

# Índice

## Capítulo 0

<b>Preparar el Arsenal. Comienza tu Imperio .....</b>	<b>11</b>
<b>1. ¿Un laboratorio?.....</b>	<b>11</b>
<b>2. Requerimientos.....</b>	<b>11</b>
<b>3. Arquitectura.....</b>	<b>11</b>
3.1. Laboratorio estándar.....	12
3.2. Máquina atacante .....	12
3.3. Máquina víctima.....	13
3.4. Configuración de conectividad.....	15
<b>4. Evolución del entorno de pruebas.....</b>	<b>19</b>
4.1. Laboratorio avanzado sugerido .....	19

## Capítulo I

<b>En busca del Game Over .....</b>	<b>21</b>
-------------------------------------	-----------

## Capítulo II

<b>Regreso al pasado.....</b>	<b>27</b>
-------------------------------	-----------

## Capítulo III

<b>El imperio contraataca .....</b>	<b>31</b>
<b>1. Instalación y configuración.....</b>	<b>31</b>
1.1. PoC: Instalación de Empire en Kali Linux .....	31
<b>2. Comandos básicos .....</b>	<b>33</b>
<b>3. Arquitectura .....</b>	<b>37</b>
3.1. Agents.....	38
3.2. Listeners .....	38
3.2.1. PoC: HTTP Listener “Classic” .....	39
3.3. Stagers.....	43

3.3.1. Staging y el funcionamiento .....	44
3.3.2. PoC: Utilizando un launcher de Powershell para desplegar un agente .....	45
3.4. Módulos.....	47
<b>4. Tipos de Listeners.....</b>	<b>48</b>
4.1. HTTP COM.....	49
4.1.1. PoC: HTTP_COM en Kali contra Windows 8.1 .....	50
4.2. HOP Listener .....	53
4.2.1. PoC: Hopping con Ubuntu: Entre Kali y Windows 7.....	54
4.3. HTTP Foreign Listener: Session Pass .....	56
4.4. Dropbox: DBX Listener .....	59
4.5. Integrando a Metasploit: MSF Foreign Listener .....	62
4.5.1. Code Execution. Metasploitpayload.....	62
4.5.2. MSF Foreign Listener.....	65
4.6. Onedrive .....	67
4.6.1. PoC: Configuración de Onedrive .....	67
4.7. Redirector.....	72
4.7.1. PoC: Pivoting con Redirector .....	73

## Capítulo IV

<b>Estrategias de combate .....</b>	<b>77</b>
<b>1. Introducción.....</b>	<b>77</b>
<b>2. Acceso Inicial.....</b>	<b>77</b>
2.1. Ataques de acceso físico.....	77
2.1.1. Descarga y ejecución de stager a través de un navegador .....	78
2.1.2. Ejecución de stager con Rubber Ducky y Bash Bunny .....	79
<b>3. Descubrimiento (Situational Awareness).....</b>	<b>84</b>
3.1. Bloodhound.....	84
<b>4. Escalada de privilegios.....</b>	<b>88</b>
4.1. PowerUp.....	88
4.1.1. PowerUp AllChecks.....	89
4.1.2. Powerup y los servicios con rutas sin comillas .....	92
4.1.3. Powerup y el abuso de permisos débiles en servicios .....	95
4.2. Bypass de UAC.....	100
4.3. Vulnerabilidades en Sistema Operativo .....	102
4.3.1. MS16-135 .....	103
4.3.2. Tater .....	108
<b>5. Movimiento lateral .....</b>	<b>114</b>
5.1. Almacén de credenciales.....	115
5.1.1. Steal Token y Mimikatz.....	116
5.2. Inveigh.....	120

5.3. Kerberoasting .....	125
5.4. Golden Ticket .....	131
5.5. Comprometer hashes del controlador de dominio .....	136
5.6. Empire y CrackMapExec .....	138
<b>6. Persistencia.....</b>	<b>141</b>
6.1. Persistencia en registro.....	141
6.2. Suscripción de evento WMI.....	143

## Capítulo V

### Capitán ‘Moonshots’ .....147

<b>1. Preparación del entorno .....</b>	<b>148</b>
1.1. Configuración de Git y Github.....	148
1.2. Creación de ambiente de desarrollo para Empire .....	151
<b>2. Desarrollo de módulos para agentes.....</b>	<b>153</b>
2.1. Tipos de módulos .....	154
2.2. Creación del código principal .....	156
2.3. Control de flujo y manejo de excepciones .....	158
2.4. Pruebas de calidad sobre el código principal .....	160
2.5. Creación y estructura de un módulo para Empire.....	162
2.6. Pruebas funcionales de módulos de agentes .....	167
<b>3. Contribuir al repositorio oficial .....</b>	<b>170</b>
3.1. Documentación del código.....	170
3.2. Código con estilo.....	172
3.3. Pruebas finales.....	173
3.4. Push to the Empire .....	173
<b>4. Conclusión.....</b>	<b>178</b>

## Capítulo VI

### iBombShell: El lanzacohetes .....179

<b>1. iBombShell. La importancia de Powershell.....</b>	<b>179</b>
<b>2. iBombShell. Utilidad y aportación.....</b>	<b>179</b>
<b>3. Arquitectura.....</b>	<b>181</b>
<b>4. Funcionamiento: Everywhere .....</b>	<b>182</b>
<b>5. Funcionamiento: Silently .....</b>	<b>185</b>
<b>6. Creación de un módulo .....</b>	<b>186</b>
6.1. Funciones para Everywhere .....	187
6.2. Módulos para Silently .....	187

<b>7. Escenarios de post-explotación.....</b>	<b>189</b>
7.1. Bypass AMSI y Windows Defender en Windows 10.....	190
7.2. Bypass UAC mediante Mocking Trusted Directory en Windows 10 .....	194
7.3. Movimiento lateral con PtH.....	197
7.4. Extracción de claves SSH privadas en Windows 10.....	199
7.5 Integración de RID Hijacking a iBombShell .....	201

## Capítulo VII

<b>El lado oscuro del imperio.....</b>	<b>207</b>
<b>1. Introducción.....</b>	<b>207</b>
<b>2. Evasión de sistemas de detección de intrusos en red.....</b>	<b>207</b>
2.1. Configuración personalizada de listener .....	208
2.2. Integración de certificado HTTPS .....	213
2.3. Empire a través de SSH.....	219
2.4. Configuraciones adicionales.....	221
<b>3. Evasión de sistemas de protección endpoint .....</b>	<b>223</b>
3.1. Invoke-Obfuscation y Empire .....	223
<b>4. Algunas medidas y soluciones.....</b>	<b>227</b>
<b>Índice alfabético .....</b>	<b>229</b>
<b>Índice de imágenes .....</b>	<b>231</b>