.
* Product owner: representa a los clientes del software y traslada la visión del Proyecto al equipo.
* Team: grupo de personas que poseen conocimientos técnicos necesarios para llevar a cabo el proyecto de manera conjunta [26].

Wireshark

Es un analizador de red que permite capturar y monitorear paquetes de red que pasan por un equipo. Permitiendo inspeccionar a profundidad el trafico que circula por una red y así tomar decisiones de esta [27].

Funcionalidades:

* Capturar datos de red en tiempo real.
* Mostar, filtrar y buscar paquetes de datos.
* Importación de paquetes de datos desde archivos de texto.
* Examinar paquetes de datos y sus detalles de protocolo.

IV. OBJETIVOS

1. *Objetivo General*

Desarrollar una aplicación web que permita generar un tablero de control web con relación a los servicios consumidos en un rango de tiempo determinado, mediante la utilización de un lenguaje de programación orientado a web y una base de datos relacional.

1. *Objetivos específicos*

- Plantear la arquitectura tecnológica que dé soporte a la infraestructura del sistema de información.

- Elaborar modelos que permitan especificar el sistema de información a través de la utilización de herramientas de modelado.

- Diseñar un sistema de información mediante herramientas de software libre que permitan cumplir con los requerimientos establecidos.

V. METODOLOGÍA

Se utilizará la metodología de desarrollo Ágil Inception, la cual consiste en elaborar una lista de actividades ordenadas por prioridad, luego de esto se hace una repartición equitativa entre todos los miembros del equipo y se definen las reuniones regulares para presentar los avances respectivos con las actividades propuestas en la lista. Las reuniones regulares se realizan para tener un avance mayor y que todo el equipo concuerde con lo desarrollado [28].

La metodología que se seguirá consiste en los siguientes pasos, teniendo en cuenta que al existir un problema se regresa al anterior hasta encontrar una solución:

1. *Investigación preliminar.*

* Investigar temas relacionados al proyecto que permitan analizar y desarrollar los requerimientos previamente proporcionados.

1. *Planteamiento del proyecto.*

* Realizar la propuesta del proyecto.
* Realizar el documento de especificación de requerimientos (funcionales y no funcionales)
* Seleccionar el lenguaje de programación con el cual se realizará el aplicativo web.
* Seleccionar el sistema gestor de base de datos idóneo para el proyecto.

1. *Elaboración de modelos.*

* Elaborar el diagrama de casos de uso
* Elaborar documento de especificación de arquitectura tecnológica
* Realizar un prototipo de papel de la interfaz.
* Elaborar el modelo entidad-relación y diccionario de datos.
* Elaborar el Diagramas de UML de acuerdo con el avance del proyecto (estructuras, comportamientos, despliegue, infraestructura).

1. *Desarrollo del sistema de información*

* Desarrollar el diseño del aplicativo web en JavaScript
* Diseñar un algoritmo que permita la captura del tráfico de la red, y mediante este algoritmo poder capturar la Dirección IPv4 y/o IPv6, Nombre del dispositivo o sistema operativo, Servicio de red consumido, Tiempo de inicio de la medición, Tiempo de fin de la medición y Total de tiempo consumido medido en segundos.
* Documentar el código fuente a medida que se va desarrollando el software.
* Elaborar una base de datos relacional mediante el sistema de gestión de bases datos.
* Generar un respaldo de la base de datos.
* Implementar librerías que permitan graficar las estadísticas más relevantes acerca de los datos recolectados en la base de datos.
* Desarrollar un tablero web donde se incluyan las gráficas de las estadísticas más relevantes acerca de los datos recolectados.

1. *Documentación*

* Realizar el documento de políticas de backup, manual de usuario.

1. *Validación*

* Verificar el correcto funcionamiento del aplicativo web por medio de un protocolo de pruebas para la verificación del correcto funcionamiento de la aplicación.

Diagrama

Descripción generada automáticamente

Fig. 2. Metodología Ágil Inception

VI. RESULTADOS

De acuerdo con el cronograma se han obtenido los siguientes resultados:

|  |  |
| --- | --- |
| BASE DE DATOS II | Modelo Entidad-Relación y Diccionario de Datos. |
| REDES DE DATOS | Extracción de cabeceras de protocolos de servicio por medio de un archivo json, topología de red de prueba y servidor DHCP. |
| INGENIERIA DE SOFTWARE | Prototipo de Interfaz, Diagrama de casos de Usos, Requerimientos Funcionales y no Funcionales, Documento de especificación de Arquitectura Tecnológica y políticas de backup. |

VII. CRONOGRAMA

A continuación, se muestra el cronograma de actividades del proyecto, el cual se ha desarrollado en un 80% aproximadamente. Este se encuentra anexado en los documentos enviados.



Fig. 3. Cronograma del proyecto

VIII. DISCUSIÓN.

Según los resultados, se ha logrado llevar acabo el proyecto utilizando la herramienta wireshark, la cual se decidió implementar debido a retrasos en la investigación, gracias a esta herramienta se adquirieron los datos para filtrar los servicios de red consumidos en un hogar y evitar retrasos en el cronograma.

IX. CONCLUSION.

Se pudo concluir que es importante una buena práctica de documentación, dado que el diagrama de casos de uso y el documento de especificaciones permite que se desarrolle el proyecto con los parámetros correspondientes, y que la interfaz de usuario cumpla con lo propuesto. Además, la Arquitectura Tecnológica es fundamental al momento de realizar el proyecto ya que se especifican los componentes que integran el sistema de información y contribuye al buen desarrollo del proyecto. Por otro lado, es posible deducir el servicio que cuenta con mayor flujo y la dirección ip con mayor cantidad de peticiones por servicio.

XI. TRABAJO FUTURO

Se tiene pensado en un futuro mejorar el rendimiento y funcionalidad del proyecto.

XII. AGRADECIMIENTOS

Un especial agradecimiento a nuestros profesores, su ayuda fue indispensable a la hora de forjar las bases del proyecto.

XIII. ANEXOS

* Cronograma: El archivo anexado tiene como nombre “Cronograma\_Proyecto.xlsx”.
* Requerimientos Funcionales y no Funcionales: El archivo anexado tiene como nombre “Documento REQUERIMIENTOS FUNCIONALES.pdf”.
* Arquitectura Tecnológica: El archivo anexado tiene como nombre “ARQUITECTURA TECNOLOGICA.png”.
* Prototipo de Interfaz: El archivo anexado tiene como nombre “PROTOTIPO DE INTERFAZ.pdf”.
* Modelo Entidad-Relación: El archivo anexado tiene como nombre “Modelo Entidad Relacion\_Proyecto.mwb”.
* Diccionario de Datos: El archivo anexado tiene como nombre “Diccionario de Datos\_proyecto.sql”.

REFERENCIAS

[1] J. Salinas, «Tesis Diseño y construcción de una red IP virtualización para la aplicación de hacking ético,» 05 2013. [En línea]. Available: http://dspace.ups.edu.ec/handle/123456789/4908.

[2] E. M. D. P. C. C. Hernan Dominguez, «Aplicación de técnicas de fuerza bruta con diccionario de datos, para vulnerar servicios con métodos de autenticación simple “Contraseñas”, pruebas de concepto con software libre y su remediación,» de Actas del IV Congreso Ecuatoriano de Tecnologías de la información y comunicación, Ibarra, Ecuador, 2016.

[3] J. d. l. p. Garcillan, «Repositorio comillas,» [En línea]. Available: https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/32809/TFM%20-%20delaPazGarcillanJavier.pdf?sequence=1&isAllowed=y.

[4] E. Lara, «Repositorio ESPE,» [En línea]. Available: http://repositorio.espe.edu.ec/bitstream/21000/22400/1/T-ESPE-043755.pdf.

[5] A. Pallavi y P. Hemlata, «CiteSeerx,» 5 Mayo 2012. [En línea]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.429.567&rep=rep1&type=pdf. [Último acceso: 3 Septiembre 2021].

[6] B. Usha, V. Ashutosh y S. Mukul, «ResearchGate,» 7 Septiembre 2010. [En línea]. Available: https://www.researchgate.net/profile/Usha-Banerjee/publication/46280039\_Evaluation\_of\_the\_Capabilities\_of\_WireShark\_as\_a\_tool\_for\_Intrusion\_Detection/links/0deec519eb16b798ef000000/Evaluation-of-the-Capabilities-of-WireShark-as-a-tool-for-Intrusion-Detect. [Último acceso: 3 Septiembre 2021].

[7] «ORACLE,» [En línea]. Available: https://www.oracle.com/co/database/what-is-database/.

[8] «Verizon,» [En línea]. Available: https://espanol.verizon.com/info/definitions/bandwidth/.

[9] F. Quiñonez, «Repositorio Digital Pucese,» 03 2016. [En línea]. Available: https://repositorio.pucese.edu.ec/bitstream/123456789/632/1/QUI%C3%91ONEZ%20ANGULO%20FRANCISCO%20XAVIER.pdf.

[10] J. Castillo, «Profesional Review,» 07 02 2019. [En línea]. Available: https://www.profesionalreview.com/2019/02/07/ancho-de-banda-definicion/.

[11] «Google Sites,» [En línea]. Available: https://sites.google.com/site/investigacionesitlm/3-capas-inferiores-del-modelo-osi-y-tcp-ip/3-1-4-direccionamiento-ip.

[12] «Avast academy,» [En línea]. Available: https://www.avast.com/es-es/c-what-is-an-ip-address.

[13] «Speedcheck,» [En línea]. Available: https://www.avast.com/es-es/c-what-is-an-ip-address.

[14] «Solvetic,» 19 11 2019. [En línea]. Available: https://www.solvetic.com/page/recopilaciones/s/internet/caracteristicas-diferencias-protocolo-internet-ipv4-ipv6.

[15] F. d. e. d. C. d. Andalucia, «Feandalucia,» [En línea]. Available: https://www.feandalucia.ccoo.es/docu/p5sd7257.pdf.

[16] IBM AIX documentation, «IBM,» [En línea]. Available: https://www.ibm.com/docs/es/aix/7.2?topic=protocol-tcpip-protocols. [Último acceso: 29 Julio 2021].

[17] Universidad Internacional de Valencia, «VIU,» 9 Octubre 2018. [En línea]. Available: https://www.universidadviu.com/int/actualidad/nuestros-expertos/redes-de-datos-todo-lo-que-hay-que-saber-sobre-ellas. [Último acceso: 29 Julio 2021].

[18] A. A. B., «Sniifer " ventajas y desventajas para administradores y atacantes",» Valparaiso, 2004.

[19] M. P. F. M. M. S. S. David Manuel Arenas Gonzalez, «Sniffer UCM,» UNIVERSIDAD COMPLUTENSE, madrid, 2004.

[20] «Diagramas UML,» [En línea]. Available: https://diagramasuml.com/.

[21] «LucidChart,» [En línea]. Available: https://www.lucidchart.com/pages/es/que-es-el-lenguaje-unificado-de-modelado-uml.

[22] «Teatro de abadía,» [En línea]. Available: https://www.teatroabadia.com/es/uploads/documentos/iagramas\_del\_uml.pdfv.

[23] V. R. Villlan, «IEBS,» [En línea]. Available: https://www.iebschool.com/blog/que-son-metodologias-agiles-agile-scrum/.

[24] M. L. Mendoza, «OpenWebinars,» [En línea]. Available: https://openwebinars.net/blog/agile-inception-que-es-y-como-ejecutarlo/.

[25] M. M. Canelo, «Profile,» [En línea]. Available: https://profile.es/blog/que-es-scrum/.

[26] «Softeng,» [En línea]. Available: https://www.softeng.es/es-es/empresa/metodologias-de-trabajo/metodologia-scrum/proceso-roles-de-scrum.html.

[27]cl0udswx\_sequre,«https://cl0udswxsequre.wordpress.com/2020/05/09/wireshark-que-es-y-para-que-sirve/,» 9 mayo 2020. [En línea]. [Último acceso: 24 10 2021].

[28] «Atlassian,» [En línea]. Available: https://www.atlassian.com/es/agile/scrum.