Ediciones ENI

Seguridad informática
Hacking Ético
Conocer el ataque para una mejor defensa
(4ª edición)

Colección Epsilon

Contenido

Capítulo 1
Introducción y definiciones

1. La seguridad informática, ¿para qué?, ¿para quién? 23
   1.1 Hacking, piratería, seguridad informática... ¿Qué hay detrás de estas palabras? 23
   1.2 La importancia de la seguridad 25
      1.2.1 Para particulares. 25
      1.2.2 Para empresas y centros académicos 26
      1.2.3 Para un país o una nación 27
2. El hacking que pretende ser ético 28
   2.1 Trabajo en cooperación 28
   2.2 Un espíritu habilidoso y apasionado por encima de todo 29
   2.3 El hacker se está convirtiendo en un experto muy buscado 29
   2.4 En la piel del atacante. 30
   2.5 Asesoramiento y apoyo para la seguridad. 31
3. Conocer al enemigo para defenderse 32
   3.1 A cada atacante su sombrero 32
      3.1.1 Los hackers black hat. 32
      3.1.2 Los hackers grey hat 32
      3.1.3 Los hackers white hat 33
      3.1.4 Los "script kiddies". 34
      3.1.5 Los hackers universitarios 34
   3.2 Y a cada auditoría su caja de secretos 35
      3.2.1 Los test black box 35
      3.2.2 Los test grey box 36
      3.2.3 Los test white box 36

Capítulo 2
Metodología de un ataque

1. Preámbulo 37
2. Ante todo discreción 37
3. Seleccionar a la víctima 39
   3.1 Utilizar buenas herramientas. 39
   3.2 Identificar los dominios 40

3.3 Google, ese amigo tan curioso 41
3.4 Descubrir la red 43
4. El ataque 47
4.1 Aprovecharse del fallo humano 47
4.2 Abrir las puertas de la red 48
4.3 El ataque por la Web 50
4.4 La fuerza al servicio del ataque 51
5. Introducirse en el sistema y garantizar el acceso 52
5.1 Permanecer discreto 52
5.2 Garantizar el acceso 53
5.3 Ampliar su alcance 55
6. Revisión de la intrusión y la protección 55
6.1 Una política de seguridad exigente 56
6.1.1 Contraseñas 56
6.1.2 Formación del personal 57
6.1.3 A cada empleado su perfil 57
6.2 Encriptar la información esencial 58
6.3 Securizar los servidores 58
6.3.1 Realizar actualizaciones de seguridad 58
6.3.2 Enjaular servicios (chroot, jail) 59
6.3.3 Seguridad del núcleo 59
6.3.4 Evitar escaneos y ataques 60
6.3.5 Solo guardar lo esencial 61
6.3.6 Vigilancia de actividades 61
6.4 Los tests de intrusión 62

Capítulo 3
Elementos de ingeniería social

1. Aspectos generales 63
1.1 Introducción 63
1.2 Sistemas de información 65
1.2.1 Detalles de los sistemas de información 65
1.2.2 Fallos de un sistema de información 66

1.3 Presentación de la ingeniería social 66
1.3.1 Definiciones 66
1.3.2 Características y perímetro 67
1.4 Problemática de la protección 69
2. Formas de acción de la ingeniería social 71
2.1 Los principios del ataque por ingeniería social 71
2.2 Proceso genérico de la ingeniería social 72
2.2.1 Estudio previo 73
2.2.2 Preparación 76
2.2.3 Explotación 77
2.3 Competencias y herramientas del ingeniero social 78
2.3.1 Comedias, estratagemas, subterfugios y engaños 79
2.3.2 Lectura del objetivo 79
3. Conocimiento de las organizaciones atacadas 80
3.1 Tipologías generales 81
3.2 Tipologías de valores y de creencias 81
3.3 Modelos de madurez y certificaciones de calidad 84
3.4 Explotación 84
3.5 Ejercicios 85
4. Fallos humanos - bases y modelos teóricos 85
4.1 Bases biológicas y la funcionalidad del cerebro 86
4.2 Sesgos cognitivos 87
4.3 Métodos hipnóticos 88
4.4 Coherencia y búsqueda del "patrón" 89
4.5 Conclusión 89
4.6 Ejercicios 90
4.6.1 Caso particular del teléfono 90
4.6.2 Camuflaje final 90
5. Influencia y manipulación 90
5.1 Métodos de influencia 90
5.1.1 Influencia 90
5.1.2 Tentación, seducción e intimidación 91
5.1.3 Manipulación 92
5.2 Los grandes resortes de la manipulación 92
5.2.1 La coherencia 92
5.2.2 La reciprocidad 93

5.2.3 Prueba social 94
5.2.4 Autoridad 95
5.2.5 Simpatía 95
5.2.6 Escasez 96
6. Las técnicas de manipulación 97
6.1 Las técnicas mayores de manipulación 98
6.1.1 Los cebos y señuelos. 98
6.1.2 El pie en la puerta. 98
6.1.3 La puerta en las narices 99
6.2 Las técnicas menores de manipulación 99
6.2.1 Calentar la oreja, cortesía, simpatía 100
6.2.2 Contacto, toque, mirada 100
6.2.3 Las trampas de la coherencia. 100
6.2.4 Etiquetado 101
6.2.5 Declaración de libertad 101
6.2.6 Algunas pequeñas técnicas a conocer 102
6.3 Ejercicios 103
6.3.1 Cruzar técnicas mayores y menores 103
6.3.2 Cruzar técnicas y resortes 103
6.3.3 Guión de camuflaje final 103
7. Saber "actualizar" o "parchear" los fallos humanos 103
7.1 Voluntad política 104
7.2 Metodología. 105
7.2.1 Profesionalismo, calidad, procedimientos, madurez 105
7.2.2 Medida: pruebas, auditoría, experiencias de detección 105
7.2.3 Optimización y cambio de paradigma 106
7.3 Acciones concretas a emprender 106
7.3.1 Documentar una política de clasificación de la información . 106
7.3.2 Controlar los "Input/Output" (entrada/salida de información) 107
7.3.3 Instruir al personal. 107
7.3.4 Promover la recuperación de la información 108
7.4 Ejercicios 109
7.4.1 Manipular a los decisores. 109
7.4.2 Bloc-de-notas de respuesta al teléfono 109
7.4.3 Recuperación de información 109

8. Bibliografía 110

Capítulo 4
Los fallos físicos

1. Generalidades 111
2. Lockpicking 112
3. Acceso físico directo al ordenador 112
   3.1 Acceso a un ordenador apagado cuya BIOS está protegida 112
   3.2 Acceso a un ordenador apagado cuya BIOS no está protegida 116
      3.2.1 Utilización de Offline NT Password y Registry Editor v110511 116
      3.2.2 Utilización de Trinity Rescue Kit 120
      3.2.3 Obtener la base de datos SAM con Kali Linux (distribución que sucede a Backtrack5) 122
      3.2.4 Windows Password Recovery Bootdisk 127
      3.2.5 Los distintos tipos de algoritmos de encriptación 128
      3.2.6 Los hash de tipo LM y NTLM 129
      3.2.7 Utilizar John the Ripper para encontrar las contraseñas 131
      3.2.8 Hashcat 134
      3.2.9 Utilizar la potencia de la tarjeta gráfica 136
      3.2.10 Método de tablas arco iris (rainbow tables) 138
      3.2.11 Generar sus propias tablas rainbow 140
      3.2.12 Utilizar OPHCRACK 141
      3.2.13 Utilización del programa Cain & Abel 144
      3.2.14 Utilización del script Findmyhash 148
      3.2.15 Bypass de la autentificación de Windows y Linux 150
      3.2.16 Autenticación Firewire-Inception-Bypass 152
      3.2.17 Utilidades de recuperación de contraseñas 153
      3.2.18 Ejemplos de elevación de privilegios mediante exploits en Linux 157
      3.2.19 Fallos de Windows Vista, Windows 7 y Windows 8.1 158
      3.2.20 Windows-privesc-check-Búsqueda de fallos en Windows . . . 161
   3.3 Acceso a un equipo iniciado en modo sesión de usuario actual 163
      3.3.1 Las memorias USB 163
      3.3.2 U3PWN 163

3.3.3 La llave Ducky 165
3.3.4 Keyloggers hardware y software 167
3.3.5 Contramedidas para los keyloggers. 171
3.3.6 Obtención de imágenes de memoria. 174
3.3.7 Métodos de recuperación de la memoria RAM 176
3.3.8 Crear una memoria USB de arranque para vaciar la memoria. . 180
3.3.9 Extracción de memoria usando la conexión FireWire - Método Carsten Maartmann-Moe (Inception) . . . 185
3.3.10 Volcado de memoria en Linux. 186
3.3.11 Análisis de las imágenes de memoria 189
3.4 Conclusión. 201

Capítulo 5
Toma de huellas o captura de información

1. Los ataques 203
1.1 Preámbulo 203
1.2 Introducción a los diferentes tipos de ataques 203
1.3 El ataque de tipo destructivo 204
1.4 El ataque sobre los medios de comunicación. 204
1.5 Los ataques con objetivos mercantiles. 205
1.6 Los ataques de tipo APT 205
1.7 Las diferentes fases de un ataque y un test de intrusión 206
2. El análisis de riesgos 207
3. El test de intrusión. 208
3.1 Los actores del hacking 208
3.2 Tipos y estrategias de auditoría 209
3.2.1 Los tipos de auditorias 209
3.2.2 Las estrategias de auditorias 209
4. Metodología de recolección de información, también llamada "toma de huellas". 210

5. El servicio Whois 210
5.1 La gestión de direcciones IP en el mundo 211
5.2 Búsqueda de información en la Web 213
5.3 Los básicos 213
5.4 Los sitios web especializados 214
5.5 Las redes sociales y profesionales 216
5.6 Los agregadores de información especializados 218
5.7 Los add-ons de navegador especializados 220
5.8 Un navegador dedicado a la búsqueda OSINT: Oryon 221
5.9 Aplicación específica: Net Tools 223
6. Motores de búsqueda de dispositivos conectados 223
6.1 Shodan: la referencia 223
6.2 ThingFul: un motor de búsqueda para los IoT (Internet of things) . 230
6.3 Censys: todo sobre los aparatos conectados en IPv4 en Internet . . . 232
6.4 Zoomeye: la alternativa China 234
7. Búsqueda de información con Google Hack 235
7.1 El Big Data 235
7.2 Las técnicas utilizadas 235
7.3 Google: su historia y las claves de su éxito 236
7.4 Google ineludible en la Web 236
7.5 Definición de Google Hacking 236
7.6 Funcionamiento del motor de búsqueda 237
7.7 Las referencias Google 238
7.8 Google Hack: los operadores básicos de Google 238
7.9 Los operadores avanzados 239
7.10 Los operadores específicos 240
7.11 Los Google Dorks 240
7.12 Una interfaz gráfica para Google Hack y Bing Hack 246
8. Aplicaciones gráficas dedicadas a la búsqueda de información 248
8.1 Maltego 248
8.2 Foca Free 249
8.3 The Harvester 251
8.4 Uberharvest 253
9. Enumeración de DNS, comandos y scripts 253
9.1 Nslookup 253
9.2 Host 254

9.3 Dig 255
9.4 Dnsenum 256
9.5 Dnsbf 257
9.5.1 Fierce 258
9.6 Bluto 258
10. Los escáneres de puertos 259
10.1 Nmap - Network Mapper 259
10.1.1 Uso de nmap 261
10.1.2 Servicios y protocolos 262
10.1.3 Escaneo en Idle Scan 265
10.1.4 Escaneos avanzados - Utilización de los scripts nmap (.nse) . 267
10.2 El escáner en masa Masscan 269
10.3 El escáner web Httprint 270
10.4 Dmitry (Deepmagic Information Gathering Tool) 270
11. Frameworks y recogida de información 271
11.1 Metasploit 271
11.2 Recon-ng 271
11.3 SpiderFoot 273
12. Los escáneres de vulnerabilidades 274
12.1 Nessus - Escáner de red 274
12.2 OpenVAS - Escáner de red open source 282
12.3 AutoScan Network - Escáner de vulnerabilidades de red 286
12.4 Nikto - Escáner de vulnerabilidades web 288
13. El Protocolo SNMP - Simple Network Management Protocol 290
13.1 Las peticiones SNMP 291
13.2 Las respuestas SNMP 291
13.3 Las alertas (SNMP traps, notificaciones) 291
13.4 El MIB 291
13.5 Las herramientas SNMP 292
13.6 SNMP y la seguridad 292
13.7 La herramienta snmpwalk 293
13.8 La herramienta snmpcheck 294
13.9 Algunas reglas de seguridad 294
14. El reporting 294
15. Para concluir 296

Capítulo 6
Seguridad de comunicaciones inalámbricas

1. Presentación 297
2. Los objetos conectados 298
3. Las transmisiones de radio 298
4. La radio software 301
5. El hardware disponible 302
   - 5.1 La llave RTL-SDR 302
   - 5.2 El HackRF One 303
   - 5.3 El bladeRF 304
   - 5.4 El PandwaRF 305
   - 5.5 El USRP 306
6. Los protocolos 307
   - 6.1 El ZigBee 307
   - 6.2 El Zwave 311
   - 6.3 El Bluetooth 313
7. La suite GNU-RADIO 315
   - 7.1 Las bases de gnuradio-companion 317
   - 7.2 Módulo Python 324
   - 7.3 Módulo escrito en CPP (C plus plus) 331
8. Ejemplos de aplicaciones 335
   - 8.1 Comunicación NRF24 336
   - 8.2 Comunicación ZigBee 344
9. Conclusión 350

Capítulo 7
Los fallos de red

1. Introducción 351
2. Recordatorio de redes TCP/IP 351
   - 2.1 El modelo OSI 351
   - 2.2 Direccionamiento IPv4 352
   - 2.3 Noción de pasarela, máscara y subred 353
   - 2.4 TCP y UDP 355

2.5 Los servicios y los puertos. 355
2.6 Las direcciones IP públicas y privadas 356
3. Herramientas prácticas 357
3.1 Información sobre sockets 357
3.2 Información acerca de una dirección pública o un nombre de dominio 360
3.3 Escáner de puertos TCP 360
3.3.1 Escáner de nuestro propio equipo 361
3.3.2 Escanear una subred. 361
3.3.3 Escanear una red sin comunicar directamente con el objetivo . 363
3.3.4 Escaner en red sin escanear los puertos 364
3.3.5 Escanear una red via TCP SYN scan (Half Open scan) 366
3.3.6 Escanear una red vía TCP XMAS y Maimon scan. 376
3.3.7 Escanear una red vía TCP FIN scan 378
3.3.8 Escanear una red utilizando TCP NULL scan 379
3.3.9 Escaneo de red empleando TCP IDLE scan 379
3.3.10 Escanear una red empleando UDP scan 382
3.3.11 Escanear una red empleando TCP-ACK scan. 384
3.4 Gestión de sockets. 385
3.4.1 ¿Cómo tomar el control de un host remoto? 385
3.4.2 Transferencia de archivos entre dos equipos 387
3.4.3 Tomar el control de un equipo en una red privada 387
3.5 SSH 388
3.6 Túnel SSH 390
3.6.1 Rodear un firewall para acceder a un host remoto 390
3.6.2 Autorizar un acceso momentáneo desde el exterior 392
4. DoS y DDoS 393
4.1 Establecimiento de una sesión TCP. 393
4.2 Principios del ataque 394
5. Sniffing 395
5.1 Capturar datos con Wireshark 396
5.2 Filtros 397

6. Man In The Middle (MITM) 400
6.1 Teoría. 400
6.2 Práctica 402
6.2.1 Instalación de Ettercap 402
6.2.2 Configuración de Ettercap 403
6.2.3 Plug-ins con Ettercap. 406
6.2.4 Creación de un filtro 407
6.2.5 Cain & Abel 409
6.3 Contramedidas 410
7. Robo de sesión TCP (HIJACKING) y Spoofing de IP 411
7.1 El fallo: ACK/SEQ. 411
7.2 Consecuencias del ataque. 412
7.3 Puesta en práctica 412
7.4 Automatizar el ataque 415
7.5 Spoofing de dirección IP 415
8. Fallos Wi-Fi 419
8.1 Crackear una red con cifrado WEP 419
8.1.1 Capturar paquetes 419
8.1.2 Generar tráfico 420
8.1.3 Encontrar la clave 421
8.2 Crackear una red WPA 422
8.3 Rogue AP 424
8.3.1 Introducción. 424
8.3.2 Despliegue de un Rogue AP con Karmetasploit. 424
9. IP over DNS 426
9.1 Principio. 426
9.2 Explotación con la herramienta iodine 427
9.3 Contramedidas 428
10. La telefonía IP 428
10.1 Escucha de la conversación con VoIPong 428
10.2 Usurpación de la línea 430
10.3 Otros ataques 431
11. IPv6. 432
11.1 Los programas 432
11.2 El hardware 432
11.3 Factor humano 433

11.4 THC-IPv6 433
11.5 Escanear los hosts 434
11.5.1 En una red local 434
11.5.2 En Internet 434
11.6 Flooder 434
11.7 Man in the Middle Attack 435
12. Conclusión 438

Capítulo 8
Los fallos Web

1. Recordatorio sobre las tecnologías Web 439
1.1 Preámbulo 439
1.2 La red Internet 439
1.3 ¿Qué es un sitio web? 440
1.4 Consulta de una página web, anatomía de los intercambios cliente/servidor 440
1.5 ¿Cómo se construyen las páginas web? 445
2. Aspectos generales en la seguridad de sitios web 447
3. Pequeño análisis de un sitio web 448
3.1 Mapa de las partes visibles de un sitio web 448
3.1.1 ¿Es el sitio web estático o dinámico? 449
3.1.2 ¿Cuáles son las variables usadas? 450
3.1.3 ¿Qué formularios y qué campos las utilizan? 451
3.1.4 ¿Recibimos cookies? ¿Qué datos contienen? 451
3.1.5 ¿Las páginas tienen contenido multimedia? 453
3.1.6 ¿El sitio realiza consultas a base de datos? 453
3.1.7 ¿Podemos acceder a algunas carpetas? 454
3.1.8 ¿El sitio web usa JavaScript? 455
3.1.9 ¿Qué servidor se está utilizando y cuál es su versión? 456
3.1.10 Herramientas para nuestra ayuda 457
3.2 Descubrir la cara oculta de un servidor web 459
3.2.1 Utilización de Burp Suite 459
3.2.2 Utilización de Wfuzz 464
3.3 Analizar la información obtenida 473

4. Pasar al ataque de un sitio web 474
4.1 Enviar datos no esperados 474
4.1.1 Principios y herramientas 474
4.1.2 Utilización de la URL 476
4.1.3 Utilización de formularios 479
4.1.4 Utilización de la cabecera 483
4.1.5 Utilización de cookies 485
4.2 Robo de sesión 486
4.3 El almacén de archivos perjudiciales 489
5. SQL Injection 492
5.1 Preámbulo 492
5.2 Introducción a las bases de datos 492
5.3 Principio de las inyecciones SQL 504
5.4 Técnica de Blind SQL 514
5.5 Herramientas eficaces 536
6. Pasar un CAPTCHA 538
6.1 Presentación de distintos CAPTCHA 538
6.2 Saltarse CAPTCHAs básicos 539
6.3 Saltarse los CAPTCHAs de imágenes 542
7. Las nuevas amenazas en la web 548
8. Contramedidas y consejos de seguridad 549
8.1 Filtrar todos los datos 549
8.2 Fortalecer la identificación del cliente 552
8.3 Configurar sabiamente el servidor 552
9. Utilizar los frameworks para el desarrollo 553
10. Conclusión 554

Capítulo 9
Los fallos de sistema operativo

1. Generalidades 557
2. Contraseñas 558
2.1 Introducción 558
2.2 Averiguar una contraseña en Microsoft Windows 558
2.3 Complejidad 559

2.4 Almacenamiento de contraseñas 560
2.4.1 Detalles acerca del almacenamiento de contraseñas 560
2.4.2 Visualizar las improntas LM y NTLMv1-2 562
2.5 Caso práctico: encontrar las contraseñas de Microsoft Windows . . . 564
2.5.1 Obtención de las contraseñas con Ophcrack liveCD 564
2.5.2 Recuperación de condensado con Responder 565
2.5.3 Recuperación de condensado de una máquina local con SMBEXEC 567
2.5.4 Recuperación de condensado de una máquina local y elevación de privilegios con Mimikatz 569
2.5.5 Recuperación de las contraseñas de un controlador de dominio Windows 2012 R2 576
2.6 Caso práctico: encontrar las contraseñas de GNU/Linux 580
2.7 Caso práctico: encontrar las contraseñas de Mac OS X 581
2.8 Cambiar su contraseña por línea de comandos 582
2.8.1 En Windows 582
2.8.2 En GNU/Linux 583
2.8.3 En Mac OS X 583
3. Usuarios, grupos y permisos del sistema 584
3.1 Gestión de usuarios 584
3.1.1 Definición 584
3.1.2 En GNU/Linux 584
3.1.3 En Windows 585
3.1.4 En Mac OS X 586
3.2 Gestión de grupos 588
3.2.1 En GNU/Linux 588
3.2.2 En Windows 588
3.2.3 En Mac OS X 588
3.3 Asignación de permisos 588
3.3.1 En GNU/Linux 589
3.3.2 En Windows 590
3.3.3 En Mac OS X 591
4. Elevación de privilegios 592
4.1 En UNIX 592
4.1.1 Activación del suid y del sgid 593
4.1.2 Cómo encontrar los scripts suid root de un sistema GNU/Linux 594

4.2 En Windows 594
4.3 El Programador de tareas 599
5. Los procesos 599
5.1 Espiar procesos en Windows 601
5.2 El hooking y la inyección de procesos 601
5.2.1 Ejemplo de hooking de eventos de teclado en Windows 602
5.2.2 Ejemplo de hooking de paquetes de red mediante Netfilter en GNU/Linux 606
5.2.3 Ejemplo de inyección de código en otro proceso en Mac OS X 608
5.3 Las condiciones de concurrencia (race conditions) 609
6. El arranque 610
6.1 Abuso de los modos de arranque degradados 610
6.2 Los ataques de preboot 610
7. Hibernación 611
8. Las RPC 611
8.1 Principio 611
8.2 Acceso remoto al registro 612
9. SeLinux y AppArmor 612
10. La virtualización 612
10.1 Aislamiento 612
10.2 La carga de la raíz o chrooting 613
10.3 Kernel en el espacio de usuario 614
10.4 La máquina virtual 614
10.5 La paravirtualización 615
10.6 Ejemplo de solución de paravirtualización: Proxmox VE 615
10.7 Detección y ataque de una máquina virtual 616
11. Logs, actualizaciones y copias de seguridad 617
11.1 Logs 617
11.2 Actualizaciones 618
11.2.1 Implantación de actualizaciones automáticas en GNU/Linux 618
11.2.2 Implantación de actualizaciones automáticas en Microsoft Windows 618
11.2.3 Implantación de actualizaciones automáticas en Mac OS X . 618
11.3 Copias de seguridad 619

12. Big Data y confidentialidad 619
13. Balance 621

Capítulo 10
Los fallos de aplicación

1. Generalidades 623
2. Nociones de ensamblador 623
2.1 Introducción 623
2.2 Primeros pasos 624
2.2.1 Aprendamos a contar 624
2.2.2 Binario 624
2.2.3 Hexadecimal 625
2.3 ¿Cómo probar nuestros programas? 627
2.3.1 Plantilla de un programa en ensamblador 627
2.3.2 Nuestro primer programa 628
2.4 Instrucciones 629
2.4.1 Comparación 629
2.4.2 Instrucción IF 630
2.4.3 Bucle FOR 631
2.4.4 Bucle WHILE 632
2.4.5 Bucle DO WHILE 632
2.4.6 Directiva %define 634
2.4.7 Directivas de datos 634
2.4.8 Entrada/Salida 634
2.5 Interrupciones 635
2.6 Subprogramas 637
2.7 Heap y pila 638
2.7.1 Heap 638
2.7.2 Pila 639
2.7.3 Llamada y retorno de función: nociones fundamentales 640

3. Fundamentos de shellcodes 642
3.1 Ejemplo 1: shellcode.py 642
3.2 Ejemplo 2: execve() 643
3.3 Ejemplo 3: Port Binding Shell 645
4. Buffer overflow 647
4.1 Definiciones 647
4.2 Conceptos básicos 648
4.3 Stack overflow 649
4.4 Heap overflow 656
4.5 return into libc 660
5. Fallos en Windows 664
5.1 Introducción 664
5.2 Primer paso 664
5.2.1 En modo consola 665
5.2.2 Depuración 666
5.2.3 El problema de un shellcode grande 670
5.2.4 Ejecución de una función no prevista 673
5.2.5 Otros métodos 675
5.3 El método de call [reg] 675
5.4 El método pop ret 676
5.5 El método push return 676
5.6 El método jmp [reg] + [offset] 677
5.7 El método blind return 677
5.8 ¿Qué podemos hacer con un pequeño shellcode? 677
5.8.1 Principio 677
5.8.2 En la práctica 678
5.9 El SEH (Structured Exception Handling) 678
5.9.1 Conceptos básicos 678
5.9.2 SEH, protecciones 680
5.9.3 XOR y SafeSEH 681
5.10 Saltarse las protecciones 682
5.10.1 Stack cookie, protección /GS 682
5.10.2 Ejemplo: sobrepasar la cookie 686
5.10.3 SafeSEH 689

6. Caso real: Ability Server 690
6.1 Fuzzing 690
6.2 Exploit 692
7. Caso real: MediaCoder-0.7.5.4796 698
7.1 Cuelgue del software 698
7.2 Comprobación de los valores 703
7.3 Finalización del exploit 703
8. Caso concreto: BlazeDVD 5.1 Professional 706
9. Conclusión 709
10. Referencias 710

Capítulo 11
Análisis forense

1. Introducción 711
1.1 El cerebro 712
1.2 La memoria 713
1.3 Los archivos 715
2. Los métodos 716
2.1 Preparación y entorno 716
2.2 Búsqueda y análisis de archivos 717
3. Herramientas 719
3.1 Herramientas de análisis de red 719
3.1.1 Wireshark 719
3.1.2 tcpdump 720
3.1.3 Scapy 720
3.2 Herramientas de análisis de memoria 721
3.2.1 Volatility 721
3.3 Herramientas de análisis binario 722
3.3.1 Hexdump 722
3.3.2 Readelf 722
3.3.3 Gdb 723
3.4 Herramientas de análisis de sistema 723
3.4.1 The coroner's toolkit 723
3.4.2 Logstash 724

4. Conclusión 724

Capítulo 12
La seguridad de los routers

1. La funcionalidad de un router 725
   1.1 Router 725
   1.2 Switch 725
   1.3 Telefonía 726
   1.4 Televisión 726
   1.5 Servidor multimedia 726
2. Los diferentes routers 727
   2.1 Orange 727
   2.2 ONO 728
3. La configuración de los routers 728
   3.1 El modo módem 728
   3.2 El modo router 729
   3.3 Las funciones telefónicas 730
4. La configuración por defecto, un peligro 731
   4.1 La interfaz de administración web 731
   4.2 El Wi-Fi 732
   4.3 Los servicios: SSH, Telnet, Samba, TR069 732
5. Instalación de un firmware alternativo 734
   5.1 ¿Para qué? 734
   5.2 Conexión al puerto consola 734
6. La seguridad de los firmware oficiales 740
   6.1 Los fallos en estos últimos años 740
   6.2 Y ¿En la actualidad? 741

Capítulo 13
Los fallos de hardware

1. Introducción 743
2. La caja de herramientas 744
   2.1 Las herramientas básicas 744
      2.1.1 Juego de destornilladores 744
      2.1.2 El multímetro 745
      2.1.3 Placa de pruebas (protoboard) 745
      2.1.4 Los cables Dupont 746
      2.1.5 Soldador 746
      2.1.6 Arduino 747
      2.1.7 Materiales de recuperación 747
   2.2 Usuario regular 748
      2.2.1 Adaptador USB RS232 TTL 748
      2.2.2 Analizador lógico 748
      2.2.3 Interfaz JTAG 749
      2.2.4 El bus pirate de la casa Dangerous Prototypes 749
      2.2.5 SDR de bajo coste 750
   2.3 Usuario avanzado 751
      2.3.1 Software de diseño de PCB 751
      2.3.2 Programador 751
      2.3.3 Equipo de electricista 753
   2.4 Metodología de ingeniería inversa de hardware 753
      2.4.1 Ataque empleando Sniffing I2C 755
      2.4.2 Ataque empleando Sniffing UART modem 758
   2.5 Estudio y trasteo con T2G y Arduino 758
      2.5.1 Creación de un lector de tarjetas T2G 759
      2.5.2 Emulador parcial de tarjeta T2G 767

Capítulo 14
Black Market

1. Introducción 771
2. Deep Web, Dark Web, darknet, Black Market. 771
3. Black Market, entre lo visible y lo invisible 772
4. Funcionamiento. 773
5. ¿Anonimato de las tiendas? 775
6. Manual de uso de TOR. 776
   6.1 Instalación. 776
   6.2 Configuración de la seguridad 777
   6.3 Verifique su IP. 778
   6.4 Navegue. 779
   6.5 Cambiar de IP 779
   6.6 Actualización 779
7. Las referencias del Black Market. 780
8. Traductor de Onion. 784
9. Vocabulario 784
10. Lista de tiendas y autoshops. 786

Índice. 787

Ediciones ENI

Hacking y Forensic

Desarrolle sus propias herramientas en Python

Colección Epsilon

Contenido

Podrá descargar algunos elementos de este libro en la página web de Ediciones ENI: **http://www.ediciones-eni.com**. Escriba la referencia ENI del libro **EPT2HAFO** en la zona de búsqueda y valide. Haga clic en el título y después en el botón de descarga.

Prólogo

Capítulo 1
Python: Los fundamentos

1. Introducción 13
2. Historia 15
3. Características del lenguaje 15
4. Tipos de datos 19
   - 4.1 Los números 19
   - 4.2 Las operaciones aritméticas 23
   - 4.3 Las cadenas de caracteres 24
   - 4.4 Las tuplas 27
   - 4.5 Las listas 28
   - 4.6 Los diccionarios 32
   - 4.7 Tipos de datos adicionales 34
5. Estructuras condicionales y repetitivas 36
   - 5.1 Test if ... elif ... else 36
   - 5.2 Bucle while 37
   - 5.3 Bucle for 38
   - 5.4 Las listas por comprensión (list comprehension) 39
6. Funciones, módulos y paquetes 41
   - 6.1 Definición y llamadas de función 41
   - 6.2 Espacios de nombres 43
   - 6.3 Funciones particulares 44
   - 6.4 Módulos 45

6.5 Paquetes 46
6.6 Instrucción yield 47
7. Las clases 48
7.1 Declaración de una clase 49
7.2 Sobrecarga de operadores 50
7.3 Propiedades, accesores y mutadores 52
7.4 Herencia 53
7.5 Polimorfismo 54
8. Manipulación de archivos 55
9. Las excepciones 58
10. Módulos útiles para la continuación del libro 61
10.1 Módulo sys 61
10.2 Módulo os 63
10.3 Módulo re 68
10.4 Módulos pickle y shelve 72
10.5 Módulos de bases de datos 74
10.5.1 MySQLdb 74
10.5.2 PostgreSQL 79
10.6 Módulo thread 85
10.6.1 Principio del módulo 86
10.6.2 Threading 86
10.6.3 Clase Lock() 87
11. Conclusión 89

Capítulo 2
La red

1. Introducción 91
2. Los sockets 92
2.1 Creación de un socket 92
2.2 Intercambio de datos 93
2.3 Socket en UDP 94

2.4 Los errores 97
2.5 Socket y FTP 99
3. Creación de un servidor 101
3.1 Introducción 101
3.2 Conexión cliente 103
3.3 Conversación con el cliente 105
3.4 Creación de un troyano básico 106
3.5 Creación de un troyano más complejo 109
4. DNS: Domain Name Server 114
4.1 Introducción 114
4.1.1 ¿Qué significa DNS? 115
4.1.2 Principales registros DNS 115
4.2 nslookup básico 117
4.3 Reverse lookup 120
4.4 La librería DNS 121
4.5 Consulta a partir de un servidor especificado 122
4.6 Formato de los resultados obtenidos 124
5. FTP: File Transfer Protocol 127
5.1 Introducción 127
5.2 FTP anónimo 127
5.3 Descargas de archivos ASCIII 128
5.4 Descargas de archivos binarios 130
5.5 Descarga avanzada de archivos binarios 131
5.6 Envío de datos 132
5.7 Los errores FTP 133
5.8 Listar el contenido de las carpetas 134
5.9 Otros comandos útiles 137
5.10 Descarga recursiva de datos 138
6. Las expresiones regulares 140
6.1 Introducción 140
6.2 El módulo re 142

6.3 Los métodos útiles 143
6.3.1 Método search() 143
6.3.2 Método match() 144
6.3.3 Método sub() 145
6.3.4 Ir más allá con los grupos 146
6.4 ¿Cómo construir su patrón o expresión? 146
7. La Web 148
7.1 Introducción 148
7.2 Recuperación de una página fuente 149
7.3 Métodos GET y POST 150
7.3.1 Método GET 151
7.3.2 Método POST 152
7.4 Gestión de errores 153
7.4.1 Errores de conexión: urllib2.URLErrorv 153
7.4.2 Error 404 153
7.5 Autenticación 154
8. Analizar páginas HTML y XHTML 156
8.1 Introducción 156
8.2 Primer enfoque 156
8.3 Trabajo con páginas "reales" 159
8.3.1 Ampersand 159
8.3.2 Caracteres especiales 160
8.4 BeautifulSoup 162
8.4.1 Introducción 162
8.4.2 Recuperar los enlaces 163
9. El XML 165
9.1 Introducción 165
9.2 Representación de un archivo XML 165
9.3 Python y XML 166
9.4 Leer un canal RSS 170

10. Los e-mails 170
10.1 Introducción 170
10.2 La librería smtplib 172
10.2.1 El cuerpo del texto 172
10.2.2 Mail con archivo adjunto 174
10.3 Análisis de e-mails 176
10.4 Analizar las fechas 179
10.5 Errores y depuración 180
10.6 Mail y POP 182
11. SSL y Python 185
11.1 Introducción 185
11.2 Utilización de OpenSSL 186
11.3 Verificar los certificados 188
12. La utilización de bases de datos 192
12.1 Introducción 192
12.2 MySQLdb 193
12.2.1 Recordatorio 193
12.2.2 Utilización 193
12.3 PostgreSQL 198
12.3.1 Introducción y primera conexión 198
12.3.2 Ejecutar los comandos 199
12.3.3 Ocultar los cambios 201
12.3.4 Repetición de comandos 202
12.3.5 Recuperar los datos 203
13. Conclusión 205
14. Puesta en práctica 206
14.1 Caso 1: Escaneo de puertos 206
14.2 Caso 2: Envío de mails 208
14.3 Caso 3: Fuzzing FTP 214
14.4 Caso 4: Parsing de página web 215
14.5 Caso 5: Fuerza bruta MySQL 217

Capítulo 3
Red: la librería Scapy

1. Introducción 219
2. Programación de red con Scapy 221
   2.1 Lista de protocolos soportados 221
   2.2 Algunas nociones sobre las redes 227
      2.2.1 Topología de redes 227
      2.2.2 Los diferentes tipos de redes 228
      2.2.3 ¿Qué es un protocolo? 229
      2.2.4 Dirección IP 229
      2.2.5 Las clases de direcciones 230
      2.2.6 La máscara de subred 231
      2.2.7 El modelo OSI 231
   2.3 Operaciones básicas 236
      2.3.1 Comandos básicos 236
      2.3.2 Fabricación de paquetes 239
      2.3.3 Las entradas/salidas 245
      2.3.4 Entramos en detalle 249
   2.4 Utilización avanzada: seguridad de red 257
      2.4.1 traceroute 257
      2.4.2 Sniffing 263
      2.4.3 Scan TCP 266
      2.4.4 Tunneling 267
   2.5 Algunos ejemplos sencillos de "one-liner" 268
      2.5.1 Scan ACK 268
      2.5.2 Scan Xmas 269
      2.5.3 Scan IP 271
      2.5.4 Los distintos ping 271
      2.5.5 Los ataques clásicos 271

3. Scapy e IPv6 272
3.1 Nociones de IPv6 272
3.1.1 Aspectos generales 272
3.1.2 IPv6: RFC 2373 273
3.2 Aplicación 275
3.2.1 Consulta ICMP IPv6. 275
3.2.2 Enrutamiento de paquetes IPv6. 275
3.2.3 Ejemplo de enrutamiento de cabecera. 276
3.2.4 traceroute 276
3.2.5 IPv6 NA. 276
3.2.6 Aviso de daemon muertos 277
3.2.7 Ejemplo 277
4. Otros ejemplos 278
5. Conclusión 279
6. Puesta en práctica 280
6.1 Canal encubierto IP 280
6.2 Detección de Rogue AP (Access Point) 281
6.3 IP Spoofing 282
6.4 Spoofing IPv6 de los vecinos 283

Capítulo 4
Depuración en Windows

1. Introducción 285
2. El módulo ctypes de Python 286
3. Primer enfoque 288
4. Estado de los registros 302
4.1 Enumeración de los hilos (threads) 302
4.2 Recuperar los valores de los registros 303
5. Los eventos del debugger 305

6. Los puntos de parada (breakpoints) 316
6.1 Puntos de parada software 316
6.2 Puntos de parada hardware 318
6.3 Punto de parada de memoria 320
7. La librería PyDbg 321
7.1 Violación de acceso de las cabeceras (handlers) 323
7.2 Process snapshot 326
8. Puesta en práctica: Hooking 332

Capítulo 5
El fuzzing

1. Introducción 337
2. Fuzzing FTP 338
3. Fuzzing con Scapy 342
4. Fuzzing con PyDbg: Format string 345
4.1 Introducción 345
4.2 Fuzzer de archivos 346
5. Sulley 351
5.1 Introducción 351
5.2 Instalación 351
5.2.1 Instalación normal 351
5.2.2 Instalación no estándar 354
5.3 Utilización 362
5.3.1 Estructura del directorio de Sulley 363
5.3.2 Representación de datos 365
5.3.3 Primitivas estáticas y aleatorias 365
5.3.4 Los enteros 366
5.3.5 Cadenas de caracteres y delimitadores 367
5.3.6 Las extensiones Fuzz Library 368
5.3.7 Blocks 369
5.3.8 Grupos 370

5.3.9 Codificador 371
5.3.10 Dependencias 371
5.3.11 Block helpers 372
5.3.12 Legos 374
6. Puesta en práctica 375
6.1 Fuzzing 1: HTTP 375
6.2 Fuzzing 2: FTP 378

Capítulo 6
Tratamiento de imágenes

1. Introducción 381
2. Utilización 382
2.1 La clase Image 382
2.2 Leer y escribir 383
2.3 Cortar, pegar y fusionar 386
2.4 Transformaciones geométricas 387
2.5 Transformación de los colores 388
2.6 Mejora de imágenes 388
2.6.1 Filtros 388
2.6.2 Operaciones sobre los puntos 388
2.6.3 Mejoras 389
3. Ejemplos de uso 390
3.1 Creación de un captcha 390
3.2 Captura de Imagen y transformación 391
3.3 Lectura del captcha 392

Capítulo 7
Un poco más sobre la Web

1. Introducción 397
2. Recordemos lo básico 397
3. Mapping de sitios web 399
4. Fuerza bruta de carpetas o de ubicación de archivos 401
5. Fuerza bruta autenticación HTML 404
6. Selenium 407
   6.1 Introducción 407
   6.2 Instalación. 408
   6.3 Primera prueba 408
   6.4 Captura de pantalla con Selenium 409
7. Conexión a un sitio web y navegación 410
8. Conclusión 415

Capítulo 8
Análisis forense

1. Introducción 417
2. Criptografía y otros 418
   2.1 ROT13. 418
   2.2 Base 64. 420
   2.3 Hash 423
3. Extracción de metadatos de los archivos. 425
   3.1 Metadatos MP3 425
   3.2 Metadatos de imágenes 427
   3.3 Metadatos PDF 428
   3.4 Metadatos OLE2. 428
   3.5 Caso concreto 429

4. Archivos ZIP 430
4.1 Leer de un archivo ZIP 430
4.2 Ataque de fuerza bruta de contraseñas 431
5. Leer de un archivo OpenOffice o Word. 431
5.1 Recorrer un árbol 431
5.2 Buscar en un documento OpenOffice 432
5.3 Buscar en un documento Word 433
6. E-mail. 434
6.1 Encontrar e-mails en los archivos 434
6.2 Buscar en el buzón de correo 435
7. Esteganografía 436
7.1 Buscar información en una imagen 436
7.2 Ocultar un mensaje en una imagen. 437
7.3 Lectura del mensaje 439
8. Volatility 439
8.1 Información de la imagen 440
8.2 Proceso y DLL 441
8.3 Captura de contraseñas hash 442
8.4 Ejemplo de programa 444
9. Análisis de puntos de acceso inalámbrico en base al registro 451
10. Recuperar los elementos eliminados (de la papelera) 453
11. Puesta en práctica 456
11.1 Descifrado 456
11.2 OCR. 456
11.3 ZIP 457
11.4 Scapy y la geolocalización 458

Índice 459