`+

UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

NOVIEMBRE 2020 - MAYO 2021

EXAMEN COMPLEXIVO DE GRADO O FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DE TITULO DE INGENIERO EN SISTEMAS

TEMA:

ANÁLISIS DE VULNERABILIDADES EN EL TRÁFICO DE LA RED Y ESTRUCTURA FÍSICA DEL WIFI EN LA UNIVERSIDAD TÉCNICA DE BABAHOYO

EGRESADA:

DIAZ VILLACIS DENISE THALIA

TUTOR:

ING. ANA FERNANDEZ

AÑO 2021

TEMA DE ESTUDIO

Análisis de vulnerabilidades en el tráfico de la red y estructura física del wifi en la Universidad Técnica de Babahoyo.

INTRODUCCIÓN

La relevancia de internet en los últimos años crece cada día más y nunca se había notado más que en este 2020 por las medidas de confinamiento que el mundo está atravesando por la pandemia del Covid-19 y los cambios de habito en relación con el consumismo, las personas con acceso a internet de todas las formas tuvieron que adaptarse a los nuevos retos que planteaba la aparición de este nuevo virus respecto a las plataformas digitales y sus medios de conexión.

Según los indicadores del informe digital 2021 del We Are Social y Hootsuit, el crecimiento de usuarios en el mundo que consumen internet se incrementó en un 7.3% en enero del 2021 en comparación con enero del 2020. (We Are Social y Hootsuite, 2021), además, los datos del reporte del Banco Mundial para el año 2019 indican que en el Ecuador el 57% de la población tienen acceso a internet (Banco Mundial, 2019). Con estos datos podemos decir que el acceso a internet día a día se convierte en una necesidad para el desarrollo de las comunidades en general y más aun para la educación y sus estudiantes, que se convierte en una herramienta fundamental para la investigación y el desarrollo (I+D).

La Universidad Técnica de Babahoyo es una institución de educación pública, la cual para el año 2019 no contaba con una red de acceso a internet mediante WIFI para sus estudiantes, personal docente y administrativos, con la posesión del Ing. Marcos Oviedo Rodríguez PhD como Rector de esta institución se realizó la implementación de una red WIFI para la distribución de internet en todo el campus universitario de manera gratuita.

Se escogió la Universidad Técnica de Babahoyo, para realizar el caso de estudio "Análisis de vulnerabilidades en el tráfico de la red y estructura física del wifi en la Universidad Técnica de Babahoyo." Por ser una institución educativa que cuenta con 10200 estudiantes (Universidad Técnica de Babahoyo, 2021), para ello se realizó la entrevista para pedir información al responsable de la Dirección de Tecnologías y Sistemas de Información y a los técnicos responsables encargados del Área de Telemática y Soporte, donde se conoció la estructura de la red implementada para el servicio de conexión WIFI para el servicio de internet.

Se realizó un listado de todos los dispositivos que se utilizan para la red WIFI, además se realizó un monitoreo de la red mediante la aplicación WiFiman de la empresa Ubiquiti, la cual nos ayudó a tener más información del estado de todos los Access Point (AP), conociendo así su ancho de banda, canales de distribución, niveles de señal y otros datos para saber si se aplica los niveles de seguridad recomendados en dicha red.

El siguiente caso de estudio abarca el análisis de toda la infraestructura de red WIFI para evaluar la información recogida y determinar si existen problemas en la red y así poder llegar

a una conclusión para brindar las respectivas recomendaciones que puedan llegar a obtener una posible solución de estos.

DESARROLLO

El análisis de una red es un proceso importante ya que mediante este se puede conocer el estado actual de la misma y a su vez conocer las debilidades, vulnerabilidades, problemas y fallos que puede tener la misma, esta tarea debe ser realizada de manera periódica en una red para brindar el mantenimiento preventivo y correctivo respectivamente de ser el caso y garantizar la seguridad de esta. (welivesecurity, 2014)

El alcance de este análisis es verificar cuales son las fallas y vulnerabilidades de la red WIFI con la recopilación de la información brindada por el Departamento de Tecnologías y Sistemas de Información, dicho análisis cuenta con dos fases, la primera es una revisión del equipamiento físico y la segunda es analizar el apartado lógico para determinar si existen vulnerabilidades o fallas en su implementación, para al final poder realizar una conclusión y recomendación luego del análisis de estos.

INFORMACION DE LA INSTITUCIÓN

La Universidad Técnica de Babahoyo es una institución de educación superior la cual está dirigida en la actualidad por su Rector el Ing. Marcos Oviedo Rodríguez PhD. En dicha institución en la actualidad se brindan 18 carreras universitarias, en las que estudian 10200

estudiantes, la mayoría de ellos provienen de la provincia de Los Ríos y la otra parte provienen de las provincias aledañas, además, cuenta con un total de 461 docentes y está dividida en 4 facultades y 2 extensiones. (Universidad Técnica de Babahoyo, 2021).

Por la necesidad de conexión a internet mediante WIFI y satisfacer la demanda de los estudiantes, personal docente y administrativo, la institución implemento una red de conexión para instalar todos los equipos necesarios requeridos para el despliegue de internet WIFI en todo el campus universitario.

DESCRIPCIÓN ACTUAL DE LA INFRAESTRUCTURA DE LA RED WIFI DE LA UNIVERSIDAD TECNICA DE BABAHOYO.

Para la implementación de este servicio, se realizó el despliegue de una nueva red de fibra óptica, la cual permitía instalar varios gabinetes ubicados estratégicamente en todos los edificios de la universidad, los mismo que sirven de organizador para la instalación de los Switch donde van a ir conectados los equipos que funcionan como Access Point.

Imagen #1: Despliegue de la nueva red de fibra óptica para el WIFI en el Campus Central foto satelital.

Fuente: Dirección de Tecnologías y Sistemas de Información.

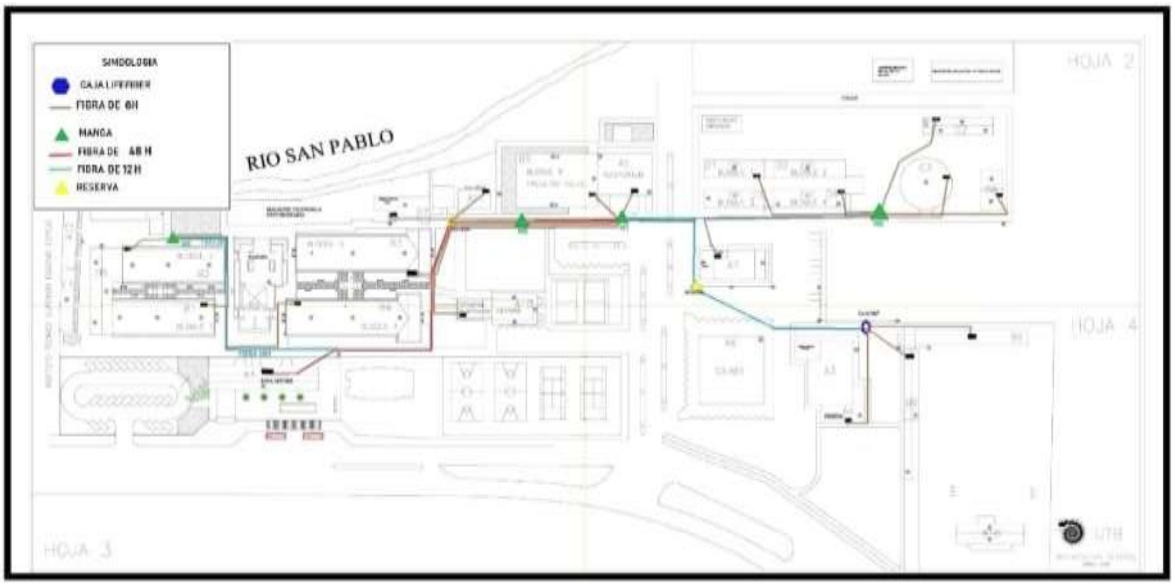

Imagen #2: Despliegue de la nueva red de fibra óptica para el WIFI en el Campus Central.

Fuente: Dirección de Tecnologías y Sistemas de Información.

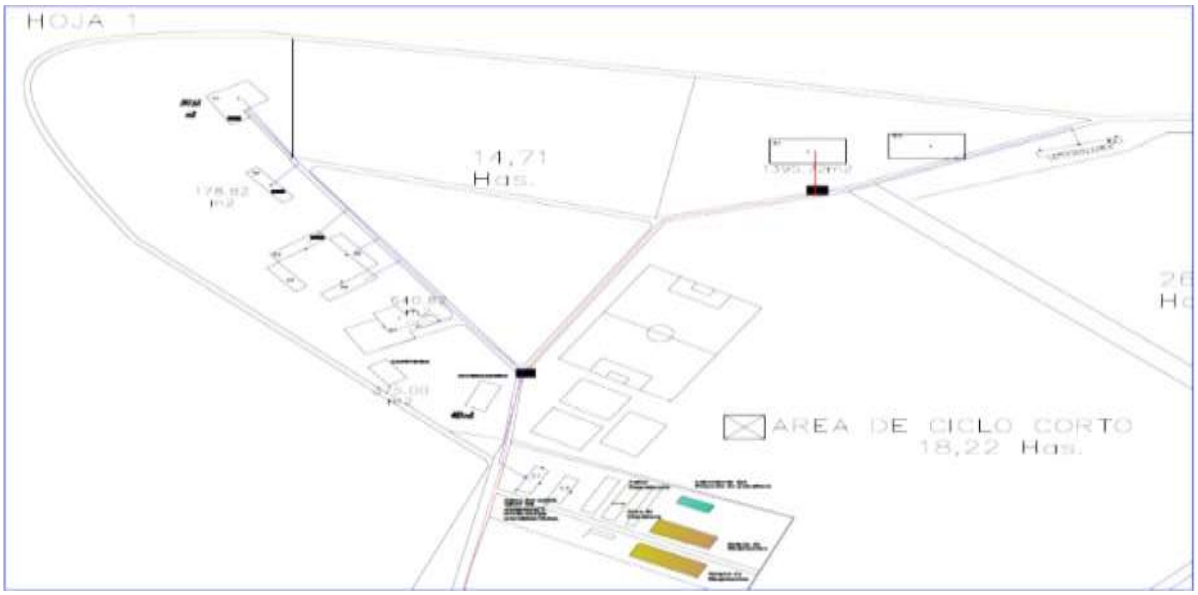

Imagen #3: Despliegue de la nueva red de fibra óptica para el WIFI en FACIAG.

Fuente: Dirección de Tecnologías y Sistemas de Información.

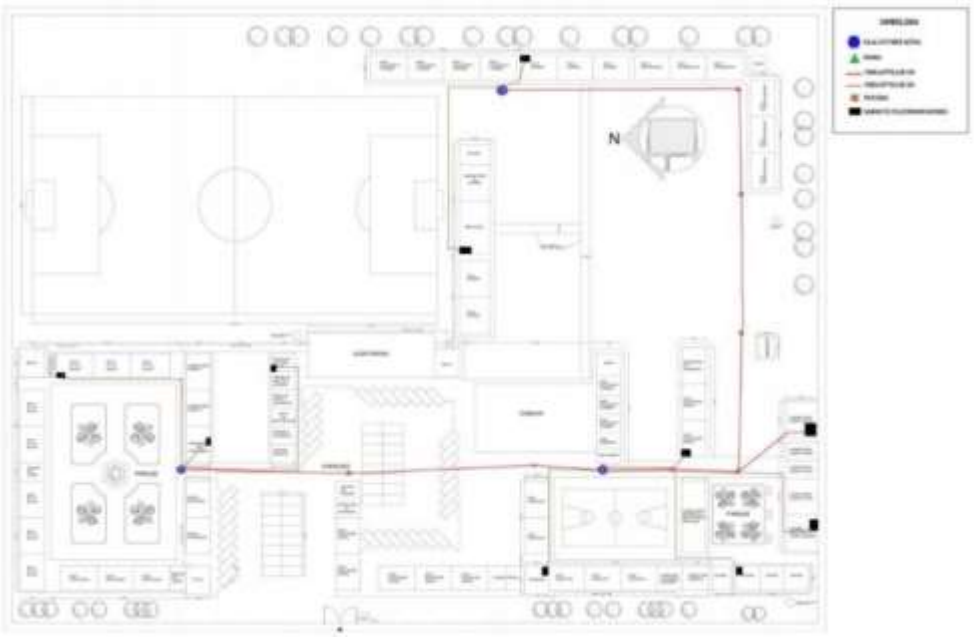

Imagen #4: Despliegue de la nueva red de fibra óptica para el WIFI en la Extensión Quevedo.

Fuente: Dirección de Tecnologías y Sistemas de Información.

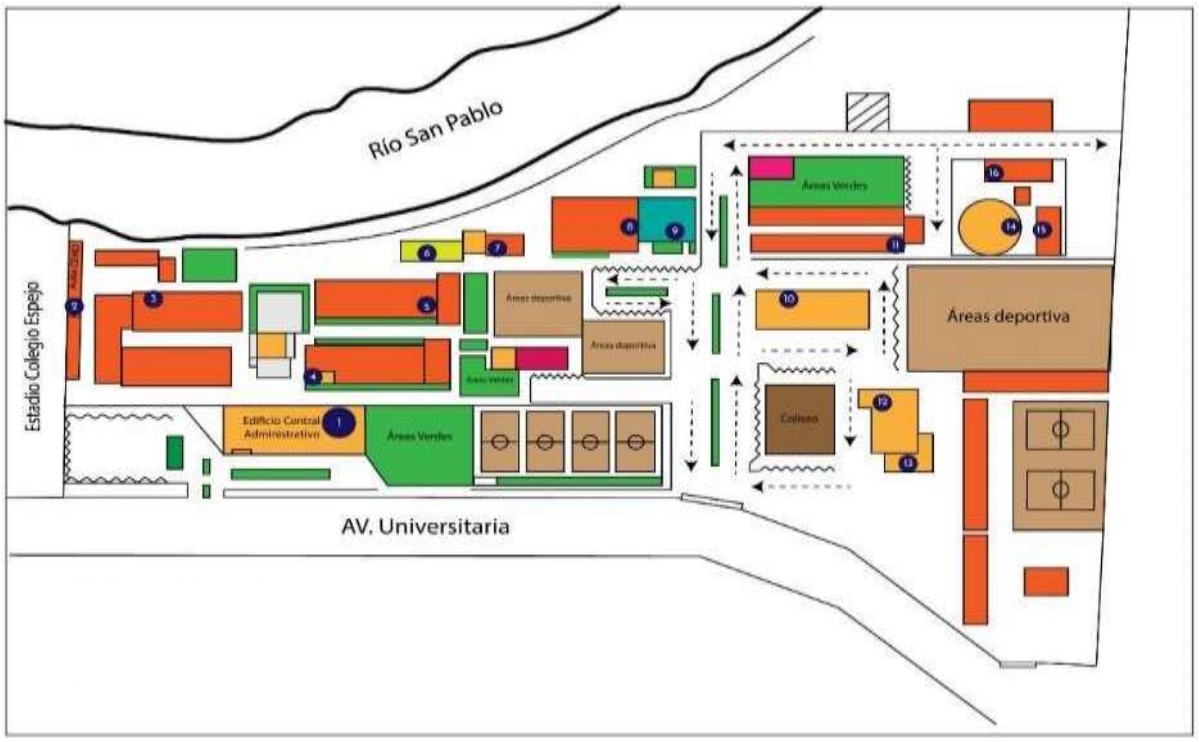

Imagen #5 Despliegue y ubicación Gabinetes para los Switchs.

Fuente: Dirección de Tecnologías y Sistemas de Información.

Como se observa en la imagen #5 la universidad realizo el despliegue lo gabinetes de manera estratégica donde se ubican los switch que a su vez permitirán la conexión de los Access Point.

A continuación, se muestra el esquema lógico de la infraestructura de la red WIFI:

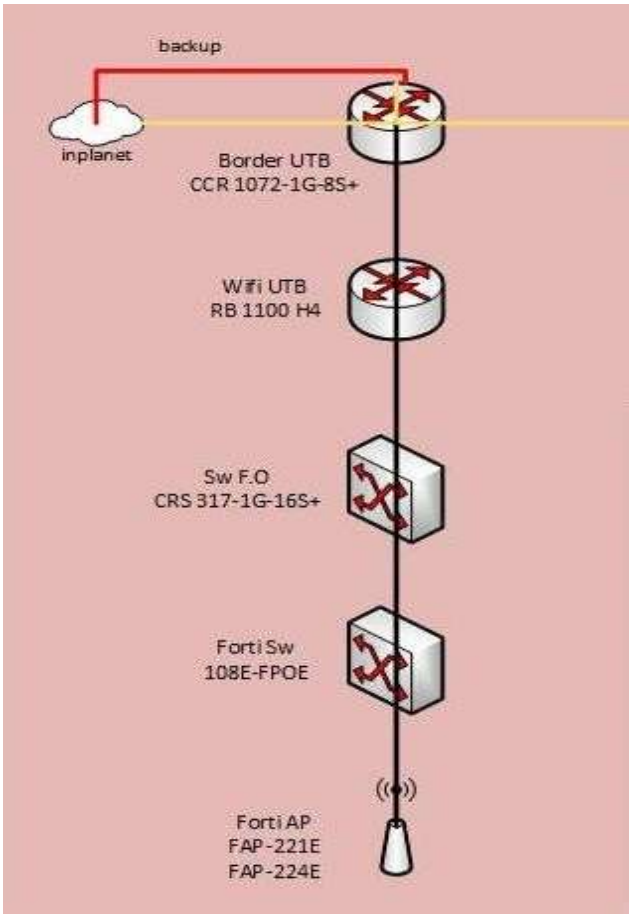

Imagen #6: Mapa lógico de la red WIFI.

Fuente: Dirección de Tecnologías y Sistemas de Información.

En la imagen #6 se puede observar el diagrama de red lineal que la Universidad Técnica de Babahoyo utiliza para la distribución del internet a los diferentes puntos de acceso.

Descripción de equipos utilizados en la implementación son los siguientes:

Mikrotik RB1100 4H.- Este equipo es utilizado como equipo máster de control de tráfico de red, es en este equipo donde se declaran las redes, servidor DHCP, tabla de routeo y configuración de NAT.

Mikrotik Switch CRS 317-1G-16S+. - Este equipo es utilizado para la distribución del internet a los gabinetes mediante fibra óptica.

Fortiswitch 108E-FPOE. - Hay un total de 17 de estos switch distribuidos en los gabinetes colocados estratégicamente en la casona universitaria, estos equipos a diferencia de otros switch trabajan con el protocolo 802.11 af que sirve para energizar los AP.

FortiAP FAP-221E.- Estos equipos de la marca Fortinet, son equipos Access Point de alta redundancia, en su datasheet mencionan que soportan el tráfico de hasta 250 clientes concurrentes conectados y además trabajan en doble banda, es decir en 2.4Ghz y 5Ghz, existen 77 equipos AP en todo el campus.

ANALISIS DEL TRAFICO DE RED WIFI DE LA UNIVERSIDAD TECNICA DE BABAHOYO

Para el siguiente análisis del tráfico de red se consideran varios aspectos que involucran a una buena distribución del internet y sus vulnerabilidades, a continuación, mencionaremos los siguientes puntos a analizar:

- Trafico del Internet.
- Calidad del Internet.
- Cobertura de la señal WIFI.

Trafico del Internet.

La Dirección de Tecnologías y Sistemas de Información, para el análisis del tráfico de internet ya utiliza un firewall centralizado, en el que se analiza el tráfico de internet y se aplican distintas políticas de seguridad, para mitigar las diferentes vulnerabilidades que existen en internet.

El equipo hardware utilizado para el análisis de red es un Next Generation Firewall (NGFW), de la marca Fortinet, el Fortigate 600e, este equipo es utilizado para el análisis del tráfico de toda la universidad, tanto cableada como WIFI.

El análisis de red se realiza en dos canales diferentes, conectados mediante interfaces físicas separadas, esto quiere decir que se analiza de manera separa el tráfico de la red cableada y el tráfico de la red WIFI.

Para analizar el tráfico de la data generada por las conexiones WIFI el equipo de borde CCR1070-1G-8S+ realiza un redireccionamiento al Fortigate 600e mediante un canal dedicado, en este último equipo mediante políticas generadas internamente, se trata de mitigar la mayor parte de Trafico Basura, Spam, Virus, Malware, Botnets, Ataques DoS, Pishing, Ataques DNS, Rasomware, Minería de criptomonedas, entre otros.

FortiGate Network Firewalls NGFW, al estar enfocado a redes controladas por seguridad, que protege cualquier borde a cualquier escala, por ser el premio a la mejor elección por los clientes de Gartner Peer Insights (Gartner Peer Insights, 2020) y por estar entre los mejores en el cuadrante de Gartner (Fotinet, 2020), es una de las alternativas de análisis de trafico de red más acertadas al momento de realizar dicho análisis.

Imagen #7: Cuadrante mágico de firewalls de red.

Fuente: Fortinet 2020.

A continuación, se muestra imágenes de las principales amenazas que detecta el análisis en el firewall y los equipos que están vulnerables y pueden estar originando o son víctimas de dichas amenazas.

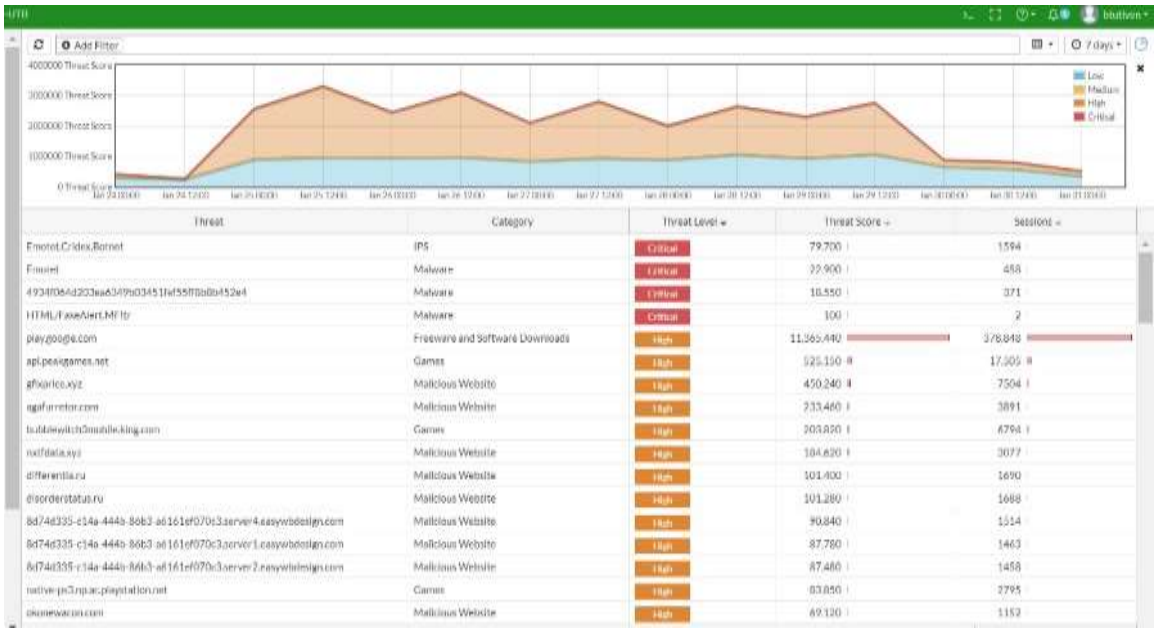

Imagen #8: Grafica de amenazas de red.

Fuente: Dirección de Tecnologías y Sistemas de Información.

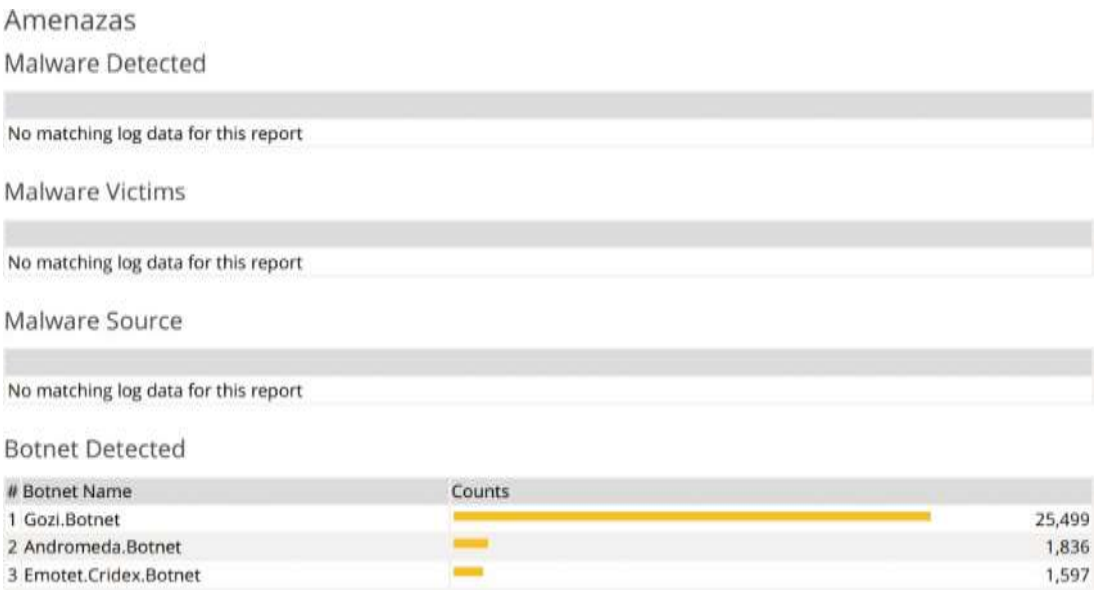

Imagen #9: Imagen de las principales amenazas de red.

Fuente: Dirección de Tecnologías y Sistemas de Información.

Botnet Victims

#	Victim Name (or IP)	Counts
1	172.16.11.40	3,395
2	172.16.4.21	3,161
3	172.16.4.49	2,693
4	172.16.10.52	2,659
5	172.16.10.62	2,400
6	172.16.10.89	2,388
7	172.16.6.248	2,136
8	172.16.10.35	2,043
9	172.16.12.147	2,031
10	172.16.10.56	1,760
11	172.16.6.116	1,597
12	172.16.10.46	1,244
13	172.16.12.21	1,003
14	172.16.10.84	300
15	172.16.10.91	122

Imagen #10: Imagen de las principales víctimas en la red LAN de Botnet.

Fuente: Dirección de Tecnologías y Sistemas de Información.

Intrusions Detected

#	Attack Name	Severity	CVE-ID	Counts
1	Gozi.Botnet	Critical		25,499
2	Andromeda.Botnet	Critical		1,836
3	Emotet.Cridex.Botnet	Critical		1,597
4	MikroTik.RouterOS.Arbitrary .File.Read	Critical	CVE-2018-14847	4
5	malicious-url	High		836
6	WebRTC.Local.IP.Addresses. Disclosure	Medium	CVE-2018-6849	9
7	TCP.Split.Handshake	Medium		7

Imagen #11: Imagen de las principales Intrusiones detecta das.

Fuente: Dirección de Tecnologías y Sistemas de Información.

Intrusion Victims

#	Attack Victim	Counts
1	63.251.235.71	1,827
2	91.121.153.56	421
3	93.190.138.164	399
4	88.198.35.181	395
5	178.63.80.208	386
6	91.121.181.195	361
7	78.46.76.121	355
8	144.76.8.48	354
9	5.9.144.217	349
10	5.9.108.185	344

Imagen #12: Imagen de las principales víctimas de intrusiones.

Fuente: Dirección de Tecnologías y Sistemas de Información.

En las imágenes anteriores se puede observar que las principales amenazas son detectadas y neutralizadas por el servidor de análisis de amenazas (Fortigate), son los botnets en su mayoría, también se puede observar las IPs tanto públicas como privadas que están comprometidas o generan esta amenaza de red.

Calidad del Internet.

Para el análisis de calidad de Internet y la calidad de la señal de Internet se utilizó un programa de análisis de red diseñado y desarrollado por la empresa Ubiquiti que se dedica a la distribución y fabricación de equipos del internet, WiFiman nos permitirá realizar: test de velocidad, conocer el estado de la conexión, el estado de la señal inalámbrica y los equipos conectados a la misma.

Para la realización de dicho análisis, se realizaron conexiones en diferentes puntos de acceso ubicados en el campus principal de la universidad.

Cabe mencionar que el SSID (*Service Set IDentifier* o identificador de paquetes de servicio en español) de la red pública de la universidad se denomina PorTiUTB y fue sobre la misma que se realizó dicho análisis.

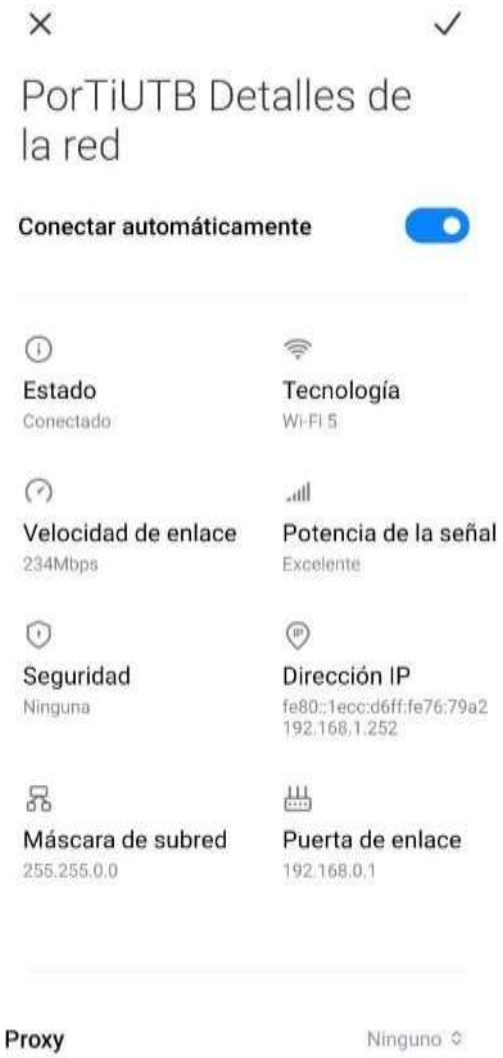

Imagen #13: Imagen del estado de conexión a la red PorTiUTB.

Fuente: Dirección de Tecnologías y Sistemas de Información.

Se utilizo un teléfono móvil con la capacidad de conexión a una red 5Ghz, como se observa en la imagen 13, los análisis se realizan en con un nivel de potencia excelente o bueno y con una velocidad de enlace que varía entre los 150 Mbps y los 350 Mbps.

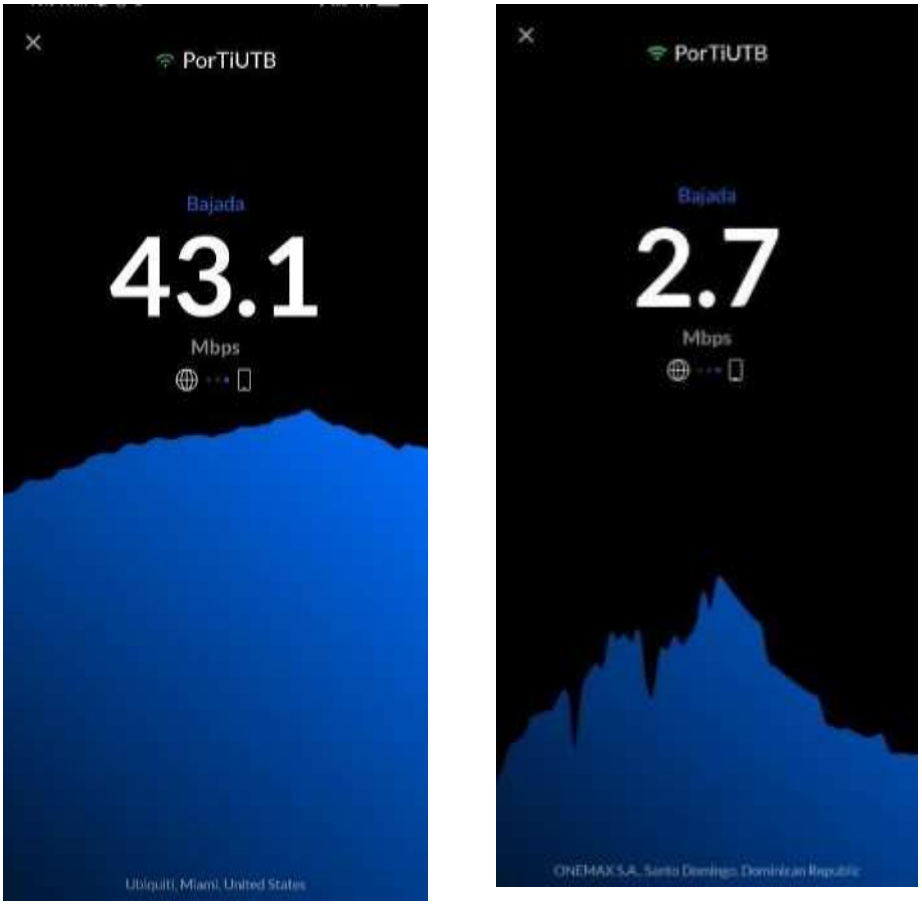

Imagen #14: Imágenes de la velocidad de bajada de la red PorTiUTB en distintos puntos de acceso.

Fuente: Universidad Técnica de Babahoyo.

Se realizo test de velocidad en el 50% de los AP del campus central de la universidad y se pudo observar que en toda la lectura de la medición varia de entre 50 Mbps y 0.5 Mbps, como se puede observar en la imagen 14 de este documento, se representa dos velocidades de bajada de 2 AP diferentes escogidos aleatoriamente.

Imagen #15: Imágenes del estado de red, nivel de señal y continuidad de señal.

Fuente: Universidad Técnica de Babahoyo.

Se realizo el análisis del estado de red, donde se pudo observar que en todas las oficinas y lugares de asentamientos estudiantiles como aulas y pasillos de los edificios existe un buen nivel de señal que fluctúa entre los -80 dBm y los -36 dBm, sin perdidas de señal manteniendo una recepción de señal continua y sin variantes. Un dato importante que se observo es que, pese a los niveles de señal en excelente estado, el ping hacia los distintos servicios como Google, Facebook, DNS de Google, y la Puerta de enlace son muy elevados.

Imagen #16: Imágenes del estado de los canales de las frecuencias 2.4Ghz.

Fuente: Universidad Técnica de Babahoyo.

Se procedió con el análisis de los canales de la frecuencia 2.4 Ghz de la conexión Wireless y se pudo observar que existen muchas redes WIFI, muchas de las cuales transmiten por el

mismo canal, causando un fenómeno denominado solapamiento de canal. La frecuencia 2.4 Ghz al solo contar con 13 canales de transmisión, cada uno con un ancho de banda de 22Mhz (wifi scan, s.f.), no permite la distribución correcta de frecuencias al tener muchas conexiones WIFI, esto ocasiona que dicho fenómeno aparezca lo cual puede causar distintos problemas como:

- Baja velocidad.
- Señal inestable.
- Pérdida de señal y menor cobertura.
- Desconexiones.
- Problemas para conectarnos a nuestra red.

Imagen #17: Imágenes del estado de los canales de las frecuencias en 5Ghz.

Fuente: Universidad Técnica de Babahoyo.

En las imágenes anteriores (Imagen #11) se observa que también existe solapamiento de canal en la frecuencia de 5Ghz, pese a que este existe 23 canales no superpuestos, los Access Point superponen su canal de distribución.

Cobertura de la señal WIFI

A continuación, se presenta el mapa de calor de la red WIFI en el campus central de la Universidad Técnica de Babahoyo.

Imagen #12 Ubicación y mapa de calor de los Access Point.

Fuente: Dirección de Tecnologías y Sistemas de Información.

En cuanto a la señal se refiere, la Dirección de Tecnologías y Sistemas de Información muestra una imagen del mapa de calor de la señal WIFI, misma señal que se verifico con la aplicación WiFiman que se utilizó en este caso de estudio, para el análisis y se comprobó que la mayor parte de espacios concurridos están cubiertos con una señal dentro del rango de lo aceptable.

CONCLUSIONES

Tras haber analizado la manera en que se procesa el trafico de red, observando que para dicho procesamiento y análisis se utiliza un Next Generation Firewall de la marca Fortinet, siendo esta una empresa reconocida por sus firewalls de gran eficiencia se concluye que la UTB si analiza y protege la información que circula por la infraestructura dedicada a la distribución de la red WIFI, no agregando ninguna recomendación al respecto.

En cuanto a la calidad del internet utilizando la aplicación de WiFiman y luego de observar las imágenes se puede llegar a la conclusión de que el internet en ciertos puntos del campus universitario no llega con la calidad que se espera, pese a que el nivel de señal es muy bueno en ocasiones se experimenta niveles de bajada muy lentos, además, se observo que el causante de que el internet llegue lento o con deficiencia podría ser el solapamiento de canales, ya que existen muchas redes aparte del PorTiUTB que es el SSID oficial de la red universitaria, las cuales utilizan el mismo canal para su transmisión, tanto en las redes de 2.4 y 5 Ghz.

Una recomendación para una posible solución a esto podría ser la configuración adecuada de todos los AP tomando en consideración las buenas prácticas en la ocupación de canales en las frecuencias en las conexiones por radio enlaces, además, de eliminar muchos Routers caseros que aportan a la saturación de canales y causando deficiencia en la calidad del internet.

Lo que se puede decir de la cobertura de la señal wifi es que se analizó en la mayor parte de rincones de los lugares concurridos y con aforo personal y se concluye que dichos lugares

están cubiertos por una señal aceptable para la navegación de internet.

Luego de realizar un análisis objetivo de los componentes que forman la red WIFI de la Universidad técnica de Babahoyo se concluye que la red WIFI podría mejorar en la calidad de navegación solucionando el problema de solapamiento de canal que tienen en casi todo el campus universitario.

Bibliografía

Banco Mundial. (2019). *Banco Mundial*. Obtenido de https://datos.bancomundial.org/indicador/IT.NET.USER.ZS?end=2019&start=2014&view= chart

Fotinet. (2020). *Fortinet*. Obtenido de https://www.fortinet.com/solutions/gartner-network- firewalls

Gartner Peer Insights. (2020). *Gartner Peer Insights*. Obtenido de https://www.gartner.com/reviews/market/network-firewalls

ostec. (2015). *Primeros pasos para realizar un Análisis de Vulnerabilidad en redes corporativas*. Obtenido de https://ostec.blog/es/generico/primeros-pasos-para-realizar-un-analisis-de- vulnerabilidad-en-redes-corporativas/#:~:text=La%20realizaci%C3%B3n%20de%20an%C3%A1lisis%20constantes,s u%20red%20y%20sus%20aplicaciones.

Ruiz, V. G. (25 de diciembre de 2013). *W3*. Obtenido de UAL: https://w3.ual.es/~vruiz/Docencia/Apuntes/Networking/Protocols/Level-3/index.html

Universidad Técnica de Babahoyo. (2021). *Universidad Técnica de Babahoyo*. Obtenido de https://www.utb.edu.ec/

Velasco, R. (17 de marzo de 2019). *Redes Zone*. Obtenido de Redes Zone: https://www.redeszone.net/2019/03/17/rack-armario-que-es/

We Are Social y Hootsuite. (27 de Enero de 2021). *Datareportal*. Obtenido de https://datareportal.com/reports/digital-2021-global-overview-report

welivesecurity. (12 de Noviembre de 2014). *La importancia de identificar, analizar y evaluar vulnerabilidades*. Obtenido de https://www.welivesecurity.com/la-es/2014/11/12/identificar-analizar-evaluar-vulnerabilidades/

wifi scan. (s.f.). *solapamiento de canal* . Obtenido de https://wifiscan.wordpress.com/solapamiento-wifi/#:~:text=Uno%20de%20los%20problemas%20m%C3%A1s,frecuencia%20de%202%2C

4%20GHz.&text=Cada%20canal%20ocupa%20un%20ancho,velocidad)%20de%20las%20re des%20afectadas.

RESUMEN.

En el presente caso de estudio se realiza un análisis de la estructura de red, como se maneja y se analiza el fluido de trafico de internet del servicio WIFI de la Universidad Técnica De Babahoyo, para así detectar posibles fallas y vulnerabilidades que presente la red, se utilizó una herramienta de análisis de redes WIFI desarrollado por el empresa Ubiquiti llamada WiFiman, la cual permitió medir varios aspectos principales los cuales brindaron datos e información importante para estudiarlos y llegar a las conclusiones pertinentes y brindar recomendaciones a las posibles fallas que tengan dicha red.

PALABRAS CLAVE.

Vulnerabilidad

Estructura de Red

Herramienta de analisis

Análisis de red,

Análisis de vulnerabilidades,

Tráfico de la red,

Análisis wifi.

ABSTRACT.

In this case study, an analysis of the network structure is carried out, how the Internet traffic flow of the WIFI service of the Technical University of Babahoyo is handled and analyzed, in order to detect possible failures and vulnerabilities that the network presents, A WIFI network analysis tool developed by the Ubiquiti company called WiFiman was used, which measured several main aspects which provided important data and information to study them and reach the relevant conclusions and provide recommendations to the possible failures that said red may have.

KEYWORDS.

Vulnerability

Network Structure

Analysis tool

Network analysis,

Vulnerability scan,

Network traffic,

Wifi analysis.