GESTIÓN Y MEDICIÓN DE PROTOCOLOS DE CIBERSEGURIDAD, UTILIZANDO LA HERRAMIENTA AIRCRACK-NG

Mtro. Flores Montaño Luis Alberto
luisfloresmontano@hotmail.com
M. en C. Esther Viridiana Vázquez Carmona
evazquezc1801@alumno.ipn.mx
M. en C. Rodrigo Vázquez López
rvazquezl1800@alumno.ipn.mx
Dr. Juan Carlos Herrera Lozada
jlozada@ipn.mx

Instituto Politécnico Nacional
Centro de Innovación y Desarrollo Tecnológico en Cómputo

Resumen

En los comienzos de la revolución tecnológica, se han tenido diversos avances en esta, una de ellas son los sistemas basados en redes inalámbricas o en otras palabras se usa la fidelidad inalámbrica también conocida como Wi-Fi. Sin embargo, los sistemas que hacen uso de esta tecnología sufren de amenazas potenciales, teniendo en cuenta la seguridad sobre los datos. Es por esto, que diversas organizaciones son responsables de estas fallas, ya que no cuenta con protocolos de seguridad y por consecuente estos modelos tienen diversas vulnerabilidades. Algunos aspectos por retomar en este artículo son sobre el análisis de vulnerabilidades de distintos protocolos de seguridad ante una herramienta de hackeo ético conocido como Aircrack-ng, la cual puede quebrantar la seguridad de módems Wi-Fi o en su defecto de enrutadores. Para poder realizar esto, es necesario contar con los protocolos de seguridad WPA/WPA2, un sistema operativo Kali Linux en conjunto con los paquetes Aircrack-ng instalados en un equipo de cómputo.

Palabras Clave: Ciberataque, Ciberseguridad, Aircrack-ng, router, Kali Linux.

Abstract

At the beginning of the technological revolution, there have been various advances in this, one of them is systems based on wireless networks or in other words, wireless fidelity is used, also known as Wi-Fi. However, the systems that make use of this technology suffer from potential threats, taking into account data security. This is why various organizations are responsible for these failures, since they do not have security protocols and consequently these models have various vulnerabilities. Some aspects to return to in this article are about the vulnerability analysis of different security protocols against an ethical hacking tool known as Aircrack-ng, which can break the security of Wi-Fi modems or routers. In order to do this, it is necessary to have the WPA/WPA2 security protocols, a Kali Linux operating system together with the Aircrack-ng packages installed on a computer.

Keywords: Cyberattack, Cybersecurity, Aircrack-ng, router, Kali Linux.

I Introducción

Las redes inalámbricas también conocidas como WLAN o más popularmente conocidas como Wi-Fi, brindan la transferencia de datos en un área determinada de red; adicionalmente este tipo de tecnología es barata y sencilla de utilizar para compartir datos en cualquier lugar y en el momento que sea. Esto quiere decir que diversos usuarios pueden acceder para compartir archivos y a internet sin la necesidad de usar un cable. Sin embargo, la transmisión de datos a través del aire puede ser una desventaja ante distintos tipos de ciberataques, así como vulnerabilidades encontradas durante dicha transmisión.

Debido a lo anterior, la ciberseguridad es una de las áreas más importantes en las redes inalámbricas, debido a las conexiones de este tipo y la transferencia de datos a través del aire. Siendo así, la confidencialidad de datos es muy relevante, así como la integridad de estos, por lo que deben de permanecer fuera del alcance de personas externas o cibercriminales. Con el propósito de mantener la confidencialidad, integridad y disponibilidad de los datos, diversas organizaciones enfocadas a WLAN, se dedicaron a crear diversos protocolos de ciberseguridad como el WEP, WPA, WPA2, y actualmente el protocolo conocido como WPA3.

La herramienta Aircrack-ng es una de tantas técnicas para hacer ataques a las redes cableadas o inalámbricas, está herramienta puede ser programada en diferentes sistemas operativos, como Windows, MacOS, o diferentes distribuciones de Linux; sin embargo, la mejor opción se considera Kali Linux, ya que es un sistema operativo abierto, que contiene distintas versiones en línea que ayudan a descifrar y vulnerar contraseñas con las encriptaciones ya mencionadas, no obstante es más complicado para WPA3, este último ha sido analizado e investigado, para quebrantar su seguridad.

En cuanto al protocolo de seguridad WEP (en inglés Wired Equivalent Privacy), es una algoritmo antiguo basado del año 1999, basado en el algoritmo RC4 para el cifrado; posteriormente se encontraron fallas por lo que fue sustituido en el 2003 por otro cifrado de nombre WPA (en inglés Wi-Fi Protected Access), el cual también fue sustituido por el estándar completo de IEEE 802.11i conocido también como WPA2, este mostraba una seguridad más robusta, usando como algoritmo principal a AES (en inglés Advanced Encryption Standard), para la encriptación de contraseñas, este último incluso fue utilizado por la NASA. Finalmente, después de estos llega con un poder encriptación mayor el cifrado WPA3, y con una dificultad más compleja para romper el cifrado.

Cabe mencionar que no solo la herramienta de Aircrack es capaz de descifrar algunos de las contraseñas de Wi-Fi o enrutadores, existen muchas otras herramientas y técnicas para lograrlo tal es el caso de ataques de incautación de reuniones, problemas de resolución MAC, ataques DOS y paquetes de esnifeo; no obstante, estos se pueden configurar y personalizar para que funcionen con Aircrack-ng de Kali Linux. En este artículo se menciona de manera breve como se puede realizar un ataque sencillo para el descifrado de una contraseña de un punto de acceso; sin embargo, cabe resaltar que en algunas situaciones no llega a ser exitoso el uso de esta herramienta debido a la complejidad de esta.

II Investigaciones relevantes en el área de vulnerabilidad en protocolos de ciberseguridad

Existen diversos investigadores enfocados en el área de las fallas de ciberseguridad WLAN, enfocándose en diversos protocolos y específicamente en el WPA3, esto con el propósito de conocer las medidas de seguridad de cada uno de estos.

Los investigadores Vanhoef y Eyal (Vanhoef & Eyal, 2020), utilizaron una brecha de seguridad conocida como “Dragonblood” para intentar quebrantar el protocolo WPA3; por otro lado, el investigador Dahiya (Dahiya,2017), señaló los principales problemas de los protocolos de seguridad Wi-Fi, dando sugerencias para mejorar la seguridad de estos en su debido momento; al igual que el Dr. Reddy y Srikanth (Reddy, and Srikanth, 2019), los cuales presentaron algunas fallas de la seguridad, específicamente en los protocolos WEP, WPA, WPA2 y WPA3. Por su cuenta los investigadores Singh y Sharma (Singh & T.P. Sharma, 2019), realizaron un análisis riguroso en vulnerabilidades de seguridad antigua, señalando los peligros potenciales, así como las debilidades de estas.

Adicionalmente, el investigador de seguridad el Dr. Akshika Aneja (Aneja, 2016), encontró que cada convención de seguridad no proporciona ninguna un estado del 100 % en la seguridad. Por su parte, los investigadores Zulkernie y Lounis (Lounis & Zulkernie, 2020), sugirieron un modelo de coordinación de red en una estructura funcional, para que pudiera ser analizada vía remota y encontrar desafíos en el reconocimiento de aperturas en la red. Finalmente, el Dr.Vanhoef (Vanhoef, 2017), realizó un ataque de reinstalación de clave, utilizando una herramienta conocida como ”KRACK”, la cual puede utilizarse con la paquetería de Aircrack-ng, por lo que en parte es muy fácil de corromper la seguridad, ya que la

herramienta “KRACK”, puede transmitir la información posteriormente, y de esta manera vulnerar los protocolos de seguridad WPE, WPA Y WPA2.

Herramienta de hackeo ético Aircrak-ng

La herramienta Aircrack-ng es un conjunto de paquetes con codificación predefinida, para la penetración en la seguridad de las redes WLAN o Wi-Fi. Dicha herramienta puede instalarse en diversos sistemas operativos, teniendo en cuenta que es una herramienta de código abierto. Cabe resaltar que esta viene instalada en el sistema operativo de Kali Linux, donde es más recomendable de utilizar debido a los paquetes y otras herramientas que complementan su uso, por lo que se puede utilizar para fines de penetración y de ingeniería social, además contiene paquetes de monitoreo como es el caso de bssid, airodump para los “handshakes” y el Aireplay para el envío de paquetes de datos a la dirección de la máquina víctima y obtener el bsssid y otros datos útiles; por otro lado como se ha mencionado el uso de Aircrack-ng, en conjunto con herramientas complementarias, podrían incluso quebrantar al protocolo de seguridad más actual, el WPA3. Cabe resaltar que la herramienta Aircrack-ng además de utilizarse en una PC o laptops, es compatible por móviles como es el caso de dispositivos Android.

En resumen, con la herramienta Aircrack-ng con códigos predefinidos y algunas otras técnicas de penetración, son capaces de generar una degradación adecuada en los protocolos de seguridad; por lo tanto, sigue siendo motivo de seguir con investigaciones enfocadas a las vulnerabilidades y amenazas dentro de las comunicaciones WLAN.

Para el uso adecuado de esta herramienta, es necesario primeramente establecer el sistema operativo que se va a utilizar, en este caso se hace uso del sistema operativo Kali Linux, instalado de manera nativa en una PC. Posteriormente es necesario el uso de un adaptador de red Wi-Fi, esto con el propósito de establecer el dispositivo el modo de inyección y el modo monitor, este último permite la captura de datos a través de la red; cabe mencionar que no todas las tarjetas de red o adaptadores son compatibles con estas funciones, por lo que es muy probable que el adaptador de fábrica en un equipo de cómputo no sea la más adecuada para realizar este tipo de ejecuciones.

En este caso, se utiliza un adaptador de red Alfa AWUS036NHA con un Chipset Atheros, ya que además de ofrecer el modo inyección y monitor, este tipo de adaptadores son muy compatibles con Kali. En la figura 1 se muestra un ejemplo de este tipo de adaptador

Figura 1. Tarjeta inalámbrica Alfa AWUS036NHA

Una vez que ya se tiene la tarjeta inalámbrica seleccionada, se procede a conectarla en el puerto USB del equipo huésped; esta será reconocida automáticamente por el equipo; es importante mencionar que se debe de seleccionar el hardware en las configuraciones de red, para que este pueda ser utilizado, al momento de utilizar la herramienta. Para visualizar el estado de las tarjetas de red, es necesario abrir la consola de Kali Linux y utilizar el comando iwconfig; en la figura 2 se muestra una captura del resultado de utilizar este comando.

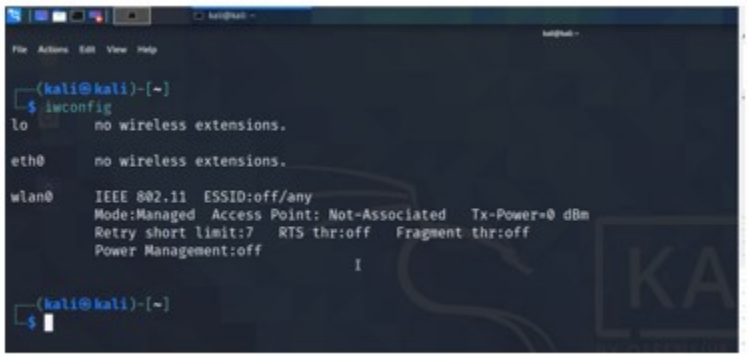

Figura 2. Comando iwconfig.

Como se muestra en la imagen, hay que identificar la tarjeta de red, por lo general este suele ser el wlan0, también se tiene que identificar el modo en el que está, como se puede observar está en modo administrativo o “Managed”, por lo que es necesario ponerlo en modo monitor.

Una vez que se verifica el tipo de tarjeta, es importante ejecutar el comando sudo airmon-ng check kill, esto para obtener los privilegios de raíz o de root, y con la herramienta airmon-ng se verifica si hay procesos que puedan generar conflictos, y si existen los elimina; esto es necesario para que Aircrack-ng, pueda funcionar adecuadamente. Cómo ya se dijo es necesario tener la tarjeta de red en modo monitor, esto puede ser logrado con el comando sudo airmon-ng start wlan0; es importante tener en cuenta que no todas las tarjetas llevan ese nombre, por lo que es importante verificar el nombre de la tarjeta que se pondrá en modo monitor.

Una vez que la tarjeta está en modo monitor, es necesario verificarla nuevamente con el comando iwconfig. En la figura 3 se puede mostrar el procedimiento de lo antes mencionado; también se puede verificar el estado del modo de la tarjeta con el comando airmon-ng. Cabe resaltar que una vez que se pasa a modo monitor el nombre de la tarjeta tendrá un sufijo -mon, por lo que en nuestro caso será wlan0mon.

Figura 3. Comprobación del modo monito en la tarjeta de red.

Estando en modo monitor se realiza la búsqueda y descubrimiento de puntos de acceso, por lo que es importante tomar en cuenta únicamente el punto de acceso de interés; esto es logrado con el

comando sudo airodump-ng wlanmon. En la figura 4 puede observarse la lista de los puntos de acceso o redes inalámbricas disponibles, donde se puede visualizar su BSSID o direcciones MAC, así como el tipo de cifrado que utilizan.

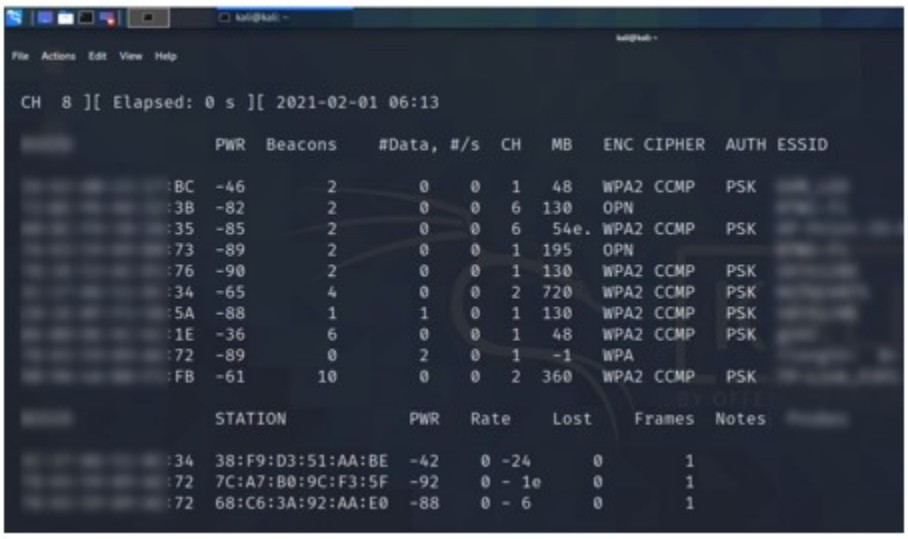

Figura 4. Lista y especificaciones de redes inalámbricas.

Teniendo la lista es necesario tener la red inalámbrica objetivo y revisando las especificaciones de cada una de estas, en especial número de canal y el BSSID; (estas son necesarias para futuros procedimientos). Se puede hacer uso del comando sudo airodump-ng wlan0mon -d número_de_MAC, para visualizar la lista de dispositivos conectados a esa red inalámbrica; por lo que se puede hacer una prueba conectado un dispositivo al punto de acceso (módem).

Posteriormente, es necesario almacenar los datos transmitidos en un archivo .cap, esto es necesario para poder hacer un análisis de los datos en otra herramienta conocida como WireShark, dicho archivo lleva por nombre hack1; por lo que para lograr esto, es necesario hacerlo con el siguiente comando: sudo airodump-ng -w hack1 -c #de canal –bssid Nombre_de_dirección_MAC wlan0mon. Ejecutando esto, es necesario abrir una segunda ventana de consola para ejecutar otro comando que desautentique al cliente de red, esto es logrado con el comando sudo aireplay-ng –deauth 0 -a Nombre_de_dirección_MAC, en este caso el valor 0, significa que no se va a detener la cantidad de desautenticaciones utilizadas en ese punto de acceso. Al realizar esto, los dispositivos conectados al punto de acceso serán desconectados y tratarán de conectarse nuevamente a este; por otro lado, esto ayudará a capturar el protocolo de enlace WPA (este se muestra en la primera consola), una vez logrado esto se detiene el proceso de la segunda consola (Control + C).

Realizado este procedimiento, también se ha generado el archivo hack1.cap, en el cual se ha guardado diversa información de autentificación entre el punto de acceso y el dispositivo conectado a este, durante el “handshak”. En la figura 5, puede observarse los archivos que se generan.

Figura 5. Archivo .cap

Teniendo el archivo anterior es necesario abrirlo en un analizador de protocolos, en este caso es el ya mencionado Wireshark, que ya se ha mencionado anteriormente, esto con el propósito de ser analizado su contenido, en su búsqueda de esta herramienta se busca mediante la palabra “eapol” (en inglés Extensible Authentication Protocol). En la figura 6, se muestra el despliegue de los archivos de interés.

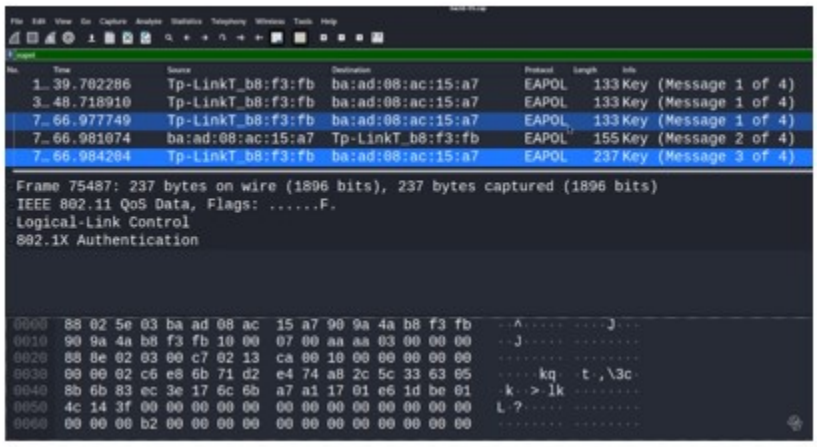

Figura 6. Búsqueda del protocolo de autenticación en Wireshark

Teniendo esto se busca los mensajes de autenticación entre un dispositivo conectado al punto de acceso; sin embargo, dicho mensaje se encuentra encriptado bajo el protocolo de comunicación WPA, por lo que ese mensaje será el que se va a descifrar. Es importante tomar en cuenta que para realizar esto se necesitan 2 tarjetas inalámbricas, una la tarjeta Alfa que va estar en modo monitor y otra que será necesaria para conectarse a la red; esto debido a que al ponerlo en modo monitor la tarjeta se quedará sin conexión al punto de acceso.

Después de tener este archivo y analizar el intercambio de los mensajes, se coloca la tarjeta Alfa nuevamente en modo administrativo, esto puede ser logrado con el comando stop wlan0mon. Finalmente para descifrar el mensaje que viene incluido en el archivo.cap, se utiliza el comando de la herramienta aircrack-ng, haciendo uso también de una lista de palabras por nombre rockyou.txt, almacenada en /usr/share/wordlists/rockyou, cabe mencionar que dicha lista está por defecto incluida en el sistema operativo (está lista debe ser descomprimida previamente antes de su uso); dicha lista contiene diversas palabras o frases comunes que los usuarios suelen utilizar como contraseñas de sus módems.

Finalmente, en consola se pone el siguiente comando aircrack-ng Nombre del archivo_,cap -w Dirección_del_archivo_listado_de_palabras, en este caso es aircrack-ng hack1-01.cap -w /usr/share/wordlists/rockyou.txt. Siendo así esto genera el resultado de la contraseña el cual es “hellohello”. En la figura 7 se muestra el resultado de esto.

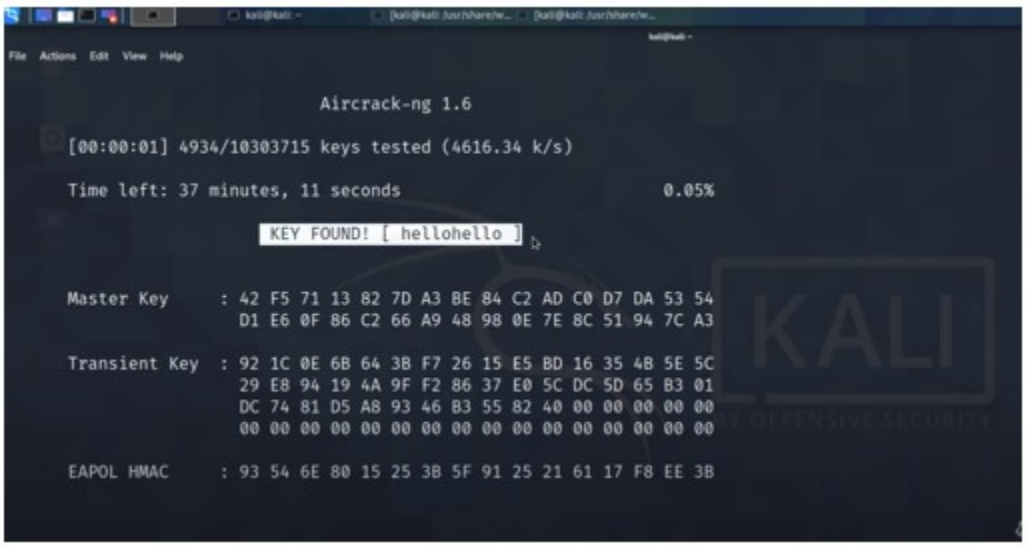

Figura 7. Resultado del cifrado de la herramienta aircrack

VI. Conclusiones

En este documento se hace un análisis de los protocolos de seguridad WEP, WPA, WPA2 Y WPA3 de las redes inalámbricas WLAN, también conocidas también como Wi-Fi; así como las investigaciones realizadas para romper los protocolos previos al WP3 y los posibles procedimientos para quebrantar el WP3, en conjunto con la herramienta Aircrack-ng. Adicionalmente, con esta herramienta se desarrolló un ejemplo sencillo para quebrantar la seguridad de la contraseña de un punto de acceso como un módem o un router; por lo que esto puede ser logrado con la herramienta Aircrack-ng, el uso de Kali Linux, una tarjeta inalámbrica Alfa, una lista de palabras y la herramienta de esnifeo Wireshark. Por último, es sencillo realizar este tipo de procedimiento; sin embargo, solo funciona para contraseñas que coincidan en la lista de palabras a utilizar.

Referencias

1. Doyle, C. (**2002**). *CRS Report for Congress Received through the CRS Web The USA PATRIOT Act : A Sketch.* 3162.

2. Vanhoef, M., & Ronen, E. (**2020**). *Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In 2020 IEEE Symposium on Security and Privacy (SP)* (pp. 517-533). IEEE.

3. Dahiya,
Security Issues and Solutions in Wi-Fi.

4. Reddy, B. I., & Srikanth, V. (**2019**). *Review on wireless security protocols (WEP, WPA, WPA2 & WPA3). International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* 28-35.

5. Singh, R., & Sharma, T. P. (**2019**). *Security in Wireless Local Area Networks (WLANs). Computer and Network Security,* 51.

6. Aneja, A., & Sodhi, G. (**2016**).

A Study of Security Issues Related With Wireless Fidelity (WI-FI). /em>*)International Journal of Computer Science Trends and Technology (IJCST),* 4(2), 346-350.

7. Lounis, K., & Zulkernine, M. (**2020**). *Attacks and defenses in short-range wireless technologies for IoT. IEEE Access,* 8, 88892-88932.

8. Vanhoef, M. (**2017**). *Key Reinstallation Attacks: Breaking the WPA2 Protocol. In Black Hat Europe Briefings,* Location: London, UK.