ÍNDICE

INTRODUCCIÓN 1
Resumen de los capítulos..... 3

CAPITULO 1: Los protocolos TCP/IP 7

1.1 Redes IP..... 8
1.2 El protocolo IP versión 4..... 12
1.3 El protocolo ICMP..... 16
1.4 El protocolo UDP..... 19
1.5 El protocolo TCP..... 21
1.5.1 Establecimiento de una conexión TCP..... 25
1.5.2 Finalización de una conexión TCP..... 27
1.6 Encaminamiento de datagramas..... 29
1.7 Resumen..... 32

CAPITULO 2: Denegación de servicio: DOS / DDOS 34

2.1 Contexto histórico y tecnológico..... 35
2.2 Fuentes de origen de los ataques DOS/DDOS..... 36
2.3 Ataques DOS..... 37
2.3.1 IP Flooding..... 38
2.3.2 Broadcast..... 40
2.3.3 Smurf..... 41
2.3.4 Teardrop / Boink / Bonk / Nestea..... 42
2.3.5 ECHO-CHARGEN / Snork..... 44
2.3.6 DOOM / QUAKE..... 45
2.3.7 Land..... 46
2.3.8 Ping of death..... 47
2.4 Ataques DDOS..... 48
2.4.1 Trinoo / Trin00..... 49
2.4.2 Tribe Flood Network / TFN..... 53
2.4.3 Stacheldraht..... 56
2.4.4 SHAFT..... 57
2.4.5 Tribe Flood Network 2000 / TFN2K..... 60
2.4.6 Distributed Reflection DOS..... 62
2.5 Defensas contra DOS/DDOS..... 63
2.6 Ejemplo de ataque DDOS..... 66
2.7 Resumen..... 70

CAPITULO 3: Sistemas de detección de intrusos (IDS) 71

3.1 Firewalls..... 72
3.2 Historia de los IDS..... 74
3.3 IDS..... 74
3.3.1 Monitorización de redes en tiempo real..... 76
3.3.2 Signatures (Firmas)..... 78

3.3.3 Eventos de interés (EOI)..... 80
3.4 Arquitecturas de los NIDS..... 82
3.4.1 CIDF..... 84
3.4.2 DIDS..... 86
3.5 Ubicación de los NIDS..... 88
3.6 Protocolos de comunicación Sensor-Consola..... 89
3.7 Análisis de los datos obtenidos por sistemas NIDS. 93
3.8 Falsos positivos y falsos negativos..... 97
3.9 IPS..... 101
3.10 Limitaciones de los IDS..... 106
3.11 El taque Mitnick..... 108
3.12 Resumen..... 112

CAPITULO 4: Honeypots y Honeynets 113

4.1 Nuevos escenarios de ataques..... 114
4.2 Historia de los Honeypots..... 116
4.3 Honeypots..... 117
4.3.1 Valor añadido..... 120
4.3.2 Clasificación..... 123
4.3.3 Ubicación..... 126
4.3.4 Honeytokens..... 130
4.3.5 WI-FI Honeypots..... 132
4.3.6 Repercusiones legales..... 133
4.4 Honeynets..... 136
4.4.1 Valor añadido..... 138
4.4.2 GEN I..... 139
4.4.3 GEN II..... 141
4.4.4 Honeynets virtuales..... 144
4.4.5 Honeynets distribuidas..... 147
4.5 Resumen..... 148

CAPITULO 5: Análisis de un sistema conectado a Internet 151

5.1 Objetivos..... 152
5.2 Red de pruebas..... 153
5.2.1 Requisitos estructurales..... 153
5.2.2 Arquitectura propuesta..... 156
5.2.3 Configuración..... 158
5.3 Herramientas..... 160
5.3.1 Apache..... 162
5.3.2 Ethereal..... 163
5.3.3 IPaudit..... 164
5.3.4 MRTG..... 171
5.3.5 NMAP..... 173
5.3.6 TCPdump..... 174
5.3.7 TCPreplay..... 175
5.4 Resultados..... 176
5.4.1 Día 21 de Agosto..... 179
5.4.2 Día 22 de Agosto..... 185
5.4.3 Día 23 de Agosto..... 187

5.4.4 Día 24 de Agosto..... 189
5.4.5 Día 25 de Agosto..... 191
5.4.6 Día 26 de Agosto..... 194
5.4.7 Día 27 de Agosto..... 197
5.4.8 Resumen semanal..... 201
5.5 Conclusiones..... 204
5.6 Resumen..... 207

Conclusiones 208
Parte experimental..... 211
Líneas futuras de continuación..... 213

Bibliografía 214
Bibliografía WWW..... 219