

# Índice

<b>Introducción .....</b>	<b>13</b>
<b>Capítulo I</b>	
<b>Conceptos básicos de PowerShell .....</b>	<b>15</b>
<b>1. ¿Qué es y qué engloba a PowerShell? .....</b>	<b>15</b>
<b>2. Instalación de una PowerShell .....</b>	<b>16</b>
Los requisitos .....	16
<b>3. ¿Cómo puede ayudar en un pentest? .....</b>	<b>18</b>
<b>4. Versiones .....</b>	<b>19</b>
PowerShell 1.0 .....	19
PowerShell 2.0 .....	19
PowerShell 3.0 .....	20
PowerShell 4.0 .....	20
<b>5. Lo más básico: Comenzando .....</b>	<b>20</b>
Cmdlet .....	20
Alias .....	21
Comandos *NIX y CMD en PowerShell .....	22
Provider .....	22
Parámetros .....	24
Archivos .....	24
Pipe y pipeline .....	25
Módulos .....	25
<b>6. La ayuda en PowerShell al detalle .....</b>	<b>26</b>
¿Help o get-help? .....	27
Categorías .....	27
Atajos de teclado .....	27
<b>7. Seguridad en PowerShell .....</b>	<b>28</b>
Políticas de ejecución de PowerShell .....	29
Ámbitos .....	29



Bypass a la política de ejecución de PowerShell .....	30
La ejecución remota y cómo comunicarse .....	31
Creación y configuración de una sesión remota .....	31
Las ejecuciones remotas .....	33
Utilidades remotas .....	34
Fortificar la información en la línea de comandos .....	35
Creación de una cadena segura .....	35
Leyendo las cadenas seguras.....	36
Las credenciales tratadas por PowerShell .....	37
Scripts firmados digitalmente.....	38
Los requisitos .....	38
Certificados .....	39
Firma tu script .....	41

## Capítulo II

<b>Scripting en PowerShell .....</b>	<b>43</b>
<b>1. Interactuando con la shell.....</b>	<b>43</b>
Personalización del entorno .....	44
Modificación del entorno .....	44
Perfiles.....	46
<b>2. Entorno de Scripting: PowerShell ISE.....</b>	<b>47</b>
<b>3. Variables.....</b>	<b>50</b>
Variables necesarias en el desarrollo.....	51
<b>4. Operadores.....</b>	<b>52</b>
Operadores aritméticos.....	52
Operadores de comparación.....	52
Operadores lógicos.....	53
Operadores de tipo .....	54
Operadores de intervalo .....	54
<b>5. Arrays y hash tables .....</b>	<b>54</b>
Las dimensiones de los arrays.....	55
Tratamiento de datos .....	55
Tablas hash .....	56
<b>6. Los cmdlet de salida .....</b>	<b>57</b>
<b>7. Condicionales.....</b>	<b>57</b>
La sentencia If.....	58
El condicional de selección: Switch.....	58
PoC: CheckVBox.....	59
<b>8. Bucles.....</b>	<b>60</b>



For .....	61
Foreach.....	61
Do-While.....	62
While.....	62
PoC: Encontrando servicios vulnerables.....	63
<b>9. Creación de objetos .NET .....</b>	<b>64</b>
New-Object .....	64
Creación de objetos COM .....	65
Filtros .....	66
<b>10. Utilización de clases y métodos de .NET .....</b>	<b>67</b>
<b>11. Funciones.....</b>	<b>69</b>
El provider de las funciones.....	69
Crear funciones .....	69
<b>12. Administración y recopilación de información.....</b>	<b>72</b>
Recopilando información sobre el software de la máquina .....	74
<b>13. WMI.....</b>	<b>75</b>
Clases e instancias.....	76
Ejemplo 1: Capacidad de disco.....	77
Ejemplo 2: Estado de los servicios.....	77
Monitorización de recursos.....	78
<b>14. Un exploit con PowerShell.....</b>	<b>79</b>
PoC: Explotando Shellshock desde PowerShell .....	80
<b>15. Un bot en PowerShell para pentesting .....</b>	<b>84</b>
<b>16. Workflows.....</b>	<b>88</b>
El flujo.....	89
<b>17. Otros productos .....</b>	<b>92</b>
Directorio activo, ¿Por qué?.....	93
ADSI: La API para equipos locales .....	93
Ejemplo 1: Listado de usuarios.....	94
Ejemplo2: Listado de usuarios remotos.....	95
Ejemplo 3: Crear usuario .....	95
Ejemplo 4: Eliminar usuario.....	95
ADSI: La API para Active Directory .....	96
Conexión al AD .....	96
Buscar objetos en el AD .....	97
Ejemplo 1: Listar equipos.....	97
Ejemplo 2: Listar usuarios y grupos .....	97
Administración .....	98
Ejemplo 3: Crear objetos .....	98



Ejemplo 4: Mover objetos .....	98
Cmdlets desde Windows 2008 R2.....	99
El proveedor de Active Directory .....	99
Ejemplo 1: Crear objetos .....	100
Ejemplo 2: Buscar objetos con filtros.....	101
Ejemplo 3: Adición / Eliminación de miembros a un grupo .....	102
Internet Information Services.....	102
El proveedor de IIS.....	104
Gestión de sitios.....	105

## Capítulo III

### PowerShell puro: El arte del pentesting ..... 109

#### 1. Introducción..... 109

#### 2. Powercat: la navaja suiza ..... 110

Conexión simple.....	112
Dar y recibir shells .....	113
Transferencia de archivos.....	113
Escanear puertos TCP con Powercat.....	114
PoC: Descarga y ejecución de Shellcodes desde Powercat.....	114

#### 3. Veil-Framework..... 116

PowerUp.....	117
PoC: Configuraciones erróneas en servicios que permiten escalada de privilegio.....	121
PoC: Configuración errónea en el registro que permite la obtención de privilegio.....	124
PowerView .....	125
PoC: Resumen de PowerView .....	131

#### 4. Posh-SecMod..... 133

Módulos para comenzar .....	134
Discovery .....	137
PoC: Tipos de escaneos .....	138
Post-Explotación con Posh-SecMod.....	141
PoC: Base64, compresión, descargas y ejecución .....	142
PoC: Shell inversa, SAM y NTDS con Posh-SecMod .....	145
Servicios externos .....	148
PoC: Shodan y VirusTotal en tu PowerShell .....	151

#### 5. PowerSploit..... 154

Code Execution .....	155
Script Modification.....	156
Persistence.....	156
Exfiltration.....	157
Otros: Mayhem, Recon y AV Bypass.....	158



PowerShell Arsenal: Disassembly.....	159
PowerShell Arsenal: Malware Analysis.....	159
PowerShell Arsenal: Memory Tools .....	159
PowerShell Arsenal: Parsers .....	160
PowerShell Arsenal: Windows Internals.....	160
PowerShell Arsenal: Misc.....	161
PoC: Code Execution + Recon.....	161
PoC: Post-Exploitation con Exfiltration + Persistence .....	166
<b>6. Nishang.....</b>	<b>170</b>
Prasadhak, Scan, Escalation y Antak .....	171
Backdoors.....	172
Client.....	173
Execution.....	174
Gather.....	175
Pivot.....	176
Shells.....	177
Utility.....	178
PoC: Backdoors, jugando con DNS y Wireless .....	178
PoC: Client-Side Attack con Nishang.....	181
PoC: Shells.....	182
<b>7. Otros scripts en acción.....</b>	<b>183</b>
PoC: Sniffing y Spoofing de protocolos con PowerShell.....	183
PESecurity.....	184
Respuesta ante incidentes.....	185
Kansa .....	185
Voyeur.....	186
Find-MsfPSExec.....	186

## Capítulo IV

<b>PowerShell y otras herramientas: Pentesting sin límites .....</b>	<b>189</b>
<b>1. La post-explotación con PowerShell.....</b>	<b>189</b>
<b>2. PowerShell: Ejecución de payloads .....</b>	<b>190</b>
<b>3. PowerShell Shellcode Injection con Python.....</b>	<b>192</b>
<b>4. Payloads de PowerShell en Metasploit .....</b>	<b>193</b>
<b>5. Posh-Metasploit .....</b>	<b>196</b>
Console.....	197
Db.....	198
Jobs.....	200
Module .....	201



Plugin .....	203
Posh .....	203
Session.....	204
Variables.....	206
<b>Índice alfabético .....</b>	<b>207</b>
<b>Índice de imágenes y tablas.....</b>	<b>209</b>
<b>Libros publicados.....</b>	<b>215</b>

