

# Índice

<b>Introducción .....</b>	<b>13</b>
<b>Capítulo I</b>	
<b>Ethical Hacking .....</b>	<b>17</b>
<b>1. Objetivos .....</b>	<b>17</b>
<b>2. Tipos de auditoría .....</b>	<b>18</b>
<b>3. Agregados al proceso .....</b>	<b>20</b>
Pruebas de stress: DOS/DDOS .....	20
APT: Amenazas avanzadas persistentes .....	21
Fuga de información interna .....	21
Comunicaciones wireless & VOIP .....	22
La importancia del rol .....	22
<b>4. Evaluación de seguridad .....</b>	<b>23</b>
Vulnerabilidades .....	23
Estándares y modelos .....	24
Ley Hacking 23 de Diciembre de 2010 .....	27
<b>5. Metodología .....</b>	<b>28</b>
El equipo de auditoría .....	29
Alcance del proyecto .....	29
Selección e información del objetivo .....	31
Confección del ataque e intrusión controlada: Ampliación de miras .....	32
Revisión del proceso: Medidas correctoras .....	34
Documentación .....	34
Interlocutores y almacenamiento de la información .....	34
<b>6. Publicación de una vulnerabilidad .....</b>	<b>35</b>
Reservar CVE .....	35
Detalles técnicos para CVE .....	35
Ejemplo real: CVE-2013-5572 .....	36
<b>7. Nuevas tendencias .....</b>	<b>38</b>

Pentesting by Design .....	38
<b>8. Atacantes de sombrero .....</b>	<b>39</b>
<b>Capítulo II</b>	
<b>La información es poder .....</b>	<b>41</b>
<b>1. Procesos asociados .....</b>	<b>41</b>
Footprinting .....	42
PoC: Shared hosting .....	44
PoC: DNS Caché Snooping y Evilgrade .....	47
PoC: El correo .....	49
Fingerprinting .....	53
Half Scan .....	53
ACK Scan .....	53
Null Scan .....	53
Xmas Scan .....	54
FIN Scan .....	54
Idle Scan .....	54
Técnicas de escaneo para evasión de protecciones .....	55
Nmap .....	61
Fingerprint Web .....	61
PoC: Nmap + scripts .....	64
PoC: Shodan .....	67
<b>2. Google y cia .....</b>	<b>70</b>
<b>3. Creación del mapa de información .....</b>	<b>72</b>
<b>4. Orientando el pentesting hacia un APT .....</b>	<b>78</b>
PoC: Obteniendo correos .....	79
<b>Capítulo III</b>	
<b>Confeccionando el ataque .....</b>	<b>83</b>
<b>1. Entornos .....</b>	<b>83</b>
<b>2. Auditoría perimetral .....</b>	<b>83</b>
Pruebas .....	84
Identificación de servicios .....	85
PoC: Identificación de vulnerabilidad explotable .....	86
Análisis de información .....	87
Crawling, bruteforce y otras técnicas .....	87
Localización de puntos de entrada .....	97
Métodos HTTP .....	98
Protección contra Clickjacking .....	100

Detección y explotación .....	100
Análisis SSL .....	101
Fuzzing .....	105
Manipulación de parámetros .....	106
Inclusión local y remota .....	108
Búsqueda de Path Disclosure .....	110
Acceso no autorizado .....	111
Subida de ficheros .....	112
Ataques a los puntos de entrada .....	114
Gestión de sesiones .....	115
Top 10 OWASP 2013 .....	116
Top 10 OWASP 2017 .....	117
<b>3. Auditoría interna .....</b>	<b>118</b>
Pruebas .....	119
PoC: Escenario inicial de auditoría interna .....	121
Wireshark: El analizador amigo .....	128
PoC: Sniffing remoto con Wireshark .....	134
Satori y p0f herramientas: sniffer pasivo .....	136
Pintar tráfico de red .....	137
Immunity Stalker .....	137
PoC: Obtención del primer dato de interés .....	138
PoC: Pass The Hash (PtH Attack) .....	143
PoC: Escalada de privilegios .....	146
PoC: Pivoting + PtH = Paseo por la organización .....	149
<b>4. Interna con privilegios .....</b>	<b>150</b>
Pruebas .....	151
PoC: Evaluación de configuraciones .....	151
<b>5. Wireless &amp; VOIP .....</b>	<b>153</b>
Pruebas .....	154
PoC: Descubriendo el mundo inalámbrico en la empresa .....	156
Wifite .....	158
PoC: Análisis de seguridad en la red .....	158
La red de invitados .....	159
La red WPA/WPA2 con PSK .....	160
La red Enterprise .....	161
PoC: Rogue AP en la empresa .....	162
PoC: Rogue AP inyectando Javascript botnet .....	164
Otras PoC's posibles en distintos entornos Wireless .....	165
PoC: Conociendo el entorno VOIP de la organización .....	168
PoC: Recogida de información y evaluación de seguridad .....	168
<b>6. DoS/DDOS .....</b>	<b>169</b>

Historia de las técnicas DDoS .....	170
Técnicas .....	172
Objetivos en una auditoría .....	173
El proceso ético .....	174
Pruebas .....	175
Resumen: Ataques en general .....	175
PoC: Poco tiempo de actuación y mucho de preparación .....	176
PoC: Colapsando las conexiones .....	179
Herramientas utilizadas .....	181
<b>7. APT .....</b>	<b>182</b>
Historia de APT .....	183
Pruebas .....	184
PoC: Estudio del conjunto de muestra a auditar .....	185
PoC: Preparación y configuración de pruebas .....	187
PoC: Cebos para dispositivos móviles .....	189
<b>8. Fuga de información .....</b>	<b>193</b>
Pruebas .....	194
PoC: Powershell y obtención de sesión remota .....	195
PoC: Shellcodes no detectables .....	197
PoC: Evasiones de proxy con paciencia y pruebas .....	198

## Capítulo IV

<b>Recomendaciones del proceso .....</b>	<b>201</b>
<b>1. Las recomendaciones .....</b>	<b>201</b>
<b>2. Medidas correctoras en auditoría perimetral .....</b>	<b>202</b>
Autenticación .....	202
Acceso .....	203
Criptografía y datos sensibles .....	204
Sesiones .....	205
Comunicaciones y protocolos .....	206
Entradas, codificación y errores .....	207
<b>3. Medidas correctoras en auditoría interna .....</b>	<b>208</b>
Medidas correctoras para ataques PtH .....	208
Configuración de elementos de seguridad en la red .....	212
Inventariado de máquinas y acotar responsabilidades .....	212
Evaluación de redes y recomendación .....	213
<b>4. Medidas correctoras en auditoría de caja blanca .....</b>	<b>213</b>
<b>5. Medidas correctoras en DOS/DDOS .....</b>	<b>214</b>
<b>6. Otras medidas correctoras .....</b>	<b>215</b>

**Capítulo V**

<b>Generar informe .....</b>	<b>217</b>
<b>1. Nociones de un informe .....</b>	<b>217</b>
<b>2. Plantillas .....</b>	<b>218</b>
Auditoría perimetral .....	218
Auditoría interna .....	219
Auditoría wireless .....	220
<b>3. Control de cambios .....</b>	<b>221</b>
<b>4. Ejecutivo Vs Técnico .....</b>	<b>221</b>
Ejemplo ejecutivo .....	222
<b>5. Reportes automáticos .....</b>	<b>222</b>
Análisis .....	223
<b>Índice alfabético .....</b>	<b>225</b>
<b>Índice de imágenes y tablas .....</b>	<b>227</b>