Index

A

absolute pathnames, reading tapes, 71
access control violations, 150
accounting
  process, 157
  system, 157
administration, system
  documentation, xvii-xviii
archiving audit data, 154
audit
  a file, 146, 152
  a label, 146
  a user, 145, 152
  customizing, 135
  data archiving, 154
  data removing, 154
  event types, 137
  guidelines, 153
  improper use, 153
  particularly interesting users, 152
  sample record, 147
  sat_select, 137
  system data files modification, 153
  system programs modification, 153
  the audit trail, 154
audit data
  interpreting, 147
  understanding, 147
auditing
  cofiguration utilities, 135
  customizing, 135
  default environment, 134
  enabling, 134
  list of items to audit, 137
  reading output, 147
  recovery, 143
  saved files, 143
  saving, 143
auditing, description, 133
auditing, *satconfig* utility, 141

B

Backup, 24
  about, 4
backup and restore
  using *xfsdump* and *xfsrestore*, 30-62
Backup and Restore window, 13
backups
  about, 3
  across a network, 8
  automatic, 9
  available programs, 4-5
  by date, 20
  byte swapping, 70
  compressed with *bru*, 20
  dd conversion options, 70
  error messages, 74
  errors, 71
  estimate space with *bru*, 19, 24
  how often, 6
  incremental, 7

incremental with *bru*, 21
incremental with *cpio*, 63, 66
incremental with *dump*, 27
incremental with *tar*, 63, 66
listing contents with *bru*, 21
making, 12
restored wrong one, 72
root filesystem, 6
storing, 9
strategies for, 6
unreadable, 69
user filesystems, 7
verifying *bru* archives, 22
bru
about, 4
making backups, 20
restoring data, 23
restoring files, 23

C

changing passwords, 92
cpio
about, 4
capabilities, 65
making backups, 65
restoring files, 64, 67
cumulative restores, *xfsrestore*, 57
customizing auditing, 135

D

data segments, *xfsdump*, 32
dbedit utility, 153
dd
about, 4
capabilities, 67
conversion options, 70
default backup device
changing, 18
/dev/tape, 12
disabling IP packet forwarding, 120
disabling NFS, 125
disabling NIS, 124
DNS configuration of internal network, 127
dual-homed host
hardware setup, 117
software setup, 120
dump
about, 4
/etc/dumpdates, 27
incremental backups, 27
making backups, 27
vs. *xfsdump*, 30
dump inventory, *xfsdump*, 32
dump session, *xfsdump*, 32
dump stream, *xfsdump*, 32

E

educating users about security, 126
error messages, backup and recovery, 74
/etc/dumpdates, 27
/etc/hosts.equiv file, 108
/etc/inetd.conf file, 111
/etc/passwd file, 108

F

file audit, 146
firewall
definition, 113
design philosophy, 114
hardware configuration, 115-119

software configuration, 119-129
firewalls, 111-129
forwarding IP packets, 120
FTP services, 121

H

hardware configuration
firewall, 115-119
routers, 116
host
dual-homed, 117
screened, 117
housekeeping directory, 61

I

incremental dumps, *xfsdump*, 45
inetd daemon, 111
inetd services
limiting, 121
insider security violation, 150
interactive restore, *xfsrestore*, 55
internal network configuration, 127
Internet, definition, 112
interrupted restores, *xfsrestore*, 60
inventory, *xfsdump*, 32, 47
IP packet forwarding, 120
IRIX administration
documentation, xvii-xviii

L

label audit, 146
locking logins, 92
log files, 125
login
disable time, 98
locking, 92, 94
maximum attempts, 97
options, 95
recording, 98
restricting root, 96
special accounts, 93

M

mail
configuration of internal network, 127
spool isolation, 128
media
layout, *xfsdump*, 32
object, *xfsdump*, 32
storing, 9
modification of system data files, 153
modifications of system programs, 153

N

ncheck command, 100
network
access control, 108
backups, 8
screened, 118
security issues, 112
NFS
limiting or disabling, 125
NIS
disabling, 124

O

operating the system
  general, 157
orphanage directory, 61
outside connections, 150
outsider security violation, 148

P

password
  aging, 90-92
  changing, 92
  checking, 93
  choosing, 84
  dialup, 87
  forcing, 98
  PROM, 85
  protection, 123
password PROM, 85
passwords
  administration, 84
potential security violations, 148
process accounting, 157
PROM passwords
  clearing, 86
  setting, 86
  use of, 85
proxy servers, 128
pwck command, 93

R

Recover System, 13
recovery
  after system corruption, 13
  error messages, 74
removing
  audit data, 154
Restore
  about, 4
  restoring data, 25
restore
  about, 4
  interactive mode, 28
  restoring filesystems, 28
  restoring individual files, 28
  vs. *xfsrestore*, 30
restoring data
  bru, 23
  cpio, 64, 67
  Restore, 25
  restore, 28
  tar, 64, 67
restoring interrupted dumps, *xfsrestore*, 58
.rhosts file, 108
root privilege violation, 151
routers and firewalls, 116
RPC services
  limiting, 124

S

SAT
  customizing, 135
  event types, 137
  sample record, 147
  sat_select, 137
  understanding data, 147
sat_interpret utility, 147
sat_reduce utility, 147
sat_select, 137
sat_select utility, 142
sat_summarize utility, 147
satconfig utility, 141

screened host
  hardware setup, 117
screened network
  hardware setup, 118
security
  guidelines, 81
  IRIX standard, 80
  LAN, 107
  network, 107
  process accounting, 157
  tightening for firewall, 120
  Trojan horse attack, 82
  xhost command, 109
security violation
  insider, 150
security violation (auditing)
  access control, 150
  outside connections, 150
  outsider, 148
  potential, 148
  root privilege, 151
  unauthorized entry, 148
  unusual system usage, 149
sendmail
  configuration, 127
Set-GID, 100
Set-UID, 100
software
  checking integrity, 125
stream terminator, *xfsdump*, 32
system access, 92
system accounting, 157
system administration
  documentation, xvii-xviii
system backups, 13
system data files
  modification, 153
System Maintenance Menu, 13
system passwords
  password
    system, 85
system recovery, 13

T

tape device, default, 12
tapes
  reusing, 10
  storing, 9
  testing, 73
tapes, absolute pathnames, 71
tapes, reusing with *xfsdump*, 44
tar
  about, 4
  capabilities, 62
  comparison key characters, 64
  making backups, 63
  restoring files, 64, 67
terminator, *xfsdump*, 32
Trojan horse attack, 82

U

unauthorized entry, 148
understanding the audit data, 147
unusual system usage, 149
user accounts
  forcing a password, 98
user audit, 145
users and security, 126

V

violations
  of access control security, 150
  of root privilege security, 151
  of security by insiders, 150
  of security by outsiders, 148
  of security by unauthorized entry, 148
  of security by unusual system usage, 149
  possible, 148
  through outside connections, 150

W

World Wide Web
  and security, 115

X

xfsdump
  dump inventory, 47
  incremental dumps, 45
  media layout, 32
  network usage, 62
  resumed dumps, 45
  reusing media, 44
  specifying media, 40
  STDOUT, 62
  using, 40
xfsrestore
  cumulative restores, 57
  interactive restore, 55
  interrupted restores, 60
  network usage, 55, 62
  restoring files, 54
  restoring interrupted dumps, 58
  session ID, 52
  session label, 52
  simple restores, 52
  STDIN, 62
  using, 50
xhost command, 109
X server access
  changing, 109
  checking, 110
  controlling, 109
  default, 109