

Índice

Introducción	11
Capítulo I	
Estrategia de la intrusión	13
1. Introducción.....	13
2. El proceso de staging.....	14
3. Staged/Stageless	18
4. Payloads en entornos restrictivos.....	20
Reverse TCP All Ports	20
Reverse Hop HTTP	23
WinINet/WinHTTP stagers	25
DNS TXT Record Payload.....	29
5. Ocultación, seguimiento y protección de la shell.....	32
Hidden Bind Shell / IP Knock Bind Shell.....	33
Identificador de Payload: UUID.....	36
Autenticación del stager: Certificate Pinning.....	39
6. Migración y respaldo de la shell.....	42
Meterpreter: migrate.....	43
Prependmigrate	45
Sesiones de respaldo	47
7. Técnicas de evasión y ofuscación	51
Unicorn Scan / Invoke-Obfuscation / DKMC.....	52
Process Hollowing con Meterpreter.....	59
Ofuscación del stage	62
Modificación del template.....	64
Shellter	71
EAT vs IAT.....	73
Falsificación de firmas.....	76

Capítulo II

Desarrollo e integración de payloads	79
1. Introducción.....	79
2. Reflective DLL injection	80
Reflective Injection con Empire.....	87
Meterpreter Injection con Fuzzbunch	89
3. Payload single	93
4. Stager Payload	98

Capítulo III

Desarrollo e integración de nuevos módulos en Metasploit.....	105
1. Introducción.....	105
2. IRB (Interactive Ruby shell) y Meterpreter Scripts	105
3. Módulos de Post-Explotación.....	113
Railgun.....	124
4. Módulos Auxiliares.....	130
PoC: Módulo auxiliar para el CVE-2013-5572 (Zabbix)	139
PoC: Retromalware. Detectando y controlando un Netbus con MSF.....	143
5. Integración de exploits	148
PoC: Integrando un exploit básico	157
Local exploits.....	161
Fileformat exploits	166
6. Automatización de tareas	168
RPC API.....	171

Capítulo IV

Pentesting avanzado con Metasploit	177
1. Introducción.....	177
2. Túneles, pivoting y proxies	177
PoC: Pivoting entre redes.....	178
PoC: MitM en remoto a través de una VPN y Meterpreter.....	184
PoC: Pivoting + Proxychains	189
PoC: Pivoting con túneles SSH y Metasploit.....	191
PoC: Portfwd en Metasploit.....	194
PoC: PortProxy en Windows y Metasploit.....	198
3. Explotación local y obtención de privilegios.....	203

Escalada de privilegios.....	204
PoC: Bypass UAC x86/x64.....	208
PoC: Bypass UAC. DLL Hijacking y CompMgmtLauncher.exe	210
PoC: Bypass UAC con eventvwr	214
Bypass UAC con fodhelper.....	218
Elevación de privilegios en sistemas OS X.....	221
PoC: Rootpipe & Rootpipe II & Client-Side en Firefox	221
PoC: Dylid_print_to_file_root - un exploit que cabe en un tweet	224
PoC: Sudo password bypass en OS X	226
4. Credenciales y movimientos laterales.....	227
Volcado de hashes	229
SMB Relay Attacks	234
Mimikatz	235
Persistencia mediante Golden Tickets.....	236
Recuperación de hashes del DC vía MS-DRSR	238
PoC: NetRipper. Hooking de procesos con Meterpreter	239
5. Extensiones de interés	241
6. Listado de módulos para OS X	244
Índice alfabético	247
Índice de imágenes	249

