Index

Numbers and Symbols

4-clause BSD license
  Honeyd open-source agreement, 122
8086 register types and common functions, 347
80x86 instructions
  common, 348
(pound sign)
  using to comment out unnecessary Snort rules, 263
  using to remark out lines in a Honeyd template, 160–161
\\. parameter
  using to indicate local computer, 307

A

A86/A386 assembler
  website address, 353
AccessEnum utility
  for listing permissions, 314
  website address, 314
ACK (Acknowledgment) flag
  in TCP, 234
acknowledgment number field
  in TCP, 233
active fingerprinting
  function of and tools for, 27–28
Active@ UNDELETE program
  for recovering deleted files and formatted disks, 315
Active@ UNERASER program
  for recovering deleted files and formatted disks, 315
ActiveState Perl engine
  preferred by Perl programmers, 145
Activeworx, Inc.
  free software offerings, 294
  website address, 293
Activeworx Security Center (ASC)
  as honeynet security console, 294
ADD command
  for adding service scripts to Honeyd configuration files, 171–172
address resolution protocol
  how it works, 43
administrator accounts
  renaming to protect your honeypots, 117
ADSScan data stream checker
  function of, 281–282
Advanced Attachments Processor tool
  for extracting file attachments from e-mail databases for analysis, 315
Advanced Process Manipulation tool
  for controlling target processes, 283
Afind program
  for analyzing file system, 312
  website address, 312
Akonix L7 Enterprise tool
  for checking for IM services hacker activity, 317
alert messages
  considerations for, 295–296
alert or message throttling
  defined, 295
alert utilities
  additional for honeypots and monitoring systems, 299
  for honeypots, 296–299
alerting mechanism
  flexible in IDSs, 226
  importance of in honeypot systems, 295–299
  needed for operating a honeypot, 12
  using the NET SEND command in Windows, 296
Alkasis Corporation
  website address for PatriotBox honeypot, 212
AllAPI
  website address, 343
"An Evening with Berferd" paper (Bill Cheswick)
  website address, 20
Analyze menu
  in Ethereal protocol analyzer utility, 246–248
analyzing honeypots. *See* data analysis, for honeypots
annotate command
  in Honeyd, 129
ANNOTATE keyword
  example showing use of, 157
annotation
  syntax for Windows personalities, 156–157

anonymous enumerations
disabling, 118
antispam relay server
Jackpot tarpit as, 9
API enforcement, 345
application and presentation layers
in OSI model, 229
application fingerprinting. *See also* fingerprinting
function of, 29–30
application folders and files
restricting access to, 106–108
Application Programming Interfaces (APIs)
defined, 340
using third party, 343–344
ArcSight
website address, 294
Argus
website address, 309
Arkin, Ofir
PowerPoint presentation about ICMP fingerprinting by, 29
ARP flooding
using to overwhelm switches, 46
ARP poisoning
using to overwhelm switches, 46
ARP proxying, 128
assembler and disassembler programs
choosing, 349–357
assemblers
choosing, 349–353
other available, 352–353
Webster's web site for information about, 353
assembly language
learning, 339–349
resources for learning, 346
using, 344
website address for resources, 340
assembly language instructions
on computer platforms, 345–349
AT&T Mexican honeynet
website address, 8
attack models
summary of, 32
used by hackers, 26–32
attack programs
automated, 30
Audit Account Logon Events
Windows auditing category, 286
Audit Account Management enabling
Windows auditing category, 286
Audit Directory Service Access
Windows auditing category, 286
Audit Logon Events
Windows auditing category, 286
Audit Object Access
Windows auditing category, 286
Audit Policy Change
Windows auditing category, 287
Audit Privilege Use
Windows auditing category, 287
Audit Process Tracking
Windows auditing category, 287
Audit System Events
Windows auditing category, 287
authentication protocols
securing, 118–119
automated attack programs
types of, 30
Autoruns monitoring utility
checking for changes to the Registry and autorun keys with, 319
function of, 279
AutoStart Viewer utility
function of, 283

B

-b switch
for binary logging mode in Snort, 255
Back Officer Friendly (BOF) honeypot
installation and configuration of, 189–190
website address, 189
Back Orifice tools
recognized by Back Officer Friendly honeypot, 190
Back2Life program
for recovering deleted files and formatted disks, 315
Bait and Switch Honeypot
website address, 10
banner grabbing
defined, 29
baseline measurements
methods for getting for your honeypot, 98–99
sampling of Microsoft tools for documenting, 271
taking as first step in honeypot data collection, 269
bind command
in Honeyd, 128–129
BinText tool
function of, 281
BIOS interrupt routines
stored on BIOS chips and used to manipulate data, 341
website address for list of, 341
blackholes. *See* tarpits (blackholes)
Blaster worm
Microsoft patches for, 87
on RPC servers, 73

Blat utility
website address, 299
blended attacks
methods used in, 31–32
BOF honeypot. *See* Back Officer Friendly (BOF) honeypot
bootable forensic distributions, 324
Borg disassembler
function of and website address, 356–357
botnet
defined, 304
breakpoints
as debugging tricks, 359
bridges
as honeypot network system devices, 46
broadcast packets
defined, 41
bs option
in Dd.exe command-line syntax, 307
Bugbear worm
website address, 77

C

-c command-line parameter
for putting Snort into network IDS mode, 256
Cache Reader tool
for tracking Internet Explorer hacker activity, 316
Cache View tool
for tracking hacker activity, 316
CacheInfo tool
ActiveX control for tracking hacker activity, 316
CacheX utility
for tracking Internet Explorer hacker activity, 316
CALs. *See* client access licenses (CALs)
Cambia Security Inc.
website address for CM utility, 276
Capture menu options
using in Ethereal protocol analyzer utility, 244–246
CARO naming convention. *See* Computer Antivirus Researcher's Organization (CARO) naming convention
Center for Internet Security
website address, 40
Cheswick, Bill
"An Evening with Berferd" paper by, 20
CIFS protocol
updated version of SMB, 74
Cisco telnet session script
login prompt for, 173
Router-telnet.pl, 173–176
Cleaver, Jack
Jackson tarpit written by, 215
client access licenses (CALs)
required for Windows honeypots, 91
CM utility
for documenting and monitoring networks, 276
website address, 276
CMOS BIOS
importance of password protecting, 101
settings for disabling booting from removable media, 100
code disassembly
overview of, 337–339
steps for becoming a competent disassembler, 338
code listing
for adding a static route to a multihomed Windows computer, 138
for adding proxies to Honeyd templates, 160
for adding service scripts to Honeyd templates, 159
banner text received from various Exchange Server Services, 83
basic syntax for using Dd.exe, 306
of Code Red worm buffer overflow exploit, 24
for configuring preprocessors in Snort, 260
for creating Honeyd templates, 155
for defining the default port state in Honeyd templates, 158
example of full syntax Declare statement, 342
example of Nmap entry for Windows 2000 server with SP2, 125
example of rules from Snort's Web-IIs.rules rule set, 262
examples of Dd commands, 307
of Honeyd.bat configuration file with multiple runtime configurations, 153
IIS virtual SMTP server banner text, 82
for listing all available storage devices and their GUIDs, 307
for loading Snort rule sets at runtime, 264
of Microsoft FTP Service login banner, 79
of ms-ftp.sh script mimicking a Microsoft FTP server, 183–187
for putting Snort into network IDS mode, 256
of sample Honeyd.bat file, 153
of a sample Honeyd configuration file, 162–165
of sample Snort configuration file, 265–267
for setting system variable for Honeyd templates, 160
showing Honeyd.log file entries, 134–135
showing sample Honeyd Exchange Server template, 161

for Snort command for fastest performance, 255
of source code for Cisco telnet session script, 174–176
of source code for Test.sh, 172–173
of source code for Test.sh modified for Windows, 173
source code for Web.sh script, 177–178
syntax for adding ports in Honeyd, 158–159
syntax for typical Snort rules, 260
Telnet Server Logon banner text, 80
for testing and troubleshooting Honeyd on the local host, 166
for testing nmapNT fingerprinting process, 27–28
for testing your Snort configuration file, 267
using Netcat to retrieve IIS HTTP headers, 81–82
using the SET command, 157
for Windows auto-run areas for honeypots, 98–99
Code Red worm
LaBrea tarpit developed in response to, 9
Cogswell, Bryce
monitoring utilities created by, 278–280
Cohen, Dr. Fred
website address, 21
Comcraft tap maker
website address, 44
ComLog utilities. *See also* commercial ComLog utility; open-source ComLog utility
disabling Windows File Protection to use, 281
website address, 23
command-line options
case-sensitivity of, 151
using in Honeyd, 151–152
command-line tools
using built-in in Ethereal utility, 249–250
commercial ComLog
function of vs. open-source ComLog, 281
Comp.exe
comparing two sets of files on command line with, 272
Computer Antivirus Researcher's Organization (CARO) naming convention
failure of, 291
Computer Associates
website address, 294
Computer Forensics, Cybercrime and Steganograph Resources
website address, 335
Computer Management window
configuring services in, 108–109
computer platforms
assembly language instructions on, 345–349
computer roles
defined, 68–72
configuration settings
documenting for honeypots, 98
configuring
Honeyd templates, 154–165
Jackpot SMTP tarpit, 216–218
service accounts to protect honeypots, 115–117
services in Computer Management window, 108–109
services in LocalSystem account, 115–116
services in Windows Computer Management Services window, 108–109
Snort, 252–268
Connection Type dialog box
in Cygwin Setup dialog box, 143
console keystroke loggers. *See* monitoring programs
CookieView tool
for decoding internal cookie data, 316
Coordinated Universal Time (UTC), 128
CREATE command
using to create a Honeyd template, 155–156
/Create options
table of for EVENTTRIGGERS command, 298
Crucial ADS
for listing alternate data streams, 313
Ctrl-C
ending a Netcat session with, 14
exiting Snort with, 255
Cute FTP, 178
Cygwin
adding directories to the system PATH statement after installation, 144
installing, 142–145
website address for downloading, 142
Cygwin Setup dialog box
choosing the Installation Directory dialog box in, 143

D

-d command-line parameter
displaying activity summaries in Honeyd with, 134
-d parameter
Snort command-line switch, 253–254

data analysis. *See also* forensic analysis
determining if attack was manual or automated, 302–303
for honeypots, 301–336
a structured forensic approach, 304–325
data backup
needed for operating a honeypot, 12
data capture
in honeypots, 36
keystroke logging programs, 22–23
methods for honeypots, 22–23
data collection
applications for collecting and prioritizing Windows log files, 288–290
importance of centralizing, 287–290
data control
for honeypots, 21–22, 36
data correlation
tools for honeynets, 293
data filtering
importance of, 291–293
data filtering tools, 291–292
DataGrab
for checking for IM services hacker activity, 317
data-link layer
in OSI model, 228
DataRescue's IDA Pro. *See* IDA Pro Disassembler and Debugger
Davis, Michael
porting of Honeyd to Windows environment by, 121
porting of Sebek from Unix to Windows by, 277
DBXpress tool
for recovering deleted e-mail files from Outlook Express databases, 315
DCF Software's Hard Disk Copy
website address, 308
dd --list command
for listing all available storage devices and their GUIDs, 307
Dd.exe command-line tool
example of Dd commands, 307
making copies of the hard drive with, 306–307
website address, 306
Debug register command
using, 347
Debug.exe disassembler
in Windows, 318
Debug.exe program
for seeing an example of Windows 16-bit registers, 346–348
use of by malware programs after initial exploitation, 349
Deception Tool Kit (DTK)
honeypot developed by Dr. Fred Cohen, 21
Decompilation Wiki
website address for links related to decompilation, 357
decompilers
mixed results from for malicious code disassemble, 338
default delay policy
for firewalls, 51
default folder locations
rejecting for honeypot software or applications, 103
default template
creating in Honeyd, 156
defined, 134
defense-in-depth security paradigm
importance of in procting a network, 8
deleted files and formatted disks
recovering after hackers exploit a system, 315
demilitarized zone (DMZ)
defined, 5
Developer.com Windows API Tutorial
website address, 343
DiamondCS forensic utilities
website address, 283
DiamondCS's Open Ports utility
website address, 276
DiamondCS's Port Explorer utility
for listing active listening ports, 276
Digital Detective's hashing tool
website address, 312
Directory Snoop
disk viewer program, 314
disassemblers
free, 356–357
importance of in malware code analysis, 353–357
disassembly
defined, 337
disassembly environment
importance of choice you make for, 360
disassembly practice
steps for code behavior analysis before disassembly, 360–361
disk viewers
programs, 313–314
using to search your entire hard drive, 313–314
disk-cloning software tools
for making copies of a hard drive, 306
shareware and commercial, 308
virtual machine options, 308–309
disk-copying tools. *See* disk-cloning software tools

DMZ. *See* demilitarized zone (DMZ)
DMZ placement
of honeypots, 57–58
DNS resolver
use of in TCP/IP communication session, 230
domain controller ports
list of common Windows 2000, 69–70
DOS Attack setting dialog box
in KFSensor honeypot, 211
DOS ATTRIB command
for locating hidden, system, and read-only files, 313
DOS DIR command
for listing all hidden files and folders, 313
Download Sites dialog box
in Cygwin Setup dialog box, 143
DPORT
memory variable useful in scripts, 171
DRA. *See* EFS data recovery agent
dynamic linking
function of, 342

E

-e parameter
Snort command-line switch, 253–254
early warning system (EWS) honeypot
for your network, 301–302
ECMAScript
international scripting standard JScript is based on, 170
Edit menu options
using in Ethereal protocol analyzer utility, 244
Edit Sim Banner dialog box
in KFSensor honeypot, 200
Editcap.exe
command-line capturing utility, 250
EditPlus text editor
website address, 357
eEye Digital Security
website address, 27
EFS. *See* Encrypting File System (EFS)
EFS data recovery agent
website address for information about, 107
Electronic Evidence Information Center
website address, 335
E-Mail Detective
for viewing and recovering AOL deleted or cached mail, 315
e-mail messages
tools for recovering after hacker attack, 315
emulated honeypot systems
benefits to deploying, 19
disadvantages of, 19–20
what you need to know, 63–65
emulation services
in KFSensor honeypot, 198–208
in PatriotBox honeypot, 212–214
emulation service scripts
feature in Honeyd, 132
website address for downloading, 132
EnCase software
website address, 308
Encrypting File System (EFS)
for encrypting and protecting files, 107–108
encryption
used by malware to hide infection, 358
endpoint mapper
Windows port 135 known as, 73
Engage Security
website address, 296
Ethereal Capture Options dialog box
setting options in, 245–246
Ethereal protocol analyzer utility
Analyze menu, 246–248
columns in top pane, 242
command-line version (Tethereal.exe), 250
data payload information in the bottom pane, 242
downloading and installing, 147–148
example of main screen with packet-capture data, 241
features of, 240–250
getting a quick distribution screen report with, 310
information in the middle pane, 242–243
Microsoft-specific display filters in latest version, 238
screen showing HTTP traffic on a port other than 80, 243
screen showing packets of a captured hacker session, 247
screen showing the TCP stream feature for a packet, 248
starting, 241
TCP Conversation screen, 246
TCP Stream feature in, 247–248
using all of the features together, 248
using Tcpdump or WinDump with, 249
using the built-in command-line tools, 249–250
using the features of, 244–248
viewing packet information in, 241–243
website address, 43
Ethernet cable
methods for constructing receive only, 44–45
Ethernet cards
WinPcap conflicts with some, 142

Ethernet switches
as honeypot network system devices, 46–47
Ethernet tap (sensor)
for hiding honeynet monitoring devices, 44–45
event ID528
example of, 320
event IDs
list of interesting for logon events, 322–323
website address for information about, 323
Event Properties dialog box
event description information in, 321
Event Viewer
example showing filtering successful logins, 291
Event Viewer Microsoft Management console
for collecting and prioritizing Windows log files, 288
EventCombMT application
for remotely collecting multiple security log files, 288–289
website address, 288
Eventlog to Syslog Utility
for copying Windows event log messages to remote Syslog servers, 290
EVENTTRIGGERS command
syntax for, 298
table of /Create options, 298
Eventtriggers.exe program
for creating, deleting, listing, and querying trigger events, 298–299
EWS honeypot. *See* early warning system (EWS) honeypot
Exchange Server
banner text received from various Exchange Server Services, 83
Exchange Server ports, 83
lists of common and complex, 71–72
Exchange Server SMTP banner text
vs. IIS virtual SMTP server banner text, 83
Exchange Server template
example code listing for, 161
Exchange sim server
for KFSensor honeypot, 203–204
executable code pathway
example of, 338
executable files
list of potentially dangerous, 107
Exploiting Software: How to Break Code (Greg Hoglund and Gary McGraw)
book about disassembly, 359
external placement
of honeypots, 55–56
EXTERNAL_NET variable
syntax for using in Snort, 258

F

Faketelnet.pl script
website address, 179
false-negatives
as number one reason for using honeypots, 5–7
false-positives
as number one reason for using honeypots, 5–7
Fc.exe
using to compare two sets of files on command line, 272
feature packs
for specific applications, 101
Febotti Command Line utility
website address, 299
File and Printing Service
NetBIOS services as the heart of, 73–74
file extensions
learning which are associated with which programs, 314
file handle
defined, 344
file hashing programs
website addresses for, 312
File Investigator
for determining a files real content, 314
File menu options
using in Ethereal protocol analyzer utility, 244
file properties analyzer
Forensic Toolkit as, 281
file system
analyzing for malicious activity, 311–317
looking for hidden files and alternate data streams in, 313
file types
confirming in network traffic analysis, 314
FileCheckMD5
website address, 312
Filemon monitoring utility
function of, 279
FileStat
analyzing file systems with, 312
filters
needed by network analysis tools, 238
FIN (Finish) flag
in TCP, 234
FIN port scans
keywords for allowing and disallowing, 156–157
FIN scan
use of by hackers, 236
FINALeMail tool
for recovering Outlook Express and Eudora e-mail, 315

fingerprinting
active, 27–28
as part of manual hacking attacks, 26–30
passive, 29
firewalls
as honeypot network system devices, 51
importance of in stopping hackers, 8
forensic analysis
in action, 325–332
beginning by taking the honeypot offline, 305
of honeypot data, 301–336
making copies of the hard drive, 306–309
recovering RAM data in Windows honeypots, 305–306
reviewing log files for logon/logoff activity, 319–322
steps for a structured approach, 304–305
a structured approach, 304–325
forensic analysis toolkits
website address for overview of all major, 324
forensic analysis tools
bootable forensic distributions, 324
for documenting and analyzing honeypot systems, 280
needed for operating a honeypot, 12
web sites for, 335
Forensic and Incident Response Environment
website address for bootable forensic distribution, 324
Forensic Toolkit
file properties analyzer, 281
Foundstone utilities
website address, 276, 280, 335
Foundstone's Bin Text utility
for finding text and Unicode strings in a file, 318
Foundstone's Galleta tool
for examining contents of Internet Explorer cookies, 316
Foundstone's NTLast utility
for keeping track of logon information, 321
Foundstone's Pasco tool
for tracking Internet Explorer hacker activity, 316
Foundstone's Rifiuti utility
for examining Recycle Bin activity, 315
Fport and Vision utilities
for collecting network traffic baseline data, 276
looking for new network ports and services with, 319
frag attack
defined, 124
reasons for using, 233
Frag2 preprocessor
in Snort, 259
FRAGMENT instruction
in Honeyd templates, 157
Fragment Offset field
in IP packet, 232
fragmentation attack. *See* frag attack
freeware
defined, 122
FTP login session
Windows event log message generated by, 211
FTP server daemon
most popular used on the Internet, 168
FTP sim standard server
behavior, 202–203
for KFSensor honeypot, 202–203
FTP Windows service
ports used by, 79–80
ftp.sh script
website address, 180

G

Galeta tool
for examining Internet Explorer cookies, 280
gawk
website address for downloading Windows version, 188
generic Windows server ports
list of, 68–69
GenI honeypots, 21–24
vs. GenII model, 24–26
problems with, 24
GenII honeypot
vs. GenI honeypots, 24–26
model, 24–26
setup, 25
GenII honeywall
released by the Honeynet Project, 25–26
GFI LANguard Security Event Log Monitor
function of, 289
GhostRAdmin remote-access trojan
website address, 333
Gibson, Steve
Small Is Beautiful (SIB) assembly language starter kit by, 353
SpinRite written by, 339
GlobalSCAPE's Cute FTP
tarball unzipper, 178
website address, 178
Grimes, Roger
website address, 166
Group NetBIOS names, 74
Group Policy Objects (GPOs)
using to enforce security, 119–120
website address for information about, 119

Group Policy Resource Center
website address, 119
guest accounts
renaming to protect your honeypots, 117
Guild's FTP Server
website address, 202

H

hackers
attracting to your honeypot, 37
defined, 7
hacking activity
redirecting to protect systems, 8
Hacking Disassembly Uncovered (Kris Kaspersky, et al.)
book on disassembling malicious code, 359
hacking prevention
effect of honeypots on, 8–10
hardware
Windows OS minimum and hardware requirements, 95–96
hardware solutions
for hiding honeynet monitoring devices, 44–45
HD95Copy
website address, 308
Helix bootable forensic distribution
website address, 324
Hex2dec converter
website address, 318
hexidecimal-to-decimal converter
using Sysinternal's Hex2dec as, 318
HFind tool
for finding hidden files and alternate data streams, 313
hidden files and alternate data streams
looking for in file system, 313
utilities for finding, 313
High Level Assembler (HLA)
created as a learning tool for programmers, 352
high-interaction honeypots
determining need for, 90
function of, 14
Hogle trojan virus
website address, 207
Hogwash
website address, 52
HOME_NET variable
syntax for using in Snort, 258
Homename utility
website address, 311
Honeycomb research tool
website address, 7
Honeyd (honeypot daemon)
creating a default template in, 156
creating a runtime batch file in, 152–154
creator of, 10
default directories, 145
default scripts in Windows version of, 172
downloading script files, 146
emulation of ICMP behavior by, 128
example with multiple templates, 134
features of, 123–136
installation, 121–149
IP stack emulation settings in, 123–124
list of simple port behaviors, 131
logging, 134–136
memory variables useful in scripts, 171
mimicking IP information in, 124
mimicking TCP/IP stack in, 124–126
on-screen logging, 135
OS personalities, 129–130
output fields for on-screen logging, 134
proxy services, 132
reasons for using, 122–123
recommended directories, 148
runtime options, 152
steps for a typical installation, 136
steps for installing, 145
steps for testing your installation, 145–146
subsystems and plug-ins for Unix, 133
TCP/IP port emulation, 131–134
website address, 121, 123
Honeyd configuration, 151–166
using command-line options, 151–152
Honeyd configuration files
adding port instructions to, 158–160
assembling templates in, 161–165
sample code list for, 162–165
setting up, 154–165
setting up virtual honeypots (templates) in, 154
syntax for, 171–172
testing, 165–166
Honeyd emulation service scripts, 132
Honeyd installation
deciding logistics, 137–139
default directories, 145
installing Cygwin, 142–145
installing WinPcap, 140–142
resolving local subnet problems, 138–139
resolving routing problems, 138
steps for, 145
steps for hardening the host, 139
steps for testing, 145–146
Honeyd log files
fields included in default, 135
using the -l parameter to enable, 134–135
Honeyd logging
choices, 134–136
Honeyd OS personalities, 129–130
Honeyd runtime command
example of, 152

Honeyd script files
steps for downloading, 146
Honeyd service scripts, 167–188
available from Honeyd.org, 179–180
basic tasks they can be used for, 167–172
to catch the MBlaster worm, 181
common languages for, 168–170
custom, 180–188
default in Windows version, 172
downloadable from Honeyd web site, 178–180
input/output routines, 170–171
memory variable useful in, 171
for an offensive response to the MBlaster worm, 181–182
using JavaScript for, 170
using Python for writing, 169
using shell command language for, 168
using Visual Basic languages for, 169–170
a worm catcher script, 180–181
Honeyd simple port behaviors
list of, 131
Honeyd templates
adding personality instructions to, 156–157
adding port instructions to, 158–160
adding proxies to, 160
adding service scripts to, 159
blocking certain ports in, 159
code example for creating, 155
configuring, 154–165
contents of, 133–134
creating, 155–156
defining the default port state in, 158
for an Exchange Server 2003 honeypot, 161
naming rules, 155
order for defining necessary parameters, 154–155
personality defined, 156
setting system variables for, 160
Honeyd.bat configuration file
example of with multiple runtime configurations, 153
Honeyd.config file
recommended logical order of templates in, 154
Honeyd.org
service scripts available at, 179–180
Honeydscan.tar script
website address, 179
Honeyd.tar script
website address, 179
honeynet monitoring devices
hardware solutions for hiding, 44–45
software solutions for hiding, 42–43
Honeynet Project
formed by Lance Spitzner, 21
function of, 3
future generations of honeypot technology, 26
Honeynet Project Scan of the Month
website address, 248
honeynet security console
Activeworx Security Center (ASC) as, 294
honeynets
defined, 5
example of, 6
example of complex IP address scheme, 54
system network devices for, 41–54
honeypot daemon. *See* Honeyd (honeypot daemon)
honeypot data analysis. *See also* data analysis
investigations, 302–304
honeypot deployment
in Windows, 89–120
honeypot emulation software
function of, 18–20
honeypot farm
defined, 9
honeypot interaction levels, 14–15
honeypot layers
function of, 13–14
honeypot modeling
what you need to know, 63–65
in Windows, 63–88
honeypot monitoring, 269–299
honeypot network system devices
bridges as, 46
Ethernet switches as, 46–47
firewalls as, 51
hubs as, 41–45
summary, 52–54
honeypot placement
location comparison table, 59
honeypot platform
deciding what OS to use as, 89
honeypot system deployment
steps for, 35–36
honeypot system placement
main locations for, 54–59
honeypot systems
defined, 35
modifying and redeploying, 324–325
honeypot traffic
as malicious traffic, 3–4
honeypots
attracting hackers to, 37, 95
automated vs. manual attacks, 302–303
automating security for, 119–120

availability of OS software support tools for, 93
basic components of, 11–12
blocking certain ports in, 159
choosing real or virtual, 39–40
common reasons for using, 5–11
configuring service accounts to protect, 115–117
creating and storing user accounts on, 94
The Cuckoo's Egg by Clifford Stoll's about, 20
data capture, 22–23, 36
data control, 21–22, 36
deciding on research or production, 37–39
deciding to patch or not patch OS on, 93
deciding to run as client or server, 93
deciding which applications to install on, 94
deciding which OS to choose for, 90–93
defined, 3–5
defining goals for, 37–41
deployment in Windows, 89–120
deployment plan, 35–59
deployment steps, 35–36
design tenets, 36
determining need for high interaction, 90
determining the number of collected network packets, 309
disabling unneeded services on, 108–117
documenting configuration settings for, 98
emulated, 18–20
external placement of, 55–56
filtering network traffic on, 105–106
firewall DMZ placement, 57–58
as forensic tools, 10
function of high interaction, 14
function of low interaction, 14
general installation guidelines, 99
guidelines for reducing your legal risk, 33
history of, 20–26
hub network devices, 41–45
identifying the IP addresses and top talkers, 309–310
importance of using complex passwords, 118
improving computer security with, 10
information resources, 33
initial compromise of, 303
installation guidance, 96–100
installation steps to deploy and operate, 97
installation tips, 99–100
installing necessary patches to, 101
internal placement, 56–57
introduction to, 3–34
modifying and redeploying after analysis, 324–325
monitoring, 269–299
monitoring programs for, 277–283
need for licenses for all virtual machines, 18
need for update plan for, 90
new threat detection by, 7
physically securing, 100–101
placement summary, 58–59
potentially dangerous executable files list, 107
preferred by hackers, 94–95
production, 8
of real operating systems, 15–16
recommended hardware requirements for, 96
rejecting default folder locations for software, 103
removing or securing network shares before making live, 104–105
renaming administrator and guest accounts for, 117
research, 8
restricting unauthorized software execution on, 106–117
risks of using, 32–33
a sample deployment of, 11
scenarios for high levels of exploitation, 94–95
summary of other available Windows based, 220
summary of types, 20
system network devices, 41–54
taking baseline measurements for, 98–99
telltale signs of a manual attack on, 303
telltale signs of an automated attack on, 302–303
testing, 97–98
things they can mimic, 13
tools for recovering e-mail messages, 315
tracking the hackers, 311
types of, 13–20
using IPSec as a firewall on, 105–106
using real OS or virtual machine, 90
using Software Restriction Policies with, 107
using Symantec's Norton Ghost to restore, 16
virtual, 16–20
VM installation guidelines, 99–100
web site addresses for hardening information, 40–41
what happens after initial compromise, 303–304
Windows based, 61–220
Windows OS minimum and hardware requirements, 95–96
Windows-based other than Honeyd, 189–220

"Honeypots: Are They Illegal?" paper (Lance Spitzner)
website address, 33
Honeypots book
by Lance Spitzner, 21
Honeypots.net
website address for list of honeypots, 219
Honey-Potter
website address, 219
honeytoken
ensuring early detection of threats with, 7
honeywall. *See* honeywall gateways
Honeywall Administration menu
for Honeynet Project, 52
honeywall gateways
benefits of, 51–52
for redirecting malicious activity, 9–10
use of in GenII model, 24–26
HoneyWeb-0.4 tgz script
website address, 179
host baseline programs
for documenting current computer settings, 272–275
host documentation tools, 272–275
host enumeration
defined, 77–78
hot fixes, 101
HTTP header
using Netcat to read, 81–82
Http_decode preprocessor
in Snort, 259
hub network device
for honeypots, 41–45
using to create a honeynet, 42

I

IBM
website address, 294
ICMP. *See* Internet Control Message Protocol (ICMP)
ICMP behavior
emulation of by Honeyd, 128
ICMP fingerprinting
use of ICMP by hackers for, 237
website address for presentation about, 29
IDA Pro Disassembler and Debugger
classes for using to disassemble malware, 318
for doing detailed code analysis, 318
example disassembling Netlog1.exe instructions, 354
function of, 353–355
logic diagram, 355
website address, 353
Identification field
in IP packet, 232
identification number
for IP packets, 124
IDSs
benefits of using in a honeypot environment, 225–226
flexible alerting mechanisms in, 226
importance of in stopping hackers, 8
vs. sniffers, 223–224
IDSs and sniffers
how they complement each other, 226
where to place them, 226
if argument
in Dd.exe command-line syntax, 307
IIS
components of, 80–81
versions and related operating systems, 81
IIS directory structure
default folder and subfolder locations of an IIS installation, 82
IIS server ports
list of common, 69
IIS sim server
KFSensor honeypot, 201–202
IIS virtual SMTP server banner text
vs. Exchange Server SMTP banner text, 83
IIS virtual SMTP servers, 82–83
IIS web emulation script
for a simple emulated IIS 5.0 web page, 176–178
iisemu18.pl script
website address, 180
IM activity and file trading
tools for checking for hacker activity, 317
IM Grabber
for checking for IM services hacker activity, 317
Implementing CIFS, "Introduction"
website address, 77
in-band monitoring
advantages of, 276
vs. out-of-band monitoring, 276
inband monitoring tools
defined, 90
InCtrl5 (PC Magazine) utility
function of, 283
website address, 283
information system resource
honeypot as, 3
InfoWorld
website address for summary article about SIM/SEM, 294
initial sequence number (ISN)
Honeyd creation of, 127
inline IDS
implementation of, 24
input/output routines
support in Honeyd service scripts, 170–171

Installation Directory dialog box
in Cygwin Setup dialog box, 143
installation tips
for installing honeypots, 99–100
installing
Snort, 252
IntegCheck utility
file system integrity checker, 282
integrity checkers (snapshot software), 23
intelligent bridges. *See* bridges
internal placement
of honeypots, 56–57
Internet Connection Firewall (ICF)
using to filter network traffic on your honeypot, 105–106
Internet Control Message Protocol (ICMP). *See also* ICMP behavior; ICMP fingerprinting
for troubleshooting network connections, 237
Internet Explorer
tools for tracking hacker activity, 316
Internet Protocol (IP)
fields that need inspecting during a forensic investigation, 231–232
packet structure, 231
Internet Protocol version 6 (IPv6). *See* IPv6 (Internet Protocol version 6)
internet simulation environment, 10–11
Intrusion Inc. tap maker
website address, 44
iOpus Software's STARR
spying program, 317
IP. *See* Internet Protocol (IP)
IP addresses
assigning for honeypots, 43
obscuring of by intervening routers, 171
tools for finding hosts without, 43
IP addressing
and network emulation in Honeyd, 128–129
IP Filtering feature
enabling in Honeyd, 139
on all Microsoft Windows NT-based OSs, 106
IP Flags field
in IP packet, 232
IP information
mimicking in Honeyd, 124
IP (Instruction Pointer) register
of particular interest to malicious hackers, 348
IP Security (IPSec)
Windows default encryption communication's protocol, 284
IP stack emulation
in Honeyd, 123–130
settings in Honeyd, 123–124
IPList utility
for enumerating network interfaces, 283
IPOST
memory variable useful in scripts, 171
IPSRC
memory variable useful in scripts, 171
IPv6 (Internet Protocol version 6)
use of by hackers inside IPv4 traffic, 8

J

Jackpot SMTP tarpit, 214–219
configuring, 216–218
console screen showing SMTP connection activity, 218
installing, 216
as Java-based antispam relay server, 9
main administration screen, 219
running, 218–219
settings to automate trapping and tracking spam, 215–216
as sticky honeypot, 9
website address, 9, 215
written by Jack Cleaver, 215
JavaScript
using for Honeyd service scripts, 170
JpegDump tool
for recovering deleted JPEG files, 315

K

KaZaA .dat Viewer
for viewing and managing KaZaA data, 317
Kerberos
hardening a Windows machine with, 118–119
kernel mode programs
use of to attack honeypots, 345
KeyFocus Ltd.
HTTP engine that runs as a freeware web server, 202
website address, 196
keystroke logger
needed for operating a honeypot, 12
used for honeypot data capture, 22–23
keystroke monitoring programs
used for honeypot data capture, 22–23
KFSensor honeypot
analysis of Ethereal capture files, 326–329
anti-DoS setting dialog box, 211
capture showing Windows Media Service buffer overflow attack, 330
configuring listeners and anti-DoS settings, 210–211
Edit Sim Banner dialog box in, 200
emulated IIS 6.0 Under Construction error page, 202
emulating services with, 198–208

Ethereal generated protocol distribution report, 327
Event Details screen for an FTP session, 204
example of SMTP sim standard server screen, 204
forensic analysis in action, 325–332
function of, 196
IIS sim server, 201–202
initial review, 325–326
installation versions, 201
installing and running, 197–198
by KeyFocus Ltd., 196
lessons learned from attacks, 331–332
listing of event column fields, 209
log detail for one of the attacks, 329
log example showing an FTP login session, 210
logging and alerting with, 208–210
logs of the spam open relay, 331
logs showing the first IIS attack, 328
monitor in Ports view, 199
NetBIOS sim banner server, 205
open proxy server for, 205
open-relay attack, 330
other emulated Microsoft services offered by, 207–208
scenarios for sim standard server listener ports, 201
sim banner server banner parameters list, 200
sim banner servers in, 199–200
sim standard servers in, 200–201
SMTP alert configuration dialog box, 208
SMTP sim standard server, 203–204
SQL Server SA password-guessing attack, 330
Terminal Server sim standard server, 207
types of sim servers, 198
website address, 196
Windows Media Service buffer overflow attack, 329–330
KFSensor Monitor
function of, 197
KFSensor Server
function of, 197
KFSensor Set Up Wizard
components (port listeners) selection, 197
Kiwi Syslog
function of, 290
website address, 290
Knoppix bootable forensic distribution
website address, 324
Know Your Enemy (Lance Spitzner)
honeypot book, 8
Kuang2.pl script
website address, 179
-l <*logfiledirectory*> Snort parameter
for logging packet traffic to an ASCII text file, 255

L

LaBrea tarpit
developed in response to Code Red worm, 9
getting a list of all command-line options for, 191
installing and running, 191
as sticky honeypot, 9
using, 191–192
website address, 9, 190
Lan Manager (LM) protocol
weakness of, 118–119
layer 2 bridge devices
Ethernet switches as, 46–47
layer 2 bridging
implementation of, 24
LibnetNT
needed to run LaBrea tarpit, 191
website address, 191
licenses
needed for operating honeypots, 18
Linux-based Bait and Switch Honeypot
website address, 10
listening ports
listing all with Netstat.exe, 276
LiveScript. *See* JavaScript
LM password hashing
website address for information about disabling, 119
LM protocol. *See* Lan Manager (LM) protocol
Local Computer Policy object
accessing, 119
Local Package Directory dialog box
in Cygwin Setup dialog box, 143
local subnet problems
fixing in Honeyd installations, 138–139
LocalService account, 116
LocalSystem account
configuring services in, 115–116
log file formats, 290–291
log files
analyzing, 319–323
reviewing logon/logoff activity, 319–322
useful information extraction from, 294
Log Parser
in the Microsoft IIS 6 Resource Kit, 289
website address, 289
log protection
in honeypots, 295
log rotation and permanence
importance of, 287

log tools
for detecting various types of intrusions, 282
logging
of data captured from honeypot monitoring systems, 284–285
in-band methods, 284
out-of-band methods, 284
logging and alerting
with KFSensor honeypot, 208–210
with PatriotBox honeypot, 214
with SPECTER honeypot, 194–195
Logon event properties
fields in the Event Properties dialog box, 320
logon events
list of interesting IDs, 322–323
reviewing log files for, 319–322
logon/logoff activity
reviewing log files for, 319–322
LogProc utility
function of, 282
LogShares utility
function of, 282
LogStartup utility
function of, 282
LogUser utility
function of, 282
Longhorn. *See* Microsoft Longhorn
low-interaction honeypots
function of, 14–15

M

MAC address
changing for VM network interface card, 100
machine/assembly language instructions
common 80x86, 348
Macro Assembler. *See* MASM (Macro Assembler)
mail servers
Exchange Server as most popular, 83
malicious code
analyzing, 317–318
performing string analysis on, 317–318
malicious programming techniques, 358–359
malicious programming tutorials
list of available, 359
malware attack
analyzing packet time distribution for, 310
malware code analysis, 337–361
debugging tricks, 359
executable code pathway, 338
an overview of code disassembly, 337–339
of registers, 346–348
Malware: Fighting Malicious Code (Ed Skoudis and Lenny Zeltser)
book about malware vectors, 359
management workstation
needed for operating a honeypot, 12
man-in-the-middle attacks, 127
manual hacking models
function of, 26–30
MASM (Macro Assembler)
example showing disassembly of the Thing Trojan, 351
function of, 350–352
sampling of disassembly of Thing Trojan, 352
MBlaster worm
Honeyd used to catch, 180–181
script used to clean from originating hosts, 182
MBlaster.sh script, 181
media access control (MAC) address, 43
memory variables
useful in Honeyd scripts, 171
Mergecap.exe
for combining multiple capture longs into one log file, 250
MessageLabs antispam resource
website address, 304
Microsoft Audit Collection System (MACS)
website address for information about, 289
Microsoft Foundation Classes (MFC)
C++ API libraries for coders to use, 342
Microsoft FTP
characteristics of, 79
Microsoft FTP server
creating by customizing an existing script, 183–188
Microsoft FTP Service login banner
code example, 79
Microsoft Longhorn
availability of, 92
Microsoft network model
website address for information about, 227
Microsoft patches
different levels of, 101–103
patching pathway, 102
to protect against Blaster worm, 87
tools for checking status, 101
Microsoft POP3 server
emulated by KFSensor honeypot, 208
Microsoft Security Baseline Analyzer tool
website address, 101
Microsoft Security web site
website address, 41
Microsoft sharing
NetBIOS services as the heart of, 73–74
Microsoft Software Update Services (SUS)
using to update virtual systems, 17

Microsoft tools
for documenting baseline measurements, 271
Microsoft Visual Basic (VB). *See* Visual Basic (VB)
Microsoft Windows
hardening for your honeypots, 100–120
Microsoft Windows ports and services
list of common, 66–68
Microsoft's Automated Deployment Services
website address, 306
Microsoft's ExMerge utility
for recovering deleted e-mail when Outlook uses Exchange Server, 315
Microsoft's Virtual PC
undo disks in, 100
monitoring
after a baseline has been documented, 276–283
monitoring communications
protection for, 284
monitoring devices. *See* honeynet monitoring devices
monitoring programs, 277–283
monitoring/logging tools
needed for operating a honeypot, 12
MS03-026 patches
to protect against Blaster worm, 87
Ms-ftp.sh script file
mimicking a Microsoft FTP server, 183–187
multicast packets
defined, 41
Mydoom.pl script
website address, 179

N

NAT. *See* Network Address Translation (NAT)
NAT routing
example of, 48
National Security Agency
website address, 40
nbtscan enumeration tool
website address, 77
NET SEND command
for sending short console messages in Windows, 296
Net Send Command Line utility
website address, 299
NET SEND console alert message
example of, 298
NetBEUI protocol, 75
NetBIOS Auditing Tool
website address, 77
NetBIOS Datagram Service
port for sending data, 76
NetBIOS enumeration tools
website address, 77
NetBIOS Extended User Interface (NetBEUI), 75
"NetBIOS: Friend or Foe?"
website address, 77
NetBIOS names
command for listing local, 75
understanding, 74–75
NetBIOS operations, 75–77
NetBIOS over TCP/IP (NetBT or NBT), 75
NetBIOS ports
list of, 76–77
NetBIOS services
importance of Windows honeypot running or emulating, 73–78
list of common suffixes, 74
list of resources, 77
NetBIOS Session Service
port for sending data, 76
NetBIOS sim banner server
for KFSensor honeypot, 205
NetBIOS/CIFS attacks, 77–78
Netcat tunnel
function of, 281
Netcat utility
command for logging probes to port 21, 14
creating a simple port listener with, 14
website address, 14, 81
netForensics
website address, 294
Netmon (Network Monitor) utility
for collecting network traffic baseline data, 275
Netscape
development of JavaScript by, 170
Netsky worm
website address, 265
Netstat.exe
listing all active listening ports with, 276
looking for new network ports and services with, 319
Network Address Translation (NAT)
function of, 47–48
network analysis
and the OSI model, 229
network device hardware
needed for operating a honeypot, 11
network emulation
and IP addressing in Honeyd, 128–129
Network General Sniffer
packet-capturing program, 43
network layer
in OSI model, 228
Network Neighborhood
NetBIOS services as the heart of, 73–77
network packet protocol analyzers. *See* sniffers
network packets
performing string analysis on, 311

network protocol analyzers. *See also* sniffers
  network traffic capturing basics, 239–240
network protocol basics, 227–239
network protocol capturing
  basics of, 239–240
Network Security
  SPECTER honeypot by, 192
Network Service account, 116
network shares
  removing or securing, 104–105
Network Sniffer's Netasyst Network Analyzer
  website address, 246
network system devices. *See* honeypot network system devices
network traffic
  analysis of, 223–268
  capturing basics, 239–240
  filtering, 105–106
network traffic analysis
  analyzing malicious code, 317–318
  analyzing packet time distribution, 310
  analyzing the file system, 311–317
  analyzing the operating system, 318–319
  confirming file types, 314
  determining number of collected packets, 309
  discerning patterns in, 310–311
  doing detailed code analysis, 318
  drawing conclusions from, 324
  filtering by packet size, 310
  for honeypot systems, 309–311
  identifying the IP addresses and top talkers, 309–310
  learning which ports were involved, 310
  tracking Internet Explorer hacker activity, 316
network traffic baselines
  utilities for collecting data, 275–276
NISER Computer Forensics Laboratory
  website address, 335
Nmap active fingerprinting tool
  for fingerprinting OSs, 124–125
  website address, 27
Nmap documentation
  website address, 156
nmapNT active fingerprinting tool
  website address, 27
nmapNT fingerprinting process
  code example for testing, 27–28
Nmap.prints file
  in Honeyd, 125–126
  website address for updated, 151
NMapWin
  website address, 27
Norton Ghost. *See* Symantec's Norton Ghost
Norton System Utilities
  for recovering deleted files and formatted disks, 315
Nslookup.exe program
  resolving an IP address to a domain name with, 311
NT Objective's ntoinsight's
  website address, 316
NTFS permissions
  restricting access to the application folder and files with, 106–107
NTLast utility
  keeping track of logon information with, 321
  Windows security log analyzer, 281
NTLM authentication
  using to review log files for logon/logoff activity, 319
NTLMv2 protocol
  securing authentication protocols with, 118–119

O

of argument
  in Dd.exe command-line syntax, 307
OllyDbg disassembler
  function of and website address, 356
on-screen logging
  in Honeyd, 135
Open Ports utility
  for listing active listening ports, 276
  looking for new network ports and services with, 319
  website address, 276
open proxy server
  for KFSensor honeypot, 205
open relays
  sources of, 206–207
  what happens to, 207
open source software
  defined, 122
Open System Interconnection (OSI) models. *See* OSI models
Open Watcom assembler
  website address, 352
open-source ComLog utility
  function of, 281
open-source Windows forensics tools
  website address, 335
operating system
  analyzing as part of your network traffic analysis, 318–319
  checking for pending file changes, 319
OS personalities
  IP stack characteristic emulations as, 129–130

OSI model
example of, 228
importance of in network analysis, 227–229
network analysis and, 229
website address, 227
OSI models
within OSI models, 224–225
Oudot, Laurent
Honeyd used by to catch MBlaster worm, 180–181
website address for MBlaster worm article, 181
Outlook for Web Access
for retrieving e-mail, 83
OutlookRecovery tool
for recovering e-mail from Outlook PST files, 315
out-of-band monitoring
advantages of, 277
defined, 90
vs. in-band monitoring, 277

P

-p parameter
defined, 138
P0f tool
website address, 29
Packages dialog box
in Cygwin Setup dialog box, 143–144
packers
used by malware to hide infection, 358–359
packet analyzer
needed for operating a honeypot, 12
packet capturing
implementation of, 24
packet filters
commercial alternative products to building your own, 246
packet injectors
using to exactly duplicate hacker's actions, 224
packet size
filtering network traffic by, 310
packet time distribution
analyzing, 310
packing
used by malware to hide infection, 358
parsers
needed by network analysis tools, 238
Pasco utility
for documenting and analyzing honeypot systems, 280
Passdump utility
function of, 283
passive fingerprinting
function of and tools for, 29
passive fingerprinting tool
POf website address, 43
passwords
importance of using complex for user accounts, 118
password-stealing trojan script
website address, 179
patch management tools
availability of, 101
patches. *See* Microsoft patches
pathping utility
fooled by Honeyd network emulation, 129
PatriotBox honeypot
creating custom port listeners in, 214
emulating services in, 212–214
interface and HTTP configuration dialog box, 213
logging and alerting with, 214
website address, 212
PC hardware
pros and cons of writing directly to, 344
PC Magazine's InCtrl5 utility
function of, 283
PE Explorer disassembler
example disassembling Netlog1.exe, 356
function of, 355–356
website address, 355
PE files. *See* Portable Executables (PE files)
PE file segments, 349
PendMove utility
website address, 319
Performance Monitoring console. *See* Windows Performance Monitoring console
Perkeo program
for finding hidden pornography files, 317
Perl
using for Honeyd service scripts, 168
website address for information about, 168
permissions
checking for changes in files and folders, 314
Perms.exe utility
for checking permissions, 314
personalities. *See also* Windows personalities
annotating, 156–157
associating a template with, 157
personality instructions
adding to Honeyd templates, 156–157
Photo Retriever tool
for recovering deleted multimedia files, 315
physical layer
in OSI model, 228
Pictuate program
for finding hidden pornography files, 317

Ping of Death attacks
use of ICMP by hackers for, 237
website address for information about, 237
POF utility
using to identify remote computers, 311
website address, 311
pop3.sh script
website address, 180
popping
information to the stack, 348
port analysis
in network traffic analysis, 310
port emulation
TCP/IP in Honeyd, 131–134
Port Explorer utility
looking for new network ports and services with, 319
website address, 276
port instructions
adding to Honeyd templates, 158–160
port listeners
creating custom in PatriotBox honeypot, 214
Foundstone's Attacker, 190
using to create low-interaction honeypots, 14–15
port mirroring (port spanning), 23
using with a managed switch, 46–47
port scans
use of by hackers, 235–236
port spanning. *See* port mirroring (port spanning)
Portable Executables (PE files)
website address for tutorials on, 349
Windows 32-bit executables known as, 348–349
ports
common Windows applications and their, 86–87
common Windows listening TCP by platform, 85–86
common Windows listening UDP by platform, 84
ports and services
common ports by platform, 83–86
list of common for Windows, 66–68
PORTS variable
syntax for using in Snort, 258
Portscan preprocessor
in Snort, 259
preprocessors
in Snort, 259
presentation and application layers
in OSI model, 229
Process Explorer monitoring utility
function of, 280
investigating processes or services with, 319
ProDiscover software
website address, 308
production honeynet
example of, 38
production honeypots
complexity of, 39
defined, 8
function of, 37–39
setting up IP addressing for, 38–39
programming interfaces
choices available, 340
pornography
programs for finding hidden on exploited computers, 317
protocol analyzer utilities
downloading and installing Ethereal, 147–148
features of Ethereal, 240–250
Microsoft-specific display filters in latest version, 238
Protocol Type field
in IP packet, 233
Provos, Dr. Niels
Cisco telnet session script created by, 174–176
creator of Honeyd honeypot, 10
website address, 121
website address for MBlaster worm document, 181
proxy services
adding to Honeyd templates, 160
in Honeyd, 132
proxying
defined, 160
PSH (Push) flag
in TCP, 234
PsTools monitoring utilities
investigating processes or services with, 319
list and functions of, 280
public domain software
defined, 122
pushing
information to the stack, 348
Putty SSH program
website address, 284
Python
using for Honeyd service scripts, 169

R

RDP protocol
used by Windows Terminal Server and related services, 78
real honeypots
choosing over virtual, 39–40
Realtime-Spy
spying program, 317

receive-only Ethernet cable
methods for constructing, 44–45
wiring schematic for, 45
redirectors
redirecting malicious activity with, 9–10
RegisterEventSource function
for writing to the Windows Application log, 341
registers
in Intel processors, 346
Registry
checking for changes to autorun keys and, 319
Registry key
enabling before creating a Windows STOP error, 305–306
RegistryProt utility
for real-time monitoring of Registry activity, 283
Regmon monitoring utility
function of, 279
relevancy
defined, 10
Remote Administrator
website address, 333
remote computers
utilities for identifying, 311
Remote Desktop
in Windows XP, 78
Remote Desktop for Administration
in Windows Server 2003, 78
Remote Desktop Protocol (RDP)
remotely managing Windows 2000 and above computers with, 284
remote-access trojans (RATs)
dropped by Bugbear worm, 77–78
installed on the WhiteDoe honeypot, 333
use of in blended attacks, 31–32
removable media
disabling booting from in CMOS BIOS, 100
repeater. *See* hub network device
research honeypots
complexity of, 39
defined, 8
function of, 39
research resources
needed for operating a honeypot, 12
Rifiuti tool
for examining content of the Info2 file in the Recycle Bin, 280
Robinton, Michael
LaBrea tarpit developed by, 190
Roesch, Martin
Snort network packet analysis tool written by, 250
rooted tree network topology model
Windows version of Honeyd limited to, 128–129
rootkits
use of in blended attacks, 31
routers
capabilities of, 48–49
example of simple segment IP address scheme, 53
as layer 3 network devices, 47
Router-telnet.pl script
example of in action, 174
routing tables
displaying local, 49
function of, 49–50
RPC patch
for Blaster worm, 73
RPC services
understanding, 72–73
RST (Reset) flag
in TCP, 234
Rstack team
Honeyd used by to catch MBlaster worm, 180–181
Rugrat virus
website address, 93
rule sets
list of Snort default, 263
RULE_PATH variable
checking for forward slashes in the default Snort.conf file, 259
Russinovich, Mark
monitoring utilities created by, 278–280

S

SafeBack software
website address, 308
SANS
website address, 318
Sbk_extract tool
for collecting Sebek packets for analysis, 278
Sbk_ks_log.pl
Perl script for displaying attacker keystrokes on the screen, 278
Sbk_upload.pl
Perl script that uploads Sebek packets for advance analysis, 278
scanning scripts
use of in blended attacks, 31
scenarios
for sim standard server listener ports, 201
script files
steps for downloading for Honeyd, 146
script languages
common, 168–170

scripts. *See* Honeyd service scripts; service scripts
\scripts folder
  Honeyd Windows version default scripts in, 172
Search or Find Files and Folder Windows feature
  using to find files modified since a certain date, 312
Sebek
  monitoring tool for Windows honeypots, 277
  website address, 23, 277
Sebek server
  tools that make up, 278
Secure Hash Signature Generator
  website address, 312
SecurIT Informatique Inc. utilities
  example of several monitoring system processes, 282
  for honeypot or IDS data collection, 281–282
  others available, 282
  website address, 281
SecurIT Intrusion Detection Kit
  components of, 282
security
  automating, 119–120
  using honeypots to improve, 10
Security Assertion Markup Language (SAML)
  website address, 291
security audit files
  events of interest in, 292–293
security event logging
  of data captured from honeypot monitoring systems, 284–285
  importance of for honeypots, 285–286
  useful information extraction from, 294
Security Event Management. *See* SEM (Security Event Management)
security event manager
  Activeworx Security Center (ASC) as, 293–294
Security Incident Management. *See* SIM (Security Incident Management)
security logs
  noise on, 6
security monitoring tools
  as protection for monitoring communications, 284
security patches. *See* Microsoft patches
security roll-ups, 101
security updates or hot fixes, 101
SecurityProfiling, Inc.
  website address, 121
sed
  website address for downloading Windows version, 188
SEM (Security Event Management)
  vendors, 294
Sendmail utility
  function of, 283
  setting up a spam tarpit with, 215
  website address, 215
sequence number field
  in TCP, 233
server ports
  list of common complex Exchange Server, 71–72
  list of common IIS, 69
  list of common simple Exchange Server, 71
  list of common SQL Server, 70
  list of generic, 68–69
SERVER variable
  using in Snort, 258
ServerSentry utility
  website address, 299
service accounts
  configuring to protect your honeypot, 115–117
service pack patches, 101
service scripts. *See also* Honeyd service scripts
  adding to Honeyd templates, 159
  in Honeyd, 167–188
session layer
  in OSI model, 229
SET command
  for associating a template with a personality, 157
SFind utility
  for listing NTFS alternate data streams and their access times, 313
SHA-160 Hash utility
  function of, 283
shareware
  defined, 122
shell command language
  using for Honeyd service scripts, 168
  website address for information about, 168
Showacls.exe utility
  for checking permissions, 314
ShoWin utility
  function of, 281
SIM (Security Incident Management)
  vendors, 294
sim banner servers
  in KFSensor honeypot, 199–200
  list of banner parameters, 200
sim (simulated) servers
  in KFSensor honeypot, 198–208

sim standard servers
emulated services included with, 201
in KFSensor honeypot, 200–201
simple ports
defined, 131–132
Simple TCP/IP services
provided in a TCP/IP add-on component, 78
slack space
storage of malicious code in by hackers, 345
Slammer worm
website address, 303
Small Is Beautiful (SIB) assembly language starter kit
by Steve Gibson, 353
SMB protocol
as workhorse of NetBIOS, 73
SMTP sim standard server
example of screen, 204
SMTP tarpit
Jackson tarpit as, 215
smtp.sh script
website address, 180
Smurf amplification
use of ICMP by hackers for, 237
Smurf attacks
website address for information about, 237
snapshot software. *See* integrity checkers (snapshot software)
snapshot utilities
website addresses for free, 23
sniffers
availability of, 224
benefits of using in a honeypot environment, 223–225
vs. IDSs, 223–224
sniffers and IDSs
how they complement each other, 226
where to place them, 226
Snort
benefits of using in a honeypot environment, 225–226
binary log file, 256
command for fastest performance, 255
configuring, 252–268
configuring the configuration file, 257–264
creating a Snort.bat file, 267
deciding what you want it to do, 253–256
default variables list, 257
defining variables in, 257
directories and their functions, 252
example of alert file, 262
example of rules from Snort's Web-IIs.rules rule set, 262
exiting to finish with a packet statistics screen, 255
in full packet capture mode, 255
function of, 250–268
installing, 252
list of some preprocessors, 259
packet pathway, 251
sample configuration file, 265–267
steps for configuring the first time, 252
steps for installing, 146–147
syntax for configuring preprocessors, 260
understanding how it works, 250–251
website address for community support, 250
website address for downloading, 146
website address for downloading GUI-based installers and management tools for, 268
Snort configuration file
configuring, 257–264
sample of, 265–267
testing, 267
Snort GUI ISDcenter configuration console
from Engage Security, 296
Snort network IDS mode
putting Snort into, 256
Snort output plug-ins
function of, 264
Snort packet dump mode
command-line switches, 253–254
fields captured on TCP packets, 254
Snort point-and-click
using, 268
Snort rules
function of, 260
syntax fields list, 262
syntax for typical, 260
Snort rule sets
list of default, 263
Snort.bat file
creating, 267
Snort-inline
website address, 52
software
restricting unauthorized execution of on honeypots, 106–117
software interrupts. *See* BIOS interrupt routines
Software Restriction Policies (SRP)
for preventing unauthorized software execution, 107
software solutions
for hiding honeynet monitoring devices, 42–43
Software Update Services (SUS). *See* Microsoft Software Update Services (SUS)
SONET backbone
function of, 224–225

spam malware
effect on open relays, 207
spam tarpits
setting up, 215
spammers
how they work and the damage they do, 206–207
using Jackpot tarpit to slow down and frustrate, 9
SPECTER honeypot
characters available for each emulated OS, 193
function of, 192–195
installing and setting up, 193–194
Log Analyzer tool, 195
logging and alerting with, 194–195
main Control screen, 194
on-screen log, 195
traps and services, 192
website address, 192
SpinRite
for recovering damaged hard drive data, 339
Spitzner, Lance
Honeypots book by, 21
Know Your Enemy honeypot book by, 8
SPORT
memory variable useful in scripts, 171
SpyAgent software
for checking for IM services hacker activity, 317
spying programs
website addresses for, 317
SQL Server ports
list of common, 70
SQL Slammer worm
defenses against, 10
detection of, 7
function of, 30
SRP. *See* Software Restriction Policies (SRP)
Ssed program
for extracting text, 318
using, 188
SSH programs
for protecting monitoring communications, 284
SSH test script, 172–173
stack
popping and pushing of information to, 348
Startup type settings. *See* Windows Services Startup type settings
static linking
defined, 342
STDERR (standard unbuffered output stream for writing errors)
in Honeyd, 171
STDIN (standard input stream)
in Honeyd, 170
STDOUT (standard buffered output stream)
in Honeyd, 170
stealth mechanisms
used by malware to hide infection, 358
sticky honeypots
preventing malicious activity with, 9
Stoll, Clifford
The Cuckoo's Egg by, 20
STOP error
creating intentionally, 305–306
stream4 preprocessor
in Snort, 259
string analysis
performing on packets, 311
Strings.exe program
example revealing text strings in a malicious file, 350
searching for ASCII text with, 350
website address, 311, 350
SubSeven emulation service
used by PatriotBox honeypot, 212
SuperDIR
website address, 312
switches. *See* Ethernet switches
Symantec's Norton Ghost
for making copies of a hard drive, 306
using to restore honeypots, 16
Symantec's Norton System Utilities
disk editor program, 314
SYN (Synchronization) flag
in TCP, 234
SYN flood DoS attack
use of by hackers, 235
Sysdiff
website address, 23, 272
Sysinternal PsTools utilities
list and functions of, 280
Sysinternal utilities, 278–280
website address, 278
Sysinternal's AccessEnum utility
for listing who has permissions to files, Registry keys, and folders, 314
Sysinternal's Hex2dec
using as hexidecimal-to-decimal converter, 318
Sysinternal's Hostname utility
for resolving an IP address to a domain name, 311
Sysinternal's PendMove utility
checking for OS pending file changes with, 319
Sysinternal's Stream program
for listing any hidden NTFS streams by file or directory, 313

Sysinternal's Strings.exe program
for performing string analysis on network packets, 311
Sysinternal's Strings utility
for searching for ASCII and Unicode strings, 318
Sysinternal's TCPView utility
website address, 276
Syslog (system log daemon)
for collecting log files, 289–290
system network devices
for honeypots, 41–54
system variables
setting for Honeyd templates, 160

T

TamoSoft SmartWhois query tool
website address, 311
taps
using in hubs and bridge scenarios, 46
tarball unzippers
for the Windows platform, 178
tarpits (blackholes)
as sticky honeypots, 9
TCP Conversation screen
in Ethereal protocol analyzer utility, 246
TCP flags
list of, 234
used in a TCP connection session, 126–127
TCP packets
timestamp for, 127–128
TCP packet structure
example of, 233
TCP ports
common Windows listening by platform, 85–86
TCP Stream feature
in Ethereal protocol analyzer utility, 247–248
TCP window size
function of, 126
tcpdump utility
using with Ethereal protocol analyzer utility, 249
website address for downloading, 249
TCP/IP configuration
documenting for your honeypot system, 270
TCP/IP packet types
list of, 125–126
TCP/IP pathway
basic function of, 230–232
TCP/IP port emulation
in Honeyd, 131–134
TCP/IP ports
website address for comprehensive listing of, 65
TCP/IP protocol
flow example, 231
reliability of vs. UDP, 234
three-way handshake process, 234–236
use of vs. UDP, 236–237
TCP/IP protocol suite
basics of, 230–237
TCP/IP stack
mimicking in Honeyd, 124–126
recommended registry entries to harden, 104
TCPView utility
for listing listening network ports, 276
Telnet Server (Tkbtsvr.exe)
availability of, 80
Telnet Server Logon banner text
code example, 80
Telnet_negotiation preprocessor
in Snort, 259
templates
in Honeyd, 154
TCP/IP port setting recommendations, 133–134
Terminal Server
included starting with Windows Server 2000, 93
Terminal Server sim standard server
in KFSensor honeypot, 207
Terminal Services, Application Mode
in Server 2003, 78
Test2pcap.exe
for converting an ASCII hexidecimal dump to a tcpdump-style log, 250
Test.sh
source code for, 172–173
Tethereal.exe
command-line version of Ethereal utility, 250
text editors
website addresses for, 357
TextPad text editor
website address, 357
The Cuckoo's Egg (Clifford Stoll)
about honeypots, 20
The Disk Investigator program
disk viewer, 314
The Shellcoder's Handbook: Discovering and Exploiting Security Holes
book exploring different ways to secure your system, 359
Thing Trojan
MASM disassembly of showing called Windows APIs, 351
sampling of MASM disassembly of, 352
website address, 350
third-party APIs
using, 343–344

threats
ensuring early detection of with honeytokens, 7
time synchronization
importance of for security logging of honeypots, 285
timestamp
for TCP packets, 127–128
tools
for finding hosts without IP addresses, 43
for making copies of a honeypot hard drive, 306–308
top talkers
identifying in network traffic analysis, 309–310
Tower of Babel problem
of establishing common names for viruses, 292
traceroute utility
fooled by Honeyd network emulation, 129
Tracking Hacker's web site
website address, 219
Transmission Control Protocol (TCP)
packet structure, 233
transport layer
in OSI model, 229
traps and services
in SPECTER honeypot, 192–193
Tribble
hardware-based solution for capturing and storing RAM data, 306
trigger events
command for displaying, 298
Tripwire program
website address, 23, 272
troubleshooting
your Honeyd configuration files, 165–166
TUCOFS-The Ultimate Collection of Forensic Software
website address, 335
TYPE
memory variable useful in scripts, 171

U

UDP packet structure
example of, 236
UDP ports
common Windows listening by platform, 84
use of by hackers and malicious programs, 234
undo disks
in Microsoft's Virtual PC, 100
undoable disks
in VMware, 100
unicast packets
defined, 41
Unique NetBIOS names, 74
Unix
Honeyd subsystems and plug-ins for, 133
Uptime utility
function of, 283
UPX packer
website address, 358
URG (Urgent) flag
in TCP, 234
USB ports
disabling unneeded in the CMOS BIOS, 100–101
user accounts
protecting for your honeypots, 117–118
User Datagram Protocol (UDP). *See also* UDP ports
use of in NetBIOS traffic, DNS queries, 236–237
use of vs. TCP, 236–237
"Using Microsoft Windows IPSec to Help Secure an Internal Corporate Server"
website address for presentation about, 106
UTC. *See* Coordinated Universal Time (UTC)
UTP port doublers, 45
UTP Y-adapters, 45

V

-v parameter
Snort command-line switch, 253–254
van Rossum, Guido
development of Python language by, 169
VBScript
website address for information about, 170
version number field
in IP packet, 232
virtual honeypot host
steps for hardening, 40–41
virtual honeypots
setting up templates for, 154
types of, 16–20
virtual machine honeypots
function of, 16–18
VMware as, 39–40
virtual networks
creating with Honeyd, 10–11
virus rules sets
reasons for using, 265
Vision and Fport utilities
for collecting network traffic baseline data, 276
Visual Basic (VB) languages
using for Honeyd service scripts, 169–170
VM honeypot
installation guidelines, 99–100

VMware
choosing between virtual and raw disk types in, 308
software, 16–18
as virtual machine honeypots, 39–40
website address, 16

W

W= parameter
defined, 126
war drivers
using wireless honeypots to detect, 9
Web.sh script
source code for, 177–178
website addresses
for 4-clause BSD license, 122
for Active@ UNDELETE program, 315
for Active@ UNERASER program, 315
for Activeworx, Inc., 293
for Advanced Attachments Processor tool, 315
Afind program, 312
for Akonix L7 Enterprise tool, 317
for AllAPI, 343
for "An Evening with Berferd" paper by Bill Cheswick, 20
ArcSight, 294
Argus for Linux, Unix, and Solaris users, 309
AT&T Mexican honeynet, 8
for author of this book, 166
for Back Officer Friendly (BOF) honeypot, 189
for Back2Life program, 315
Bait and Switch Honeypot, 10
Blat utility, 299
for bootable CD-ROM for GenII honeywall, 25
Bugbear worm, 77
for Cache Reader tool, 316
for CacheInfo tool, 316
for CacheX utility, 316
Center for Internet Security, 40
CM utility, 276
Comcraft tap maker, 44
ComLog utilities, 23
for common NetBIOS enumeration tools, 77
for community support for Snort, 250
for comprehensive listing of TCP/IP ports, 65
Computer Associates, 294
Computer Forensics, Cybercrime and Steganograph Resources, 335
for CookieView tool, 316
Crucial ADS, 313
for DataGrab, 317
for DBXpress tool, 315
DCF Software's Hard Disk Copy, 308
Dd.exe command-line tool, 306
for a detailed discussion on IPSec, 106
for details about SRP, 107
for the Developer.com Windows API Tutorial, 343
DiamondCS forensic utilities, 283
DiamondCSOpen Ports utility, 276
DiamondCSPort Explorer utility, 276
Digital Detective's hashing tool, 312
for Directory Snoop, 314
for disabling Windows File Protection, 281
for disk editor programs, 314
for The Disk Investigator program, 314
for downloading ActivePerl Perl engine, 145
for downloading a Honeyd configuration file, 161
for downloading Cygwin, 142
for downloading GUI-based installers and management tools for Snort, 268
for downloading Honeyd emulation scripts, 132, 146
for downloading MASM, 350
for downloading ms-ftp.sh script, 183
for downloading Snort, 146
for downloading tcpdump utility, 249
for downloading the Windows version of gawk, 188
for downloading the Windows version of sed, 188
for downloading WinDump utility, 141, 249
Dr. Fred Cohen, 21
for ECMAScript scripting standard, 170
EditPlus text editor, 357
eEye Digital Security, 27
Electronic Evidence Information Center, 335
for E-Mail Detective, 315
EnCase software, 308
Engage Security, 296
for Ethereal install executable, 147
Ethereal network protocol analyzer, 43
EventCombMT application, 288
for Eventlog to Syslog Utility, 290
Exploiting Software: How to Break Code (Greg Hoglund and Gary McGraw), 359
for Faketelnet.pl script, 179
Febotti Command Line utility, 299
File Investigator, 314
FileCheckMD5, 312
for FINALeMail tool, 315
Foundstone utilities, 276, 280, 335
for Foundstone's Attacker, 190
Foundstone's Bin Text utility, 318

for Foundstone's Fport and Vision utilities, 276
for Foundstone's Galleta tool, 316
for Foundstone's NTLast utility, 321
for Foundstone's Pasco tool, 316
for Foundstone's Rifiuti utility, 315
for ftp.sh script, 180
for GFI LANguard Security Event Log Monitor, 289
GhostRAdmin remote-access trojan, 333
for GlobalSCAPE's Cute FTP, 178
for Guild's FTP Server, 202
Hacking Disassembly Uncovered (Kris Kaspersky, et al.), 359
HD95Copy, 308
HFind tool, 313
for High Level Assembler (HLA), 352
for Hogle trojan virus, 207
Hogwash, 52
Honeycomb research tool, 7
Honeyd (honeypot daemon), 121
for the Honeyd Development web site, 33
for Honeydscan.tar script, 179
for Honeyd.tar script, 179
for the Honeynet Project, 33
Honeynet Project Scan of the Month, 248
for the Honeynet Project's Scans of the Month, 324
for "Honeypots: Are They Illegal?" paper (Lance Spitzner), 33
for Honeypots: Tracking Hackers honeypot information, 33
for Honeypots.net, 219
for HoneyWeb-0.4 tgz, 179
IBM, 294
IDA Pro Disassembler and Debugger, 318
for iisemu18.pl script, 180
for IM Grabber, 317
Implementing CIFS, "Introduction", 77
InCtrl5 (PC Magazine) utility, 283
for information about disabling LM hashing, 119
for information about EFS data recovery agent, 107
for information about event IDs, 323
for information about EVENTTRIGGERS command, 299
for information about GPOs, 119
for information about JavaScript or JScript, 170
for information about Perl, 168
for information about Ping of Death attacks, 237
for information about settings for hardening TCP/IP stacks, 104
for information about Smurf attacks, 237
for information about VBScript, 170
for information about Visual Basic languages, 170
for information about Windows command-line shell language, 169
for information about Windows STOP errors, 306
for InfoWorld summary article about SIM/SEM, 294
Intrusion Inc. tap maker, 44
Jackpot SMTP tarpit, 9
for JpegDump tool, 315
for KaZaA .dat Viewer, 317
KeyFocus Ltd. KFSensor honeypot, 196
for KeyFocus's HTTP engine that runs as a web server, 202
KFSensor honeypot, 196
Kiwi Syslog, 290
for Kuang2.pl password-stealing trojan script, 179
LaBrea tarpit, 9, 190
for the latest Honeyd version, 123
for learning which file extensions are associated with which programs, 314
LibnetNT, 191
list of BIOS interrupt routines, 341
for a list of disassemblers, 357
for Log Parser in Microsoft IIS 6 Resource Kit, 289
for MACS security event log collection information, 289
Malware: Fighting Malicious Code (Ed Skoudis and Lenny Zeltser), 359
for the MBlaster worm, 181
for MBlaster worm article by Laurent Oudot, 181
for MBlaster worm document by Dr. Niels Provos, 181
MessageLabs antispam resource, 304
for Michael Davis, 121
for Microsoft network model information, 227
Microsoft Security Baseline Analyzer tool, 101
Microsoft Security web site, 41
for Microsoft's Automated Deployment Services, 306
Microsoft's ExMerge utility, 315
for more hashing program alternatives, 312
for Mydoom.pl script, 179
National Security Agency, 40
nbtscan enumeration tool, 77
Net Send Command Line utility, 299
NetBIOS Auditing Tool, 77
NetBIOS enumeration tools, 77
"NetBIOS: Friend or Foe?, 77
for NetBIOS information, 77

website addresses *(continued)*
for NetBIOS name suffix information, 74
Netcat utility, 14, 81
netForensics, 294
for Netsky worm, 265
for Network General's Sniffer, 43
for Network Sniffer's Netasyst Network Analyzer, 246
NISER Computer Forensics Laboratory, 335
Nmap active fingerprinting tool, 27
for Nmap documentation, 156
nmapNT active fingerprinting tool, 27
NMapWin, 27
for Norton System Utilities, 315
NT Objective's ntoinsight's, 316
Open Ports utility, 276
Open Watcom assembler, 352
for open-source Windows forensics tools, 335
for OSI model, 227
for OutlookRecovery tool, 315
for packers, 358
for PatriotBox honeypot, 212
for PE Explorer disassembler, 355
for Perkeo program, 317
for Photo Retriever tool, 315
for Pictuate program, 317
for POf passive fingerprinting tool, 43
POF utility, 311
for pop3.sh script, 180
for Pop.emulator.tar.gz script, 180
for presentation about ICMP fingerprinting, 29
ProDiscover software, 308
Provos, Dr. Niels, 121
Putty SSH program, 284
Remote Administrator, 333
Rugrat virus, 93
SafeBack software, 308
Sebek, 23
Secure Hash Signature Generator, 312
SecurIT Informatique Inc. utilities, 281
Security Assertion Markup Language (SAML), 291
for SecurityFocus honeypot mailing list, 166
SecurityProfiling, Inc., 121
Sendmail, 215
ServerSentry utility, 299
SFind utility, 313
for shell command language information, 168
The Shellcoder's Handbook: Discovering and Exploiting Security Holes, 359
Slammer worm, 303
for Small Is Beautiful (SIB) assembly language starter kit, 353
for smtp.sh script, 180
Snort-inline, 52
for SpinRite, 339
for SpyAgent software, 317
for Ssed program, 318
Strings.exe program, 350
SuperDIR, 312
for Symantec's Norton Ghost, 306
Symantec's Norton System Utilities, 314
Sysdiff, 272
for Sysinternal's Hostname utility, 311
Sysinternal's PendMove utility, 319
Sysinternal's Stream program, 313
for Sysinternal's String.exe program, 311
for Sysinternal's Strings utility, 318
Sysinternal's TCPView utility, 276
TamoSoft SmartWhois query tool, 311
TCPView utility, 276
TextPad text editor, 357
Thing Trojan, 350
for Tracking Hacker's web site, 219
for Tribble, 306
TUCOFS-The Ultimate Collection of Forensic Software, 335
for tutorials on PE files and their structure, 349
for Unix version of Tripwire program, 23
for updated Nmap.prints file, 151
UPX packer, 358
for "Using Microsoft Windows IPSec to Help Secure an Internal Corporate Server", 106
for utilities for checking permissions, 314
for virtual machine honeypots in forensic analysis whitepaper, 309
VMware, 16
for Webster's Art of Assembly Language tutorial, 346
for Webster's web site for assembler information, 353
Welchia worm, 182
WhatFormat program, 314
for WildPackets' EtherPeek NX, 246
for the Win32 API FAQ, 343
Winalysis, 274
Windiff, 272
Windows Forensic Toolchest (WFT), 274
for Windows GUI for nmapNT, 27
Windows implementation guides, 284
"Windows Internet Naming Service (WINS): Architecture and Capacity Planning", 77
Windows IT Pro magazine, 41
Windows Update Services (WUS), 102
for Windows version of Tripwire program, 272

WinDump utility, 309
Winfingerprint, 272
Winfo enumeration tool, 77
for Wingate proxy server, 206
Winhex software, 308
WinInterrogate, 272
WinMessenger utility, 299
WinPcap, 191
WinPcap packet capture driver, 43
for WinRAR tarball unzipper, 178
for WinZip tarball unzipper, 178
Xprobe2 active fingerprinting tool, 27
for Xprobe2 and fingerprinting article, 28
Webster's Art of Assembly Language
tutorial for learning assembly language, 346
Webster's HLA support page
website address, 352
Welchia worm
website address, 182
WhatFormat program
for determining a files real content, 314
website address, 314
WhiteDoe real honeypot
bogus .system directory in, 334
finding exploit code on, 332–335
hacker's malicious folder structure, 333
lessons learned from the attacks on, 335
R_bot.ini IRC configuration file, 334
whitehat vulnerability testing tools
coding of in Perl, 168–169
whois query tools
TamoSoft SmartWhois, 311
WildPackets' EtherPeek NX
website address, 246
Win32 API FAQ
website address, 343
Win32 API files
main for Windows core functionality, 342
Winalysis
snapshot comparison screen, 273
website address, 23, 274
Windiff
website address, 272
Window Size field
in TCP, 234
Windows
NET SEND command for sending short console messages in, 296
website address for implementation guides, 284
Windows 2000 domain controller ports
list of common, 69–70
Windows 32-bit executables
known as Portable Executables (PE files), 348–349
Windows API
housekeeping tasks handled by, 341
resources for learning how to use, 343
using, 341–343
Windows API files
searching for a larger list of, 342
Windows applications
common and their port numbers, 86–87
Windows command-line shell language
using for Honeyd service scripts, 169
Windows Computer Management Services window
configuring services in, 108–109
Windows event logging, 285–286
main auditing categories, 286–287
Windows event triggers
using, 298–299
Windows File Protection
disabling to use ComLog, 281
website address for disabling, 281
Windows Firewall
filtering network traffic on your honeypot with, 105–106
Windows Forensic Toolchest (WFT)
website address, 274
Windows honeypot deployment, 89–120
decisions to make for, 89
Windows honeypot emulation
common ports and services, 65–68
Windows honeypot modeling. *See also* honeypot modeling
port-related protocols and services review, 63–65
Windows implementation guides
website address, 284
"Windows Internet Naming Service (WINS): Architecture and Capacity Planning"
website address, 77
Windows IT Pro magazine
website address, 41
Windows Performance Monitoring console
using to collect network traffic baseline data, 275
Windows personalities
annotation syntax, 156–157
common choices of, 156
Windows platform
tarball unzippers for, 178
Windows ports and services
list of common, 66–68
Windows protocols, 237–239
Windows security audit files
events of interest in, 292–293
Windows security log analyzer
NTLast as, 280
Windows Server 2003
editions available in, 91

Windows server ports
list of generic, 68–69
Windows services
for honeypot modeling, 72–83
steps for hardening, 116–117
Windows Services Startup type settings
recommended on a Windows Server 2003 computer, 109–115
Windows STOP errors
creating intentionally, 305–306
website address for information about, 306
Windows TCP/IP stack
Microsoft use of a four-layer network mode to describe, 227
Windows Terminal Server
RDP protocol used by, 78
Windows Update Services (WUS), 17
checking for system patches with, 102–103
website address, 102
Windows workstation ports
list of common, 70
Windows XP
Remote Desktop in, 78
Windows-based honeypots
Honey-Potter as, 219
other than Honeyd, 189–220
WinDump utility
confirming successful installation of WinPcap with, 141–142
determining the number of collected network packets with, 309
using with Ethereal protocol analyzer utility, 249
website address, 309
website address for downloading, 141, 249
Winfingerprint
website address, 272
Winfo enumeration tool
website address, 77
Wingate proxy server
website address, 206
Winhex software
website address, 308
WinInterrogate
scanning local files, 274
website address, 272
WinMessenger utility
website address, 299
WinPcap
confirming successful installation of, 140–141
conflicts with some Ethernet cards, 142
needed to run LaBrea tarpit, 191
steps for installing using the auto-installer package, 140
website address, 43, 140, 191
WinRAR tarball unzipper
website address, 178
WinZip tarball unzipper
website address, 178
wireless access points (WAPs)
exploitation of weakly protected, 9
workstation ports
list of common Windows, 70
worm catcher script, 180–181
worm cleaners
problem with, 182
WU-FTPD daemon
developed at Washington University, 168

X

Xprobe2 active fingerprinting tool
for fingerprinting OSs, 124–125
website address, 27
XWhois utility
advanced domain registration query tool, 283

Y

Y-adapters
using in hubs and bridge scenarios, 46

Z

Zavdi, Moran
website address for Honey-Potter written by, 219
zombie trojans
defined, 304