

INDICE

Introducción	1
Parte I. Información básica	
1. Para entender TCP/IP	9
La historia TCP/IP	10
Como explorar direcciones, subredes y nombres de anfitrión	11
Clases de direcciones	12
Subredes	14
Nombres de anfitrión	17
Como trabajar con interfaces de red	18
Como configurar mediante el uso del IFCONFIG	20
Revisión de los archivos de configuración de a red	
El archivo/etc/hosts	22
El archivo/etc/ethers	23
El archivo/etc/networks	23
El archivo/etc/protocols	
El archivo/etc/services	24
El archivo/etc/servicesinetd.conf	25
Como entender los archivos de acceso a la red	
El archivo/etc/hosts.equiv	26
El archivo.rhosts	
Equivalencia entre usuarios y anfitrión	27
Revisión de los demonios TCP/IP	
El demonio slink	28
El demonio ldsocket	
El demonio CPD	
El demonio Line Printer (LDP)	
El demonio SNMP (SNMPD)	29
El demonio CPD	
El demonio RARP (RARPD)	
El demonio BOOTP (BOOTPD)	
El demonio Route (ROUTED)	
El servicio de nombre de demonio: NAMED	30
El registrador de sistema: SYSLOGD	
INETD: el superservidor	31
El demonio RWHO (RWHOD)	
Incursión en las utilerías de TCP/IP	
Comandos de administración	32
Comandos del usuario	45
Resumen	54
2. Seguridad	55
Análisis de los niveles de seguridad	
Nivel D1	56
Nivel C1	
Nivel C2	
Nivel B1	57
Nivel B2	
Nivel B3	58

Nivel A	
Análisis de los asuntos de seguridad local	
Políticas de seguridad	
El archivo Password	59
El archivo Shadow Password	61
El archivo Dialup Password	62
El archivo Group	64
Caducidad y control de la contraseña	65
Vándalos y contraseñas	69
Para entender como “adivinan” las contraseñas los vándalos	70
Seguridad C2 y la base computacional confiable	71
Como entender la equivalencia de red	
Equivalencia de anfitrión	73
Equivalencia del usuario	75
Como definir usuarios y grupos	76
Como entender los permisos	
Unas revisión a los permisos estándares	77
Raíz y NFSÇ	
Como explorar los métodos de encriptación de datos	80
Como encriptar las contraseñas	
Como encriptar archivos	82
Un examen al sistema Kerberos	83
Como entender Kerberos	
Desventajas de Kerberos	84
Como entender IP spoofing	85
Resumen	
Reconocimientos	86
Un programa de muestra	
Listado 2.1: PWEXP.PL	
3. Como diseñar una política de red	89
Planeación de la seguridad en la red	
Política de la seguridad en la red	90
Planteamiento de la política de seguridad	91
Como asegurar la responsabilidad de una política de seguridad	
Análisis de riesgos	94
Como identificar recursos	
Como identificar las amenazas	98
Definición de acceso no autorizado	
Riesgo de divulgar información	99
Servicio denegado	
Uso de la red y responsabilidades	100
Como identificar quien se le permite utilizar los recursos de la red	
Identifique el uso correcto de un recurso	101
Como determinar quien esta autorizado a otorgar acceso y a aprobar el uso	103
Como determinar las responsabilidades del usuarios	107
Como determinar las responsabilidades de los administradores del sistema	108
Que hacer la información delicada	109

Plan de acción cuando la política de seguridad ha sido violada	
Como responder a las violaciones de la política	110
Respuesta a las violaciones de la política por usuarios locales Estrategias de respuesta	111
Como definir las responsabilidades para ser un buen ciudadano en Internet	114
Contactos y responsabilidades con organizaciones externas Como interpretar y publicar la política de seguridad	115
Para identificar y prevenir problemas de seguridad	116
Puntos de acceso	117
Sistemas mal configurados	119
Problemas de software Amenazas del usuario de confianza Seguridad física	120
Confidencialidad	121
Implantación de controles costeables a la política Selección de la política de control	122
Como utilizar estrategias de amortiguamiento Como detectar y vigilar la actividad no autorizada Como vigilar el uso del sistema	123
Como vigilar los mecanismos	124
Horario de vigilancia	125
Procedimientos para informar Procedimientos para manejo de cuentas	126
Configuración de procedimientos de administración	127
Procedimientos de recuperación	128
Procedimientos para informar a los administradores del sistema Como proteger las conexiones de la red	131
Como utilizar la encriptación para proteger la red	132
Entandar de encriptación de datos (DES) Crypt Correo de privacidad mejorada (PEM)	133
Autenticación del origen	134
Integridad de la información Como usar las sumas de verificación	135
Las sumas de verificación criptográfica Como usar los sistemas de autenticación	136
Como utilizar tarjetas inteligentes Como utilizar Kerberos	137
Como mantenerse actualizado Listas de correo	138
Listas de correo de seguridad en Unix La lista del foro de riesgos	139
La lista VIRUS-L La lista Bugtraq	140
El comprendió no comercial de computación La lista de correo CERT	141
La lista de correo CERT-TOOLS La lista de correo TCP/IP	142

La lista de correo SUN-NETS	
Grupo de noticias	143
Equipo para respuestas de seguridad	
Equipo para respuestas de emergencia de la computadora	144
Centro de coordinación de seguridad DDN	145
Centro NIST de respuesta y recursos de seguridad para computadoras	
Capacidad asesora de incidentes de computadora (CIAC) del DOE	146
Equipo de respuesta de seguridad de red de computadora	
Ames de la NASA	147
Resumen	
Parte II. Enrutadores de selección y barreras de protección	
4. Introducción a los enrutadores de selección	151
Definiciones claras	
Zonas de riesgo	152
El modelo de referencia OSI y los enrutadores de selección	153
Capas del modelo OSI	154
enrutadores de selección y barreras de protección con relación al modelo OSI	173
Como entender la filtración de paquetes	
Filtración de paquetes y política de red	174
Un modelo sencillo de filtración de paquetes	175
Operaciones del filtro de paquetes	176
Diseño de filtro de paquetes	178
Reglas del filtro de paquetes y asociaciones completas	182
Resumen	184
5. Filtros de paquetes	185
Como implantar las reglas de filtro de paquetes	
Definición de las listas de acceso	186
Como utilizar las listas de acceso estándares	187
Como utilizar las listas de acceso extendidas	188
Como filtrar las llamadas entrantes y salientes	
Como comprender la opción de seguridad IP para los enrutadores Cisco	191
Como examinar la colocación de filtro de paquetes y la suplantación de dirección	192
Colocación de filtro de paquetes	
Como filtrar en puertos de entrada y salida	194
Como examinar los temas relacionados con el protocolo en la filtraron de paquetes	196
Como filtrar el trafico en una red FTP	
Como filtrar el trafico en la red TELNET	217
Como filtrar sesiones X-Windows	218
Filtración de paquetes y el protocolo de transporte UDP	219
Filtración de paquetes ICMP	221
Filtración de paquetes RIP	222
Configuraciones de ejemplo sobre los enrutados de selección	
Caso 1	223
Caso 2	224
Caso 3	226
Resumen	229

6. Filtración de paquetes en PCs	231
Filtros de paquetes en PC	
El filtro de paquetes KarlBridge	232
El filtro de paquetes Drawbridge	252
Resumen	270
7. Arquitecta y teoría de las barreras de protección	273
Análisis de los componentes de las barreras de protección	274
Anfitrión de dos bases	275
Anfitriones de bastión	283
Subredes seleccionadas	297
Compuertas a nivel de aplicación	298
Resumen	302
8. Implantación de las barreras de protección	303
TCP Wrapper	304
Ejemplo 1	
Ejemplo 2	305
Ejemplo 3	
Ejemplo 4	306
La compuerta FireWall-1	
Requerimientos de recursos para FireWall-1	
Vista general de la arquitectura FireWall-1	307
Modulo de control FireWall-1	311
Network Objects Manager	312
Services Manager	315
Rules-Base Manager	316
Log Viewer	321
Ejemplos de aplicaciones Fire-Wall-1	323
Desempeño de Fire-Wall-1	324
Lenguaje de reglas Fire-Wall-1	325
Como obtener información en Fire-Wall-1	
ANS InterLock	327
Requerimientos de recursos para InterLock	
Vista general de InterLock	329
Como configurar InterLock	331
InterLock ACRB	333
Servicios de compuerta InterLock para a aplicación apoderada	335
Fuentes adicionales de información para ANS InterLock	
Gauntlet de Trusted Information Systems	343
Ejemplo de configuración con el uso de Gauntlet	345
Como configurar Gauntlet	346
Vista de usuarios sobre la barrera de protección Gauntlet	349
TIS Fire Wall Toolkit	352
Como construir TIS Fire Wall Toolkit	353
Como configurar el anfitrión de bastión con servicios mínimos	360
Instale los componentes de Toolkit	362
La tabla de autorizaciones en red	365
Resumen	372
Parte III. Apéndices	
A. lista de hojas de trabajo	375

B. Fuentes de información	377
Un sondeo a las herramientas disponibles al público TCCPWRAPPER y mapeador de puertos TIS Fire Wall Kit Bellcore S/Key	378
Monitor de bitácoras swtach Tcpcdump TAMU tiger COPS	379
Crack Descubra a los proveedores de barreras de protección comerciales Un recorrido por las barreras de protección y listas de correo de seguridad	380
Listas de correo de barreras de protección Foros de seguridad	381
C. Listas de proveedores	383
Índice	385