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

Jefe de edición:
Magaly Ramon Quiroz

Diseño de portada:
Fernando Cavassa Repetto

Diseño y diagramación:
Fernando Cavassa Repetto

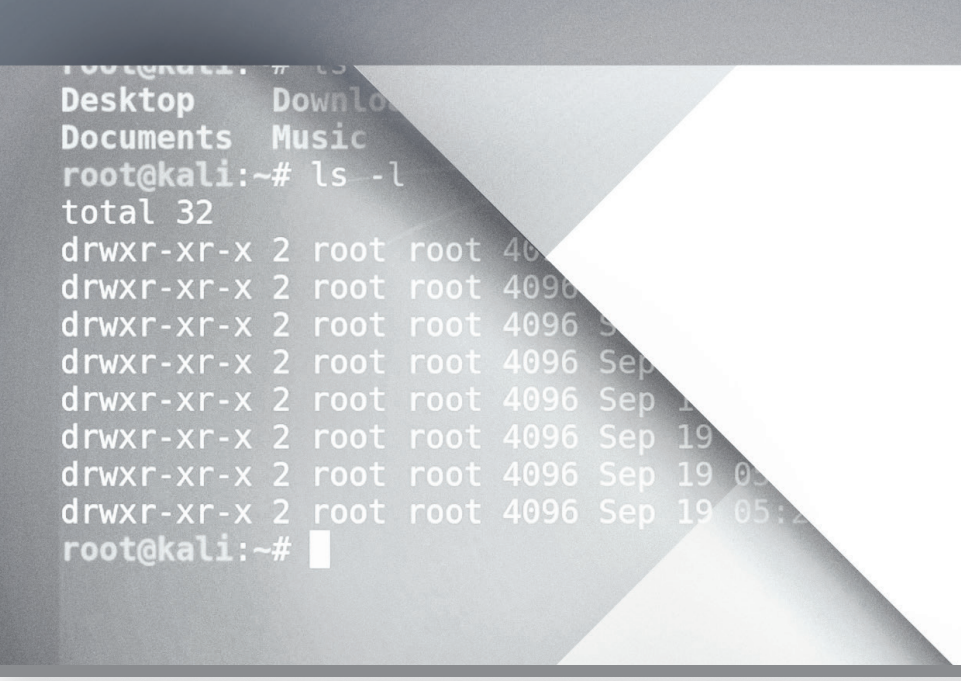
Edición a cargo de:
© Empresa Editora Macro EIRL
Av. Paseo de la República N.° 5613, Miraflores, Lima, Perú

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



Índice

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