Índice

Prólogo 11

Introducción 13

Capítulo I
Kali 2.0 15

1. ¿Qué es Kali y Por qué elegirlo? 15

2. Visión global de Kali en un test de intrusión 17
La auditoría interna 18
La auditoría externa 19
La auditoría web 19
La auditoría wireless 20
Análisis forense 20

3. Trabajando con Kali 22
Live-CD 23
Instalación en máquina física 25
Instalación en máquina virtual 29

4. Paseando por Kali 2.0: Aplicaciones 32

5. Detección de funciones inseguras en repositorios 37
Resultados y vulnerabilidad Memory Corruption 41

6. Políticas 43
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

7. Kali Rolling 2017: Nuevas releases 45
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

Capítulo II
Recogida de información 49

1. Introducción al Gathering 49

2. External Footprinting 50
Active Footprinting 50
Passive Footprinting 77

Capítulo III
Análisis de Vulnerabilidades y ataques de contraseñas 85

1. Vulnerabilidad 85

2. Análisis de vulnerabilidades 87
Pruebas 88
Validación 90
Investigación 92

3. Análisis con Kali 94
Nmap + NSE 94
OpenVAS 95
Nessus 95
Escáner activo de Burp Suite 98
Yersinia 98
Spike 98

4. Ataques a contraseñas en Kali Linux 99
Métodos de ataque 101
Tipos de ataque 102

Capítulo IV
Explotación 111

1. Introducción a los exploits 111
Conceptos 112
Tipos de payloads 113

2. Explotación en Kali 114
Base de datos de exploits 114
Metasploit 116

Network Exploitation 130
SE Toolkit 138

Capítulo V
Auditoría de aplicaciones web 145
1. Introducción a las vulnerabilidades web 145
2. Explotación de vulnerabilidades web comunes 145
Cross Site Scripting 146
Cross Site Request Forgery 152
SQL Injection 154
Local File Include/Path Transversal 158
Remote File Include 162
3. Aplicaciones de seguridad web en Kali 163
Aplicaciones Proxy 163
Aplicativos para fuzzing 165
Escáneres de vulnerabilidades web 168
Explotación de bases de datos 170
Identificación de CMS 172
Identificación de IDS/IPS 174
Indexadores web 175
Conclusiones 177

Capítulo VI
Ataques Wireless 179
1. Tipos de ataques inalámbricos 179
Definiciones 181
2. Herramientas Wireless en Kali 181
Requisitos 182
La suite air* 183
Evasión de configuraciones básicas de seguridad 186
Captura e interpretación de tráfico abierto 189
Hacking WEP 192
Hacking WPA & WPS 196

Capítulo VII
Forense con Kali 201
1. Introducción al análisis forense 201
2. Captura de evidencias 202

3. Tratamiento 205
Proof Of Concept: Análisis de una imagen 206
4. Forense de red 212
Captura de evidencias en red 212
Fingerprint 213
Proof Of Concept: Los grupos hacktivistas y la red 215
5. Forense de RAM 217

Capítulo VIII
Ataques a redes 225
1. Herramientas en Kali 225
2. Envenenamiento de redes 228
Ataques a IPv4 228
Ataques a IPv6 228
VOIP 229
3. Man In The Middle 229
ARP Spoofing 229
DNS Spoofing 235
SSL Strip 237
Hijacking 238
IPv6 238
Network Packet Manipulation: Modificando paquetes al vuelo 242

Índice alfabético 247

Índice de imágenes 251