Contenido

Prólogo

Capítulo 1
Introducción y definiciones

1. La seguridad informática: para qué y para quién. 25
   - 1.1 La actualidad cibercriminal 25
   - 1.2 Hacking, pirateo, seguridad informática, ciberdefensa, etc... ¿Qué hay detrás de estos términos? 26
   - 1.3 La importancia de la seguridad 28
     - 1.3.1 Para los particulares 28
     - 1.3.2 Para las empresas y escuelas 29
     - 1.3.3 Para un país o una nación. 30
2. El hacking se considera ético. 31
   - 2.1 El trabajo en cooperación 31
   - 2.2 Sobre todo, una mente curiosa, habilidad y pasión. 32
   - 2.3 El hacker se convierte en un experto codiciado 32
   - 2.4 Ponerse en el lugar del atacante 33
   - 2.5 Asesoramiento y apoyo par conseguir seguridad. 34
3. Conocer al enemigo para defenderse 34
   - 3.1 A cada atacante, su sombrero 34
     - 3.1.1 Los hackers black hats 34
     - 3.1.2 Los hackers grey hats 35
     - 3.1.3 Los hackers white hats 36
     - 3.1.4 Los script kiddies. 36
     - 3.1.5 Los hackers universitarios. 37
   - 3.2 Y cada auditoría tiene su propia caja de secretos. 38
     - 3.2.1 Las pruebas black box 38
     - 3.2.2 Las pruebas grey box. 38
     - 3.2.3 Las pruebas white box 39
4. Conclusión 39

Capítulo 2
Elementos de ingeniería social

1. Aspectos generales 41
   1.1 Introducción 41
   1.2 Sistemas de información 43
      1.2.1 Precisión de los sistemas de información 43
      1.2.2 Vulnerabilidades de un sistema de información 44
   1.3 Presentación de la ingeniería social 44
      1.3.1 Definiciones 44
      1.3.2 Características y perímetro 45
   1.4 Problemática de la protección 48
2. Modelos de actuación de la ingeniería social 49
   2.1 Aspectos principales del ataque por ingeniería social 49
   2.2 Procesos genéricos de la ingeniería social 50
      2.2.1 Estudio inicial 51
      2.2.2 Preparación 54
      2.2.3 Explotación 55
   2.3 Habilidades y herramientas de la ingeniería social 56
      2.3.1 Teatro, artimañas, subterfugios y engaños 57
      2.3.2 Lectura del objetivo 57
3. Conocimiento de las organizaciones atacadas 58
   3.1 Tipologías generales 59
   3.2 Tipologías de valores y creencias 59
   3.3 Modelos de madurez y certificaciones de calidad 62
   3.4 Explotación 63
   3.5 Ejercicios 63
4. Vulnerabilidades humanas: aspectos básicos y modelos teóricos 63
   4.1 Aspectos básicos biológicos y funcionalidades del cerebro 64
   4.2 Sesgos cognitivos 65
   4.3 Métodos hipnóticos 66
   4.4 Coherencia y búsqueda de un «pattern» 67
   4.5 Conclusión 67
   4.6 Ejercicios 68
      4.6.1 Caso particular del teléfono 68
      4.6.2 Camuflaje final 68

5. Influencia y manipulación 68
5.1 Métodos de influencia 68
5.1.1 Influencia 68
5.1.2 Tentación, seducción e intimidación 69
5.1.3 Manipulación 70
5.2 Los grandes resortes de la manipulación 70
5.2.1 Coherencia 70
5.2.2 Reciprocidad 71
5.2.3 Prueba social 72
5.2.4 Autoridad 73
5.2.5 Simpatía 73
5.2.6 Rareza 74
6. Las técnicas de manipulación 75
6.1 Las grandes técnicas de manipulación 76
6.1.1 Cebos y señuelos 76
6.1.2 El pie en la puerta 76
6.1.3 La puerta en las narices 77
6.2 Las pequeñas técnicas de manipulación 77
6.2.1 Pie en la boca, cortesía, simpatía 78
6.2.2 Contacto, tacto, mirada 78
6.2.3 Errores de coherencia 78
6.2.4 Etiquetado 79
6.2.5 Declaración de libertad 79
6.2.6 Algunas pequeñas técnicas que es necesario conocer 80
6.3 Ejercicios 81
6.3.1 Combinación de técnicas grandes y pequeñas 81
6.3.2 Combinar técnicas y motivaciones 81
6.3.3 Script de camuflaje final 81
7. Saber "parchear" las vulnerabilidades humanas 81
7.1 Voluntad política 82
7.2 Metodología 83
7.2.1 Profesionalismo, calidad, procedimientos y madurez 83
7.2.2 Medición: pruebas, auditoría y experiencia de detección 83
7.2.3 Optimización y cambio de paradigma 84
7.3 Acciones concretas para llevar a cabo 84
7.3.1 Documentar una política de clasificación de la información . 84
7.3.2 Controlar los "input/output" (entrada/salida de información) .

85
7.3.3 Sensibilizar al personal 85
7.3.4 Favorecer el flujo de información 86
7.4 Ejercicios 87
7.4.1 Manipular a los que toman las decisiones 87
7.4.2 Bloc de notas de respuesta al teléfono 87
7.4.3 Flujo de información 87
8. OSINT 87
9. Bibliografía 90

Capítulo 3
Black Market

1. Introducción 91
2. Deep Web, Dark Web, Darknet y Black Market 91
3. Black Market, entre lo visible y lo invisible 92
4. Funcionamiento 94
5. ¿La tiendas son anónimas? 95
6. Cómo se utiliza Tor 97
6.1 Instalación 97
6.2 Configuración de la seguridad 98
6.3 Verificación de la dirección IP 98
6.4 Navegación 99
6.5 Cambio de dirección IP 99
6.6 Actualización 100
7. Hacer referencia al Black Market 100
8. Directorio de sitios web en .onion 104
9. Vocabulario 104
10. Lista de markets y autoshops 106

Capítulo 4
Toma de datos o Information Gathering

1. Los ataques . . . 107
   - 1.1 Preámbulo . . . 107
   - 1.2 Tipos y metodologías de los ataques . . . 108
   - 1.3 La evolución de la criminalidad . . . 108
   - 1.4 Las motivaciones . . . 108
   - 1.5 Los diferentes tipos de ataques . . . 109
     - 1.5.1 El ataque de tipo destructivo . . . 109
     - 1.5.2 Los ataques con motivaciones económicas . . . 110
     - 1.5.3 Los ataques de tipo APT . . . 110
   - 1.6 La cyber kill chain o las diferentes fases de un ataque . . . 111
2. El análisis de los riesgos . . . 113
3. La prueba de intrusión . . . 114
   - 3.1 Los actores del hacking . . . 115
   - 3.2 Tipos y estrategias de auditoría . . . 115
     - 3.2.1 Los tipos de auditoría . . . 115
     - 3.2.2 Las estrategias de auditoría . . . 116
4. Metodología de una recogida de información o information gathering . . 116
5. El servicio Whois . . . 117
   - 5.1 Presentación . . . 117
   - 5.2 La gestión de las direcciones IP en el mundo . . . 117
6. La búsqueda de información en la Web . . . 120
   - 6.1 Los aspectos básicos . . . 121
   - 6.2 Búsqueda en línea: los sitios web especializados . . . 122
   - 6.3 Las redes sociales y profesionales . . . 124
   - 6.4 Los agregadores de información especializada . . . 130
   - 6.5 Los add-ons de navegadores especializados . . . 132
7. Los motores de búsqueda de periféricos conectados . . . 135
   - 7.1 Shodan: la referencia . . . 135
   - 7.2 Censys: todo sobre los aparatos conectados en IPv4 en la red . . . 141
   - 7.3 ZoomEye: la alternativa china . . . 143
8. La búsqueda de información con Google Hack . . . 143
   - 8.1 El Big Data . . . 143
   - 8.2 Las técnicas utilizadas . . . 144

8.3 Google: histórico y claves de su éxito . . . 144
8.4 Google, inevitable en la Web . . . 145
8.5 Definición de Google Hacking . . . 145
8.6 Funcionamiento del motor de búsqueda . . . 146
8.7 El SEO Google . . . 146
8.8 Google Hack: los operadores básicos de Google . . . 147
8.9 Los operadores avanzados . . . 147
8.10 Los operadores específicos . . . 148
8.11 Los Google Dorks . . . 149
8.12 Una interfaz gráfica para Google Hack y Bing Hack . . . 155

9. Aplicaciones gráficas dedicadas a la búsqueda de información . . . 156
9.1 Maltego . . . 156
9.2 Foca Free . . . 159

10. Los scripts de búsqueda de información . . . 161
10.1 TheHarvester . . . 161
10.2 CrossLinked . . . 163
10.3 Emailfinder . . . 164
10.4 Parsero . . . 165
10.5 Dirsearch . . . 166

11. Enumeración DNS: comandos y scripts . . . 166
11.1 Nslookup . . . 166
11.2 Host . . . 167
11.3 Dig . . . 168
11.4 Dnsenum . . . 169
11.5 Subwalker . . . 170
11.6 Dnsrecon . . . 171
11.7 Fierce . . . 171
11.8 Knockpy . . . 172
11.9 SecLists . . . 173
11.10 Bluto . . . 174

12. Los escáneres de puertos . . . 174
12.1 Nmap . . . 174
12.1.1 Uso de nmap . . . 176
12.1.2 Servicios y protocolos . . . 177
12.1.3 Evasión de firewall . . . 178
12.1.4 Escaneado en Idle Scan . . . 181

12.1.5 Escaneados avanzados: utilización de scripts nmap (.nse). . 182
12.2 El escáner masivo Masscan 184
12.3 El escáner web Httprint 184
12.4 Dmitry (Deepmagic Information Gathering Tool) 185
13. Frameworks y recogida de información 186
13.1 Metasploit 186
13.2 Recon-ng 186
13.3 SpiderFoot 188
14. El escáner de vulnerabilidades. 189
14.1 Nessus: escáner de redes 189
14.2 OpenVAS: escáner de redes de código abierto 197
14.3 Nikto: escáner de vulnerabilidades web 201
15. Faraday: IPE (Integrated Penetration- Test Environment) 202
16. TL-OSINT: una máquina virtual para OSINT 207
17. El protocolo SNMP (Simple Network Management Protocol) 208
17.1 Las consultas SNMP 209
17.2 Las respuestas SNMP. 209
17.3 Las alertas SNMP (traps, notifications) 209
17.4 La MIB 210
17.5 Las herramientas SNMP 210
17.6 SNMP y la seguridad 211
17.7 La herramienta snmpwalk 211
17.8 La herramienta snmpcheck 212
17.9 Onesixtyone: búsqueda de las comunidades SNMP 213
17.10 Algunas reglas de seguridad 213
18. El reporting 213
19. Sitios que indexan muchas herramientas y guías OSINT 214
20. Para terminar 215

Capítulo 5
Las vulnerabilidades del sistema

1. Aspectos generales 217
2. Las vulnerabilidades físicas 218
   2.1 Introducción 218
   2.2 Lockpicking 218
   2.3 Acceso físico directo al ordenador 219
      2.3.1 Acceso a un ordenador apagado con la BIOS protegida 219
      2.3.2 Acceso a un ordenador encendido con la BIOS protegida . . 221
      2.3.3 Acceso a un ordenador encendido sin la BIOS protegida . . . 222
      2.3.4 Acceso a un ordenador encendido en modo sesión de usuario actual 225
3. Las contraseñas 233
   3.1 Introducción 233
   3.2 Complejidad 234
4. Cifrado y encriptado 235
   4.1 Introducción 235
   4.2 El cifrado simétrico 235
   4.3 El cifrado asimétrico 236
   4.4 Los algoritmos One Way Digest 236
   4.5 Las tablas arcoiris (rainbow tables) 236
      4.5.1 Aspectos principales 236
      4.5.2 Generar sus tablas arcoiris 238
   4.6 Métodos de determinación de contraseña 240
5. Los procesos 240
6. El arranque 242
   6.1 El abuso de los modos de arranque degradados 242
   6.2 Los ataques de preboot 243
   6.3 La hibernación 243
   6.4 Las copias de seguridad 244
7. Windows 244
   7.1 Gestión de los usuarios 244
   7.2 Gestión de grupos 245
   7.3 Asignación de permisos 246
   7.4 Las contraseñas 247

7.4.1 Cambiar su contraseña en línea de comandos 248
7.4.2 Almacenamiento de las contraseñas en un grupo de trabajo 248
7.4.3 Almacenamiento de las contraseñas en un dominio 249
7.4.4 Extracción de los datos de una SAM 250
7.4.5 Cifrado LM (LAN Manager) 253
7.4.6 Cifrado NTLM (NT hash) NTLMv1 254
7.4.7 Cifrado NTLM (NT hash) NTLMv2 255
7.4.8 Elección del nivel de autenticación 256
7.5 Elevación de privilegios 258
7.6 El programador de tareas 263
7.7 Espiar los procesos en Windows 263
7.8 Las llamadas de procedimientos remotos 264
7.9 El acceso al registro remoto 265
7.10 Los logs 265
7.11 Las actualizaciones 266
7.12 Casos prácticos 267
7.12.1 Revelar una contraseña almacenada por una aplicación . . . 267
7.12.2 Utilización de Hiren's BootCD 272
7.12.3 Vulnerabildiad física osk.exe 273
7.12.4 Encontrar los hashes en línea 274
7.12.5 Utilización de John the Ripper 275
7.12.6 Utilización de Hashcat 277
7.12.7 Recuperación del condensado con Responder 281
7.12.8 Pass The Hash 284
7.12.9 Recuperación de condensado de una máquina local y elevación de privilegios con Mimikatz 286
7.12.10 Explotación del krbtgt (Golden Ticket) 289
8. Linux 295
8.1 Gestión de usuarios 295
8.2 Gestión de grupos 296
8.3 Asignación de permisos 296
8.4 Las contraseñas 297
8.5 Elevación de privilegios 299
8.5.1 Activación del suid y del sgid 300
8.5.2 Cómo encontrar los scripts suid root de un sistema GNU/Linux 300
8.6 El cambio de raíz o chrooting 301

8.7 Los logs . . . 301
8.8 Las actualizaciones . . . 301
8.9 Casos prácticos . . . 301
8.9.1 Utilización de John the Ripper . . . 301
8.9.2 GRUB . . . 302
9. macOS X . . . 304
9.1 Gestión de usuarios . . . 304
9.2 Las contraseñas . . . 306
9.3 Gestión de grupos . . . 307
9.4 Asignación de permisos . . . 307
9.5 Los logs . . . 308
9.6 Las actualizaciones . . . 308
10. Explotación de las vulnerabilidades de los sistemas operativos . . . 308
10.1 Caso práctico . . . 315
11. Big Data y confidencialidad . . . 316
12. Conclusión . . . 318

Capítulo 6
Las vulnerabilidades de la red

1. Aspectos generales . . . 319
2. Recordatorio sobre las redes TCP/IP . . . 319
2.1 El modelo OSI . . . 319
2.2 Dirección MAC y dirección IP . . . 320
2.3 Nociones de pasarela, máscara y subred . . . 321
2.4 TCP y UDP . . . 323
2.5 Los servicios y puertos . . . 323
2.6 Las direcciones IPv4 públicas y privadas . . . 325
3. Herramientas prácticas . . . 326
3.1 Información sobre los sockets . . . 326
3.2 Información de una dirección pública o un nombre de dominio . . . 328
3.3 Escáner de puerto TCP . . . 329
3.3.1 Escanear su propia máquina . . . 329
3.3.2 Escanear una subred . . . 330

3.3.3 Escanear una red sin comunicarse directamente con el destino 332
3.3.4 Escanear una red sin escanear los puertos 333
3.3.5 Escanear una red a través de "TCP SYN scan" (half open scan) 334
3.3.6 Escanear una red a través de "TCP XMAS scan" y "Maimon scan" 345
3.3.7 Escanear una red mediante "TCP FIN scan" 346
3.3.8 Escanear una red mediante "TCP NULL scan" 347
3.3.9 Escanear una red mediante "TCP IDLE scan" 347
3.3.10 Escanear una red mediante "UDP scan" 349
3.3.11 Escanear una red mediante "TCP-ACK scan" 351
3.4 Gestión de los sockets 353
3.4.1 ¿Cómo asumir el control de un host remoto? 353
3.4.2 Transferencia de archivos entre dos máquinas 354
3.4.3 Controlar un ordenador de una red privada 355
3.5 SSH 356
3.6 Tunnel SSH 357
3.6.1 Omitir un cortafuegos para llegar a un host remoto 357
3.6.2 Autorizar un acceso temporal desde el exterior 360
4. DoS y DDoS 361
5. Sniffing 362
5.1 Capturar datos con Wireshark 363
5.2 Los filtros 365
6. Man In The Middle en una red local 367
6.1 Corrupción de la caché ARP (teoría) 367
6.2 Corrupción de la cache ARP (práctica) 372
6.2.1 Instalación de Ettercap 372
6.2.2 Configuración de Ettercap 374
6.2.3 Los plugins en Ettercap 377
6.2.4 Creación de un filtro 378
6.2.5 Cain & Abel 380
6.3 Corrupción de la caché ARP (contramedidas) 380
6.4 Utilización de un servidor DHCPv4 clandestino (teoría) 382
6.5 Utilización de un servidor DHCPv4 clandestino (práctica) 383
6.6 Utilización de un servidor DHCPv4 clandestino (contramedidas) . 384

7. Robo de sesión TCP (hijacking) y spoofing de IP 385
7.1 La vulnerabilidad: ACK/SEQ. 385
7.2 Consecuencia del ataque 386
7.3 Puesta en práctica 386
7.4 Automatizar el ataque 389
7.5 Spoofing de direcciones IP 389
8. Vulnerabilidades Wi-Fi 392
8.1 Crackear una red WEP 392
8.1.1 Capturar los paquetes 393
8.1.2 Generar tráfico. 393
8.1.3 Encontrar la clave 394
8.2 Crackear una red WPA2. 396
8.3 Rogue AP 400
8.3.1 Introducción a Rogue AP 400
8.3.2 Puesta en práctica de un Rogue AP con Karmetasploit 401
9. IP over DNS 403
9.1 Principios básicos 403
9.2 En la práctica 403
9.3 Contramedidas 404
10. La telefonía sobre IP. 405
10.1 Escuchar la conversación 405
10.2 Usurpación de la línea 406
10.3 Otros ataques 408
11. IPv6 408
11.1 El software 409
11.2 El hardware. 409
11.3 El ser humano. 409
11.4 THC-IPv6 410
11.5 Escanear los hosts. 410
11.5.1 En una red local 410
11.5.2 En Internet. 410
11.6 Ataque Man In the Middle 411
12. Conclusión 413

Capítulo 7
La seguridad de las comunicaciones inalámbricas

1. Presentación 415
2. Los objetos conectados 416
3. Las transmisiones de radio 416
4. La radio de software 419
5. El hardware disponible 420
   5.1 La llave RTL-SDR 420
   5.2 El HackRF One 421
   5.3 El bladeRF 422
   5.4 El PandwaRF 423
   5.5 El USRP 424
6. Los protocolos 425
   6.1 El ZigBee 425
   6.2 El Z-Wave 428
   6.3 El Bluetooth 430
7. El paquete de software GNU Radio 432
   7.1 Aspectos básicos de GNU Radio Companion 434
   7.2 Módulo Python 440
   7.3 Módulo escrito en CPP (C++) 448
8. Ejemplos de aplicaciones 452
   8.1 Comunicación NRF24 453
   8.2 Comunicación ZigBee 461
9. Conclusión 467

Capítulo 8
Las vulnerabilidades web

1. Recordatorios sobre la Web 469
2. Composición y consulta de un sitio web 470
   2.1 Composición de un sitio web 470
   2.2 Consulta de una página web 470

3. Las vulnerabilidades web 482
3.1 Definición e importancia 482
3.2 Exposición y arquitectura de un sitio web 482
3.3 Cómo abordar la seguridad de los sitios web 485
3.3.1 Elegir su área de estudio 485
3.3.2 Las vulnerabilidades más extendidas 487
3.4 Instalación y configuración de un servidor web completo 491
3.4.1 Instalación y configuración del servidor básico 491
3.4.2 Instalación y configuración del servidor de bases de datos . . 497
3.4.3 Instalación de un lenguaje en el lado del servidor 500
3.5 Presentación de algunas vulnerabilidades web 505
3.5.1 Preámbulo 505
3.5.2 Las inyecciones SQL clásicas 505
3.5.3 Las inyecciones SQL a ciegas 521
3.5.4 Las inyecciones en el lado cliente 524
3.5.5 Pasar los controles del lado cliente 528
3.6 Practicar la auditoría y detectar varias vulnerabilidades web 530
3.6.1 Para practicar 530
3.6.2 Herramientas para auditar 531
4. Contramedidas y consejos de seguridad 536
4.1 Filtrar todos los datos 536
4.1.1 Observaciones 536
4.1.2 Evitar las inyecciones SQL 537
4.1.3 Filtrar los datos 538
4.2 Utilizar los frameworks para el desarrollo 541
5. Conclusión 542

Capítulo 9

Las vulnerabilidades de las aplicaciones

1. Aspectos generales 543
2. Nociones de ensamblador 544
2.1 Introducción 544
2.2 Primeros pasos 544
2.2.1 Aprender a contar 544
2.2.2 El sistema binario 544

2.2.3 El sistema hexadecimal . . . 546
2.3 ¿Cómo probar nuestros programas? . . . 547
2.3.1 Esqueleto de un programa en ensamblador . . . 547
2.3.2 Nuestro primer programa . . . 548
2.4 Las instrucciones . . . 549
2.4.1 La comparación . . . 549
2.4.2 La instrucción IF . . . 550
2.4.3 El bucle FOR . . . 551
2.4.4 El bucle WHILE . . . 552
2.4.5 El bucle DO WHILE . . . 552
2.4.6 La directiva %define . . . 554
2.4.7 Las directivas de datos . . . 554
2.4.8 Las entradas-salidas . . . 554
2.5 Las interrupciones . . . 555
2.6 Las subrutinas . . . 557
2.7 El heap y la pila . . . 558
2.7.1 El heap . . . 558
2.7.2 La pila . . . 559
2.7.3 Llamada y retorno de una función: las nociones fundamentales . . . 560
3. Aspectos básicos de los shellcodes . . . 562
3.1 Ejemplo 1: shellcode.py . . . 562
3.2 Ejemplo 2: execve() . . . 563
3.3 Ejemplo 3: Port Binding Shell . . . 565
4. Los buffers overflows . . . 566
4.1 Algunas definiciones . . . 566
4.2 Nociones esenciales . . . 567
4.3 Stack overflow . . . 569
4.4 Heap overflow . . . 576
4.5 return-into-libc . . . 580
5. Las vulnerabilidades de Windows . . . 584
5.1 Introducción . . . 584
5.2 Primeros pasos . . . 584
5.2.1 En modo consola . . . 585
5.2.2 Depuración . . . 586
5.2.3 El problema de un shellcode grande . . . 590

5.2.4 Ejecución de una función no prevista . . . 593
5.2.5 Otros métodos . . . 595
5.3 El método de call [reg] . . . 595
5.4 El método pop ret . . . 595
5.5 El método de push return . . . 596
5.6 El método de jmp [reg] + [offset] . . . 596
5.7 El método de blind return . . . 597
5.8 ¿Qué hacer con un shellcode pequeño? . . . 597
5.8.1 Principio . . . 597
5.8.2 En la práctica . . . 597
5.9 SEH (Structured Exception Handling) . . . 598
5.9.1 Los aspectos básicos . . . 598
5.9.2 SEH: las protecciones . . . 600
5.9.3 XOR y Safe-SEH . . . 600
5.10 Pasar las protecciones . . . 601
5.10.1 Stack cookie, protection /GS . . . 601
5.10.2 Ejemplo: exceder la cookie . . . 605
5.10.3 SafeSEH . . . 608
6. Caso concreto: Ability Server . . . 609
6.1 Fuzzing . . . 609
6.2 Explotación . . . 611
7. Caso concreto: MediaCoder-0.7.5.4796 . . . 616
7.1 Crash del software . . . 616
7.2 Verificación de los valores . . . 621
7.3 Finalización del exploit . . . 622
8. Caso concreto: BlazeDVD 5.1 Professional . . . 624
9. Conclusión . . . 627
10. Referencias . . . 628

Capítulo 10
Forensic

1. Introducción . . . 629
1.1 El cerebro . . . 630
1.2 La memoria . . . 631
1.3 Los archivos . . . 633

2. Los métodos 634
2.1 Preparación y entorno 634
2.2 Búsqueda y análisis de archivos 635
3. Las herramientas 637
3.1 Las herramientas de análisis de red 638
3.1.1 Wireshark 638
3.1.2 tcpdump 638
3.1.3 Scapy 639
3.2 Las herramientas de análisis de memoria 639
3.2.1 Métodos de recuperación de la memoria RAM 641
3.2.2 Dump de memoria en Linux 646
3.2.3 Análisis de las imágenes de memoria 647
3.2.4 El framework Volatility 648
3.2.5 Volatility y Linux 660
3.2.6 Introducción a Volatility 3 662
3.2.7 Otras herramientas de análisis de memoria 663
3.3 Las herramientas de análisis binario 664
3.3.1 Hexdump 664
3.3.2 Readelf 665
3.3.3 gdb 665
3.4 Las herramientas de análisis de sistema 666
3.4.1 The Coroner's Toolkit 666
3.4.2 Logstash 667
4. Conclusión 667

Capítulo 11

Malwares: estudio del código malintencionado

1. Introducción 669
2. ¿Qué es un malware? 670
3. La mejor clasificación 671
4. La detección por base de conocimiento 672
5. Correspondencias parciales 675
6. Estructura de un PE e imphash 677
7. Entropía y packing 679

8. Análisis y herramientas 683
9. Simulaciones y perfilado 688
10. Sitios de clasificaciones y sandboxes 691

Capítulo 12
Dispositivos móviles: vulnerabilidades

1. Aspectos generales 693
2. Los vectores de ataque 694
   2.1 Introducción 694
   2.2 Anatomía de los ataques móviles 694
   2.3 Los datos objetivo 695
3. Top 10 de las vulnerabilidades de los móviles 695
   3.1 Utilización incorrecta de la plataforma 695
   3.2 Almacenamiento de datos de forma no segura 696
   3.3 Comunicación no segura 696
   3.4 Autenticación no segura 696
   3.5 Cifrado insuficiente 696
   3.6 Autorización no segura 697
   3.7 Calidad del código débil 697
   3.8 Falsificación de código 697
   3.9 Ingeniería inversa 697
   3.10 Funcionalidad extranjera 698
4. Red móvil 698
   4.1 Definiciones 698
   4.2 IMSI-catcher 699
   4.3 Intercepción pasiva 699
      4.3.1 Instalación 700
      4.3.2 Demostración 700
   4.4 Conclusión 702
5. Android 703
   5.1 Introducción 703
   5.2 Las diferentes versiones 704
      5.2.1 Introducción 704
      5.2.2 Problemática 704

5.2.3 Soluciones . . . 705
5.3 Las ROM Custom . . . 707
5.3.1 Procesos de arranque . . . 708
5.3.2 Bootloader . . . 708
5.3.3 Recovery . . . 710
5.3.4 Root . . . 712
5.4 La arquitectura . . . 714
5.4.1 Linux Kernel . . . 715
5.4.2 Hardware Abstraction Layer . . . 715
5.4.3 Librerías . . . 715
5.4.4 Android Runtime . . . 716
5.4.5 Java API Framework . . . 717
5.4.6 System Apps . . . 717
5.5 Estructura de una aplicación . . . 717
5.5.1 Activity . . . 718
5.5.2 View . . . 719
5.5.3 Service . . . 719
5.5.4 Intent . . . 720
5.5.5 BroadcastReceiver . . . 721
5.5.6 ContentProvider . . . 722
5.6 Android Package . . . 722
5.7 Sistema de archivos . . . 723
5.7.1 Las particiones . . . 723
5.7.2 La jerarquía . . . 724
5.8 Emuladores . . . 727
5.8.1 Genymotion . . . 727
5.9 Forensic . . . 731
5.9.1 ADB . . . 731
5.9.2 Evitar la pantalla de bloqueo . . . 734
5.9.3 Adquisición de datos . . . 736
5.9.4 Análisis de memoria . . . 742
5.9.5 Solución todo en uno . . . 743
5.10 Conclusión . . . 747
6. Vulnerabilidades de las aplicaciones . . . 747
6.1 Distribución . . . 747
6.2 ADB . . . 748
6.3 Frameworks . . . 748

6.4 DIVA 748
6.5 Conclusión 768
7. Conclusión 768

Capítulo 13
Las vulnerabilidades del hardware

1. Introducción 769
2. Las herramientas básicas 770
2.1 Juego de destornilladores 770
2.2 Multímetro 771
2.3 Placa de pruebas 771
2.4 Cables Dupont 772
2.5 Soldador 772
2.6 Arduino 772
2.7 Hardware de recuperación 773
3. Usuario habitual 773
3.1 Adaptador USB RS232 TTL 773
3.2 Sonda de análisis lógico 774
3.3 Interfaz JTAG 774
3.4 Bus pirate de Dangerous Prototypes 775
3.5 SDR low cost 775
4. Usuario avanzado 776
4.1 Software de diseño de PCB 776
4.2 Programador 777
4.3 Equipos electrónicos 778
5. Metodología de ingeniería inversa de hardware 779
5.1 Ataque a través de sniffing I^2C 781
5.2 Ataque con sniffing UART modem 783
6. Estudio sobre los T2G y Arduino 784
6.1 Creación de un lector de tarjetasT2G 785
6.2 Emulador parcial de la tarjeta T2G 793

Capítulo 14
La seguridad de las box

1. Introducción 797
2. Las funcionalidades de una box 797
   - 2.1 Rúter 797
   - 2.2 Switch 798
   - 2.3 Telefonía 798
   - 2.4 TV 798
   - 2.5 Almacenamiento multimedia 799
   - 2.6 Servicios domóticos 799
3. Las diferentes box 799
   - 3.1 Orange 799
   - 3.2 ONO 800
4. La configuración de las box 801
   - 4.1 El modo módem 801
   - 4.2 El modo rúter 802
   - 4.3 Las funciones telefónicas 803
5. La configuración por defecto, un peligro 804
   - 5.1 La interfaz de administración web 804
   - 5.2 Wi-Fi 805
   - 5.3 Los servicios: SSH, Telnet, Samba y TR069 805
6. Instalación de un firmware alternativo 807
   - 6.1 ¿Para qué? 807
   - 6.2 Conexión al puerto de consola 807
7. La seguridad de los firmwares oficiales 812
   - 7.1 Las vulnerabilidades en los últimos años 812
   - 7.2 ¿Y en la actualidad? 814
8. Ingeniería inversa de la Neufbox 5 814
   - 8.1 Introducción 814
   - 8.2 Características técnicas 815
   - 8.3 Búsqueda del puerto serie 815
   - 8.4 Conexión al puerto serie 817
   - 8.5 Creación de una imagen completa 821
   - 8.6 Flasheado de la imagen 823
   - 8.7 Utilización de la box como rúter 826

8.8 Telefonía SIP 827
8.9 Instalación de un firmware libre OpenWRT 830

Capítulo 15
Hacking del vehículo conectado

1. Introducción: hacia el vehículo autónomo. 831
2. Vehículo conectado y autónomo 832
3. Servicios de un vehículo conectado/autónomo 833
4. El vehículo conectado, una enorme superficie de ataque 834
5. Motivaciones del hacking del vehículo conectado. 835
6. Los sistemas internos del vehículo conectado 836
7. Ataque físico de la ECU: chiptuning o remapping 840
   7.1 ECU y puertos de comunicación de la MCU 840
   7.2 Hacking de memoria: hardware, herramientas y software utilizado. 844
   7.3 Hacking de la memoria ROM: reprogramación de una "key immobilizer" de Toyota/Lexus 846
8. Ataque backdoor: la inyección en la red CAN 853
   8.1 Presentación del OBD 853
   8.2 Presentación del bus CAN y de sus tramas 856
   8.3 Hacking del CAN: consecuencias y advertencias. 859
   8.4 Presentación de los mensajes de diagnóstico a través de OBD2 y el protocolo UDS 860
   8.5 Presentación del hardware para la inyección 866
      8.5.1 ELM327 867
      8.5.2 Arduino 868
      8.5.3 Raspberry Pi. 868
      8.5.4 CANTACT 869
   8.6 Las herramientas de sniffing e inyección para el bus CAN 870
      8.6.1 SocketCAN y las herramientas can-utils 870
      8.6.2 Kayak 875
      8.6.3 CANalyzat0r 878
      8.6.4 SavvyCAN 879
      8.6.5 Katy OBD 880

8.7 Los simuladores de tramas del bus CAN 881
8.7.1 ICSim 881
8.7.2 UDS Server 886
8.7.3 ICSim de la conferencia Barbhack 2020 887
8.7.4 VIC 888
8.7.5 UDSim 889
8.7.6 CANdevStudio 890
8.8 Openpilot y la conducción autónoma para todos 894
8.9 Una consecuencia de OpenPilot, la interpretación estandarizada de las tramas CAN con el formato DBC 896
8.10 Las inyecciones remotas 899
8.10.1 Car Backdoor Maker y The Bicho 899
8.10.2 CANalyse y la mensajería Telegram 901
9. Otros ataques del vehículo conectado 902
9.1 Aplicación mal securizada: el caso Nissan Leaf de 2016 902
9.2 El hacking del TPMS 906
9.2.1 Hardware de radio 909
9.2.2 El software RTL_433 909
9.2.3 El simulador de tramas TPMS: TXTPMS 910