



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.



| | |
|---|-----|
| 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 (aircrack-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 Caffé 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 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