

# Índice

<b>Prólogo .....</b>	<b>11</b>
<b>Capítulo I</b>	
<b>Introducción .....</b>	<b>13</b>
<b>Capítulo II</b>	
<b>Las redes de datos y sus dispositivos .....</b>	<b>19</b>
<b>Capítulo III</b>	
<b>Sniffing, Spoofing y Haijacking .....</b>	<b>31</b>
<b>Capítulo IV</b>	
<b>Atacando por capas.....</b>	<b>43</b>
4.1 Identificación y ataques a dispositivos de red.....	44
4.2 Ataque en la capa de enlace .....	50
4.3 Ataque en la capa de red .....	59
4.4 Ataque en la capa de aplicación.....	61
4.5 Rogue DHCP .....	72
4.6 Network Packet Manipulation .....	77
4.6.1 Aplicando NPM sobre Wordpress.....	82
4.6.2 Aplicando NPM sobre Moodle .....	85
4.7 Evilgrade y los ataques de actualización .....	87
4.8 Encapsulación de tráfico en protocolos de red.....	90
4.8.1 Enviar un fichero encapsulado en el protocolo DNS.....	91
4.8.2 Extraer información a través de la cuenta de Gmail.....	94
4.9 Frameworks de automatización de auditoría de red .....	95
4.9.1 MITMf: Man in the Middle Framework.....	95
4.9.2 MITMf: Vulnerabilidad SMBTrap .....	99
4.9.3 Bettercap.....	101

4.10 El protocolo SSDP y las debilidades .....	107
4.10.1 Funcionamiento .....	107
4.10.2 EvilSSDP .....	108
4.10.3 PoC: EvilSSDP. El lagarto discreto .....	111

## Capítulo V

<b>Ataques en redes de datos IPv6 .....</b>	<b>115</b>
Ataques en redes de datos IPv6 .....	115
5.1 Conceptos básicos sobre IPv6.....	119
5.1.1 Probando IPv6 en la red.....	119
5.1.2 Configuración básica de IPv6 en sistemas Microsoft Windows.....	121
5.1.3 Direcciones de Vínculo o Enlace Local en IPv6 .....	123
5.1.4 Direcciones Well-Known en IPv6 .....	125
5.1.5 Precedencia de protocolos .....	126
5.1.6 Descubrimiento de vecinos con Neighbor Discovery Protocol.....	128
5.1.7 Resolución de nombres a direcciones IP en ámbito local.....	130
5.1.8 Configuración de equipos IPv6 en la red.....	130
5.1.9 DNS Autodiscovery .....	131
5.2 Ataque man in the middle de Neighbor Spoofing.....	131
5.2.1 Parasite6 (The Hacker's Choice) .....	133
5.2.2 Scapy Project .....	135
5.2.3 Neighbor Spoofing con Evil FOCA.....	138
5.3 Descubrimiento de equipos de la red.....	140
5.4 Ataque man in the middle con SLAAC .....	142
5.4.1 Ataque man in the middle SLAAC con Evil FOCA.....	143
5.4.2 NAT64 (Network Address Translation 6 to 4).....	149
5.4.3 Ataque man in the middle SLAAC con Radvd & NATPD.....	153
5.4.4 Ataque man in the middle SLAAC con SuddenSix.....	157
5.5 WebProxy Autodiscovery en IPv4/IPv6 .....	157
5.6 Conexiones HTTP-s en ataques mitm en la red IPv6 .....	162
5.6.1 El Stripping de HTTPs: Bridging HTTPs(IPv4)-HTTP(IPv6).....	162
5.7 Montaje de un servidor Rogue DHCPv6 .....	166
5.7.1 Montaje servidor DHCPv6 en Windows Server .....	166
5.7.2 Montaje del servidor Rogue DHCPv6 con Evil FOCA.....	172
5.8 Otros Ataques y Herramientas para IPv6.....	173
5.8.1 DOS RA Storm .....	173
5.8.2 The IPv6 Attack Toolkit.....	174
5.8.3 Topera 2 .....	175
5.8.4 IPv6 Toolkit & Idle scanning en IPv6 .....	176

5.9 Desactivar IPv6 en Windows y MAC OS X.....	179
<b>Capítulo VI</b>	
<b>La protección que ofrecen los “protocolos seguros” .....</b>	<b>183</b>
<b>Capítulo VII</b>	
<b>Cuando el usuario es un espectador de la ausencia de seguridad .....</b>	<b>203</b>
7.1 SSLStrip.....	204
7.2 El contenido mixto.....	210
7.3 La seguridad está en la MAC.....	211
7.4 Cabecera HSTS y SSL Strip v2.0 .....	215
7.4.1 El problema de la primera conexión.....	216
7.4.2 ¿Cómo se puede saber si un sitio devuelve HSTS?.....	217
7.4.3 PoC: Ejemplificando el ataque de la técnica SSL Strip 2 .....	218
7.5 Ataque Delorean .....	219
<b>Capítulo VIII</b>	
<b>Protección frente a ataques .....</b>	<b>223</b>
8.1 Seguridad por oscuridad. IPsec.....	224
8.2 Redes Virtuales Privadas (VPN). La seguridad “garantizada” .....	234
8.3 Protección de acceso a redes.....	242
8.4 DHCP Snooping.....	246
8.5 Prevención de ARP Poisoning .....	248
8.6 Detección de ataques de ARP Poisoning .....	249
8.7 Protección contra Network Packet Manipulation .....	254
<b>Capítulo IX</b>	
<b>Segmentación de una red.....</b>	<b>259</b>
9.1 VLAN: protección y ataques .....	261
9.2 Salto a redes de VoIP.....	267
<b>Índice de palabras .....</b>	<b>271</b>
<b>Índice de imágenes .....</b>	<b>273</b>
<b>Otros libros publicados.....</b>	<b>281</b>

