DESCIFRADO DE CLAVES EN REDES INALÁMBRICAS CON SEGURIDAD WPA2 A TRAVÉS DE UN SISTEMA RASPBERRY PI 2

Antonio Pérez Bautista, Miguel Hernández Bolaños y Patricia Pérez Romero
Email: apbesimez@hotmail.com, mbolanos@ipn.mx y promerop@ipn.mx
Centro de Innovación y Desarrollo Tecnológico en Cómputo, IPN.

Resumen

Este trabajo tiene como propósito exponer la metodología y alcances que tiene la implementación del sistema embebido Raspberry Pi 2® para obtener la clave de acceso a una red inalámbrica de internet conocida comúnmente como red Wi-Fi, la cual utiliza el protocolo de seguridad WPA2. Para esto se instalará el sistema operativo Kali Linux™, que es empleado para la auditoría de redes, este sistema proporciona las herramientas necesarias para corromper la seguridad de una red Wi-Fi y con esto dar acceso a la red. Es común que se den estos ataques para deducir la clave y con esto disfrutar los privilegios que brinda el punto de conexión Wi-Fi, como el poder conectarnos a Internet sin tener que ser parte del grupo que paga este servicio. O bien, se puede verificar la seguridad de la red, para evitar un posible ataque y con esto prevenir la intrusión de equipos y personas ajenas que puedan general algún daño o gocen de los beneficios que nos brinda el punto de acceso Wi-Fi.

I. Introducción

La comunicación inalámbrica es aquella que se lleva a cabo entre dispositivos que participan en un intercambio de información sin el uso de un medio físico que la transporte. La tecnología inalámbrica cada día está ganando más terreno, por las ventajas que presenta como el poder enlazar varios equipos entre sí con un solo punto de interconexión, la posibilidad de que los dispositivos conectados puedan desplazarse en su entorno, es decir equipos móviles, entre otras ventajas.

En un artículo de la revista Forbes México expone que las cuatro violaciones a la seguridad informática más caras a la que se enfrentan las empresas según un estudio elaborado por Kaspersky Lab en cooperación con B2B International son [1]:

1. Fraude de empleados.
2. Ciberespionaje.
3. Intrusión a la red.
4. Incumplimiento de proveedores.

En donde se aprecia que el ataque a las redes de comunicación es un serio problema, que no solo afecta a las empresas, sino a los usuarios, ya que la presencia de los teléfonos inteligentes a crecido un 58% a nivel nacional y de estos el 87% son empleados para navegar en internet, así crece la demanda de puntos de acceso de manera inalámbrica, por lo que se corre el riesgo de ser víctima de los delincuentes cibernéticos si no se cuenta con la debida seguridad para proteger la conexión a dichas redes [2].

II. Antecedentes

En 1990 el Instituto de Ingenieros Eléctricos y Electrónicos conocido por sus siglas en inglés como IEEE aprobó la creación de la norma 802, la cual sería para regular el funcionamiento de las redes de área local y metropolitanas [3]. En 1999 varias compañías de alcance mundial decidieron formar una alianza para generar un estándar que normalizara la recién creada tecnología de redes inalámbricas, con esto se dio creación a la Alianza de Compatibilidad de Ethernet Inalámbrica conocida también por su nombre en inglés como Wireless Ethernet Compatibility Alliance (WECA), tiempo después se cambió su nombre a Wi-Fi Alliance, que dio como resultado el desarrollo de la norma IEEE 802.11 para regular la redes inalámbricas, esta norma fue puesta en marcha en el año 2000, fecha en la que se creó el sello Wi-Fi Certified®, el cual servía para garantizar a los usuarios la compatibilidad de los equipos para que trabajen en la misma red inalámbrica sin la necesidad de pertenecer al mismo fabricante; de ahí que la redes inalámbricas de internet sean mejor conocidas como redes Wi-Fi [4].

El protocolo de seguridad de Acceso Protegido Wi-Fi o conocido en inglés como Wi-Fi Protected Access (WPA) es un sistema de seguridad más robusto y eficiente que el protocolo WEP. La seguridad WPA utiliza claves de cifrado de 128 bits que se pueden asignar de forma dinámica por usuario o sesión y un vector de inicialización de 48 bits, por lo que este protocolo es menos vulnerable a los ataques de fuerza bruta [5]. La mejora fue la implementación del Protocolo de Integración de la Clave Temporal (TKIP), el cual modifica de forma sincroniza las claves a medida que el sistema se utiliza, también implementa un Código de Integración del Mensaje (MIC), conocido como Michael. EL protocolo WPA y WPA2 usan para autentificarse un servidor Radius donde se almacenan las credenciales y contraseñas de los usuarios, cuando es utilizada en el ámbito empresarial; o una clave compartida PSK en redes personales. A pesar de que el protocolo de seguridad WPA proporciona un buen nivel de seguridad, es todavía susceptible a ser corrompida cuando se realizan ataques con diccionario [6].

Un ataque por diccionario es un ataque de fuerza bruta, que consiste en capturar el paquete que transmite un cliente al punto de conexión inalámbrica para ser autenticado en la red. Una vez conseguido el paquete, se procesa para buscar en una lista de posibles claves que se conoce como diccionario de ahí el nombre que recibe este tipo de ataque. A pesar de que el protocolo de seguridad WPA/WPA2 brinde una gran protección, como este implementa el protocolo TKIP, resulta ser vulnerable a la recuperación de la clave encriptada [6].
EL sistema operativo Back Track fue una plataforma que servía para realizar auditorías y hacer evaluaciones de seguridad como las pruebas de intrusión con una gran cantidad de herramientas de código abierto y gratuitas, con el fin de detectar, identificar y explorar las vulnerabilidades de los sistemas informáticos [6]. Tiempo después este sistema fue retirado para dar paso al nuevo sistema operativo llamado Kali Linux™, el cual es una versión más avanzada y poderosa que su antecesor. Kali Linux™ está basado en el sistema Debian y es un procedimiento de ficheros FHS [7].

El sistema embebido Raspberry Pi 2® modelo B, como se observa en la figura 1, es la segunda generación de minicomputadora desarrollada por la fundación que lleva el mismo nombre. Este dispositivo ahora utiliza un procesador ARM Cortex-A7 de cuatro núcleos que corre a una velocidad de 900 MHz y una memoria RAM de 1GB, superando con esto a su antecesora. Conserva el mismo diseño que la tarjeta Raspberry Pi® modelo B+ en dimensiones, así como la distribución de sus puertos de conexión [8].

Figura 1. Tarjeta Raspberry Pi 2®

III. Desarrollo

Se abre la Terminal de Kali Linux™ y se ingresa el comando:

root@kali:~# airmon-ng

Este comando nos indicará la interfaz que se está usando, como se observa en la figura 2, para la conexión a la red inalámbrica.

Figura 2. Ejecución del comando airmon-ng

Antes de realizar la intrusión se debe de cambiar la dirección MAC (Media Access Control), esto se realiza mediante el programa Macchanger, para instalar esta aplicación se ingresa la siguiente línea de comando en una Terminal:

root@kali:~# apt-get install macchanger

Luego se ingresan los siguientes comandos para cambiar la dirección MAC:

root@kali:~# airmon-ng stop [Interfaz]
root@kali:~# ifconfig [Interfaz] down
root@kali:~# macchanger -r [Interfaz]

Después se abre una nueva Terminal. Antes de entrar en modo monitor, se ingresa el siguiente comando:

root@kali:~# airmon-ng check

Para cerciorarse que ningún proceso interfiera con el modo monitor. Si se da el caso de procesos encontrados, se ingresa el comando:

root@kali:~# airmon-ng check kill

Para terminar los procesos que se interponen en el escaneo de señales.

Una vez cambiada la dirección MAC y eliminados los procesos, se activa el modo monitor de la tarjeta de red con el comando:

root@kali:~# airmon-ng start [Interfaz]

Ya activado el modo monitor, se empieza a escanear las redes inalámbricas disponibles con el comando:

root@kali:~# airodump-ng [Interfaz]

La figura 3 muestra las redes escaneadas con la tarjeta de red empleada, para detener el escaneo se emplea la combinación de teclas Ctrl+C, se escoge la red para la experimentación con seguridad WPA o WPA2, los datos que debemos de recordar son el BSSID y el número de canal.

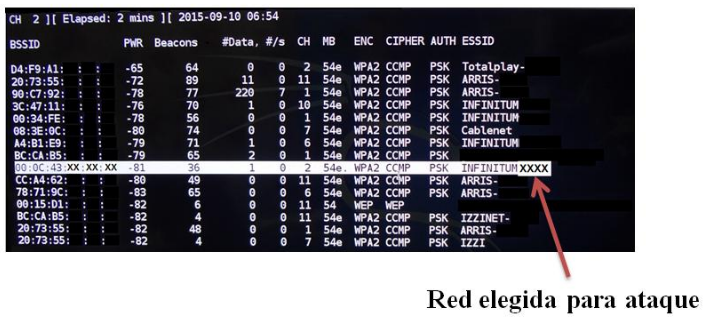

Figura 3. Redes detectadas con la tarjeta de red inalámbrica en modo monitor

Ahora se deben de capturar los paquetes que son transmitidos por la red para después ser analizados y decodificar la clave de acceso, para realizar el almacenaje de estos paquetes se emplea el siguiente comando en una nueva Terminal:

root@kali:~# airodump-ng –c [Canal de la red] –w [Nombre del archivo donde se almacenaran los paquetes] –-bssid [BSSID de la red] [Interfaz]

Una vez empleado este comando, se empezará el almacenaje de paquetes en el archivo designado para esta tarea, la figura 4 muestra este proceso. El objetivo de capturar los paquetes es que alguno deberá de transportar la clave encriptada, esto solo ocurre cuando un cliente se trata de conectar a la red y este tiene la clave correcta para hacerlo, se podría esperar hasta que esto suceda con el inconveniente de que pase un largo tiempo o en el mejor de los casos, si ya hay clientes conectados tratar de desconectar alguno para que este trate de volverse a conectar a la red y con esto capturar el paquete que transporta la clave; a este procedimiento en inglés se le conoce como “Handshake”, ver figura 4. Para realizar este paso se utiliza el siguiente comando en una nueva Terminal:

root@kali:~# aireplay-ng –-deauth [Número de veces a repetir esta acción] –a [BSSID de la red] –c [Dirección MAC de un cliente conectado a la red] [Interfaz]

En la Terminal en donde se realiza la captura de paquetes se puede ver a los clientes conectados a la red que se está monitoreando con el encabezado “STATION”. Una vez realizado el proceso para desconectar a un cliente, aparecerá en esta misma pantalla el encabezado “WPA handshake [BSSID de la red]” si hubo éxito en este paso y se debe detener el proceso de captura de datos con Ctrl+C.

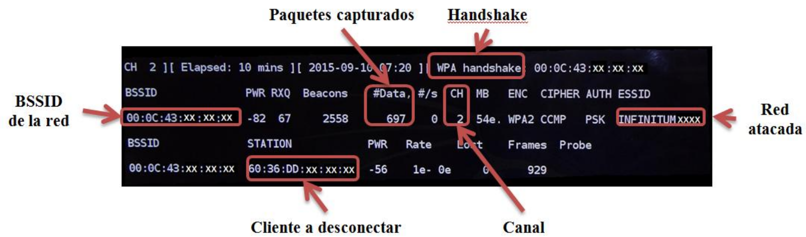

Figura 4. Captura de paquetes y Handshake

Se abre una nueva Terminal donde se usará el comando:

root@kali:~# aircrack-ng –w ./[Dirección del diccionario que se usara] [Nombre del archivo donde se almacenaron los paquetes]

En este paso se empieza a buscar la clave en el archivo conocido como diccionario.

IV. Experimentación y resultados

El diccionario empleado para obtener la clave de acceso a la red inalámbrica contaba con un millón de contraseñas, siendo la última la correcta. El tiempo empleado para la localización de la clave fue de 3 horas con 40 minutos aproximadamente, lo que nos da como resultado que si el diccionario es muy pequeño, la ejecución se realizará en un menor tiempo pero corriendo el riesgo de que no esté la clave o si se emplea un diccionario más grande el tiempo de búsqueda será muy elevado, alcanzando tiempos de días, semanas, meses o en el peor de los casos años, pero consiguiendo un resultado favorable. La figura 5 muestra la captura de pantalla cuando se encuentra la clave de acceso.

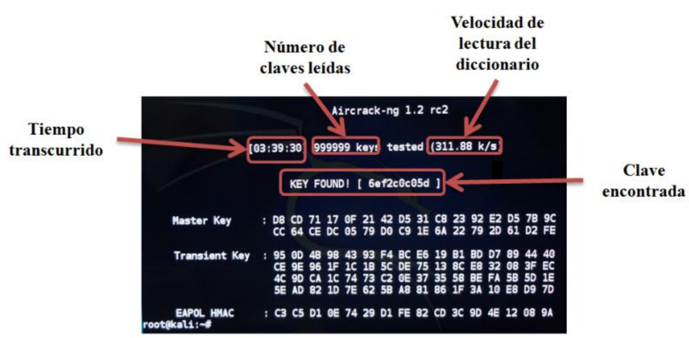

Figura 5. Clave encontrada

V. Conclusiones

La seguridad de una red inalámbrica es un factor muy importante y por ende se deben de contar con medidas para prevenir un ataque. Un factor decisivo es el uso de protocolos de seguridad robustos que no proporcionen fallos, uno de ellos es el protocolo WPA2, el cual es el más empleado en redes personales, pero no está exento de ser corrompido. Una de sus debilidades es el uso de contraseñas débiles como nombres, fechas o palabras comunes que el usuario utiliza por su sencillez o por su facilidad de ser recordadas y que un diccionario con pocas claves pueda ser suficiente para romper la seguridad. Por eso es recomendable utilizar contraseñas las cuales contengan números, letras mayúsculas, minúsculas y signos; además de que deben de ser de una longitud larga para hacer más difícil un ataque por diccionario, ya que un archivo que contenga este tipo de claves tardaría tanto en encontrarla que sería casi inútil deducirla por el tiempo empleado. Otro consejo es el cambio periódico de la clave. También se puede deducir que la potencia de los nuevos sistemas embebidos está creciendo con lo que se tiene un gran aliado o amenaza con respecto a la seguridad de redes inalámbricas, ya que se tiene un equipo móvil y discreto el cual nos brinda las herramientas necesarias para realizar ataques o pruebas de seguridad a las redes Wi-Fi.

Referencias

[1] Gary Parker, William T. Tarimo, Michael Cantor; "*Quadruped Gait Learning Using Cyclic Genetic Algorithms*"; Department of Computer Science Connecticut College: New London, CT, USA; 6-2011.

[2] Chaohong Cai, Hong Jiang, "*Performance Comparisons of Evolutionary Algorithms for Walking Gait Optimization* ", Computer and Information College Hohai University Nanjing, 210000, China Robotics Laboratory, Hohai Universitry Wentian College.

[3] Lourdes Araujo "*Algoritmos Evolutivos un Enfoque Práctico*", Editorial Alfaomega, Abril 2009.

[4] Francisco Barroso José Gómez Miguel Rodríguez Antonio Peregrín; "*Optimización Evolutiva de la Locomoción de un Robot Bípedo*"; Universidad de Huelva.

[5] Arranz de la Peña, Jorge, Parra Truyol, Antonio, "*Algoritmos Genéticos*" Universidad Carlos III.

[6] Tomoyuki Hosoyaand Kenichiro Nonaka; *"Experiment of Integrated Steeringand DrivingForce Controller with Embedded CPU for Front Wheel Steering Vehicles";* Mechanical Systems Engineering, Tokyo City University, Tokyo, Japan.

[7] Fariboz Ahmadi, Reza Tati, Soraia Ahmadi, Veria Hossaini; "*New hadware engine for genetic algorithms (Nuevo motor de hadware para los algoritmos genéticos)*". Islamic Azad University; Ghorveh, Iran; 2011 Fifth International Conference on Genetic and Evolutionary Computing.

[8] Disponible en: http://learn.parallax.com/propeller-c-simple-devices
Consultado en Septiembre de 2015.

[9] Pablo Gumiel Moreno, Yago Sáez Achaerandio, David Quintana Montero; "*Implementación de técnicas de computación evolutivas a la programación automática de un robot*"; Universidad Carlos III de Madrid; 18 de junio de 2009.

[10] Masaki Takahashi, Member, Takafumi Suzuki, Francesco Cinquegrani, Rosario Sorbello, Member, and Enrico Pagello, Member; *"A Mobile Robot for Transport Applications in Hospital Domain with Safe Human Detection Algorithm";* International Conference on Robotics and Biomimetics; 2009, Guilin, China.