UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

OCTUBRE 2017 – MARZO 2018

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCION DEL TITULO DE INGENIERA EN SISTEMAS

TEMA

ANÁLISIS DE AMENAZAS Y VULNERABILIDADES EN LA RED WIFI DE LA PREFECTURA DE LA PROVINCIA DE LOS RÍOS.

EGRESADA

TATIANA LISETH BAJAÑA MOLINA

TUTOR

ING, ANA FERNÁNDEZ.

AÑO 2018

INTRODUCCIÓN

En el Ecuador es muy común observar un asiduo incremento de forma exponencial del uso de las redes *Wireless Fidelity (Wi-Fi);* debido a este factor la sociedad contemporánea avanza vertiginosamente basado en las bondades que proveen el uso directo e indirecto del equipamiento físico y lógico orientado a las comunicaciones y telecomunicaciones, contribuyendo de forma clara y especifica con desarrollo tecnológico, transferencia de conocimientos, renovación e innovación de los criterios de pensamiento y por ende el desarrollo del entorno socio político, cultural, académico y social.

Por tal razón se pretende a través de esta investigación aportar con un contenido equilibrado con un estudio de caso que se enmarca en el análisis de amenazas y vulnerabilidades en la red WiFi de la Prefectura de la Provincia de Los Ríos, incursionando en teorías y métodos de investigación que se acogen de manera estricta a la técnica de observación, análisis e interpretación de resultados.

Al hablar de innovación, se refriere a la estructuración de una guía técnica del comportamiento que posee la red *Wireless Fidelity (Wi-Fi)* de la Prefectura de la Provincia de los Ríos en el instante que existan incidencias causadas por las amenazas ya sean de tipo internas o externas y de igual forma identificar cuáles son los tipos de vulnerabilidades y el grado de afectación a la infraestructura de la institución a causa de los elementos adversos a su naturaleza.

La investigación estará basada en toda la información que se haya recopilado, tabulado y compilado luego de haberse ejecutado visitas técnicas, observación directa al

entorno de la red de forma implícita con el objetivo de identificar el nivel de tráfico y los focos de incidencias en el backbone inalámbrico de la institución.

Desde un punto de vista Social se plantea un caso de estudio con la finalidad de solventar los conocimientos de los estudiantes de pregrado en las materias relacionadas al tema de investigación en un ambiente versátil con la utilización de elementos y herramientas técnicas para la toma de muestras y luego llegar a su conceptualización; así las personas que hagan uso de este documento lograrán comprender todo lo que concierne a un escenario de comunicaciones inalámbricas con sus amenazas y vulnerabilidades.

DESARROLLO

En esta sección se establece las razones por la cual se efectúa la investigación, se destaca las premisas previas que sirven de sustento para fundamentar la ejecución del presente caso de estudio desde el punto de vista técnico, social y académico; siendo así que el objeto de investigación es la red *Wireless Fidelity (Wi-Fi)* del *Gobierno Autónomo Descentralizado Provincial de los Ríos (GADPRL).*

Para el desarrollo de esta investigación se toma como referencia que la sociedad contemporánea se basa en el uso de equipos electrónicos, internet, WiFi, redes de datos y redes celulares; todas ellas forman parte del día a día de los seres humanos como un consumidor potencial de los productos tecnológicos con medidas estadísticas relativamente altas de acuerdo a lo que indica el banco mundial en su último reporte sobre los niveles de penetración del uso tecnológico en el Ecuador, que de cada 100 habitantes 73 se encuentran cerca de una red inalámbrica y de ellos 51 hacen uso de la misma diariamente. (Mundial, Muchos móviles, poco internet, 2017).

Por ello es imprescindible contar con un equipo que tenga las cualidades y características técnicas para la generación y propagación de señales inalámbricas capaz de concatenar múltiples propósitos y que converjan las distintas disciplinas con la finalidad de dar acceso a un mundo de información en el cual prima el intercambio y transferencia de información cada vez a mayor velocidad y distancias con mayor cobertura; logrando que la distancia geográfica literalmente se acorten o en su defecto se eliminen. (Mundial, Penetración e impacto del Internet en el mundo, 2017).

Para su análisis es importante que el escenario propuesto posea los dispositivos y accesorios siendo los equipos de acceso inalámbrico de suma importancia puesto que serán los encargados de gestionar las conexiones red-usuario y pese a ello poco se sabe sobre las amenazas y vulnerabilidades, tampoco existe documentación autorizada que describa su comportamiento o explique qué procesos realiza para solventar los problemas que confronta su operatividad; el aporte práctico de la presente investigación pretende dotar de un enfoque más objetivo de las amenazas y vulnerabilidades que aquejan a las redes inalámbricas.

ESCENARIO DE INVESTIGACIÓN

El escenario propuesto son las instalaciones del *Gobierno Autónomo Descentralizado de la Provincia de Los Ríos (GADPLR)*; lugar donde se encuentra distribuida y desplegada la red *Wireless Fidelity (Wi-Fi)*, ver anexo 1.

En las inmediaciones del edificio principal del GADPLR se constata la existencia de una infraestructura basada en hormigón armado y una estructura vertebral de hierro fundido para dotar a la edificación con características sismo resistente, ver anexo 2.

Adicionalmente se observa a su alrededor un supermercado, un sector residencial, un viaducto de transporte terrestre, hoteles, discotecas y edificios con oficinas estatales; todas ellas con redes inalámbricas y un alto índice de elementos que alteran la armonía de las frecuencias de transmisión de la red WiFi del Gobierno Provincial de Los Ríos, ver anexo 3.

LA RED WIFI Y LOS FACTORES DE RIESGO

Entre las cosas más habituales en el día a día son sin duda alguna las conexiones a internet la misma que cumple la función principal de pasarela entre las acciones del ser humano y los sistemas mecanizados o electrónicos; televisión, banca, consultas, correos electrónicos, redes sociales, sistemas académicos y un sin número de servicios que se encuentra en la web o en la nube con altos niveles de prestaciones.

Todos estos factores anteriormente descritos son la principal causa para que las redes inalámbricas sean objeto de ataques, escaneo e intentos de acceso por fuerza bruta; hasta el momento se describen dos tipos de comportamientos por parte de los atacantes:

- El placer de acceder a la red inalámbrica con el fin de hurgar e ir descubriendo información confidencial o comprometedora entre las computadoras o dispositivos móviles que se encuentran directamente conectados a la red.

- La necesidad de conectarse a la red con múltiples técnicas ya sean con conocimiento de causa o empíricas solo por saciar la necesidad de tener internet de manera gratuita y acceder a los beneficios que brinda las conexiones clandestinas (WhatsApp, Facebook, Twitter, correos electrónicos, sitios webs con contenido nocivo y malicioso) este último hecho causa la intrusión de virus, adware, malware que se propagan por toda la red dejando en desventaja la seguridad del *Service Set Identifier* (SSID)

Uno de los motivos más evidente es que los sistemas o redes WiFi son el método más utilizado para conectarse a cualquier tipo de ambiente, aunque esto no implica que sea el método más seguro; en la actualidad se registran varios problemas de seguridad y vulnerabilidades debido al mejoramiento de los mecanismos de intrusión, sin embargo, los sistemas y técnica de autodefensa han mejorado de manera significativa no obstante las estadísticas de ataques siguen incrementándose (IEEE, Exploring an open WiFi detection vulnerability as a malware attack vector on iOS devices, 2015).

Recientes observaciones demuestran que los dispositivos WiFi con funciones de escaneo activo habilitado exponen información trivial para los distintos usuarios, la información toma un grado de valiosa para los que se definen como atacantes. Es decir, permite reunir la misma información de una manera más eficiente y en menos tiempo necesario sin mayor esfuerzo lo cual es la idea principal de todo atacante. (Oljasz, 2015).

Claramente, la idea de diseñar un método automatizado (dispositivo o mecanismo) que utilizara la vulnerabilidad del escaneo activo (solicitudes de sonda) y la conexión automática para abrir puntos de acceso WiFi desde dispositivos con capacidad WiFi se precede como uno de los delitos más comunes y utilizados en la mayoría de agresiones perpetradas; (Cormac Callanan, The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013) , 2015).

Obviamente, al utilizar un dispositivo que pueda detectar y sondear el espectro y posteriormente crear automáticamente SSID falsificados se puede captar el "tamaño de

esta vulnerabilidad al escanear un mayor número de dispositivos en un período de tiempo más reducido. (Sidiropoulos, 2014).

En el GADPLR se ha detectado el uso de múltiples dispositivos móviles y un nivel de saturación de los canales de comunicación ligeramente aceptables, entre las aplicaciones detectadas se encuentran "UltraSurf, Wireshark, uTorrent y accesos directos a redes sociales y video juegos".

Estas aplicaciones en el caso de UltraSurf se constata que hace un salto a las políticas de seguridad establecidas por el administrador de red con el afán de acceder a sitios y herramientas de uso totalmente restringidos; para este efecto lo que produce es la apertura de puertos varios puertos de comunicación por fuerza bruta ocasionando la intrusión de adware's y malware's, siendo este evento un foco de contaminación e infección en la red inalámbrica y luego propagándose hacia la red cableada (Cormac Callanan, EMPIRICAL ASSESSMENT OF DATA PROTECTION AND CIRCUMVENTION TOOLS AVAILABILITY IN MOBILE NETWORKS, 2016).

ASOCIACIÓN DE CLIENTES Y PUNTOS DE ACCESO

Una parte clave del proceso fomentado y regulado por el estandar IEEE 802.11 es en primera instancia realizar un descubrimiento de cualquier tipo de *Wireless Local Área Network (WLAN)* y posteriormente negociación de credenciales y permisos para conectarse a ella. (IEEE, Wireless hacking - a WiFi hack by cracking WEP, 2015)

Este proceso comienza con la red WLAN que envía cuadros llamados “Beacons” o “Balizas” con el propósito de publicitar su presencia en el radio espectro antes de ser revelado su *Service Set Identifier (SSID)*. Después de eso, el cliente móvil envía marcos de solicitud de sondeo:

- Identificar (explorar / buscar).
- Conectarse a su WLAN.
- La autenticación y la asociación como pasos finales.

Estos pasos que son propios del algoritmo de asociación se cumplen de manera estricta en todo proceso abierto de la asociación entre el router y los clientes móviles; teniendo en cuenta a través de un escáner de actividades se puede acceder y descubrir las claves de acceso de la red inalámbrica a base de la instalación de un *sniffer* (Es un programa informático que registra la información que envían los periféricos en la red y de esta forma produce un análisis de paquetes con lo cual se logra describir todo tipo de información transmitida en la red), ver anexo 4.

SOLAPAMIENTO DE CANALES EN LA RED WIFI DEL GADPLR

Uno de los problemas más comunes con las redes *wireless fidelity (WiFi)* es el solapamiento de canales debido a la enorme cantidad de equipos que funcionan en la banda de frecuencia de 2,4 GHz. Cada dispositivo *WiFi* que cumple con el estándar 802.11 a/b/g/n/ac, utilizan uno de los 13 canales establecidos y de igual forma 2 o más equipos cercanos utilizan el mismo canal, produciendo de esta forma el solapamiento. Generalmente

cada canal ocupa un ancho de banda de 22 MHz. Uno de los efectos del solapamiento es la reducción y lentitud en el rendimiento de la velocidad de la red afectada. Ver figura 1.

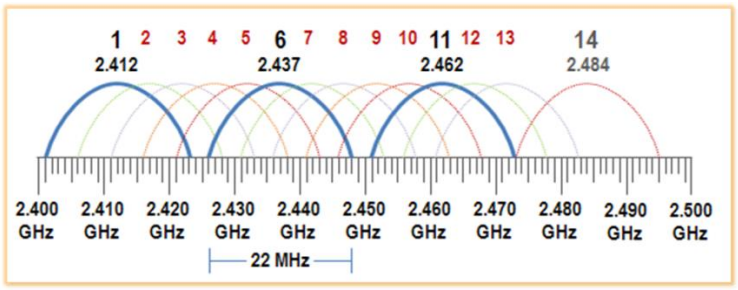


Figura 1 *Recomendación para evitar un solapamiento de canal en la red inalámbrica del GADPLR.*

Autora: *Tatiana Bajaña*

Para evitar los efectos del solapamiento de canales en las redes WiFi, lo ideal es que una red esté separada de la otra en 5 canales, un ejemplo de ello es lo siguiente:

- Si una red utiliza el canal 1, la siguiente debería utilizar el 6. De esta forma, no se produce solapamiento alguno.

- En el caso de no poder utilizar un canal separado a una distancia de 5 canales, lo ideal es utilizar el canal más alejado de la señal más débil.

En el siguiente gráfico se visualiza el ancho de banda utilizado por cada canal y el solapamiento que se produce entre ellos. Ver figura 2.

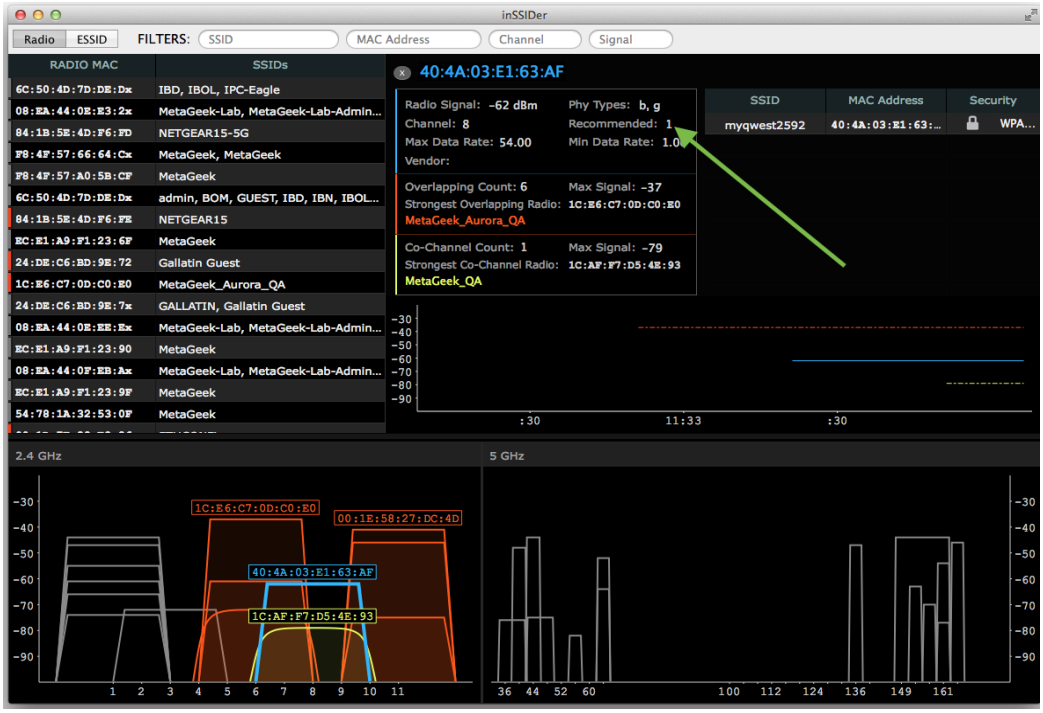


Figura 2 *Análisis y detección de solapamiento de canales en la red WiFi del GADPLR a través del analizador de espectro inSSIDer.*

Autora: *Tatiana Bajaña.*

Como se puede observar en el gráfico anterior las frecuencias van desde los 2,412 GHz hasta los 2,472 GHz quedando un espacio relativamente pequeño para colocar 13 canales de 22 MHz cada uno cuando el espacio total es de 60MHz; por esta razón se produce el solapamiento entre la red WiFi del GADPLR y las redes adyacentes con un alto índice de atenuación en horas pico por la afectación del espacio radioeléctrico a causa del ruido y la interferencia externa al edificio.

PRUEBAS DE ASOCIACIÓN, ESCANEO, VULNERABILIDAD, MÉTODOS Y SUPLANTACIÓN.

Hay dos formas para que un cliente móvil explore los *Access Point (AP)* disponibles:

- Escaneo activo.
- Escaneo pasivo, ver anexo 5.

Durante el escaneo activo, el cliente sintoniza su radio detector *Institute of Electrical and Electronics Engineers (IEEE 802.11);* dependiendo del canal en el que se esté escaneando y transmitiendo una solicitud de sonda a fin de obtener respuesta de cualquier AP disponible en el canal especificado con un SSID que logre coincidir en el proceso de match (definir congruencias y similitudes que permitan una asociación transparente a base de coincidencias), en las pruebas realizadas se toma un tiempo máximo de 10 ms. Para ello fue necesario ejecutar pruebas de sondas dirigidas y sondas de difusión.

Sonda dirigida: el cliente envía una solicitud de sonda SSID específica del nombre donde solo el AP (s) que tiene el SSID solicitado debe responder a esta solicitud con una respuesta de sondeo, ver anexo 5. (Serres, 2014).

En la prueba de sonda de difusión el cliente envía una solicitud de sonda de difusión con un SSID nulo en el que todos los puntos de acceso que la reciben responden con una respuesta de sonda para cada uno de los SSID que admiten, ver anexo 5. (Muauricio, 2016).

Durante las pruebas realizadas en las inmediaciones del GADPLR se evidencia una fuerte incidencia y nivel de saturación en el tráfico multimedia de la red WiFi, para el efecto se hace las pruebas de rigor para detección de los intentos de intrusión. Se implementa un mapa de calor con el objetivo de identificar el nivel de uso, los puntos calientes y puntos fríos de la red; para obtener estos resultados se emplea la herramienta NetSpot (Herramienta que

permite visualizar, administrar, solucionar problemas, auditar, planificar e implementar redes inalámbricas.) ver figura 3 y 4.

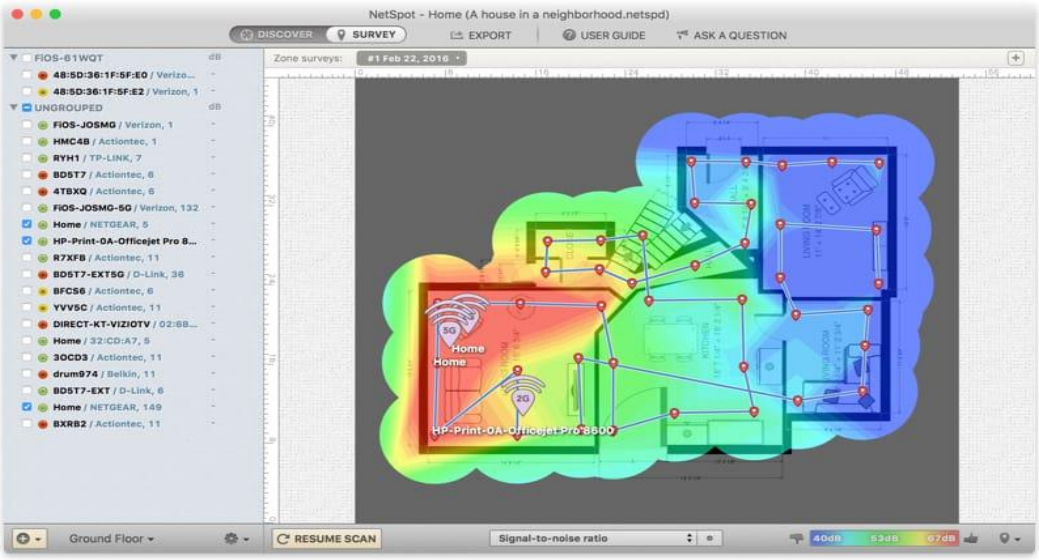


Figura 3 *Auditoría a la red WiFi del GADPLR con la herramienta NetSpot, se visualiza las incidencias y los niveles de gestión en cada dispositivo WiFi conectado a la red.*
Autora: *Tatiana Bajaña*

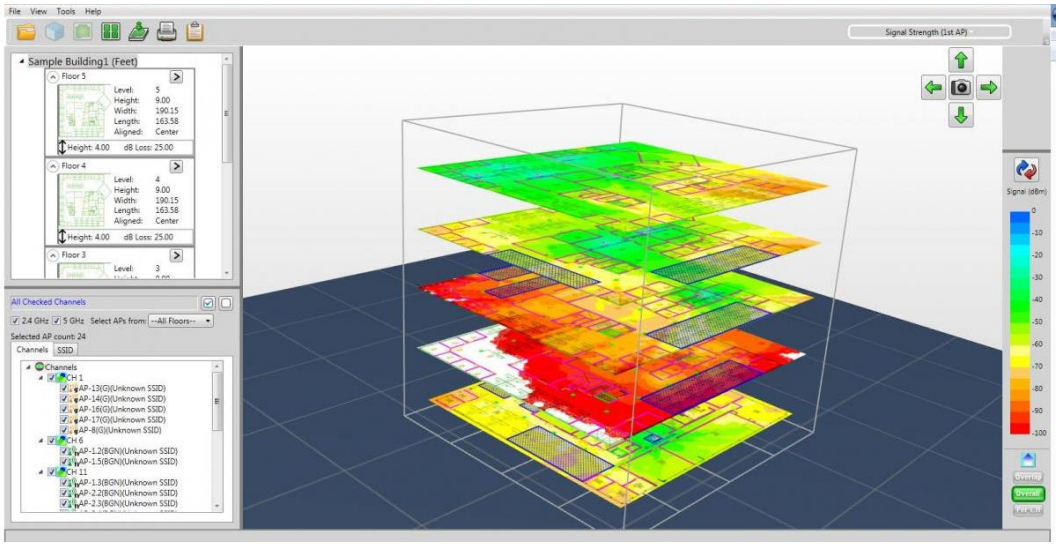


Figura 4 *Modelamiento en 3D del edificio del GADPLR con la herramienta NetSpot y la definición de mapas de calor en todos los niveles, se evidencia los puntos fríos y calientes de la red inalámbrica.*
Autora: *Tatiana Bajaña*

En la suplantación de identidad se utiliza mucho el concepto del punto de acceso dinámico, esto se refiere a automatizar el proceso de recopilación de datos para el SSID y la dirección MAC del equipo al que se desea atacar, el siguiente paso es automatizar el proceso de suplantación de identidad de esos SSID para descubrir cuál de ellos podría permitir acceso sin dificultad. (Yang L, 2014).

Si un dispositivo realiza la conexión, se puede concluir que el SSID específico está abierto y que la configuración realmente funciona, sin embargo, para automatizar el principio de falsificación se prepara un hardware con software personalizado para lograr esto. Esta pieza de hardware se llama Punto de Acceso Dinámico (DAP). Es responsable de ajustar el proceso de suplantación de acuerdo con su entrada. (IEEE, WiFi can be the weakest link of round trip network latency in the wild, 2016).

La entrada por sonda de difusión puede ser información definida y / o capturada por el usuario desde la interfaz inalámbrica. El DAP creado en esta investigación puede operar en dos modos de ataque: modo general y modo directo. En el modo general, todas las solicitudes de sondas se recopilan y se utilizan para configurar los SSID falsificados. En el modo directo, solo las solicitudes de sondeo se utilizan desde una dirección *Media Access Control (MAC)* específica en el edificio. (ETSI, 2014).

En esta investigación, se utiliza un enrutador TP-LINK con OpenWRT como su sistema de operación. Hay dos dispositivos utilizados para cada parte del proceso. La primera parte es la recopilación de información donde el dispositivo escucha el tráfico inalámbrico y lo filtra, en consecuencia. Se escribe línea de código para realizar este paso. La interfaz

inalámbrica se configura en modo monitor para que todos los paquetes se capturen. (IEEE, Physical Interference Modeling for Transmission Scheduling on Commodity WiFi Hardware, 2015).

Entonces todos los paquetes se filtran excepto las Solicitudes de Sonda. A partir de estas Solicitudes de Sonda, se genera una lista con SSID únicos. Los primeros siete se usan para spoofing. Si el sistema está en modo directo, los SSID solo se usan desde una dirección MAC definida por el usuario. (Pariente, 2016).

La segunda parte de la configuración también es un enrutador TP-LINK con OpenWRT. Este enrutador está configurado para actuar como un punto de acceso mediante el uso de *Host Access Point Daemon (hostapd)* como servicio. Hostapd es un proceso de espacio de usuario que maneja los clientes conectados al punto de acceso. El enrutador puede distribuir a los clientes una dirección IP mediante el uso de DHCP y proporciona acceso a Internet. Cuando el primer enrutador tiene suficientes SSIDs recopilados, genera un archivo de configuración en un formato que el servicio hostapd entiende. Envía el archivo a través de ssh, utilizando el comando scp, al segundo enrutador y vuelve a cargar el servicio. Después de volver a cargar, el segundo enrutador actúa como punto de acceso para los SSID provistos. Ver figura 5. (Ulices, 2016).

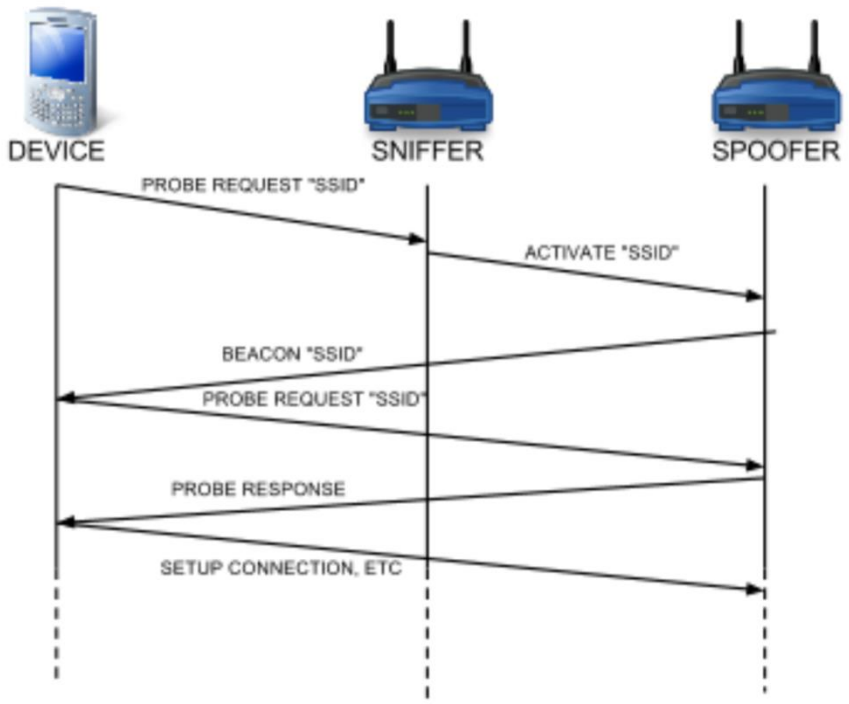


Figura 5 *Escenario de Suplantación de identidad en la red WiFi del GADPLR, técnicas de ataque y analizador de tráfico.*

Autora: *Tatiana Bajaña.*

RECOPILACIÓN DE DATOS Y DISCUSIÓN DE RESULTADOS.

Esta parte de la investigación trata sobre la recopilación de datos de todos los tipos de pruebas e inclusiones realizadas a la red WiFi del GADPLR, la configuración que se utilizó para este proceso se basa en dos aspectos:

- Software: Se utilizó un sistema operativo con el nombre de OpenWRT basado en Linux, analizadores de tráficos con el nombre de NetSpot, ssINSIDer, un sniffer o analizador de paquetes con el nombre de Wireshark.

- Hardware: Se utilizó varios router’s en la marca TP-LINK, un computador portátil marca Apple modelo MacBook Pro Retina de 15”, dos computadoras portátiles marca *Hewlett-Packard (HP),* la infraestructura de red WiFi del GADPLR.

Con relación a las configuraciones realizadas, se procedió a configurar un enrutador como un equipo adicional en la red inalámbrica y operado a su vez desde un computador portátil MacBook Pro y desde ese equipo se procedió a dar permisos y operatividad a los demás router para las distintas pruebas realizadas.

Los datos recopilados se basan en tres fases; la primera es por medio del uso de un sniffer, la segunda es a través de las identificaciones de los dispositivos por su dirección MAC y la tercera por acceso de intrusión con la ayuda de codificación y texto malicioso inyectado en la red. (Basalamah, 2016).

Al utilizar el *sniffer* se pudo obtener los datos de transmisión entre los distintos dispositivos, clientes móviles, computadores portátiles y terminales cableadas, esto es posible mediante el empleo de *Tcpdump*, la misma que es una herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red.

Para el segundo método se logra la identificación de los equipos una vez realizado el escaneo de toda la red, esto fue posible mediante la incorporación de un router en la red WiFi del objeto de estudio, fue necesario implementar un servidor DHCP para obtener los datos

adicionales de los clientes y posteriormente se los transfirió a un servidor web cautivo para obtener un login.

Para el caso de inyectar código fuente en la red es necesario crear un código que sea capaz de obtener el SSID, la MAC y demás detalles que sean necesarios para la finalidad de la investigación en términos generales, ver tabla 1 y 2.

```
SELECT ssid , count(∗) AS count FROM (
SELECT ssid.mac, ssid.ssid FROM ssid  WHERE ssid.ssid != "" GROUPBY ssid.mac
) AS P  GROUPBY ssid ORDERBY count DESC
```

Tabla 1 *Código SQL ejecutado en la red WiFi del GADPLR a través de spoofing y sniffer.*
Autora: *Tatiana Bajaña.*

SSID	Usuarios
Consejo	32
Prefectura	17
Tic	5
Aki	13
SanaSana	6
Hotel	21
Miduvi	14
Flores	18
Cachari	2
Hotel2	6

Tabla 2 *Resultados obtenidos de la ejecución del código fuente.*
Autora: *Tatiana Bajaña.*

CONCLUSIÓN

Se concluye que la fiabilidad de la red WiFi de GADPLR es débil debido a que no posee las políticas adecuadas para una correcta protección de los datos así; se evidencia que no hay mecanismos que detecten y ejecuten un protocolo de autodefensa previo a intentos de intrusión o ataques de negación de servicios.

Este hecho deja entrever que los niveles de vulnerabilidad de la red WiFi objeto de investigación es alta, adicionalmente se evidencia la existencia de múltiples redes inalámbricas en el interior como exterior del edificio lo cual provoca un solapamiento de canales en todos los dispositivos de acceso inalámbrico dando paso a la atenuación de la señal de transmisión y por ende se comprueba que la saturación es mayor al ancho de banda registrado en cada equipo en la capa de acceso y distribución de la red del edificio.

La principal amenaza de la red WiFi es el ruido exterior ya que este se encuentra en una frecuencia mayor a la que está transmitiendo el equipo local, se registran pérdidas de paquetes y latencia en el piso 3, 2, 1 y planta baja; otro hecho anómalo es cuando los router dejan sin tiempo de respuesta a los clientes móviles a causa de un enlace entre ellos y logran ocupar todos sus canales por la interferencia en el espectro, causando una caída de la red la cual es solucionada cuando se reinicia o se desconecta de la toma eléctrica al router para que se reinicie los servicios.

BIBLIOGRAFÍA

Mundial, B. (2017). *Penetración e impacto del Internet en el mundo.* New York: Banco Mundial.

Mundial, B. (2017). *Muchos móviles, poco internet.* New York: Banco Mundial.

IEEE. (2015). Exploring an open WiFi detection vulnerability as a malware attack vector on iOS devices.

Sidiropoulos, N. (2014). Open Wifi SSID Broadcast vulnerability. *SSN Project Assessment*.

Oljasz, P. l. (2015). Open Wifi SSID Broadcast.

Cormac Callanan, B. J.-B.-Z. (2016). EMPIRICAL ASSESSMENT OF DATA PROTECTION AND CIRCUMVENTION TOOLS AVAILABILITY IN MOBILE NETWORKS.

Cormac Callanan, B. J.-B.-Z. (2015). The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013) .

IEEE. (2015). Wireless hacking - a WiFi hack by cracking WEP.

Serres, O. d. (2014). Procedimiento y dispositivo de gestión de acceso a una red WiFi comunitaria. *Patente Europea*, 979.

Muauricio, O. (2016). CÓMO ELEGIR EL MEJOR CANAL PARA CONFIGURAR TU RED WIFI. 318.

IEEE. (2016). WiFi can be the weakest link of round trip network latency in the wild.

Ulises, P. M. (2016). Encaminador para redes TCP/IP con interfaces Ethernet y WIFI basado en Linux Kubuntu 10.04 LTS.

Ulices, P. M. (2016). Encaminador para redes TCP/IP con interfaces Ethernet y WIFI basado en Linux Kubuntu 10.04 LTS.

Pariente, G. P. (2016). Cloudlet- and NFV-based carrier Wi-Fi architecture for a wider range of services.

ETSI. (2014). Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges & Call for Action", White paper, SDN and OpenFlow World Congress. *ETSI*.

Yang L, Z. P. (2014). Architecture taxonomy for control and provisioning of wireless access points . *CAPWAP*.

IEEE. (2015). Physical Interference Modeling for Transmission Scheduling on Commodity WiFi Hardware.

Basalamah, A. (2016). Crowd Mobility Analysis using WiFi Sniffers .

ANEXOS

Anexo 1 (Escenario de investigación).

Gráfico 1 *Edificio del GADPLR*

Autora: *Tatiana Bajaña.*

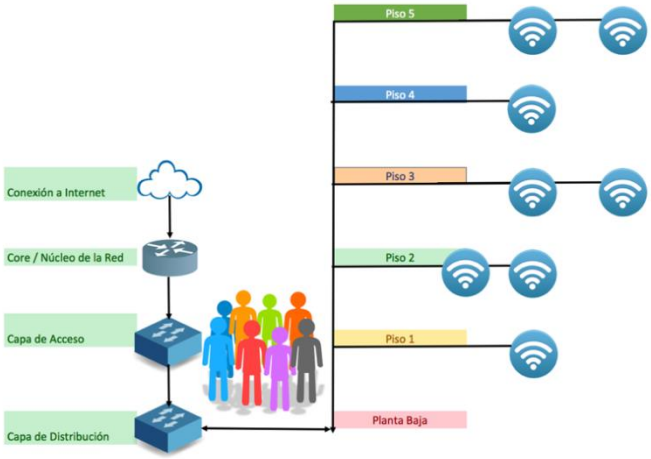


Gráfico 2 *Infraestructura de red y red WiFi del GADPLR*

Autora: *Tatiana Bajaña.*

Anexo 2 (Estructura de edificio sismo resistente).

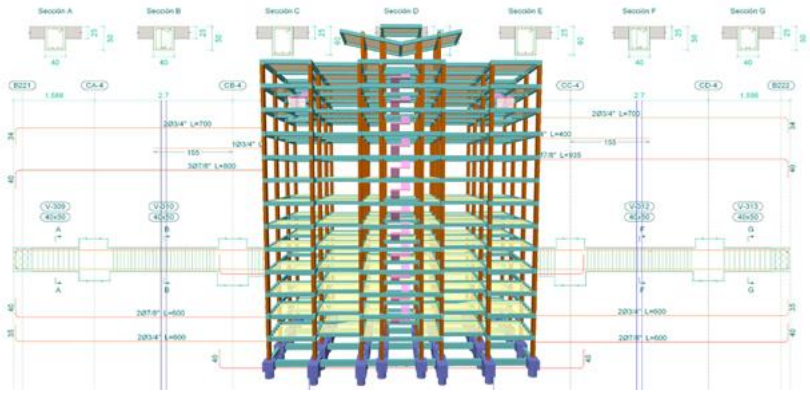


Gráfico 3 *Modelamiento estructural del edifico del GPRL donde se despliega la red WiFi objeto de estudio.*

Autora: *Tatiana Bajaña*.

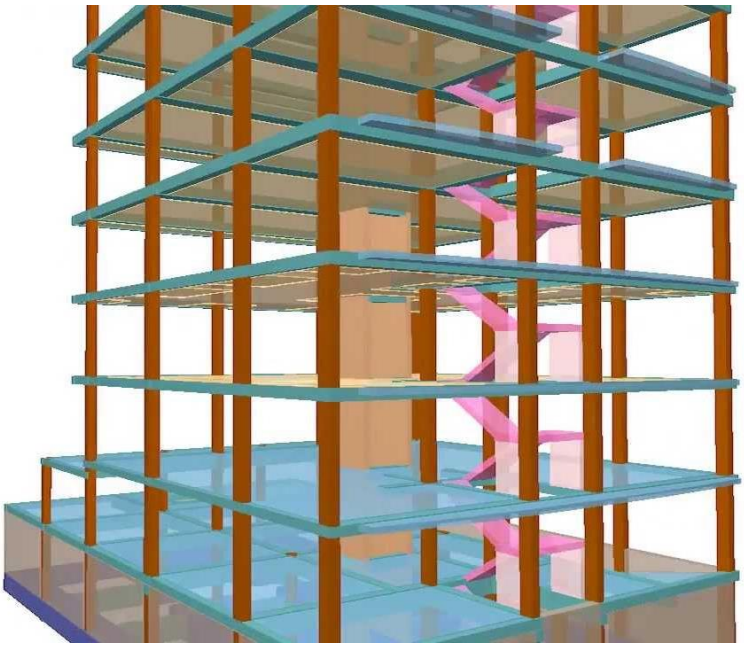
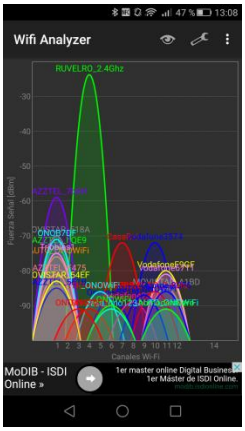


Gráfico 4 *Modelamiento en 3D de los niveles y estructura vertical del edifico del GPRL donde se despliega la red WiFi objeto de estudio*

Autora: *Tatiana Bajaña.*

Anexo 3 (Estructura e inmediaciones del edificio).

IMAGEN	DESCRIPCIÓN
	• Estructura en Hormigón armado y hierro fundido como base para edificación sismo resistente.
	• Inmediaciones exteriores del GADPLR, se verifica la presencia de hoteles, cadenas de farmacias, supermercado, discoteca y un viaducto vehicular que conecta el casco urbano con las parroquias urbanas El Salto y Barreiro.
	• Se evidencia un alto contenido de ruido externo a causa de la interconexión entre dos avenidas y un puente vehicular interprovincial.

	• Se evidencia un alto contenido de interferencia entre las redes inalámbricas adyacentes, dejando al descubierto un grave problema relacionado con el solapamiento de canal.

Índice 1 Estructura e inmediaciones del GADPLR.

Autora: *Tatiana Bajaña.*

Anexo 4 (Asociación de clientes y punto de acceso).

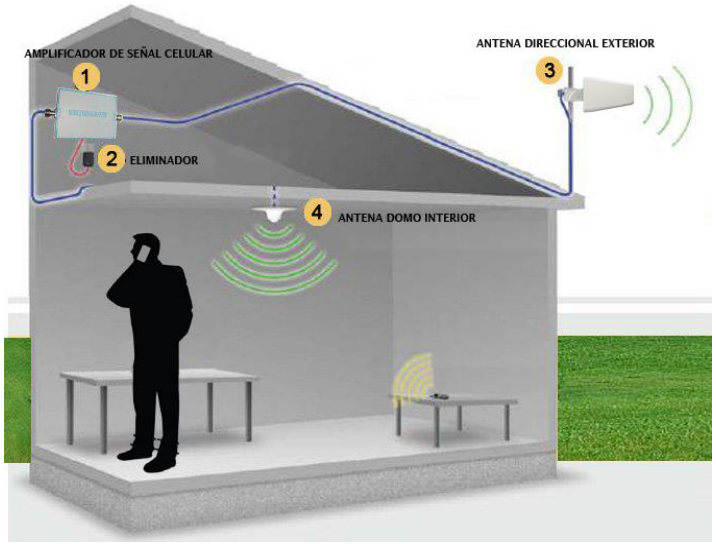


Gráfico 5 *Asociación de Clientes móviles y puntos de acceso, aprovisionamiento de cobertura WiFi y propagación de Señal WLAN.*

Autora: *Tatiana Bajaña.*

Anexo 5 (Pruebas de asociación, escaneo, vulnerabilidad, métodos y suplantación).

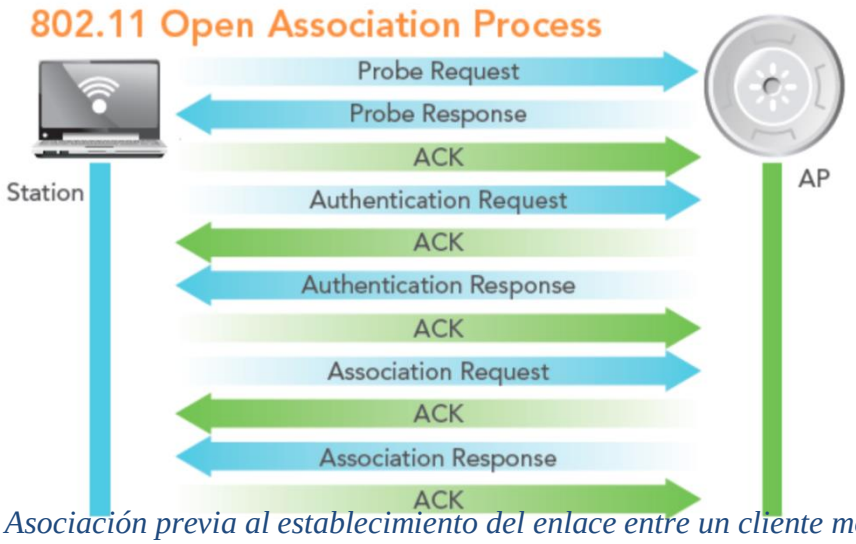
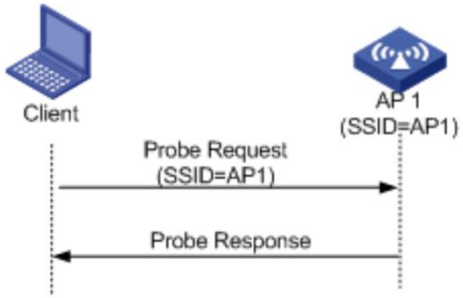
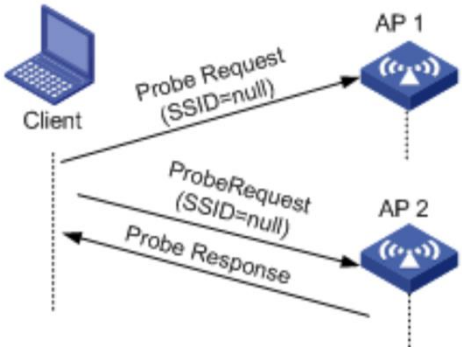


Gráfico 6 *Asociación previa al establecimiento del enlace entre un cliente móvil y un AP.*

IMAGEN	DESCRIPCIÓN
	• Escenario de prueba para sonda dirigida.
	• Escenario de prueba para sonda de difusión.

Índice 2 *Pruebas realizadas para el proceso de Match con sondas de testeo en el radioespectro.*

Autora: *Tatiana Bajaña.*

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS