

ÍNDICE

PRÓLOGO	XV
CAPÍTULO 1. EL RIESGO DE INTERNET	1
INTRODUCCIÓN.....	2
EL RIESGO DE LA BANDA ANCHA	2
QUÉ QUIERE UN PIRATA DE NOSOTROS.....	4
Cuál es el valor de nuestro ordenador	5
QUIÉN SE DEDICA A LA PIRATERÍA INFORMÁTICA.....	6
LA HISTORIA	7
<i>Hackers, crackers</i> y otras tribus.....	9
El cóndor. El pirata más famoso de nuestros días	11
LAS HERRAMIENTAS DE LOS PIRATAS.....	14
El primer gusano.....	15
El famoso gusano de Internet.....	15
El primer caballo de Troya.....	17
CAPÍTULO 2. QUÉ ES UN FIREWALL	21
INTRODUCCIÓN.....	22
QUÉ HACE UN <i>FIREWALL</i>	23
Cómo trabaja.....	24
QUÉ NO HACE UN <i>FIREWALL</i>	25
TIPOS DE <i>FIREWALL</i>	26
Software o hardware.....	27
Personal o corporativo.....	28
Profundidad del análisis	29
<i>FIREWALL</i> PERSONAL	30
Diferencias entre <i>firewall</i> personal y corporativo.....	30
Características de un <i>firewall</i> personal	32

CAPÍTULO 3. EL PROTOCOLO DE INTERNET	35
INTRODUCCIÓN.....	36
LOS ORÍGENES	36
Nacimiento de TCP/IP	37
Nacimiento de Internet	38
PROTOCOLOS DE COMUNICACIONES.....	39
EL MODELO DE CAPAS	39
El modelo OSI	40
EL MODELO INTERNET	42
Protocolos de la capa aplicación	44
Protocolos de transporte. TCP/UDP	45
Protocolo de red. IP	46
PAQUETES Y CABECERAS	47
Los paquetes IP.....	48
Los paquetes TCP y UDP	50
Los paquetes de control ICMP.....	53
El número MAC	55
Los paquetes ARP	55
ESTABLECIMIENTO DE UNA SESIÓN TCP.....	56
DOCUMENTACIÓN SOBRE INTERNET	57
CAPÍTULO 4. EL DIRECCIONAMIENTO IP	59
INTRODUCCIÓN.....	60
LOS NÚMEROS BINARIOS.....	60
Convertir de binario a decimal.....	61
Convertir de decimal a binario.....	62
LAS DIRECCIONES IP	63
Clases de red	63
Máscara de red.....	66
IP estática e IP dinámica	67
IP PRIVADA E IP PÚBLICA.....	68
LOS NÚMEROS DE PUERTO	69
NAT.....	72
DHCP	73
Puerta de enlace	75
IPV4 E IPV6	75
HERRAMIENTAS ÚTILES	77
Ping.....	78
Traceroute	79
Netstat.....	79

CAPÍTULO 5. LOS SERVIDORES DNS.....	81
INTRODUCCIÓN.....	82
LOS NOMBRES DE DOMINIO.....	82
DOMINIOS DE NIVEL ALTO.....	83
DNS.....	85
La jerarquía DNS.....	85
Tipos de consultas.....	86
El proceso de resolución.....	87
Protocolos utilizados.....	88
REGISTRO DE DOMINIO.....	88
 CAPÍTULO 6. MÉTODOS DE ATAQUE.....	 91
INTRODUCCIÓN.....	92
EL PROCESO DE ATAQUE.....	93
RECONOCIMIENTO DEL SISTEMA.....	94
Reconocimiento pasivo.....	95
Reconocimiento activo.....	96
Ingeniería social.....	98
REALIZAR UN ATAQUE.....	99
Ataques desde Internet.....	100
Ataques desde la red local.....	101
Ataques desde el propio equipo.....	103
CONSEGUIR ACCESO.....	104
Puntos débiles.....	104
Una vez dentro.....	105
NEGACIÓN DE SERVICIO.....	106
<i>Jamming</i> o <i>flooding</i>	107
<i>Land attack</i>	108
<i>Nuke</i>	108
<i>Teardrop</i>	108
Ataques al correo.....	109
CABALLOS DE TROYA.....	109
Tipos de troyanos.....	111
Troyano cliente.....	112
BORRANDO EL RASTRO.....	113
 CAPÍTULO 7. CÓMO FUNCIONA UN FIREWALL.....	 115
INTRODUCCIÓN.....	116
FILTRADO DE PAQUETES.....	117
IP <i>spoofing</i> o IP falso.....	118
ICMP.....	118
Fragmentación.....	119

FILTRO DINÁMICO DE PAQUETES	121
NAT	122
Inconvenientes de NAT	123
PROXY O GATEWAY DE APLICACIÓN	124
Debilidades del <i>proxy</i>	125
REGISTRAR Y ANALIZAR	126

CAPÍTULO 8. FUNCIONES AVANZADAS DEL FIREWALL..... 129

INTRODUCCIÓN.....	130
DIRECCIONES ESTÁTICAS O REDIRECCIONAMIENTO IP.....	130
REDIRECCIONAMIENTO DE PUERTO	131
DETECCIÓN DE INTRUSIÓN	132
SERVIDOR CACHE	133
REPARTO DE CARGA	135
FILTRO DE CONTENIDOS.....	135
Otros tipos de filtros	137
EL CIFRADO Y LOS FIREWALLS.....	137
Protocolos de autenticación	138
SSL	139
IPSec.....	140
Red privada virtual	142
Los protocolos de tunelado	144

CAPÍTULO 9. DEFINIR LAS REGLAS..... 145

INTRODUCCIÓN.....	146
LAS TÉCNICAS DE ANÁLISIS	147
Tipo de análisis	147
Lista de excepciones.....	148
SERVICIO WEB.....	148
ACCESO A DNS	150
CORREO ELECTRÓNICO	152
TRANSFERENCIA DE ARCHIVOS.....	154
MENSAJERÍA INSTANTÁNEA.....	156
BLOQUEAR TROYANOS.....	158
ICMP	159
SERVICIOS DE TERMINAL	160
RADIUS	160
CIFRADO IPSEC	161
Utilizar un túnel	162

CAPÍTULO 10. EL <i>FIREWALL</i> DE LINUX	163
INTRODUCCIÓN.....	164
EVOLUCIÓN DEL <i>FIREWALL</i> DE LINUX.....	165
Instalación de Iptables	166
ESTRUCTURA DE IPTABLES	168
La tabla <i>filter</i>	169
La tabla <i>nat</i>	169
DEFINIR LAS REGLAS	171
El orden de las reglas.....	172
Añadir una regla.....	174
Identificar el tipo de tráfico	175
Filtro dinámico de paquetes	175
<i>Snat</i> y <i>masquerade</i>	176
<i>Dnat</i>	176
IPSec a través del <i>firewall</i>	177
Registrar la actividad.....	177
REALIZAR UN <i>SCRIPT</i> PARA IPTABLES.....	178
UTILIZAR UNA INTERFAZ GRÁFICA	180
CAPÍTULO 11. LA SEGURIDAD EN WINDOWS	181
INTRODUCCIÓN.....	182
LAS COMUNICACIONES CON WINDOWS.....	182
Los componentes de la comunicación.....	184
Red local de Microsoft	184
LA SEGURIDAD DE LA RED MICROSOFT	186
La seguridad de NTFS.....	188
CARACTERÍSTICAS DE SEGURIDAD DE WINDOWS.....	190
WINDOWS 98 Y ME	190
Red privada virtual	191
Compartir una conexión a Internet	192
WINDOWS NT.....	193
WINDOWS 2000.....	194
CAPÍTULO 12. LO SENCILLO. EL <i>FIREWALL</i> DE WINDOWS XP Y DE MCAFEE	197
LA SEGURIDAD EN WINDOWS XP.....	198
EL <i>FIREWALL</i> DE WINDOWS.....	199
EVITAR QUE UN PROGRAMA DEJE DE FUNCIONAR.....	200
Crear excepciones.....	201
Abrir un puerto.....	202
Los programas de juegos.....	203

DAR PASO A LOS SERVIDORES INTERNOS	204
CONTROLAR LOS PAQUETES ICMP	206
EL REGISTRO DE ACTIVIDAD	208
Formato del registro de actividad	209
McAfee Personal Firewall	211
USO HABITUAL	213
La ficha <i>Resumen</i>	215
Ver el registro de actividad	216
Control del tráfico.....	218
PARTICULARIZAR LA CONFIGURACIÓN.....	218
Configuración de las alertas	219
IP fiables y prohibidas	220
Abrir puertos para los servicios internos	221
Las aplicaciones de Internet	222
CAPÍTULO 13. LO POPULAR. ZONEALARM PERSONAL FIREWALL	225
INTRODUCCIÓN.....	226
LA PROTECCIÓN DE ZONEALARM.....	227
Las zonas de seguridad.....	228
BLOQUEO DE EMERGENCIA	228
LA CONFIGURACIÓN DE ZONEALARM.....	229
EL SERVIDOR DE SEGURIDAD. EL <i>FIREWALL</i>	230
Las reglas de experto	232
Crear una regla.....	233
CONTROL DE PROGRAMAS	235
Control de servidores.....	237
Pasar el bloqueo de Internet	237
ALERTAS Y REGISTROS.....	237
Las alertas.....	238
El registro de actividad	241
PROTECCIÓN DEL CORREO ELECTRÓNICO	243
CAPÍTULO 14. LO DISTINTO. KERIO PERSONAL FIREWALL.....	245
INTRODUCCIÓN.....	246
COMPONENTES DEL PROGRAMA	246
FUNCIONAMIENTO.....	247
Mensajes de alerta.....	248
Áreas de seguridad.....	251
CONFIGURACIÓN DEL <i>FIREWALL</i>	252
Seguridad de red	253
Seguridad del sistema	255

Detección de intrusos	257
Filtro Web	258
LOS REGISTROS DE ACTIVIDAD	261
CREACIÓN DE REGLAS AVANZADAS	261
CAPÍTULO 15. FIREWALL PARA RED LOCAL.....	265
INTRODUCCIÓN.....	266
COORDINACIÓN DE LA DEFENSA.....	266
REACCIÓN FRENTE A UN INCIDENTE DE SEGURIDAD.....	267
LAS POSIBILIDADES	268
EL ORDENADOR COMO <i>FIREWALL</i> DE RED.....	270
<i>FIREWALL</i> HARDWARE.....	271
<i>Firewall</i> en un hardware compartido	273
<i>FIREWALL</i> CON EL PROVEEDOR DE ACCESO	274
CREAR UNA ZONA DE SERVIDORES.....	275
<i>Firewall</i> en el servidor.....	276
<i>Firewall</i> de tres patas.....	277
Utilizar múltiples <i>firewalls</i>	278
CAPÍTULO 16. OTROS ASPECTOS DE LA SEGURIDAD	279
INTRODUCCIÓN.....	280
PROTECCIÓN DE LAS COMUNICACIONES.....	280
PROTECCIÓN DE LA CONFIDENCIALIDAD. EL CIFRADO.....	282
Métodos de cifrado	283
PROTECCIÓN DE LA INTEGRIDAD. HUELLA DIGITAL	284
Función <i>Hash</i>	284
PROTECCIÓN DE LA AUTENTICIDAD. FIRMA DIGITAL.....	286
Infraestructura de clave pública	286
Certificados	287
Autoridades de certificación	288
LA TECNOLOGÍA DE SEGURIDAD EN INTERNET	288
PGP.....	289
SSL	289
SET	291
P3P y la privacidad.....	292
VIRUS INFORMÁTICO.....	295
El primer virus	295
Infecciones de virus	296
Programas antivirus.....	296
PRÁCTICA DE LA SEGURIDAD.....	297
La clave de acceso	298

Transmitir información sobre las tarjetas de crédito.....	299
Identificación de los lugares seguros.....	299
Mensajes de seguridad.....	300
Archivos de origen desconocido.....	301

APÉNDICES

A. GLOSARIO.....	303
B. NÚMEROS DE PUERTO DE LAS APLICACIONES.....	321
C. HERRAMIENTAS Y RECURSOS ÚTILES.....	327
ÍNDICE ALFABÉTICO.....	333