UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN SISTEMAS

TEMA:

Análisis de vulnerabilidad de las redes inalámbricas del departamento de operaciones y mantenimiento en la empresa CNT Babahoyo.

EGRESADO:

Byron Alejandro Mantuano Zúñiga

TUTORA:

ING. Ana Fernández Torres

AÑO:

2019

INDICE

INTRODUCCIÓN

Actualmente las tecnologías han logrado alcanzar un reconocimiento muy significativo en la sociedad, permitiendo dinamizar y facilitar los procesos que anteriormente se efectuaban de forma manual, por lo que es indispensable evaluar y analizar la funcionalidad de los dispositivos de conectividad con los que se cuenta para el desarrollo de las actividades diarias.

Las redes de conexión inalámbrica son empleadas en muchos entornos, pudiendo ser estos laborales, corporativos o familiar, las mismas que pueden ofrecer un servicio no tan bueno brindando una experiencia desfavorable para quienes manejan información digital y necesitan de una conexión óptima, considerando como factor principal de este inconveniente las vulnerabilidades que pueden presentar estas redes de conexión.

Las redes inalámbricas brindan un sinnúmero de ventajas, permitiendo disminuir recursos para su implementación, independientemente de esto las conexiones Wireless presentan problemas de vulnerabilidad, lo cual provoca que el rendimiento de la conectividad de estas redes disminuya, imposibilitando el trabajo que en las mismas se llevan a cabo.

Es por ello que en el presente trabajo de análisis se pretende encontrar si existe alguna vulnerabilidad de las redes inalámbricas del departamento de operaciones y mantenimiento en la empresa CNT Babahoyo, donde se llevan a cabo trabajos importantes referentes a la distribución de servicios de internet, siendo necesario para esta institución contar con un servicio de red inalámbrico seguro.

La Corporación Nacional de Telecomunicaciones (CNT) es una institución pública encargada de proveer de servicios de internet, televisión, telefónicos y brindar el mantenimiento correspondiente para asegurar el correcto funcionamiento. Dentro de

esta se encuentran el departamento de operaciones y mantenimiento el cual se encarga de la transmisión de los datos referentes al mantenimiento de redes de comunicación.

En el desarrollo del presente caso de estudio se analizan los datos recopilados en la empresa CNT para lo cual se emplea el método analítico-deductivo el mismo que permitirá brindar un análisis correspondiente sobre la vulnerabilidad de las redes inalámbricas, pudiendo así emplear herramientas de recolección de información y análisis como el sistema operativo Kali Linux con el cual se harán las pruebas necesarias para determinar el margen de vulnerabilidad que tiene la red Wireless del departamento, además de la aplicación de una encuesta que permita determinar la importancia y pertinencia de solución de la problemática detectada.

Para el desarrollo del presente estudio de caso se considera la línea de investigación Desarrollo de Sistemas de la información, comunicación y emprendimientos empresariales y tecnológicos cuya sublinea corresponde a procesos de transmisión de datos y telecomunicaciones, empleando una metodología enfocada en la recopilación de información mediante encuestas y pruebas de inseguridad en algunos equipos que utiliza el departamento de operaciones y mantenimiento.

DESARROLLO

En la actualidad el uso del internet ha tenido una gran acogida en múltiples contextos, debido a que este ha permitido llevar a cabo actividades de una forma mucho más rápida, dinamizando y ahorrando tiempo, lo cual en la sociedad actual es indispensable para ejecutar otras tareas que permitan mejorar la economía. Las empresas requieren de este servicio como un factor indispensable para sus actividades por lo que mantener sus redes en óptimas condiciones es indispensable.

> Usar Internet se ha convertido ya en parte de la vida cotidiana de casi todo el mundo. La influencia de Internet en la sociedad es cada día más evidente, la red ha cambiado las rutinas de la gente, las formas de comunicación y también las de relacionarse con los demás. (E. Darling, 2015)

El contexto en el cual se lleva a cabo el presente estudio de caso es en la Corporación Nacional de Telecomunicación (CNT) Babahoyo, en el departamento de operaciones y mantenimiento considerando la red inalámbrica para efectuar el proceso de testing el cual permita determinar las vulnerabilidades de la red Wireless de esta área, para de esta forma poder brindar las sugerencias correspondientes a una posible solución que ayude a mejorar la seguridad de la información.

Escenario de investigación

El escenario planteado son las instalaciones del departamento de operaciones y mantenimiento de la Corporación Nacional de Telecomunicaciones “CNT” Babahoyo; lugar donde es distribuida la red inalámbrica (Wireless), ver anexo 1.

En el interior del edificio central de la Corporación Nacional de Telecomunicaciones “CNT” se encuentran varios departamentos que llevan a cabo distintas actividades, enfocando el análisis en la red inalámbrica del departamento de

operaciones y mantenimiento, la cual presenta una estructura basada en hormigón, ver anexo 2.

Independientemente de esto se puede evidenciar que alrededor de la Corporación Nacional de Telecomunicaciones "CNT" existen varias viviendas y edificaciones comerciales que poseen redes inalámbricas, las cuales afectan el tráfico de señales Wireless, ver anexo 3.

Los dispositivos que son empleados para la emisión de señales Wireless corresponden a Routers FiberHome de 12 voltios, los mismos que son instalados en las viviendas de los usuarios, ver anexo 4.

Red inalámbrica

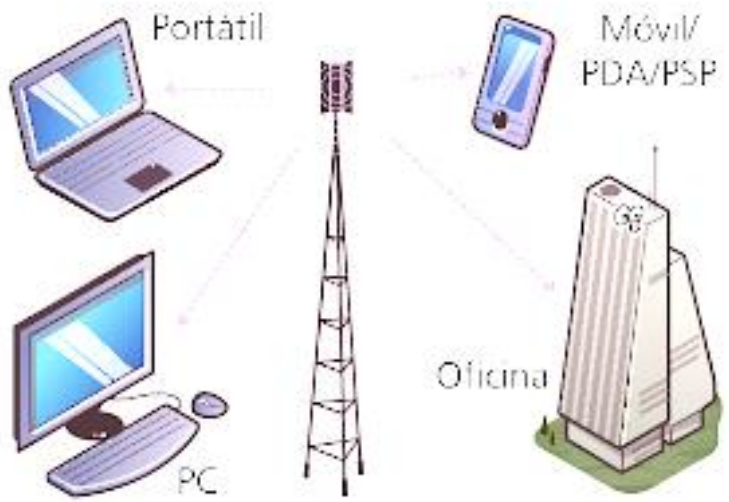
Una red inalámbrica es un tipo de conexión de internet que permite la comunicación con otros dispositivos en un área determinada, para lo cual es necesario contar con dispositivos que permitan la recepción de señales Wireless con las cuales pueda interconectarse y disfrutar de los servicios de internet, para ello es indispensable contar con un proveedor de internet de velocidad adecuada.

> Las redes inalámbricas Wireless (Wireless Network) son redes sin cable que se suelen comunicar por medios no guiados a través de ondas electromagnéticas. La transmisión y la recepción se efectúan a través de antenas. (Andreu Joaquín, 2016, pág. 212)

Las redes inalámbricas facilitan la conexión de dispositivos sin la necesidad de emplear cables, es por ello que se denominan medios no guiados, los mismos que permiten que varios dispositivos electrónicos se puedan comunicar a través del internet.

Para que este tipo de conexiones pueda darse sin complicaciones es necesario el uso de una antena que se encargue de la emisión de la señal y otra antena importante para la recepción de las mismas.

Imagen Nº 1: Conexión Wireless



Fuente: Servicio de red – Joaquín Andreu

Características de las redes inalámbricas

Las redes inalámbricas poseen varias características asociadas a las ventajas y desventajas que estas poseen:

Ventajas

- Rápida conexión
- Pueden ser transportadas
- Ahorro en costos de mantenimiento
- Accesibilidad
- Permiten el desarrollo de trabajos colaborativos

Desventajas

- Problemas de conexión por cambios climáticos (lluvias, viento, etc.)
- Vulnerabilidad de la red
- Velocidad limitada
- Errores de interferencia

> La libertad que ofrecen las redes inalámbricas hace que sean las que más proliferan. Además, los nuevos dispositivos móviles que llevan incorporadas estas tecnologías están vendiéndose exponencialmente. (Andreu Joaquín, 2016, pág. 212)

Son muchos los dispositivos que hoy en día cuentan con la conexión inalámbrica, desde los celulares hasta Smart TV los cuales requieren de una red de internet Wireless para poder brindar todo su potencial a los usuarios, siendo para ello necesario e indispensable contar con el acceso a una red con una velocidad óptima que permita disfrutar de los servicios complementarios de la misma.

Normas de red inalámbrica

Como son común todos los servicios deben estar estructurados y regidos bajo parámetros o normas que regulan su funcionamiento, para ello el internet inalámbrico posee ciertas características que permiten su estandarización.

> Los diferentes tipos de redes inalámbricas se rigen bajo normas y estándares, las cuales fueron establecidas por el instituto de ingenieros eléctricos y electrónicos, más conocido como la IEEE. La norma más utilizada es la IEEE 802.X. (Estrada Elmer, 2017)

Tabla Nº 1: Estándares Wireless 802.11

Estándares Wireless			
Estándar Velocidad	802.11b Hasta 11Mbps	802.11a Hasta 54 Mbps	802.11g Hasta 54 Mbps
Costo	Barato	Relativamente caro	Relativamente barato
Banda de Frecuencia	2.4-2.497GHz	5.15-5.35GHz 5.425-5.675GHz 5.725-5.875GHz	2.4-2.497GHz
Cobertura	Buena cobertura, 100m en interior y 300 a 400m en exterior, con buena conectividad con determinados obstáculos.	Cobertura baja, 50m. En interior y 150 m en interior y 150 m en exterior con mala conectividad con obstáculos	Buena cobertura, 100m en interior y 300 a 400m en exterior, con buena conectividad con determinados obstáculos.
Acceso Publico	El numero de HotSpots crece exponencialmente	Ninguno en este momento	Compatible con los HotSpots actuales de 802.11b. El paso a 802.11g no es traumático para los usuarios
Compatibilidad	Compatible con 802.11g y no compatible con 802.11a	Incompatible con 802.11b y g	Compatible con la 8002.11b, no es compatible con la 802.11a
Modos de Datos	1,2,5.5,11Mbps	6,9,12,18,24,36,48, 54 Mbps	1,2,5.5,11Mbps 6,9,12,18,34,36,48 Mbps
Modulación	CCK(DSSS)	OFDM	OFDM Y CCK (DSSS)

Fuente: https://sites.google.com/site/redesinalambricas3/tipos-de-redes-inalambricas/comparacionesentrenormas

Seguridad de las redes

La seguridad de las redes es un tema de mucho análisis, debido a que con el objetivo de salvaguardar los datos ha sido necesario emplear alternativas que permitan proteger la información, por otro lado ha sido muy evidente el trabajo de vulnerar los métodos de seguridad, ocasionando la fuga de datos y un déficit en la velocidad del internet, lo cual provoca lentitud en el desarrollo de los trabajos.

> La seguridad de la red es la práctica de prevenir y proteger contra la intrusión no autorizada en redes corporativas. 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. (Fruhlinger Josh, 2018)

Para las empresas u organizaciones es de suma importancia contar con una velocidad de internet adecuada, el cual permita que sus actividades sean llevadas a cabo de una forma rápida y sin pérdida de tiempo, es por ello que es indispensable mantener una seguridad adecuada para evitar vulnerabilidades y así no tener intrusos que hagan que la velocidad del internet disminuya y se torne lenta.

> El servicio de seguridad de una red inalámbrica es indispensable debido que este garantiza la protección adecuada de los sistemas o de las transferencias de datos proporcionando un sistema que brinde políticas que son indispensables para un trabajo organizacional. (Stallings William, 2016, pág. 9)

En una red inalámbrica es indispensable contar con los servicios de seguridad los mismos que ayuden a impedir que se den vulnerabilidades en la red, para ello se consideran las siguientes:

Autentificación

Es un servicio que se encarga de garantizar la veracidad del proceso de comunicación con la red de comunicación. Existen dos tipos de autentificación, el primero es de entidades, el cual consta de credenciales de ingresos con los cuales se puede determinar la pertinencia en la conexión o de la información ingresada; el segundo es la autentificación del origen de los datos, el mismo que corrobora la fuente de una unidad de datos tales como correo electrónico.

Control de acceso

Permite limitar y controlar el acceso a sistemas es decir, con este se puede establecer el número de usuarios que pueden interactuar desde una misma red, adaptando los derechos de acceso de manera individual, siempre y cuando exista un espacio disponible para su posterior conexión. Con esto se puede mejorar el flujo de datos que rigen la velocidad del internet.

Ataques a las redes inalámbricas

Las redes inalámbricas han tenido grandes amenazas que vulneran su seguridad, entre estos ataques se pueden mencionar los ataques pasivos y los ataques activos los mismos que tienen como objetivo principal interceptar, atacar y descubrir una red, lo mismo que conlleva a poseer una red inalámbrica lenta y poco segura.

Tanto el ataque pasivo como el activo buscan obtener información que permita vulnerar la seguridad de una red, además de esto pueden modificar el flujo de datos o alterar su comportamiento colapsando los servicios de red. Al vulnerar una red inalámbrica se da paso a un sinnúmero de problemas en una conexión, siendo para esto necesario una restructuración de los servicios.

Herramientas empleadas

Herramientas de recolección de información

Para la obtención de información que permita determinar la pertinencia del trabajo efectuado se aplica una encuesta con preguntas mixtas (abiertas y cerradas), considerando a 10 involucrados que laboran en esta empresa, para ello se lleva a cabo la tabulación de los datos recopilados, ver anexo 5

Análisis e interpretación de resultados

Tras la aplicación de las encuesta se obtuvieron los siguientes resultados, ver anexo 6.

- De acuerdo a las preguntas efectuadas el 70% de los encuestados mencionan que si existe vulnerabilidad en la red Wireless, mientras que el 30% consideran que no hay vulnerabilidad en la misma. Concluyendo en que la gran mayoría considera que si existe índice de vulnerabilidad en esta red inalámbrica.

- Referente a la velocidad del internet y su importancia para el desarrollo de la actividad laboral, el 100% de los encuestados mencionan que si es necesario contar con una rápida velocidad del internet para llevar a cabo las actividades laborales del departamento de operaciones y mantenimiento de CNT, debido a que este departamento se encarga de la solución de inconvenientes de conectividad de los usuarios en general.

- Acerca de la frecuencia con el que cambian la contraseña en los Router's el 50% de los encuestados mencionan que las cambian con poca frecuencia, el 30% mencionan que lo hacen frecuentemente y el 20% aseguran que lo hacen muy frecuentemente, llegando a la conclusión en que la mayoría concuerda en que no se realiza el cambio de la contraseña constantemente.

- Sobre la frecuencia con la que cambian o actualizan los dispositivos de conexión inalámbrica el 80% mencionan que es poco frecuente el cambio o actualización de estos dispositivos, mientras que el 20% mencionan en que lo hacen frecuentemente. Concluyendo en que la mayoría hace referencia en que estos dispositivos no son cambiados muy a menudo.

- La gran parte de los funcionarios del departamento de operaciones y mantenimiento de CNT Babahoyo coinciden en que la vulnerabilidad en este departamento si perjudica a los servicios ofrecidos por CNT, ya que al ser un departamento de mantenimiento son los encargados de solucionar los problemas o inconvenientes de conectividad, dependiendo de ellos la satisfacción de los clientes.

Herramientas de análisis de redes Inalámbricas

Para brindar un análisis adecuado y conocer el índice de vulnerabilidad en la red inalámbrica del departamento de operaciones y mantenimiento en la empresa CNT Babahoyo se hace uso de las siguientes herramientas MITM, para así posteriormente llegar a las conclusiones correspondientes a los datos obtenidos mediante el presente estudio de caso.

Entre las herramientas empleadas para analizar este trabajo se obtuvieron los siguientes resultados:

Kali Linux

Kali Linux es una herramienta que permite analizar y testear las redes inalámbricas, permitiendo de esta manera comprobar su estado de vulnerabilidad para de esta forma poder corregir aquellos problemas de conectividad que impiden un trabajo adecuado bajo la conexión Wireless.

> Kali es una distribución de Linux basada en Debian, diseñada para la auditoria de seguridad, los tests de intrusión y la informática forense. Es una mejora sobre la muy conocida y ya obsoleta Back Track. Mientras Back Track no se actualiza desde el 2012, Kali está muy activa. (Santo Orcero David, 2018, pág. 15)

Esta herramienta cuenta con más de 600 aplicaciones que permiten la auditoria de seguridad, contribuyendo además a la informática forense con los cuales se ha podido resolver muchos casos de violaciones informáticas. Además posibilita un análisis profundo sobre la conectividad, todo esto mediante el uso USB o desde un CD, convirtiéndose en una herramienta excepcional.

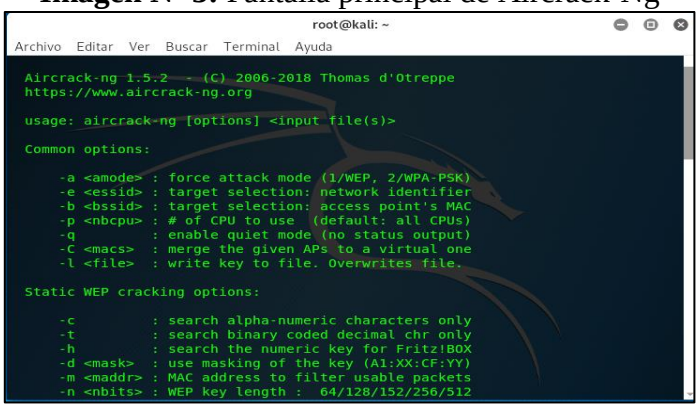
Imagen Nº 2: Pantalla principal de Kali Linux

Elaborado por : Byron Mantuano

Aircrack-Ng

Es una suite de herramientas que viene integrado en Kali Linux el cual permite analizar las redes inalámbricas, además permite la recuperación de contraseñas y puede ser empleado como herramienta de auditoria de redes. Está diseñada para trabajar con tarjetas inalámbricas generalmente Atheros y Ralink.

Imagen Nº 3: Pantalla principal de Aircrack-Ng



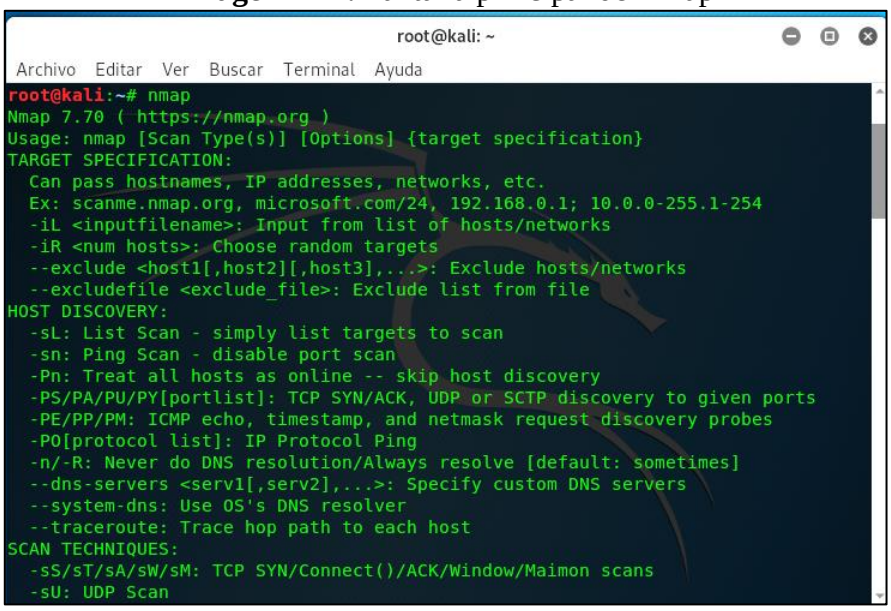
Elaborado por : Byron Mantuano

Con la aplicación de la herramienta Aircrack-Ng se pudo obtener la clave del departamento de operaciones y mantenimiento, comprobando que esta presenta un índice de vulnerabilidad alto, ya que la contraseña que se emplea es muy simple y fácil de descifrar con unos cuantos comandos, ver anexo 7.

Nmap

Es una herramienta multiplataforma el cual se encarga de rastrear puertos inalámbricos determinando su vulnerabilidad, empleado generalmente para evaluar el nivel de seguridad de los sistemas informáticos incluidas las redes de internet, enviando paquetes definidos a otros dispositivos analizando las respuestas brindadas por aquellos, obteniendo de esta manera las credenciales de ingreso de una red inalámbrica.

Imagen Nº 4: Pantalla principal de Nmap



Elaborado por: Byron Mantuano

Al ejecutar esta aplicación se pudo comprobar que existen varios puertos de red Wireless habilitados, lo cual ocasiona que la red inalámbrica sea inestable y presente problemas de conexión, ver anexo 8.

Fluxion

Es una herramienta de terceros la cual trabaja con el sistema operativo Kali Linux el cual engaña a los usuarios para que estos introduzcan su contraseña, para ello duplica el nombre de la red en los dispositivos y de esta forma provoca que de manera inconsciente los usuarios ingresen su contraseña y así poder obtenerla. Para poder utilizarla es indispensable obtenerla desde repositorios GitHub.

Imagen Nº 5: Pantalla principal de Fluxion

Elaborado por: Byron Mantuano

Con esta herramienta se pudo esclarecer ciertas dudas acerca de los problemas de vulnerabilidad de las redes Wireless del departamento de operaciones y mantenimiento, ya que con fluxión se realizó una prueba que permita comprobar el nivel de facilidad para la obtención de la clave, lo cual fue muy acertado, ver anexo 9.

CONCLUSIÓN

Con la realización del presente estudio de caso y la aplicación de las herramientas de análisis de vulnerabilidades de las redes se llega a las siguientes conclusiones:

- El departamento de operaciones y mantenimiento de CNT Babahoyo presenta vulnerabilidades en la red inalámbrica, ya que esta tiene una velocidad de navegación lenta, la misma que impide el desarrollo óptimo de las actividades laborales realizadas en dicha dependencia.

- Con el test realizado con la herramienta de análisis Nmap se pudo encontrar varios puertos que se encuentran activados, lo cual no es recomendable ya que al encontrarse activos el nivel de vulnerabilidad es mayor y cualquier persona con afinidad a la informática podría hacker las redes inalámbricas.

- Empleando la herramienta Aircrack-Ng la cual hace uso del método diccionario se pudo hackear la contraseña de la red inalámbrica del departamento de mantenimiento y operaciones de CNT Babahoyo, concluyendo en que este tipo de entidades deben colocar claves con un nivel de complejidad mayor para de esta forma evitar vulnerabilidades.

BIBLIOGRAFÍA

Andreu Joaquín. (2016). *Servicios de Red.* España: Editex.

E. Darling. (2015). *Influencia de Internet en la sociedad*. Obtenido de https://www.edarling.es/consejos/vida-de-soltero-y-busqueda-de-pareja/influencia-de-internet-en-la-sociedad

Estrada Elmer. (2017). *Normas de redes inalámbricas*. Obtenido de https://cableadoestrycturado.weebly.com/normas-para-redes-inalaacutembricas-ieee-80211a-802b-802g.html

Fruhlinger Josh. (04 de 07 de 2018). *¿Qué es la seguridad de la red?* Obtenido de https://www.networkworld.es/seguridad/que-es-la-seguridad-de-la-red

Jimenez Castro Rodrigo. (2018). *Vulnerabilidades en redes WiFi.* España: LATEX.

Medina Javier. (2014). *Evaluacion de Vulnerabilidades TIC.* Murcia: C/Angel.

Santo Orcero David. (2018). *Kali Linux.* Madrid: RA-MA.

Stallings William. (2016). *Fundamentos de seguridad en redes aplicaciones y estandares.* Madrid: Person Practice Hall.

Vanhoef Mathy. (2017). *Key Reinstallation Attacks.* Bélgica: imec-DistriNet.

ANEXOS

Anexo 1: Edificio CNT.

Foto Nº1: Edificio Principal CNT

Anexo 2: Departamento de operaciones y mantenimiento CNT.

Foto Nº2: Departamento de operaciones y mantenimiento CNT

Anexo 3: Área externa de CNT

Foto Nº3: Área externa de CNT

Anexo 4: Router y servidor

Foto Nº4: Servidor y router

Anexo 5: Encuestas aplicadas

UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

ENCUESTA

1. ¿Cree usted que la red inalámbrica del departamento de operaciones y mantenimiento de CNT Babahoyo presenta alguna vulnerabilidad?

Si	
no	

2. ¿Considera necesario contar con una rápida velocidad del internet para llevar a cabo las actividades laborales del departamento de operaciones y mantenimiento de CNT?

Si	
no	

3. ¿Con que frecuencia cambian las contraseñas del /los Router's en el departamento de operaciones y mantenimiento de CNT?

Muy frecuentemente	
Frecuentemente	
Poco frecuente	

4. ¿Con que frecuencia actualizan o cambian los dispositivos de conexión inalámbrica en los departamentos de CNT?

Muy frecuentemente	
Frecuentemente	
Poco frecuente	

5. ¿Cree usted que la vulnerabilidad de la red inalámbrica en el departamento de operaciones y mantenimiento perjudica a los servicios que ofrece la empresa CNT? ¿Por qué?

_____

_____

_____

Anexo 6: Tabulaciones

TABULACIÓN DE DATOS

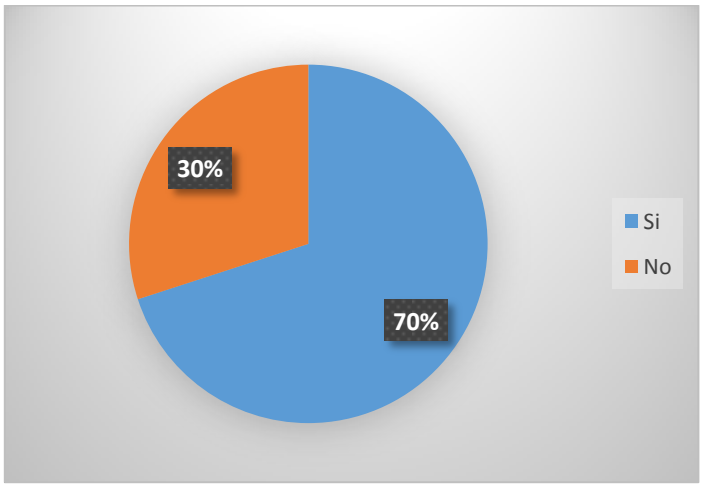
1. ¿Cree usted que la red inalámbrica del departamento de operaciones y mantenimiento de CNT Babahoyo presenta alguna vulnerabilidad?

Tabla Nº 2: Vulnerabilidad en la red inalámbrica

Ítems	Frecuencia	Porcentaje
Si	7	70%
No	3	30%
Total	**10**	**100%**

Elaborado por: Byron Mantuano

Gráfico Nº 1: Vulnerabilidad en la red inalámbrica



Elaborado por: Byron Mantuano

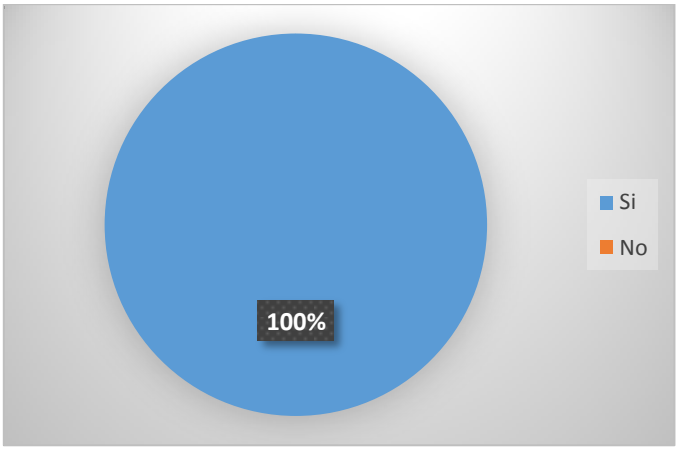
2. ¿Considera necesario contar con una rápida velocidad del internet para llevar a cabo las actividades laborales del departamento de operaciones y mantenimiento de CNT?

Tabla Nº 3: Velocidad del internet

Ítems	Frecuencia	Porcentaje
Si	10	100%
No	0	0%
Total	**10**	**100%**

Elaborado por: Byron Mantuano

Gráfico Nº 2: Velocidad del internet



Elaborado por: Byron Mantuano

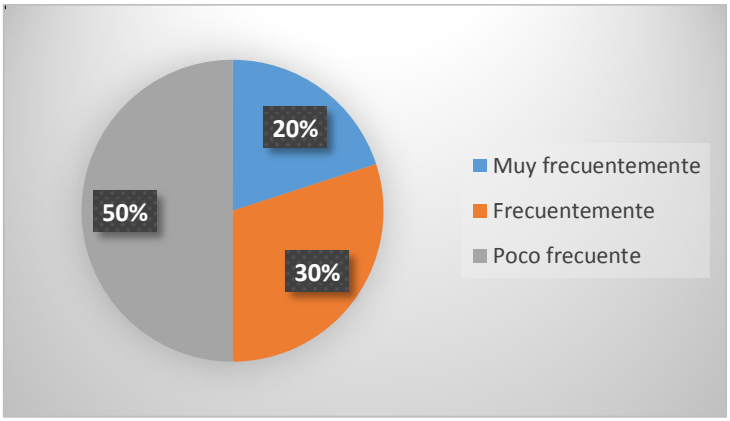
3. ¿Con que frecuencia cambian las contraseñas del /los Router's en el departamento de operaciones y mantenimiento de CNT?

Tabla Nº 4: Cambio de contraseña

Ítems	Frecuencia	Porcentaje
Muy frecuentemente	2	20%
Frecuentemente	3	30%
Poco frecuente	5	50%
Total	**10**	**100%**

Elaborado por: Byron Mantuano

Gráfico Nº 3: Cambio de contraseña



Elaborado por: Byron Mantuano

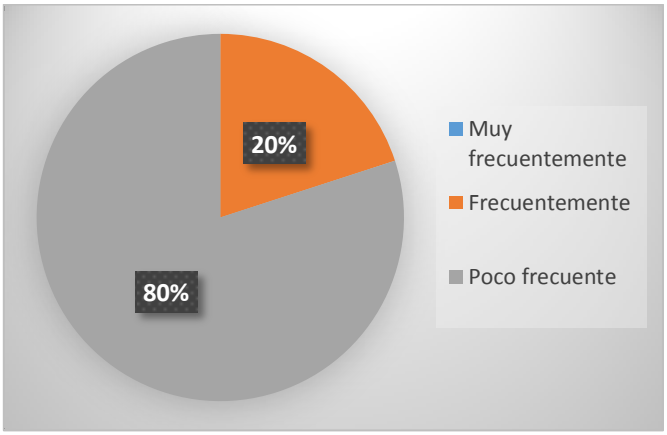
4. ¿Con que frecuencia actualizan o cambian los dispositivos de conexión inalámbrica en los departamentos de CNT?

Tabla Nº 5: Cambio de dispositivos de conexión inalámbrica

Ítems	Frecuencia	Porcentaje
Muy frecuentemente	0	0%
Frecuentemente	2	20%
Poco frecuente	8	80%
Total	**10**	**100%**

Elaborado por: Byron Mantuano

Gráfico Nº 4: Cambio de dispositivos de conexión inalámbrica



Elaborado por: Byron Mantuano

Ejecución de las herramientas de análisis

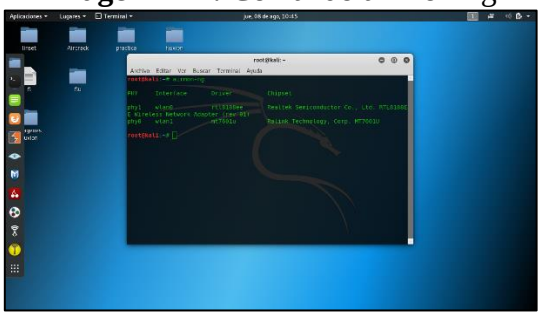
A continuación se realiza la aplicación de las herramientas de análisis con su respectiva interpretación, llevadas a cabo en el departamento de operaciones y mantenimiento de CNT Babahoyo:

Anexo 7: Aircrack -Ng

AIRCRACK-NG

Se procede a abrir una terminal y se digita el comando airmon-ng, el cual permite visualizar todas las tarjetas inalámbricas conectadas en el computador.

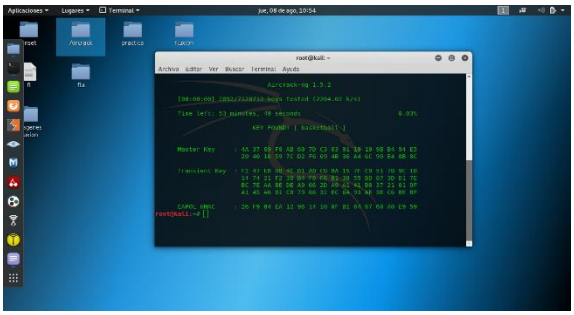
Imagen Nº 7: Comando airmon-ng



Elaborado por: Byron Mantuano

Tras la ejecución del comando anterior se debe esperar un tiempo determinado según el nivel de complejidad de la clave registrada, pudiendo así vulnerar la red inalámbrica obteniendo su clave.

Imagen Nº 8: Obtención de la clave y vulneración de la red



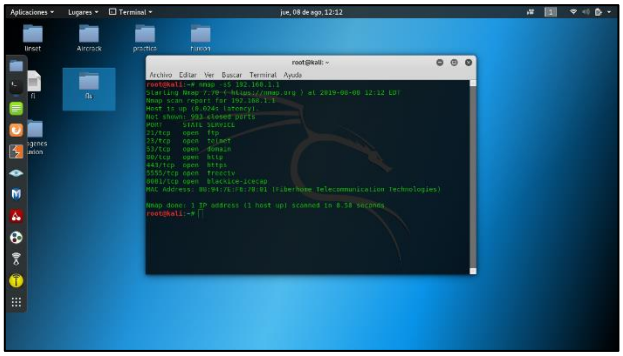
Elaborado por: Byron Mantuano

Anexo 8: Nmap

NMAP

Con el comando nmap – sS y la dirección ip del Router procedemos a escanear todos los puertos y servicios y determinaremos cuáles de ellos está abierto y cual están cerrados.

Imagen Nº 9: Nmap



Elaborado por: Byron Mantuano

Anexo 9: Fluxion

FLUXION

Iniciamos la herramienta de análisis Fluxion con el siguiente comando ./fluxión.sh

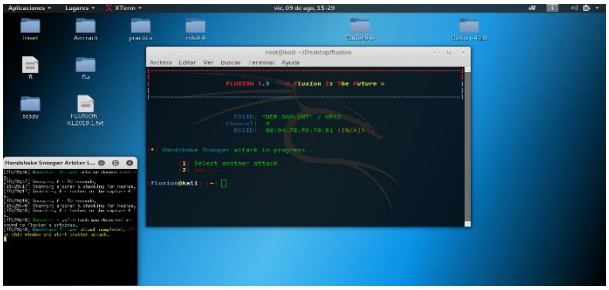
Imagen Nº 10: Inicio de Fluxion

Elaborado por: Byron Mantuano

Seleccionamos la opción 2 la cual corresponde a un cifrado WPA – WPA2

Al haber culminado los 30 segundo el handshake fue capturado por la herramienta.

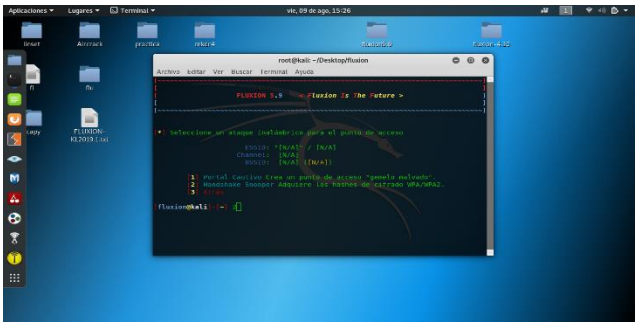
Imagen Nº 11: Captura del handshake



Elaborado por: Byron Mantuano

En esta ventana seleccionamos la opción 1 para crear un portal cautivo malvado

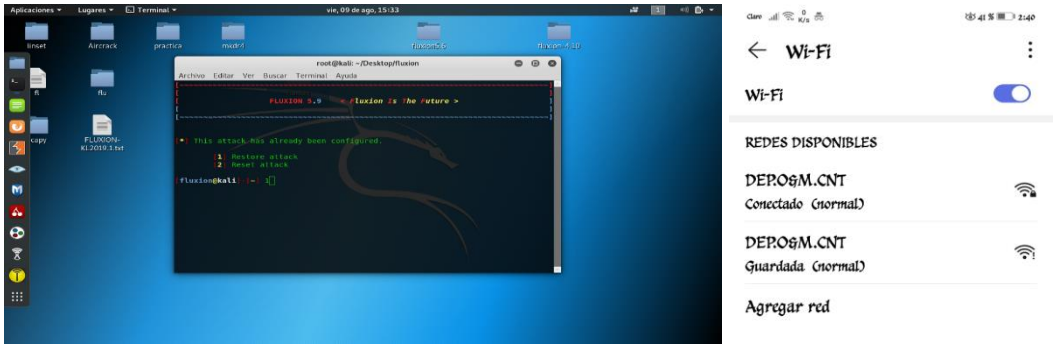
Imagen Nº 12: Portal cautivo



Elaborado por: Byron Mantuano

Seleccionamos la opción 1 para que se genere una red falsa y de esta forma el usuario se pueda conectar

Imagen Nº 13: Red falsa



Elaborado por: Byron Mantuano

Al realizar la conexión se direcciona a una web falsa en la cual se solicita la contraseña como medida de seguridad, lo cual permite obtener la contraseña.

Imagen Nº 14: Contraseña solicitada por la red falsa

Elaborado por: Byron Mantuano

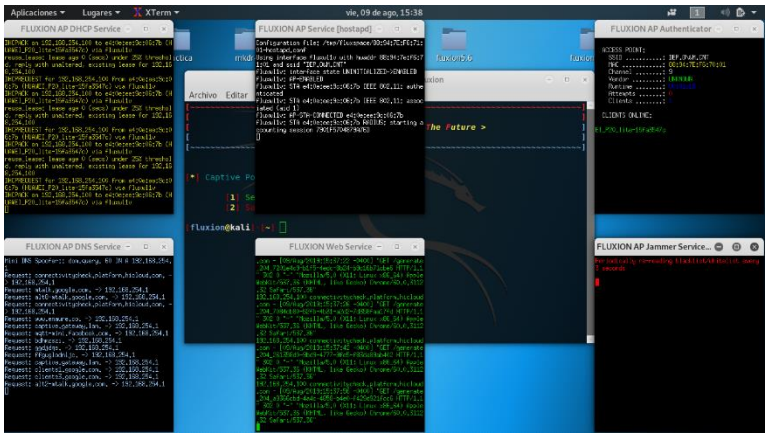
Una vez ingresada la contraseña se mostrará el siguiente mensaje.

Imagen Nº 15: Mensaje de confirmación

Elaborado por: Byron Mantuano

Mientras la victima ingresa la contraseña en la web falsa en la herramienta se muestran los siguientes procesos.

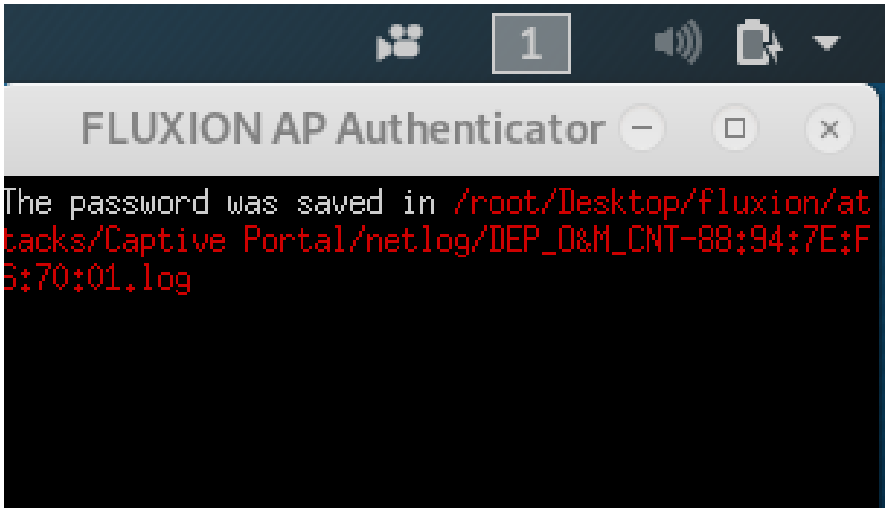
Imagen Nº 16: Procesos en la herramienta



Elaborado por: Byron Mantuano

En esta ventana se muestra la dirección donde se capturo la contraseña de la víctima.

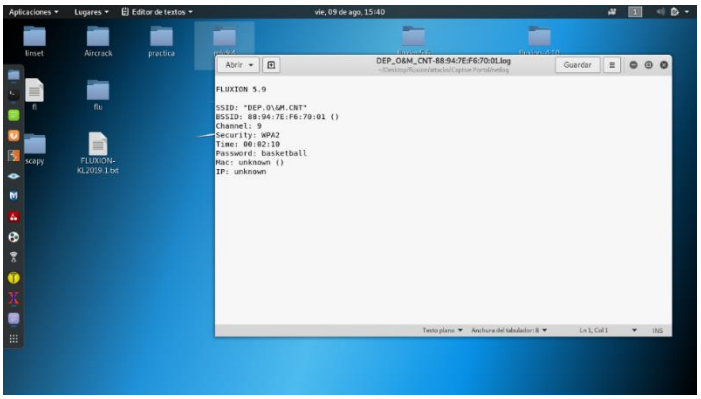
Imagen Nº 17: Dirección de la contraseña capturada



Elaborado por: Byron Mantuano

Al haber buscado la dirección abrimos el archivo.log la cual contiene los siguientes datos, incluida la contraseña.

Imagen Nº 18: Archivo.log que posee la contraseña



Elaborado por: Byron Mantuano

Anexo 10: Realización de encuesta al responsable del departamento de operaciones y mantenimiento CNT Babahoyo Tecnólogo Milton Rodríguez.

Foto Nº5: Realización de encuesta