Revista Científica Mundo de la Investigación y el Conocimiento

Freddy Bravo-Duarte [a]; Silvia Pacheco Mendoza [b]; Ruth Peña-Holguín [c]

Análisis de Seguridad de Redes Inalámbricas a través del modelado Matemático Susceptible-Infectado-Recuperado (SIR)

Security analysis of wireless networks through mathematical modeling Susceptible-Infected-Retrieved

Revista Científica Mundo de la Investigación y el Conocimiento. Vol. 2 núm.3, julio, ISSN: 2588-073X, 2018, pp. 658-682

DOI: 10.26820/recimundo/2.(3).julio.2018.658-682

Editorial Saberes del Conocimiento

Recibido: 05/04/2018 Aceptado: 15/02/2018 Publicado: 30/07/2018

Correspondencia: fbravod@unemi.edu.ec

a. Magister en Gerencia de Tecnologías. Universidad Estatal de Milagro, email fbravod@unemi.edu.ec
b. Doctora en Educación, Magister en Educación Superior, Especialista en Gestión de Procesos Educativos, Diplomado Superior en currículo por competencias, Licenciada en Ciencias de la Educación: Especialización en Informática, Profesora en Educación Primaria Bachiller en ciencias de la Educación. 17 años de experiencia en docencia universitaria y educación primaria. Profesora de posgrado, Tutora de proyectos de investigación en grado y posgrado. Desarrollo de proyectos de investigación con financiamiento. Universidad Estatal de Milagro spachecom@unemi.edu.ec
c. Ingeniera en Sistemas Computacionales, Estudiante de Master Universitario en Tecnología Educativa y Competencias Digitales - UNIR. Analista de Publicaciones en el Departamento de Investigación - UNEMI, email rpenah1@unemi.edu.ec

RESUMEN

Esta investigación tiene como objetivo analizar e identificar las posibilidades de un ataque masivo a las redes inalámbricas de negocios y hogares ubicados geográficamente en diferentes sectores de la ciudad de San Francisco de Milagro, basados en una muestra aleatoria. Este estudio permitirá obtener un control de la mayor cantidad de puntos de acceso y así robar información, o incluso controlarlos para realizar ataques dirigidos de denegación de servicio distribuido (DDoS). La hipótesis planteada para el estudio realizado consistió en la existencia de una alta probabilidad de llegar a infectar los firmwares de los puntos de acceso mediante la obtención de credenciales aprovechando las vulnerabilidades conocidas de WEP y de WPS. En esta investigación se utiliza un enfoque epidemiológico para investigar la propagación de la infección de puntos de acceso, el tipo de investigación aplicada es cuantitativa, permitiendo determinar el número de puntos de acceso inalámbricos posibles a vulnerar de un grupo que cumple con ciertas características, se utilizó un grafo para determinar la probabilidad de infección y se usó un método de simulación de tiempo para encontrar la cantidad de equipos infectados según el tiempo y frecuencia que utilicemos para los ataques de obtención de credenciales. Como resultado de la investigación realizada se demostró la facilidad con la cual se pueden dar los ataques a este tipo de redes, lo cual representan una amenaza a la seguridad de los usuarios; la evidencia de esta problemática demanda la búsqueda de medidas para mejorar la gestión de los puntos de acceso entre las cuales está la capacitación a sus usuarios. Por último se realizaron algunas conclusiones que mejoraran el nivel de seguridad, aplicando buenas prácticas al nivel de configuración y uso de las redes.

Palabras clave: Redes inalámbricas, seguridad, vulnerabilidades, simulación.

ABSTRACT

The objective of this research is to analyze and identify the possibilities of a massive attack on the wireless networks of businesses and households located geographically in different sectors of the city of San Francisco of Milagro, based on a random sample. This study will make it possible to obtain control over the largest number of access points and thus steal information, or even control them to carry out targeted denial of service (DDoS) attacks. The hypothesis proposed for the study consisted in the existence of a high probability of infecting the access point firmwares by obtaining credentials taking advantage of known WEP and WPS vulnerabilities. This research uses an epidemiological approach to investigate the spread of infection of access points, the type of research applied is quantitative, allowing to determine the number of possible wireless access points to violate a group that meets certain characteristics, used a graph to determine the probability of infection and a time simulation method was used to find the number of computers infected according to the time and frequency that we use for credentialing attacks. As a result of the research carried out, it was demonstrated the ease with which attacks to this type of networks can occur, which represent a threat to the security of the users; the evidence of this problem demands the search of measures to improve the management of the access points among which is the training to its users. Finally, some conclusions were made to improve the level of security, applying good practices at the level of configuration and use of the networks.

Keywords: Wireless networks, security, vulnerabilities, simulation.

Introducción.

Las redes inalámbricas permiten la interconexión entre dos o más puntos, esto se da por medio de ondas electromagnéticas que viajan a través del espacio permitiendo compartir información de un lugar a otro. Para que el intercambio de información exista, se han creado diferentes mecanismos de protocolos, los cuales establecen reglas que permiten que el flujo de información sea confiable entre los puntos interconectados (Lilian & Pietrosemoli, 2007).

El presente trabajo de investigación, tuvo la finalidad de identificar la vulnerabilidad de las redes inalámbricas simulando una infección, para esto partimos de un estudio de simulación de propagación de malware (Sabater, Martín, Rey, & Rodríguez Sánchez, 2014), y un estudio experimental en la difusión de infecciones inalámbricas utilizando fallas WPS (Sanatinia, Narain, & Noubir, 2013), se conoce que el algortimo WPA2 es capaz de ser vulnerado mediante un ataque de reinstalación de llaves KRACK (Vanhoef & Piessens, 2017), pero este ataque no está destinado a capturar la clave sino a hacer un espionaje de todo aquello que se transmita en la conexión a la que se ataca, por tal motivo no lo consideramos como vulnerabilidad para nuestro estudio.

En los últimos años se han desarrollaron diversos estándares de seguridad para las redes inalámbricas, a pesar de aquellos en la práctica nos encontramos con variables ajenas como limitantes en el hardware, configuraciones no adecuadas, software desactualizado y el desconocimiento de los usuarios sobre problemáticas (Monsalve Pulido, Aponte Novoa, & Chaparro Becerra, 2015).

Consideramos la posibilidad de la modificación del firmware de los punto de acceso inalámbricos, existe un proyecto para la creación de firmware de puntos de acceso denominado

LEDE, basado en OpenWrt el cual ofrece soporte para la modificación de firmware de distintos dispositivos, como es software libre, es posible realizar modificaciones en su código para insertar malware que permita, por ejemplo, instalar software de minado de criptomonedas (Cimpanu, 2018).

En la actualidad, Ecuador ha experimentado un gran crecimiento en el consumo de Internet, muchos proveedores en la cuidad de Milagro ofrecen el servicio y, en la mayoría de casas, se configura el acceso mediante red inalámbrica. Es importante recalcar que ningún sistema es seguro al 100% y las conexiones inalámbricas el riesgo de ser vulneradas incrementa.

Las redes configuradas en las casas están dentro de la norma 802.11, la cual es de las más populares debido al bajo costo de los equipos necesarios para su implementación, denominados Acces Point (AP) y al hecho de que casi la totalidad de dispositivos de comunicación móviles, smartphones, smartwatchs, etc, poseen acceso wifi.

El uso de internet en el área urbana de la República del Ecuador tiene un crecimiento sostenido, y de acuerdo a datos proporcionados por el Instituto Nacional de Estadística y Censos en el 2012 un 31.4% del familias del área urbana tienen acceso a internet, este porcentaje incrementó para el 2016 llegando al 44.6% (INEC, 2014).

El contar con este recurso ha permitido el cambio de hábitos en el entretenimiento de la población, influyendo cada vez más en la adquisición dispositivos móviles que cuenten con acceso a internet, según datos del INEC al 2016 el 90.1% de los hogares contaba con telefonía celular (INEC, 2014), el incremento de adquisición de tecnología favorece a la población. Sin embargo el tener acceso a redes poco seguras, atentan contra la privacidad de los usuarios y en

muchos de los casos debido a la falta de información de la población con respecto a las formas de asegurar sus puntos de acceso inalámbrico.

Existen estudios que buscan aplicar metodologías para aplicar una seguridad avanzada en la redes inalámbricas (Sánchez Espinosa, Vivero García, & Llanos, 2018), además se estudian técnicas de penetración de redes inalámbricas utilizando la vulnerabilidades que poseen los elementos WPS en los puntos de acceso (Aked, Bolan, & Brand, 2012).

Marco teórico

Para el propósito del análisis que se realizó, se utilizaron diferentes herramientas para proceder a la captura de datos de las distintas redes wifi ubicadas en la ciudad de San Francisco de Milagro, provincia del Guayas.

Redes inalámbricas

La comunicación inalámbrica, es aquella que prescinde de cualquier cable entre el emisor y el receptor, resulta necesaria para aquellos usuarios móviles que tienen que estar continuamente conectados. También es de mucha utilidad cuando resulta muy costoso tender hilos de comunicación en zonas geográficas de difícil acceso.

Redes IEEE 802.11

Las redes 802.11 especifican el uso de los niveles inferiores del modelo de interconexión de sistemas abiertos OSI, esto es la capa física y la de enlace de datos, en Ecuador se usan 11

canales, mientras que, en otros países, Japón, por ejemplo, estos llegan hasta el canal 14 en la banda de los 2.4 GHz (International, 2005).

Debido a esta limitación, es común encontrar varios puntos de acceso emitiendo señal en el mismo canal, sin embargos los canales 1, 6 y 11 suelen ser los más utilizados, debido a que, por su separación, no provocan solapamiento (Castignani, Loiseau, Montavont, & An, 2011) .

Función de Distribución Acumulada

Una función de distribución acumulada (fda) describe la probabilidad de que una variable aleatoria real sujeta a cierta ley de probabilidad se sitúe en zonas de valores menores o iguales a cierto valor x.

Esta función está definida por la función.

$$F(x) = P(X \leq x) = \int_{-\infty}^{x} f(s)ds$$

Una función de nombre “F”, le asigna a cada valor real x, el de la probabilidad de que una variable aleatoria X asuma un valor inferior o igual a x.

Punto de acceso inalámbrico

Un punto de acceso inalámbrico, Access Point en inglés, abreviado AP, es un dispositivo de red que interconecta equipos de comunicación inalámbrica, dispositivos móviles o equipos de comunicación alámbrica con dispositivos inalámbricos incorporados.

Herramientas utilizadas

La captura de datos se la realizó usando un dispositivo Huawey NXT-L09 y el aplicativo Wigle Wifi.

Este dispositivo es capaz de capturar información en la banda de los 2.4 GHz y los 5GHz, pero se analizó la banda de 2.4 GHz debido a que es la banda más utilizada en el despliegue de redes inalámbricas caseras.

Wigle Wifi

Esta aplicación permite encontrar redes inalámbricas, las añade a una base de datos y permite marcar puntos capturados previamente.

Esta herramienta muestra las señales inalámbricas capturadas, la hora de la captura, la ubicación obtenida por GPS, la seguridad de la señal, su potencia y demás datos que emite el punto de acceso. Es posible, luego de la captura de datos, exportar los mismos a formatos CSV con las características de cada punto de acceso, así como exportar los datos a un formato KML para su representación en mapas como google maps.

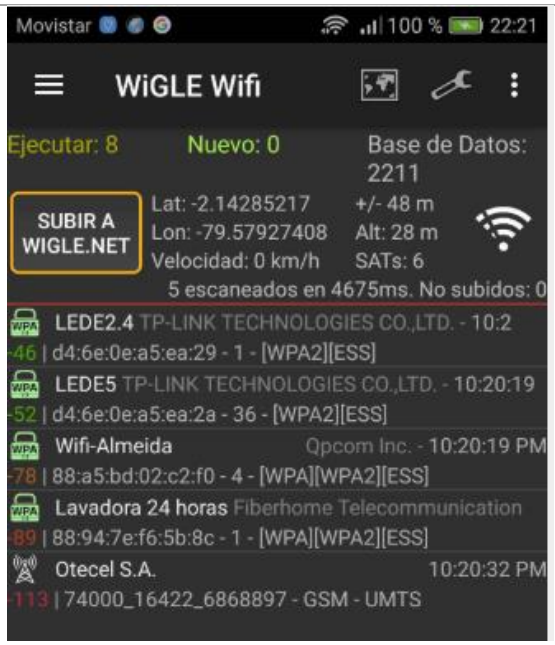

Figura 1 Herramienta Wigle Wifi

Desarrollo

Levantamiento Topológico

Con la finalidad de revisar el despliegue de redes inalámbricas en la cuidad de Milagro, se realizó un escaneo de redes inalámbricas mediante el uso de wardriving, esto es, realizar un recorrido por las calles céntricas de Milagro haciendo uso de un dispositivo móvil, el cual se encarga de receptar y almacenar todos los puntos de acceso reconocidos por el dispositivo cerca de la posición en la que se ubique.

La aplicación se denomina Wigle Wifi, la misma que permite la exportación de datos en formato CSV, el mismo que es de fácil uso para poder exportarlo a Excel.

En este estudio se realizó una investigación de alcance exploratorio, descriptivo y además documental, que, para Hernández S, Fernández C, & Batista L (2014), se aplica en problemas poco estudiados, se indagan desde una perspectiva innovadora, ayudan a identificar conceptos promisorios y se preparan el terreno para nuevos estudios.

Con este antecedente el análisis de estos datos han sido analizados para obtener un conjunto de resultados para su posterior investigación y realizar una representación gráfica de los principales aspectos importantes que han surgido de esta captura de datos.

El recorrido fue realizado en un automóvil a una velocidad de entre 20 y 30 Km/h, haciendo un recorrido 2 veces por estas vías, entre el 3 de mayo y el 30 de mayo del 2018, esto para obtener la mayor precisión en la toma de datos.

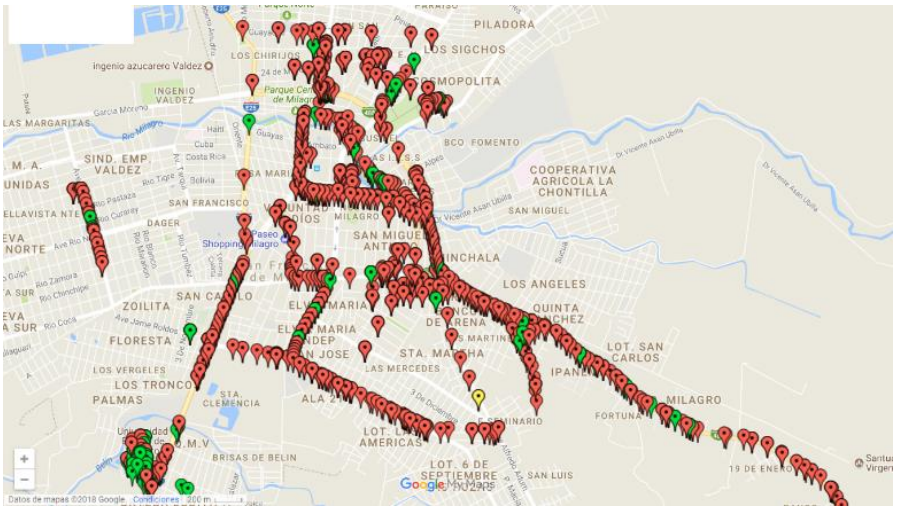

Figura 2 Mapa de puntos de acceso capturados

La figura 2 muestra los puntos de acceso capturado durante el recorrido que se realizó en el proceso de wardriving, para esto se usó la herramienta Wigle Wifi (Madrid Molina, 2006).

Se usó el filtrado por dirección MAC, para obtener puntos de acceso únicos y así evitar duplicados, pues se hizo el recorrido 2 veces.

La potencia con la que se recibía la señal de los puntos de acceso era variable, en la tabla 1 se observa el promedio de la potencia de las señales obtenidas.

Tabla 1 Potencia de señal obtenida de puntos de acceso capturados

Rangos de potencias	Porcentaje de equipos detectados
Mayor que 90 dBm	49.34%
Entre 80 y 90 dBm	49.51%
Menor que 70 dBm	1.14%

Fuente: Elaboración propia.

Los datos obtenidos mostraron distintos protocolos de seguridad, entre señales abiertas, encriptación WEP, WPA2.

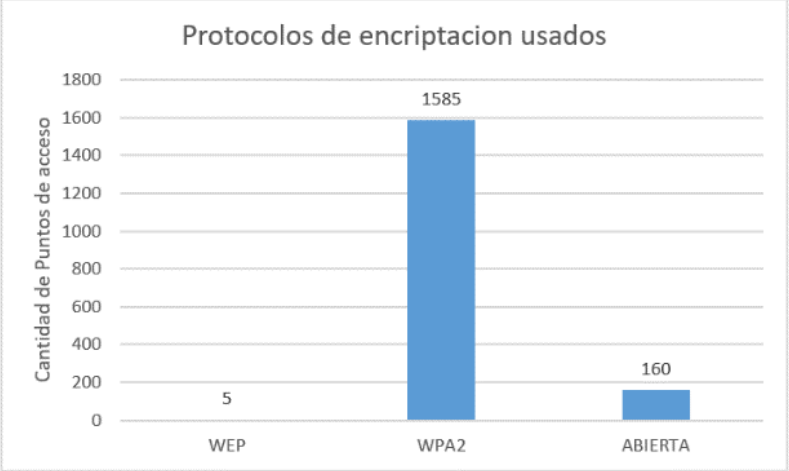

Figura 3 Seguridad de redes inalámbricas

La grafica 3 muestra que del total de capturas realizadas, 1586 esto es el 90.58% usan seguridad WPA2, el uso de WEP, que es un tipo de encriptación débil, debido a sus vulnerabilidades, solo es usado por 5 puntos de acceso, esto es el 0.29%, mientras que señales abiertas se encontraron 160, esto es el 9.14% de los puntos de acceso capturados.

Las redes 802.11 están definidos en canales, en nuestro país, en la frecuencia de 2.4 Ghz, se usan solo 11 de los 14 canales disponibles,

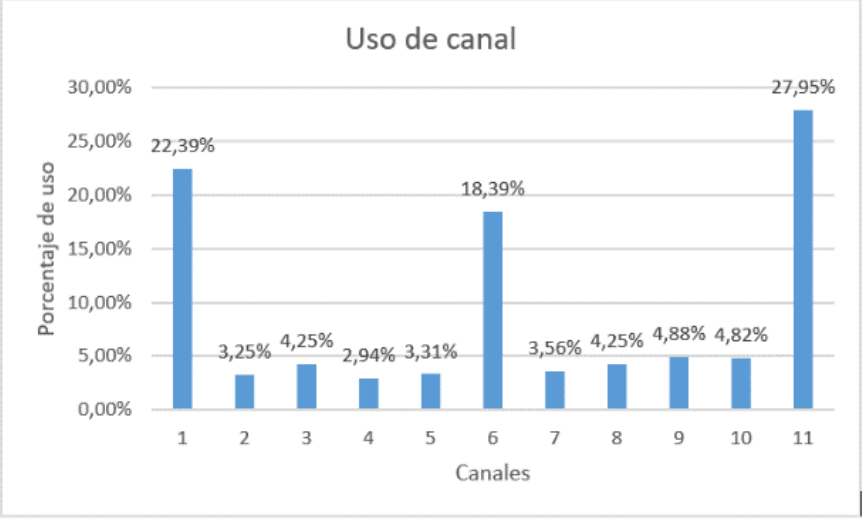

Figura 4 Uso de canales

En la figura 4 se muestra el uso de los canales del conjunto de puntos de acceso escaneados durante el mes de mayo, en ese gráfico se puede observar claramente que los canales más usados son el 1, con un 22,39%, el canal 6 con un 18,39% y el canal 11 con un 27.95%.

Observamos que los canales 1, 6 y 11 está en ubicaciones que no se solapan y que el 68.73% de los puntos de acceso trabajan en estos canales.

Cabe indicar que, durante la captura de información, se encontraron puntos de acceso los cuales emitían señal en los canales 100. 104. 108,112 124, 128, 132, 136, 140, etc. estos canales son usados en la frecuencia de 5GHz.

Se realizó una función de distribución acumulada, para el registro de las potencias obtenidas en la captura de datos.

En el gráfico 5 se realiza la confirmación, indicando que la mayoría de puntos de acceso capturados en el escaneo presentan una potencia entre los 80 y 90 dBm.

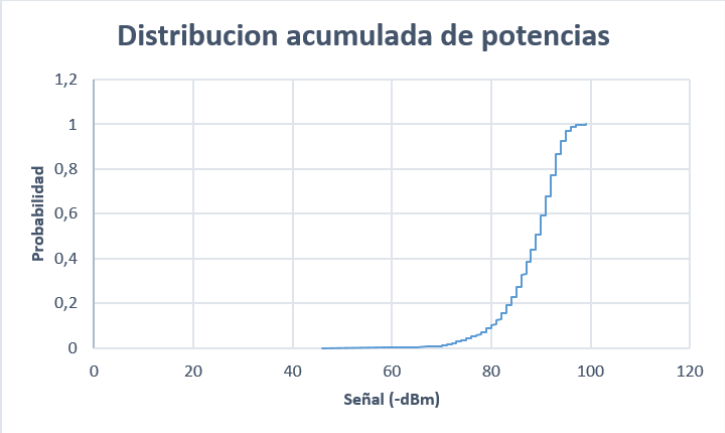

Figura 5 Grafico de distribución acumulado de potencia de señal

Análisis de seguridad

Se realizó un estudio con las posibles vulnerabilidades en las redes inalámbricas, usando los defectos conocidos en redes WEP y WPS, es de indicar que, aunque el cifrado WEP (Castro, 2005) es muy débil aún hay puntos de acceso que todavía la usan, aunque son muy pocos.

Basados en estudios previos el tiempo promedio para recuperar un pin WPS suele ser entre 4 a 10 horas, en la práctica suele tomar la mitad de ese tiempo es más con programas que usan los pines WPS por defecto, como WPS Connect, este tiempo suele caer a minutos, debido a la nula configuración de ese elemento del punto de acceso por parte del usuario.

En la figura 3 se observa la encriptación de los puntos de acceso en la cual se pude notar que la mayoría usa WPA2, de estos un 41.32% usa WPS, como se ve en la tabla 2.

Tabla 2 Equipos encriptados con WPA que tienen WPS habilitado

WPS Habilitado	Cantidad	Porcentaje
Si	655	41.32%
No	930	58.68%

Fuente: Elaboración propia.

Aun teniendo muy pocos puntos de acceso con la encriptación WEP, solo 5, se lo ha considerado en su análisis puesto que es probable su vulneración, debido a fallas en su protocolo ya conocidas (Vibhuti, 2005)

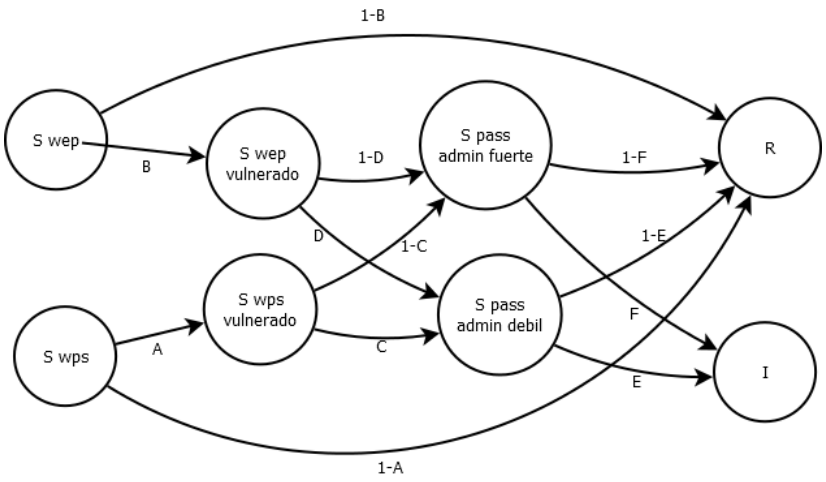

Figura 5 diagrama de modelo SIR utilizado para investigar la simulación del ataque

Se ha considerado el intento de vulnerar los pines WPS y la clave WEP como se ve en la figura 5, existe una probabilidad A de que un pin WPS sea vulnerado en un tiempo At, si en ese

tiempo no se logra descifrar de forma satisfactoria, existe la probabilidad (1-A) de que aquel punto de acceso se considere inmune/recuperado, por el lado del intento de vulnerabilidad del cifrado WEP, existe la probabilidad B de que la contraseña se resuelva fácilmente en un tiempo Bt, sin embargo también consideramos la probabilidad (1-B) de que la contraseña no sea vulnerada en el tiempo estimado, para lo cual se concluirá que ese punto de acceso es inmune/recuperado. Si el pin WPS es exitosamente recuperado hay una probabilidad C de que el punto de acceso use una contraseña de administrador débil y una probabilidad (1-C) de que use una contraseña de administrador fuerte, si usa una contraseña débil, en ese caso, existe la probabilidad E de que el equipo sea vulnerado en un tiempo Et y al modificar su firmware el equipo quedará infectado, pero si pese a poseer una contraseña débil, no es posible modificar su firmware para infectarlo después de cierto tiempo, existe una probabilidad (1-E) de que el equipo se considere inmune/recuperado, por otro lado si el equipo usa una contraseña de administrador fuerte existe una probabilidad F de que el equipo sea infectado en un tiempo Ft y modificado su firmware, y si pasado aquel tiempo, no es posible modificar su firmware, existe una probabilidad (1-F) de que el equipo sea considerado inmune/recuperado.

Consideramos que un atacante va a utilizar las vulnerabilidades WPS y WEP para realizar una propagación de malware, para el WPS hicimos pruebas con REAVER en Kali Linux y con WPS connect en Android por lo que consideramos que la A=60% y At=60 minutos

Por lo general, los usuarios no suelen cambiar las contraseñas de acceso a sus puntos de acceso (Shah, 2005), por ejemplo aquellos que usan proveedores de acceso a internet del estado, las contraseñas de administrador suelen publicarse en varias páginas web, por lo que

consideramos C=50% y D=50%, debido a lo documentado de la vulnerabilidad de las redes WEP (Beck & Tews, 2008) (Bittau, Handley, & Lackey, 2006) establecimos B=100% Bt=20 minutos (Bittau et al., 2006) . Para las contraseñas, si son débiles, o contraseñas por defecto consideramos E=80% y F=10%, esto datos los obtuvimos en nuestras pruebas de intento de obtención de contraseñas ya sea por defecto, las más fáciles, o por fuerza bruta las más difíciles, con respecto a los tiempos de intento de acceso a una contraseña, basado en las pruebas realizadas, con un ataque por fuerza bruta se pueden probar de 20 a 30 contraseñas por segundo se pueden probar con los puntos de acceso, así que se consideró Et=60 minutos y Ft=120 minutos.

En el grafico se puede observar que el ataque posee 2 raíces, por la vía de WPS y por la vía de WEP, por lo que la probabilidad de que el equipo atacado sea vulnerado está dada por las formulas:

$$\%WPS \ X \ (A \ X \ C \ X \ E + A \ X \ (1-C) \ X \ F)$$

$$\%WEP \ X \ (B \ X \ D \ X \ E + B \ X \ (1-D) \ X \ F)$$

En nuestras simulaciones, si hubiera la cantidad de recursos suficientes para atacar todos los puntos de acceso susceptibles, se llegaría a afectar a 179 puntos de acceso en total, pero debido al limitante de recursos se considera un atacante durante 2, 4 y 6 horas diarias para realizar el ataque durante 1 mes, encontramos un total de 660 equipos a atacar, 655 con WPS y 5 con WEP, los ataques se hacen según la probabilidad de encontrar equipos con WPS o WP cerca del área donde se encuentra el atacante, la tabla 3 muestra el resultado de la simulación de ataques durante 1 mes y la cantidad de equipos vulnerados.

Tabla 3 Resultados de simulación de ataques por hora durante 1 mes

Horas atacando	Equipos con WEP Atacados	Equipos con WPS Atacados	Vulnerados
2	0	30	6
4	1	59	17
6	1	120	30

Fuente: Elaboración propia.

Para el análisis epidemiológico de propagación de infección, se ha considerado que no se incrementa nuevos puntos de acceso ni que se eliminan, por tal motivo usamos el modelo SIR de Kermack y McKendrick (Isea & Lonngren, 2013).

Este modelo supone que la población se encuentra mezclada, por lo que un individuo susceptible tiene una probabilidad fija β por unidad de tiempo de poder contraer la enfermedad, a su vez este está combinado por una probabilidad fija γ por unidad de tiempo que indica la probabilidad de curarse de la infección, al ser la población que estamos considerando cerrada, sin aumentos ni disminuciones, las ecuaciones diferenciales ordinarias son las siguientes:

$$\frac{dS}{dt} = -\beta SI,$$

$$\frac{dI}{dt} = \beta SI - \gamma I,$$

$$\frac{dR}{dt} = \gamma I.$$

En esta fórmula, S es la población fija, la cual va a decrecer en el tiempo, R es una población creciente en el tiempo y por ultimo I, que puede crecer de forma inicial para luego disminuir su valor.

En este modelo hemos considerado el valor de γ en 0 debido a que recuperar un firmware de un punto de acceso comprometido, es una tarea que difícilmente un usuario común está preparado para ejecutar.

Según el diagrama de la figura 6, la tasa de infección β fue de 27,14%, el cual fue utilizado para el modelamiento matemático de la simulación de infección, para el modelamiento de tiempos de ataque, fue utilizado el software Bizagi versión 3.2.7.242 publicado el 20 de junio del 2018, el mismo que permite el modelamiento de procesos, pero que también permite simulaciones, por lo que se aprovechó esta funcionalidad en la obtención de equipos infectados por tiempo que dure el ataque.

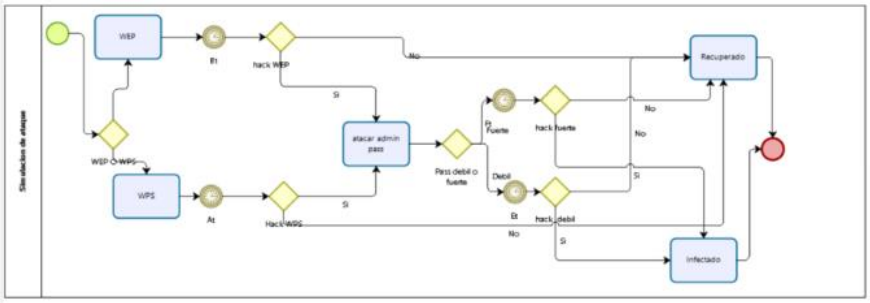

Figura 6 Modelado en Bizagi para la simulación de tiempos de ataque

Los datos para los gráficos del modelado SIR mostrados en la figura 7, 8 y 9 fueron los siguientes:

Tabla 4 Datos para la creación del grafico SIR

Descripción	Valores
Total susceptibles	660
Tasa de Infección	0,2714
Tasa de Interacción	variable
Infectado inicial	1
Unidad de tiempo	1
Tasa de recuperación	0

Fuente: Elaboración Propia.

Los puntos de acceso no interactúan entre sí, por lo tanto, no era posible tener un valor de tasa de interacción, motivo por lo que en la tabla 4 aparece como variable, para obtener este valor se procedió a hacer uso de la herramienta Bizagi, para obtener los equipos infectados según el tiempo de ataque, y según los equipos analizados, con estos valores procedimos a inferir la tasa de interacción, la que para las 2, 4 y 6 horas de ataque tuvimos valores de 3.45, 5.575 y 6.7857 respectivamente.

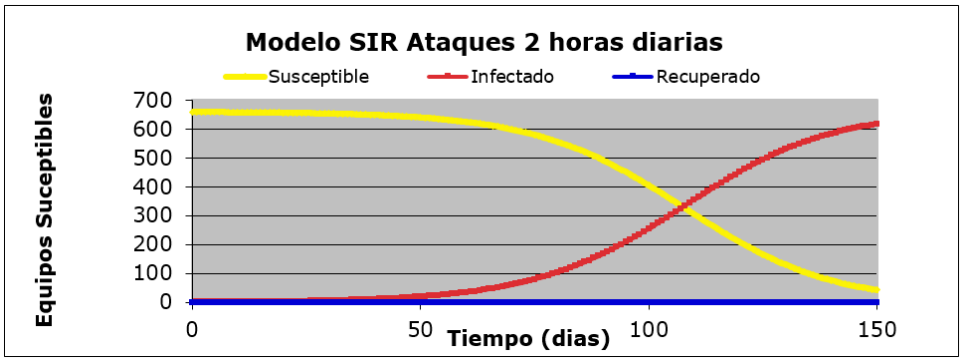

Figura 7 Modelo se simulación SIR de ataque durante 2 horas diarias

La figura 7 muestra el gráfico del proceso de infección que se daría para un ataque de 2 horas diarias, de acuerdo con la simulación, la infección total de los equipos susceptibles se daría en un total de 220 días, si se realiza un ataque durante 4 horas diarias, la infección total de los equipos se daría en 136 días, como se observa en la figura 8, mientras que, para un ataque de 6 horas diarias, se alcanzaría en 113 días, como se puede observar en la figura 9.

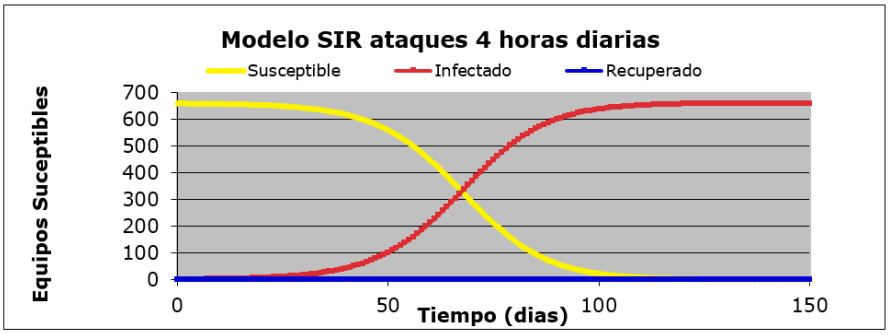

Figura 8 Modelo se simulación SIR de ataque durante 4 horas diarias

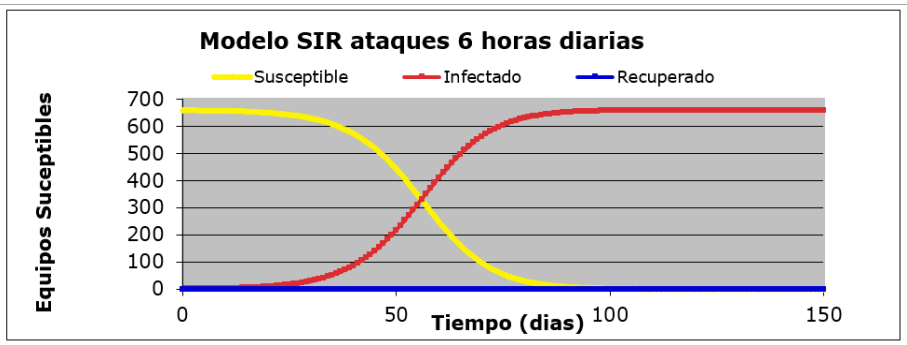

Figura 9 Modelo se simulación SIR de ataque durante 6 horas diarias

Conclusión

Este trabajo ha recopilado de forma pasiva información de puntos de acceso mediante la técnica de Wardriving, para analizar vulnerabilidades conocidas en WEP y WPS, se usó un modelo SIR previamente desarrollado para la aplicación del mismo en un escenario de ataque a las redes inalámbricas de la ciudad de San Francisco de Milagro, provincia del Guayas para estudiar los ataque a infraestructura de red inalámbrica, la investigación, demuestra la viabilidad de los ataques, en especial si se dedica tiempo para el mismo.

Aunque hay muy pocos equipos usando WEP, el hecho de que existan es preocupante debido a lo estudiado que esta este protocolo y sus defectos de sobra conocidos, los proveedores de servicio de Internet, ISP por sus siglas en inglés, deberían comunicar a los usuarios respecto a su uso y ofrecer un servicio adicional en la configuración de los puntos de acceso inalámbricos.

En muchos puntos de acceso el WPS está activado por defecto, el usuario normal que quisiera configurar su propio punto de acceso podría no conocer el uso de esta característica de su equipo y muy probablemente no sabrá desactivarlo, recientes estudios muestran que incluso

protocolos como WPA2, que se considera seguro, tiene vulnerabilidades (Vanhoef & Piessens, 2017), por lo cual, el avance en estos estudios podría dejar a mayor merced de hackers a los usuarios de redes inalámbricas.

El estudio evidenció malas prácticas de configuraciones en las redes inalámbricas en las zonas de estudio, en el análisis en las configuraciones se muestra un desconocimiento por parte de los administradores de internet aumentando los riesgos de ataques desde el exterior, exponiendo datos importantes.

La seguridad de una red inalámbrica dependerá de muchos factores, entre los cuales se destacan el tipo de autenticación utilizado y el cifrado. Muchas de estas falencias son conocidas por todo el mundo, por ello hoy en día existen varias alternativas entre hardware y de software que permiten realizar ataques a este tipo de redes de una forma más efectiva, como se lo evidencio en el estudio realizado. Por ello es necesario tomar medidas de seguridad robustas para evitar ser víctimas de ataques, que violenten contra la privacidad.

Entre los dispositivos encontrados, no solo aparecieron aquellos que se encuentran en casas, sino también en negocios, como una gasolinera, si la red de control de dispositivos de los surtidores está en la misma que la del punto de acceso, las probabilidades de un ataque con un posible siniestro se incrementarían enormemente, esto por no asegurar adecuadamente no solo el equipo de acceso inalámbrico, sino la red de datos.

Bibliografía.

Aked, S., Bolaz, C., & Brand, M. (2012). A Proposed Method for Examining Wireless Device Vulnerability to Brute Force Attacks via WPS External Registrar PIN Authentication Design Vulnerability. *ECU PUBLICATIONS*, 6.

Beck, M., & Tews, E. (2008). *Practical attacks against WEP and WPA*. Retrieved from http://dl.aircrack-ng.org/wiki-files/doc/breakingwepandwpa.pdf

Bittau, A., Handley, M., & Lackey, J. (2006). *Introduction Fragmentation Attack Implementation Conclusion The Final Nail in WEP's Coffin*. Retrieved from http://www.scs.stanford.edu/~sorbo/bittau-wep-slides.pdf

Castignani, G., Loiseau, L., Montavont, N., & An, N. M. (2011). An evaluation of IEEE 802.11 community networks deployments. *HAL*, 498–503. https://doi.org/10.1109/ICOIN.2011.5723148>

Castro, R. (2005). Avanzando en la seguridad de las redes WIFI Going forward more Secure WIFI Networks. *Boletín de La Red Nacional de I+D RedIRIS*, (N°. 73), 23–32. Retrieved from http://www.rediris.es/rediris/boletin/73/enfoque1.pdf

Cimpanu, C. (2018). Massive Coinhive Cryptojacking Campaign Touches Over 200,000 MikroTik Routers. Retrieved August 4, 2018, from https://www.bleepingcomputer.com/news/security/massive-coinhive-cryptojacking-campaign-touches-over-200-000-mikrotik-routers/

Hernández Sampieri, R., Fernández Collado, C., & Batista Lucio, M. (2014). *Metodologia de la Investigación (Sexta Edición)*. México: Mc GRAW-HILL/INTERAMERICA EDITORES, S.A. DE C.V.

INEC. (2014). Tecnologías de la Información y Comunicaciones. *Educación Médica*, *7*(2), 15–22. https://doi.org/10.4321/S1575-18132004000200004

International, P. S. (2005). Seguridad en redes Inalámbricas Índice general.

Isea, R., & Lonngren, K. E. (2013). *On the Mathematical Interpretation of Epidemics by Kermack and McKendrick*. *Gen. Math. Notes* (Vol. 19). Retrieved from www.i-csrs.orgavailablefreeonlineathttp://www.geman.in

Lilian, C., & Pietrosemoli, E. (2007). Redes Inalámbricas para el desarrollo en América Latina y el Caribe. *Apc,Isbn*, *3*, 17. Retrieved from https://www.apc.org/es/pubs/issue/redes-inalambricas-para-el-desarrollo-en-america-l

Madrid Molina, J. M. (2006). Seguridad en redes inalámbricas 802.11. *Sistemas y Telemática*, (3), 13–28. https://doi.org/10.18046/syt.v2i3.934

Monsalve Pulido, J. A., Aponte Novoa, F. A., & Chaparro Becerra, F. (2015). Security analysis of a WLAN network sample in Tunja, Boyacá, Colombia. *Dyna*, *82*(189), 226–232. https://doi.org/10.15446/dyna.v82n189.43259

Sabater, A. F., Martín, A., Rey, D., & Rodríguez Sánchez, G. (2014). Simulación de la propagación del malware: Modelos continuos vs. modelos discretos. *RECSI*, 6. Retrieved from https://web.ua.es/es/recsi2014/documentos/papers/simulacion-de-la-propagacion-del-malware-modelos-continuos-vs-modelos-discretos.pdf

Sanatinia, A., Narain, S., & Noubir, G. (2013). Wireless spreading of WiFi APs infections using WPS flaws: An epidemiological and experimental study. In *2013 IEEE Conference on Communications and Network Security, CNS 2013* (pp. 430–437). IEEE. https://doi.org/10.1109/CNS.2013.6682757

Sánchez Espinosa, F., Vivero García, J., & Llanos, D. B. (2018). Aplicación de una metodología de seguridad avanzada en redes inalámbricas. *RISTI*, *15*, 16. Retrieved from https://media.proquest.com/media/hms/PFT/1/SG3K5?_a=ChgyMDE4MDgwNDIxMzc1MDg0NToyODU2MTkaCk9ORV9TRUFSQ0giDzEzOC4xMjIuMTEwLjIyMCoHMTAwNjM5MzIKMjA0MTE0MzU3MDoQT3BlbnZpZXdDaXRhdGlvbkIBMVIGT25saW5lWgJGVGIDUEZUagoyMDE4LzA0LzAxcgoyMDE4LzA0LzMwegCCAR1QLTEwMDY5ODQtbnVsbC1udWxsLW51bGwtbnVsbJIBBk9ubGluZcoBANIBElNjaG9sYXJseSBKb3VybmFsc6oCJk9TOkVNUy1VbkF1dGhEb2NWaWV3LWdldFByZXZpZXdQZGZMaW5rygITR2VuZXJhbCBJbmZvcm1hdGlvbtICAVnyAgD6AgFZggMDV2Vi&_s=m4aP7wEQnSHr43WQRGiy0gFMvNc%3D

Shah, R. (2005). *Software defaults as de facto regulation: The case of wireless aps*. Retrieved from https://www.researchgate.net/publication/228866619

Vanhoef, M., & Piessens, F. (2017). Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. https://doi.org/10.1145/3133956.3134027

Vibhuti, S. (2005). IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability, 6. Retrieved from https://pdfs.semanticscholar.org/beb2/90fb1db86715c5ddb256245bff2ca1bb1dec.pdf