

Índice

Introducción	13
---------------------------	-----------

Capítulo I

Instituto de Ingeniería Eléctrica y Electrónica	15
--	-----------

1. IEEE 802.11: Wireless LAN (WLAN)	17
IEEE 802.11 legacy	20
IEEE 802.11b	20
IEEE 802.11a	22
IEEE 802.11n	22

Capítulo II

Arquitecturas Inalámbricas	23
---	-----------

1. Conceptos básicos	23
2. Modos de operación inalámbricos	24
Modo infraestructura	24
Modo Ad-Hoc	25
Modo Wireless Distribution System	25
3. Resumen de conceptos	26

Capítulo III

Tramas inalámbricas 802.11	29
---	-----------

1. Modelo OSI	29
2. Nivel de enlace de datos	30
Logical Link Control (LLC)	30
MAC Service Data Unit (MSDU)	30
Media Access Control (MAC)	30
MAC Protocol Data Unit (MPDU)	31
3. Formato de la trama Media Access Control (MAC)	31

Cabecera MAC.....	32
Frame Control.....	33
Duration/ID.....	44
Addresses.....	45
Sequence Control.....	47
QoS Control.....	48
Data.....	49
Frame Check Sequence (FCS).....	50
4. Tramas de datos.....	51
Null.....	52
Data.....	53
QoS Data.....	54
5. Tramas de control.....	55
ACK.....	55
PS-Poll.....	56
6. Tramas de gestión.....	58
Probe Request.....	62
Probe Response.....	64
Authentication.....	66
Association Request.....	69
Association Response.....	70
Reassociation Request y Reassociation Response.....	72
Deauthentication y disassociation.....	75

Capítulo IV

Proceso de adición de una estación cliente a la red inalámbrica.....79

1. Etapa Probe.....	80
2. Etapa Authentication.....	82
Open System Authentication.....	82
Shared Key Authentication.....	83
3. Etapa Association.....	86
4. Diagrama de estados.....	87

Capítulo V

Autenticación inalámbrica.....89

1. Redes abiertas (Open Networks).....	89
2. Wired Equivalent Privacy (WEP).....	89
3. Wi-Fi Protected Access (WPA).....	90

Acuerdo sobre protocolos de seguridad	92
Autenticación 802.1x (únicamente en un contexto de autenticación empresarial).....	92
Distribución y verificación de claves	95
Derivación de claves.....	97
EAP y métodos de encapsulación	100
EAP-MD5	101
Lightweight EAP (LEAP).....	102
Protected EAP (PEAP)	102
EAP-TLS	104
EAP-TTLS.....	105
EAP y métodos de autenticación.....	106
Password Authentication Protocol (PAP)	106
Challenge Handshake Authentication Protocol (CHAP).....	106
Microsoft Challenge Handshake Authentication Protocol v2 (MSCHAPv2)	107

Capítulo VI

Cifrado inalámbrico.....109

1. Redes abiertas (Open Networks)..... 109

2. Wired Equivalent Privacy (WEP)..... 109

Sistema de cifrado WEP.....	111
Sistema de descifrado WEP	113
Debilidades WEP	113

3. Wi-Fi Protected Access (WPA)..... 115

Temporal Key Integrity Protocol (TKIP).....	115
Sistema de cifrado TKIP.....	116
Message Integrity Code (MIC).....	117
Counter Mode with CBC-MAC Protocol (CCMP).....	117
Sistema de cifrado CCMP.....	118
Debilidades en WPA/WPA2.....	119

Capítulo VII

La suite Aircrack-ng121

1. Airmo-ng121

Modo estación (Station Mode).....	121
Modo promiscuo (Promiscuous Mode).....	122
Modo monitor (Monitor Mode)	122
Modo máster (Master Mode)	123

2. Airodump-ng..... 125

3. Aireplay-ng..... 128

Ataque de desautenticación (Deauthentication attack)	129
Test de inyección (Injection Test)	131
4. Aircrack-ng	132

Capítulo VIII

Hacking WPA/WPA2 Personal Authentication.....139

1. Rompiendo la seguridad de la red	139
Resumen de los comandos utilizados.....	142
2. Resistencia al ataque de fuerza bruta.....	143
Diccionario combinatorio.....	145
Diccionario común	146
Diccionario dirigido	146
3. Empleando el Cloud de Amazon	147
Compute Unified Device Architecture (CUDA).....	147
Pyrit.....	148
CUDA y el Cloud en armonía	148
Instalación de Pyrit.....	153
Ultimando el entorno.....	155
Pyrit y su uso más básico	157
4. Otras alternativas	161
5. Wi-Fi Protected Setup (WPS).....	161
Métodos de intercambio.....	162
Arquitectura básica y esquema de funcionamiento.....	162
Estación con capacidades de Registrar configura un AP con rol de Enrollee.....	163
AP con capacidades de Registrar configura un Enrollee	165
Estación con capacidades de Registrar configura otra estación con rol de Enrollee	166
Vulnerabilidades de WPS.....	167
Fundamentos sobre el ataque online de fuerza bruta al protocolo WPS	167
Ejemplificación del ataque online de fuerza bruta.....	168
Contra medidas aplicables a WPS.....	170

Capítulo IX

Implementando puntos de acceso con hostapd

1. Fundamentos de hostapd	173
2. Parámetros del fichero de configuración de hostapd	174
AP ofreciendo red abierta.....	176
AP ofreciendo red WEP	177
AP ofreciendo red WPA-PSK	177

AP ofreciendo red WPA2-PSK	177
AP ofreciendo red WPA2-PSK y trabajando sobre 5 Ghz	177
Tres APs en una misma tarjeta	178
AP ofreciendo red WPA2-Enterprise usando el servidor EAP integrado.....	178
AP ofreciendo red WPA2-Enterprise usando un servidor RADIUS externo.....	179
3. Evolución a hostapd-wpe	179
4. Preparando el entorno hostil	180
Configuración del punto de acceso	182
Redirección de tráfico	183
Integración del servicio DHCP	184
Ejecución de los comandos	185

Capítulo X

Hacking a estaciones clientes189

1. Ingeniería social.....	189
2. Wireless phishing.....	190
Instalación de Wifiphisher.....	190
Engañando al usuario	191
3. AP-less.....	199
Red abierta en el punto de mira.....	200
Obtención del handshake a distancia	202
4. Ataque KRACK.....	207
Fundamentos del ataque.....	208
Entendiendo la metodología del ataque	209
Demostración del ataque por Mathy Vanhoef.....	212

Capítulo XI

Hacking WPA/WPA2 Enterprise Authentication213

1. Rompiendo la seguridad de EAP-TTLS/PAP	215
Configurando la red legítima.....	216
Suplantando la identidad del punto de acceso.....	219
Obteniendo las credenciales de acceso	222
Aplicando buenas prácticas de configuración.....	226
2. Rompiendo la seguridad de EAP-TTLS/MSCHAPv2	228
Configurando la red legítima a partir del escenario anterior.....	230
Suplantando la identidad del punto de acceso.....	231
Obteniendo las credenciales de acceso	233
Aplicando fuerza bruta al proceso de desafío	236

Índice alfabético	239
Índice de imágenes y tablas	243