PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
SEDE ESMERALDAS

ESCUELA

INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

INFORME DE ESTUDIO DE CASO

Tema:

Las Redes WiFi en Sitios de Mayor Concurrencia de Usuarios en la Ciudad de Esmeraldas

Previo a la obtención del título de Ingeniero de Sistemas y Computación

Autor:

Luis Alberto Herrera Izquierdo

Asesor:

Ing. Juan Casierra

Esmeraldas – Ecuador
Noviembre 2015

HOJA DE APROBACIÓN

Disertación aprobada luego de haber dado cumplimiento a los requisitos exigidos por el reglamento de Grados de la Pontificia Universidad Católica del Ecuador sede Esmeraldas previa obtención del Titulo de Ingeniero de Sistema y Computación.

……...…….

DIRECTOR DE DISERTACIÓN

……

LECTOR 1

..…….

LECTOR 2

……

DIRECTOR DE ESCUELA

FECHA: ……..……..

AUTORÍA

Yo, **Luis Alberto Herrera Izquierdo,** portador de la cédula de ciudadanía Nº **080378668-0**, decreto que la presente investigación es de total responsabilidad del autor y que se ha respetado las diferentes fuentes de información realizando las citas correspondientes.

_____

Herrera Izquierdo Luis Alberto

AUTOR

Índice

1. Resumen

Con la creciente tendencia del uso de dispositivos inteligentes ha aumentado también el uso de las redes sociales o acceso a diferentes aplicaciones como lo es la banca en línea, correo electrónico o aplicaciones e-commerce en las que se puede hacer compras en línea. Para acceder a estas aplicaciones se requiere del servicio de internet el cual se encuentra disponible en los café-net, centros comerciales, parques, entre otros. Luego de conectarse a esta red, se debe ingresar un usuario y contraseña cuya información puede estar expuesta a capturas de tráfico en puntos intermedios de conexión.

Muchas personas desconocen de los peligros a los que se exponen cuando se conectan a las redes de internet públicas vía WiFi que están disponibles ya sean en los parques, centros comerciales, hoteles e incluso universidades. Una persona con conocimientos técnicos en seguridad podría aprovechar las vulnerabilidades que posean los dispositivos y obtener información personal o privada de todas las personas que se conectan a estas redes e incluso cambiar información que se está enviando a otra persona.

Con este estudio de caso se pretende dar a conocer a las personas cuáles son las vulnerabilidades y los peligros que conlleva conectarse a este tipo de redes y que medidas pueden tomar para evitar que accedan o roben su información privada.

Abstract

With the increasing trend of using smart devices it has also increased the use of social networks or access to different applications as it is online banking, email and e-commerce applications in which they can shop online. For access to these applications require

internet service which is available in the coffee-net, shopping centers, parks, among others. After connecting to the network, you must enter a username and password which information may be exposed to capture traffic at intermediate points of connection.

Many people are unaware of the dangers they are exposed when connected to the network via WiFi public Internet that are available either in parks, shopping malls, hotels and even universities. A person with expertise in security could exploit vulnerabilities that have the devices and obtain personal or private information of all people who connect to these networks and even change information that is being sent to someone else.

This case study is intended to inform people what the vulnerabilities and dangers connected to these networks and that measures be taken to prevent access or steal your private information.

2. Justificación.

En la ciudad de Esmeraldas existen diferentes empresas que proveen el servicio de internet vía WiFi a sus clientes (Centro comercial, parque, hotel, café net, entre otros), en los cuales de estar disponibles sin contraseña o en caso de tenerlas algunos puntos proveen una contraseña genérica y los usuarios se conectarán con la finalidad de tener acceso a internet, por lo tanto estas redes están disponibles ya sea para usuarios comunes que solo acceden a internet o usuarios que tiene un conocimiento técnico de redes, considerando adicionalmente que en el internet existe mucha información para aprovechar las vulnerabilidad de las conexiones, con la cual podrían incurrir en delitos informáticos, por esta razón es recomendable que los usuarios conozcan que están expuestos a que otras personas accedan a la información de sus dispositivos violentando la integridad de sus datos.

A pesar de que la mayoría de los dispositivos que proveen internet vía WiFi están protegidos por contraseña esto no es impedimento para que personas con conocimiento técnico amplio sobre estos tipos de redes intenten vulnerarlas, puesto que no solo se trata de proteger al dispositivo con una contraseña también se debe elegir el tipo de encriptación. Cualquier persona que esté conectada a la red puede tomar la información concurrente en la red de otros usuarios que entra y sale del dispositivo para usarla a su conveniencia lo cual nos facilita el medio compartido en este caso.

En el País desde que entró en vigencia el Código Orgánico Integral Penal (COIP) se ha registrado alrededor de 626 denuncias por delito informático (El Comercio, 2015) y según el director de Kaspersky Lab se anticipa que esta tendencia seguirá y aumentará en 2015 (La Hora, 2015) por lo tanto se pretende que al informar a la ciudadanía de cómo podrían evitar estar involucrados en este tipo de situaciones se pueda disminuir el número de afectados.

La presente investigación permitirá orientar a los usuarios o involucrados en este tema a tener conocimientos de las situaciones a las que se enfrentan al momento de conectarse a

una red vía WiFi, además de las precauciones que deben implementar en sus dispositivos al conectarse a este tipo de red.

Tener conocimientos en seguridad y redes es de vital importancia para el desarrollo de la investigación, ya que van a permitir evidenciar mediante la elección de información publicada, el peligro al cual se enfrentan los terminales que se conecten a la red y además analizar el tráfico que hay por parte de los usuarios conectados, esto se hace con la finalidad de que las demás personas conozcan las vulnerabilidades de estas redes y que tomen las debidas precauciones.

3. Objetivos.

Determinar el nivel de vulnerabilidad en las redes WiFi detectadas en áreas de mayor concurrencia de usuarios de la ciudad de Esmeraldas mediante la aplicación de herramientas de pen-test a los dispositivos de los usuarios

- Diagnosticar la existencia de vulnerabilidad en los sitios que proveen el servicio de internet vía WiFi.

- Aplicar herramientas de pen-test que permitan detectar la vulnerabilidad de las redes WiFi en los sitios donde hayan mayor concurrencia de usuarios.

- Determinar el nivel de conocimiento de los usuarios acerca de las redes WiFi y proveer información necesaria para que eviten ser afectados por las vulnerabilidades detectadas.

4. Caso

4.1. Marco Teórico.

El WiFi es un tipo de comunicación inalámbrica (Ondas de radio) cuyas siglas en ingles significan Wireless-Fidelity (Fidelidad Inalámbrica). Este tipo de red está basado en el estándar 802.11 de la IEEE, el estándar 802.11 fue creado con la finalidad de satisfacer las necesidades de conexión que las redes cableadas no lograban (Moreno Carlos, 2014).

En vista de que el WiFi es un tipo de conexión que se realiza de manera inalámbrica los dispositivos son susceptibles de interceptar la comunicación y por lo tanto tener acceso al flujo de información. Por este motivo es imprescindible cifrar la comunicación. El cifrado que muchos módems traen por defecto suele ser el WEP (Wired Equivalent Privacy) sin embargo WEP es muy inseguro, por tal motivo se mejoró el modo de cifrar la comunicación y se lo llamo WPA (Wi-Fi Protected Access) este es considerado como el estándar recomendado (García Prieto, 2014) . En Junio de 2004 se publicó el nuevo estándar WPA2 este se considera más seguro que el WPA ya que utiliza el algoritmo AES (Advanced Encryption Standard) (USERS, 2012)

En el Ecuador existe un creciente uso de dispositivos inteligentes o Smartphone como se puede apreciar en la figura 1. También se ha incrementado el uso del medio de comunicación inalámbrico WiFi para acceder a internet el mismo que en la mayoría de los casos es usado desde el hogar del usuario, según estadísticas (INEC, 2013) el segundo lugar donde las personas a nivel nacional hacen uso de internet son en los centros de acceso público los cuales pueden ser: parques, centros comerciales, etc. (Ver Figura 2). Como consecuencia esto expone a los usuarios a que su información pueda ser interceptada o robada.

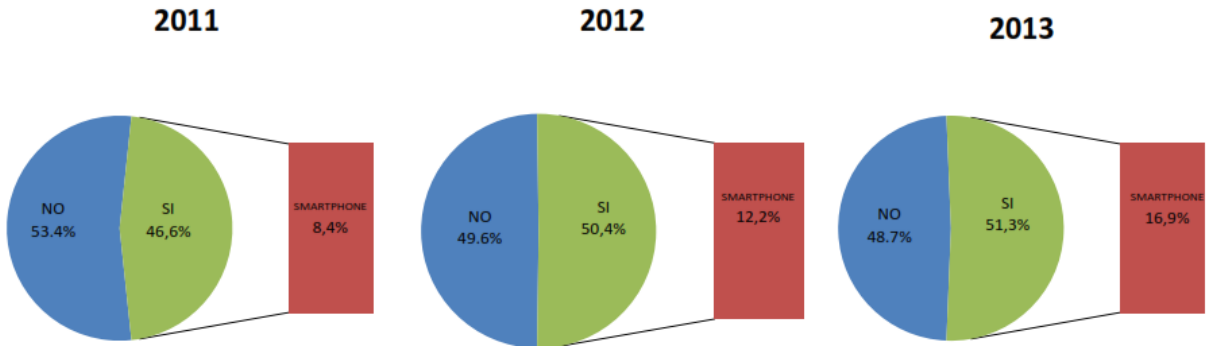

Figura. 1 Porcentaje de personas que tienen teléfonos inteligentes en el País. Fuente: (INEC, 2013)

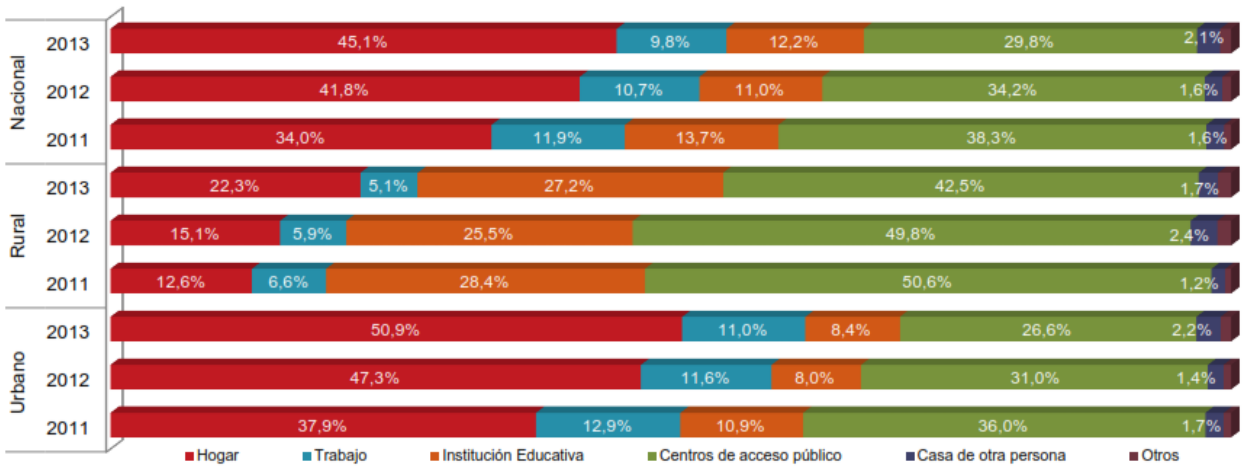

Figura. 2 Lugar de uso de internet por Áreas. Fuente: (INEC, 2013)

Según (Offensive Security , 2011) y (UGR Cyber Security Group, 2015) los riesgos más comunes que se pueden dar en una red son:

a) Escucha de protocolos o Sniffing
b) Ataque de denegación de servicios (DOS)
c) Ataque hombre en el medio o Man In The Middle (MITM)
d) Ataque de envenenamiento ARP
e) Spoofing o suplantación de identidad

f) Secuestro de sesiones o Hijacking

Además hay otro tipo de ataque que podría ser generados en base a los riesgos antes indicados el cual es: ataques de control remoto

La técnica de Sniffing es usada para monitorear y analizar tráfico de la red, después de la captura, estos datos pueden ser analizados y la información sensible puede ser recuperada. Capturar el tráfico es particularmente útil en la recopilación de información, ya que dependiendo de los sitios web visitados por los usuarios víctimas, se puede ver las URL visitadas, nombres de usuario, contraseñas y otros detalles que se pueden utilizar contra ellos. Tal ataque a la red comienza con una herramienta como Wireshark (ver figura 3). (Conocimiento, 2015)

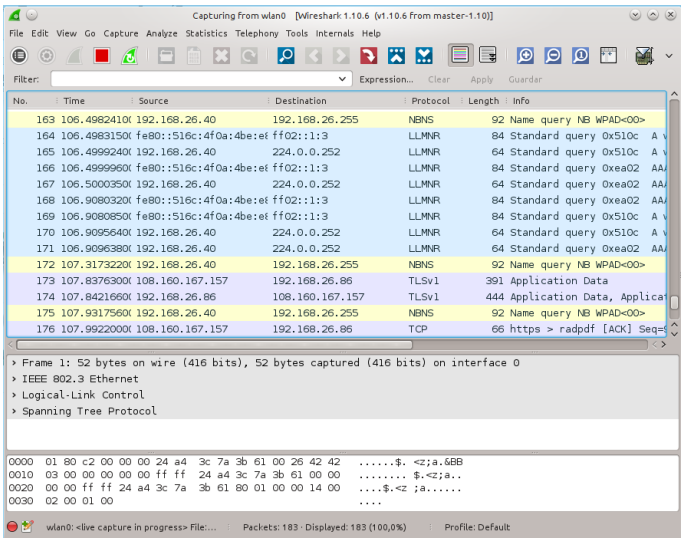

Figura. 3 Ejemplo de uso de Wireshark. Fuente: Elaboración propia

En un ataque de denegación de servicio que se ejecuta sobre una red inalámbrica el principal objetivo es saturar los recursos del usuario víctima durante algún tiempo, para hacer esto hay hacerse pasar por el AP (Punto de Acceso o Access Point) poniendo al dispositivo que se va a usar la dirección MAC del AP (esta se obtiene mediante el uso de

un sniffer) y negarle la comunicación al terminal o terminales escogidos (USERS, 2012). En un ataque Man in the middle o "hombre en el medio" (ver figura 4) se hace creer al usuario victima que el atacante es el AP y al mismo tiempo se convence al AP de que el atacante es el cliente para ello se debe obtener: SSID de la red, dirección MAC del AP, dirección MAC del usuario víctima. El atacante en este caso, tiene la habilidad de desviar o controlar las comunicaciones entre dos partes. Por ejemplo, si se tratase de un ataque MITM a tu correo, el perpetrador podría desviar todos los e-mails a una dirección alterna para leer o alterar toda la información antes de enviarla al destinatario correcto (Gabriela, 2014).

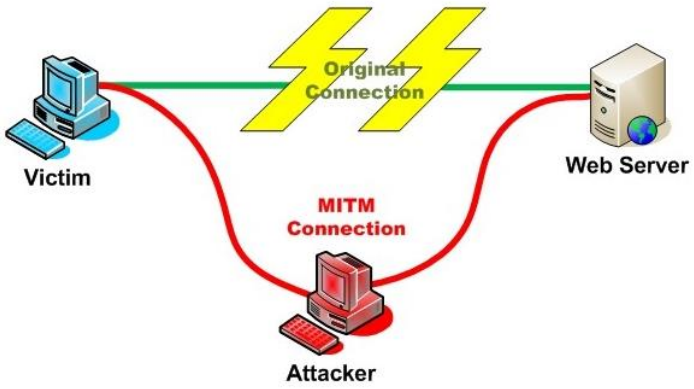

Figura. 4 Ataque MITM. Fuente: (Soto, 2014)

En un ataque ARP Poisoning (ver figura 5) el objetivo principal es interponerse entre una o varias máquinas con el fin de interceptar, modificar o capturar paquetes, el atacante falsifica los paquetes ARP, este tipo de ataque es similar al MITM.

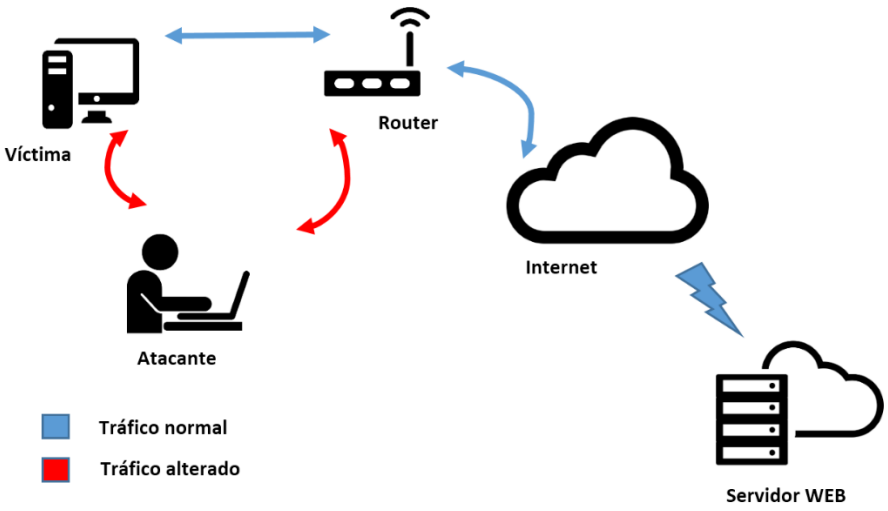

Figura. 5 Ataque envenenamiento ARP. Fuente: Elaboración propia

La técnica de Spoofing o suplantación de identidad como se puede apreciar en la figura 6 consiste en realizar un camuflaje online donde se suplanta la identidad de un dispositivo en una red cuyo objetivo principal es obtener información restringida o falsificar datos. (Silva Larry, 2011)

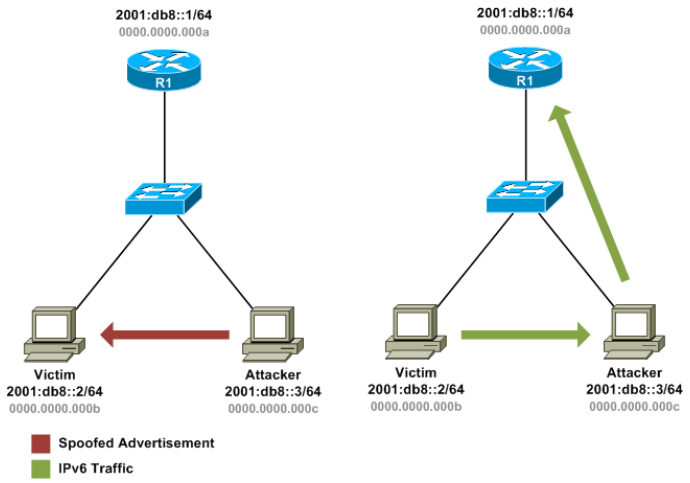

Figura. 6 Técnica de spoofing o suplantación de identidad. Fuente: (Stretch, 2009)

La técnica de hijacking o secuestro de sesiones como se muestra en la figura 7 consiste en interceptar o robar una sesión que ha sido iniciada por el usuario victima desde otro ordenador que se encuentra conectado a la misma red del atacante, el principal objetivo de esta técnica es secuestrar una conexión ya establecida de manera legal por otro usuario que está dentro de la misma red. (Silva Larry, 2011)

Figura. 7 Técnica de hijacking o secuestro de sesiones. Fuente: (Aema, 2012)

Un usuario atacante luego de obtener información crítica del usuario victima estará en la capacidad de lanzar un ataque para tener control remoto del dispositivo (Ver figura 8), En concreto, se proporciona una interfaz gráfica de usuario para la conexión de un ordenador a otro ordenador. Un escenario típico en el que se utiliza el protocolo de escritorio remoto es cuando un administrador de red intenta ayudar a otro usuario de la computadora para la instalación del programa, a la vez que el usuario de la computadora está asistida se registra actualmente en el equipo. En su estado predeterminado, la función de RDP (Remote Desktop Protocol) está abierto a los ataques que los cibercriminales pueden utilizar para ejecutar código de forma remota en los sistemas con RDP habilitado.

Figura. 8 Ataque de control remoto. Fuente: (Kunkle, 2013)

Las redes WiFi que se utilizan en la ciudad de Esmeraldas trabajan comúnmente en la banda 2.4 GHz., toda red que trabaje sobre esta banda dispone de un total de 14 canales (Ver figura 9) se puede apreciar un rango de frecuencias entre 2,412GHz – 2,484GHz; en el Ecuador y varios países de Latinoamérica se utilizan los canales del 1 al 11 como puede observarse en la Tabla 1.

Relación entre canal y frecuencia	
Canal	**Frecuencia**
1	2.412 GHz
2	2.417 GHz
3	2.422 GHz
4	2.427 GHz
5	2.432 GHz
6	2.437 GHz
7	2.442 GHz
8	2.447 GHz
9	2.452 GHz
10	2.462 GHz
11	2.462 GHz
12	2.467 GHz
13	2.472 GHz
14	2.484 GHz

Tabla 1 Relación entre canal y frecuencia.

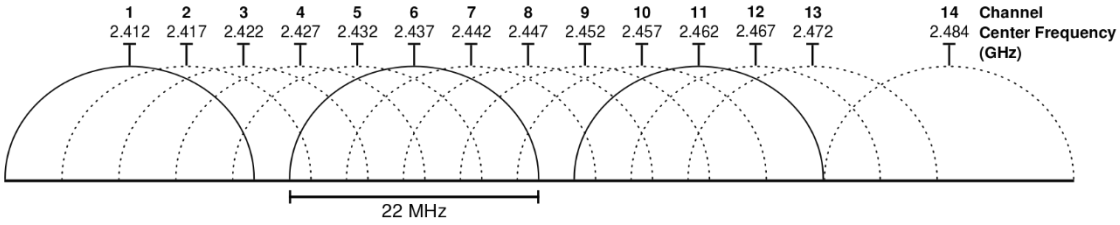

Figura. 9 Canales con ancho de banda 22 MHz. Fuente: (WNDW, 2007)

Los canales de transmisión en la frecuencia 2.4 GHz, tienen un uso de 22 Mhz en lo referente a la propagación de su ancho de banda, considerando este valor los canales deben tener una separación para que no se cree interferencia entre los mismos, por lo tanto los canales 1, 6, 11 tienen usa separación que le permite transmitir en su canal con su respectiva separación de 5Mhz entre ellos. El análisis del presente caso se utilizara como referencia las conexiones en frecuencia 2.4 GHz puesto que como se explicó anteriormente es la más usada por los usuario de equipos móviles en la provincia, la información que puede variar en las redes son los canales sin embargo esto no afectara en el proceso de análisis.

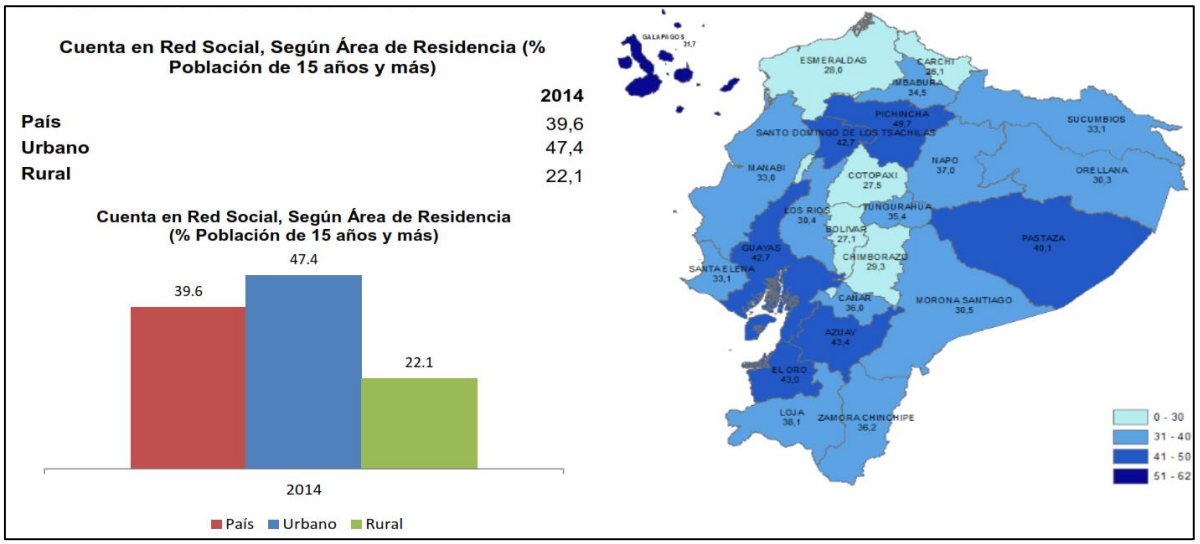

Figura. 10. Uso de redes sociales en Ecuador por edad. Fuente: (INEC, 2015)

Estos datos demuestras que los jóvenes y adultos constantemente hacen uso de internet ya sea para acceder a su red social o hacer otra actividad personal mediante internet, es recomendable que estas personas conozcan todos los riesgos que conlleva el hacer uso de un punto de acceso que es usado por muchos usuarios al mismo tiempo, esto no solo implica los puntos de acceso libre si no también los puntos de acceso privados o en los que se deben autenticar para tener acceso a la red como es el caso de puntos de ventas en centros comerciales o universidades.

En la provincia de Esmeraldas el Municipio ha puesto a disposición de la ciudadanía el servicio de internet gratuito en sitios de mayor concurrencia como lo son: El Parque Central, Parque Infantil y Parque de Las Palmas. La investigación se va a realizar en puntos donde se ha notado gran concurrencia de personas por lo que se ha seleccionado cuatro puntos estratégicos para el análisis de las redes WiFi los cuales son:

1. Parque Roberto Luis Cervantes (Infantil)
2. Parque 20 de Marzo (Central)
3. Parque Luis Tello (Las Palmas)
4. PUCESE (Universidad)

El análisis que se va a realizar consiste en:

1. Conectarse a las redes libres o privadas a nivel de usuario, de esta manera se aplicaran técnicas de pen-test a un equipo de propiedad del investigador el cual servirá como referencia ya que si se aplica a los equipos de los usuarios concurrentes sería un delito de invasión de privacidad inclusive teniendo la autorización del administrador de la infraestructura de red.

2. Realizar encuestas a los administradores de las redes y a los usuarios.

Luego del análisis se procederá a utilizar las herramientas de pen-test para detectar posibles vulnerabilidades en las redes WIFI.

Según CNT en el Artículo 30 literal i de los reglamentos para clientes de la resolución CANATEL 29 se indica lo siguiente:

> "El Cliente será el único responsable por el uso del servicio de telecomunicaciones y/o televisión que se origine en su equipo terminal y/o línea telefónica, de cualquier tipo sean nacionales o internacionales; o, conexiones de internet y datos, ya sean automáticas, semiautomáticas o manuales, realizadas a teléfonos fijos, celulares o a cualquier tipo de equipo terminal." (CNT, 2011).

Esto quiere decir que si un usuario autorizado o no, realiza un delito informático desde uno de los sectores que propaga el servicio de internet vía WiFi y el cliente que contrato el plan no encuentra la manera de localizarlo o identificarlo el será responsable por ser de su tráfico interno dicho evento, considerando este antecedente es importante conocer el nivel de vulnerabilidad de las redes WIFI.

Para el uso de las herramientas de pen-test se solicitó la autorización previa de los administradores de redes en los lugares de estudios (ver Anexo 1 y 2) para respetar lo establecido en el artículo 190 del COIP (Código Orgánico Integral Penal) sobre: Apropiación fraudulenta por medios electrónicos (COIP, 2015).

4.2. Metodología.

El tipo de investigación aplicada fue de tipo descriptiva, puesto que se analizó si las redes WiFi de acceso público que se encontraban ubicadas en las áreas más concurrentes de la ciudad de Esmeraldas tenían vulnerabilidades y también se analizó el nivel de conocimiento por parte de los usuarios sobre estos peligros.

Para determinar el nivel de vulnerabilidad de las redes se utilizó la metodología: OWISAM, acrónimo de Open Wireless Security Assessment Methodology (Metodología de evaluación de seguridad Wireless abierta). Esta metodología indica cuáles son los controles de seguridad que se deben verificar sobre redes de comunicaciones inalámbricas

para minimizar el impacto de los ataques informáticos y a garantizar la protección de las infraestructuras Wireless (OWISAM, 2013)

La metodología OWISAM surgiere que de los 10 controles se utilicen las que se puedan adaptar al caso de estudio, por esta razón luego de un análisis previo de los lugares de estudio se utilizaron los siguientes controles:

1. Descubrimiento de dispositivos
2. Fingerprinting
3. Cifrado de las comunicaciones
4. Configuración de la plataforma
5. Pruebas de denegación de servicio
6. Pruebas sobre los clientes inalámbricos

Los controles no utilizados fueron los siguientes:

1. Pruebas sobre la autenticación
2. Pruebas de infraestructura
3. Pruebas sobre directivas y normativas
4. Pruebas sobre hostspots y portales cautivos

Las pruebas sobre autenticación no se aplicaron puesto que el único lugar que utiliza autenticación para acceder al servicio WiFi es la PUCESE, sin embargo las otras ubicaciones analizadas en este caso proveen el servicio WiFi sin autenticar el acceso. Las pruebas de infraestructura no se aplicaron ya que los administradores de las redes manifestaron que la red WiFi se maneja de manera independiente, es decir, hay un servidor o dominio de broadcast exclusivo para dicho servicio.

La estrategia de acceso antes indicada, no compromete a los servicios y aplicaciones que se manejan internamente en las instituciones. Tampoco se aplicaron los controles sobre directivas y normativas ni pruebas sobre hostpots y portales cautivos puesto que ninguno de los lugares de estudio ejecutan esto.

Para realizar el análisis de las redes WiFi se utilizó una laptop con el sistema operativo BackBox (Ver Figura 11) el cual es una distribución GNU/Linux especializada en pruebas de penetración y evaluaciones de seguridad, dotada de un amplio grupo de programas que facilitan el análisis de redes y sistemas.

Figura. 11 Sistema Operativo BackBox. Fuente: (BackBox, 2015)

La herramienta utilizada para el desarrollo de la investigación son basadas en software libre, entre ellas se indican las siguientes: LinSSID (Ver Figura 13) la cual permite realizar un escaneo de redes WiFi con interfaz gráfica funcional, ésta permite conocer de manera detallada la configuración del WiFi, también se utilizó ZenMap con la cual se escaneó la seguridad de los dispositivos en la red.

La captura de todo el tráfico de la red se realizó mediante la utilización de Wireshark (Ver Figura 14) con esta herramienta se puede obtener las credenciales de los dispositivos conectados en la red. Con esta herramienta se pudo conocer cuáles eran las páginas más visitadas en ese momento, cabe destacar que no se accedió a la información privada de los usuarios cumpliendo con el artículo correspondiente al COIP, a pesar que la herramienta si permitía hacer este tipo de acciones pero la intención de la investigación

fue de tipo netamente académica y permitió determinar el nivel de vulnerabilidad en la red.

Otra de las herramientas utilizadas fue NetworkMiner (Ver Figura 15) la cual permitió estructurar la información capturar desde Wireshark de una manera mucho más fácil y sencilla de comprender.

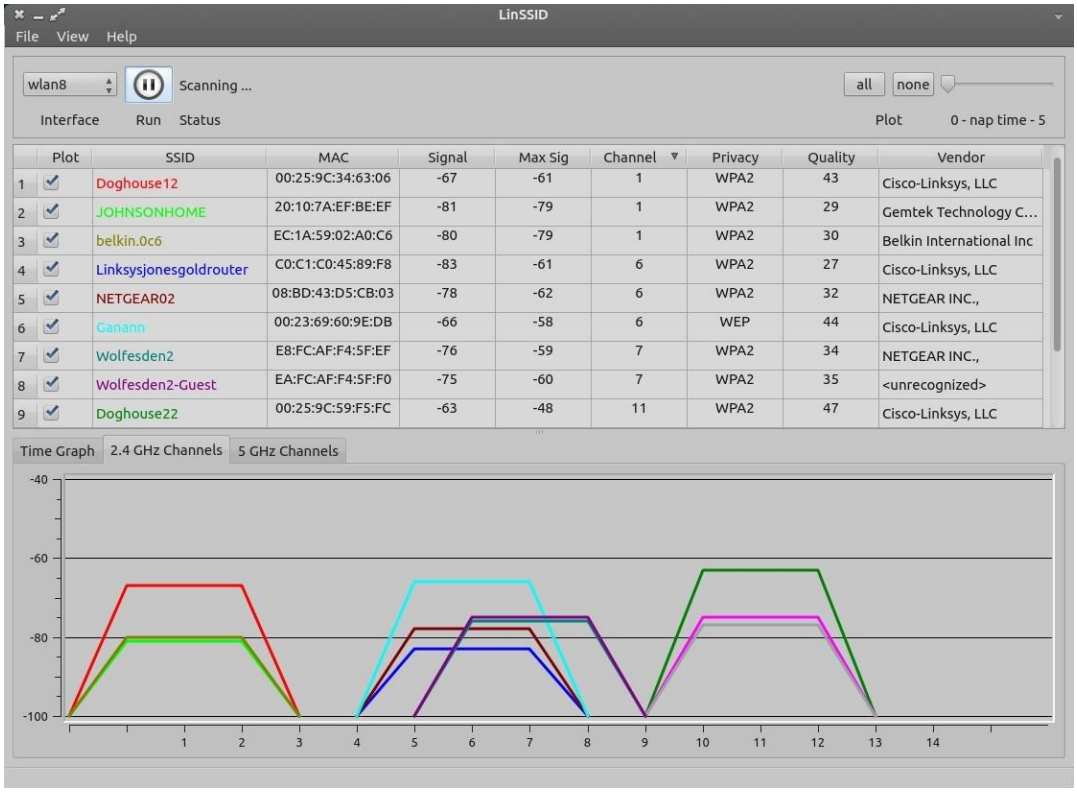

Figura. 12 LinSSID. Fuente: (SourceForge, 2014)

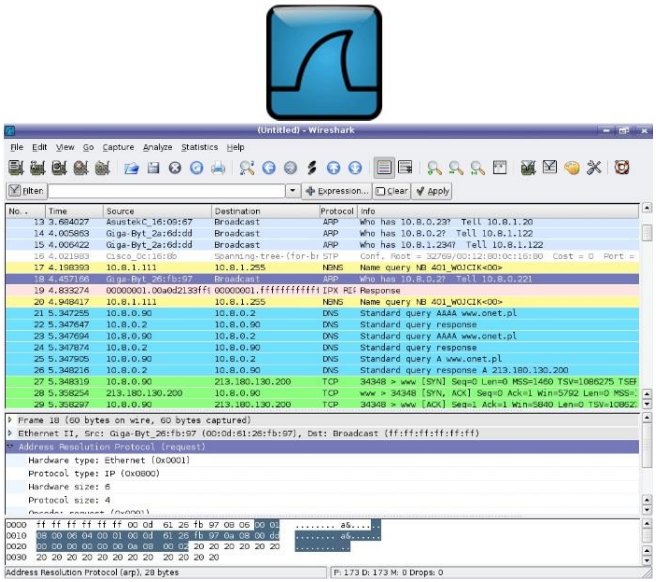

Figura. 13 Wireshark. Fuente: Elaboración Propia

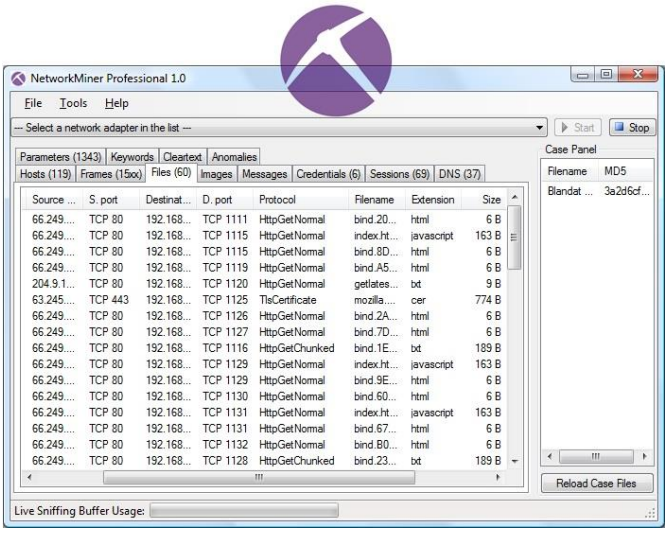

Figura. 14 NetworkMiner fuente: (Netresec, 2015)

La investigación realizada fue cuantitativa ya que se analizó los datos estadísticos que se recogieron de manera prospectiva a través de la herramienta Formulario de Google, también se utilizó las herramientas Excel 2013 y SPSS para tabular la información y realizar tablas informativas.

Los lugares donde se realizó la investigación tenían un gran número de concurrencia y eran de acceso público, se trabajó con adolescentes que son los que más concurren a los parques, además, participaron personas mayores de edad, estudiantes, personal administrativo y docentes de la PUCESE (ver Tabla 2), en los cuales se ha observado un mayor uso de teléfonos inteligentes y laptops, también participaron en la investigación los administradores de las redes de las áreas de estudios, estos mediante la información brindada nos permitieron determinar la existencia de vulnerabilidad en las redes WiFi y su nivel.

PUCESE	
Estudiantes	1454
Docentes	174
Personal administrativo	71
TOTAL	**1699**

Tabla 2 Población de la PUCESE. Fuente: Elaboración Propia

4.2.1. Población:

1. Administradores de red: En este estudio se realizó el análisis de 4 infraestructuras WiFi de acceso masivo:

    a. Municipio de Esmeraldas: Administrador de 3 puntos de distribución de servicio de internet vía Wifi para acceso público en los siguientes lugares: Parque Infantil, Parque de Las Palmas y Parque Central

    b. PUCESE: Administrador de 1 punto de distribución del servicio de internet de manera cableada e inalámbrica para los estudiantes y todo el personal que labora en la Institución.

2. Clientes:

a. Formada 1699 personas entre ellos estudiantes de primer a noveno ciclo de todas las carreras y personal que labora en la PUCESE
b. Integrada por aproximadamente 18000 personas las cuales se conectan en las redes WiFi de los parques de la ciudad de Esmeraldas

4.2.2. Muestras

Los administradores de las redes WiFi son muy pocos, por este motivo no se aplicó la técnica de muestreo y se procedió a realizar la encuesta al total de población que este caso eran dos.

Para obtener la muestra de los clientes de las redes WiFi se los dividió en dos sectores para que los resultados sean más fiables.

4.2.3. Muestra de clientes de redes WiFi PUCESE.

Esta muestra se obtuvo aplicando la siguiente formula:

$$n = \frac{N * d^2 * Z^2}{(N-1)\,E^2 + d^2 * Z^2}$$

N = Población 1699
d^2 = 0.25
N – 1 = 1698
E = Error de muestreo 0.06 6%
Z = Nivel de confiabilidad 1.96 95%

$$n1 = \frac{1699 * 0,25 * 3,8416}{(1698)\,0,0036 + 0,25 * 3,8416}$$

$$n1 = \frac{1631,7196}{7,0732}$$

n1 = 230,69

Valor de la muestra n1= 231

4.2.4. Muestra de clientes de redes WiFi Parques Provincia Esmeraldas

Para obtener la muestra a investigar en este caso se aplicó la siguiente formula:

$$n = \frac{N * d^2 * Z^2}{(N-1)\, E^2 + d^2 * Z^2}$$

N = Población 18000
d^2 = 0.25
N – 1 = 1698
E = Error de muestreo 0.065 6.5%
Z = Nivel de confiabilidad 1.96 95%

$$n1 = \frac{18000 * 0{,}25 * 3{,}8416}{(17999)\ 0{,}004225 + 0{,}25 * 3{,}8416}$$

$$n1 = \frac{17287{,}2}{77{,}0061}$$

n1 = 230,69

Valor de la muestra n2= 224

Una vez conocido el marco muestral para los clientes de las redes WiFi de la PUCESE y de las personas que se conectan en los parques de la ciudad de Esmeraldas, se realizaron los ensayos de encuestas respectivas para validar las preguntas de acuerdo a las observaciones dadas tanto por los pre encuestados como por los expertos, en base a este análisis se procedió a realizar la encuesta final.

4.2.5. Técnica Muestral aplicada

La técnica de muestreo aplicada para los administradores de las redes WiFi de Esmeraldas involucrados en el caso y los clientes PUCESE fue aleatorio simple, puesto que se conoce el número exacto de la población. Para los clientes de las redes WiFi en los parques de la ciudad de Esmeraldas se aplicó la técnica de muestreo aleatorio sistemático y muestreo aleatorio por conglomerado, debido a que en este caso no se conoce el número exacto de usuarios que hacen uso de este servicio. Las áreas donde se realizó la investigación están

ubicadas en diferentes sectores, debido a las observaciones de concurrencia se realizó la misma cantidad de encuestas en ambos sectores.

4.2.6. Análisis e interpretación de los datos.

La encuesta realizada a los administradores de las redes WiFi con la finalidad de medir el nivel de vulnerabilidad, estaba compuesta por 10 preguntas, de las cuales se pudo obtener un valor de 0,816 de confiabilidad como se puede apreciar en la Tabla 3.

Alfa de Cronbach	N de elementos
0,816	10

Tabla 3 Fiabilidad de encuesta para administradores de las redes WiFi. Fuente: Elaboración propia

Las encuestas que se realizaron a los clientes de las redes WiFi estaban compuestas por 9 preguntas y en este grupo se pudo obtener un valor de 0,702 de fiabilidad como se puede ver en la Tabla 4.

Alfa de Cronbach	N de elementos
0,702	9

Tabla 4 Fiabilidad de encuesta para clientes de las redes WiFi. Fuente: Elaboración propia

Como criterio general, George y Mallery (2003, p. 231) sugieren las recomendaciones siguientes para evaluar los valores de los coeficientes de alfa de Cronbach:

- Alfa > 0.9 es excelente
- Alfa > 0.8 es bueno
- Alfa > 0.7 es aceptable

Esto quiere decir que las encuestas realizadas son válidas para la investigación.

4.2.7. Preguntas a los administradores de las redes WiFi

A continuación se va analizar las preguntas más importantes de las encuestas que se realizaron a los administradores de las redes, para de esta manera determinar el nivel de vulnerabilidad.

Pregunta 2.

¿Utiliza un portal cautivo para el acceso de los usuarios a la red?

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	No	4	100,0	100,0

Tabla 5 Respuesta de la pregunta 2 para administradores

En esta pregunta se puede ver que los administradores no hacen uso de un portal cautivo para el acceso a la red, por lo tanto los usuarios tienen un tiempo ilimitado del servicio de internet y además un ancho de banda no controlado pudiendo de esta manera afectar a la calidad del servicio y además volver en cierto grado a la red vulnerable de crear descargas de información masivas o envió de peticiones o ataques a sitios remotos.

Pregunta 5.

¿Con que frecuencia analiza los log de conexión o de dispositivos activos de la infraestructura de comunicaciones?

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	A veces	3	75,0	75,0
	Casi Siempre	1	25,0	100,0
	Total	4	100,0	100,0

Tabla 6 Respuesta de la pregunta 5 para administradores

En la tabla 6 la misma que describe la pregunta 5, el 75% respondió que a veces revisa el log de conexiones en la red, por lo tanto hay pocas probabilidades de que se pueda detectar a tiempo un ataque en la red y por esta razón no se podría garantizar a los usuarios que la red es segura.

Pregunta 6.

¿Qué técnicas usa para evitar la clonación de la MAC del dispositivo que provee internet?

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Ninguno	3	75,0	75,0
	Tabla ARP	1	25,0	100,0
	Total	4	100,0	

Tabla 7 Respuesta de la pregunta 6 para administradores

Las respuestas en la pregunta 6 según la tabla 7 fue: ninguna, en un 75% esto quiere decir que la red es susceptible de tener ataques: MITM, envenenamiento ARP y Hijacking, es decir la información de los usuarios que se conecten a estas redes estarían corriendo peligro de ser intersectadas por terceros.

Pregunta 7.

¿Administra los puertos de los dispositivos activos mediante reglas de firewall?

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	No	3	75,0	75,0
	Si	1	25,0	100,0
	Total	4	100,0	

Tabla 8 Respuesta de la pregunta 7 para administradores

Como se puede apreciar en la tabla 8 el 75% de los administradores no aplican reglas de firewall para controlar los puertos de los dispositivos activos, esto quiere decir que estos dispositivos están susceptibles de ser atacado en cualquier momento de tal manera que esta red no sería segura.

Pregunta 8.

¿Realiza un análisis del espectro óptimo para la configuración del punto de acceso WIFI?

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Si	4	100,0	100,0

Tabla 9 Respuesta de la pregunta 8 para administradores

Los datos de la tabla 9 demuestran que el 100% de los encuestados respondieron que sí, por lo tanto el servicio WiFi que se propaga en los sectores que administran cada uno de ellos cubre todo el espacio de manera óptima es decir la señal llega de manera adecuada en cada uno de los rincones de las áreas que tienen a cargo.

Pregunta 9.

¿Valida la cantidad de puntos de acceso existentes con el fin de evitar suplantación de SSID?

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	No	4	100,0	100,0

Tabla 10 Respuesta de la pregunta 9 para administradores

Según la tabla 10 las respuestas fueron: No en un 100%, según estas respuestas cualquier persona podría estar en estos lugares y brindar internet vía WiFi con el mismo SSID que posee el punto de acceso oficial, de esta manera puede obtener todo el tráfico de red de las personas que se conecten en su AP y capturar contraseñas, correos, sesiones u otra información que pudiera comprometer a estos usuarios.

4.2.8. Resultado del análisis a las redes WiFi

En la tabla 11 se muestra el valor cuantitativo (Ver significado de los valores en el Anexo 3) que se obtuvo, sobre el nivel de vulnerabilidad de las redes WiFi.

Red WiFi	Valor	Nivel de vulnerabilidad
PUCESE	6.42	Medio
Parque Infantil	7.13	Alta
Parque Central	7.13	Alta
Parque de Las Palmas	7.13	Alta

Tabla 11 Nivel de vulnerabilidad de las redes WiFi de la ciudad de Esmeraldas

Nivel de vulnerabilidad promedio general = (PUCESE + Parque Infantil + Parque Central + Parque de Las Palmas) / 4

Nivel de vulnerabilidad promedio general = (6.42+7.13+7.13+7.13)/4

Nivel de vulnerabilidad promedio general = (27.81) / 4 = **6.95 (Alta)**

En base a las respuestas de las encuestas de los administradores de las redes y a las pruebas basadas en la metodología OWISAM se pudo constatar que a los usuarios de las redes públicas no se les puede garantizar protección cuando navegan en internet, ya que en promedio general se obtuvo un nivel de vulnerabilidad alto, esto quiere decir que la mayoría de estas redes son susceptibles de ataques MITM, envenenamiento ARP, Hijacking, Spoofing, Sniffing, y Ataque DOS desde estos puntos tanto a servicios internos como externos.

4.2.9. Preguntas a los clientes de las redes WiFi

A continuación se va analizar las preguntas más importantes de las encuestas que se realizaron a los clientes de las redes públicas, para de esta manera determinar su nivel de conocimiento.

Pregunta 2.

¿Ha configurado su dispositivo para no conectarse automáticamente a una red WiFi pública o de acceso libre?

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Desconozco esta opción	74	16,2	16,2
	No	232	50,7	66,8
	Si	152	33,2	100,0
	Total	458	100,0	

Tabla 12 Respuesta de la pregunta 2 para clientes

Las respuestas de la pregunta 2 fueron el 68,8% entre: No y Desconozco esta opción y un 33,2% respondió que Si, en base a estas respuestas, mayor parte de las personas que poseen dispositivos con WiFi están expuestos a que un tercero pueda acceder a su información y dispositivo a través del WiFi.

Pregunta 3.

¿Con que frecuencia abre su cuenta bancaria o realiza pagos de ciertos servicios mientras está conectado en una red WiFi de acceso público?

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Siempre	1	,2	,2
	Casi Siempre	75	16,4	16,6
	A veces	165	36,0	52,6
	Casi Nunca	100	21,8	74,5
	Nunca	117	25,5	100,0
	Total	458	100,0	

Tabla 13 Respuesta de la pregunta 3 para clientes

Las respuestas de la pregunta Nº 3, demuestran que el 52,6% como promedio de ocurrencia de los encuestados abren su cuenta bancaria o realizan pagos cuando están conectados a una red WiFi de acceso público, estas personas estarían corriendo el riesgo de que su información que en este caso es delicada sea tomada por un tercero y verse involucrados en situaciones de fraude.

Pregunta 4.

¿Conoce los riesgos que conlleva conectarse a una red WiFi de acceso público?

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	No	268	58,5	58,5
	Si	190	41,5	100,0
	Total	458	100,0	

Tabla 14 Respuesta de la pregunta 4 para clientes

Los resultados de la pregunta Nº 4, en su mayoría fueron No, es decir mayor parte de la población no está bien informada sobre el riesgo corren en las redes WiFi de acceso público, esto hace relación a las respuestas de las preguntas 3 y 2.

Pregunta 7.

¿Tiene activado el firewall en su dispositivo?

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Desconozco esto	68	14,8	14,8
	No	200	43,7	58,5
	Si	190	41,5	100,0
	Total	458	100,0	

Tabla 15 Respuesta de la pregunta 7 para clientes

El firewall es uno de los principales mecanismos de seguridad en los dispositivos, en la pregunta 7 la mayoría ha contestado que No lo tiene activado, otra parte han contestado que desconocen esto, esto es preocupante puesto que la información de estas personas y también sus dispositivos están con alta posibilidad de encontrarse expuestos a ser intersectados por cualquiera.

4.2.10. Resultado de encuestas a los clientes de las redes WiFi

Las respuestas de las encuestas demuestran que mayor parte de la población desconoce los riesgos en las redes WiFi y es por esta razón que hacen pagos en internet, sus dispositivos se conectan sin aviso previo a cualquier punto WiFi público, no tienen

activado el firewall y en algunos casos desconocen lo que es este mecanismo de seguridad, en base a estas respuestas se puede determinar que el nivel de conocimiento de la población en Medio y Bajo sobre las redes WiFi.

4.2.11. Uso de herramientas para detectar vulnerabilidades ejemplo a nivel Usuario.

Para detectar las vulnerabilidades en las redes se utilizó las herramientas mencionadas anteriormente en la sección 5. Estas herramientas brindan información que transita a través de la red, por este motivo se las aplico en un ambiente controlado y en un horario en el que no había mucha concurrencia de personas.

Primeramente se analizó el espectro de las redes WiFi en la PUCESE en la cual se pudo constatar la existencia de varios AP en canales distintos pero con una contraseña en común la cual es conocida por todas las personas que transitan en estas instalaciones, en la figura 16 y 17 se puede observar la información recolectada por la aplicación LinSSID.

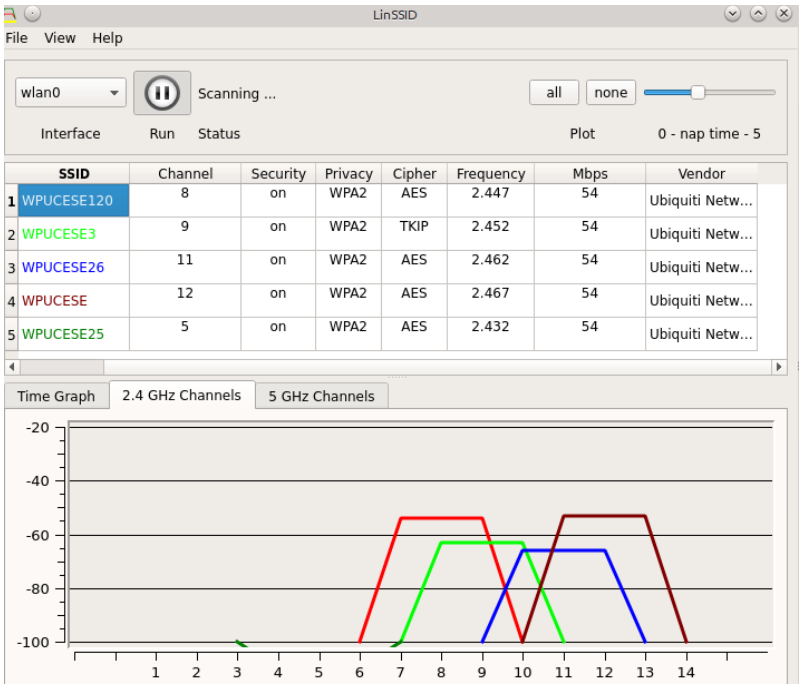

Figura. 15 Análisis 1 de la señal WiFi en la PUCESE. Fuente: Elaboración propia

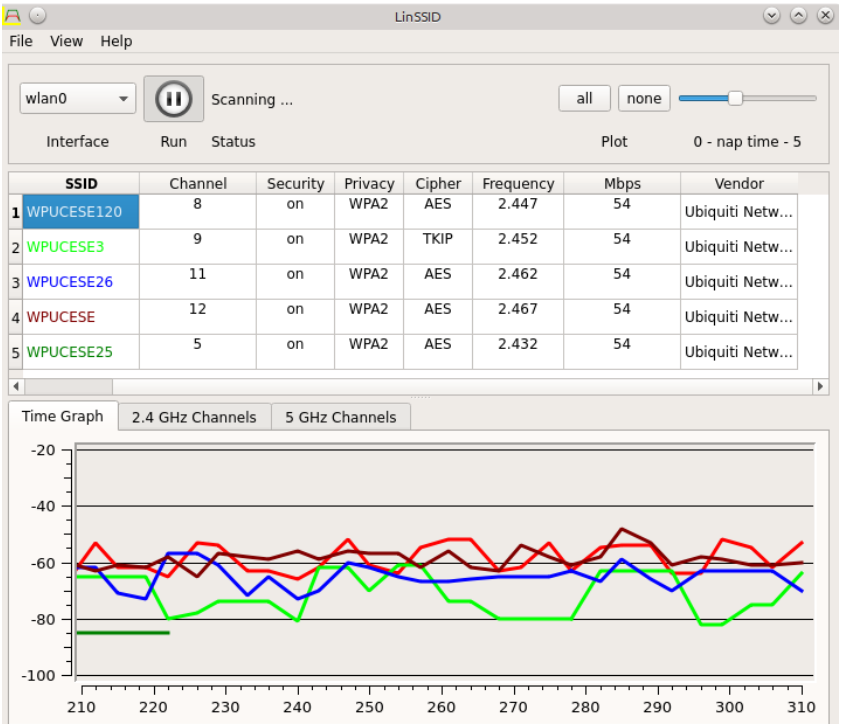

Figura. 16 Análisis 2 de la señal WiFi de la PUCESE Fuente: Elaboración propia

En los parques de la ciudad de Esmeraldas se aplicó el mismo proceso antes mencionado, durante el análisis se obtuvo los nombres de las diferentes redes WiFi que se encuentran alrededor de los parques (Ver Figura 17), de igual manera se obtuvo información detalla de estas redes, luego de un análisis se pudo notar que hay probabilidades de interferencia entre las redes puesto que hay algunas que se están propagando sobre el mismo canal, adicional a ello también se detectó un AP con el SSID WiFi-Gratis que se está propagando en la misma área de cobertura de la WiFi Oficial y no tiene clave de acceso, esto da posibilidades de que alguien se conecte a este AP pensando que es la red del parque y su información sea interceptada.

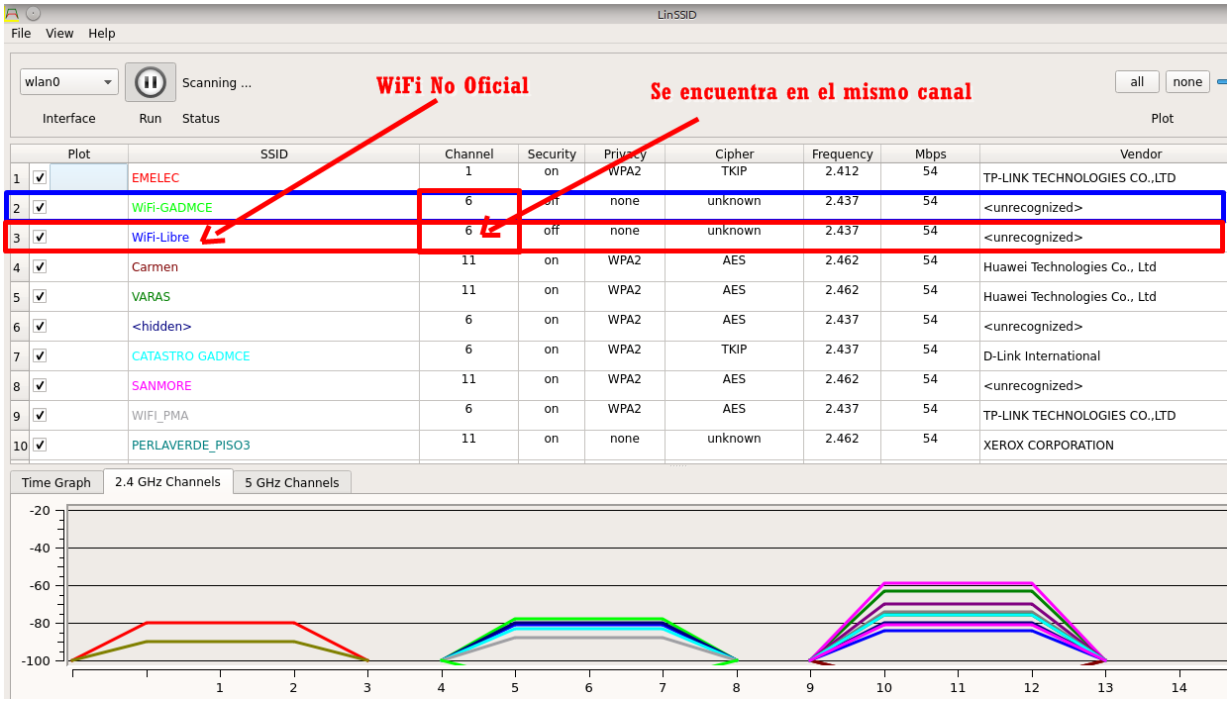

Figura. 17 Análisis de la señal WiFi en los parques de Esmeraldas. Fuente: Elaboración propia

Luego de conocer todos los AP disponibles se procedió a conectarse, para de esta manera explorar y conocer quiénes están utilizando la red y la configuración que tienen aplicada en sus dispositivos, para esto se utilizó la herramienta ZenMap.

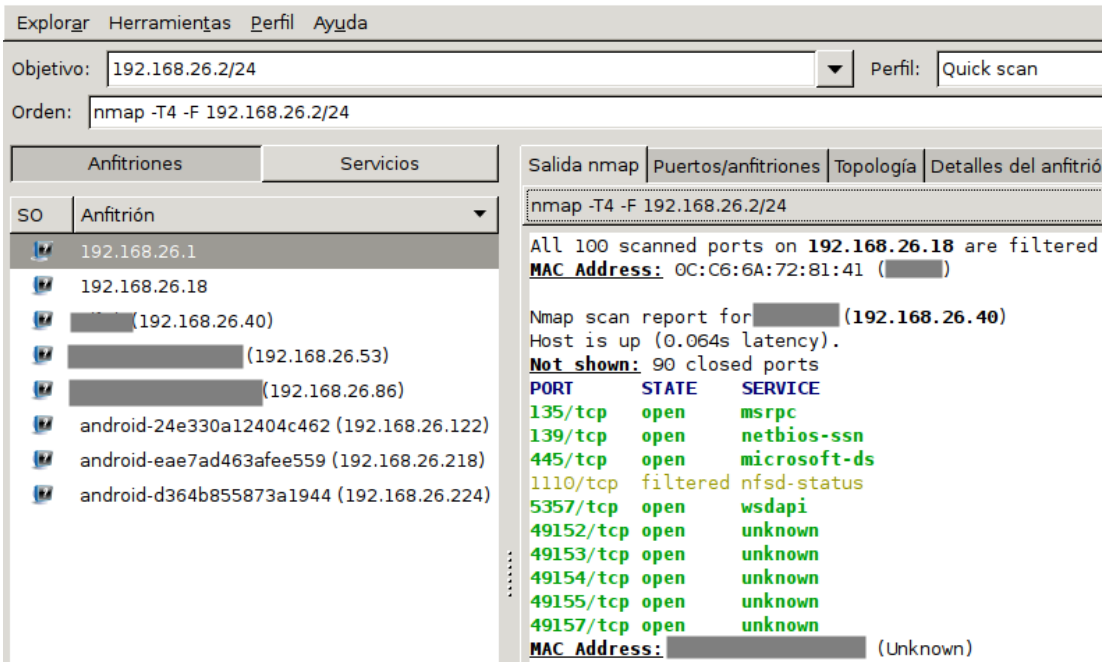

Figura. 18 Análisis de la red con ZenMap. Fuente: Elaboración propia

Como se puede apreciar en la figura 18 y 19 uno de los dispositivos conectados en la red posee muchos puertos abiertos, lo cual brinda muchas posibilidades a que se pueda acceder a su dispositivo con exploits automáticos.

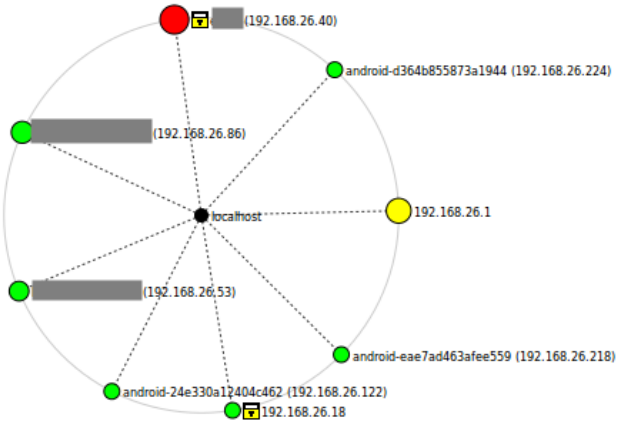

Figura. 19 Topología de la red explorada con ZenMap. Fuente: Elaboración propia

Siguiendo con el proceso de análisis de la red se procedió a utilizar Wireshark para obtener el tráfico generado por los clientes conectados a la red y posteriormente filtrar la información con la aplicación NetworkMiner como se puede ver en las figuras 20 y 21.

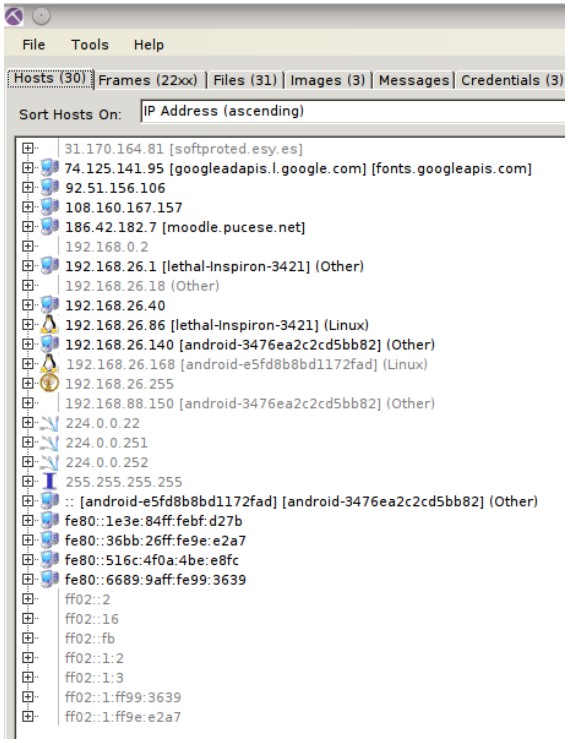

Figura. 20 Reporte de host visitados. Fuente: Elaboración propia

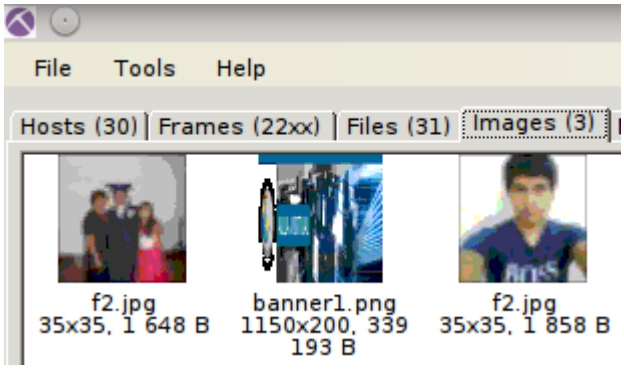

Figura. 21 Captura de imágenes. Fuente: Elaboración propia

A continuación se va a mostrar que es posible la obtención de información privada como: nombres de usuarios, contraseñas e incluso sesiones ya iniciadas anteriormente.
Cabe destacar que esta información es de mi propiedad y se hace la demostración con fines educativos.

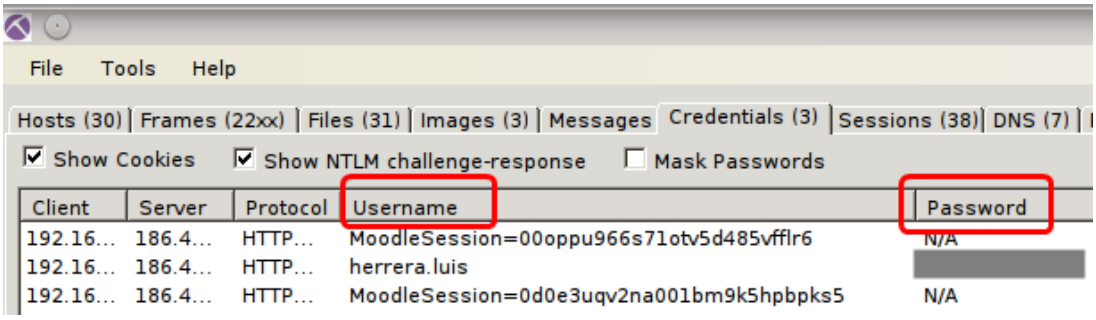

Figura. 22 Credenciales obtenidas. Fuente: Elaboración propia.

La obtención de una sesión es similar a obtener el usuario y contraseña de una persona puesto que este identificador de sesión (Ver figura 23) se puede usar para ingresar al

sistema obteniendo un pase inmediato sin necesidad de ingresar usuario a esto se lo conoce como Hijacking.

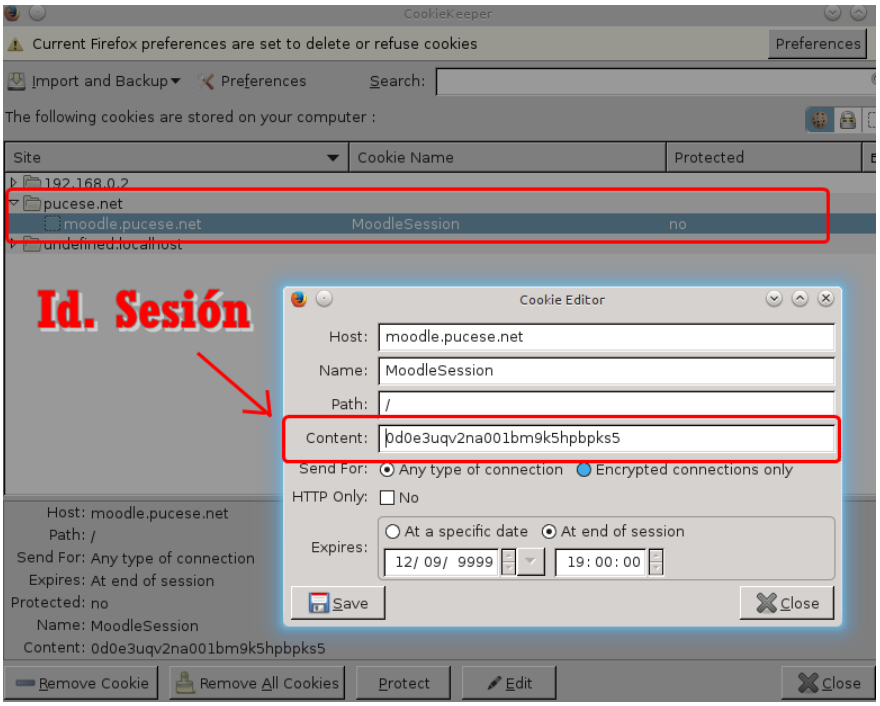

Figura. 23 Demostración de Hijacking. Fuente: Elaboración propia.

Con esto se pudo demostrar que la información de un usuario que está conectado en una red WiFi pública no está segura, en este caso se obtuvo las credenciales de una plataforma de educación web (Moodle), pero también se podría obtener las credenciales del acceso al banco, tarjetas bancarias, correos, entre otros servicios.

4.2.12. Uso de herramientas para detectar vulnerabilidades ejemplo a nivel proveedor de internet (Suplantación SSID)

En esta ocasión se utilizó una laptop para proveer internet vía WiFi con una SSID un poco similar a la que oficialmente provee internet en la Universidad PUCESE a la cual se la llamo WPUCESE_FIBRA_OPTICA (Ver imagen 24) y no se le puso clave para acceder.

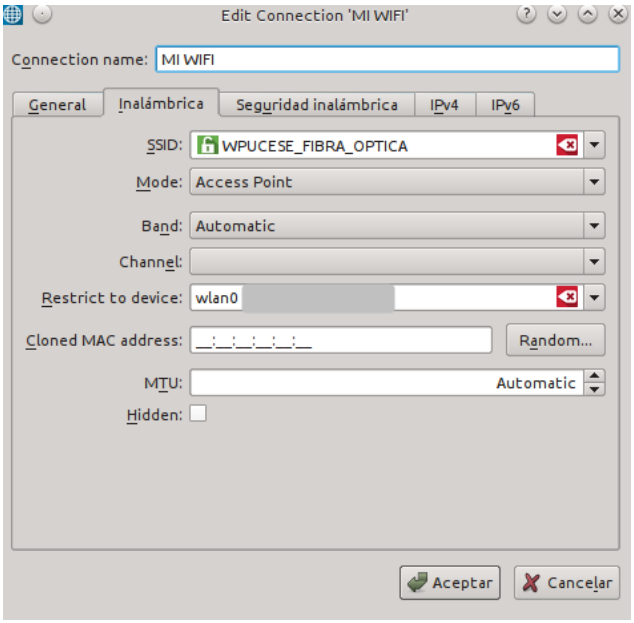

Figura. 24 Configuración de AP. Fuente: Elaboración propia

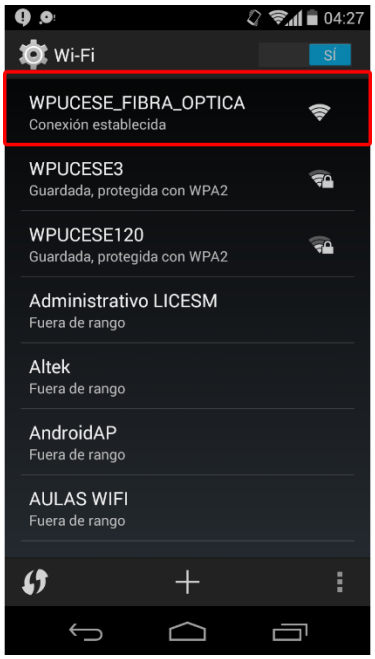

Figura. 25 Conexión a la AP desde Celular. Fuente: Elaboración propia

Luego de conectar el celular a la red se procedió a visitar páginas y acceder a aplicaciones, cuya información fue capturada por el AP en este caso la laptop, mediante la aplicación Wireshark, al momento de analizarla se obtuvo los siguientes datos.

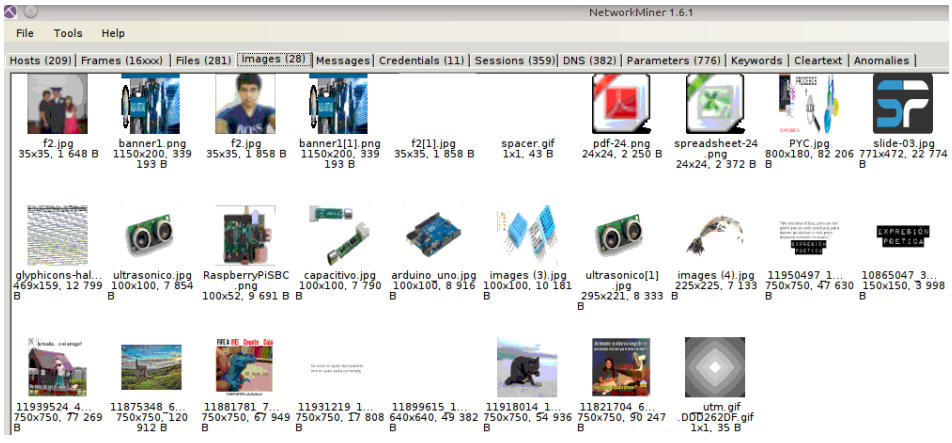

Figura. 26 Captura de imágenes del cliente. Fuente: Elaboración propia

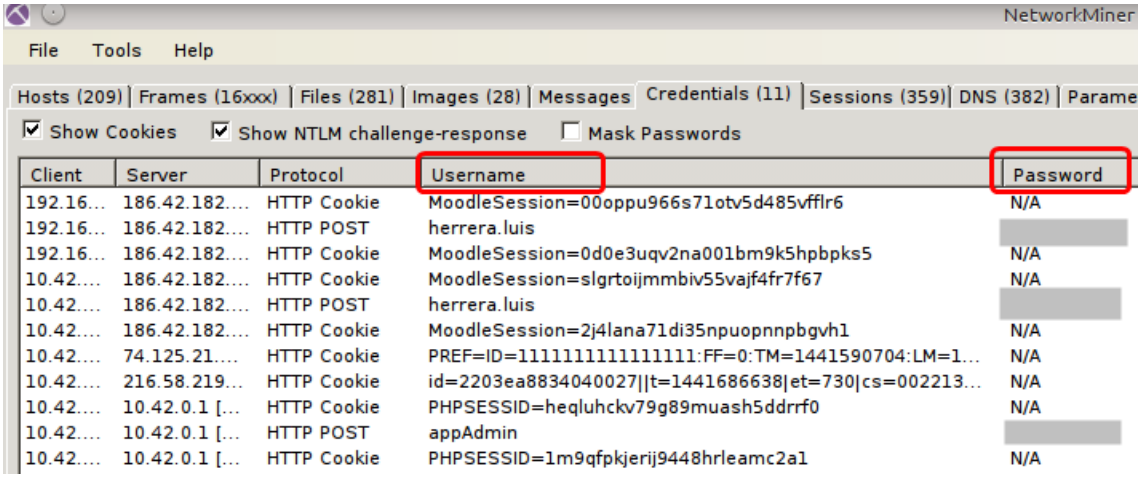

Figura. 27 Credenciales del cliente. Fuente: Elaboración propia.

Como se pudo observar en las figuras 26 y 27 el AP que se instaló funciono sin ninguna restricción por parte de los AP oficiales, logrando de esta manera obtener toda la información del cliente que se conectó en ese momento.

5. Propuesta

5.1.1. Para los administradores de red.

Considerando que:

- La empresa que les brinda el servicio de internet a los sectores que se analizaron utilizan la infraestructura y se rigen a las normativas de CNT y en base a los Reglamentos para clientes de la resolución CANATEL 29, Capítulo V (De Las Obligaciones Y Responsabilidades) que establece esta empresa pública.

- Las recomendaciones de SOPHOS sobre seguridad para administradores de redes.

- Recomendaciones de Ramos Valencia en su investigación análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico para el acceso seguro en redes Wifi.

- La metodología OWISAM mediante sus indicadores de nivel de vulnerabilidad.

- Tomando en cuenta que en los lugares de estudio se utiliza tecnologías Mikrotik se propone lo siguiente:

1. Autenticar los usuarios mediante pre registro de dispositivo en su respectiva tabla ARP estática. Puede encontrar más información en: http://wiki.mikrotik.com/wiki/How_to_secure_a_network_using_ARP

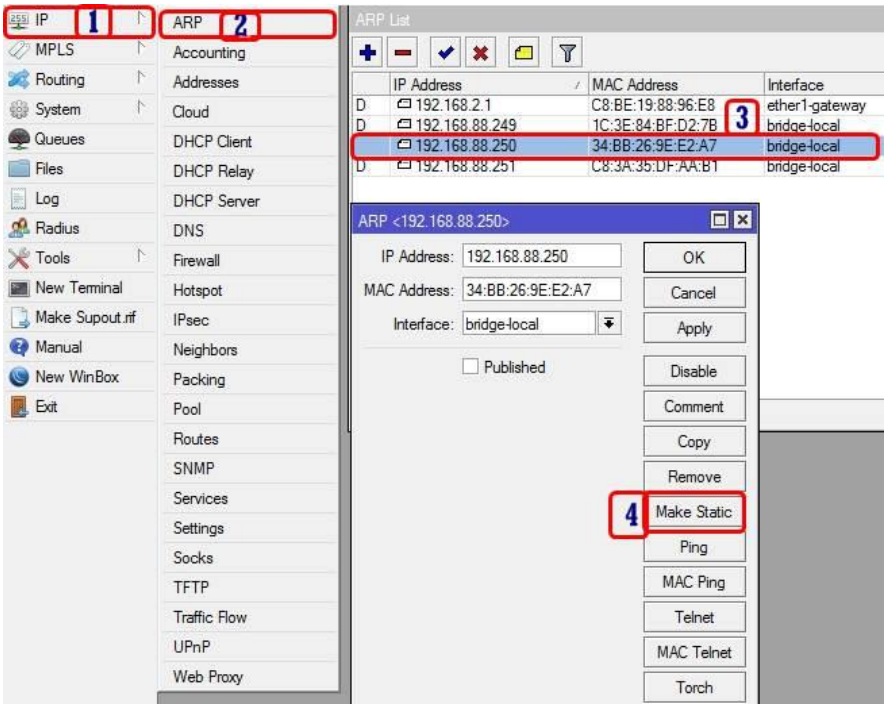

Figura. 28 Pasos para registro de clientes en tabla ARP estática en Mikrotik Fuente: Elaboración propia

2. Colocar en puntos estratégicos información de los riesgos que conlleva conectarse a una red pública y además indicarles a los usuarios cual es la configuración adecuada que deben tener sus dispositivos.

3. Establecer puntos para registro de usuarios permitidos en la red con sus respectivos equipos.

4. Se debe hacer que los usuarios firmen la aceptación de responsabilidad del uso de esta tecnología y adicionar autenticación con RADIUS para que de esta manera los usuarios puedan conectarse a la red desde cualquiera de los AP oficiales. Puede encontrar más información en:
   http://wiki.mikrotik.com/wiki/Hotspot_server_setup

Figura. 29 Ejemplo de formulario de aceptación de términos de uso de la red WIFI e ingreso de credenciales Fuente: Elaboración propia

Para implementación del servidor RADIUS hay varias opciones tanto gratis como de pago entre ellas tenemos:

1. Free RADIUS
2. ChilliSpot
3. Radius manager en su versión resiente 4

4. Crear reglas de bloqueo a usuarios que intenten acceder a servicios no autorizados mediante script generando listas de accesos. Ver más información en: http://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter

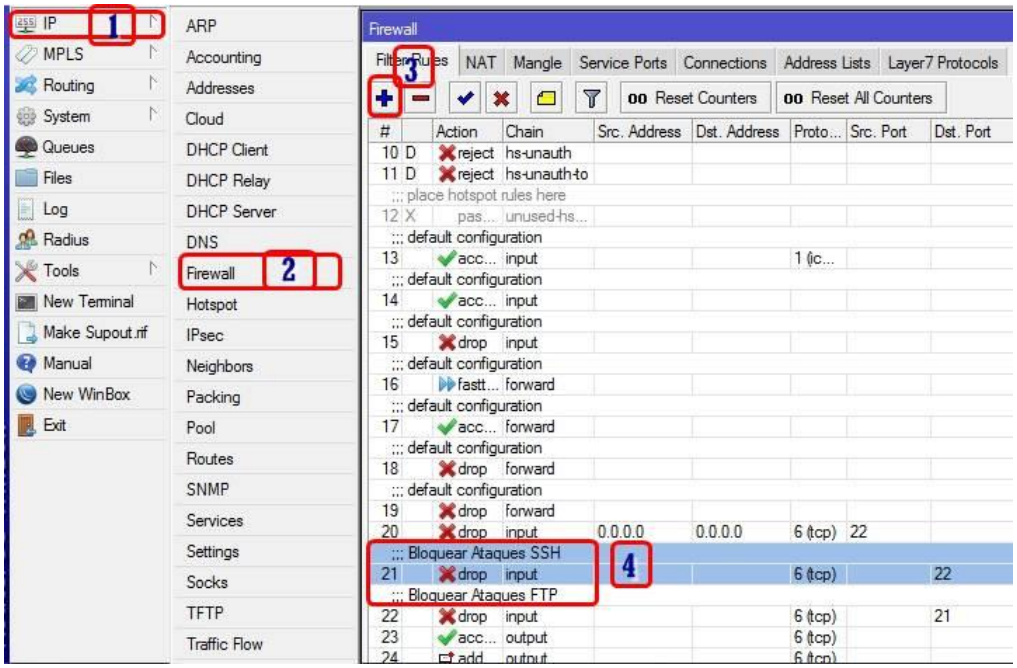

Figura. 30 Ejemplo de creación de reglas de bloqueos en Mikrotik Fuente: Elaboración propia

5. Crear una rutina de análisis de log en los equipos para saber el comportamiento de la infraestructura.

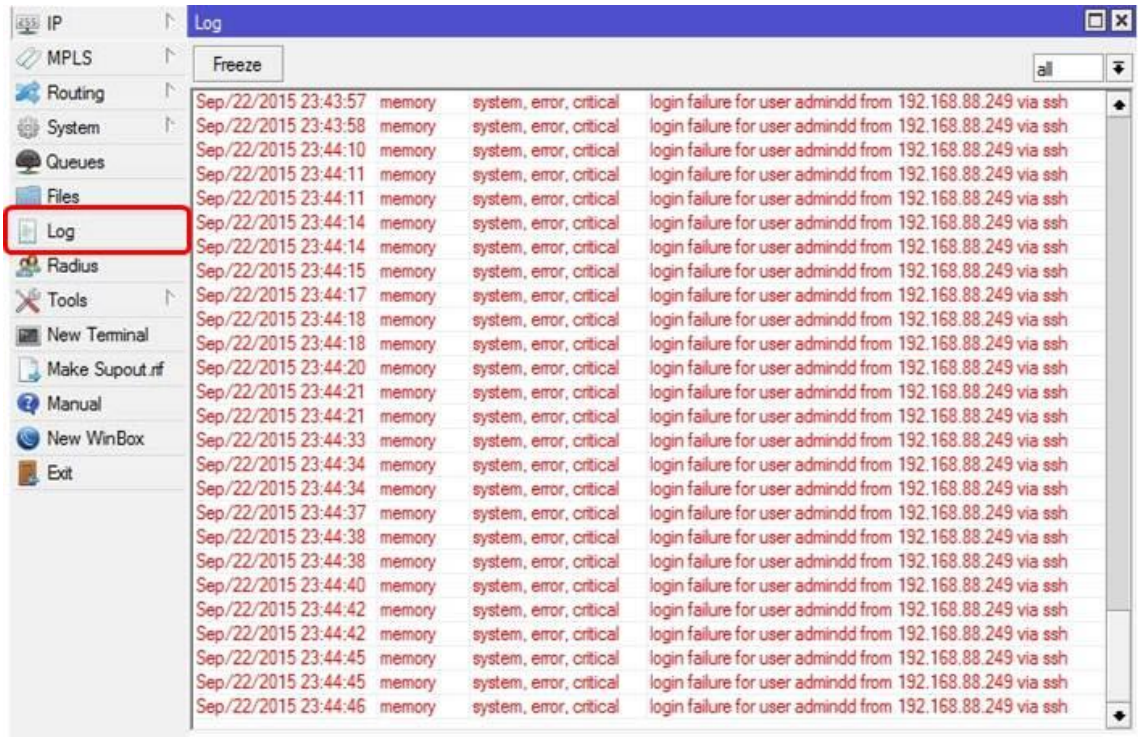

Figura. 31 Ejemplo de revisión del Log de conexiones en Mikrotik Fuente: Elaboración propia

6. Monitorear las diferentes SSID que se encuentren en el rango de acceso y de encontrar una no autorizada bloquearla.

   Para esto se recomienda usar tecnologías cisco CleanAir ya que permite manejar grandes volúmenes de usuarios en una red y además:

   - Detecta las interferencias de RF que otros sistemas no detectan.
   - Identifica la fuente y la ubica en un plano de planta.
   - Realiza ajustes automáticos para optimizar la cobertura inalámbrica y superar los problemas de interferencia (Cisco, 2015)

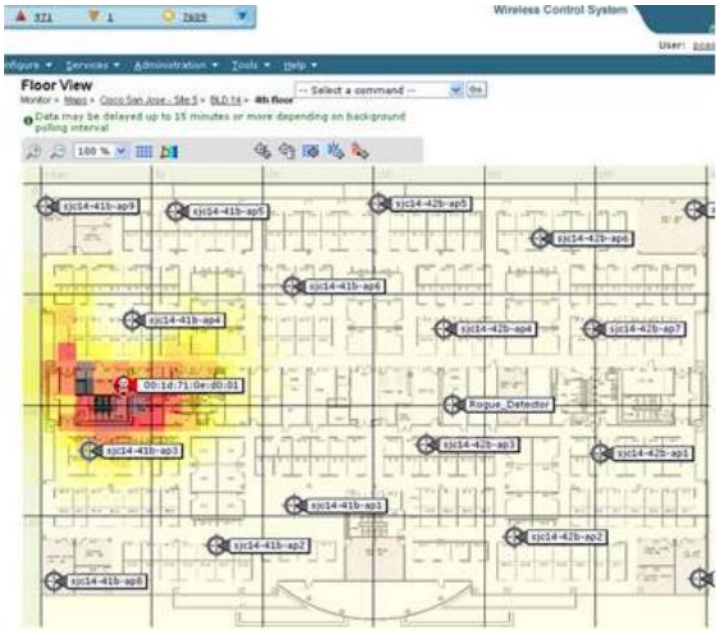

Figura. 32 Tecnologías Cisco CleanAir. Fuente: (Cisco, 2015)

5.1.2. Para los clientes de la red.

De acuerdo a las recomendaciones de varios autores en internet entre ellos Kaspersky Internet Security 2015 y Panda media center sobre las vulnerabilidades de las redes WiFi públicas y como protegerse se recomienda lo siguiente:

1. No hacer transacciones bancarias o pagos de servicios en los cuales tenga que ingresar los datos de su tarjeta bancaria.

2. El caso de tener trabajar con información confidencial relacionada con: contraseñas, banco, documentos, etc. Use el protocolo HTTPS o una VPN. Ver más información en:

   http://www.welivesecurity.com/2010/11/10/vpn-ssl-and-https/

3. Asegurarse de tener activado el Firewall de su dispositivo antes de conectarse a este tipos de redes. Ver más información en:
   https://support.microsoft.com/es-es/kb/283673

4. Informarse de las consecuencias de incurrir o ser víctima de un delito informático. Ver más información en:
   http://www.justicia.gob.ec/

6. Referencias Bibliográficas

Aema, G. (2012, 10 27). *Robo de sessiones mediante cookies s7k.* Obtenido de https://losindestructibles.files.wordpress.com/2012/10/11.png?w=400&h=246

BackBox. (2015, 07 13). *BackBox Linux*. Obtenido de https://www.backbox.org/

Cisco. (2015, 09 15). *Tecnología CleanAir.* Obtenido de http://www.cisco.com/web/LA/soluciones/cleanair.html

CNT. (2011, 06 11). *Reglamento para clientes de servicios que presta la CNT EP*. Obtenido de http://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Reglamento-para-Clientes-de-Servicios-que-Presta-la-CNT-EP.pdf

COIP. (2015, 05). *Ministerio de justicia, derechos humanos y cultos.* Obtenido de http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf

Conocimiento. (2015, 02 05). *Estrategias de Ataque Red Común: Packet Sniffing*. Obtenido de http://www.slickpalm.com/estrategias-de-ataque-red-comun-packet-sniffing/

El Comercio. (2015, 06 16). *Ojo con los delitos informáticos; sea más cuidadoso*. Obtenido de http://www.elcomercio.com/actualidad/ojo-delitos-informaticos-cuidado-robo.html

Escudero Pascual Alberto, L. I. (2007). *Seguridad en Redes Inalámbricas.* Tricalcar.

Espinosa, C. (2014, 12 29). *Cobertura Digital.* Obtenido de Redes Sociales Ecuador: Facebook pasó los 8 millones (2015): http://www.coberturadigital.com/2014/12/29/redes-sociales-ecuador-facebook-paso-los-8-millones-2015/

Gabriela, G. (2014, 06 05). *Qué es un ataque "Man in The Middle"*. Obtenido de Hipertextual: http://hipertextual.com/archivo/2014/06/ataque-man-in-the-middle/

García Prieto, D. (2014, 09). *Seguridad en redes inalámbricas: el protocolo WEP*. Obtenido de UNIVERSIDAD DE CANTABRIA: http://repositorio.unican.es/xmlui/bitstream/handle/10902/5944/Diego%20Garcia%20Prieto01.pdf?sequence=5&isAllowed=y

INEC. (2013, 01 01). *Instituto Nacional de Estadística y Censos.* Obtenido de http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/Resultados_principales_140515.Tic.pdf

INEC. (2015). *Instituto Nacional de Estadisticas y Censo.* Obtenido de Encuesta Condiciones de Vida ECV: http://www.ecuadorencifras.gob.ec/documentos/web-inec/ECV/ECV_2015/documentos/ECV%20COMPENDIO%20LIBRO.pdf

Kaspersky. (2015, 03 19). *How to enable or disable notifications of vulnerabilities in Wi-Fi networks in Kaspersky Internet Security 2015*. Obtenido de http://support.kaspersky.com/us/10965#public

Kunkle, S. (2013, 05 23). *IT Support | The Evolution of Cyber Attacks & US Concerns*. Obtenido de http://trigon.com/tech-blog/bid/97439/IT-Support-The-Evolution-of-Cyber-Attacks-US-Concerns

La Hora. (2015, 01 04). *Amenazas cibernéticas para el año 2015*. Obtenido de CIENCIA Y TECNOLOGÍA: http://www.lahora.com.ec/index.php/noticias/show/1101768475#.VZ_X4Pl_NBc

Mallery D, P. G. (2003). *SPSS for Windows step by step: A simple guide and reference. 11.0 update (4 th ed.).* Boston: Allyn & Bacon.

Moreno Carlos, P. A. (2014, 05 13). *Diseño e implementación de una red WIFI y y un circuito cerrado de televisión para el sistema de seguridad, monitoreo y control de la Unidad Académica Héroes del Cenepa de la ESPE.* Obtenido de Repositorio Digital ESPE: http://repositorio.espe.edu.ec/handle/21000/8689

Netresec. (2015, 08 8). *NetworkMiner*. Obtenido de http://www.netresec.com/?page=NetworkMiner

Offensive Security . (2011). *Penetration Testing with Backtrack.* Offensive Security.

OWISAM. (2013, 04 09). *OWISAM.* Obtenido de https://www.owisam.org/es/P%C3%A1gina_principal

Panda Media Center. (2015, 07 8). *Cómo conectarnos de manera segura a una red WiFi pública*. Obtenido de http://www.pandasecurity.com/spain/mediacenter/consejos/redes-wifi-publicas-seguras/

Ramos Valencia, M. V. (2015, 08 21). *Análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico para el aceso seguro en redes Wifi.* Obtenido de http://dspace.espoch.edu.ec/handle/123456789/4058

Silva Larry, R. E. (2011). *Universidad Tecnológica de Pereira.* Obtenido de http://repositorio.utp.edu.co/dspace/bitstream/11059/2518/1/0058S586.pdf

SOPHOS. (2015, 08 25). *Consejos de seguridad para administradores de redes empresariales*. Obtenido de https://www.sophos.com/es-es/security-news-trends/best-practices/10-tips.aspx

Soto, J. (2014, 07 05). *Ataque MITM mediante ARP Poisoning con Kali Linux*. Obtenido de http://www.jsitech.com/linux/ataque-mitm-mediante-arp-poisoning-con-kali-linux/

SourceForge. (2014, 08 31). *SourceForge*. Obtenido de http://sourceforge.net/projects/linssid/

Stretch, J. (2009, 02 02). *PacketLife.net.* Obtenido de http://media.packetlife.net/media/blog/attachments/338/neighbor_spoofing.png

UGR Cyber Security Group. (2015). *Introducción al Hacking Ético de sistemas y redes.* Obtenido de http://ucys.ugr.es/download/taller1/Taller1_Intro_hacking.pdf

University of Maryland. (2015, 08 18). *MC2 Researcher Weighs In On Public Wi-Fi Vulnerabilities*. Obtenido de http://www.cyber.umd.edu/news/news_story.php?id=9203

USERS. (2012). *Hacking desde cero.* Buenos Aires: Fox Andina & Gradi S.A.

WNDW. (2007). *Wireless Networking in the Developing World.* Obtenido de http://wndw.net/pdf/wndw2-en/wndw2-ebook.pdf

7. Anexos.

Esmeraldas 23 de Septiembre de 2015.

Ingeniero.
Jhonny Quiñonez.
Jefe de redes y telecomunicaciones.
PUCESE

En su despacho.-

Mediante el presente extiendo un cordial saludo y a la vez solicito su autorización para la realización de procesos de prueba sin interferir en el normal funcionamiento de la infraestructura de red específicamente en las conexiones inalámbricas, lo cual me servirá para evidencias dentro del desarrollo de mi proyecto de tesis como estudiante de la carrera de ingeniería en sistemas y computación en la PUCESE.

Agradeciendo por la atención prestada.

Luis Herrera.
Egresado PUCESE.

Autorizado
23/09/2015

Anexo 1. Autorización para análisis de la red PUCESE

Esmeraldas Al Mundo

Departamento de Sistemas

GADMCE-FXGS

PARA: Luis Alberto Herrera Izquierdo
Egresado de la PUCESE

DE: Ing. Francel García Sacoto.
JEFE DPTO. DE SISTEMAS.

ASUNTO: En el Texto

FECHA: Esmeraldas, 7 de octubre del 2015

Por medio de la presente damos la autorización respectiva a su solicitud, referente a la realización del proceso de pruebas en las zonas públicas "Wifi libres.

Sin otro particular, suscribo de usted.

Atentamente,

Ing. Francel García Sacoto
JEFE DPTO. SISTEMAS

Bolívar y 9 de Octubre (esquina)
Teléfonos: 2 727 943 | 2 723 202
www.municipioesmeraldas.gob.ec

Anexo 2. Autorización para análisis de la red de los parques de Esmeraldas

Tabla de valoración		
Valor	**Nivel de riesgo**	**impacto**
0 – 2	**Mínimo**	Mínimo riesgo de acceso no autorizado. Un ataque exitoso requeriría de una ventana temporal mayor al definido en el alcance de esta revisión así como un nivel de especialización alto.
3 – 4	**Bajo**	Riesgo muy reducido de que un usuario no asociado a la organización sea capaz de acceder a la infraestructura inalámbrica existente. El impacto que puede tener sobre la infraestructura es limitado.
5 - 6	**Medio**	Existe la posibilidad no despreciable de modificación de información, robo de credenciales o modificación del comportamiento normal del sistema, aunque las consecuencias para el sistema son limitadas. Este ataque es viable dentro de un marco temporal inferior a 1 mes.
7 - 9	**Alto**	La probabilidad de que ocurra un acceso no autorizado a los activos de la Organización es alta, debido principalmente a la existencia de debilidades en las redes inalámbricas existentes. Un atacante podrá impactar significativamente en la operación normal de los sistemas.
10	**Crítico**	La probabilidad de que ocurra un acceso no autorizado en los activos de la organización es muy elevada, debido a la existencia de redes inalámbricas que tienen visibilidad de sistemas internos y que pueden ser accedidas por usuarios externos.

Anexo 3. Tabla de valoración de vulnerabilidad de la red Wifi. Fuente: (OWISAM, 2013)

8. Glosario

AP: Punto de acceso a internet

ARP: Conocido también como Protocolo de resolución de direcciones, es el encargado de relacionar la dirección física (MAC) de un dispositivo en la red a una determinada IP.

Firewall: Mecanismo de seguridad que filtra la información proveniente de internet y permite el paso de esta al dispositivo o la bloquea, esto depende de la configuración que se establezca.

MAC: También conocida como dirección física, es identificador único que poseen los dispositivos.

Pen-test: Herramientas para hacer auditoria informática o buscar vulnerabilidades en sistemas

Portal Cautivo: Servidor en una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal.

RADIUS: Palabra proveniente del acrónimo Remote Authentication Dial-In User Service es un protocolo de autenticación y autorización de sesiones para tener acceso a una red.

SSID: Es el nombre o identificador de una red.

Sniffer: También conocido como analizador de paquetes este es un programa informático que registra la información que envían los dispositivos que están conectados en la red de comunicación.