Índice de contenidos

Introducción **15**

Cómo está organizado el libro 16

1. Para empezar... ..... **19**

Introducción 19
Definir la seguridad 19
Los dos puntos de vista de la seguridad de redes 20
Fuentes u orígenes de amenazas externas 20
Hackers (piratas informáticos) y crackers (intrusos) 21
Tipos de ataques 22
Pasos para vulnerar la seguridad de una red 23
Fuentes u orígenes de amenazas internas 24
Amenazas originadas por los empleados 24
Accidentes 26
Proceso de seguridad desde el punto de vista organizativo 27
Apoyo de la alta dirección 27
¿Qué nivel de seguridad puede obtener? 28
La importancia de una política de seguridad 29
Legislación sobre seguridad en Estados Unidos 31
Ley sobre la Protección de Privacidad "online" de Menores, de 1998 31

Ley de Gramm-Leach-Bliley (GLB, Gramm-Leach-Bliley Act) 32
Ley de Información Justa sobre Crédito (FCRA, Fair Credit Reporting Act) 33
Ley de Responsabilidad y Portabilidad del Seguro Médico de 1996 (HIPAA, Health Insurance Portability and Accountability Act) 34
Personal de seguridad 35
Responsable de la organización 35
Mandos intermedios 37
Personal involucrado 38
Subcontratar los servicios de seguridad 40
Cómo diseñar una política de seguridad 41
Auditorías de seguridad 46
Resumen 48

2. Arquitectura básica de seguridad 51

Introducción 51
Disposiciones de la red de seguridad 51
Cortafuegos (Firewalls) 55
Cortafuegos de filtrado de paquetes 56
Cortafuegos de estado 57
Cortafuegos proxy a nivel de aplicación 57
Comparar los distintos tipos de cortafuegos 58
Ejercicios prácticos: Establecer los permisos sobre archivos y directorios 59
Windows 60
UNIX 61
Cambiar los permisos de los archivos y directorios 63
Modificar los propietarios y grupos de los archivos 64
Mac OS X 65
Resumen 65

3. Seguridad física 69

Introducción 69
Cómo actuar frente al robo y los actos vandálicos 69
Proteger la consola del sistema 72
Gestionar los fallos del sistema 73
Soluciones de respaldo 73
Plan de respaldo 74

Medios de respaldo 76
Respaldo interno 81
Respaldo externo o externalización del respaldo 81
Sitios alternativos para casos de emergencia 81
Protección contra caídas de energía eléctrica 82
Protección contra aumentos de tensión o sobretensiones 82
Estabilizadores de tensión 83
Fuentes de alimentación ininterrumpida 84
Ejercicios prácticos: Proporcionar una seguridad física 85
Soluciones físicas 85
Sistemas de seguridad de los ordenadores individuales 86
Candados y "llaves" de las salas 86
Controlar mediante cámaras 89
Simulacros de recuperación ante desastres y/o siniestros 89
Resumen 90

4. Recopilación de información 93

Introducción 93
Ingeniería social 94
Ingeniería social electrónica: phishing 95
Utilizar la información publicada 99
Escaneo de puertos 103
Correspondencia de red 105
Ejercicios prácticos 109
Limitar la información publicada 109
Deshabilitar servicios innecesarios y cerrar puertos 110
Abrir puertos en el perímetro y utilización de servicios proxy 117
Resumen 119

5. Acceso al usuario root 121

Introducción 121
Root kits 121
Nivel de amenaza de los root kit 123
Funcionamiento de un root kit 124
Ataques de fuerza bruta y detección de intrusos 124
Registros del sistema 126
Software de detección de intrusos 130

Software de prevención contra intrusos 132
Honeypots 133
Ataques de sobrecarga del buffer 133
Ejercicios prácticos 135
Ver y configurar los registros de eventos de Windows 135
Parches y su mantenimiento 137
Resumen 138

6. Spoofing 141

Introducción 141
Spoofing de TPC 141
Spoofing de DNS 145
Spoofing de IP (y de correo) 148
Spoofing Web 150
Ejercicios prácticos 157
Detectar correo falso 157
Detectar sitios Web falsos 159
Resumen 161

7. Ataques de denegación de servicio 163

Introducción 163
Ataques Dos con fuente única 163
Ataques de flujo SYN 164
El ping de la muerte 165
Pitufos (smurfs) 165
Ataque de desbordamiento de UDP 166
Ataques DoS distribuidos 166
Ataque tribal 167
Trinoo 168
Stacheldraht 168
Ejercicios prácticos 169
Detectar un ataque DoS usando un IDS 169
Usar los registros del sistema para detectar ataques DoS 171
Controlar un ataque DoS en marcha 175
Estrategias de defensa contra los ataques DoS 176
Encontrar ficheros 177
Resumen 179

8. Malware 181

Introducción 181
Una breve historia del malware 182
Tipos de malware de acuerdo a sus métodos de propagación 183
Malware que se descarga y ejecuta 186
Virus de sector de arranque 187
Virus de tipo macro 188
Malware de correo electrónico 189
Malware de sitio Web 190
Ejercicios prácticos 191
Antivirus 191
Antivirus en el propio puesto 192
Sistemas de detección de virus basados en redes y servidores 196
El peligro de los dispositivos extraíbles 198
Esquemas de restricción 199
Resumen 201

9. Nombre de usuario y contraseña de seguridad 203

Introducción 203
Política de contraseñas 203
Contraseñas seguras 205
Seguridad del archivo de contraseñas 207
Windows 207
Windows 9x 207
Windows NT y sucesivos 209
UNIX 210
Auditorías de contraseñas 211
UNIX: John the Ripper 211
Windows: L0phtCrack 212
Mejora de la seguridad de las contraseñas con artilugios 213
Ejercicios prácticos: Software de mantenimiento de contraseñas 215
Mantenimiento de contraseñas centralizado 215
Mantenimiento de contraseñas individual 216
Norton Password Manager 216
Acceso a Llaves en Mac OS X 218
Resumen 219

10. Acceso remoto 221

Introducción 221
Vulnerabilidades de acceso remoto 221
Acceso telefónico 222
Software de control remoto 223
Comandos de acceso remoto 226
Conexiones telnet bajo Windows 226
Conexiones telnet bajo UNIX 227
Vulnerabilidad de Telnet 227
Otros comandos de acceso remoto en UNIX 228
ssh: la alternativa segura 228
VPN229 IPSec VPN 229
PPTP VPN 232
L2TP/IPSec 233
SSL VPN 233
Autentificación de usuario remoto 234
RADIUS 234
Kerberos 235
CHAP y MS-CHAP 236
Ejercicios prácticos: VPN basado en sistemas operativos 237
VPN bajo Windows 237
La interfaz de Windows 2003 Server 237
Configuración de un cliente VPN bajo Windows 240
VPN bajo Mac OS X 245
La interfaz del servidor Mac OS X 245
Configuración de la conexión del cliente en Mac OS X 246
Resumen 249

11. Seguridad en una red inalámbrica 251

Introducción 251
Estándares de red inalámbrica 252
Estándar de redes inalámbricas 802.11 253
Bluetooth 254
El próximo 802.16 255
Vulnerabilidades de las redes inalámbricas 256
Filtrado de señal y ataques de inserción 256

Filtrado de señal y ataques de intercepción 257
Vulnerabilidades SSID 257
Ataques de denegación de servicio 258
Ataques de agotamiento de batería 258
Medidas de seguridad inalámbrica 259
Seguridad de 802.11x 259
WEP 259
Seguridad en 802.11i y WPA 260
Autentificación en 801.11 261
Seguridad Bluetooth 263
Ejercicios prácticos: Seguridad en una red inalámbrica 802.11x 264
Resumen 267

12. Cifrado 269

Introducción 269
Cifrar o no cifrar 269
Esquemas de cifrado de clave única 270
Algoritmos de sustitución 271
Algoritmos de cifrado de clave única 273
Estándar de cifrado de datos (DES) 273
Triple DES 274
Estándar de cifrado avanzado (AES) 274
RC4 275
Problemas de mantenimiento de contraseñas 277
Esquemas de cifrado de doble clave 277
La matemática detrás de PKE 278
Combinación del cifrado de clave única y clave doble 280
Integridad del mensaje 281
Algoritmos de creación de resúmenes 282
Checksums 283
CRC Checksums 283
Checksums en el protocolo TCP 284
Autentificación de mensajes y certificados digitales 285
Autentificación mediante PKE 285
Autentificación mediante certificados digitales 285
Composición y propósito de PKI 287
Ejercicios prácticos 288

Certificados digitales 288
VeriSign 288
RSA 288
Software de cifrado 289
PGP 289
Instalación del software 290
Envío de la clave a un servidor 295
Localización de claves públicas 298
Cifrado de mensajes 299
GPG 301
Resumen 301

Apéndice A. El protocolo TCP/IP 303

Introducción 303
Funcionamiento de un conjunto de protocolos 303
El nivel de Aplicación 305
El nivel de Transporte 306
TCP 307
UDP 309
El Nivel de Internet 310
El nivel de Control de Enlace Lógico 312
El nivel MAC 313
El nivel Físico 314

Apéndice B. Puertos TCP y UDP 317

Listas de puertos 323

Apéndice C. Sitios de actualizaciones de seguridad 325

Sitios de actualizaciones de seguridad profesionales 325
Otros sitios de interés 326

Glosario 329

Índice alfabético 337