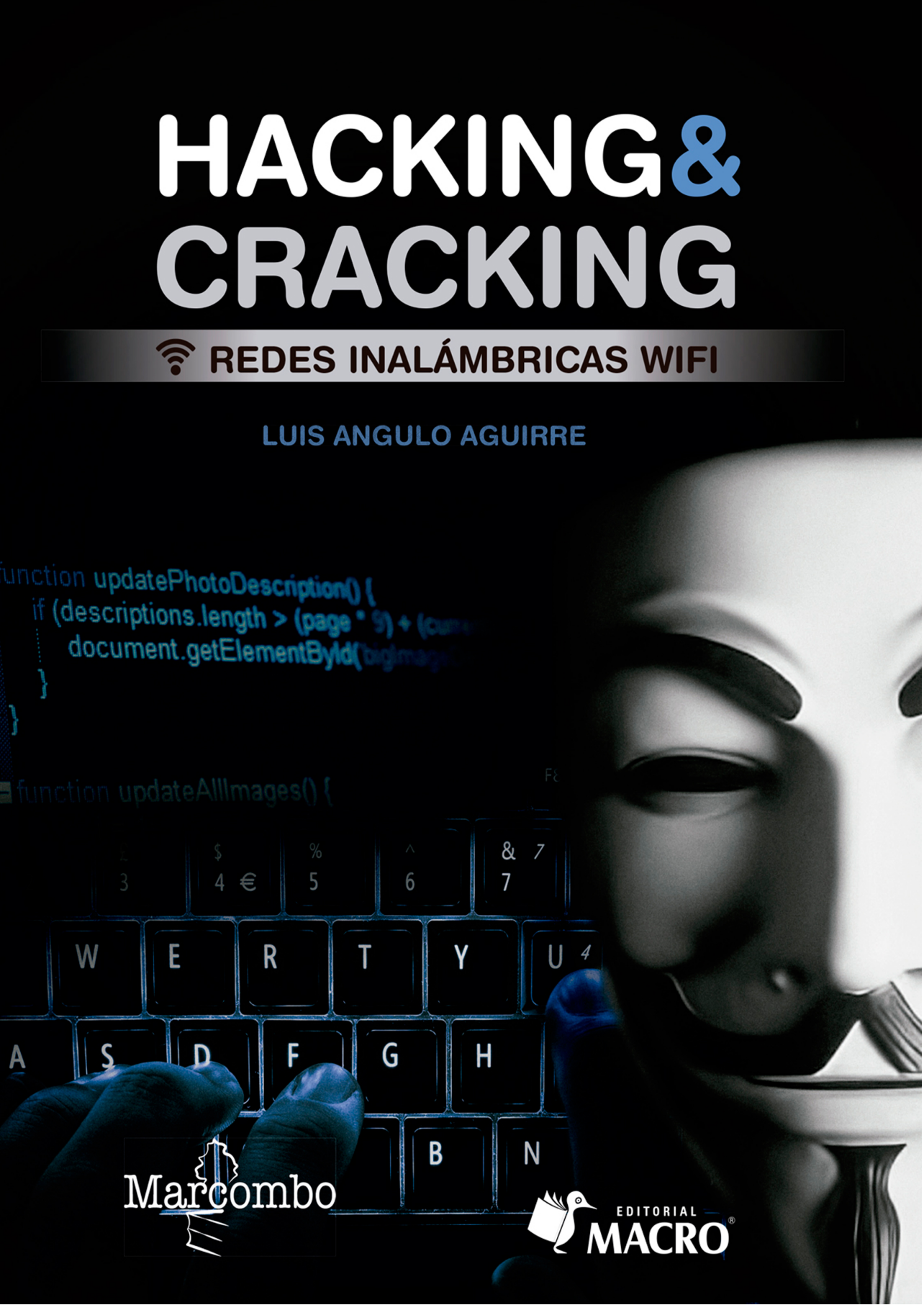
HACKING & CRACKING

REDES INALÁMBRICAS WIFI

LUIS ANGULO AGUIRRE



Marcombo
EDITORIAL MACRO®

HACKING & CRACKING

Redes inalámbricas wifi

Luis Angulo Aguirre

Marcombo

EDITORIAL MACRO

Hacking & cracking
Redes inalámbricas wifi

Primera edición: Empresa Editora Macro EIRL, Lima – Perú, noviembre de 2018

Primera edición: MARCOMBO, S.A. 2019

ISBN: 978-84-267-2695-7

D.L.: B-7987-2019

Impreso en Servicepoint

Printed in Spain

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).

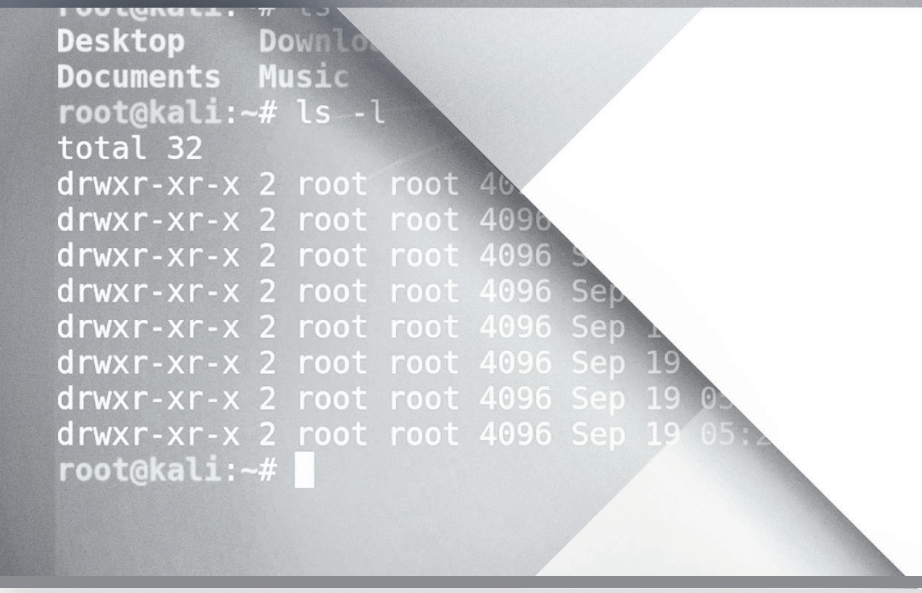
Actualmente, es docente en el Centro de Extensión y Proyección Social (CEPS) de la Universidad Nacional de Ingeniería (UNI) y en la Universidad Tecnológica del Perú (UTP). También trabaja como consultor independiente de empresas públicas y privadas.

Ha sido director general del Instituto Perú Pacífico y del Instituto Unicenter. Asimismo, trabajó 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

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 o aeropuertos), zonas wifi gratuitas al aire libre y en la mayoría de los hogares.

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

Hacking y cracking, *Redes inalámbricas wifi* 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 exitosa distribución de seguridad de Kali Linux), analizando cada fase desde la planificación inicial hasta el informe final. Aparte de explicar la teoría básica de la seguridad inalámbrica (protocolos, vulnerabilidades y ataques), centra sus esfuerzos en enseñar sus aspectos prácticos, utilizando las valiosas herramientas gratuitas y de código abierto que proporciona 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 trata sus cuatro fases principales centrándose 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 un portátil con Kali Linux» muestra los diferentes métodos de instalación de la distribución Kali Linux y, también, explica 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» analiza 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, explica 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 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 necesita un portátil 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 quién 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.

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 a 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 analizará, de modo general, las principales fases para realizar un proceso de pruebas de penetración (*pentesting*), con especial atención 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 la 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 realizar acciones para las 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 centrar 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 los siguientes capítulos.

Pero antes, una analogía muy simple que relaciona los tres términos:

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


Vulnerabilidad


Exploit

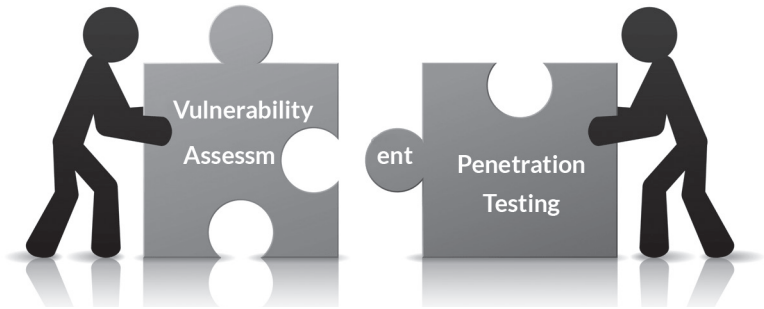

Payload

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 evaluación completa 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 para acceder al sistema 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 pueden diferenciar tres tipos:

- **Exploit local**: Para ejecutar este tipo de exploit, es necesario haber accedido previeamente 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 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 los equipos de los 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. Encender simplemente 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 una alta exigencia.

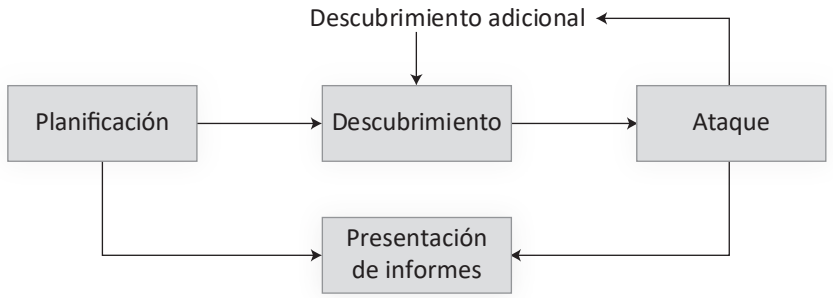
El proceso de pruebas de penetración se puede dividir en cuatro fases o etapas:

- 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].

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

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.

1.2.1 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 él, 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 establecido, el pentester deberá estimar cuánto tiempo necesita 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 contener las pruebas que realizar y definir claramente aspectos como el nivel de indemnización, el 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 que usará para la ejecución de la prueba.

Una vez que se cumplan todos los requisitos anteriores, ¡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

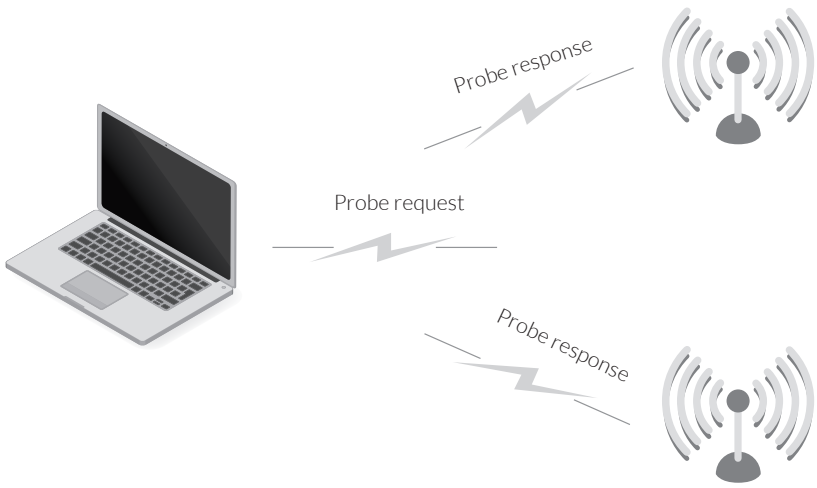
información posible sobre las redes que se encuentran en el alcance de la prueba de penetración. Esta fase también se denomina la fase de recopilación de información. Es muy importante porque define precisamente los objetivos de su prueba y permite recoger información detallada acerca de ellos y exponer sus vulnerabilidades potenciales.

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

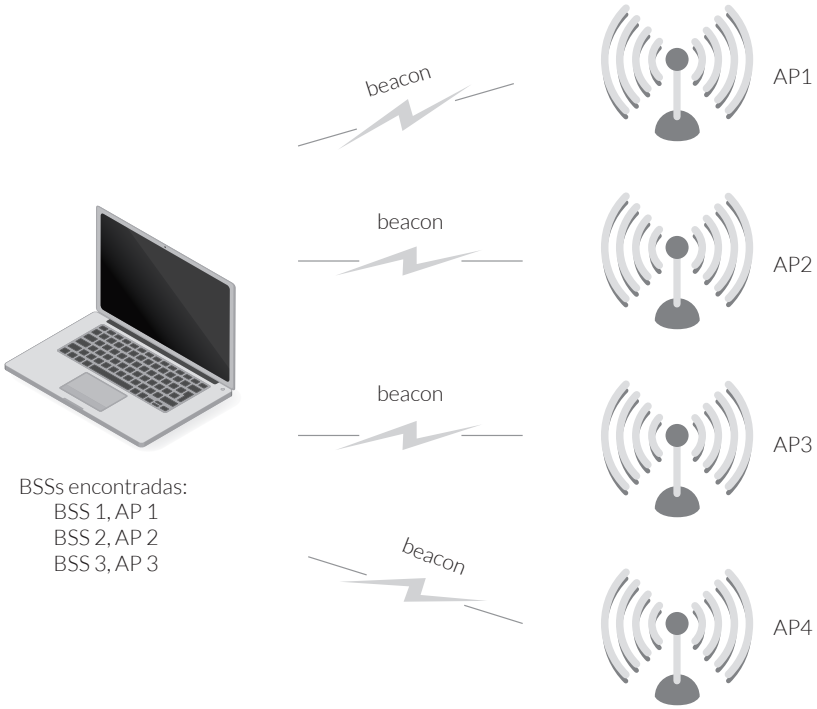
- Listado de los AP no autorizados, así como las redes visibles y ocultas en el área.
- Enumeración de los clientes conectados a las redes objetivo.
- Tipo de autenticación utilizado por las redes; céntrese en aquellas redes que están abiertas o que usan WEP y que, por lo tanto, son vulnerables.
- El 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.

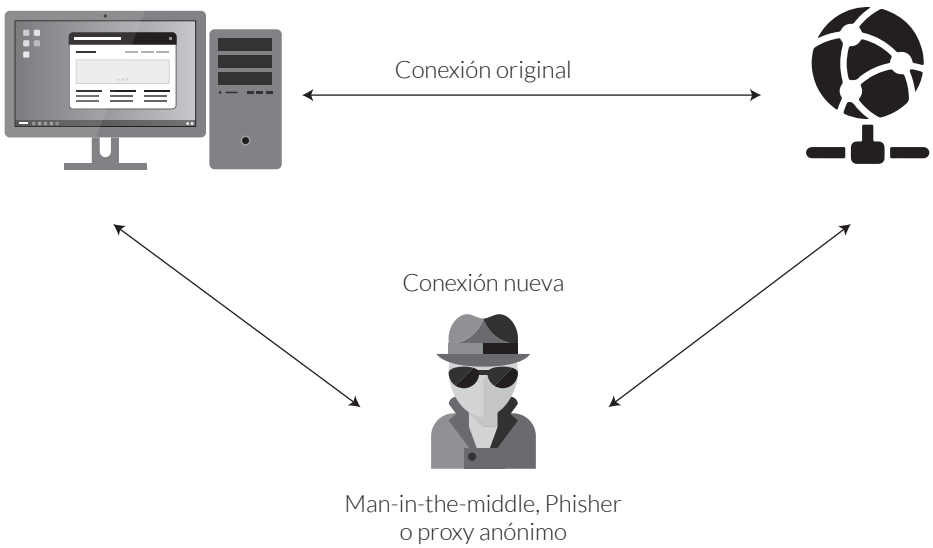
Verá más sobre escaneo inalámbrico y cómo usar las herramientas de escaneo inalámbrico incluidas en Kali Linux, como airmon, airodump y Kismet para llevar a cabo la fase de descubrimiento del pentesting inalámbrico en el capítulo 5 «Reconocimiento de WLAN».

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».