

# Índice

<b>Prólogo .....</b>	<b>11</b>
<b>Introducción .....</b>	<b>13</b>
<b>Capítulo I</b>	
<b>Kali Linux .....</b>	<b>15</b>
<b>1. ¿Qué es Kali y Por qué elegirlo? .....</b>	<b>15</b>
<b>2. Visión global de Kali en un test de intrusión .....</b>	<b>17</b>
La auditoría interna .....	18
La auditoría externa.....	19
La auditoría web.....	19
La auditoría wireless .....	20
Análisis forense.....	20
<b>3. Trabajando con Kali.....</b>	<b>22</b>
Live-CD.....	23
Instalación en máquina física .....	25
Instalación en máquina virtual .....	29
<b>4. Paseando por Kali 2.0: Aplicaciones.....</b>	<b>32</b>
<b>5. Detección de funciones inseguras en repositorios.....</b>	<b>37</b>
Resultados y vulnerabilidad Memory Corruption.....	41
<b>6. Políticas.....</b>	<b>43</b>
Política de código abierto.....	43
Política de Marcas .....	43
Política de usuarios Root.....	43
Política de Herramientas para Pruebas de Penetración .....	44
Políticas de Servicio de Red .....	44
Políticas de Actualizaciones de Seguridad .....	44
<b>7. Kali Rolling 2017: Nuevas releases .....</b>	<b>45</b>
Kali Linux 2016.1 .....	45

Kali Linux 2016.2 .....	46
Kali Linux 2017.1 .....	46
Kali Linux 2017.2 .....	47
Historial de versiones de Kali Linux.....	47
<b>8. Kali Linux 2020 .....</b>	<b>48</b>
Kali Linux 2020.1 .....	48
Kali Linux 2020.2 .....	50
<b>9. Kali Linux en contenedores Docker.....</b>	<b>51</b>
Desplegando una imagen de Kali Linux con Docker.....	52

## Capítulo II

<b>Recogida de información .....</b>	<b>53</b>
<b>1. Introducción al Gathering .....</b>	<b>53</b>
<b>2. External Footprinting .....</b>	<b>54</b>
Active Footprinting .....	54
Passive Footprinting.....	81

## Capítulo III

<b>Análisis de Vulnerabilidades y ataques de contraseñas.....</b>	<b>89</b>
<b>1. Vulnerabilidad .....</b>	<b>89</b>
<b>2. Análisis de vulnerabilidades .....</b>	<b>91</b>
Pruebas .....	92
Validación.....	94
Investigación .....	96
<b>3. Análisis con Kali .....</b>	<b>98</b>
Nmap + NSE .....	98
OpenVAS.....	99
Nessus .....	99
Escáner activo de Burp Suite .....	102
Yersinia.....	102
Spike.....	102
<b>4. Ataques a contraseñas en Kali Linux .....</b>	<b>103</b>
Métodos de ataque.....	105
Tipos de ataque.....	106

## Capítulo IV

<b>Explotación .....</b>	<b>115</b>
<b>1. Introducción a los exploits .....</b>	<b>115</b>

Conceptos.....	116
Tipos de payloads.....	117
<b>2. Explotación en Kali .....</b>	<b>118</b>
Base de datos de exploits .....	118
Metasploit.....	120
Network Exploitation.....	134
SE Toolkit.....	142
Empire: El ave fénix de la post-explotación .....	154

## Capítulo V

### Auditoría de aplicaciones web .....159

<b>1. Introducción a las vulnerabilidades web.....</b>	<b>159</b>
<b>2. Explotación de vulnerabilidades web comunes .....</b>	<b>159</b>
Cross Site Scripting.....	160
Cross Site Request Forgery .....	166
SQL Injection .....	168
Local File Include/Path Transversal.....	172
Remote File Include .....	176
<b>3. Aplicaciones de seguridad web en Kali .....</b>	<b>177</b>
Aplicaciones Proxy .....	177
Aplicativos para fuzzing .....	179
Escáneres de vulnerabilidades web.....	182
Explotación de bases de datos.....	184
Identificación de CMS.....	186
Identificación de IDS/IPS.....	188
Indexadores web.....	189
Conclusiones .....	191

## Capítulo VI

### Ataques Wireless .....193

<b>1. Tipos de ataques inalámbricos .....</b>	<b>193</b>
Definiciones.....	195
<b>2. Herramientas Wireless en Kali .....</b>	<b>195</b>
Requisitos.....	196
La suite air*.....	197
Evasión de configuraciones básicas de seguridad.....	200
Captura e interpretación de tráfico abierto .....	203
Hacking WEP.....	206
Hacking WPA & WPS.....	210

## Capítulo VII

<b>Forense con Kali.....</b>	<b>215</b>
<b>1. Introducción al análisis forense.....</b>	<b>215</b>
<b>2. Captura de evidencias.....</b>	<b>216</b>
<b>3. Tratamiento.....</b>	<b>219</b>
Proof Of Concept: Análisis de una imagen.....	220
<b>4. Forense de red.....</b>	<b>226</b>
Captura de evidencias en red.....	226
Fingerprint.....	227
Proof Of Concept: Los grupos hacktivistas y la red.....	229
<b>5. Forense de RAM.....</b>	<b>231</b>

## Capítulo VIII

<b>Ataques a redes .....</b>	<b>239</b>
<b>1. Herramientas en Kali.....</b>	<b>239</b>
<b>2. Envenenamiento de redes .....</b>	<b>242</b>
Ataques a IPv4 .....	242
Ataques a IPv6 .....	242
VOIP.....	243
<b>3. Man In The Middle .....</b>	<b>243</b>
ARP Spoofing.....	243
DNS Spoofing .....	249
SSL Strip .....	251
Hijacking.....	252
IPv6 .....	252
Network Packet Manipulation: Modificando paquetes al vuelo.....	256

## Capítulo IX

<b>Windows Resources &amp; Binaries en Kali Linux .....</b>	<b>261</b>
<b>1. Windows Resources &amp; Binaries .....</b>	<b>261</b>
<b>2. Ejemplos básicos .....</b>	<b>262</b>
<b>Índice alfabético .....</b>	<b>265</b>
<b>Índice de imágenes .....</b>	<b>269</b>