UNIVERSIDAD DEL SURESTE: DE LA FRONTERA COMALAPA.

DOCENTE: Ervin Silvestre Castillo.

ASIGNATURA: Seminario de tesis.

ALUMNO: Ramiro Gerardo Resendíz Valdéz.

CUATRIMESTRE: Séptimo (8vo).

CARRERA: Ingeniería en sistemas computacionales.

GRUPO: ISC13SDC0220-A.

UNIDAD: Primera (1ra).

TRABAJO: Capítulo 1 de la tesis.

FECHA DE ENTREGA: 20/Marzo/2023.

CAPÍTULO 1: PLANTEAMIENTO DEL PROBLEMA

"PROTOCOLO EN REDES INFORMÁTICAS"

1.1. DESCRIPCIÓN DEL PROBLEMA

(Navas, 2017) Explica:

Wi-Fi es un conjunto de especificaciones para las redes de área local inalámbricas (WLAN), basadas en el estándar IEEE 802.11. El nombre de Wi-Fi es tenido como una abreviatura del término inglés "Wireless Fidelity", aunque Wi-Fi Alliance, la entidad responsable principalmente por el licenciamiento de productos basados en la tecnología, nunca haya afirmado tal conclusión.

Es común encontrar el nombre Wi-Fi escrito como "wi-fi", "Wi-fi" o incluso "wifi". Todas estas denominaciones se refieren a la misma tecnología. Con la tecnología Wi-Fi, es posible implementar redes que conectan ordenadores y otros dispositivos (smartphones, tablets, consolas de videojuegos, impresoras, etcétera) que están próximos geográficamente. Estas redes no requieren el uso de cables, ya que efectúan la transmisión de datos por medio de radiofrecuencia. Este esquema ofrece varias ventajas, entre ellas: permite al usuario utilizar la red en cualquier punto dentro de los límites de alcance de la transmisión, posibilita la inserción rápida de otros equipos y dispositivos de la red, evita que las paredes o estructuras de la propiedad inmobiliaria sean de plástico o adaptadas para el paso de cables.

La flexibilidad del Wi-Fi es tan grande que se hizo viable la implementación de redes que hacen uso de esta tecnología en los más variados lugares,

principalmente por el hecho de que las ventajas mencionadas en el párrafo anterior muchas veces resultan en disminución de costos. Así, es común encontrar redes Wi-Fi disponibles en hoteles, aeropuertos, carreteras, bares, restaurantes, centros comerciales, escuelas, universidades, oficinas, hospitales, y muchos más sitios. Para utilizar estas redes, solo es necesario que el usuario tenga un ordenador portátil, smartphone o cualquier dispositivo compatible con Wi-Fi. Actualmente cualquier empresa tiene que hacer frente a una mayor demanda de accesos inalámbricos, ya sea por parte clientes, proveedores o empleados.

Desafortunadamente, también los hackers continúan intentando lograr acceder dentro de las redes. Para proteger una red inalámbrica, primero hay que conocer las principales amenazas a las que se ven afectadas y que ponen en riesgo la seguridad del usuario. Cada vez tenemos más dispositivos conectados a Internet de forma inalámbrica. Si pensamos en cómo navegábamos hace unos años, seguro que la mayoría de nosotros utilizaba un ordenador conectado por cable al router. Sin embargo, esto ha cambiado en los últimos tiempos.

Las redes inalámbricas han ganado peso poco a poco. Hoy utilizamos más equipos conectados sin cables a Internet. La cuestión es que esto también puede traer algunos problemas. En esta investigacion vamos a hablar de cuáles son los principales problemas del Wi-Fi y qué hacer para solucionarlos. En la actualidad las redes Wi-Fi tienen un gran peso en la sociedad. Podemos encontrar puntos de acceso por muchas partes y que nos ofrecen la posibilidad de navegar desde nuestros dispositivos móviles casi en cualquier lugar.

El auge de lo que conocemos como el Internet de las casas también ha ayudado a que las conexiones sin cables sigan creciendo. Son muchos los aparatos que tenemos conectados en nuestro hogar. Necesitamos que

nuestros routers Wi-Fi funcionen correctamente. A veces hay problemas con el Wi-Fi, fallos que hacen que no funcione correctamente o que la velocidad de Internet no sea la adecuada. Vamos a detallar cuáles son los principales. También daremos recomendaciones para mejorar la velocidad y que funcione mejor.

Las redes inalámbricas son mucho más sensibles que el cableado, esto significa que vamos a tener más problemas de estabilidad, velocidad e incluso tener que soportar cortes continuos. Esto no siempre ocurre; lógicamente todo dependerá de nuestros dispositivos, la configuración que tengamos o cómo sea la conexión. No obstante, a veces surgen problemas que conviene corregir.

Uno de los problemas más importantes a la hora de conectarnos de forma inalámbrica es tener una mayor latencia. Es algo que puede lastrar el buen funcionamiento para algunos usuarios. Hablamos de por ejemplo a la hora de realizar vídeo llamadas o jugar por Internet. Siempre que lo comparemos con una conexión cableada, en este sentido va a salir perdiendo el Wi-Fi, tomándolo como un punto negativo. Esto puede afectar a la hora de llevar a cabo determinadas acciones, como hemos indicado. Debemos evitar que esto ocurra y lograr que el ping sea lo más bajo posible.

La velocidad de Internet también puede verse mermada si nos conectamos de forma inalámbrica. Es algo que está presente en los usuarios que utilizan este medio para navegar por Internet. Siempre que hagamos un test de velocidad en un mismo equipo conectado por cable o a través de Wi-Fi habrá diferencias. Puede ser mayor o menor en función de determinados factores, como por ejemplo qué dispositivo estemos utilizando, la distancia con el router o si usamos amplificador de señal o no. Hay determinados equipos que pueden ayudar a que la pérdida de velocidad sea lo mínimo posible.

Los problemas de seguridad son sin duda uno de los problemas del Wi-Fi más comunes y es un factor muy importante para los usuarios, pero no siempre está presente cuando navegamos de forma inalámbrica. Nuestro router puede ser atacado por intrusos que busquen la manera de robar la clave de acceso y entrar en nuestra conexión. Lo mismo ocurre cuando nos conectamos a una red inalámbrica ajena.; allí también tendríamos problemas de seguridad. No sabemos realmente quién puede estar detrás de la conexión y si ese Wi-Fi ha podido ser creado con el único objetivo de robar información personal.

Para evitar estos problemas viene bien hacer uso de una VPN que pueda cifrar la conexión. La cobertura no es la que nos gustaría y esto es otra cuestión muy influyente dentro del tema, Especialmente en cuanto nos alejamos un poco del router o nos conectamos desde un lugar donde no está optimizado. Es cierto que existen dispositivos que pueden ayudarnos, como sistemas Mesh, repetidores o PLC, pero no siempre funcionan correctamente o no siempre ayudan realmente a mejorar la cobertura como nos gustaría.

Por último, algo que también ocurre es la pérdida de inestabilidad y cortes. No es lo mismo una conexión cableada que a través del Wi-Fi. La fiabilidad no es la misma y también pueden venir problemas.

(Quero, 2013) Menciona:

Siempre conviene saber qué tipos de vulnerabilidad en una red existen. El mundo (Wireless), como la gente suele llamarlo, ha desencadenado una lucha entre desarrolladores y usuarios acerca de la vulnerabilidad de las redes inalámbricas. Todos queremos WiFi gratis y no está mal usar una red de acceso libre de vez en cuando, pero ten cuidado, porque podrías exponer

tu información bancaria. No todas las redes WiFi gratuitas son creadas con el afán de dañar la privacidad de los usuarios, sin embargo, existen personas malintencionadas y con el conocimiento suficiente para aprovechar una de las vulnerabilidades de este tipo de conexiones y los riesgos y amenazas en las redes inalámbricas públicas. La razón por la que los datos pueden ser vulnerados en una red de acceso libre es que este tipo de conexiones no cifran la información, y, por esta causa, si se tiene una conexión WiFi en casa, se debe emplear seguridad WPA o WPA2.

Este tipo de seguridad no solamente protege a la red de intrusos, sino que también cifra todos los datos enviados a través de ésta, como cuentas bancarias, contraseñas, nombres, números telefónicos, etc. Según Think Big, estas redes predominan en restaurantes, aeropuertos o sitios públicos como parques o bibliotecas, existen brechas de seguridad que deben ser tomadas en cuenta. Otro problema muy importante es que hay muchos routers desactualizados. Cualquier dispositivo puede sufrir vulnerabilidades, pero esos fallos suelen ser corregidos por los propios fabricantes a través de parches y actualizaciones. Pero claro, si no instalamos esas nuevas versiones no podremos corregirlos. Ahí está el problema, ya que estamos rodeados de routers que pueden llevar incluso años sin actualizar. Por otra parte, un punto también esencial es el tipo de cifrado que estemos utilizando. Hoy en día los más fuertes y fiables son WPA-2 y WPA-3. Sin embargo, muchos usuarios, especialmente aquellos que tienen routers más antiguos, siguen utilizando algunos cifrados obsoletos e inseguros, como podría ser el WEP. Es muy importante evitar esto, ya que podría habilitar la entrada de intrusos.

1.2 FORMULACIÓN DEL PROBLEMA

1. ¿Qué son los cifrados de redes wifi?

2. ¿Cuáles son los riesgos de conectarse a una red pública?

3. ¿Conocen los estudiantes de la Universidad del Sureste los riesgos de no tener una red wifi segura?

4. ¿Identifican los estudiantes de la Universidad del sureste las páginas de dudosa procedencia?

5. ¿Saben los estudiantes de la Universidad del Sureste los riesgos de no cambiar la configuración predeterminada del modem?

6. ¿Por qué las redes públicas son un punto de acceso de robo de información más fácil de manipular?

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Crear estrategias educativas para mejorar la seguridad las redes informáticas en los hogares de los estudiantes de la Universidad del Sureste.

1.3.2. OBJETIVOS ESPECÍFICOS

- Proporcionar información de manera simple y entendible sobre los riesgos de conectarse a una red wifi.
- Aportar el conocimiento básico a los estudiantes de la Universidad del Sureste sobre cómo cambiar la configuración de su modem.
- Informar a los estudiantes de la Universidad del Sureste el riesgo que conlleva conectarse a una red pública y lo vulnerable que somos al robo de información.
- Explicar a los estudiantes de la Universidad del Sureste las diferencias de una red de hogar (privada) a una red pública.
- Listar los detalles de una página segura de navegar para que las personas no tengan ningún riesgo de navegar en ellas.
- Enseñar a los estudiantes de la Universidad del Sureste a identificar paginas de dudosa procedencia.

1.4. HIPÓTESIS

Entre más información tengan los estudiantes de la Universidad del Sureste sobre las medidas de seguridad en las redes informáticas, menos riesgo de hackeo tendrán.

1.5 JUSTIFICACIÓN

(Jurado, 2023) Menciona:

Una red inalámbrica es insegura de manera predeterminada. Esto significa que está abierta a todos y cualquier persona dentro del área de cobertura del punto de acceso puede potencialmente escuchar las comunicaciones que se envían en la red. En el caso de un individuo, la amenaza no es grande ya que los datos raramente son confidenciales, a menos que se trate de datos personales. Sin embargo, si se trata de una compañía, esto puede plantear un problema serio.

Este tipo de ataques, conocidos como Man in the Middle u Hombre en el medio ocurren cuando un hacker se aprovecha de la falta de mecanismos de seguridad en una red Wi-Fí pública para establecer su equipo como intermediario entre los datos que comparte tu ordenador o smartphone con la red WiFi a la que estás conectado. Así, podrá acceder a tus contraseñas o datos bancarios si entras a sitios para hacer compras en línea o ver tu estado de cuenta. También podrá interceptar tus contraseñas, algo especialmente peligroso si te conectas desde un ordenador de trabajo a cualquier red WiFi Pública. Como también está la variable de intrusión de datos, la instalación de un punto de acceso en una red local permite que cualquier estación acceda a la red conectada y también a Internet, si la red local está conectada a ella.

Es por esto que una red inalámbrica insegura les ofrece a los hackers la puerta de acceso perfecta a la red interna de una compañía u organización. En las redes públicas, este tipo de ataques puede aparecer en forma de redes sin contraseña que tienen un nombre similar al establecimiento en el que te encuentras. A simple vista, parecen un buen punto para conectarte desde donde estás; sin embargo, estarás compartiendo tus datos

directamente con una persona malintencionada. Además de permitirle al hacker robar o destruir información de la red y de darle acceso a Internet gratuito, la red inalámbrica también puede inducirlo a llevar a cabo ataques cibernéticos.

Como no existe manera de identificar al hacker en una red, puede que se responsabilice del ataque a la compañía que instaló la red inalámbrica. También existe la problemática llamada interferencia radial y denegación del servicio que son básicamente las ondas radiales son muy sensibles a la interferencia. Por ello una señal se puede interferir fácilmente con una transmisión de radio que tenga una frecuencia cercana a la utilizada por la red inalámbrica. Hasta un simple horno de microondas puede hacer que una red inalámbrica se vuelva completamente inoperable si se está usando dentro del rango del punto de acceso.

El método de acceso a la red del estándar 802.11 se basa en el protocolo CSMA/CA, que consiste en esperar hasta que la red este libre antes de transmitir las tramas de datos. Una vez que se establece la conexión, una estación se debe vincular a un punto de acceso para poder enviarle paquetes. Debido a que los métodos para acceder a la red y asociarse a ella son conocidos, un hacker puede fácilmente enviar paquetes a una estación solicitándole que se desvincule de una red.

El envío de información para afectar una red inalámbrica se conoce como ataque de denegación de servicio. Asimismo, conectarse a redes inalámbricas consume energía. Incluso cuando los dispositivos inalámbricos periféricos tengan características de ahorro de energía, un hacker puede llegar a enviar suficientes datos cifrados a un equipo como para sobrecargarlo.

Muchos periféricos portátiles, como los PDA y ordenadores portátiles, tienen una duración limitada de batería. Por lo tanto, un hacker puede llegar a provocar un consumo de energía excesivo que deje al dispositivo inutilizable durante un tiempo. Esto se denomina ataque de agotamiento de batería.

Actualmente cualquier empresa tiene que hacer frente a una mayor demanda de accesos inalámbricos, ya sea por parte clientes, proveedores o empleados. Desafortunadamente, también los hackers continúan intentando lograr acceder dentro de las redes. Para proteger una red inalámbrica, primero hay que conocer las principales amenazas a las que se ven afectadas y que ponen en riesgo la seguridad del usuario. Las reúne WatchGuard con motivo del lanzamiento de un nuevo punto de acceso inalámbrico para empresas.

Los usuarios que son víctimas de un Rogue AP son susceptibles de verse afectados por código malicioso, que a menudo pasa desapercibidos. La colocación de malware consiste en que los usuarios que se unen a una red inalámbrica de invitados son susceptibles de, sin saberlo, llevarse malware no deseado de algún vecino con malas intenciones. Una táctica común utilizada por los hackers es colocar una puerta trasera en la red, lo que les permite regresar más tarde para robar datos confidenciales. Los ataques móviles, tales como Stagefright de Android, se propagan de un usuario a otro, incluso sin que la "víctima cero" lo sepa.

En la actualidad hay muchas formas de ser víctima de un ataque cibernético con el simple hecho de conectarse a cualquier tipo de red inalámbrica estas expuesto a cualquier tipo de amenazas y virus, por eso hemos decididos estudiar este tema para comprender aún más como es el uso de las redes inalámbricas todos los tipos de vulnerabilidades y cómo es que estos se roban la información de los usuarios para así poder brindar la ayuda e

información a las personas que menos tiene conocimientos en redes informáticas para qué así ellos puedan estar o tener un poco más de seguridad la conectarse a una red inalámbrica y navegar usando dicha red.

1.6 DELIMITACIÓN DEL ESTUDIO

(Jurado, 2023) Explica:

En el mundo actual, dominado por la tecnología y las redes informáticas, es fundamental saber qué es seguridad informática y poder utilizarla eficazmente. Los sistemas, archivos importantes, datos y otras cosas virtuales importantes están en riesgo si no hay seguridad para protegerlos. Tanto si se trata de una empresa de TI (Acrónimo de Tecnologías de la Información) como si no lo es, todas ellas deben estar protegidas por igual. Con la mejora de la nueva tecnología en seguridad informática, los atacantes tampoco se quedan atrás. Están utilizando cada vez mejores técnicas de hacking y se dirigen a los puntos débiles de muchas empresas.

La seguridad informática, es un proceso de protección de datos sensibles, redes y aplicaciones de software contra un posible ataque cibernético. Los ataques cibernéticos pueden ser considerados como una explotación de recursos, acceso no autorizado a los sistemas, ataques de rescate para encriptar datos y extraer dinero.

El uso de redes inalámbricas no está exento de riesgos de ataques cibernéticos o hackeos, especialmente cuando nos conectamos a redes WiFi públicas. En el ámbito empresarial esto puede tener consecuencias graves, como el robo de información, mientras que en las redes personales puede darse la duplicación de identidad y el fraude.

La seguridad de redes consiste en las políticas y prácticas adoptadas para prevenir y supervisar el acceso no autorizado, el uso indebido, la modificación o la denegación de una red informática y sus recursos accesibles. La seguridad de redes involucra la autorización del acceso a datos en la red, que es controlada por el administrador de red.

La macro localización: es en la cuidad de Frontera Comalapa que está ubicada en los puntos fronterizos de Chiapas y Guatemala perteneciente a unas de las localidades de la ciudad de Comitán de Domínguez, una ciudad muy transitada por el paso de fronteras.

Frontera, es un adjetivo refiriéndose al límite que hace con la República de Guatemala y el término Comalapa proviene de la voz náhuatl: Comalapan En el agua de los comales, que deriva de las voces: Comalli, comal; Atl, agua; y -Pan, adverbio de lugar. Pero también se considera que su nombre se debe al recuerdo de la extinta San Juan Comalapa, y está sobre el paraje Cushú, que se encontraba cerca de Tecpan, Guatemala; es decir en la frontera.

La localidad de Frontera Comalapa está situada en el Municipio de Frontera Comalapa (en el Estado de Chiapas). Hay 21,727 habitantes. Es el pueblo más poblado en la posición número 1 de todo el municipio. Frontera Comalapa está a 645 metros de altitud.

La Micro localización: será en el instituto universitario de “Universidad del Sureste, campus Frontera Comalapa” que está ubicado en barrio la lima en la carretera internacional en libramiento de la ciudad de Comalapa aquí será donde obtendremos la mayor parte de nuestra investigación.