Index

A

-a assoc runtime flag, Honeyyd, 115
-A flag, NMap, 17
Abstract Syntax Notation One (ASN.1) vulnerability, 237
Abuse reports, 164
ACK flag, TCP, 6
Acknowledgement, TCP, 5
action, template, 118
Active client-side honeypots defined, 238–239
high-interaction. See High-interaction client honeypots
overview of, 239–241
Active Sink, iSink, 226–228
Ad Aware antispyware tool, 265–266
ADDCOMMAND, Kebes, 288
Address Resolution Protocols. See ARPs (Address Resolution Protocols)
Address space, detecting UML, 300–301
ADS (Alternate Data Stream), 363
Advertisement addons, with botnets, 385
Agobot, 293
searching for e-mail address on infected host, 367
stealing CD-keys, 367
and variants of, 362–363
AIMBuddyList honeypot, 88
AIRCBot, 365–366
Ajax (Asynchronous JavaScript and XML), 333
Alerts, Argos, 62
Alias interfaces, configuring nepenthes, 184
Alternate Data Stream (ADS), 363
Analysis engine, HoneyC, 247–248
Analysis report

C

cWSandbox, 405–413
Honeytrap, 197
ANI files vulnerability, 232–233
AntiVir Workstation, 407
Antivirus engines, 244–245, 407, 411
API hooking
with cWSandbox, 393
integrity checks using, 256
overview of, 396–400
with cWSandbox, 402, 404
Application Layer, Internet protocol suite, 2
Architecture
Collapsar, 211–213
cWSandbox, 402–404
HoneyC, 246–248, 260–262
HoneyClient, 258–259
Honeyd, 110
nepenthes, 167–170
Potemkin, 216–219
RolePlayer, 222
VMware, 22–23, 290
Argos, 52–62
control socket, 61–62
nepenthes integration with, 187
network setup for, 57–61
overview of, 52–54
system setup with QEMU, 54–57
ARPs (Address Resolution Protocols)
Honeyd and, 106–107, 113
LaBrea detecting available IP addresses with, 74
overview of, 4
ASCII code, analysis of, 395
ASN.1 (Abstract Syntax Notation One) vulnerability, 237
Asynchronous JavaScript and XML
Automation, CWSandbox dynamic analysis, 392–393
Autonomous spreading malware
nepenthes collecting, 176
overview of, 391–392
AV signatures, 389
-b (-log-bandwidth), LaBrea installation, 77

B
Backdoor
bindtty, in Red Hat compromise, 343
Data ChaOS Connect Back Backdoor, 334, 340
I/O, detecting virtual machines, 293–294
Multipot emulating, 204
shell.php, in Windows 2000 compromise, 347
Backus-Naur form (BNF), 313
BADTHINGS, IN-limit log, Tiny Honeypot, 86
BADTHINGS, IN log, Tiny Honeypot, 86
Bait and Switch networks, 125
Behavior analysis, 395–396
Best effort protocol, IPv4 as, 3
BGP (Border Gateway Protocol), Potemkin, 216–217
BHOs (Browser Help Objects), 240, 385
Billy Goat, 205–206
Binary packers, 395
Bind command, 123–124
Bindtty, 343
Bitdefender, 407
Blackholes, 206
Blacklists, 242
Blast-o-Mat, 308–321
as alternative to classic IDS system, 309
Haxdoor trojan and, 316–320
lessons learned, 320–321
mitigating infected system, 312–316
modules, 310–311
overview of, 308
Blast-PortScan module, Blast-o-Mat, 310
Blast-Sniffer module, Blast-o-Mat, 310
Blast-SpamDet module, Blast-o-Mat, 310
Blaster worm, 220–221
Bleeding Edge Threats, 242
BNF (Backus-Naur form), 116
Bobax, 365
Bofra worm, 235–236
Border Gateway Protocol (BGP), Potemkin, 216–217
Botnets, 359–390
Agobot and variants, 362–363
aIRC.Bot, 365–366
Bobax, 365
control structure of, 369–372
Datapay Network X, 365
DDoS attacks caused by, 373
defending against, 387–390
defined, 359
kaiten, 366
mIRC-based bots, 364
overview of, 360–362
possible usages of, 384–387
Q8Bot, 366
SDBot and variants, 363–364
social life of owners, 384
spyware in the form of bots, 366–369
Storm Worm, 365
Toxbot, 365
tracking, 373–376
Xot and XT Bot, 365
Zotob/Mytob, 364
Botnets, case studies
Mocbot and MOS06-040, 381–384
other observations, 384–387
overview of, 376–380
Bots, 360–362. See also Botnets
Botspy, 376
Bridged networking, 27
Bridging modules, 186–187
Broadcast, 3
Browser Help Objects (BHOs), 240, 385
Brute-force attacks, 341–342
Byte alignment algorithm, RolePlayer, 223

C
C&C (Command and Control) server
Agobot and variants using, 362–363
in botnet case studies, 376–380
in CWSandbox analysis reports, 410–411, 412
defending against bots, 388–389
defined, 360
setting up botnets with, 369–371
Index

Call tree, CWSandbox analysis report, 406
Capture logs, Tiny Honeypot, 83–84
CD-keys, bots stealing, 367
CD-ROMs
  Honeywall installation, 67–69
  installing OS on virtual honeypots, 33–34, 36–37
Chats, 243
chroot jails, 98–100
ClamAV
  CWSandbox analysis report, 407, 411
  detecting malicious web pages, 244
SpyBye using, 268
cleanup_module(), disabling Sebek with, 284–285
Client-side honeypots, 231–272
  active vs. passive, 238–239
  client-side threats and. See Client-side threats
detecting rootkits or Trojan horses, 176
  high-interaction. See High-interaction client honeypots
  low-interaction, finding malicious websites, 241–246
  low-interaction, HoneyC, 246–253
overview of, 231–232
Pezzonavante, 263–264
research on, 271–272
SiteAdvisor, 270–271
SpyBye, 267–270
studying spyware on Internet, 264–267
Client-side threats, 232–241
  client-side honeypots for, 238–241
  exploited Internet Explorer vulnerabilities, 232–233
  MS04-040, 233–236
  other types of, 236–238
Clone attacks, 386
Clone command, 124
Codbot, 365
Code analysis, of malicious software, 394–395
Code injection, DLL, 393, 400–401
Code Red, 72
Collapsar
  architecture, 211–213
  live testing of, 214
  Potemkin vs., 214–215
  research summary of, 224
Command and Control server. See C&C (Command and Control) server
Command-line flags. See Runtime flags, command-line
Command line flags, nepenthes, 181–183
Command redirection, nepenthes, 169–170, 174
Commands
  Argos control socket, 62
  botnet setup, 371–372
  Kebes, 288
Commercial off-the-shelf (COTS) computer, 20
Congestion control, TCP, 5
Connecting limiting, 65
Connection monitors, Honeytrap, 198
Connections, Honeyd packet logs, 132
Containment policies
  minimizing attacks on third-party systems, 285
  Potemkin, 215, 218
Control socket, Argos, 61–62
Control structure, botnets, 369–372
Copy On Write. See COW (copy-on-write)
Correlation module, Collapsar, 213
COTS (commercial off-the-shelf) computer, 20
COW (copy-on-write)
  Potemkin using, 219
  UML using, 41–42
  virtual high-interaction honeynet with, 52
Crawling engines, 243, 246
Create command, 117, 121
Crypt layer, Kebes, 287–288
Crypters, 395
CSend, 371
Curl command, 96–97
Cursor format (.ANI files) vulnerability, 232–233
Custom mode, VMware, 28
cwmonitor.dll, 402–404
CWSandbox, 391–413
  analysis of Haxdoor, 319
  analysis of lightweight IDS based on nepenthes, 323
  API hooking, 396–400
  architecture, 402–404
  behavior analysis, 395–396
  code analysis and, 394–395
CWSandbox (continued)
code injection, 400–401
dynamic analyses, 406–411
large-scale analysis, 411–413
overview of, 392–394
results of, 405–406
system description, 401–404
cwsandbox.exe, 402–404
Cyberdefense exercise, with Honeyd, 107
-d runtime flag, Honeyd, 115

D
Darknets, 206
Data Analysis, Honeywall, 63–64, 66–68
Data Capture
  honeytrap, 197
  Honeywall, 63–64, 66, 68
Data ChatOS Connect Back Backdoor,
  334, 340
Data Control, Honeywall, 63–65, 68
Data Link Layer, Internet protocol suite, 2
Data mining, 132
Data-oriented protocol, IPv4 as, 3
Data streams, 4
Datagrams, 4
Dataspy Network X (DNX) bot, 365
Date column, Honeyd, 131
DCOM vulnerability, Windows, 361
dd-attack, 282, 287
DDoS (Distributed Denial of Service) attacks
  caused by botnets, 361, 373, 377–378
  Honeywall mitigating risk of, 62–63
  IRC wars as, 360
Debian
  installing Honeyd, 108
  installing LaBrea, 75
  installing nepenthes under Linux, 177–178
  installing UML, 42–43
  running honeypot in chroot jail, 99
Debugging
  Electric Fence for, 201
  Honeyd runtime flag for, 115
Deception service, DTK, 73
Deception Toolkit (DTK), 73
Delete command, 124–125
Denial of Service (DoS) attacks, 64–65
DFN-CERT (Computer Emergency Response Team), 376

DHCP
  Honeyd configuration, 124, 128–129
  LaBrea configuration, 81
Dialog boxes, 256
Diffie-Hellman key exchange, Kebes, 288–289
Dikes, Jeff, 42
Distributed Denial of Service attacks. See
  DDoS (Distributed Denial of Service) attacks
DLLs (dynamic link libraries)
  CWSandbox analysis report, 407–408
  CWSandbox architecture, 402–403
  DLL injection, 393, 400–401
  mIRC-based bots using, 364
DMZ, 197, 332
DNX (Dataspy Network X) bot, 365
Domain Name System (Domain Name System), 4, 388
DoS (Denial of Service) attacks, 64–65
download.*.conf, nepenthes, 180
Drone, 360, 376
Drop sites (zones), 316
droprate option, set, 136
Dynamic IP settings, 313–314
Dynamic link libraries. See DLLs (dynamic link libraries)
Dynamic remote settings stub (DRSS), 365
Dynamic taint analysis
  Argos and, 53–54, 60
  defined, 52–53
Dynamic templates, Honeyd configuration, 148–150
Dynamic translation, 53–54

E
E-mail
  honeyclients based on, 259, 272
  phishing for identity theft, 386–387
  spyware in the form of bots and, 367
eCSIRT.net, 207
Elapsed time (ET), Tiny Honeypot, 84
Electric Fence malloc debugger, 201
Encoding, nepenthes, 169
Index

Encryption, botnet, 379–380
EPA (execution path analysis), 302–303
ET (elapsed time), Tiny Honeypot, 84
Ethereal. See Wireshark
Ethernet option of set command, 120–121, 128–129
Everything honeypot, 88
exclude, LaBrea configuration, 80
Execution path analysis (EPA), 302–303
-F (-bpf-file) filename, LaBrea installation, 79
-f configfile runtime flag, Honeyd, 114
-f (-no-resp-excluded-ports), LaBrea installation, 78

F
Fedora Core, 42–43
Fetch modules, 167–169, 174
Fidelity
  motivating hybrid systems, 209–210
  Potemkin, 215
  VMM, 291
File Transfer Protocol (FTP), botnet setup, 371
Filesystem, CWSandbox analysis report, 408
FileUploadManager honeypot, 88
FIN flag, TCP, 6
Financial information, identity theft and, 317
Fingerprint databases, Honeyd, 115
Fingerprinting tools, 13–18
  Honeyd deceiving, 111
  Nmap, 16–18
  Tcdump, 13–15
  Winnie, 279
  Wireshark, 15–16
Firewalls
  Collapsar frontend acting as, 211–212
  configuring LaBrea without, 81
  enabling on host system, 38
Flags. See Runtime flags, command-line
Flow, of malicious network traffic, 207
FRAG_ICMP log, Tiny Honeypot, 86
Fragmentation, IP, 3
FRAG_UDP log, Tiny Honeypot, 85–86
FreeBSD
  how Honeyd works, 106–107
  installing Honeyd on, 108–109
  installing LaBrea on, 75–80
setting up Honeyd on local network, 126–128
Wireshark for, 15–16
Frontend, in Collapsar architecture, 211–212
FTP (File Transfer Protocol), botnet setup, 371

G
Gateway, Potemkin, 216–218
GDI (Graphical Device Interface) vulnerability, 233
GenIII honeypots, 63, 166
Gentoo, 177–178
GHH (Google Hack Honeypot), 87–94
  access logging, 92–94
  detecting hitlist-based malware, 177
  general installation, 87–91
  installing transparent link, 91–92
  overview of, 87
  protecting with Systrace, 103
  GNU adns, nepenthes installation, 178
  Google AdSense attacks, 385
  Google Hack Honeypot. See GHH (Google Hack Honeypot)
  Graphical Device Interface (GDI)
    vulnerability, 233
  GRE (generic routing encapsulation) tunnels
    Collapsar, 211–213
    Honeyd, 113
    Potemkin, 216–219
  GT-bots, 364
  Guest kernel, UML, 298
  Guest system (guest virtual machine)
    based on Argos. See Argos
    based on UML. See UML (User-mode Linux)
    based on VMware. See VMware defined, 22
    -H (-auto-hard-capture), LaBrea installation, 79

H
handshake, TCP, 6–7
Hard drives, searching victim’s, 368
hardexclude, LaBrea, 80
Haxdoor, 316–320
Haxplorer honeypot, 88–91
Heap spraying technique, 234–235
Heritrix, 244, 264–265
Hidden page faults, 290, 302
HideWindow executable, in mIRC-based bots, 364
High-interaction client honeypots, 253–263
  designing, 254–258
  HoneyClient, 258–262
  HoneyMonkey, 262–263
  overview of, 253–254
High-interaction honeypots, 19–69
  advantages and disadvantages of, 9–11, 20–22
  Argos. See Argos
defined, 8, 20
Hybrid solutions. See Hybrid honeypot systems
  overview of, 19–20
  physical honeypot implying, 11
  safeguarding, 62–69
  user-mode Linux. See UML (user-mode Linux)
  VMWare. See VMWare
High-interaction honeypots, detecting, 280–301
  circumventing Honeynet logging, 286–289
  Honeywall, 285
  overview of, 280–281
  QEMU, 297–298
  Sebek, 281–285
  UML, 298–301
  VMware and other virtual machines, 289–297
HipHop module, for PHP .PoP, 96–97
History mode, Potemkin, 218
Hitlist-based malware, detecting, 176–177
Holy Father, 399
HoneyBOT, 205
HoneyC, 246–253
  architecture, 246–248
  built-in help for, 249–250
  configuration of, 250–253
  installation of, 248–249
  overview of, 246–253
HoneyClient
  detecting rootkits or Trojan horses with, 176 e-mail, 259
  overview of, 258–262
Honeycomb, 158–160
Honeyd, 105–161
  design overview, 109–111
  detecting, 276–279
  dynamic templates, 148–150
  experimenting with, 125–129
  features, 107–108
  high-interaction honeypots and, 228–230
  Honeycomb plug-in, 158–160
  Honeydctl application, 156–158
  Honeydstats analysis software, 154–156
  installation and setup, 108–109
  limitations of, 166
  overview of, 106–107
  packet-level logging, 131–133
  performance, 160–161
  protecting with Systrace, 103
  Python Internal Services, 146–148
  receiving network data, 112–113
  routing topology, 150–153
  runtime flags, 114–115
  service-level logging, 133–134
  services, emulating, 139–141
  services, overview of, 129–131
  subsytems, 142–146
Honeyd, configuration, 115–125
  add command, 121–123
  advanced features for, 136–138
  bind command, 123–124
  create command, 117
  delete command, 124–125
  include command, 125
  overview of, 115–116
  set command, 117–121
Honeydctl application, 125, 156–158
Honeydstats analysis software, 154–156
HoneyMonkey, 176, 262–263
Honeynets
  circumventing logging, 286–289
  defined, 21
  high-interaction, 9
  low-interaction, 11
  minimizing risk of attacks on third-party systems, 285
  virtual high-interaction, with UML, 52
  virtual high-interaction, with VMware, 40
Honeypots
  collecting malware. See Malware
defined, 7–8
Index

detecting high-interaction. See

High-interaction honeypots, detecting

detecting low-interaction, 274–280

detecting rootkits, 302–304

fingerprinting tools, 13–18

high-interaction, 9–10

hybrid. See Hybrid honeypot systems

legal aspects of, 12

low-interaction. See Low-interaction

honeypots

overview of, 7–9

physical, 11

virtual, 11–12

Honeytrap, 197–204

installation and configuration,

200–203

overview of, 197–200

running, 203–204

Honeywall

detecting, 285

installation of, 67–69

overview of, 9, 63–67

Hooking

API, 396–399

System Service, 400

 Horde Application Framework
vulnerabilities, 351

Host kernel, UML, 298

Host system

Argos. See Argos

defined, 22

taking contaminated hosts offline, 313

UML. See UML (User-Mode Linux)

VMware. See VMware

Hot swap, 187

Houseofdabus, 171

HPOT_DATA log, Tiny Honeypot,

85–86

hppfs, 300

HTML vulnerability

analyzing suspicious sites, 256–257

MS04-040 threat, 232

overview of, 233–236

HTTP (HyperText Transfer Protocol)

analyzing CWsandbox reports, 412

botnet setup using, 369–371

SDBot and variants using, 363

HTTPS web service exploits, 286

Hybrid honeypot systems, 209–230

building own, 224–230

Collapsar, 211–214

overview of, 209–210

Potemkin, 214–220

research summary of, 224

RolePlayer, 220–224

HyperText Transfer Protocol. See HTTP

(i-device) interface, LaBrea installation, 79

-i interface flag, tcpdump, 14

-i interface runtime flag, Honeyd, 114

-I (-my-ip-addr) octet.octet.octet.octet[/size],

LaBrea installation, 79

I

I/O backdoor, VMware, 293–294

ICMP, Honeyd packet logs, 132

ICMP, ping requests, 275–276

Icon format (.ANI files) vulnerability,

232–233

ICS (Internet connection sharing), 29

IDE device, detecting UML with, 300

Identity theft, 316–317, 386–387

IDS (intrusion detection system). See also

NIDS (network intrusion detection

systems)

Blast-o-Mat vs. classic IDS, 309

high-interaction honeypot vs., 20

Honeywall and, 65–66

low-interaction honeypots as, 10–11

monitoring UML-based honeypots, 50

monitoring VMware-based honeypots, 38

ephemerals as, 196, 321–325

IDT (Interrupt Descriptor Table), 397, 400

Ifconfig, 184

IFRAMES (Inline Floating Frame) tag

vulnerability, 232, 233–236

Ignore mode, Honeytrap, 199

IM (instant messaging), 243, 271

IMS (Internet Motion Sensor), 206

include command, 125

-init-file filename, LaBrea installation, 79

Inline Code Overwriting, CWsandbox,

397–399

Inline Floating Frame (IFRAMES) tag

vulnerability, 232, 233–236

Insider attacks, 332
Installation, 67
  Argos, 54–57
  Google Hack Honeypot, 87–91
  HoneyC, 248–249
  Honeyd, 108–109
  honeytrap, 200–201
  Honeywall, 67–69
  LaBrea, 75–80
  nepenthes, 177–179
  PHP PoP, 95
  SpyBye, 268–269
  Tiny Honeypot, 82–83
  UML, 42–45
  VMware Player, 29–31
  VMware Server, 31–33
Instant messaging (IM), 243, 271
Integrity checks, 255–256
internal keyword, Honeyd, 122
Internal Reflect mode, Potemkin, 218
Internet
  connecting honeypot running Argos to, 60
  connecting honeypot running UML to, 51–52
  connecting honeypot running VMware to, 39–40
  studying spyware on, 264–267
  testing high-interaction client honeypots, 257
Internet Archive, 244
Internet connection sharing (ICS), 29
Internet Explorer, 232–233, 270–271
Internet Motion Sensor (IMS), 206
Internet protocol suite. See TCP/IP (Transmission Control Protocol/ Internet Protocol)
Internet protocols. See Network protocols
Internet Sink (iSink), 226–228
Internet Storm Center (ISC), 206
Interprocess communication (IPC), CWSandbox, 402
Interrupt Descriptor Table (IDT), 400
Intrusion detection system (IDS). See also NIDS (network intrusion detection systems)
Intrusion Prevention System (IPS), 65–66
IP addresses
  binding templates to, 123–128
  configuring nepenthes with multiple, 183–185
  defined, 3
  detecting worms with Billy Goat, 205–206
determining, 3–4
  Honeyd handling multiple, 106–107, 111
  Honeyd receiving network data, 112–113
  Honeywall installation, 67–69
  LaBrea and, 74–75
IP Aliasing, 184
IP forwarding, 29
IP routing, 7
IPC (interprocess communication), CWSandbox, 402
ipconfig, 48
ipignore, LaBrea configuration, 80
ip. queue interface, 198
iproute2 utilities suite, 183–184
IPS (Intrusion Prevention System), 65–66
Iptables rule, 198
IPv4, 3
IRC-based honeypots, 271
IRC bots, 240
IRC (Internet Relay Chat) server
  Agobot and its variants using, 362–363
  analyzing in CWSandbox reports, 412
  botnet case studies, 377–380
  botnet setup using, 369
  mIRC-based bots using, 364
  observing botnets with, 375–376
  SDBot and variants using, 363
IRC wars, 360
ircoffer, 214
ISC (Internet Storm Center), 206
ISink (Internet Sink), 226–228
ISO images
  Honeywall installation, 68
  installing OS on virtual honeypot, 33–34, 36–37
K
  Kaiten, 366
  Kebees, 287–288
  Kernel memory, detecting Sebek, 282–284
Index

Kernel Rebuild Guide, 45
Keylogger
  bots using, 366–367, 386
  client-side attacks installing, 240
Spybot, 368–369
KQEMU, 54–57
  -l (-log-to-syslog), LaBrea installation, 78
  -l logfile runtime flag, Honeyd, 115

L
LaBrea, 74–81
  configuration, 79–80
  detecting, 277
  installation, 75–79
  observations, 81
  overview of, 74–75
Legal issues, of honeypots, 12
libcurl, 178
libdnet, 75–76, 108
libevent, 108
libmagic, 178
libpcap
  Agobot and its variants using, 363
  honeytrap connection monitor based on, 198
  installing for Honeyd, 75–76
  installing for LaBrea, 75–76
Libraries, vulnerabilities in, 237. See also DLLs (dynamic link libraries)
Link analysis, 334
Linux
  chroot utility and, 99–100
Honeyd and, 106–109, 126–128
  Honeytrap connection monitor in, 198
  installing LaBrea, 75–80
  installing nepenthes, 177–179
NMap for, 16–18
  setting up virtual honeypots with, 12, 29–33
Systrace for, 101–102
  UML only running on, 41
VMware Player for, 30
VMware with, 28–29, 34–37
Wireshark for, 15–16
Linux Kernel Archives, 43
LKM (loadable kernel module), 302
Loadable kernel module (LKM), 302
Local nepenthes sensor, 185–186, 196
Locking infected systems, 313–314
log-*.conf, nepenthes, 180
Logging
  circumventing on Honeynet, 286–289
  detecting Sebek, 281–282
Logging module
  Collapsar, 213
  defined, 167–168
  Google Hack Honeypot, 92–93
  Honeyd, 115, 131–133
  Tiny Honeypot, 83–86
  UML-based honeypots, 50–51
Logical discrepancies, detecting virtual machines, 295–296
Low-interaction client honeypots
  finding malicious websites, 241–246
  HoneyC, 246–253
  overview of, 241
Low-interaction honeypots, 71–103
  advantages and disadvantages of, 10–11, 72–73
Deception Toolkit, 73
  defined, 8, 72
detecting, 274–280
Google Hack Honeypot. See GHH
  (Google Hack Honeypot)
Honeyd. See Honey
Hybrid solutions. See Hybrid honeypot systems
LaBrea, 74–81
nepenthes. See Nepenthes
PHP HoP, 94–97
  securing with chroot jail, 98–100
  securing with Systrace, 100–103
Tiny Honeypot, 81–86
LSASS vulnerability, Windows, 361
LSASSDialogue.cpp, Windows, 172

M
MAC addresses
  configuring Honeyd with ethernet option, 120–121, 128–129
defined, 3
detecting virtual machines via, 292–293
Mac OS X
  installing Honeyd, 108–109
  using Parallels as VMM for, 292–293
Mac OS X (continued)
virtualization options for, 23
Wireshark for, 15–16
Malicious software. See Malware
Malicious websites
analyzing downloaded content, 244–246
attackers setting up, 239
finding suspicious sites, 241–244
high-interaction client honeypots searching for, 254–255
HoneyC searching for, 246–253
Malware, 163–207
analyzing with CWSandbox. See CWSandbox
client-side attacks installing, 239–240
collecting with Billy Goat, 205–206
collecting with HoneyBOT, 205
collecting with Honeytrap. See Honeytrap
collecting with Multipot, 204–205
collecting with nepenthes. See Nepenthes
introduction to, 164–165
learning about malicious traffic, 206–207
overview of, 163–164
spreading sequentially or randomly, 185
spreading with botnets, 385
as threat to Internet, 309
top ten types of, 195
MD5 hash, code analysis of, 395
memory, detecting Sebek from, 282–284
Memory dumps, Argos, 60
Meta-honeypots, 199
MHTML processing vulnerability, 232
Microsoft. See also Windows
MS03-039 exploit, 60–61
MS04-007 exploit, 237
MS04-011 exploit, 171
MS04-013 exploit, 322
MS04-040 exploit, 232–236
MS05-002 exploit, 232–233
MS05-039 exploit, 187–188, 364
MS05-051 exploit, 188
MS06-001 exploit, 232–233
MS06-040 exploit, 381–384
MS06-057 exploit, 232–233
popular programs targeted, 236
vulnerabilities of Internet Explorer, 232–233
Microsoft Distributed Transaction Coordinator (MSDTC), 188
mIRC-based bots, 364
Mirror mode, honeytrap, 199, 202–203
Mitigation, nepenthes, 311–312
Mocbot, 381–384
module*.conf, nepenthes, 180
Monitoring honeypots
UML-based, 50–51
VMware-based, 37–39
Morphine, 362
Mozilla Firefox, 236, 270–271
MSDTC (Microsoft Distributed Transaction Coordinator), 188
Multipot, 204–205
Mutex objects, 408–409
MySQL database, 93–94
Mytob, 364
-n flag, tcpdump, 14–15
-n (-network) octet.octet.octet.octet [size], Labrea installation, 79
N
NAT (network address translation)
creating virtual honeypots, 33
deploying honeypots, 12
high-interaction honeypots and, 224–228
virtual networks with UML and, 48
virtual networks with VMware and, 27–29
National Security Agency (NSA), 107
Native API, 396–397
Needleman-Wunsch algorithm, RolePlayer, 223
NefFlow/cflow, 206–207
Nepenthes, 165–197. See also Blast-o-Mat
analyzing CWSandbox reports with, 411–413
architecture of, 167–170
assigning multiple IP addresses with, 183–185
benefits of, 321
capturing new exploits with, 186–187
command line flags, 181–183
configuring, 179–181
customizing, 181
detecting, 279–280
element of, 170–176
flexible deployment of, 185–186
installing, 177–179
lessons learned, 196–197
lightweight IDS based on, 321–325
limitations of, 176–177
overview of, 165–167
results of, 188–196
Surfnet IDS use of, 326
tracking botnets with, 374
vulnerability modules of, 187–188
nepenthes.conf, 179
NetBSD
Honeyd and, 106–109, 126–128
Systrace for, 101–102
Wireshark for, 15–16
Netcat, 347
Netfilter logs, Tiny Honeypot, 85–86
Netflow/cflow, 389
network address translation. See NAT
(network address translation)
Network intrusion detection systems. See
NIDS (network intrusion detection systems)
Network Layer, Internet protocol suite, 2
Network protocols
Honeyd packet logs, 131–132
Honeyd receiving network data, 112–113
TCP/IP, 1–6
Network socket, Argos, 61–62
Network telescopes, 206
Networks, 126–128
configuring Argos, 57–61
of honeypots. See Honeynets
setting up Honeyd on local, 126–128
virtual. See Virtual networks
vulnerabilities in university, 309
New Zealand Honeynet Project, 195
Newsgroups, 243
NIDS (network intrusion detection systems).
See also Blast-o-Mat
decreasing usefulness of, 7
honeypots vs., 8–9
Surfnet IDS, 325–326
Nmap
assigning personality to templates from,
117–120
circumventing honeynet logging using, 287
detecting nepenthes, 279–280
overview of, 16–18
reading files with Kebes and, 288
testing Honeyd’s deception of, 127–128
-no-arp-sweep, LaBrea installation, 79
NSA (National Security Agency), 107
-O flag, NMap, 17
-o (-log-to-stdout), LaBrea installation, 78
-O pOf-file runtime flag, Honeyd, 115
Oberheide, John, 278–279
Observed behavior, CWsandbox analysis,
406–407
Office applications, vulnerabilities in, 238
OLE automation, 255
-oN/-oX/-oG file, NMap, 18
Online polls/games, and botnets, 386
Online resources
AdAware, 265
Argos honeypots, 54
bot attacker tools, 362
botnets, 390
Collapsar research study, 214
crawling engines, 243–244
CWsandbox, 394, 413
Deception Toolkit (DTK), 73
defining honeypots, 8
e-mail honeyclient, 259
Heritrix, 264
HoneyBOT, 205
HoneyC, 246, 261–262
HoneyClient, 258–259
Honeyd, 108–109
HoneyMonkey, 262–263
Honeynet groups, 12
Honeytrap, 197
Honeywall, 67, 69
iproute2 utilities suite, 183
LaBrea installation, 76
legal aspects of running honeypots, 12
Linux Kernel Archives, 43
memory dumps, 60
MS04-040 threat, 233–234
Multipot, 204
nepenthes, 166, 186
nepenthes installation requirements,
178–179
NMap, 17
Outlook Redemption, 259
Online resources (continued)
QEMU, 34–35
root filesystem download, 46
Sebek, 39
SiteAdvisor, 270
tcpdump, 13
typosquatting, 243
UML, 42
VMM, 292
VMware Player download, 30
VMware Server download, 32
VMware Technology Network, 31
VMware versions, 25–26
Windump, 13
Wireshark, 15
open, Honeyd configuration, 118
open system call, 101
OpenBSD
Honeyd installation, 109
setting up Honeyd on local network, 126–128
Systrace for, 101–102
Operating systems
configuring Honeyd to simulate, 107
installing on virtual honeypot, 33–34, 36–37
Oracle databases, vulnerabilities in, 236
Outlook/Outlook Express, 236–237, 259–260
Outlook Redemption, 259–260
-p fingerprints runtime flag, Honeyd, 115
-p (-max-rate) datarate, LaBrea installation, 76–77
-P (-persist-mode-only), LaBrea installation, 77
-p port-ranges flag, NMap, 17

P
P2P (Peer-to-Peer) communications
Agobot and its variants using, 362
botnet setup using, 371
bots propagating using, 361–362, 365
honeyclients based on, 272
Packet-level logs, Honeyd, 131–133
Packet sniffers, 386
Packet switched networks, 3
Packets, TCP, 4–5
Parallels
Desktop, 23
as VMM for Mac OS X, 292–293
Workstation, 23
Parameters, set command, 118
Passive client-side honeypots, 238–239
Passlist.txt honeypot, 88
Passwd.list honeypot, 88
Password dumpers, 347
Passwords
botnet setup using, 371–372
bots using weak, 361–362
configuring Honeywall, 68
pause command, Argos, 62
pcap, honeytrap, 201–202
PCRE (Perl Compatible Regular Expressions) library, 178, 363
Peer-to-Peer (P2P) communications. See P2P (Peer-to-Peer) communications
Performance
Collapsar, 213
Honeyd, 160–161
hybrid systems, 209–210
VMM, 291
VMware guest system, 23
Perl Compatible Regular Expressions (PCRE) library, 178, 363
Perl scripts, 340, 341
Persistent capture, LaBrea, 75
Personality, assigning, 117–120
Pezzonavante, 263–264
Phishing, 351, 354, 386–387
phpAdsNew vulnerability, 333
PHPBB_Installer honeypot, 88
PHPFM honeypot, 88
PHP_HoP
HipHop module, 96–97
installation, 95
overview of, 94
PhpMyAdmin module, 97
PhpMyAdmin module, 97
PHP_Ping honeypot, 88
PHP_Shell honeypot, 88
Phrack magazine, fake release of
articles on honeypot detection, 280
detecting and disabling Sebek, 281–283
detecting Honeyd, 277
Index

Physical honeypots, 8, 11. See also
  High-interaction honeypots
Physical Layer, Internet protocol suite, 2
PhysSysInfo honeypot, 89
PID (process ID), Tiny Honeypot, 84
ping flood, 275
Plug-ins
  HoneyC, 248
  honeytrap, 200, 203–204
pmn, LaBrea configuration, 80
Policies
  configuring Systrace, 101–103
  minimizing attacks on third-party systems
    with containment, 285
  Potemkin containment, 215, 218
  Revisit, 245–246
port-helper utility, UML, 49
Port ranges, LaBrea configuration, 80
portignore, LaBrea configuration, 80
Portwatch modules, nepenthes, 186–187
Potemkin, 166
  architecture, 216–220
  live testing of, 219–220
  overview of, 214–216
  research summary of, 224
/proc, 300
Process ID (PID), Tiny Honeypot, 84
Protected Storage (PStore), 317–318
Protocol Proxy mode, Potemkin, 218
Proxy ARP, 106, 113, 120
proxy keyword, Honeyd, 122
Proxy mode, Honeytrap, 199
PSH flag, TCP, 6
PStore (Protected Storage), 317–318
Ptrace vulnerability, Linux, 340, 343
Python, 288–289
Python Internal Services, 146–148

R
RADIUS (Remote Authentication Dial In
  User Service), 314
RAM
  high-interaction virtual honeypot
    requirements, 29
  HoneyBOT requirements, 205
  Honeywall installation requirements, 67–69
  MWare requirements, 24
  SiteAdvisor requirements, 270
  virtual machine requirements, 24
RATs (Remote Access Trojans), 204
RBot, 323, 363–364
read() method, Sebek, 281–284, 286–287
RealPlayer vulnerabilities, 236
Reconnaissance, high-interaction honeypots,
  20
Red Hat 8.0 case study, 332–343
  evaluation of attack, 343
  overview of, 332–333
  summary of attack, 334–335
  timeline of attack, 335–338
  tools involved in attack, 338–343
RedPill VMM detection code, 296–297
Registry access, CWSandbox, 409–410,
  412–413
Remote Access Trojans (RATs), 204
Remote Authentication Dial In User Service
  (RADIUS), 314
reset command, Argos, 62
reset command, Honeyd, 118
Resource discrepancies, detection with, 295
resume command, Argos, 62
Revisit policy, 245–246
Risk, of honeypots
  high-interaction, 21
  high-interaction vs. low-interaction, 11
  legal aspects of, 12
RolePlayer
  applications of, 223–224
  overview of, 220–223
  research studies, 224
Root filesystem, UML, 41–42, 46–49
root user, 100

Rootkits
- CWSandbox functionality for, 404
detecting, 302–304
Haxdoor capabilities, 316
nepenthes incapable of detecting, 176
SHv5 rootkit, 338–340

Routers
- as high-interaction honeypots, 20
how Honeyd works, 106–107
Potemkin architecture, 216–218
Routing topologies, Honeyd, 108, 150–153

RPC DCOM exploit, 60–61
RPM-based VMPlayer, 30
RST flag, TCP, 6
Ruby, 248–249

Runtime flags, command-line
- Honeyd, 114–115
honeytrap, 203–204
LaBrea installation, 76–79
nepenthes, 181–183
NMap, 17–18
TCP, 6
tcpdump, 14–15
-UML runtime, 46–49
-S flag, tcpdump, 15
-s servicelog runtime flag, Honeyd, 115
-s snaplen flag, tcpdump, 15
-s (-switch-safe), LaBrea installation, 78

S
Safety, VMM, 291

Sandbox, Norman, 405–406
Sandboxing. See CWsandbox
SANS Top-20 Internet Security Attack Targets for 2006, 237

Santy worm, 327–332

Scalability
- Collapsar, 213
motivating hybrid systems, 209–210
nepenthes, 166, 170, 190–193
Potemkin, 215
virtual honeypots, 11–12
VMware, 23–24

SCM (Service Control Manager)
- vulnerabilities, Windows, 319–320

Scoopy Doo, 296–297

Scripts
- configuring Honeyd with services, 129–131
Data ChaOS Connect Back Backdoor, 340
UDP flooder, 341
web applications and, 333
SDBot, 363–364, 367–368
SDL (Simple DirectMedia Layer)
development libraries, 55

Search engines, finding malicious websites, 242
Search Worms, 327–332
applied to Santy worm, 328–332
overview of, 327
sequence of operations executed by, 327–328

Sebek
capturing information with, 9
circumventing logging by, 286–287
detecting, 281–284
disabling, 284–285
monitoring VMware-based honeypots, 39
overview of, 66–67

Security
connecting virtual honeypots to Internet, 39–40, 51–52
high-interaction honeypots, 62–69
honeytrap, 201
Honeywall, 63–69
LaBrea installation, 76
low-interaction honeypots, 98–103
nepenthes installation, 178

Seed, Heretrix, 265

Segments, TCP, 4

Semiglobal alignment algorithm, RolePlayer, 223

Sensors, nepenthes, 185–186, 196
Sequence numbers, TCP, 4–5
Service Control Manager (SCM)
- vulnerabilities, Windows, 319–320

Service emulation, honeytrap, 198–199

Services, Honeyd
- configuring, 107, 129–131
eulating, 139–141
log files, 133–134
runtime flag, 115

Session ID (SID), Tiny Honeypot, 84–85
Session logs, Tiny Honeypot, 85
set command, Honeyd
Index

droprate option, 136
ethernet option, 120–121
overview of, 117–120
uid option, 137
uptime option, 120
setSlice () vulnerability, WebViewFolderIcon
Active X control, 233
SGDT instructions, 295–296
SHA-512 hash, 395
Shadow honeypots, 187
Shell emulation, nepenthes, 169–170, 176
Shell scripts, configuring Honeyd, 129–131
Shellcode-executer extension, Python, 288–289
shellcode-generic.conf, nepenthes, 180
Shellcode parsing modules
defined, 167–168
example of, 172–174
overview of, 169
shutdown command, Argos, 62
SHv5 rootkit, 338–340
SID (session ID), Tiny Honeypot, 84–85
SIDT instructions, 295–296
Simple DirectMedia Layer (SDL) development libraries, 55
SiteAdvisor, 270–271
skas, 301
SLDT instructions, 295–296
SMTP, analyzing CWSandBox, 412
Snapshot mechanism, of QEMU, 57
Snort system
HoneyC searching for malicious web servers based on, 246–248
monitoring VMware-based honeypots, 38
snort-inline
IPS based on, 65
minimizing risk of attacks on third-party systems, 285
SOCKS proxy, 240
Software
malicious. See Malware
monitoring VMware-based honeypots, 37–39
virtualization, 22
SP2, Windows, 327
Spamming, 385
Spear phishing, 367
Spybot, 363–364, 368–369
SpyBye, 268–270
Spyware
as bots, 366–369
client-side attacks installing, 240
studying on Internet, 264–267
SquirrelMail honeypot, 89
SSDT (System Service Dispatch Table), 397, 400
Static analysis, malicious software, 392–393
Static IPs, 313
Statistics, nepenthes, 188–189, 193–196
stdin, Honeyd, 129–130
stdout, Honeyd, 129–130
Storm Worm bot, 365
strace tool, 99–100
su command, Honeywall, 68
Submission modules, 167–169, 174
submit-*.conf, nepenthes, 180
Subsystems, Honeyd, 108, 142–146
sudo command, Honeyd, 126
SURFnet IDS, 325–326
SUSE 9.1 case study, 351–357
evaluation of attack, 356–357
overview of, 351
summary of attack, 351–352
timeline of attack, 352–354
tools involved in attack, 354–356
-sV flag, NMap, 17
svchost processes, 176
SVM (Pacifica), 296
Switches, 20
Symantec, 405–406
SYN flag, TCP, 6
System call interposition, 101
System Service Dispatch Table (SSDT), 397, 400
System Service hooking, 400
Sytrace, 100–103

T
T (-dry-run), LaBrea installation, 78
-t (-throttle-size) database, LaBrea installation, 76
-T[0–5] flag, NMap, 17
tap0 virtual device, 48–49
tar.gz-ball, 30
Tarpits, 74
Tarpitting module, Collapsar, 213
Tcddump, 13–15
TCP/IP (Transmission Control Protocol/Internet Protocol), 1–2
TCP SYN flooding attacks, 372–373
TCP SYN packets, 279
TCP (Transmission Control Protocol)
detecting low-interaction honeypots, 276–280
Honeyd packet logs, 132
Honeytrap and, 198–200
LaBrea utilizing, 74–75
understanding, 4–7
tcddump, 50, 66
Templates, Honeyd
add command, 121–123
advanced configuration, 136–138
bind command, 123–124
create command, 117
defined, 117
delete command, 124–125
dynamic, 148–150
set command, 117–120
TFTP (Trivial File Transfer Protocol), botnets using, 371
thp (Tiny Honeypot), 81–86
capture logs, 83–85
installation, 82–83
netfilter logs, 85–86
observations, 86
overview of, 81–82
session logs, 85
Throttling, LaBrea, 75
Timestamps, 120, 131
Timing-based detection, 295
detecting low-interaction honeypots, 276–280
detecting virtual machines, 295
through hidden page faults, 302
Tiny Honeypot. See thp (Tiny Honeypot)
Titan Rain attacks, 238
TLB (translation look-aside buffer), 295
Tools, fingerprinting, 13–18
Nmap, 16–18
tcddump, 13–15
Wireshark, 15–16
Toxbot, 365
Tracing Thread (TT) mode, UML, 298
Tracking, botnets, 373–376
Traffic redirectors, Collapsar, 211–212
Translation look-aside buffer (TLB), 295
Transmission Control Protocol. See TCP
Transmission Control Protocol/Internet Protocol (TCP/IP), 1–2
Transport Layer
Internet protocol suite, 2
TCP, 4–6
UDP, 4
Trivial File Transfer Protocol (TFTP), botnets using, 371
Trojan horses, 176, 316–320
TT (Tracing Thread) mode, UML, 298
tty logging, 50–51
TUN/TAP device, 48, 300
tunctl utility, UML, 49
Typosquatting (URL hijacking), 242–243
U
UDP (User Datagram Protocol)
flooding attacks, 341, 372–373
Honeyd packet logging with, 132
overview of, 4–5
uid option, set command, 137
UML (User-mode Linux), 41–52
building virtual high-interaction honeynet, 52
connecting virtual honeypot to Internet, 51–52
detecting, 298–301
installation and setup, 42–45
monitoring honeypots, 50–51
overview of, 41–42
runtime flags and configuration, 46–49
setting up virtual honeypots, 12, 21
umlnet utility, UML, 49
uml_switch utility, UML, 49
UNICODE, analysis of, 395
Updates
bots using, 361, 378
Windows vulnerabilities, 361
uptime option, set command, 120
UPX, 362
UrBot, 363–364
URG flag, TCP, 6
Index

URLs, malicious
   analyzing suspicious sites, 244–246
   analyzing with SpyBye, 268–270
   high-interaction client honeypots
      finding/analyzing, 254–258
      looking for, 241–244
urls.txt file, 260
UrXBot, 363–364
User-Agent field, HTTP header, 243
User Datagram Protocol. See UDP (User Datagram Protocol)
User-mode Linux. See UML (User-mode Linux)
Usernames
   botnet setup, 372
   bots using weak, 361–362
   configuring Honeywall, 68
USR1 signal, 132–133
-v (-verbose), LaBrea installation, 78

V
Vanderpool (VT), 296
Variable expansion, Honeyed, 122–123
Versions, VMware, 25–26
Virtual filesystem, nepenthes, 170
Virtual honeypots
   advantages and disadvantages, 11–12
   connecting to Internet, 39–40
   creating, 33–37
   defined, 8
Virtual machine monitor. See VMM (virtual machine monitor)
Virtual machines. See also .vmx files
   analyzing spyware on Internet with, 265
   Collapsar architecture, 212
   detecting, 289–297
   Potemkin architecture, 216–217
   virtualization vs. emulation of, 297–298
Virtual networks
   setting up with Argos, 59–61
   setting up with UML, 47–49
   setting up with VMware, 26–29
Virtual PC, 23
Virtual system, 22
Virtualization software. See VMWare
Virusscan, CWSandbox, 407
Visitor, HoneyC, 246–247
VMM (virtual machine monitor)
   detecting presence of, 295–296
   overview of, 290–292
   Potemkin using, 218–219
vmnet, 28
VMTN (VMware Technology Network), 31
VMware, 22–40
   adding monitoring software, 37–39
   building virtual high-interaction honeynet, 40
   combining with Honeyed, 111
   connecting virtual honeypot to Internet, 39–40
   creating virtual honeypot, 33–37
   detecting, 289–296
   overview of, 22–25
   preventing detection of, 296–297
   setting up virtual high-interaction honeypot, 29–33
   setting up virtual honeypots, 12, 21
   versions of, 25–26
   virtual network with, 26–29
VMware ESX Server, 26
VMware Fusion, 23
VMware GSX Server, 25–26
VMware Player
   creating virtual honeypot for VMware, 34–37
   overview of, 25–26
   setting up virtual honeypot, 29–33
VMware Technology Network (VMTN), 31
VMware Workstation, 25, 33–34
VMWareServer
   creating virtual honeypot for VMware, 33–34
   installation and setup for, 31–33
   overview of, 25–26
.vmx files
   creating virtual honeypot for VMware with QEMU, 35
   preventing detection of VMware, 297
   virtual machine format, 31
VPN tunnel, deploying nepente, 186
VT (Vanderpool), 296
vuln-*.conf, nepenthes, 180
Vulnerabilities. See also botnets; client-side threats; Microsoft; Windows Horde Application Framework, 351 ptrace in Linux, 340, 343 search engines for finding, 327 in XAMPP, 344 Vulnerability modules defined, 167–168 detecting nepenthes remotely, 177 example of, 172–173 implementing, 187–188 overview of, 168 results of, 188–189


X x2.conf, nepenthes, 180 XAMPP, vulnerabilities in, 344 XOR encoder, 169, 173–174 Xot bot, 365 XT Bot, 365

Y Yahoo search queuer, HoneyC, 246–247

Z Zero-day (0day) attacks defined, 253 detecting with Argos. See Argos extending nepenthes to handle, 186–187 handling, 189 high-interaction honeypots detecting, 253–254 Internet Explorer vulnerabilities to, 233 low-interaction honeypots not for, 72 against Office applications, 238 Zombie, 360 Zotob worm, 187–188, 364