Contenido

Prólogo 1

Capítulo 1. Introducción a la criptografía 19

1.1. La función de cifrado 19
1.1.1. El algoritmo estándar de cifrado triple de datos (3DES) 20
1.1.2. El algoritmo estándar de cifrado avanzado (AES) 24
1.1.3. El algoritmo de Rivest, Shamir y Adleman (RSA) 27
1.1.4. El algoritmo de cifrado de curvas elípticas (ECC) 28
1.2. La función *hash* 29
1.2.1. El algoritmo MD5 29
1.2.2. El algoritmo SHA 32
1.2.3. El mecanismo de HMAC 35
1.3. Intercambio de claves 37
1.3.1. La generación de la clave secreta 37
1.3.2. Distribución de la clave pública 38

Capítulo 2. El mecanismo 802.1x 43

2.1. Presentación general 43
2.2. EAPOL 44
2.2.1. Mensaje EAPOL-Start 45
2.2.2. Mensaje de EAPOL-Logoff 45
2.2.3. Mensaje EAPOL-Key 46
2.2.4. Mensaje EAPOL-Encapsulated-ASF-Alert 46
2.2.5. Mensaje EAPOL-MKA 46

2.2.6. Mensaje EAPOL-Announcement 46
2.2.7. Mensaje EAPOL-Announcement-Req. 47
2.3. El *Extensible Authentication Protocol* (EAP). 47
2.3.1. Mensaje EAP-Method Identity 50
2.3.2. Mensaje EAP-Method Notification 50
2.3.3. Mensaje EAP-Method Legacy NAK. 51
2.4. El protocolo RADIUS 51
2.4.1. Mensajes RADIUS 52
2.4.2. Atributos RADIUS 53
2.5. Procedimientos de autentificación 55
2.5.1. El procedimiento EAP-MD5 57
2.5.2. El procedimiento EAP-TLS 57
2.5.3. El procedimiento EAP-TTLS 60

Capítulo 3. Mecanismos del WPA 63

3.1. Introducción a la tecnología Wi-Fi 63
3.2. Mecanismos de seguridad 66
3.3. Políticas de seguridad 67
3.4. Gestión de claves 69
3.4.1. La jerarquía de claves 69
3.4.2. Los mensajes EAPOL-Key 71
3.4.3. El procedimiento *4-Way Handshake* 73
3.4.4. El procedimiento de handshake de las claves de grupo (*Group Key Handshake*) 76
3.5. El protocolo WEP 77
3.6. El protocolo TKIP 79
3.7. El protocolo CCMP 82

Capítulo 4. El mecanismo IPSec 85

4.1. Repaso sobre el protocolo de Internet (IP) 85
4.1.1. IPv4 85
4.1.2. IPv6 88
4.2. La arquitectura IPSec 90
4.2.1. Cabeceras de seguridad 91
4.2.2. La asociación de seguridad 96
4.2.3. El mecanismo PMTU 97
4.3. El protocolo IKEv2 98

4.3.1. La cabecera del mensaje 98
4.3.2. Los bloques 100
4.3.3. El procedimiento 107

Capítulo 5. Protocolos SSL / TLS / DTLS 113

5.1. Introducción 113
5.2. Protocolos SSL/TLS 114
5.2.1. La cabecera *Record* 114
5.2.2. El mensaje *change_cipher_spec* 115
5.2.3. El mensaje *alert* 116
5.2.4. Mensajes de *handshake* 118
5.2.5. Información criptográfica 126
5.3. El protocolo DTLS 129
5.3.1. Adaptación al transporte UDP 129
5.3.2. Adaptación al transporte del protocolo DCCP 131
5.3.3. Adaptación al transporte del protocolo SCTP 131
5.3.4. Adaptación al protocolo SRTP 132

Capítulo 6. Gestión de la red 135

6.1. Gestión SNMPv3 135
6.1.1. Introducción 135
6.1.2. La arquitectura SNMPv3 136
6.1.3. La estructura del mensaje SNMPv3 143
6.2. El protocolo de *shell* seguro (SSH) 145
6.2.1. El protocolo SSH-TRANS. 145
6.2.2. El protocolo SSH-USERAUTH 149
6.2.3. El protocolo SSH-CONNECT 150

Capítulo 7. Tecnología MPLS-VPN 153

7.1. La red de conmutación de etiquetas multiprotocolo (MPLS). 153
7.1.1. La arquitectura de la red 153
7.1.2. Las tablas del router LSR 155
7.1.3. La función PHP 156
7.1.4. El formato de la cabecera MPLS 157
7.1.5. Soporte *DiffServ*. 158
7.2. El protocolo de distribución de etiquetas (LDP) 159
7.2.1. Los principios de funcionamiento 159
7.2.2. El formato de la PDU LDP 162

7.3. La construcción de la VPN 167
7.3.1. La arquitectura de la red 167
7.3.2. La distinción entre rutas 170
7.3.3. El objetivo de ruta 171
7.3.4. Los principios de funcionamiento 172

Capítulo 8. VPN Ethernet 177

8.1. Tecnología Ethernet 177
8.1.1. La capa física 177
8.1.2. La capa MAC 180
8.1.3. La partición VLAN 182
8.2. Tecnología PB (PBT, *Provider Bridge Technology*) 185
8.3. Tecnología VPLS 186
8.3.1. La arquitectura de la red 186
8.3.2. La cabecera EoMPLS 190
8.3.3. El protocolo de distribución de etiquetas (LDP) 191
8.4. Tecnología L2TPv3 193
8.4.1. El mensaje de datos 193
8.4.2. Mensajes de control 195
8.4.3. Los procedimientos 197

Capítulo 9. Los servidores de seguridad 203

9.1. Las tecnologías 203
9.1.1. El filtrado de paquetes 203
9.1.2. La pasarela de la aplicación 206
9.1.3. El dispositivo NAT/NAPT 206
9.2. El cruce del dispositivo NAT/NAPT 210
9.2.1. El protocolo de mensajes de control en Internet (ICMP) 210
9.2.2. El mecanismo IPSec 212
9.2.3. Protocolos SIP, SDP y RTP 213
9.2.4. El protocolo de transferencia de archivos (FTP) 218
9.2.5. Fragmentación 220

Capítulo 10. Detección de intrusos 221

10.1. La tipología de los ataques 221
10.2. Métodos de detección 223
10.2.1. Detección basada en firmas 223
10.2.2. Detección basada en anomalías 224
10.2.3. Análisis de protocolos 224

10.3. Las tecnologías 225
10.3.1. El dispositivo N-IDPS 226
10.3.2. El sistema inalámbrico IDPS (WIDPS) 228
10.3.3. El sistema H-IDPS 230
10.3.4. El sistema de análisis de comportamiento de la red (NBA) . . . 231

Bibliografía 233

Lista de abreviaturas 239

Índice alfabético 247