

# CONTENIDO

Introducción	1
<b>PARTE I ❖ ANTECEDENTES DE LA SEGURIDAD EN REDES</b>	
1 Conozca TCP/IP	7
La historia de TCP/IP .....	8
Exploración de direcciones, subredes y nombres de host .....	9
<i>Clases de dirección</i> .....	10
<i>Subredes</i> .....	12
<i>Direcciones sin clase y CIDR</i> .....	15
<i>Nombres de host</i> .....	16
Interfaces de red .....	18
<i>El uso de ifconfig</i> .....	19
Revisión de los archivos de configuración de la red .....	22
<i>El archivo /etc/hosts</i> .....	22
<i>El archivo /etc/ethers</i> .....	23
<i>El archivo /etc/networks</i> .....	23
<i>El archivo /etc/protocols</i> .....	24
<i>El archivo /etc/services</i> .....	24
<i>El archivo /etc/inetd.conf</i> .....	25
Conozca los archivos de acceso a la red .....	26
<i>El archivo /etc/hosts.equiv</i> .....	26
<i>El archivo .rhosts</i> .....	26
<i>Equivalencia de usuario y de host</i> .....	27
Revisión de los daemons TCP/IP .....	28
<i>El daemon slink</i> .....	28
<i>El daemon ldsocket</i> .....	28
<i>El daemon cpd</i> .....	29
<i>El daemon impresor de líneas (lpd)</i> .....	29
<i>El daemon SNMP (snmpd)</i> .....	29
<i>El daemon RARP (rarpd)</i> .....	29
<i>El daemon BOOTP (bootpd)</i> .....	30
<i>El daemon de ruta (routed)</i> .....	30
<i>El Servidor de Nombre de Dominio (named)</i> .....	31
<i>El registrador del sistema (syslogd)</i> .....	31



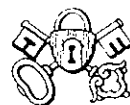
<i>inetd - El superservidor</i> .....	32
<i>El daemon RWHO (rwhod)</i> .....	32
Exploración de las utilerías TCP/IP .....	32
<i>Comandos de administración</i> .....	32
<i>Comandos de usuario</i> .....	48
Resumen .....	57
<b>2 Seguridad</b> .....	<b>59</b>
Análisis de los niveles de seguridad .....	60
<i>Nivel D1</i> .....	60
<i>Nivel C1</i> .....	60
<i>Nivel C2</i> .....	61
<i>Nivel B1</i> .....	62
<i>Nivel B2</i> .....	62
<i>Nivel B3</i> .....	62
<i>Nivel A</i> .....	62
Seguridad canadiense .....	62
<i>Nivel EAL-1</i> .....	63
<i>Nivel EAL-2</i> .....	63
<i>Nivel EAL-3</i> .....	63
<i>Nivel EAL-4</i> .....	63
<i>Nivel EAL-5</i> .....	64
<i>Nivel EAL-6</i> .....	64
<i>Nivel EAL-7</i> .....	64
Análisis de las cuestiones de seguridad local .....	64
<i>Políticas de seguridad</i> .....	65
<i>El archivo Password</i> .....	65
<i>El archivo shadow password</i> .....	67
<i>El archivo dialup password</i> .....	68
<i>El archivo Group</i> .....	70
Caducidad y control de la contraseña .....	72
Vándalos y contraseñas .....	75
<i>Cómo adivinan las contraseñas los vándalos</i> .....	76
Seguridad C2 y la Base de Cómputo Confiable .....	78
La equivalencia de red .....	80
<i>Equivalencia del host</i> .....	80
<i>Equivalencia de usuario</i> .....	82



Definición de usuarios y grupos .....	83
Comprensión de los permisos .....	84
<i>Repaso de los permisos estándar</i> .....	84
<i>Ratiz y NFS</i> .....	87
Exploración de los métodos de encriptación de datos .....	87
<i>Cómo se encriptan las contraseñas</i> .....	87
<i>Encriptación de archivos</i> .....	89
Examen de la autenticación Kerberos .....	90
<i>Conozca a Kerberos</i> .....	91
<i>Desventajas de Kerberos</i> .....	91
IP Spoofing .....	92
Resumen .....	92
Reconocimientos .....	93
Programa de muestra .....	93
<b>3</b> <b>Cómo diseñar una política de red</b> .....	<b>97</b>
Planeación de seguridad en redes .....	98
Política de seguridad del sitio .....	98
Planteamiento de la política de seguridad .....	99
Cómo asegurar la responsabilidad hacia la política de seguridad .....	102
Análisis de riesgo .....	102
Identificación de recursos .....	106
Identificación de las amenazas .....	106
<i>Definición del acceso no autorizado</i> .....	107
<i>Riesgo de revelación de información</i> .....	107
<i>Negación del servicio</i> .....	108
Uso y responsabilidades de la red .....	108
Identificación de quién está autorizado para usar los recursos de la red .....	109
<i>Identificación del uso adecuado         de los recursos</i> .....	109
<i>Quién está autorizado para conceder acceso y aprobar el uso</i> .....	111
<i>Determinación de las responsabilidades del usuario</i> .....	116
<i>Determinación de las responsabilidades de los administradores         de sistemas</i> .....	117
<i>Qué hacer con la información delicada</i> .....	117
Plan de acción cuando se viole la política de seguridad .....	118
<i>Respuesta a las violaciones de la política</i> .....	118
<i>Respuesta a las violaciones de la política por usuarios locales</i> .....	119
<i>Estrategias de respuesta</i> .....	119



<i>Definición de responsabilidades para ser buen ciudadano de Internet</i> .....	122
<i>Contactos y responsabilidades con organizaciones externas</i> .....	123
Interpretación y publicación de la política de seguridad .....	123
Identificación y prevención de problemas de seguridad .....	124
<i>Puntos de acceso</i> .....	125
<i>Sistemas mal configurados</i> .....	127
<i>Problemas de software</i> .....	128
<i>Amenazas internas</i> .....	128
<i>Seguridad física</i> .....	128
<i>Confidencialidad</i> .....	129
Implementación de controles costeables para la política .....	130
Selección del control de la política .....	130
Uso de estrategias de reserva .....	131
Detección y vigilancia de actividades no autorizadas .....	131
Inspección del uso del sistema .....	131
Mecanismos de inspección .....	132
Horario de inspección .....	133
Procedimientos de reporte .....	134
<i>Procedimientos de administración de cuentas</i> .....	134
<i>Procedimientos de administración de configuración</i> .....	135
<i>Procedimientos de recuperación</i> .....	136
Procedimientos de reporte de problemas para los administradores del sistema .....	139
Protección de las conexiones de red .....	139
Uso de la encriptación para proteger la red .....	140
<i>Estándar de Encriptación de Datos (DES)</i> .....	141
<i>Crypt</i> .....	142
<i>Correo de Privacidad Mejorada (PEM)</i> .....	142
<i>Privacidad Bastante Buena (PGP)</i> .....	142
<i>Autenticación de origen</i> .....	143
<i>Integridad de la información</i> .....	144
<i>Sumas de verificación</i> .....	144
<i>Sumas de verificación criptográfica</i> .....	145
<i>Cómo usar sistemas de autenticación</i> .....	145
<i>Cómo utilizar tarjetas inteligentes</i> .....	146
Cómo utilizar Kerberos .....	146
Cómo mantenerse actualizado .....	146
Listas de correo .....	147
<i>Listas de correo de seguridad de Unix</i> .....	148
<i>La lista del foro de riesgos</i> .....	148



<i>La lista VIRUS-L</i> .....	149
<i>La lista Bugtraq</i> .....	149
<i>El compendio no comercial de la computación</i> .....	150
<i>La lista de correo CERT</i> .....	150
<i>La lista de correo CERT-TOOLS</i> .....	151
<i>La lista de correo TCP/IP</i> .....	151
<i>La lista de correos SUN-NETS</i> .....	151
Grupos de noticias .....	152
Equipos de respuesta de seguridad .....	153
<i>Equipo de Respuesta a Emergencias de Cómputo</i> .....	153
<i>Centro de Coordinación de Seguridad DDN</i> .....	154
<i>Centro de Recursos y Respuesta de Seguridad en Computado-     ras del NIST</i> .....	155
<i>Capacidad de Asesoría en Incidentes de Computadoras del DOE</i> ....	156
<i>Equipo de Respuesta de Seguridad de Red de Computado-     ras Ames de la NASA</i> .....	156
Resumen .....	157
<b>4 Sistema de autenticación con contraseña usada una sola vez</b> .....	<b>159</b>
¿Qué es OTP? .....	160
La historia de OTP .....	162
Implementación de OTP .....	163
<i>Decisión acerca de la versión de OTP que se utilizará</i> .....	165
<i>Cómo funcionan S/KEY y OPIE</i> .....	166
La versión 1.0 de S/KEY .....	167
OPIE de los laboratorios de investigación naval .....	168
<i>Cómo obtener el código fuente de OPIE</i> .....	168
<i>Compilación del código OPIE</i> .....	170
<i>Prueba de los programas compilados</i> .....	172
Instalación de OPIE .....	177
<i>Los componentes OPIE</i> .....	180
LogDaemon 5.0 .....	183
<i>Cómo obtener el código LogDaemon</i> .....	184
<i>Compilación del código LogDaemon</i> .....	185
<i>Pruebas de los programas compilados</i> .....	187
<i>Instalación de LogDaemon</i> .....	189
<i>Los componentes de LogDaemon</i> .....	189
Uso de las calculadoras S/KEY y OPIE .....	191
<i>Unix</i> .....	191
<i>Macintosh</i> .....	192



<i>Microsoft Windows</i> .....	193
<i>Calculadoras externas</i> .....	193
Cómo poner en práctica OTP .....	194
Notas de seguridad acerca de /bin/login .....	196
Uso de OTP y X Windows .....	196
Cómo obtener mayor información .....	197
Resumen .....	198

## PARTE II ❖ ROUTERS DE SELECCIÓN Y FIREWALLS

5	Introducción a los routers de selección	201
	Aclaración de definiciones .....	202
	<i>Zonas de riesgo</i> .....	202
	<i>El Modelo de Referencia OSI y los routers de selección</i> .....	203
	<i>Las capas del modelo OSI</i> .....	204
	<i>Routers de selección y firewalls en relación con el modelo OSI</i> .....	224
	Comprensión de la filtración de paquetes .....	225
	<i>Filtración de paquetes y política de red</i> .....	225
	<i>Modelo simple para la filtración de paquetes</i> .....	226
	<i>Operaciones de filtración de paquetes</i> .....	227
	<i>Diseño de la filtración de paquetes</i> .....	229
	<i>Reglas de filtración de paquetes y asociaciones totales</i> .....	233
	Resumen .....	235
6	Filtros de paquetes	237
	Implementación de reglas de filtración de paquetes .....	238
	<i>Definición de listas de acceso</i> .....	238
	<i>Uso de las listas de acceso estándar</i> .....	239
	<i>Uso de las listas de acceso extendidas</i> .....	240
	<i>Filtración de llamadas entrantes o salientes de la terminal</i> .....	243
	Examen de la colocación del filtro de paquetes y la suplantación de direcciones .....	244
	<i>Colocación del filtro de paquetes</i> .....	244
	<i>Filtración en puertos de entrada y salida</i> .....	245
	Examen de temas específicos del protocolo en la filtración de paquetes .....	248
	<i>Filtración del tráfico de la red FTP</i> .....	248
	<i>Filtración del tráfico de red de TELNET</i> .....	269
	<i>Filtración de sesiones X-Windows</i> .....	270
	<i>Filtración de paquetes y el protocolo de transporte UDP</i> .....	271



	<i>Filtración de paquetes de ICMP</i> .....	273
	<i>Filtración de paquetes RIP</i> .....	274
	Ejemplo de configuraciones de router de selección .....	275
	<i>Caso 1</i> .....	275
	<i>Caso 2</i> .....	276
	<i>Caso 3</i> .....	278
	Resumen .....	281
<b>7</b>	<b>Filtración de paquetes en PC</b> .....	<b>283</b>
	Filtros de paquete basados en PC .....	284
	<i>El filtro de paquetes KarlBridge</i> .....	284
	<i>El filtro de paquetes Drawbridge</i> .....	304
	Resumen .....	322
<b>8</b>	<b>Arquitectura y teoría de firewalls</b> .....	<b>325</b>
	Examen de los componentes de firewall .....	326
	<i>Host de base dual</i> .....	327
	<i>Hosts de bastión</i> .....	335
	<i>Subredes seleccionadas</i> .....	349
	<i>Gateways a nivel de aplicación</i> .....	350
	Resumen .....	354
<b>9</b>	<b>Implementaciones de firewall</b> .....	<b>355</b>
	TCP Wrapper .....	356
	<i>Ejemplo 1</i> .....	357
	<i>Ejemplo 2</i> .....	357
	<i>Ejemplo 3</i> .....	358
	<i>Ejemplo 4</i> .....	358
	El gateway FireWall-1 .....	358
	<i>Requisitos de los recursos para FireWall-1</i> .....	359
	<i>Panorama de la arquitectura de FireWall-1</i> .....	359
	<i>Módulo de control de FireWall-1</i> .....	363
	<i>Network Objects Manager</i> .....	364
	<i>Services Manager</i> .....	367
	<i>Rules-Base Manager</i> .....	368
	<i>Log Viewer</i> .....	373
	<i>Ejemplos de aplicaciones de FireWall-1</i> .....	375
	<i>El desempeño de FireWall-1</i> .....	376
	<i>El lenguaje de las reglas de FireWall-1</i> .....	377
	<i>Cómo obtener información sobre FireWall-1</i> .....	379



ANS InterLock .....	379
<i>Requisitos de recursos para InterLock</i> .....	381
<i>Panorama de InterLock</i> .....	381
<i>Cómo configurar InterLock</i> .....	383
<i>La ACRB de InterLock</i> .....	385
<i>Servicios proxy del gateway de aplicación de InterLock</i> .....	387
<i>Fuente adicional de información sobre ANS InterLock</i> .....	395
Gauntlet de Trusted Information Systems .....	395
<i>Ejemplos de configuración con Gauntlet</i> .....	397
<i>Configuración de Gauntlet</i> .....	398
<i>La perspectiva del usuario sobre el uso de la firewall Gauntlet</i> .....	401
El TIS Firewall Toolkit .....	404
<i>Construcción del TIS Firewall Toolkit</i> .....	405
<i>Configuración del host de bastión con servicios mínimos</i> .....	408
<i>Instalación de los componentes del kit de herramientas</i> .....	410
<i>La tabla de permisos de red</i> .....	413
Resumen .....	420
10 El TIS Firewall Toolkit .....	421
Concepto de TIS .....	422
Dónde se encuentra el TIS Toolkit .....	422
Compilación bajo SunOS 4.1.3 y 4.1.4. ....	423
Compilación bajo BSDI .....	423
<i>Cambios de código</i> .....	424
Instalación del Toolkit .....	424
Preparación para la configuración .....	426
Configuración de TCP/IP .....	430
<i>Envío IP</i> .....	430
La tabla netperm .....	431
Configuración de netacl .....	433
<i>Conexión con netacl</i> .....	436
<i>Reinicio de INETD</i> .....	437
Configuración del proxy de Telnet .....	438
<i>Conexión mediante el proxy de Telnet</i> .....	441
<i>Reglas de acceso del host</i> .....	442
<i>Verificación del proxy de Telnet</i> .....	443
Configuración del gateway rlogin .....	444
<i>Conexión mediante el proxy de rlogin</i> .....	447
<i>Reglas de acceso del host</i> .....	448
<i>Verificación del proxy de rlogin</i> .....	448





Configuración del gateway FTP .....	449
<i>Reglas de acceso del host</i> .....	451
<i>Verificación del proxy de FTP</i> .....	452
<i>Conexión mediante el proxy de FTP</i> .....	453
<i>Aceptación de FTP con netacl</i> .....	454
Configuración de smap y smapd del proxy de sendmail .....	454
<i>Instalación del cliente smap</i> .....	455
<i>Configuración del cliente smap</i> .....	455
<i>Instalación de la aplicación smapd</i> .....	457
<i>Configuración de la aplicación smapd</i> .....	457
<i>Configuración DNS para smap</i> .....	459
Configuración del proxy de HTTP .....	460
<i>Clientes HTTP no específicos para proxy</i> .....	462
<i>Uso de un cliente HTTP específico para proxy</i> .....	463
<i>Reglas de acceso al host</i> .....	463
Configuración del proxy de X Windows .....	466
Conceptos del servidor de autenticación .....	467
<i>La base de datos de autenticación</i> .....	469
<i>Adición de usuarios</i> .....	472
<i>El shell de autenticación—authmgr</i> .....	476
<i>Administración de base de datos</i> .....	477
<i>La autenticación en funcionamiento</i> .....	479
Uso de plug-gw para otros servicios .....	480
<i>Configuración de plug-gw</i> .....	481
<i>plug-gw y NNTP</i> .....	482
<i>plug-gw y POP</i> .....	485
Herramientas administrativas adicionales .....	487
<i>Portscan</i> .....	487
<i>Netscan</i> .....	488
<i>Herramientas para elaboración de reportes</i> .....	489
<i>Reporte del servidor de autenticación</i> .....	491
<i>Reporte de denegación de servicios</i> .....	492
<i>Reporte de uso de FTP</i> .....	494
<i>Reporte de uso de HTTP</i> .....	494
<i>Reporte netacl</i> .....	495
<i>Reporte de uso del correo</i> .....	496
<i>Reporte de uso de Telnet y rlogin</i> .....	497
En dónde hay ayuda .....	498



11	Black Hole	501
	Conceptos de Black Hole .....	502
	<i>Requerimientos del sistema</i> .....	504
	<i>Módulos centrales de Black Hole</i> .....	506
	<i>Módulos de extensión de Black Hole</i> .....	509
	Diseño de una red con Black Hole .....	510
	<i>Repaso de la política de seguridad</i> .....	512
	Uso de la interfaz Black Hole .....	512
	Conceptos de la base de datos de políticas .....	514
	<i>Resolución de políticas y de reglas</i> .....	519
	Servicios, usuarios y reglas .....	521
	<i>Reglas</i> .....	521
	<i>Usuarios y mantenimiento de usuarios</i> .....	521
	Configuración de Black Hole .....	528
	<i>Configuración de un DNS interno y externo</i> .....	528
	<i>Configuración de servicios de aplicación</i> .....	531
	Generación de reportes .....	537
	Para mayor información .....	541
	Resumen .....	541

### PARTE III ❖ APÉNDICES

A	Lista de hojas de trabajo	545
B	Fuentes de información	547
	Herramientas .....	548
	<i>Tcpwrapper y portmapper</i> .....	548
	<i>Kit para firewall</i> .....	548
	<i>Bellcore S/Key</i> .....	549
	<i>One-Time Passwords In Everything (OPIE)</i> .....	549
	<i>Monitor de archivos de registro Swatch</i> .....	549
	<i>Tcpdump</i> .....	549
	<i>TAMU Tiger</i> .....	550
	<i>COPS</i> .....	550
	<i>Crack</i> .....	550
	<i>SATAN</i> .....	551
	<i>Passwd+</i> .....	551
	<i>npasswd</i> .....	551
	<i>Tripwire</i> .....	551



Vendedores de firewalls comerciales .....	552
Listas de correo sobre firewalls y seguridad .....	552
<i>Listas de correo sobre firewalls</i> .....	552
<i>Formas de seguridad</i> .....	553
<b>C Lista de vendedores</b> .....	<b>555</b>
<b>D Las páginas del manual para OPIE y Log Daemon</b> .....	<b>557</b>
Las páginas del manual OPIE .....	558
<i>opiefipd</i> .....	558
<i>opiekey</i> .....	561
<i>opiepasswd</i> .....	563
<i>opieinfo</i> .....	564
<i>opielogin</i> .....	565
<i>opiesu</i> .....	567
Las páginas del manual de Log Daemon .....	568
<i>fipd</i> .....	568
<i>key</i> .....	572
<i>keyinfo</i> .....	572
<i>keyinit</i> .....	573
<i>rexecd</i> .....	574
<i>rlogind</i> .....	576
<i>rshd</i> .....	577
<i>skey.access</i> .....	579
<i>skeysh</i> .....	582
<i>su</i> .....	582
<i>telnetd</i> .....	584
<b>Índice</b> .....	<b>585</b>