

SEGURIDAD EN UNIX Y REDES

Versión 2.1'

Antonio Villalón Huerta

Julio, 2000 – Julio, 2002 – Enero, 2020

© Antonio Villalón Huerta

© Derechos de edición:

Nau Llibres - Edicions Culturals Valencianes, S.A.

Tel.: 96 360 33 36, Fax: 96 332 55 82.

C/ Periodista Badía, 10. 46010 Valencia

E-mail: nau@naullibres.com web: www.naullibres.com

Diseño de portada e interiores:

Carol López, Pablo Navarro y Artes Digitales Nau Llibres

ISBN: 978-84-18047-04-6

Dep.Legal: V-3368-2019

Imprime:

Safekat

Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la ley. Diríjase a CEDRO (Centro Español de Derechos Reprográficos) si necesita fotocopiar o escanear algún fragmento de esta obra (www.conlicencia.com; 91 702 19 70 / 93 27204 45).



Copyright © 2000,2002 Antonio Villalón Huerta.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.1 or any later version published by the Free Software Foundation; with the Invariant Sections being ‘Notas del Autor’ and ‘Conclusiones’, with no Front-Cover Texts, and with no Back-Cover Texts. A copy of the license is included in the section entitled ‘GNU Free Documentation License’.

Índice general

Notas del autor	XVII
1. Introducción y conceptos previos	1
1.1. Introducción	1
1.2. Justificación y objetivos	2
1.3. ¿Qué es <i>seguridad</i> ?	3
1.4. ¿Qué queremos proteger?	5
1.5. ¿De qué nos queremos proteger?	7
1.5.1. Personas	7
1.5.2. Amenazas lógicas	10
1.5.3. Catástrofes	14
1.6. ¿Cómo nos podemos proteger?	14
1.7. Redes ‘normales’	17
1.7.1. Redes de I+D	18
1.7.2. Empresas	20
1.7.3. ISPs	21
1.8. ¿Seguridad en Unix?	23
I Seguridad del entorno de operaciones	25
2. Seguridad física de los sistemas	27
2.1. Introducción	27
2.2. Protección del <i>hardware</i>	28
2.2.1. Acceso físico	29
2.2.2. Desastres naturales	31
2.2.3. Desastres del entorno	34
2.3. Protección de los datos	38
2.3.1. <i>Eavesdropping</i>	39
2.3.2. <i>Backups</i>	40
2.3.3. Otros elementos	41
2.4. Radiaciones electromagnéticas	43

3. Administradores, usuarios y personal	47
3.1. Introducción	47
3.2. Ataques potenciales	48
3.2.1. Ingeniería social	48
3.2.2. <i>Shoulder Surfing</i>	49
3.2.3. Masquerading	50
3.2.4. Basureo	50
3.2.5. Actos delictivos	53
3.3. ¿Qué hacer ante estos problemas?	53
3.4. El atacante interno	55
II Seguridad del sistema	59
4. El sistema de ficheros	61
4.1. Introducción	61
4.2. Sistemas de ficheros	62
4.3. Permisos de un archivo	66
4.4. Los bits SUID, SGID y <i>sticky</i>	69
4.5. Atributos de un archivo	74
4.6. Listas de control de acceso: ACLs	76
4.7. Recuperación de datos	80
4.8. Almacenamiento seguro	81
4.8.1. La orden <code>crypt(1)</code>	81
4.8.2. PGP: <i>Pretty Good Privacy</i>	82
4.8.3. TCFS: <i>Transparent Cryptographic File System</i>	84
4.8.4. Otros métodos de almacenamiento seguro	85
5. Programas seguros, inseguros y nocivos	89
5.1. Introducción	89
5.2. La base fiable de cómputo	90
5.3. Errores en los programas	91
5.3.1. Buffer overflows	92
5.3.2. Condiciones de carrera	93
5.4. Fauna y otras amenazas	94
5.4.1. Virus	96
5.4.2. Gusanos	97
5.4.3. Conejos	99
5.4.4. Caballos de Troya	99
5.4.5. Applets hostiles	101
5.4.6. Bombas lógicas	102
5.4.7. Canales ocultos	103
5.4.8. Puertas traseras	104
5.4.9. Superzapping	105
5.4.10. Programas salami	106
5.5. Programación segura	107

6. Auditoría del sistema	117
6.1. Introducción	117
6.2. El sistema de <i>log</i> en Unix	118
6.3. El demonio <i>syslogd</i>	119
6.4. Algunos archivos de <i>log</i>	123
6.4.1. <i>syslog</i>	123
6.4.2. <i>messages</i>	124
6.4.3. <i>wtmp</i>	125
6.4.4. <i>utmp</i>	125
6.4.5. <i>lastlog</i>	126
6.4.6. <i>faillog</i>	126
6.4.7. <i>loginlog</i>	126
6.4.8. <i>btmp</i>	127
6.4.9. <i>sulog</i>	127
6.4.10. <i>debug</i>	127
6.5. <i>Logs</i> remotos	128
6.6. Registros físicos	131
7. Copias de seguridad	133
7.1. Introducción	133
7.2. Dispositivos de almacenamiento	134
7.3. Algunas órdenes para realizar copias de seguridad	138
7.3.1. <i>dump/restore</i>	139
7.3.2. La orden <i>tar</i>	144
7.3.3. La orden <i>cpio</i>	145
7.3.4. <i>Backups</i> sobre CD-ROM	147
7.4. Políticas de copias de seguridad	148
8. Autenticación de usuarios	153
8.1. Introducción y conceptos básicos	153
8.2. Sistemas basados en algo conocido: contraseñas	154
8.3. Sistemas basados en algo poseído: tarjetas inteligentes	155
8.4. Sistemas de autenticación biométrica	157
8.4.1. Verificación de voz	159
8.4.2. Verificación de escritura	161
8.4.3. Verificación de huellas	161
8.4.4. Verificación de patrones oculares	163
8.4.5. Verificación de la geometría de la mano	165
8.5. Autenticación de usuarios en Unix	167
8.5.1. Autenticación clásica	167
8.5.2. Mejora de la seguridad	169
8.6. PAM	175

III	Algunos sistemas Unix	181
9.	Solaris	183
9.1.	Introducción	183
9.2.	Seguridad física en SPARC	184
9.3.	Servicios de red	187
9.4.	Usuarios y accesos al sistema	188
9.5.	El sistema de parcheado	194
9.6.	Extensiones de la seguridad	197
9.6.1.	ASET	197
9.6.2.	JASS	199
9.6.3.	sfpDB	201
9.7.	El subsistema de red	203
9.8.	Parámetros del núcleo	207
10.	Linux	211
10.1.	Introducción	211
10.2.	Seguridad física en x86	212
10.3.	Usuarios y accesos al sistema	216
10.4.	El sistema de parcheado	222
10.5.	El subsistema de red	225
10.6.	El núcleo de Linux	227
10.6.1.	Opciones de compilación	227
10.6.2.	Dispositivos	228
10.6.3.	Algunas mejoras de la seguridad	229
11.	AIX	233
11.1.	Introducción	233
11.2.	Seguridad física en RS/6000	234
11.3.	Servicios de red	235
11.4.	Usuarios y accesos al sistema	238
11.4.1.	El fichero <code>/etc/security/.ids</code>	239
11.4.2.	El fichero <code>/etc/security/passwd</code>	240
11.4.3.	El fichero <code>/etc/security/failedlogin</code>	241
11.4.4.	El fichero <code>/etc/security/lastlog</code>	241
11.4.5.	El fichero <code>/etc/security/limits</code>	242
11.4.6.	El fichero <code>/etc/security/login.cfg</code>	243
11.4.7.	El fichero <code>/etc/security/user</code>	246
11.4.8.	El fichero <code>/etc/security/group</code>	251
11.5.	El sistema de <i>log</i>	251
11.6.	El sistema de parcheado	255
11.7.	Extensiones de la seguridad: filtros IP	256
11.8.	El subsistema de red	260

12.HP-UX	265
12.1. Introducción	265
12.2. Seguridad física en PA-RISC	266
12.3. Usuarios y accesos al sistema	267
12.4. El sistema de parcheado	270
12.5. Extensiones de la seguridad	274
12.5.1. Product Description Files	274
12.5.2. <code>inetd.sec(4)</code>	276
12.6. El subsistema de red	278
12.7. El núcleo de HP-UX	281
IV Seguridad de la subred	285
13.El sistema de red	287
13.1. Introducción	287
13.2. Algunos ficheros importantes	287
13.2.1. El fichero <code>/etc/hosts</code>	287
13.2.2. El archivo <code>/etc/ethers</code>	288
13.2.3. El fichero <code>/etc/networks</code>	288
13.2.4. El fichero <code>/etc/services</code>	289
13.2.5. El fichero <code>/etc/protocols</code>	289
13.2.6. El fichero <code>/etc/hosts.equiv</code>	290
13.2.7. El fichero <code>.netrc</code>	291
13.2.8. El fichero <code>/etc/inetd.conf</code>	292
13.3. Algunas órdenes importantes	294
13.3.1. La orden <code>ifconfig</code>	294
13.3.2. La orden <code>route</code>	295
13.3.3. La orden <code>netstat</code>	295
13.3.4. La orden <code>ping</code>	297
13.3.5. La orden <code>traceroute</code>	299
13.4. Servicios	299
14.Algunos servicios y protocolos	303
14.1. Introducción	303
14.2. Servicios básicos de red	304
14.2.1. <code>systat</code>	304
14.2.2. <code>daytime</code>	305
14.2.3. <code>netstat</code>	306
14.2.4. <code>chargen</code>	307
14.2.5. <code>tftp</code>	307
14.2.6. <code>finger</code>	308
14.2.7. <code>POP</code>	309
14.2.8. <code>auth</code>	310
14.2.9. <code>NNTP</code>	311
14.2.10. <code>NTP</code>	311

14.2.11.UUCP	312
14.3. El servicio FTP	313
14.3.1. FTP anónimo	314
14.3.2. FTP invitado	320
14.4. El servicio TELNET	323
14.5. El servicio SMTP	326
14.6. Servidores WWW	328
14.7. Los servicios r-*	330
14.8. XWindow	333
14.8.1. Autenticación por máquina	333
14.8.2. Autenticación por testigo	335
15. Cortafuegos: Conceptos teóricos	337
15.1. Introducción	337
15.2. Características de diseño	340
15.3. Componentes de un cortafuegos	342
15.3.1. Filtrado de paquetes	342
15.3.2. Proxy de aplicación	344
15.3.3. Monitorización de la actividad	345
15.4. Arquitecturas de cortafuegos	346
15.4.1. Cortafuegos de filtrado de paquetes	346
15.4.2. Dual-Homed Host	347
15.4.3. Screened Host	347
15.4.4. Screened Subnet (DMZ)	349
15.4.5. Otras arquitecturas	351
16. Cortafuegos: Casos de estudio	353
16.1. <i>Firewall-1</i>	353
16.1.1. Introducción	353
16.1.2. Arquitectura	354
16.1.3. Instalación	355
16.1.4. Gestión	357
16.1.5. El sistema de <i>log</i>	359
16.1.6. INSPECT	362
16.2. <i>ipfwadm/ipchains/iptables</i>	362
16.2.1. Introducción	362
16.2.2. Arquitectura	364
16.2.3. Gestión	365
16.2.4. El sistema de <i>log</i>	367
16.3. <i>IPFilter</i>	369
16.3.1. Introducción	369
16.3.2. Instalación	369
16.3.3. Gestión	371
16.3.4. El sistema de <i>log</i>	373
16.4. PIX Firewall	374
16.4.1. Introducción	375

16.4.2. La primera sesión con PIX <i>Firewall</i>	376
16.4.3. Interfaces de red	378
16.4.4. Accesos entre interfaces	379
16.4.5. Listas de control de acceso	380
16.4.6. Rutado	381
16.4.7. Otras órdenes útiles	382
16.4.8. El sistema de <i>log</i> remoto	387
16.4.9. <i>Failover</i>	388
17. Ataques remotos	391
17.1. Escaneos de puertos	391
17.2. <i>Spoofing</i>	395
17.3. Negaciones de servicio	397
17.4. Interceptación	400
17.5. Ataques a aplicaciones	402
17.5.1. Correo electrónico	402
17.5.2. Ataques vía <i>web</i>	410
18. Sistemas de detección de intrusos	413
18.1. Introducción	413
18.2. Clasificación de los IDSes	414
18.3. Requisitos de un IDS	417
18.4. IDSes basados en máquina	418
18.5. IDSes basados en red	421
18.6. Detección de anomalías	425
18.7. Detección de usos indebidos	427
18.8. Implementación real de un IDS	431
18.8.1. IDS en el cortafuegos	432
18.8.2. IDS en la red: SNORT	434
18.8.3. IDS en la máquina	440
18.8.4. Estrategias de respuesta	444
18.8.5. Ampliación del esquema	447
18.9. Algunas reflexiones	449
19. Kerberos	451
19.1. Introducción	451
19.2. Arquitectura de Kerberos	452
19.3. Autenticación	453
19.3.1. Login	453
19.3.2. Obtención de <i>tickets</i>	454
19.3.3. Petición de servicio	454
19.4. Problemas de Kerberos	455

V	Otros aspectos de la seguridad	457
20.	Criptología	459
20.1.	Introducción	459
20.2.	Criptosistemas	460
20.3.	Clasificación de los criptosistemas	462
20.3.1.	Criptosistemas de clave secreta	462
20.3.2.	Criptosistemas de clave pública	463
20.4.	Criptoanálisis	464
20.5.	Criptografía clásica	465
20.5.1.	El sistema Caesar	465
20.5.2.	El criptosistema de Vigènere	466
20.6.	Un criptosistema de clave secreta: DES	468
20.7.	Criptosistemas de clave pública	470
20.7.1.	El criptosistema RSA	470
20.7.2.	El criptosistema de ElGamal	471
20.7.3.	Criptosistema de McEliece	472
20.8.	Funciones resumen	473
20.9.	Esteganografía	474
21.	Algunas herramientas de seguridad	477
21.1.	Introducción	477
21.2.	Titan	478
21.3.	TCP Wrappers	492
21.4.	SSH	494
21.5.	Tripwire	498
21.6.	Nessus	500
21.7.	Crack	502
22.	Gestión de la seguridad	507
22.1.	Introducción	507
22.2.	Políticas de seguridad	509
22.3.	Análisis de riesgos	511
22.3.1.	Identificación de recursos	513
22.3.2.	Identificación de amenazas	513
22.3.3.	Medidas de protección	515
22.4.	Estrategias de respuesta	516
22.5.	<i>Outsourcing</i>	518
22.6.	El ‘Área de Seguridad’	521
VI	Apéndices	523
A.	Seguridad básica para administradores	525
A.1.	Introducción	525
A.2.	Prevención	526
A.3.	Detección	532

A.4. Recuperación	536
A.5. Recomendaciones de seguridad para los usuarios	538
A.6. Referencias rápidas	540
A.6.1. Prevención	540
A.6.2. Detección	540
A.6.3. Recuperación	541
A.6.4. Usuarios	541
B. Normativa	543
B.1. Nuevo Código Penal	543
B.2. Reglamento de Seguridad de la LORTAD	547
B.3. Ley Orgánica de Protección de Datos	555
C. Recursos de interés en INet	585
C.1. Publicaciones periódicas	585
C.2. Organizaciones	587
C.2.1. Profesionales	587
C.2.2. Gubernamentales/militares	587
C.2.3. Universidades/educación	588
C.3. Criptografía	590
C.4. Seguridad general	591
C.5. Compañías y grupos de desarrollo	592
C.5.1. Unix	592
C.5.2. General	593
C.6. Sitios <i>underground</i>	594
C.6.1. Grupos	594
C.6.2. <i>Exploits</i> y vulnerabilidades	594
C.7. Recursos en España	594
C.8. Listas de correo	595
C.9. Grupos de noticias	597
C.9.1. Criptología	597
C.9.2. Unix	598
C.9.3. Redes	598
C.9.4. Misc	599
D. Glosario de términos anglosajones	601
Conclusiones	605
Bibliografía	609
GNU Free Documentation License	631
D.1. Applicability and Definitions	631
D.2. Verbatim Copying	632
D.3. Copying in Quantity	633
D.4. Modifications	633
D.5. Combining Documents	635

D.6. Collections of Documents	636
D.7. Aggregation With Independent Works	636
D.8. Translation	636
D.9. Termination	636
D.10.Future Revisions of This License	637

Índice de figuras

1.1. Flujo normal de información entre emisor y receptor y posibles amenazas: (a) interrupción, (b) interceptación, (c) modificación y (d) fabricación.	6
1.2. Visión global de la seguridad informática.	15
3.1. El resultado de un basureo involuntario.	52
4.1. Permisos de un fichero	66
8.1. Estructura genérica de una <i>smartcard</i>	156
8.2. Huella dactilar con sus minucias extraídas.	162
8.3. Iris humano con la extracción de su <i>iriscodes</i>	165
8.4. Geometría de una mano con ciertos parámetros extraídos.	166
8.5. La herramienta de administración <i>admintool</i> (Solaris), con opciones para envejecimiento de claves.	179
11.1. Estructura jerárquica del SRC.	237
11.2. Interfaz de <i>fixdist</i> (AIX).	257
15.1. (a) Aislamiento. (b) Conexión total. (c) <i>Firewall</i> entre la zona de riesgo y el perímetro de seguridad.	338
15.2. Arquitectura DMZ.	350
16.1. Ubicación del <i>Inspection Module</i> dentro de la pila de protocolos OSI.	354
16.2. Una imagen de <i>fwlv</i>	360
18.1. Puntos clásicos de defensa entre un atacante y un objetivo.	431
18.2. Situación del sensor	440
19.1. Protocolo de autenticación <i>Kerberos</i>	455
20.1. Estructura de un criptosistema	461
21.1. Interfaz gráfico de <i>Nessus</i>	503

Índice de cuadros

4.1. Atributos de los archivos en <i>ext2fs</i>	74
7.1. Comparación de diferentes medios de almacenamiento secundario.	139
7.2. Opciones de la orden dump	140
7.3. Opciones de la orden restore	142
7.4. Opciones de la orden tar	144
7.5. Opciones de la orden cpio	146
8.1. Comparación de métodos biométricos.	158
8.2. Códigos de caracteres para el envejecimiento de contraseñas.	173
12.1. Privilegios de grupo en HP-UX	269
18.1. Algunos puertos a monitorizar en un <i>firewall</i>	433
19.1. Abreviaturas utilizadas.	453
20.1. Tableau Vigènere	467

