DESCIFRADO DE CLAVES PARA LA CONEXIÓN A REDES INALÁMBRICAS CON SEGURIDAD WPA2 EMPLEANDO EL SISTEMA EMBEBIDO RASPBERRY PI 2 Y EL SISTEMA OPERATIVO KALI LINUX

Antonio Pérez Bautista

Centro de Innovación y Desarrollo Tecnológico en Cómputo, IPN.

apbesimez@hotmail.com

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 utilice 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, podemos verificar la seguridad de una 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.

1. 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].

2. 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 normalizará la recién creada tecnología de redes inalámbricas, con esto se dio creación a la Alianza de Compatibilidad de Ethernet Inalámbrica o conocida por su nombre en inglés como Wireless Ethernet Compatibility Alliance (WECA), tiempo después cambio 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 sincronizadamente 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 autenticarse 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 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. Este sistema está basado en el sistema Debian y un sistema de ficheros FHS [7].

El sistema embebido Raspberry Pi 2® modelo B, ver 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].