

Índice

Capítulo I	
Introducción	11
Capítulo II	
Las redes de datos y sus dispositivos	17
Capítulo III	
Sniffing, Spoofing y Haijacking	29
Capítulo IV	
Atacando por capas.....	41
4.1 Identificación y ataques a dispositivos de red.....	42
4.2 Ataque en la capa de enlace	48
4.3 Ataque en la capa de red	57
4.4 Ataque en la capa de aplicación.....	59
4.5 Rogue DHCP	70
4.6 Network Packet Manipulation	75
4.6.1 Aplicando NPM sobre Wordpress.....	80
4.6.2 Aplicando NPM sobre Moodle	83
4.7 Evilgrade y los ataques de actualización	85
4.8 Encapsulación de tráfico en protocolos de red.....	88
4.8.1 Enviar un fichero encapsulado en el protocolo DNS.....	89
4.8.2 Extraer información a través de la cuenta de Gmail.....	92
4.9 Frameworks de automatización de auditoría de red	93
4.9.1 MITMf: Man in the Middle Framework.....	93
4.9.2 MITMf: Vulnerabilidad SMBTrap	97
4.9.3 Bettercap.....	99



Capítulo V

Ataques en redes de datos IPv6	105
Ataques en redes de datos IPv6	105
5.1 Conceptos básicos sobre IPv6.....	109
5.1.1 Probando IPv6 en la red.....	109
5.1.2 Configuración básica de IPv6 en sistemas Microsoft Windows.....	111
5.1.3 Direcciones de Vínculo o Enlace Local en IPv6	113
5.1.4 Direcciones Well-Known en IPv6	115
5.1.5 Precedencia de protocolos	116
5.1.6 Descubrimiento de vecinos con Neighbor Discovery Protocol.....	118
5.1.7 Resolución de nombres a direcciones IP en ámbito local.....	120
5.1.8 Configuración de equipos IPv6 en la red.....	120
5.1.9 DNS Autodiscovery	121
5.2 Ataque man in the middle de Neighbor Spoofing.....	121
5.2.1 Parasite6 (The Hacker's Choice)	123
5.2.2 Scapy Project	125
5.2.3 Neighbor Spoofing con Evil FOCA.....	128
5.3 Descubrimiento de equipos de la red	130
5.4 Ataque man in the middle con SLAAC	132
5.4.1 Ataque man in the middle SLAAC con Evil FOCA.....	133
5.4.2 NAT64 (Network Address Translation 6 to 4).....	139
5.4.3 Ataque man in the middle SLAAC con Radvd & NATPD.....	143
5.4.4 Ataque man in the middle SLAAC con SuddenSix.....	147
5.5 WebProxy Autodiscovery en IPv4/IPv6	147
5.6 Conexiones HTTP-s en ataques mitm en la red IPv6	152
5.6.1 El Stripping de HTTPs: Bridging HTTPs(IPv4)-HTTP(IPv6).....	152
5.7 Montaje de un servidor Rogue DHCPv6	156
5.7.1 Montaje servidor DHCPv6 en Windows Server	156
5.7.2 Montaje del servidor Rogue DHCPv6 con Evil FOCA.....	162
5.8 Otros Ataques y Herramientas para IPv6.....	163
5.8.1 DOS RA Storm	163
5.8.2 The IPv6 Attack Toolkit.....	164
5.8.3 Topera 2	165
5.8.4 IPv6 Toolkit & Idle scanning en IPv6	166
5.9 Desactivar IPv6 en Windows y MAC OS X.....	169



Capítulo VI

La protección que ofrecen los “protocolos seguros”	173
---	------------

Capítulo VII

Cuando el usuario es un espectador de la ausencia de seguridad	193
---	------------

7.1 SSLStrip.....	194
7.2 El contenido mixto.....	200
7.3 La seguridad está en la MAC.....	201
7.4 Cabecera HSTS y SSL Strip v2.0	205
7.4.1 El problema de la primera conexión.....	206
7.4.2 ¿Cómo se puede saber si un sitio devuelve HSTS?.....	207
7.4.3 PoC: Ejemplificando el ataque de la técnica SSL Strip 2	208
7.5 Ataque Delorean	209

Capítulo VIII

Protección frente a ataques	213
--	------------

8.1 Seguridad por oscuridad. IPsec.....	214
8.2 Redes Virtuales Privadas (VPN). La seguridad “garantizada”	224
8.3 Protección de acceso a redes.....	232
8.4 DHCP Snooping.....	236
8.5 Prevención de ARP Poisoning	238
8.6 Detección de ataques de ARP Poisoning	239
8.7 Protección contra Network Packet Manipulation	244

Capítulo IX

Segmentación de una red.....	249
-------------------------------------	------------

9.1 VLAN: protección y ataques	251
9.2 Salto a redes de VoIP.....	257

Índice alfabético	261
--------------------------------	------------

Índice de imágenes	263
---------------------------------	------------



