
Contenido

Prefacio	xiii
I: Elementos de seguridad informática	1
1: Introducción	3
¿Qué es la seguridad informática?	5
¿Qué es un sistema operativo?	6
Historia de UNIX.....	7
Seguridad y UNIX	13
El papel de este libro	17
2: Políticas y recomendaciones	19
Cómo se planean los requerimientos de seguridad	20
Análisis de riesgos	22
Análisis de costo-beneficio	25
Políticas	29
El problema de la seguridad por ocultación	34
II: Responsabilidades del usuario	39
3: Usuarios y contraseñas	41
Nombres de usuario	41
Contraseñas	43
Introducción de la contraseña	47

Cambio de contraseña	48
Verificación de la nueva contraseña	49
Cuidado y suministro de contraseñas	51
Contraseñas descartables	56
Resumen	57
4: Usuarios, grupos y el superusuario	59
Usuarios y grupos	59
Nombres de usuario especiales	65
su: cómo se cambia la identidad	70
Resumen	76
5: El sistema de archivo de UNIX	77
Archivos	77
Uso de los permisos de archivo	85
umask	96
Uso de los permisos de directorio	98
SUID	100
Archivos de dispositivos	110
chown: cómo se cambia el dueño de un archivo	112
chgrp: cómo se cambia el grupo de un archivo	114
Cosas raras y malas ideas	115
Resumen	117
6: Criptografía.....	118
Una breve historia de la criptografía	118
¿Qué es el cifrado?	121
El sistema de cifrado Enigma	125
Algoritmos criptográficos comunes	127
Compendio de mensajes y firmas digitales	143
Programas de cifrado disponibles para UNIX	150
des: el Estándar de Cifrado de Datos	152
Cifrado y las leyes de Estados Unidos	163

III: Seguridad del sistema	167
7: Respaldos	169
¡Es necesario crear respaldos!	170
Ejemplo de estrategias de respaldo	180
Respaldo de sistemas de archivos	185
Programas para respaldos	188
8: Defensa de las cuentas	193
Cuentas peligrosas	193
Monitoreo del formato de archivos	201
Logins restringidos	202
Administración de cuentas inactivas	204
Protección de la cuenta root	208
El sistema UNIX de contraseñas cifradas	211
Contraseñas descartables	215
Técnicas administrativas para contraseñas convencionales	220
9: Administración de la integridad	234
Prevención	235
Detección de cambios	239
Una nota final	247
10: Auditoría y registro en bitácoras	248
Las bitácoras simples	249
Archivo acct/pacct de contabilidad de procesos	257
Bitácoras específicas por programa	260
Trazas de cada usuario en el sistema de archivos	264
Facilidad para registro en bitácora del sistema UNIX (syslog)	266
Swatch: una herramienta de registro	274
Bitácoras manuscritas	276
Administración de archivos de bitácora	279

11: Protegerse de amenazas programadas	281
Amenazas programadas: definiciones	281
Daños	290
Autores	291
Entrada	292
Protegerse uno mismo	293
Protección del sistema	304
12: Seguridad física	308
Una amenaza olvidada	308
Protección del equipo	310
Protección de los datos	323
Una historia: Una inspección desastrosa	331
13: La seguridad y el personal.....	334
Investigación de antecedentes	335
Durante el trabajo	336
Extraños	339
IV: Seguridad en red e Internet	341
14: Seguridad del acceso telefónico	343
Módems, teoría de operación	343
Interfaces seriales	345
El protocolo seriado RS-232	345
Módems y seguridad	349
Módems y UNIX	354
Medidas adicionales de seguridad para módems	361
15: UUCP	363
Comentarios acerca de UUCP	364
Versiones de UUCP	367
UUCP y la seguridad	368
Medidas de seguridad en la versión 2 de UUCP	371
La seguridad en la versión BNU de UUCP	377

Otros asuntos sobre seguridad.....	383
Problemas de seguridad con las primeras versiones de UUCP	384
UUCP a través de las redes	386
Resumen	387
16: Redes TCP/IP	388
Establecimiento de redes	388
IPv4: el protocolo Internet versión 4	391
Seguridad de IP	407
Otros protocolos de red	413
Resumen	414
17: Servicios TCP/IP	415
Los servidores de Internet con UNIX	416
Control del acceso a los servidores	420
Servicios primarios de red en UNIX	420
Implicaciones de seguridad de los servicios de red	459
Observación de la red local con netstat	460
Exploración de la red	463
Resumen	464
18: Seguridad en el WWW.....	465
Seguridad y el World Wide Web	465
Operación de un servidor seguro	467
Control del acceso a los archivos en el servidor	476
Evitar los riesgos de escuchas indiscretos	482
Riesgos de los examinadores Web	486
Dependencia en terceros	488
Resumen	489
19: RPC, NIS, NIS+ y Kerberos.....	490
Asegurar los servicios de red	491
Llamadas a procedimientos remotos (RPC).....	491
RPC seguro (AUTH_DES)	495
Sistema de información de red (NIS) de Sun	502

NIS+ de Sun	510
Kerberos	516
Otros sistemas de autenticación en red	523
20: NFS	525
Cómo funciona NFS	525
Seguridad NFS del lado del servidor	535
Seguridad NFS del lado del cliente	539
Mejoras en la seguridad NFS	540
Algunos últimos comentarios	548
V: Temas avanzados	551
21: Cortafuegos	553
Qué es un cortafuego	554
Construcción de un cortafuego propio	564
Ejemplo: enrutadores de Cisco Systems como bobinas	567
Configuración de la puerta	573
Consideraciones especiales	578
Comentarios finales	580
22: Envoltentes y apoderados	583
Por qué se necesitan los envoltentes	583
Envoltente sendmail (smap/smapi)	584
tcpwrapper	588
SOCKS	599
El relevador UDP	608
Escribir los envoltentes propios	609
23: Elaboración de programas SUID y de red seguros	612
Una falla de programación puede arruinar todo... ..	612
Consejos para evitar las fallas de programación relacionadas con la seguridad	616
Consejos para elaborar programas SUID/SGID	626
Consejos al utilizar contraseñas	629
Consejos para generar números aleatorios	630

VI: Manejo de incidentes de seguridad	637
24: Descubrir una intrusión	639
Preludio	639
Descubrir a un intruso	641
Las bitácoras: descubrir las huellas de los intrusos	651
Arreglar los sistemas después de una introducción ilegal	652
Un ejemplo	657
Restaurar el funcionamiento	659
Control del daño	660
25: Ataques de denegación del servicio y sus soluciones	661
Ataques destructivos	662
Ataques de saturación	662
Ataques de denegación del servicio en red	674
26: Seguridad de computadoras y legislación	678
Las opciones legales después de una penetración	678
Demandas penales	679
Denuncias civiles	687
Otros puntos vulnerables	688
27: En quién se puede confiar	695
¿Se puede confiar en la computadora?	695
¿Se puede confiar en los proveedores?	699
¿Se puede confiar en la gente?	704
Qué significa todo esto	708
VII: Apéndices	709
A: Lista de control de seguridad en UNIX.....	711
B: Archivos importantes	731
Archivos y dispositivos relacionados con la seguridad	731
Archivos importantes en el directorio base	737
Los archivos SUID y SGID	737

C: Procesos UNIX.....	746
Acerca de los procesos	746
Creación de procesos	754
Señales	755
La instrucción kill	756
Iniciar UNIX y establecer una sesión.....	758
D: Bibliografía impresa	762
Referencias acerca de la seguridad en UNIX	762
Otras referencias sobre sistemas de cómputo	763
Revistas sobre seguridad	772
E: Fuentes electrónicas	775
Listas de correo	775
Grupos de Usenet	779
Páginas del WWW	780
Programas	781
F: Organizaciones	788
Organizaciones profesionales	788
Organizaciones del Gobierno de Estados Unidos	792
Organizaciones de respuesta a emergencias.....	792
G: Tabla de servicios IP	802
Índice	811