

Índice

Introducción	13
Capítulo I	
Conceptos básicos de PowerShell	15
1. ¿Qué es y qué engloba a PowerShell?.....	15
2. Instalación de una PowerShell	16
Los requisitos	16
3. ¿Cómo puede ayudar en un pentest?.....	18
4. Versiones.....	19
PowerShell 1.0	19
PowerShell 2.0	19
PowerShell 3.0	20
PowerShell 4.0	20
PowerShell 5.0	20
PowerShell 6.0 (Versión Core).....	21
PowerShell 7.0	21
5. Lo más básico: Comenzando	21
Cmdlet.....	22
Alias	22
Comandos *NIX y CMD en PowerShell	23
Provider.....	23
Parámetros.....	25
Archivos.....	26
Pipe y pipeline.....	26
Módulos.....	27
6. La ayuda en PowerShell al detalle	27
¿Help o get-help?	28
Categorías.....	28
Atajos de teclado.....	29
7. Seguridad en PowerShell	29

Políticas de ejecución de PowerShell.....	30
Ámbitos	31
Bypass a la política de ejecución de PowerShell	31
La ejecución remota y cómo comunicarse	32
Fortificar la información en la línea de comandos	36
Creación de una cadena segura	37
Leyendo las cadenas seguras.....	38
Las credenciales tratadas por PowerShell	38
Scripts firmados digitalmente.....	39
Los requisitos	40
Certificados	40
Firma tu script	42
AMSI: AntiMalware Scan Interface.....	42
Restricción de lenguaje o “Constrained Language”.....	44
PowerShell Transcription.....	45

Capítulo II

Scripting en PowerShell	47
1. Interactuando con la shell.....	47
Personalización del entorno	48
Modificación del entorno	48
Perfiles.....	50
2. Entorno de Scripting: PowerShell ISE.....	51
3. Variables.....	54
Variables necesarias en el desarrollo.....	55
4. Operadores.....	56
Operadores aritméticos.....	56
Operadores de comparación.....	56
Operadores lógicos.....	57
Operadores de tipo	58
Operadores de intervalo	58
5. Arrays y hash tables	58
Las dimensiones de los arrays.....	59
Tratamiento de datos	59
Tablas hash.....	60
6. Los cmdlet de salida	61
7. Condicionales.....	61
La sentencia If.....	62
El condicional de selección: Switch.....	62
PoC: CheckVBox.....	63

8. Bucles	64
For.....	65
Foreach.....	65
Do-While.....	66
While.....	66
PoC: Encontrando servicios vulnerables.....	67
9. Creación de objetos .NET	68
New-Object.....	68
Creación de objetos COM.....	69
Filtros.....	70
10. Utilización de clases y métodos de .NET	71
11. Funciones	73
El provider de las funciones.....	73
Crear funciones.....	73
12. Administración y recopilación de información	76
Recopilando información sobre el software de la máquina.....	78
13. WMI	79
Clases e instancias.....	80
Ejemplo 1: Capacidad de disco.....	81
Ejemplo 2: Estado de los servicios.....	81
Monitorización de recursos.....	82
14. Un exploit con PowerShell	83
PoC: Explotando Shellshock desde PowerShell.....	84
15. Un bot en PowerShell para pentesting	88
16. Workflows	92
El flujo.....	93
17. Otros productos	96
Directorio activo, ¿Por qué?.....	97
ADSI: La API para equipos locales.....	97
ADSI: La API para Active Directory.....	100
Cmdlets desde Windows 2008 R2.....	103
Internet Information Services.....	106
18. Wannacry File Restorer escrito en Powershell	111
Ejecución del script en un dominio Microsoft a través de Powershell.....	114

Capítulo III

PowerShell puro: El arte del pentesting..... 117

1. Introducción..... 117

2. Powercat: la navaja suiza	118
Conexión simple.....	120
Dar y recibir shells	121
Transferencia de archivos.....	121
Escanear puertos TCP con Powercat.....	122
PoC: Descarga y ejecución de Shellcodes desde Powercat.....	122
PoC: Powercat y el relay para pivoting.....	124
3. Veil-Framework.....	125
PowerUp.....	126
PowerView	135
4. Posh-SecMod.....	142
Módulos para comenzar	144
Discovery	147
Post-Explotación con Posh-SecMod.....	150
Servicios externos	157
5. PowerSploit.....	163
Code Execution	164
Script Modification.....	165
Persistence.....	166
Exfiltration.....	166
Otros: Mayhem, Recon y AV Bypass.....	167
PowerShell Arsenal: Disassembly.....	168
PowerShell Arsenal: Malware Analysis	168
PowerShell Arsenal: Memory Tools	169
PowerShell Arsenal: Parsers	169
PowerShell Arsenal: Windows Internals.....	170
PowerShell Arsenal: Misc.....	170
PoC: Code Execution + Recon.....	171
PoC: Post-Exploitation con Exfiltration + Persistence	176
6. Nishang.....	179
Prasadhak, Scan, Escalation y Antak	180
Backdoors.....	181
Client.....	182
Execution.....	183
Gather.....	184
Pivot	185
Shells.....	186
Utility	187
PoC: Backdoors, jugando con DNS y Wireless	188
PoC: Client-Side Attack con Nishang	191
PoC: Shells	192

7. Powershell Empire	193
PoC: Conectando el agente y el listener.....	194
PoC: Bypass a UAC, inyección en proceso y ejecución con Powershell Empire.....	198
Empire 3.X, 4.X y las nuevas versiones.....	202
8. Otros scripts en acción	204
PoC: Sniffing y Spoofing de protocolos con PowerShell.....	205
PESecurity.....	206
Respuesta ante incidentes.....	206
Poc: Tater y la escalada de privilegios	209
PoC: La escalada de privilegios con ms16-135	212
DeepBlueCli y el threat hunting con Powershell	213
Bypass AMSI: Técnicas y automatización.....	215
Bypass Constrained Language.....	217
9. iBombShell.....	218
 Capítulo IV	
PowerShell y otras herramientas: Pentesting sin límites	221
1. La post-explotación con PowerShell.....	221
2. PowerShell: Ejecución de payloads	222
3. PowerShell Shellcode Injection con Python.....	224
4. Payloads de PowerShell en Metasploit	225
5. Posh-Metasploit	228
Console.....	229
Db.....	230
Jobs.....	232
Module	233
Plugin	235
Posh.....	235
Session.....	236
Variables.....	238
 Índice de imágenes	239
 Índice de tablas.....	245
 Índice alfabético	247
 Otros libros publicados.....	249

