Index

Symbols

2000 Love Letter 16
8-node 80
802.11a 337

A

Abel 14
access control list (ACL) 48
access control system 47, 328
access denied 147
Access Devices Regulation Act of 1998 138
access management tool 233
AccessData 78
accountability 272
acquisition and implementation 252
active monitoring 144, 147
active parsing 147
active scanning 5
ActiveX security 224
ad-ware 336
admissibility 111
Adobe Photoshop 338
adware 17, 218
agent system 156
agent-based application 165
AirSnort 323
alert 140, 146
algorithmic scanning 46
alias 160
American Registry for Internet Numbers (ARIN) 5
archive 313
ARP message 317
arranged marriage 270
ASaP 12
ASCII 103
Asia Pacific Network Information Center (APNIC) 5
ASKARI project 155, 162
association rule mining 161
attachments 337
authentication 147, 233
authentication failure 147
authenticity 111
authorization 233
automated image analysis 86
availability 272

B

Back Orifice 2000 17

backtracing 116
Bayesian network 165
behaviour blocking 47
belief updating 166
Berkeley Packet Filter (BPF) 69
Bernstein v. US Dept. of Justice 280
BIOS set-up 274
bitstream 67
black list 240
black-box testing (BBT) 95
BlackIce 56
blackmail 217, 270
Blaster 33, 48
blog 38
Bluepipe architecture 81
Bonn Ministerial Declaration 277
botnet 33
BPF 69
browse 336
BSD 68
budgeting 313, 330
business continuity plan 328
ByteBack 62
byteprints 61

C

C-DCOs 252, 256
Cain and Abel 14
CARDS 140
caveat 327
CD ROM 335
CD 234
certification 316, 327
certified forensic specialist 222
chain of custody 320
chat room 270
checkpoint 224
CheckProbe 147
Cheops 8
chernobyl virus 41
child exploitation 270
choke 38
CIA paradigm 121
Cisco Systems 222
CISSP 327
civil service 315
clustering 160
CNF 313, 318
COBIT 245, 251
COBIT control objective (C-CO) 252
COBIT detailed control objective (C-DCO) 252
code emulation 46
code walkthrough 94
command line interface 322
common gateway interface (CGI) 12
common intrusion detection framework (CIDF) 140
common intrusion specification language (CISL) 140
complex scanning 45
computer crime 138
computer forensic investigative toolkit (CFIT) 56
computer forensics tool testing 93
computer intrusion squad 138
computer literacy 322
Computer Security Institute (CSI) 138
computer/network forensics (CNF) 313
concept space 160
concept space for intelligence analysis (COPLINK) 160
confidentiality 244, 272
connection failure 147
content filtering 228
content-based image retrieval (CBIR) 86
corporate electronic resources 244
corporate governance 243
corporate preparedness 217
county government 220
cover-up 20
covert channels 22
crack 14, 320, 323
cracking 270
credibility 111
credit monitoring 229
Crick 28
crime technology programme 157
criminal communication 176
criminology viewpoint 268
cross-industry standard process for data mining 162

cryptanalysis 181
cryptcat 112, 120
cryptographic technique 280
cryptography 177, 328
CSI 29, 138
cyber crime 267, 268
cyber lead 316
cyber-pimping 270
cyber-slacking 270, 296
cyberforensics 315
CyberKit 8
cyberloafing 296
cyberslouching 296
cyberterrorism 32
cyberworld 55

D

daemon 109
Danchev 222
data collection 223, 227
data communication 322
data mining 155
data packets 223
data reduction 108
data structure 322
database fundamentals 322
Daubert decision 91, 100
Dawkins 28
De Montfort University 292
decentralized site management 228
decryption algorithm 18
defamation 270
Defence Advanced Research Project Agency (DARPA) 157
delivery and support (DS) 252
DELV 79
demilitarized zone (DMZ) 221
denial of service (DOS) 12, 19, 220, 316
Department of Homeland Security 278
DF-DCOs 256
digital crime 217
digital evidence 107
digital forensic 79, 91, 107, 217, 243, 267
digital forensics control objective (DF-CO) 254
digital forensics repository (DFR) 89
digital rights management 139
digital steganographic system 177
digital storage media 334
digital watermarking 177
digitized sounds 338
disinfection 45
distributed computing 79
distributed denial of service (DDoS) 33, 128
DMZ 149, 231, 238
documentation 223
domain name system (DNS) 5, 122, 127, 339
drilling down 160
drive image 62
dsniff 13
DSTO 57
dtSearch 64

E

e*Trade 20
E-Donkey 233
e-mail forwarding service 228
E-SIGN bill 283
eavesdropping 324
eBanking 281
eBay 20
echo reply 6
echo request 6
e-commerce 281
edge network 236
EEDI 56, 77
eEye 12
Electronic Communication Privacy Act of 1986 139
electronic evidence 272
electronic payment 176
Electronic Privacy Information Center (EPIC) 139
electronic signature 283
Elk Cloner 35
e-mail 38
Encase 56, 222, 324
encryption 320, 323

end-to-end digital investigation (EEDI) 56
ENISA 277
entity extraction 160
espionage 270
ethereal 114, 119
ethics 298
European Directive 02/58/EC 282
European Network and Information Security Agency 277
European Parliament and Council Directive 282
European Union (EU) 139, 157, 267
event monitoring 139
evidence 335
Evol worm 42
exploit 14
extortion 217

F

F-Secure 42
fake employment 270
false identification 270
false negative 100
false positive 100
Farmer 65
FAT 1 103
FAT 32 103
FAT12 96
filtering 108
final-record message 113
findkey 65
firewall 20, 49, 144, 223, 237
First Amendment 280
FLOCK proxy 145
flooding attack 20
floppies 234
floppy disks 335
forensic computing 292
forensic profile 139, 141, 148
forensic readiness 255
forensic science 176
forensic specialist 314
forensic toolkit (FTK) 62, 78
forensics 272
ForensiX 57
forgery 276
forwarding service 228
fraud 176, 271
fraudster 271
free flow 282
FTK 325

G

gaining access 12
gambling 176, 271
Gaobot worm 42
Gartner Group 221
general public license (GPL) 118
generic decryptor 47
GetLog Probe 147
gigabyte 75
global information assurance certification (GIAC) 328
global reach 272
global terrorism 156
global variable 122
GNU http-tunnel 127
government espionage 271
GPS 334
Gramm-Leach-Bliley Act 223, 279
graphical interface (GUI) programming 322
graphical user interfaces 322
grave-robber 65
guidance software 222, 324

H

hacking 101, 176, 218, 323
hacktivist 271
harassment 176
hardware failure 29
hardware vendor 223
hash dictionary 83
hate crime 270
Health Insurance Portability and Accountability Act 228, 279, 283
healthcare company 220
heuristic analysis 46
hidden data 320
HIPAA 221, 223
Homeland Security Act 278

homogeneous subgroup 160
honey pot 225
host 144
HotMail 232
hotspot 235
HP-UX 68
HTCIA 326, 330
human scalability 77
hyper-terminal 6
hypertext transfer protocol (HTTP) 122

I

IACIS 107
ideal security 232, 236
identification 45
identity theft 217, 270
ifconfig 22
iLook 62, 325
image clustering 87
implanted tool 118
iNetTools 8
info wars 271
information and communication technologies (ICT) 268
information extraction (IE) 160
information security 243, 246
information technology governance 243
information terrorism 226
initial sequence number method 125
input-process-output (IPO) 316
instant message (IM) 38, 69, 233
integrity 108, 244, 272
integrity checking. 47
intellectual property 176, 270
internal hacking 220
International Organization on Computer Evidence 71
Internet control message protocol (ICMP) 6, 122, 225
Internet Explorer 336
Internet security glossary 139
Internet service provider (ISP) 56, 337
InterNIC 5
interrupt process utilization 223
intrusion detection system (IDS) 20, 66, 117, 139, 144, 148, 225, 237
investigator 328
IOCE 71
IP Traceback 66
IRItaly (Incident Response Italy) 118
ISP 56, 337

J

Java 224
John the Ripper 14, 323
Juggernaut 13
junk mail 19
just-in-time validation 95, 102

K

Kaaza 228, 233
keyword 147, 160
Kiwi 111
Klez worm 33
knowledge 328
known-carrier attack 182
known-message attack 182
known-steganography attack 182
KSA 312, 328

L

LanCope 239
LAN 109
law enforcement 315
lazarus 65
legal framework 267
LexisNexis 218
liability 229
LibPcap 114
Lincrack 14
link capture 270
Linux 56, 68
Litan 221
live digital forensics 81
localize pairs 192, 195
log file 108
log machine 109
log parsers 117
log rotation 109
long-term collaboration support 88

Love Bug virus 138
Loveletter worm 16, 32

M

MAC 317
machine scalability 77
mactime 65
magnetic force microscopy (MFM) 60
malicious code 220
malicious software 27, 218
malicious toolbar 223
malicious Web site 223
malware 27, 218
McAfee 12, 42
MD5 60
MessageLabs 30
metadata 338
metamorphism 42
MFP 85
micromuse 69
Microsoft 224
Millennium Digital Commerce Act 283
MIRADOR 140
mitigation techniques 47
mobile forensic platform 85
modelling stage 164
modifying drives 274
money laundering 271
morality 298
motivation 31, 225, 271
motivation for malice 31
multi-jurisdictional nature 272
multi-user tools 88
Mydoom worm 32

N

Napster 228
National Counterintelligence Executive 219
National High Tech Crime Unit 296
National Institute for Standards and Technology 93, 283
National Institute of Justice 70
national security 217
National Software Reference Library (NSRL) 70
National Strategy to Secure Cyberspace 220
natural language processing (NLP) 160
Nessus 12
NetAnalysis 68
Netcat 120
NetCool 69
NetDetector 2005 69
Netegrity's eTrust Identity 233
NetScanTools Pro 8
NetSky 32
network address translation (NAT) 125
network cloaking 240
network filters 225
network security 218
network-level techniques 48
network time protocol (NTP) 113
networking 322
neural network 46, 160
New Mexico Mounted Patrol 239
NIDS 122
Niksun 69
Nimda-D virus 228
NIST 93, 283
Nixon 338
Nmap 9
normalization 108
Northwest Performance Software 8
Norton 338
Norton Ghost 56
noun phrase 160
NSRL 70
NSTX 128
NTA 62
NTFS 95, 103
Nutcracker 14
NYPD detectives 321

O

OECD 276, 280
off-the-shelf (OTS) 322
on-the-spot digital forensics 81
OnLine Digital Forensic Suite 85
open network provision (ONP) 281
operating system hardware/software lockdown 225, 322

operations security 328
organized crime 156
outage 223
overwriting 337
OzyManDNS 128

P

packet dump 223
paedophile network 271
paging file 337
PalmCrack 14
parser 117
passive profile 143
passive state 147
password 14, 234
Patriot Act 278
patterns 157
payload 27, 37
Pcap 69
pedophilia 176
peer-to-peer (P2P) network 38
Perl 117
phone tag 6
PhoneSweep 6
Photoshop 338
physical security 328
PING 6, 225
piracy 270
PKI 114
plagiaris 270
planned response 222, 226
planning and organization (PO) 252
political aim 271
polymorphism 42
pornography 176, 228, 270
port scanning 7
pre-processing 162
preservation 37
prevention 43
privacy 139, 280
privacy enhancing technologies (PET) 139, 280
probe 144
Procomm Plus 6
proof 335
propagation 27, 37
prostitution 270
public hotspot 235
public interest 271
public order 271
Python 117

Q

Qint 38

R

RainbowCrack 14
Rasusers 6
real-time collaboration support 88
reference data set (RDS) 71
registry change 224
regulatory legislation 221
remote acces 223, 235
remote access server 223
remote access Trojan (RAT) 17
remote computing 235
remote procedure call (RPC) 127
removable media 234
reporting 223
Réseaux IP Euoropéens Network Coordination Centre 5
retina network security scanner 12
return on investment (ROI) 312
RFC 3164 109
risk analysis 233
robot network (botnet) 33
rootkit 21, 118, 227
router 144, 225
RPC 127
RTL 103

S

safeback 56, 62
SAINT 12
San Francisco Federal Bureau of Investigation 138
sand-boxing 47
sandtrap 6
SANS Institute 325
SANS training course 323
security auditor's research assistant

(SARA) 12
Sarbanes-Oxley 221, 223, 279
SATAN 12
scanning 45
scanning tunneling microscopy (STM) 60
school district 220
Scientific Working Group for Digital Evidence 96
script kiddies 218
SecSyslog 121
secure 137
secure copy (SCP) 112
secure shell (SSH) 127
secure socket layer (SSL) 281
SecureWave 224
security 42, 139, 220, 328, 336
security architecture 328
security breach 220
security consultant 222
security flaw 336
security incident 139
security management practice 328
security policy 222, 235
security solution 222
security topology 236
self organizing map (SOM) 160
self-preservation 41
semantic tagging 164
session hijacking 13
sexual exploitation 270
SHA 60
SHA256 63
Sharereactor 233
Shimonski 232
signature analyzer 144
simple scanning 45
site cloning 270
situational awareness 318
Skrenta 35
Slammer worm 39, 48
Sleuthkit 56
SMART 325
Smurf 20
SnapBack 62
sniffer 109
sniffing 13
Sniffit 13
snooping 336
snort 56, 69, 119
Sobig 48
social engineering 16, 218
software validation 92
software verification 92
Solaris 68
Sophos 42
spam 19, 170, 218, 220, 337
Spernow 225
spoofing 316
Spyware 17, 218, 336
Stacheldraht 20
stack-based buffer overflow attack 15
staffing 315
stealth technique 41
StealthWatch 239
steganography 80, 177, 320
steganography-only attack 181
stego sensitivity measure 208
storage channel 121
storage media 334
streaming media analysis 87
Strihavka 32
structured 158
Sub7 17
subnet proxy 144
substantive law 299
SunOS 68
suspicious entries 147
suspicious network activity 141
swap 337
SWATCH 119, 139
symantec 42, 224
symmetric multi-processor (SMP) 79
Syslog 109
system agent 109
systems development 328

T

tapes 234
TASK/autopsy 119
TCP/IP steganography 122
TCPDump 119

TcpDump 13, 56, 68, 114
teardrop attack 225
technology theft 217
telecommunications 328
Tequila virus 42
terabytes 75
terrorism 271
text mining 155, 157
TFN 20
TFN2K 20
THC scan 6
The Coroner's Toolkit (TCT) 57
The Selfish Gene 28
theft 270
Thumbs Plus 62
TIA 157
TigerTools 12
time stamping 108, 113
time-to-live (TTL) 6
timing channels 121
Toneloc 6
total information awareness (TIA) 157
traceback 66
traceroute 6
traces 275
TRACKER 162
traffic monitor 237
trafficking 270
training requirements 313
transaction atomicity 112
transaction table 145
transmission control protocol (TCP) 110
trapdoor 29
Trend Micro 42
Trin00 20
TRIPWIRE 139
Trojan horse 16, 27, 218, 227
trustworthiness 111
tunneling and authentication 115
Type I 100
Type II 100

U

U.S. code 324
UCAS (UK Colleges Admission Service) 294
unauthorized entry 270
undetectable 177
unicode 103
uniformed personnel 316
United Kingdom (UK) 156
Università Statale di Milano 118
Unix 21
unsanctioned intrusion 139
unsolicited e-mail 337
unstructured 158
US 267
USB dongles 82
USB drives 234
USB keys 335
user education 47
UTF-7 103
UTF-8 103

V

Vacca 324
validated reference data source 100
vandalism 270
vendor 223
Venema 65
versatile scanning tools 8
victim 56
view toolbar 223
virtual private network (VPN) 129, 235
virus 17, 27, 176, 218
virus attack 270
VNC 17
vulnerability scanner 11

W

war dialing 6
Washington University FTP Daemon (WU-FTPD) 149
Web browsing 234
Web conferencing tool 235
WebEx 235
Webroot 17
WEPcrack 323
when-subject-action-object 141
when-subject-object-action 147
white list 240
white-box testing 94

wi-fi 235, 337
WildList Organization 36
WildPackets' iNetTools 8
WinDump 13, 69
WinInterrogate 56, 62
wired equivalent privacy (WEP) 323
WMATRIX 163
WORDNET 163
worm 17, 27
write-blockers 62
WU-FTPD attack 149

X

X-Ways Forensics 62

Y

Yahoo 20
Yahoo mail 232
Yasinsac 319