

Índice

Capítulo I

Identificando dispositivos iOS.....13

1. Identificación de dispositivos Apple..... 13

Descubriendo dispositivos iOS en la misma red local 13

Por los puertos TCP abiertos 16

Utilizando Shodan 17

2. Identificar si un usuario utiliza un dispositivo iOS 17

Por el sistema de mensajería iMessage 18

Por los clientes de redes sociales para iOS 18

Por el User-Agent del navegador 19

El cliente de correo de iOS..... 20

Imágenes publicadas 21

Compartición de Internet por Wi-Fi..... 22

No-tech hacking 22

Capítulo II

Ataques locales (iPhone Local Tricks)23

1. Introducción..... 23

Reconocer el modelo de dispositivo en una inspección preliminar 24

Los números de serie y el IMEI 27

Códigos de marcado especiales..... 30

2. Adivinar el passcode de un iPhone..... 30

Shoulder Surfing..... 31

Shoulder Surfing con iSpy 31

Reconocimiento de la complejidad del passcode 32

Saber si tiene Wi-Fi o no 32

Compartir Internet..... 34

El passcode en la grasa de la superficie 34

Borrado de datos con número de passcodes erróneos 35

3. Previsualización de mensajes por pantalla..... 35



4. Desbloqueo de la pantalla de inicio sin conocer el passcode por medio de bugs .38	
CVE-2012-0644: El desbloqueo por la SIM hasta iOS 5.0.1	38
CVE-2011-3440: El desbloqueo de la Smart Cover en iPad 2 con iOS 5	39
CVE-2010-4012: El desbloqueo por llamada de emergencia en iOS 4.0 y 4.1	40
El bug con Activator y un iPhone iOS 4.3.3 con Jailbreak	41
CVE-2013-0980: Saltar el código de la pantalla de bloqueo en iOS 6.1 a iOS 6.1.2	42
Saltarse el código de desbloqueo en iPhone 3GS y en iPhone 4 con iOS 6.1.3	42
Un bug en LockDown Pro para iPhone con Jailbreak	43
Bug Sim Lock Screen Display Bypass	43
Bugs en iOS 7 para Bypass	44
Deshabilitar Siri pero no Voice Control	46
Bypassear Touch ID	46
Utilizando Force Touch en iOS 9.3.1	47
5. Accediendo a las fotos de un iPad por las opciones del marco de fotos.....47	
Accediendo a las fotos de un iPhone con iOS 5.X cambiando la fecha.....	48
6. Explorando la agenda usando el control de voz49	
Manejando el teléfono con Siri en iOS 5 e iOS 6 con iPhone 4S o iPhone 5	50
CVE-2012-3750: Acceso a los códigos de PassBook	52
7. Otras manipulaciones en local53	
Juice Jacking	53
Más acciones con el terminal bloqueado que pueden ser útiles.....	54
El equipo pareado o el dispositivo con Jailbreak	55
8. Creación de un laboratorio.....56	
9. Nuevo Passcode en iOS 957	
10. Hackear Siri con RF.....57	
11. NAND Mirroring: El caso de San Bernardino y el FBI.....58	
12. Siri en iOS 10: Privacidad59	

Capítulo III

Jailbreak61	
1. Requisando el dispositivo.....61	
2. Accediendo a los datos del sistema63	
Sacando el passcode con Gecko iPhone Toolkit	65
3. ¿Qué es Jailbreak?68	
Tipos de Jailbreak.....	68
Herramientas de Jailbreak	70
Herramientas de Jailbreak por DFU Pwnd.....	71
El Unlock de un dispositivo	72



4. Realizar el Jailbreak	72
RedSn0w con un dispositivo con chip A4 e iOS 6.....	73
Custom bundle de OpenSSH.....	76
Jailbreak a terminales A5 con iOS 5.X usando Absinthe.....	76
Jailbreak a iOS 6 en dispositivos con chip A4, A5 y A6.....	77
Jailbreak para iOS 7	77
Jailbreak para iOS 8	79
Jailbreak para iOS 9	79
Jailbreak para iOS 10	80
5. Acceso a datos en el dispositivo	81
6. Revertir el Jailbreak.....	82
7. Fakes en los Jailbreak	83

Capítulo IV

Atacando el backup.....	85
1. Introducción.....	85
2. Localización de los ficheros del backup.....	86
3. Estructura de un backup de iOS.....	87
4. Crackear la contraseña de cifrado del backup de Apple iTunes.....	89
5. Descifrado de los ficheros del backup de Apple iTunes.....	91
6. Análisis de ficheros de un backup de iOS.....	93
Tipos de Ficheros principales.....	93
Análisis de Ficheros SQLite.....	95
Análisis de ficheros Plist.....	97
Análisis de binary cookies	98
Análisis del Keychain	101
7. El backup en Apple iCloud	102
8. iCloud y el descifrado de datos.....	103
9. Crackear contraseñas del backup de iOS 10	104

Capítulo V

iPhone DataProtection	107
1. Introducción.....	107
2. Montando iPhone DataProtection	108
3. Clonando un iPhone bit a bit con iPhone DataProtection	109
4. Accediendo con HFS.....	110



5. Sacando claves con iPhone DataProtection.....	112
Preparando el entorno	113
Passcode	116
KeyChain.....	117
Caché en Safari	119

Capítulo VI

Análisis forense de datos de un terminal iOS con Oxygen Forensic Suite 121

1. Introducción.....	121
Análisis de datos de un dispositivo iOS con Oxygen Forensic Suite	121
El proceso de captura de datos de un iPhone	123
2. Información en los dispositivos	125
La línea temporal de un dispositivo	125
Análisis de contactos.....	127
Geolocalización de datos extraídos.....	129
Mensajes de comunicación	130
Registro de eventos	131
El calendario.....	132
Web browser & cache analyzer (Navegador web / analizador caché).....	132
Google Services	132
Yahoo! Services.....	133
Aplicaciones de redes sociales	133
Dropbox.....	134
Diccionarios	134
Aplicaciones.....	135
Aplicaciones de malware y spyware.....	136
Explorador de archivos	136
Logs de actividad del dispositivo iOS.....	137
Generación de informes	138
3. Conclusión y soporte	138

Capítulo VII

Malware en iOS.....141

1. Introducción.....	141
2. Troyanos en la AppStore.....	142
3. Troyanos sin AppStore	146
Troyanos con Provisioning Profiles	146
Construyendo un malware.....	147
Distribución del malware	159



4. Troyanos con Jailbreak	172
5. Evolución del malware en iOS: Complejidad++	182
El ransom llegó a iOS	182
Xsser mRAT	183
WireLurker: La revolución en iOS.....	184
KeyRaider	186
XCodeGhost: Infectando apps desde XCode.....	188
YiSpecter: Malware con y sin Jailbreak.....	190
AceDeceiver.....	190
SideStepper	191

Capítulo VIII

Ingeniería social y client-side en iOS	193
1. Ingeniería social	193
2. La famosa address bar de Safari	195
¿Qué es el address bar spoofing?	196
Historia en iOS y OS X de este tipo de vulnerabilidades	196
¿Qué es el address bar spoofing?	196
Historia en iOS y OS X de este tipo de vulnerabilidades	196
3. PoC: Address bar spoofing en iOS	198
Configuración y ejecución.....	199
4. PoC: Personalizando el ataque	201
Manos a la obra	201
5. Herramientas que ayudan a la ingeniería social	205
SET: Social-Engineer Toolkit.....	206
6. PoC: Hacking con Twitter	207
7. PoC: Hacking con Gmail	210
8. PoC: Hacking con Facebook	211
9. El correo electrónico en iOS	212
10. Mobile Pwn2Own	213
11. PoC: Command Injection a través de Mail en iOS	214
12. Bug en Mail en iOS 8.3	217
13. El caso del Celebgate y Apple iCloud	218

Capítulo IX

Ataques en redes Wi-Fi	219
1. Conexión inalámbrica en iOS	219



La conexión de los dispositivos y los Rogue AP	220
PoC: Suplantación de punto de acceso.....	222
2. Sniffing.....	223
Conexión a una red Wireless abierta.....	223
Conexión a una red Wireless de tipo WEP.....	224
PoC: Hijacking a tuenti en redes Wireless	225
3. Man in the middle	228
ARP Spoofing.....	228
PoC: ARP Spoofing sobre iPhone con cain en redes WEP	232
HTTP-s: CA Fake.....	234
SSLSniff y SSLStrip	237
PoC: SSLStrip en iOS	239
PoC: DOS a los dispositivos iOS en la Wi-Fi	240
IPv6 ICMP Redirect.....	241
4. VPN en iOS	243
Conexiones PPTP.....	245
MSCHAPv2	245
PoC: Crackeo de VPN en iOS con PPTP y MSCHAPv2.....	246
5. Downgrade en red: Ataques a iOS 5 hasta 7.1.1	248
6. Bypass a OpenSSL Certificate Pinning en apps	249
7. EyeBalls	252
8. Brickear un iOS en red WiFi	253
Capítulo X	
JavaScript Botnets	257
1. Rogue AP: Puntos de acceso Wi-Fi falsos.....	257
2. Preparando el entorno Linux	259
3. Configurando el punto de acceso	261
4. Ataque de infección de ficheros JavaScript.....	266
5. Prevención y desinfección	273
Capítulo XI	
Ataques GSM-GPRS a iPhone.....	275
1. Introducción.....	275
2. Herramientas necesarias.....	276
Infraestructura basada en OpenBTS.....	276
Infraestructura basada en OpenBSC	281



3. Manipulación de comunicaciones GSM (voz y SMS)	292
Preparación de la infraestructura para pruebas de ataque con estación base falsa.....	292
Interceptación de comunicaciones de voz.....	299
Interceptación de mensajes SMS	300
Ataques basados en la suplantación del número llamante	301
Ataques basados en la redirección del número destino.....	301
4. Manipulación de comunicaciones GPRS/EDGE	302
Preparación de la infraestructura para pruebas de ataque con estación base falsa.....	302
Interceptación de comunicaciones de datos	306
Redirección y/o alteración de comunicaciones IP.....	308
Ataque directo vía IP.....	310
Ataques a dispositivos especiales.....	312
5. Manipulación de fecha y hora	313
6. Ataque de denegación de servicio	315
Ataque de denegación de servicio selectivo basado en redirección de llamada	315
Ataque de denegación de servicio selectivo basado en códigos de rechazo de registro	316
7. Otros posibles ataques	317
Localización geográfica de terminales móviles	318
Índice alfabético	321
Índice de imágenes	323



