

Índice

Introducción	13
Objetivos del Libro	15
1. Como leer el Libro.....	15
PARTE I - Historia del sistema operativo y su kernel.....	15
PARTE II - Sandbox del sistema.....	16
PARTE III – Herramientas y utilidades. Hacking en Mac	16
PARTE IV – Hacking y explotación	16
PARTE V – Hardening y seguridad	16
2. Conocimiento base.....	16
Fase de un test de intrusión.....	17
Capítulo I	
Mac OS y OS X	19
1. System Software	19
2. Mac OS y OS X.....	21
2.1 macOS Sierra	25
2.2 Arquitectura del OS.....	26
2.3 Darwin.....	27
2.4 Mach.....	28
2.5 BSD.....	28
2.6 Networking.....	28
2.7 Sistema de archivos.....	29
2.8 I/O Kit	29
3. Cronología e histograma.....	29
Capítulo II	
System Integrity Protection (SIP).....	31
1. Protección de los archivos del sistema	33



2. xattr - Atributos de los archivos	33
3. Protección contra procesos en ejecución (Runtime Protection).....	37
4. csrutil - Habilitar y Deshabilitar SIP (<i>Rootless</i>).....	38
5. Deficiencias de seguridad en SIP a.k.a Rootless	41

Capítulo III

Herramientas hacking	43
1. Herramientas del sistema	43
1.1 Utilidad de Red	43
1.2 Diagnóstico Inalámbrico – Auditando la Wi-Fi	51
1.3 DNS-SD	61
1.4 Isof.....	63
1.5 Netcat	65
1.6 TCPDUMP	67
2. Herramientas de terceros.....	72
2.1 Wireshark	72
2.2 CPA – Cocoa Packet Analyzer	75
2.3 WebReaver	77
2.4 Proxy - Web Interception Proxy	80

Capítulo IV

Command line tools	87
1. Instalación	87

Capítulo V

MacPorts	91
1. Características e instalación	92
2. Ports.....	93
3. MacPorts en profundidad.....	96

Capítulo VI

Homebrew.....	101
1. Características e instalación	101
2. Homebrew en profundidad.....	104
2.1 Estructura, repositorios y creación de fórmulas	106



Capítulo VII

K0sasp	111
1. Características e instalación	111
2. K0sasp en profundidad	115

Capítulo VIII

Ataques a nivel de red.....	121
1. Nmap	121
1.1 Sondeo de red	122
1.2 Scripts de nmap – NSE (Nmap Scripting Engine).....	124
2. Nessus	127
2.1 De donde obtener Nessus	128
2.2 Instalación	128
2.3 Primer escaneo de vulnerabilidades	128
3. John the ripper – Cracking de Passwords	133
3.1 Instalación	134
3.2 Métodos de crackeo.....	136
4. Metasploit.....	140
4.1 Prueba de Concepto: Explotación de vulnerabilidades.....	143

Capítulo IX

Ataques a nivel de aplicaciones web.....	149
1. Navegadores y extensiones.....	149
2. Burp Suite	155
2.1 Prueba de concepto: Enumeración de usuarios.....	158
3. Dirbuster	165
4. OWASP ZAP: Enumeración de directorios	168
5. MITM Proxy.....	172
5.1 Prueba de Concepto: Capturando tráfico HTTP/S	175
6. SQLmap	179
6.1 Prueba de concepto: SQL Injection Blind y volcado de las bases de datos	181
7. Weevely.....	188
7.1 Generando un Backdoor.....	188
7.2 Conectando a la Shell y atacando al objetivo.....	190
8. Fimap.....	194
8.1 Ataques LFI y RFI.....	194



8.2 Prueba de concepto: LFI 197

9. Wapiti 198

Capítulo X

Ataques a nivel Wi-Fi 203

1. Aircrack-ng suite 206

1.1 airbase-ng 207

1.2 Aircrack-ng 208

1.3 airdecap-ng 208

1.4 aireplay-ng 209

1.5 airmon-ng 209

1.6 airodump-ng 210

1.7 aircrack-ng 210

1.8 airtun-ng 211

1.9 packetforge-ng 211

10 Prueba de concepto: Obtención de claves WPA/WPA2-PSK 211

2. Airport 215

3. KisMAC 216

Capítulo XI

Scripts y aplicaciones 221

1. Ofuscación de código malicioso en aplicaciones 221

2. Desempaquetado de aplicaciones 230

Capítulo XII

Análisis forense 235

1. Osx auditor 237

2. Volatility 241

3. Otras 245

3.1 Console utility 245

3.2 The Sleuth Kit (TSK) 249

3.3 Autopsy (versión 2) 250

3.4 Rkhunter 251

3.5 Disk Arbitrator 252

Capítulo XIII

Hardening y Seguridad 255



1. Firmware	255
2. Seguridad y Privacidad	258
2.1 Gatekeeper.....	258
2.2 Filevault.....	260
2.3 Firewall	263
2.4 Spotlight	276
2.5 Localización	282
3. Handoff	283
4. Borrado seguro	284
5. Terminal	287
6. Metadatos .DS_Store	289
7. Cifrado de imágenes de disco	291
8. Contraseñas seguras en OS X y macOS	292
9. Llavero (Keychains)	294
10. Bloqueo de pantalla y modo reposo	297
Anexos	299
Anexo I - Macintosh System Software	299
Anexo II - Listado de herramientas.....	303
Anexo III – Códigos en peticiones http.....	307
Referencias	311
Capítulo 1 – Mac y OS X.....	311
Capítulo 2 – System Integrity Protection	312
Capítulo 3 – Herramientas hacking.....	312
Capítulo 4 – Command Line Tools	313
Capítulo 5 – MacPorts.....	313
Capítulo 6 – Homebrew	313
Capítulo 7 – K0SASP.....	313
Capítulo 8 – Ataques a nivel de red	314
Capítulo 9 – Ataques a nivel de aplicaciones web	314
Capítulo 10 – Ataque a nivel Wi-Fi y radiofrecuencia.....	315
Capítulo 11 – Scripts y aplicaciones	315
Capítulo 12 – Análisis forense	315
Capítulo 13 – Hardening y seguridad.....	315
Índice alfabético	317
Índice de imágenes	321



