ANÁLISIS VULNERABILIDAD WPA2 EN BARRIO EL POBLADO, MEDELLÍN

Modalidad: Exploratorio

PABLO PEREZ POSADA

ALEJANDRO MERY AGUDELO

Trabajo de grado para optar al título de: Ingeniería de Sistemas y Computación

Juan Esteban Velásquez

UNIVERSIDAD EIA

INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

ENVIGADO

2019

CONTENIDO

RESUMEN

En la actualidad el uso de las redes inalámbricas se ha popularizado hasta el punto de hacer parte de la vida diaria de los individuos. Las tecnologías con protocolo IEEE 802.11, conocido como redes wifi, y concretamente las redes WPA2 son las más comunes y utilizadas; estas se pueden encontrar desde espacios residenciales como casas y apartamentos, hasta ambientes laborales y de producción. Considerando la cantidad de usuarios que utilizan esta tecnología en su día a día y dado el potencial de datos e información privada que pasa por este tipo de red, tales como: transacciones monetarias, datos personales, mensajes de redes sociales, datos de la tarjeta de crédito, imágenes privadas, información corporativa y confidencial; se vuelve necesario analizar qué tan segura es la red que se usa para este tipo de operaciones. Es por esto por lo que en el presente trabajo se desarrollará un prototipo de auditoría de redes para tener una idea de qué tan vulnerable es el protocolo IEEE.802. 11 en la ciudad de Medellín.

Palabras clave: protocolo WPA2, red Wi-Fi

ABSTRACT

In the present day, the use of wireless networks has been popularized to the point that it is part od the daily life of individuals. The technologies with IEEE 802.11 protocols, known as wifi networks, specifically WPA2, are the most common and used; these can be found in residential spaces as houses and apartments, to working places and production environments. Taking into account the large number of users that use this technology in their day to day and given the potential of data and private information that goes through this type of network, such as: monetary transactions, personal data, social network messages, credit card numbers, private images, corporate and confidential information; It becomes necessary to analyze how secure is the network that is used for this kind of operations. That is why in this paper a prototype network audit will be developed, to get a clear idea of how vulnerable the IEEE.802. 11 protocol is in the city.

Keywords: WPA2 protocol, Wi-Fi Network

INTRODUCCIÓN

En el marco de la nueva era digital o cuarta revolución industrial, cada vez el ser humano y todo aquello que lo rodea se encuentra más interconectado e interoperacionalizado, lo cual trae consigo un gran crecimiento tanto económico para los diferentes países del globo como en términos de sociedad. Ha sido tal el impacto que los gobiernos se han visto obligados a incluir en su gestión el uso de las tecnologías de la información y la comunicación, resultando en cierta modernización y aumento de eficacia de lo que es actualmente la figura del Estado. Es precisamente en países en vía de desarrollo, como lo es Latinoamérica, donde se evidencia un mayor impacto de estas tecnologías gracias al aumento en capital humano e inversión que se ha llevado a cabo en los últimos años; a pesar de que esta región cuenta con una infraestructura tecnológica, un alcance y una posibilidad de acceso mucho menor comparado con otros países desarrollados, como por ejemplo Estados Unidos o Japón, los beneficios que ha traído para las personas que aquí habitan son innumerables, permitiendo una mejoría en cuanto a conectividad y en temas de descentralización.

Dentro de este contexto de la tecnología, es claro que nacen constantemente muchos servicios y funcionalidades que los individuos llegan a utilizar sin entender su verdadero fin, especialmente en países como Colombia. Al tratarse de algo tan extendido a nivel mundial, como son las tecnologías de la información y la

comunicación, los sujetos tienden a confiar ciegamente en un servicio y no se preocupan por aspectos tan fundamentales como lo es la seguridad. Uno de estos servicios es el Internet, más concretamente el conocido Wi-Fi o WPA2, el cual es utilizado a diario por una gran cantidad de personas sin darle la importancia que merece, y desconociendo la existencia de brechas de seguridad en este protocolo y de personas dispuestas a explotarlas para obtener un beneficio propio. Es verdad que son infinitas las ventajas que algo como este tipo de red inalámbrica puede ofrecer, pero se hace imperante reconocer que el solo hecho de estar conectado a una red ya representa cierta vulnerabilidad a cualquier tipo de ataque; es necesario entonces crear conciencia en temas de seguridad informática, de manera tal que la población pueda sacar provecho de aquellas herramientas tecnológicas que aportan a la globalización, y minimizando los impactos negativos que estas puedan llegar a generar.

Durante la investigación previa se descubrió una vulnerabilidad fácilmente explotable en la cual se obtienen las contraseñas de los wifis mediante la ayuda de un dispositivo que permite escuchar las conexiones de los usuarios a un router. Preocupados por la seguridad y la cantidad de Wi-Fi vulnerables en El Poblado, Medellín se decidió desarrollar un proyecto que permite la auditoría de redes y verifique si una red es vulnerable, esto se realizó con diferentes redes a lo largo del barrio El Poblado hasta tener una muestra representativa que nos permitiera valorar el estado actual del barrio.

1. PRELIMINARES

1.1 PLANTEAMIENTO DEL PROBLEMA

1.1.1 Formulación del problema

El contexto geopolítico en el que vive la sociedad actual está sin duda marcado por los constantes avances en el sector de la tecnología y desarrollos digitales para facilitar relaciones, trabajos, comunicaciones y otra gran cantidad de realidades que cada persona debe afrontar en su rutina cotidiana. Todos los avances tecnológicos que surgen día a día traen consigo una variedad de riesgos a nivel de seguridad de la información que por lo general no son lo suficientemente valorados ni evaluados por los que son responsables de la implementación de estos nuevos desarrollos en los ambientes para los cuales fueron creados.

Uno de los principales riesgos poco contemplado, es el manejo de contraseñas que resulten realmente seguras para conservar impenetrables entornos digitales que

contengan información relevante, sea de carácter personal, empresarial o incluso gubernamental. Generalmente, las personas eligen contraseñas que resulten "fácilmente recordables" para no perderlas y tener inconvenientes posteriores para acceder a su información. Esto, sin duda crea una brecha de seguridad porque está claro que entre más sencilla sea la contraseña, más sencillo será para un atacante descubrirla mediante métodos ya desarrollados para analizar contraseñas.

Un ejemplo de estas fallas de seguridad se vive todos los días en cada uno de los hogares colombianos. La configuración de redes locales que permiten el acceso a internet para las familias en el país, por lo general están bajo la responsabilidad de las compañías que proveen el servicio de conectividad. Estas compañías, no siempre siguen protocolos que prioricen la seguridad, solo le dan prioridad al deseo del cliente para que no olvide su contraseña, lo que por supuesto tiene como resultado sean tan solo el nombre de una persona del grupo familiar, una cédula o algún número telefónico, contraseñas que, sin duda, son de fácil reconocimiento para los softwares tan desarrollados que existen en la actualidad para "crackeo" o reconocimiento de contraseñas.

Entonces, a partir de esta situación, surge la siguiente interrogante: ¿Cómo crear un sistema que permita recolectar información suficiente para determinar el porcentaje de hogares en El Poblado, Medellín que cuentan con una contraseña de red segura?

1.1.2 Justificación

Es fundamental entender que la construcción de un dispositivo que permita captar contraseñas de redes familiares para luego ser desencriptadas o crackeadas no representa un accionar ilegal ni peligroso por parte de quienes realizan esta investigación. Encontrar la contraseña se considera como accionar pasivo ya que no se está actuando a partir de la obtención de esta. Si se intentara acceder a la red que corresponda a la contraseña encontrada, en ese momento sí pasa a ser un accionar activo y por tanto ilegal, pero por supuesto no es el interés de esta investigación.

Descifrar las contraseñas que se obtengan de una muestra representativa previamente definida, va a permitir, mediante el uso de estadística, definir qué tan segura y protegida está la ciudad de Medellín en cuanto a uso de contraseñas para redes wifi, ya que al vulnerar una red WPA2 se pueden obtener paquetes de datos importantes tales como tarjetas de crédito, cuentas de redes sociales y bancarias entre muchos otros. El beneficio principal es obtener una investigación sólida que sea la base de una concientización de la población sobre la importancia de proteger correctamente su información personal. Dar claridad sobre realmente qué tan sencillo es para cualquier persona obtener tus claves, es algo que la gente que no tiene conocimientos avanzados sobre informática y redes debe tener presente dado que estos procedimientos, protocolos o hábitos, pueden prevenir brechas de seguridad y por lo

tanto ataques que desencadenan filtraciones de información no pública a personas no deseadas.

1.2 OBJETIVOS DEL PROYECTO

1.2.1 Objetivo General

Analizar la vulnerabilidad de las redes Wifi en el barrio Poblado, Medellín, mediante un prototipo de auditoría de redes.

1.2.2 Objetivos Específicos

Desarrollar un dispositivo para auditoría Wi-Fi que permita la intercepción de redes y captura de paquetes.

Aplicar un método de desencriptación que permita verificar los PKID.

Seleccionar una muestra probabilística que permita desarrollar el proyecto.

1.3 MARCO DE REFERENCIA

Wifi WPA2

WLANS (redes inalámbricas locales), han revolucionado las conexiones tecnológicas, especialmente los sistemas tipo IEEE 802.11, ya que son usadas tanto en ambientes públicos, como privados. Estas tecnologías tienen grandes beneficios, tales como movilidad, flexibilidad y libertad a la hora de acceder. Pero estos beneficios traen consigo nuevos riesgos de seguridad. *"The traditional WLAN security mechanism is*

WEP. WEP is an encryption algorithm designed in 1999 along with 802.1 lb standard to provide wireless security. However, several serious weaknesses were identified by cryptanalysts and WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, and then by the full IEEE 802.11i standard (also known as WPA2) in 2004." (Kumkar, 2012).

La tecnología Wireless Fidelity, es el líder en la comunicación inalámbrica. El Wifi WPA2, fue adoptado en 2004 e introdujo grandes cambios a comparación de sus versiones anteriores, como: "la separación de la autenticación de usuario de la integridad y la privacidad de los mensajes, proporcionando una arquitectura robusta y escalable, que sirve igualmente para las redes locales domésticas como para los grandes entornos de red corporativos". (Lehembre, 2006).

El protocolo que utiliza el WPA2 es el IEEE 802.1X, el cual es un protocolo de autenticación basado en el control de puertos de acceso, es decir, fue desarrollado para redes de cable, y posee mecanismos de autenticación, autorización y distribución de claves incorporando controles de acceso para los usuarios que se unan a la red. Su arquitectura está compuesta por tres entidades funcionales: el suplicante que se une a la red, el autenticador que hace el control de acceso y el servidor de autenticación que toma las decisiones de autorización. "En las redes inalámbricas, el punto de acceso sirve de autenticador. Cada puerto físico se divide en dos puertos lógicos, formando la PAE (Port Access Entity). La PAE de autenticación está siempre abierta y permite el paso de procesos de autenticación, mientras que el PAE de servicio sólo se abre tras

una autenticación exitosa (por ejemplo, una autorización) por un tiempo limitado (3600 segundos por defecto).“ (Lehembre, 2006). La autorización está dada por el servidor de autenticación.

En cuanto al robo de identidades, el estándar IEEE 802.1X posee la capacidad de autenticación de mensajes para que tanto el suplicante como el autenticador, quien se limita a enviar los mensajes al servidor, calculen sus claves secretas y activen la encriptación antes de acceder a la red. El suplicante y el autenticador se comunican mediante un protocolo basado en EAP, el cual transporta varios métodos de autenticación y permite sólo un número limitado de mensajes. “Cuando se completa el proceso, el suplicante y el servidor de autenticación tendrán una clave maestra secreta.” (Lehembre, 2006).

Este protocolo utiliza la implementación Advanced Encryption Standard de 128-bits (AES), el cual bloquea el algoritmo de cifrado para los procesos de autenticación y encriptación. “En WPA2 hay dos modos de autenticación que pueden ser usados, los cuales son Pre-Shared Key y Enterprise” (Khasawneh, 2014). WPA2 usa Pairwise Transient Key (PTK) para generación de key y usa CCMP (Counter Mode CBC MAC Protocol), el cual es un método ampliamente utilizado para proteger la integridad y garantizar el origen de mensajes transmitidos y datos almacenados utilizando un bloque cifrado. (Brincat, 2001).

Raspberry PI 3 modelo b

Es una plataforma de desarrollo de aplicaciones, utilizada para propósito general, como propulsor de innovación. Usa lenguajes como Python, C++ y Java y es considerada un miniordenador. “Usa el controlador Broadcom, que es un Soc (System on Chip) con un procesador ARM11 que corre a 700 MHz. No trae display, pero puede ser usado con un display HDTV. Tiene un puerto Ethernet que permite conectarlo a una red y se pueden cargar sistemas operativos desde Mac, Windows y Linux.” (Casco, 2014). Es útil para proyectos que requieren interfaz gráfica o internet. El sistema operativo standard para Raspberry Pi es Raspbian.

Hashcat

Es una aplicación que permite recuperar contraseñas a partir del valor hash para cada una.

“In order to get hold of a password, the cracker must find the sequence of characters whose CHF (Cryptographic Hash Functions) matches the hash stolen from the database. This process is called password cracking and there are specific tools able to make millions of guesses per second” (Rodrigues, 2017). Hashcat es la herramienta más avanzada para estos procesos, ya que toma las palabras en texto plano y calcular su hash, comparándolo con otro archivo que almacena las contraseñas originales.

Encriptación de datos

La encriptación de datos transforma datos a otra forma o código, para que solo las personas con una clave tengan acceso. Los datos encriptados se conocen como texto cifrado, mientras que los datos no encriptados se conocen como texto plano. La encriptación es un método utilizado para mejorar la seguridad en diferentes organizaciones.

El proceso de encriptación en el protocolo WPA2 se da de la siguiente manera: "*for each Medium access control Protocol Data Unit (MPDU) there is a packet number (PN) and this number will incremented for each next MPDU, in the header of MPDU, there is something called Additional Authentication Data (AAD) and in this field the integrity delivered by CCMP is represented. To create the CCMP Nonce block the PN and, A2 (MPDU address 2) and Priority field of MPDU will be used. The Priority field has reserved value of zero. In addition the new PN with the key identifier together will be used to build the 64 bit CCMP header, then the group of temporal key, AAD, nonce, and MPDU data are used to create the cipher text and MIC. Finally, the encryption of MPDU is obtained by combining the CCMP header, original MPDU header, encrypted data and MIC"* (Sukhija, 2012).

De igual manera el proceso de desencriptación también tiene unos pasos lógicos dependientes del proceso de encriptado, para el protocolo WPA2, se desarrolla así: "*After the encrypted MPDU is received, the AAD and nonce values could be extracted from the encrypted MPDU, the header of the encrypted MPDU is used to build the AAD.*

*To create the nonce value, the values of different fields of the header will be used which are the MPDU address 2 (A2), PN, and Priority fields. To recover the MPDU plaintext, temporal key, MIC, AAD, nonce and MPDU cipher text data are combined together. Moreover at this point the integrity of AAD and MPDU plaintext is confirmed. Finally, by combining MAC header of MPDU and decrypted MPDU plaintext data, the Plaintext of MPDU is decrypted. "(*Sukhija, 2012). De esta forma se desencripta en texto plano el texto cifrado en el protocolo.

Teoría probabilística

Rama de la matemática que proporciona los fundamentos, modelos y lenguaje que se usa en la estadística con el fin de obtener e interpretar resultados confiables para realizar conclusiones.

Estadística descriptiva

"La estadística descriptiva es la parte de la estadística que sintetiza y resume la información contenida en un conjunto de datos, por tanto, un análisis descriptivo consiste en clasificar, representar y resumir los datos." (Seoane, 2007). De esta forma se entiende que la estadística descriptiva se encarga de ofrecer un resumen de la información del total de los datos de la muestra analizada.

Inferencia estadística

“Es el conjunto de métodos estadísticos que permiten deducir cómo se distribuye la población e inferir las relaciones entre variables a partir de la información que proporciona la muestra recogida” (Seoane, 2007). Permite obtener conclusiones de la población a partir de la información de la muestra representativa de esta.

Población

Es el conjunto total de valores posibles de una característica particular, de un grupo específico de objetos, sobre los cuales se realizan observaciones.

Muestreo

Es la técnica utilizada en la estadística que se encarga de definir el tamaño, los parámetros y las reglas para seleccionar muestras representativas de una población específica. Una muestra es una cantidad finita de la población, “a partir del cual se pretende realizar inferencias respecto a la población de donde procede” (INEI, 2006) y es considerada probabilística si es obtenida aleatoriamente.

Muestreo aleatorio simple

“Es un método de muestreo donde una muestra aleatoria simple es seleccionada de tal manera que cada muestra posible del mismo tamaño tiene igual probabilidad de ser seleccionada de la población” (INEI, 2006). Es decir, al seleccionar un grupo de “n” unidades muestrales, cada muestra de tamaño “n” tiene la misma

posibilidad de ser seleccionada, lo que significa que “todos los individuos que componen la población blanca tienen la misma oportunidad de ser incluidos en la muestra.

Esto significa que la probabilidad de selección de un sujeto es independiente de la probabilidad que tienen el resto de los sujetos que integran forman parte de la población blanco.” (Otzen, 2017). “Una muestra se dice probabilística cuando la selección de los elementos que intervienen en ella se hace a través de algún procedimiento aleatorio, o sorteo, que le concede a cada uno de los elementos de la población, un cierto chance de caer en ella”. (Arveolo). Entre sus ventajas se encuentra que el cálculo es rápido, de medias y varianzas, además existen paquetes informáticos para analizar los datos. Su principal desventaja es que al trabajar con muestras pequeñas puede no representar de forma adecuada a la población.

Muestreo por conveniencia

Es una técnica de muestreo no probabilístico, no aleatorio.

El muestreo no probabilístico se basa en un proceso que no les permite a todos los individuos de una población blanco tener la misma posibilidad de ser seleccionados. Este tipo selecciona a individuos específicos que cumplen con cierta característica que beneficia la investigación.

“Una muestra es no probabilística cuando la selección de los elementos de la población que pasan a formar parte de la muestra se hace a criterio de la persona que

está tomando la muestra, sin que medie ningún tipo de procedimiento aleatorio para su selección. Los procedimientos de Inferencia Estadística no son aplicables a este tipo de muestras.” (Arveolo).

Es práctico y basado en la accesibilidad, proximidad y disponibilidad de los investigadores y de las personas que forman parte de la muestra. “Permite seleccionar aquellos casos accesibles que acepten ser incluidos.” (Otzen, 2017). Esta técnica se utiliza cuando no hay criterios de exclusión para que una persona participe. Todos los sujetos de la población pueden ser elegidos para ser parte de la muestra.

Es muy económico y eficiente pues al trabajar con un número reducido y conocido se reduce el tiempo de trabajo y de obtención de resultados. Es un método que le facilita el trabajo a quien desarrolla el estudio. La principal desventaja es que puede representar inadecuadamente la población blanco, además como la selección de la muestra no es aleatoria, no se pueden realizar conclusiones generalizadas, por esto hay riesgo que se produzca un sesgo estadístico en los resultados

Aircrack-ng

Es un software usado como herramienta para crackear WEP. El término ng se refiere a next generation. “Aircrack es en realidad un conjunto de herramientas. El homónimo es la herramienta real que hace el craqueo” (Haines,2010).

Ataque por diccionario

"Is a password-guessing technique in which the attacker attempts to determine a user's password by successively trying words from a dictionary (a compiled list of likely passwords) in the hope that one of these password guesses will be the user's actual password" (Adams, 2011). Es decir, los atacantes utilizan una compilación de contraseñas posibles, las cuales no se restringen a simples palabras de un diccionario tradicional, sino que pueden contener variaciones de las letras iniciales del usuario, información personal, palabras apareadas, famosas, de libros o cultura general, cambios sutiles de letras por números, entre otros.

Ataque de fuerza bruta

Es una técnica de desciframiento de contraseñas que consiste en probar todas las combinaciones posibles hasta lograr obtener el acceso. Se conoce también como búsqueda exhaustiva de clave. "*The cryptanalyst wishes to find the key k that was used with block cipher E to encrypt some plaintext P to produce ciphertext C, $C=Ek(P)$"* (Wiener, 2005).

BSSID y SSID

El BSSID (Basic Server Set Identifier) es un centro de identificación único de todos los paquetes de una red para ser identificados por esta red de área local como pertenecientes. "Devuelve una matriz de bytes con la dirección MAC del enrutador al que está conectado el WiFi Shield" (Monk, 2014).

El SSID (Service Set Identifier) es conocido como el identificador de la red, el nombre que esta tiene, el cual está compuesto por una secuencia específica que se encuentra en todos los paquetes que hacen parte de la misma red. “Use of SSID is intended to direct stations to the correct AP in cases where multiple APs exist” (Smith, 2014). Es decir que puede ser usado para evitar que usuarios diferentes accedan a la red.

Autenticación

Existen dos métodos implementados en este proceso. El abierto, el cual consiste en la no autenticación “The only requirement is that the two stations involved be set to "open authentication." (Smith, 2014). Y el método de Shared Key, en el cual se comparte una clave secreta entre las dos estaciones. “In 802.11 this is implemented through WEP. In this case both systems must know the WEP key in order to authenticate 802.11, which requires authentication prior to association taking place.” (Smith, 2014).

CUPP

La forma más común de autenticación es la combinación entre un usuario y una contraseña, si ambos coinciden el usuario logra obtener la conexión. Common User Password Profiler, es una herramienta que genera diccionarios creando una lista de palabras dependientes del perfil del usuario.

Handshake

Es el procedimiento de control de transmisión de datos entre dos dispositivos. Permite a la estación receptora aceptar los datos transmitidos.

3. METODOLOGÍA

Desarrollo de dispositivo para auditoria Wifi.

(Objetivo específico 1).

Dispositivo

Hardware:

El primer dispositivo utilizado fue un Raspberry Pi 3 model B como elemento principal para el desarrollo del prototipo. Se optó por este, dado que cumplía todos los requisitos necesarios para llevar a cabo la captura de handshakes, era de fácil acceso y altamente configurable. Adicionalmente se requirió una antena de recepción Wifi con un chipset específico (AWD-32), la cual se conectó al Raspberry Pi 3 model B a través de una interfaz USB.

Software:

Se decide instalar en el Raspberry Pi 3 model B el sistema operativo de “raspbian”, una distribución de Linux, ya que facilita el trabajo y es compatible con otros softwares para monitorias de red.

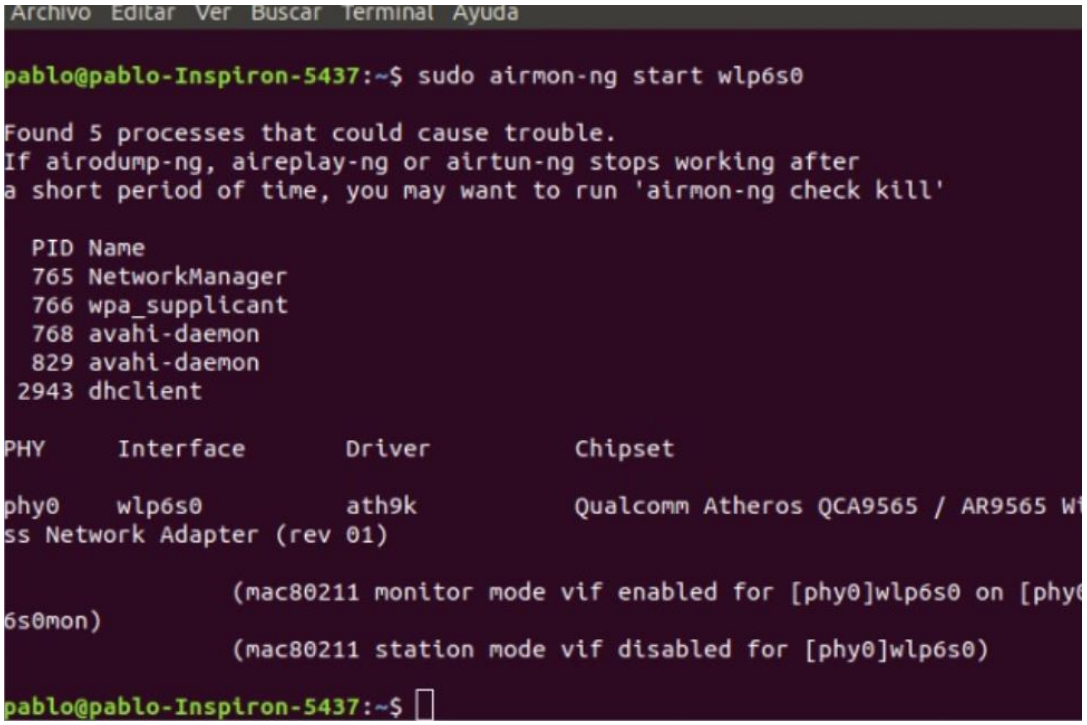
En el “raspbian” se instaló “aircrack-ng” para el monitoreo, escucha de redes y captura de “handshakes”.

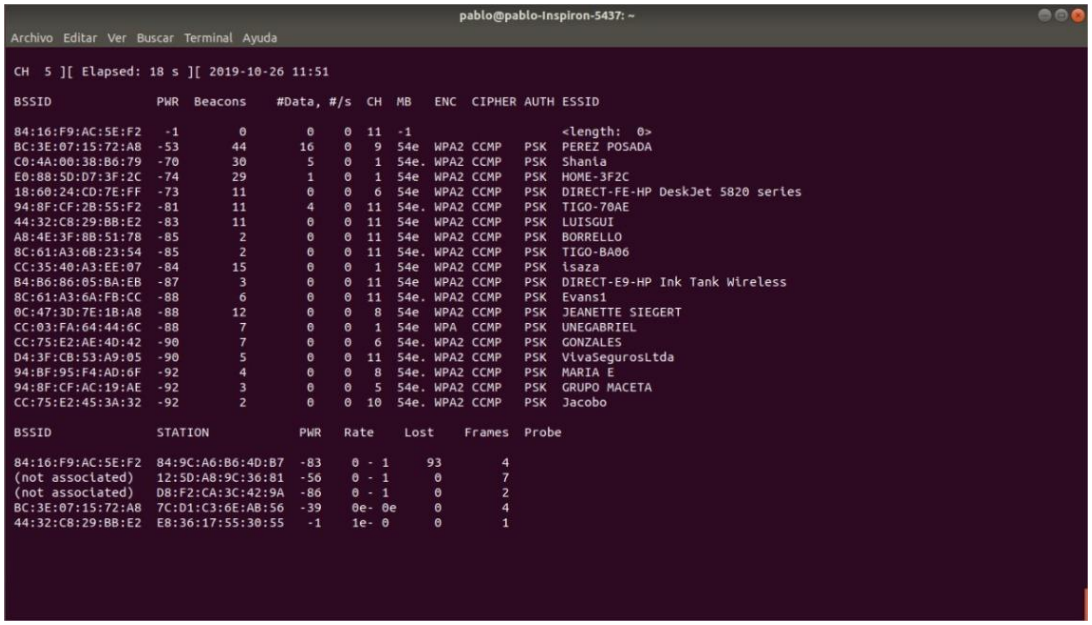
Configuración y metodología de captura:

Para la realización de este objetivo se utilizó en su gran mayoría el prototipo desarrollado y por fines prácticos, como apoyo se usaron otros dispositivos como: portátiles y computadores de mesa, con el fin de agilizar la captura de datos.

Para el monitoreo de la interfaz de red, la antena se configuró en modo monitor, esto permite que la antena escuche las redes que están en un rango cercano y entregue una información básica sobre ellas como: BSSID, SSID, tipo de protocolo de la red, canal y flujo de información. A este proceso mencionado normalmente se le denomina escaneo.

En la figura 1a se puede evidenciar el comando que permite poner la interfaz de red en modo monitor.

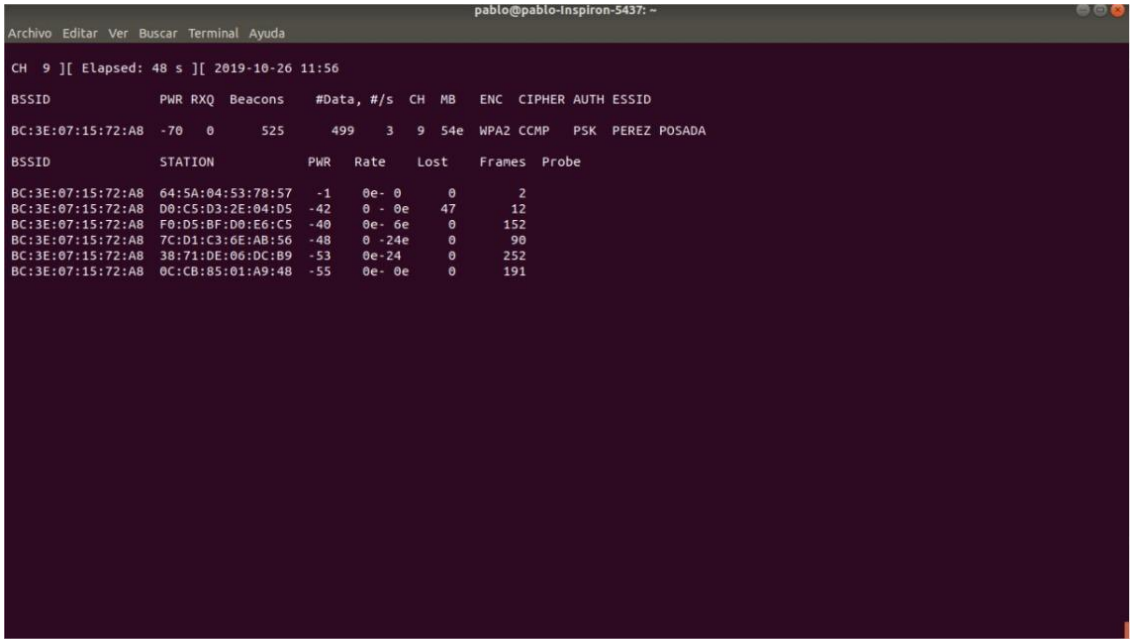




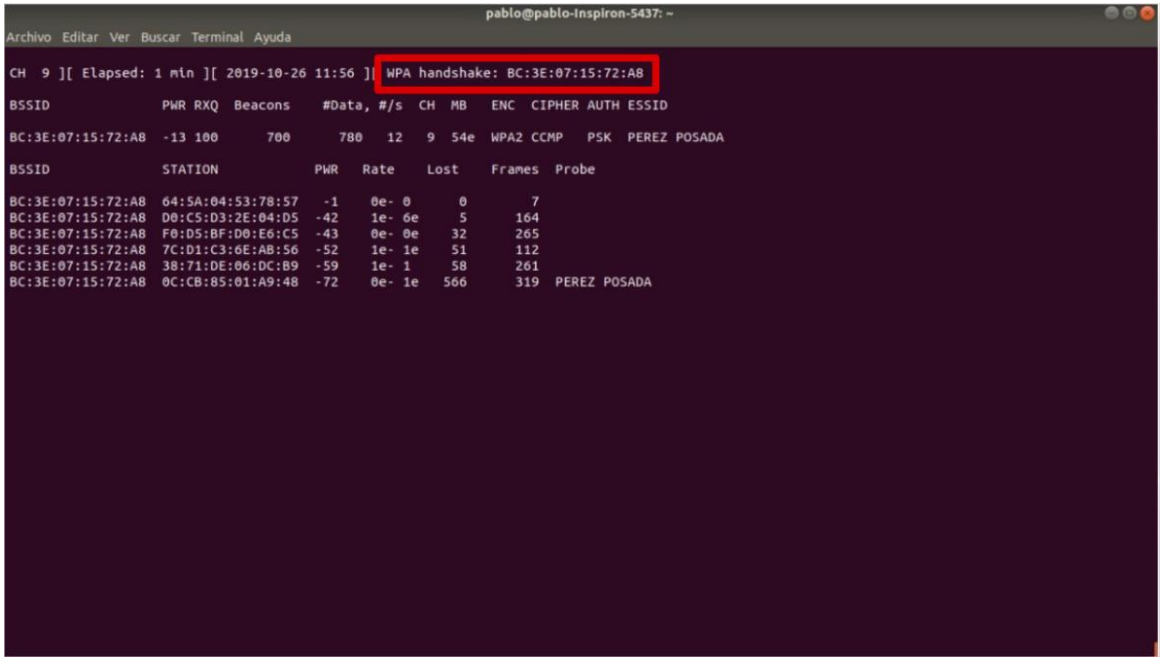
De la lista de redes resultantes del escaneo se debe elegir una que cumpla con los siguientes parámetros:

- Estar corriendo bajo el protocolo WPA2.
- Tener BSSID disponible.
- No ser una red abierta.
- Método de autenticación PSK.
- Método de cifrado CCMP.

Después haber elegido la red, se toma el BSSID correspondiente de ésta para ejecutar un nuevo escaneo dirigido.



Este comando permite escuchar la red hasta que alguien haga una conexión y se capture el handshake. Este proceso puede tardar un largo tiempo ya que es posible que nadie se conecte.



Una vez capturado el handshake se guarda en el dispositivo en formato .cap y se vuelve a iniciar el procedimiento.

Para completar este objetivo se debe tener el “handshake” correspondiente a la red deseada almacenado en formato .cap

Descifrar los PMKID

(Objetivo específico 2).

Para desarrollar adecuadamente este objetivo y delimitar correctamente su alcance, fue necesario establecer un concepto de contraseña segura. Se define que una contraseña se considera segura y no se seguirá intentando descifrar si no es un número de celular, un número de cédula o una de las contraseñas contenidas en un diccionario creado en base a los nombres de las redes y algunas claves comunes.

Una vez se tiene el archivo .cap listo, fue necesario implementar dos métodos de desencripción llamados: ataque de fuerza bruta y ataque por diccionario. Ambos ataques se realizaron mediante el framework de desencripción llamado Hashcat.

Para poder utilizar este framework fue necesario transformar todos los archivos .cap a un formato de archivo. hccapx debido a que Hashcat solo funciona con este formato. Para hacer la transformación, se utilizó la herramienta proporcionada por Hashcat en su página web.

Se determinaron dos rangos de números para realizar el ataque por fuerza bruta, estos números se basan en la definición de una contraseña segura que fue previamente establecida.

El primer rango hace referencia a la cantidad de posibles cédulas que pudieron utilizar como clave en el barrio El Poblado. Este rango se divide en 2, dependiendo del número de dígitos de la cédula. Esto se debe a que las cédulas anteriores al 2004 tienen 8

dígitos mientras que las posteriores a dicho año tienen 10 dígitos.
De esta forma se toma un número de 10 dígitos, en el cual el primer dígito siempre va a ser un 1, el resto de los dígitos rotan entre 0 y 9 teniendo así un rango final de 1000000000 a 1999999999, el cual contiene todas las cédulas de 10 dígitos que se podrían encontrar en la ciudad de Medellín.

Realizar un ataque con este rango de interacciones requirió un tiempo aproximado de 30 a 150 minutos dependiendo del equipo que lo ejecutara. Este mismo proceso se desarrolló para el rango de cédulas con 8 dígitos, con la diferencia de que se roto entre 0 y 9 todos los dígitos dado que para las cédulas más antiguas no se tenían conjuntos establecidos de numeración.

En las figuras se observan los parámetros “-m” y “-a”. El “-m” hace referencia al tipo de hash que tiene el archivo al cual se le hará el ataque (en este caso 2500 utilizado para WPA-EAPOL-PBKDF2) y “-a” el cual indica el tipo de ataque a realizar (en este caso se usa el 3 que significa ataque por fuerza bruta). Al final del comando se indica la cantidad de caracteres que se desea iterar en el ataque estableciendo “d” que

indica al programa que debe iterar solo caracteres numéricos. En el caso del rango de cédulas de 10 dígitos, se pone un “1” al principio del rango de iteración para indicar que ese número debe ser fijo y todos los demás iteran dejando ese 1 al principio en cada combinación.

El segundo rango hace referencia a la cantidad de números celulares que se pudieron utilizar como claves en el barrio El Poblado. Para esto tomamos un número de 10 dígitos en el cual se definió que el primer dígito siempre será constante y se estableció que sería el “3”, todos los otros dígitos rotan entre 0 y 9 teniendo así un rango final de 3000000000 a 3999999999, el cual representa los posibles números celulares que podríamos encontrar en la ciudad de Medellín. Realizar el ataque con este rango de iteraciones requirió un tiempo aproximado de entre 30 minutos a 150 minutos dependiendo del equipo que lo ejecutara.

Se investigó un repositorio público de donde se pudo obtener un diccionario que contiene contraseñas comúnmente utilizadas por las personas, lo cual hace que tengan un bajo nivel de seguridad. Luego, a esta lista de contraseñas se le agregó una lista que contiene todas las palabras del idioma español y varias combinaciones de estas mismas palabras. De igual forma, dada la gran posibilidad de contraseñas que puede utilizar una persona en su red, se utilizó el programa CUPP, con el cual se

modificó el contenido de esta lista agregando números aleatorios y algunos caracteres especiales al final de cada palabra. Adicionalmente se le aplicó el “Leet mode” con el fin de agregar combinaciones posibles de los elementos de la lista de forma que se cambian letras por números y se ordenan los caracteres de forma inversa. Finalmente, a cada nombre de red recogido se le aplicó nuevamente el programa CUPP de manera que se ingresó el nombre de cada red y generó las combinaciones de posibles contraseñas a partir de los números aleatorios, el “Leet mode” y la combinación de caracteres especiales. Todo esto se unió en un diccionario final que contiene aproximadamente 17 millones de contraseñas posibles a evaluar. El tiempo de ataque para este modo fue de aproximadamente 2 minutos por cada una de las redes evaluadas.

```
Microsoft Windows [Versión 10.0.17763.805]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Manuel\Desktop\DatosTesis\hashcat-5.1.0>hashcat64 -m 2500 <FILE.hccapx> -a 0 <DICCIONARIO.TXT>
```

En la figura se puede observar que el parámetro “-a” cambia a 0 dado que el tipo de ataque que se efectúa en este rango es un ataque por diccionario. Al final del comando, se pasa como parámetro el diccionario o lista de palabras que se utilizaron para el ataque al archivo hccapx.

Para ejecutar los ataques fue necesario hacerlo en un dispositivo más potente que el escogido para el objetivo específico 1, además el proceso es mucho más rápido

y eficiente si el dispositivo utilizado cuenta una GPU o tarjeta gráfica independiente pues esto acorta radicalmente el tiempo que se demora el proceso.

Se utilizaron 4 equipos personales cada uno con tarjetas gráficas independientes (Nvidia 1050Ti, Nvidia 1080Ti, Nvidia 1650 y Nvidia 1060Ti) y se reservó un día completo el Laboratorio de Configuración y Desarrollo TI de la Universidad EIA, el cual cuenta con 2 equipos con tarjeta gráfica independiente Nvidia 1060Ti 6gb y 18 equipos con tarjeta gráfica independiente Nvidia rx750, para un total de 20 equipos. En cada uno de estos se instaló Hashcat como framework de ayuda para hacer la desencriptación.

Se distribuyó la carga de trabajo entre los diferentes equipos de tal manera que cuando se terminaba un ataque, se reportaban los resultados de este e inmediatamente se activará el siguiente. Si los resultados de las 3 pruebas para un mismo. pcp eran negativas este se consideraba seguro, Si se encuentra la contraseña en uno de los ataques este se detiene y no se realizan los ataques faltantes.

Para el final de este objetivo se deben haber procesado todos los “handshakes” que en total fueron 146 los recolectados.

Muestra probabilística

(Objetivo específico 3).

De primera mano se exploraron los diferentes tipos de muestreo que se podían realizar para representar apropiadamente la población objetivo y refleja correctamente el objetivo planteado, luego se analizó el beneficio de cada uno y se definió que el tipo de muestreo a realizar sería el simple aleatorio por conveniencia, esto debido a que hace la recolección de datos y el tamaño de la muestra mucho más manejable y cercana al alcance propuesto para el lugar planteado.

Dentro del muestreo simple aleatorio por conveniencia se establecen 2 fórmulas para calcular el tamaño total de la muestra. La primera se utiliza conociendo la población blanco y la otra sin conocerla. Debido a que se desconocía cuantas redes cumplían los parámetros de inclusión del estudio en el barrio El Poblado y dada la gran cantidad de presuntos que se tendrían que asumir, se decidió utilizar una muestra aleatoria por conveniencia sin conocer el tamaño total de la población. Esta se resume en la fórmula a continuación:

$$n = \frac{z^2 * p * q}{d^2}$$

Esta fórmula determina el tamaño de la muestra basado en el nivel de confianza que se quiere alcanzar, en este caso es representado con una “z”. La “p” es la proporción de individuos en la población que tienen la característica de estudio, para este trabajo se optó por 0.05, siendo esta la opción más segura. La variable “q” es la

proporción de individuos que no tienen la característica, siendo “q” igual a 1 menos “p”. Finalmente, “d”, es la precisión del cálculo, para una mayor infalibilidad se estableció en 3%.

En las siguientes figuras se evidencia el desarrollo de la fórmula:

$$n = \frac{1.65^{2} * 0.05 * (1 - 0.05)}{0.03^{2}}$$

$$n = \frac{1.65^{2} * 0.05 * 0.95}{0.03^{2}}$$

$$n = 143.68$$

De esta forma se obtiene que el tamaño de la muestra final indicada es de: 143.68 individuos (redes), pero para fines prácticos se redondea a 144 individuos. Este tamaño se considera representativo y es con el que se trabajará el resto del proyecto, sin embargo, por la diferencia de densidades y desarrollo tecnológico entre los diferentes sitios geográficos, no es posible hacer extrapolaciones a poblaciones más grandes como lo es Medellín o Antioquia.

Este tamaño de muestra se distribuyó de manera conveniente entre centros comerciales y sectores residenciales con el propósito de capturar eficaz y eficientemente las muestras. Para mantener el anonimato tanto de las redes como de

los usuarios presentes, no se guardará registro del lugar específico en el que se capturó la red, del nombre de esta, ni de las contraseñas correspondientes a las redes.

Se logran capturar 120 redes distribuidas en 10 sectores residenciales a los cuales se les asignó el título “casas” y 26 en 4 centros comerciales para un total de 146 redes. A pesar de que se capturaron 3 redes de más, al ser un número tan pequeño la proporción de la muestra no se ve afectada.

PRESENTACIÓN Y DISCUSIÓN DE RESULTADOS

Después de seguir cada uno de los puntos específicos de la metodología obtuvimos los siguientes resultados:

De las 146 redes procesadas confirmamos un total de 57 redes inseguras a las cuales fue posible descifrar las contraseñas. De estas se confirmaron 7 mediante ataque de diccionario, 36 por el ataque de fuerza bruta de cédulas de 8 dígitos y 12 mediante el ataque de cédulas de 10 dígitos y solo 2 mediante el ataque de celulares de 10 dígitos. Estas 57 redes inseguras representan el 39% de la muestra dejándonos 89 contraseñas seguras que representan el 61% de la muestra. Lo anterior puede interpretarse con mayor facilidad en la figura 2.a.

RESUMEN RESULTADOS	
TOTAL INSEGURAS CONFIRMADAS	57
CONFIRMADAS POR DICCIONARIO	7
CONFIRMADAS 8 NÚMEROS	36
CONFIRMADAS CEDULAS 10 NÚMEROS	12
CONFIRMADAS CELULAR 10 NÚMEROS	2
TOTAL SEGURAS CONFIRMADAS	89
PORCENTAJE SEGURAS CONFIRMADAS	61%
PORCENTAJE INSEGURAS CONFIRMADAS	39%
TOTAL RECOLECTADAS	146

Ya que las redes fueron capturadas en 10 lugares residenciales y 4 centros comerciales se hace una distinción según el lugar y si fue posible encontrar la contraseña o en su defecto que esta no haya sido encontrada. Esto se evidencia en la figura 2.b.

LUGAR	Cantidad	Encontradas	Porcentaje Encontradas
Casa 1	9	5	56%
Casa 2	21	7	33%
Casa 3	20	9	45%
Casa 4	11	6	55%
Casa 5	3	2	67%
Casa 6	12	1	8%
Casa 7	2	0	0%
Casa 8	4	1	25%
Casa 9	21	9	43%
Casa 10	17	10	59%
C.C. El Tesoro	5	1	20%
C.C. Monterrey	7	1	14%
C.C. Oviedo	4	3	75%
C.C. Santa Fe	10	2	20%
TOTAL	146	57	39%

Además, se determina la efectividad de cada uno de los ataques según el lugar de recolección de muestra. La efectividad se determina mediante el porcentaje de contraseñas inseguras encontradas. Esto lo podemos evidenciar en las figuras 2.c, 2.d, 2.e, 2f.

Tipo de lugar	Cantidad	Encontradas	Encontradas por Diccionario	Porcentaje Encontradas por Diccionario
Casa	120	50	4	8%
Comercio	26	7	3	43%
TOTAL	146	57	7	12%

Tipo de lugar	Cantidad	Encontradas	Encontradas de 8 números	Porcentaje Encontradas por 8 números
Casa	120	50	32	64%
Comercio	26	7	4	57%
TOTAL	146	57	36	63%

Tipo de lugar	Cantidad	Encontradas	Encontradas 10 números cédula	Porcentaje Encontradas 10 números cédula
Casa	120	50	12	24%
Comercio	26	7	0	0%
TOTAL	146	57	12	21%

Tipo de lugar	Cantidad	Encontradas	Encontradas 10 números celular	Porcentaje Encontradas 10 números celular
Casa	120	50	2	4%
Comercio	26	7	0	0%
TOTAL	146	57	2	4%

El 63 % de las contraseñas fueron encontradas mediante el ataque de cédulas de 8 dígitos, esto nos indica que es el tipo de contraseña insegura más recurrente en el poblado.

De la figura 2.c encontramos que el método de ataque por diccionario fue más efectivo en los lugares de comercio que en los lugares residenciales, lo que nos indica

El método menos eficiente fue el ataque por fuerza bruta de números celulares de 10 dígitos, el segundo menos eficiente fue el ataque por diccionario, el segundo más efectivo fue el ataque de fuerza bruta de cédulas de 10 dígitos y el más efectivo fue el ataque de fuerza bruta de cédulas de 8 dígitos, con porcentajes de contraseñas inseguras encontradas de 4%, 12%, 21% y 63% respectivamente.

CONCLUSIONES Y CONSIDERACIONES FINALES

Se considera que las redes WPA2 en el poblado aún son muy inseguras y crean un ambiente propicio para el robo de información dado que encontramos el 39% de las redes auditas utilizando los métodos más comunes de desencripción sin aplicar ingeniería social u otras técnicas que permiten obtener más información de las redes.

Se considera que sería prudente que los proveedores de servicio de telecomunicaciones creen unos estándares mínimos para las contraseñas, los cuales incluyan un mínimo de una mayúscula, minúscula, carácter especial y un número para que así la posibilidad de encontrar la contraseña mediante ataques de fuerza bruta disminuye sustancialmente debido a los extensos tiempos de procesamiento dados por la complejidad de combinaciones posibles que se pueden generar con estos parámetros.

Se considera necesario que los proveedores de servicios de telecomunicaciones capaciten a los usuarios al momento de la instalación del servicio para que las contraseñas que se utilicen no estén relacionadas con información personal de las personas que habitan la residencia o que son dueñas de la red. Esto

representa una brecha de seguridad sensible que cualquier atacante con una investigación básica pueda aprovechar y acceder de manera abusiva a la red.

Se estima la vulnerabilidad de las redes wifi en el poblado en un 39%, eso significa que en el poblado el 39% de las personas son susceptibles a intrusiones no deseadas por parte de atacantes que robar información sensible y privada de los usuarios de esta red. Además, pueden inhabilitar la red afectando el servicio en el caso de los comercios o incluso robo de activos como lo es el dinero digital.

REFERENCIAS

1. ACOSTA-LOPEZ, E. Y. Melo-Monroy, y P. A. Linares-Murcia, (Enero de 2017). “Evaluation of the WPA2- PSK wireless network security protocol using the Linset and Aircrack-ng tools,” Rev. Fac. Ing., vol. 27 (47), pp. 9-XX.

2. ADAMS, C. (2011) Dictionary Attack. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA

3. ARVELO, A. Muestreo Aleatorio Simple. http://www.arvelo.com.ve/pdf/muestreo-aleatorio-arvelo.pdf

4. BARTOLI, A. Medvet, E. Onesti, F. (2018) “Evil twins and WPA2 Enterprise: A coming security disaster?” Computers & security 74. 1–11

5. BRINCAT K., Mitchell C.J. (2001) New CBC-MAC Forgery Attacks. In: Varadharajan V., Mu Y. (eds) Information Security and Privacy. ACISP 2001. Lecture Notes in Computer Science, vol 2119. Springer, Berlin, Heidelberg

6. CASCO, S. (Septiembre de 2014). Raspberry Pi, Arduino y Beaglebone Black Comparacion y Aplicaciones. Universidad Catolica Nuestra Senora de la Asuncion.

Recuperado de: http://jeuazarru.com/wp-content/uploads/2014/10/MiniPCs.pdf

7. CUPP. Common User Password Profiler. GitHub. https://github.com/Mebus/cupp

8. DOMIGO-FERRER, J. (Septiembre de 2014). Privacy-Preserving Group Discounts. *RECSI*, Alacant, (69-73). Recuperado de: https://rua.ua.es/dspace/bitstream/10045/40398/1/RECSI-2014_15.pdf

9. GOLD, S, (Noviembre de 2011). "Cracking wireless networks", Rev. Network Security, pp 14-17

10. HAINES,B. Chapter 1 - 802.11 Wireless – Infrastructure Attacks. Seven Deadliest Wireless Technologies Attacks. 2010. p1-24 https://doi.org/10.1016/B978-1-59749-541-7.00001-1

11. HASCHAT, advanced password recovery. Description. [aplicación]. Recuperado de: https://hashcat.net/wiki/doku.php?id=hashcat

12. INEI. Glosaria básico de términos estadísticos. Centro de Investigación y Desarrollo. Talleres de la Oficina Técnica de Administración del Instituto Nacional de Estadística e Informática. Lima. 2006. https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib0900/Libr

o.pdf

13. KHASAWNEH M., Kajman I., Alkhudaidy R., Althubyani A. (2014) A Survey on Wi-Fi Protocols: WPA and WPA2. In: Martínez Pérez G., Thampi S.M., Ko R., Shu L. (eds) Recent Trends in Computer Networks and Distributed Systems Security. SNDS 2014. Communications in Computer and Information Science, vol 420. Springer, Berlin, Heidelberg. 495-506 p. DOI https://doi-org.recursosbiblioteca.eia.edu.co/10.1007/978-3-642-54525-2_44

14. KIEF, H.; Helmut A. Roschiwal. CNC Handbook. LANs—Local-Area Networks, Chapter (McGraw-Hill Education: New York, Chicago, San Francisco, Lisbon, London, Madrid, Mexico City, Milan, New Delhi, San Juan, Seoul, Singapore, Sydney, Toronto, 2012). https://aplicacionesbiblioteca.udea.edu.co:2612/content/book/9780071799485/chapter/chapter20

15. KUMKAR, V., Tiwari, A., Tiwari, P, Gupta,A., Shrawne, S.(2012). Vulnerabilities of Wireless Security protocols (WEP and WPA2). *International Journal of Advanced Research in Computer Engineering & Technology*. Volume 1, Issue 2, (34-38)

16. LEHEMBRE, G. (2006). Seguridad Wi-Fi – WEP, WPA y WPA2. *hakin9. número 1/2006.* (12-26). Recuperado de: http://www.zero13wireless.net/wireless/seguridad/01_2006_wpa_ES.pdf

17. MONK, S. Programming Arduino Next Steps: Going Further with Sketches, Second Edition. Network and Internet of Things Programming, Chapter (McGraw-Hill Education: New York, Chicago, San Francisco, Athens, London, Madrid, Mexico City, Milan, New Delhi, Singapore, Sydney, Toronto, 2019, 2014). https://aplicacionesbiblioteca.udea.edu.co:2612/content/book/9781260143249/chapter/chapter14

18. MONK, S. Programming the Raspberry Pi: Getting Started with Python, Second Edition. Introduction, Chapter (McGraw-Hill Education: New York, Chicago, San Francisco, Athens, London, Madrid, Mexico City, Milan, New Delhi, Singapore, Sydney, Toronto, 2016). https://aplicacionesbiblioteca.udea.edu.co:2612/content/book/9781259587405/chapter/chapter1

19. OTZEN, T. & MANTEROLA C. Técnicas de muestreo sobre una población a estudio. Int. J. Morphol., 35(1):227-232, 2017.

https://scielo.conicyt.cl/pdf/ijmorphol/v35n1/art37.pdf

20. PACKET STORM SECURITY. https://packetstormsecurity.com/files/download/32018/spanish.gz

21. RODRIGUES, B, Paiva. J.R., Gomes, V., Morris, C., y Calixto W.P., (2016). Passfault: an Open Source Tool for Measuring Password Complexity and Strength. Recuperado de: https://www.owasp.org/images/1/13/Artigo-Passfault.pdf

22. SMITH, C. P.E.; Daniel Collins. Wireless Networks: Design and Integration for LTE, EVDO, HSPA, and WiMAX, Third Edition. WiFi, Chapter (McGraw-Hill Education: New York, Chicago, San Francisco, Athens, London, Madrid, Mexico City, Milan, New Delhi, Singapore, Sydney, Toronto, 2014). https://aplicacionesbiblioteca.udea.edu.co:2612/content/book/9780071819831/chapter/chapter10

23. SUKHIJA, S., Gupta, S.: Wireless Network Security Protocols A Comparative Study (January 2012)

24. SEOANE, T., JLR Martínb, E. Martín-Sáncheza, S. Lurueña-Segoviac, FJ. Alonso Morenod. Curso de introducción a la investigación clínica. Capítulo 7:

Estadística: Estadística Descriptiva y Estadística Inferencial. Introduction course to clinical research. Chapter 7: Statistics: descriptive and inferential statistics. Toledo : Noviembre 2007, Vol. 33, Núm. 9. páginas 466-471https://www.elsevier.es/es-revista-medicina-familia-semergen-40-articulo-curso-introduccion-investigacion-clinica-capitulo-13113070

25. WIENER M.J. (2005) Exhaustive Key Search. In: van Tilborg H.C.A. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA