CONTENIDO

CONTENIDO ..... **VII**

PRÓLOGO ..... **XIII**

CAPÍTULO 1. INTRODUCCIÓN **1**

1. MOTIVACIÓN DEL LIBRO 1
2. AUDIENCIA DEL LIBRO 2
3. CONTENIDO DEL LIBRO 2
4. EVOLUCIÓN DE LA SEGURIDAD EN UNIX 3
5. LIBRO NARANJA 4
6. AGRADECIMIENTOS 5

CAPÍTULO 2. CONCEPTOS SOBRE UNIX RELATIVOS A LA SEGURIDAD **7**

1. ARQUITECTURA DE UNIX 7
2. CUENTAS DE USUARIO 9
3. TIPOS DE FICHEROS 12
   3.1. Ficheros planos *12*
   3.2. Ficheros directorios *13*
   3.3. Ficheros especiales *13*
4. SISTEMA DE FICHEROS 14
5. PERMISOS DE LOS FICHEROS 17
   5.1. Modo de un fichero *17*
   5.2. Modo por defecto de un fichero *18*
   5.3. Comandos para la manipulación del modo de un fichero *18*
   5.4. Protección de la información *21*
6. COMANDOS 23
7. EJECUTABLE BINARIO, IMAGEN Y PROCESO 25
   7.1. Ejecutable binario *25*
   7.2. Imagen *26*
   7.3. Proceso *27*

CAPÍTULO 3. MECANISMOS DE SEGURIDAD 31

1. CRIPTOGRAFÍA 31
2. CRIPTOSISTEMAS 32
3. TIPOS DE CRIPTOSISTEMAS 34
4. ATAQUES 35
5. CRIPTOSISTEMAS DE CLAVE SECRETA 36
   5.1. Cifrado DES *37*
   5.2. IDEA *38*
6. CRIPTOSISTEMAS DE CLAVE PÚBLICA 40
   6.1. Cifrado RSA *41*
7. FIRMA DIGITAL 43
   7.1. PGP *44*
8. CRIPTOSISTEMAS IRREVERSIBLES 45
9. TÉCNICAS CRIPTOGRÁFICAS BÁSICAS 48
   9.1. Métodos de sustitución y de permutación *48*
   9.2. Confusión y difusión *52*
   9.3. Cifrado producto *52*
   9.4. Cifradores de flujo y cifradores de bloque *53*

CAPÍTULO 4. LIBRO NARANJA 55

1. CONCEPTOS SOBRE SEGURIDAD 55
2. REQUISITOS PARA UNA POLÍTICA DE SEGURIDAD 58
   2.1. Control de accesos discrecional *59*
   2.2. Reutilización de objetos *59*
   2.3. Etiquetas *60*
3. REQUISITOS DE RESPONSABILIDAD 61
   3.1. Identificación y autenticación *62*
   3.2. Vía fiable *62*
   3.3. Auditoría *62*
4. REQUISITOS DE CONFIABILIDAD 64
   4.1. Confiabilidad operacional *64*
   4.2. Confiabilidad del ciclo de vida *66*
5. REQUISITOS DE DOCUMENTACIÓN 68
6. CARACTERÍSTICAS DE LAS CLASES 69
   6.1. D: seguridad mínima *70*
   6.2. C1: protección mediante seguridad discrecional *70*
   6.3. C2: protección mediante accesos controlados *71*
   6.4. B1: protección mediante seguridad etiquetada *71*
   6.5. B2: protección estructurada *72*
   6.6. B3: dominios de seguridad *73*
   6.7. A1: diseño verificado *73*

CAPÍTULO 5. PRÁCTICAS DE SEGURIDAD PARA LOS USUARIOS DE SISTEMAS SEGUROS 75

1. USO DE UN SISTEMA C2 76
2. CONEXIÓN 76
2. USO DE COMANDOS MEDIANTE PRIVILEGIOS 79
3. UTILIZACIÓN DE DOMINIOS PROTEGIDOS 80
4. AUDITORÍA 81
5. CIFRADO DE LA INFORMACIÓN 82
6. RECOMENDACIONES PARA EL MANTENIMIENTO SEGURO DE UNA CUENTA 83
   6.1. Conexión y desconexión 83
   6.2. Seguridad de la contraseña 84
   6.3. Seguridad de los ficheros 85
   6.4. Ejecución de programas 86

CAPÍTULO 6. MANTENIMIENTO DE SISTEMAS SEGUROS 87

1. DIFERENCIAS ENTRE SISTEMAS SEGUROS E INSEGUROS 88
   1.1. Base segura de cómputo 88
   1.2. Identificación y autenticación 89
   1.3. Responsabilidad 89
   1.4. Control de accesos discrecional 90
   1.5. Privilegios 90
   1.6. Auditoría 91
   1.7. Subsistemas protegidos 91
2. FUNCIONAMIENTO DE UN SISTEMA SEGURO 92
   2.1. Asignación de las funciones administrativas 92
   2.2. Asignación de los privilegios de núcleo 93
   2.3. Control de accesos al sistema 94
   2.4. Restricciones sobre las contraseñas 94
   2.5. Restricciones sobre el uso de los terminales 97
   2.6. Restricciones de conexión 98
3. PROTECCIÓN DE DATOS 100
   3.1. Eliminación de los permisos SUID, SGID y "sticky" en las escrituras 100
   3.2. Importación de datos 101
4. DETECCIÓN DE INTRUSIONES EN EL SISTEMA 102
   4.1. Contraseñas hurtadas 103
   4.2. Acceso no supervisado al equipo físico 103
5. TRATAMIENTO DE SISTEMAS DE FICHEROS CORRUPTOS 104
   5.1. Ficheros de la base de datos de autenticación 104
   5.2. Comprobación del sistema tras una caída 105
   5.3. Uso del terminal de prevalecimiento 107
6. AUDITORÍA 107
   6.1. Componentes del subsistema de auditoría 108

6.2. Método de auditoría ... *112*
6.4. Informes de auditoría ... *119*
7. RECOMENDACIONES PARA EL MANTENIMIENTO SEGURO DE UN SISTEMA ... 130
7.1. Mantenimiento seguro de las cuentas administrativas ... *130*
7.2. Mantenimiento seguro del sistema ... *131*

CAPÍTULO 7. PROGRAMACIÓN DE APLICACIONES SEGURAS EN LENGUAJE C ... 135

1. FICHEROS CABECERA ... 136
2. LLAMADAS AL SISTEMA OPERATIVO ... 137
2.1. Identificación del usuario durante la conexión ... *137*
2.2. Identificadores de proceso al comienzo de su ejecución ... *141*
2.3. Privilegios de los procesos ... *148*
2.4. Parada de las operaciones de entrada/salida sobre un fichero ... *158*
3. FUNCIONES DE BIBLIOTECA ... 161
3.1. Contraseñas ... *161*
3.2. Manipulación de sesiones de auditoría ... *167*
4. RECOMENDACIONES PARA UNA PROGRAMACIÓN SEGURA ... 171

CAPÍTULO 8. INSTITUCIONES Y DOCUMENTOS SOBRE LA SEGURIDAD DE UNIX EN INTERNET ... 173

1. COMPUTER EMERGENCY RESPONSE TEAM (CERT) ... 174
2. OTROS FOROS TELEMÁTICOS DE INTERÉS ... 178
3. PREGUNTAS FRECUENTES SOBRE SEGURIDAD ... 179
3.1. ¿Cuál es la diferencia entre un "hacker" y un "cracker"? ... *179*
3.2. Seguridad y secretismo ... *180*
3.3. ¿Cuáles son las herramientas que ayudan a la seguridad? ... *183*
3.4. ¿No es peligroso proporcionar herramientas averiguadoras a cualquiera? ... *185*
3.5. ¿Dónde se pueden conseguir? ... *185*
3.6. ¿Cómo se consigue entrar en los sistemas? ... *186*
3.7. ¿Con quién se debe contactar si alguien ha entrado ya? ... *187*
3.8. ¿Qué es un cortafuegos? ... *187*
3.9. ¿Por qué no se debe utilizar procedimientos de comandos con el bit s a nivel de dueño? ... *188*
3.10. ¿Por qué no se debe dejar la cuenta root permanentemente conectada en la consola? ... *189*
3.11. ¿Por qué no se deben crear cuentas UNIX con palabras nulas? ... *189*
3.12. ¿Cuáles son los agujeros de la seguridad relacionados con X-Window (y con otros sistemas de ventanas)? ... *190*
3.13. ¿Cuáles son los agujeros en la seguridad debidos al NFS? ... *191*
3.14. ¿Cómo se puede generar contraseñas seguras? ... *193*
3.15. ¿Por qué son tan importantes las contraseñas? ... *194*
3.16. ¿Cuántas contraseñas posibles hay? ... *194*

3.17. ¿Hasta dónde se puede llegar a ser estúpido? *195*

CAPÍTULO 9. SEGURIDAD FUTURA **197**

1. NOVELL/USL UNIX SVR4 ENHANCED SECURITY 197
1.1. Privilegio mínimo *197*
1.2. Utilidad para la administración de la seguridad *199*
1.3. Control de accesos obligatorio *200*
1.4. Aislamiento de accesos *202*
1.5. Control de accesos discrecional *203*
1.6. Vía fiable *205*
2. KERBEROS: SEGURIDAD EN SISTEMAS DISTRIBUIDOS 206
2.1. Definición *206*
2.2. Funcionamiento *207*
2.3. Componentes software *207*
2.4. Credenciales *208*
2.5. Obtención del pase inicial *209*
2.6. Solicitud de un servicio *210*
2.7. Obtención de pases para servidores *211*

BIBLIOGRAFÍA **213**