

Índice

Introducción	15
Capítulo I	
Conceptos básicos.....	17
1. Definiciones	17
Software fiable vs Software seguro	17
Bug.....	17
Exploit	18
Payload	18
Shellcode	18
0-day exploit.....	19
Buffer Overflow.....	20
SQL Injection.....	20
XSS (Cross-Site Scripting).....	20
Metasploit.....	21
Módulos.....	21
Interfaces Metasploit	21
Herramientas del framework	23
Arquitectura de Metasploit.....	25
Tipos de módulos en Metasploit framework	26
2. Versiones de Metasploit.....	27
Metasploit Community Edition	27
Metasploit Pro.....	28
Metasploit Express	28
3. El test de intrusión o pentest.....	29
4. Fases del test de intrusión	30
El contrato: alcance y términos del test de intrusión.....	31
Recolección de información	31
Análisis de vulnerabilidades.....	31
Explotación de las vulnerabilidades	32
Post-explotación del sistema	32
Generación de informes.....	33
5. Comandos básicos de Metasploit.....	33
Comandos de ayuda y búsqueda.....	35
Comandos de interacción y configuración.....	36
Comandos de base de datos	40
6. Notas éticas.....	42
Capítulo II	
Preliminares.....	45
1. Ámbito.....	45

2. Recogida de información.....	46
Técnicas pasivas.....	46
Técnicas activas.....	50
3. Escáneres de vulnerabilidades.....	57
Compatibilidad con los ficheros de información de escáneres.....	57
Escáner nessus e importación de datos.....	58
Escáner MBSA e importación de datos.....	61
Técnica Autopwn.....	61
4. Escáneres dirigidos a servicios.....	66
El objetivo.....	66
Herramientas auxilari en Metasploit.....	66

Capítulo III

El arte de la intrusión..... 69

1. Ámbito.....	69
2. Payloads.....	70
3. Intrusión sin interacción.....	72
PoC: La primera intrusión.....	72
PoC: Denegación de servicio y las pérdidas.....	74
4. Intrusión con interacción.....	76
PoC: Los archivos adjuntos pueden ser muy peligrosos.....	77
PoC: QuickTime y sus conexiones por Rubén Santamarta.....	79
Dark Shadows, el mundo oscuro y real.....	82
PoC: La técnica Browser Autopwn.....	83
5. Automatizando las órdenes.....	86
Ejemplo: Descubrimiento básico.....	87
Creación de un resource script.....	89
6. Servidores Rogue.....	90
PoC: Rogue DHCP, Fake DNS y Applet de Java.....	91
Fake DNS por José Selvi.....	95
7. Personalización y actualización del framework.....	96
Actualización controlada de recursos.....	97
Ejemplo: Descarga de exploit y adición al framework.....	98
8. Hackear Windows 7 y Windows 2008 R2 con EternalBlue.....	99

Capítulo IV

Meterpreter & Post-Exploitation..... 105

1. Ámbito.....	105
2. Comandos básicos de Meterpreter.....	106
Core commands.....	107
Stdapi.....	109
Priv.....	114
3. Scripts de Meterpreter.....	116
winenum: el informador.....	117
Los scripts get.....	119
Los scripts post.....	122
Los multi scripts.....	129
4. Módulos de Meterpreter.....	130
Módulo: Espia.....	131
Módulo: Incognito.....	131
PoC: Recuperando hashes SMB con snarf_hashes.....	133
Módulo: Sniffer.....	134

PoC: Espiando la red de la víctima.....	135
5. Pass the hash.....	139
Teoría de credenciales Windows.....	139
PoC: Llegando más lejos gracias a la suplantación de identidades.....	141
6. Pivoting.....	146
7. Persistencia.....	146
PoC: Metsvc y la conexión directa.....	147
PoC: Persistence y la conexión inversa.....	149
8. Migración a un proceso.....	151
PoC: De proceso a proceso capturando pulsaciones.....	152
9. Scraper.....	153
10. Actualizando de cmd a Meterpreter.....	154
11. Railgun.....	154
12. Otras PoC interesantes.....	156
PoC: Meterpreter, troyanos y rootkits educativos.....	156
PoC: Explotado e infectado.....	159
PoC: Volcado de memoria remota y análisis.....	161
PoC: VNC Payload.....	164
PoC: Port forwarding.....	166
13. Buscando vulnerabilidades en la post-explotación.....	168
14. Metasploit Web Delivery: Simplificando el despliegue de payloads.....	170
PoC: Obtención de Meterpreter con Powershell.....	171

Capítulo V

Otras msf tools.....	173
1. msf tools.....	173
2. Msfcli: El poder de la línea.....	174
Modos de msfcli.....	175
Beneficios del uso de msfcli.....	177
Teoría de conexiones.....	178
PoC: Servidor de exploits y máquina privada para las sesiones.....	180
3. Msfpayload: payload a gusto del consumidor.....	182
Modos de msfpayload.....	182
PoC: Obtención de payload para implementación en exploit.....	185
PoC: Creación de un troyano casero.....	187
PoC: Creación de un paquete DEB malicioso.....	190
Payloads Vs Antivirus.....	192
4. Msfencode: Evadir la detección.....	193
Codificación con msfencode.....	194
PoC: Creación de un ejecutable codificado.....	195
Codificación múltiple.....	196
PoC: Creación de un ejecutable multicodificado.....	196
Teoría sobre ejecutables personalizados y sigilosos.....	197
PoC: Creación de un ejecutable personalizado.....	198
PoC: Creación de un ejecutable personalizado y sigiloso.....	199
5. Msfvenom: Payload y evasión.....	202
Beneficios del uso de msfvenom.....	202
Opciones de msfvenom.....	203
Creación de shellcode codificado.....	204
PoC: Creación de ejecutable codificado con msfvenom.....	205
6. Msfd: Gestión remota.....	206

Opciones de msfd	206
PoC: Conexión en un puerto personalizado y preparando exploit	207
7. Manipulación de memoria	209
Msfelfscan y msfpescan	209
8. Armitage y el uso de divulgación	209

Capítulo VI

Ingeniería social con SET	215
1. Ingeniería social	215
2. ¿Qué es y qué propone?	216
Configuración de SET	218
3. Vector de ataque: phishing	219
PoC: Ataque dirigido a un dominio	219
4. Vector de ataque: web	223
PoC: Recolectando credenciales	224
PoC: JAVA applet	227
5. Medios infectados	230
6. Payloads como ejecutables	231
7. Dispositivos USB HID	231
8. Ataques por correo electrónico	232
9. Falsificación de SMS	233
10. Vector de ataque: Wireless	234
11. Vector de ataque QRCode	236
PoC: Ingeniería social con un QRCode malicioso	236
12. Vector de ataque PowerShell	237
PoC: Inyección de Meterpreter a través de PowerShell	238
13. PoC: El mundo del spoofing y SET	239

Capítulo VII

Metasploit en dispositivos móviles	243
1. Introducción	243
2. Instalación de Metasploit en dispositivos iOS	244
Requisitos previos e instalación	244
Instalación del módulo SET (Social Engineering Toolkit) en iOS	246
Instalar Fast-Track en iOS	247
1. Ataques en dispositivos iOS	247
Atacar el terminal con un exploit remoto: El caso de iOS	247
Atacar las comunicaciones WiFi de dispositivos iOS	253
Atacar las comunicaciones VPN de iOS	255
Atacar las comunicaciones BlueTooth de un iOS	256
Atacar las comunicaciones 3G o GPRS de iOS	256
Ataques man in the middle en iOS	257
Ataques de Juice Jacking a iOS	258
Post-Explotación: Ataque al backup de un terminal iOS	259
3. Conclusiones	263

Capítulo VIII

Introducción al desarrollo en Metasploit	265
1. ¿Por qué escogieron Ruby?	265
2. Módulos	266
Tipo: Exploit remoto	266

Tipo: Exploit local	269
Tipo: Auxiliary.....	271
3. Meterpreter	275
El objeto client.....	275
Scripts	281
Mixins	287
4. Montaje de tu propio repositorio	288
Capítulo IX	
Metasploit 5.0	301
PoC: Meterpreter de Android en Metasploit v5.0.....	303
Índice alfabético	307
Índice de imágenes y tablas.....	309