

# Index

## Symbols

29A, 90-91

2in32::Lanman module, 441

## A

-a, 227

Aaron's Homepage, 438

Active Directory (AD), 117

troubleshooting with  
portqry, 395

ActiveState, 417

Perl installation, 418-422

Axiom Corporation, 18

AD. *See* Active Directory

Administrator passwords, 35

ADS (alternate data streams),

83-86, 88-90, 144

creating, 83

deleting while preserving

primary streams, 86

viruses, 90-91

and WFP, 144-145

adware, 269, 271

AFX Rootkit 2003, 349, 353

rkd.pl output when run against

an AFX Rootkit 2003 infected

system, 351-352

AFX Windows Rootkit 2003,

332-337

detecting, 338

AINTX Administrator Tools,

ps.exe, 199

AINTX toolkit, touch.exe, 76

alternate data stream. *See* ADS

Analyzer, 407-408, 410

packet captures, 410

analyzing

data with FSP, 377-378

*compromised Windows 2000*

*systems*, 385

*infected Windows 2003*

*systems*, 378-380

*rootkits on Windows 2000*

*systems*, 380, 384-385

files, 246

*executable files*, 246-255

anti-virus solutions, 147

anti-virus websites, 437-438

API (Application Programming

Interface), 417

AppleTree, 35

Application Configuration dialog,

IIS, 129

Application Programming

Interface (API), 417

assoc command, 56

at.exe, 323

Attack Vectors, 315

attacks. *See also* incidents

denial of service attacks, 274

ease of, 37-38, 50-52

W2K, 90-91

attributes, file attributes. *See*

file attributes

audit settings, 133-134

auditing Event Logs, 280

auditpol.exe, 134, 244

auto-rooters, 35

automatic incidents, 35

Autoruns, 319

AutoStart View, 319

## B

Back Orifice, 329

backdoors, 200, 272

locating as services, 330

open ports, 328-329

Registry keys, 325-327

services, 329-331

banner grabbing, 33

banners, returning from other

ports, 393

batch files, 118, 287

for configuring systems, 172,

174-177

Bejtlich, Richard, 441

Beyond-Security, SecuriTeam

site, 440

binding Notepad.exe and

Sol.exe, 82

BinText, 247

broadband connections, 10

buffer overflow vulner-

abilities, 316

## C

-c, 227

tlist, 197-198

cacls.exe, 229

case management component,

FSP, 365

CERT Coordination Center, 440

characteristics of incidents, 25

checksum, 301

client components

communicating with servers, 360

FSP. *See* FSP

clipboard contents, collecting

volatile information,

215-216

CLOSELOC, 359, 370, 376

cmdline.exe, 201-202

Code Red II, 141

Code Red worm, 36

collecting

data with FSP, 362

*file client component*, 373-377

*launching FSP*, 363-366

*running FRU*, 366, 369-370,

372-373

Event Log entries, 170

## 450 collecting

- non-volatile information, 224
  - collecting files*, 224-232
  - contents for the Recycle Bin*, 232-234
  - dumping Event Logs*, 244-246
  - Registry keys*, 235-237, 240
  - scheduled tasks*, 241
  - user information*, 241-243
- volatile information, 182, 358
  - clipboard contents*, 215-216
  - command history*, 216-217
  - with FSP*, 358
  - group policy information*, 220, 223
  - logged on users*, 185-186, 189
  - network information and connections*, 205-212, 215
  - process information*, 189-192, 194-195, 197, 199, 201-202
  - process memory*, 202-205
  - services and drivers*, 217-220
  - system time*, 183-185
- command history, collecting
  - volatile information, 216-217
- command line port scanners, portqry.exe, 394-396
- command line tools, 180
- command prompt, Windows XP Professional, 15
- commands
  - assoc, 56
  - CLOSELOG, 370, 376
  - dir /ah, 233
  - dir /ta, output of, 69
  - driverquery, 220
  - FILE, 376
  - ftype, 56
  - net file, 213
  - net session, 186, 213
  - net start, 217
  - openfiles, 214
  - PPM, 418-419
  - rifiuti, 234
- commercial tools, demo versions, 389
- complexity of Windows systems, 8-10
- compound files, 101-102
- Comprehensive Perl Archive Network (CPAN), 180, 420
- compromised systems, tools, 283
- computer forensics, 3
- computer security incidents. *See* incidents
- configuration of perimeter devices, 108-109
- configuring systems
  - with batch files, 172-177
  - with SCM, 112-116
- connections
  - high-speed connections, pervasiveness of, 10
  - network information and connections, 205
  - fport*, 209-210
  - ipconfig*, 205-206
  - nbtstat*, 209
  - net.exe*, 212, 215
  - netstat*, 207-208
  - openports*, 211
  - promiscdetect*, 206
- ConnectIPC() function, 49
- Coordinated Universal Time (UTC), 184
- copying files, 300-301
  - ensuring integrity of files, 229
  - FSP, 361
  - from a potentially compromised system, 225
  - from systems, 295
- corporate email addresses, public newsgroups, 271
- correlating data with FSP, 377-378
  - compromised Windows 2000 systems, 385
  - infected Windows 2003 systems, 378-380
  - rootkits on Windows 2000 systems, 380, 384-385
- CPAN (Comprehensive Perl Archive Network), 180, 420
- The Cuckoo's Egg*, 16
- Cult of the Dead cow, 329
- D**
- DACLs (discretionary access control lists), 132
- .dat file, example of contents, 375
- data
  - collecting with FSP, 362
  - file client component*, 373-377
  - launching FSP*, 363-366
  - running FRU*, 366, 369-370, 372-373
  - correlating and analyzing with FSP, 377-378
  - compromised Windows 2000 systems*, 385
  - infected Windows 2003 systems*, 378-380
  - rootkits on Windows 2000 systems*, 380, 384-385
  - hiding
    - in executables*, 104
    - in Office documents*, 95-97, 99-101
    - in the Registry*, 92, 94-95
    - steganography*, 102-104
  - hiding on live file systems
    - by changing file attributes*, 56-60
    - file binding*, 81-83
    - file segmentation*, 81
    - file signatures*, 62-63, 68
    - file times*, 68-72, 74-76, 78-80
    - hidden attribute*, 60-62
    - NTFS ADS*, 83-84, 86, 88-90
- data collection activities, 312
- DATA keyword, 359
- dd.exe, 204-205
- DebPloit (DEBugger exPLOIT), 27
- Debug Programs, 354
- defense in depth, 106
- The Defense of Duffer's Drift*, 261
- defenses against local incidents, 29
- deleting
  - ADS while preserving primary streams, 86
  - files, 299
- demo versions of commercial tools, 389
- denial of service attacks, 274
- Dependency Walker (depends.exe), 250-251
- depends.exe, 250-251

- detecting
  - file system changes, 59
  - open ports, port scanners. *See* port scanners
  - port scanners
  - rootkits, 337-351, 353
- di.pl Perl script
  - output of, 432
  - retrieving drive information, 430-431
- DiamondCD, OpenPorts, 211
- DiamondCS, 438
  - AutoStart Viewer, 319
  - cmdline.exe, 201-202
- digital signatures, verifying, 143
- dir /ah command, 233
- dir /ta command, output of, 69
- dir command, /t switch, 226
- directories, footprints, 318, 320-321
  - tasks.pl, 324
- disabling
  - script mappings, 130
  - WFP, 141-144
- discretionary access control lists (DACLS), 132
- displaying embedded strings, 246
- Dittrich, Dave, 441
- DLL injection, 354
- DLLs, 311
- documentation, 281-283, 287
- doskey, 216
- drawbacks of reinstalling systems, 259-260
- drive information, retrieving with di.pl Perl script, 430-431
- driverquery command, 220
- drivers
  - collecting volatile information, 217-220
  - WinPcap drivers, installing, 403
- dumpel.exe, 245
- dumping
  - Event Logs, collecting non-volatile information, 244-246
  - lists of workstations from PDC, 150-151
- Duronio, Roger, 17
- E**
- E-evidence Info, 440
- editors, Perl editors, 422-423
- EliteWrap, 81-83
- embedded strings, displaying, 246
- end points, 278
- EnumAccountPrivileges(), 125
- enumerating
  - contents of clipboard, 216
  - Registry key LastWrite times, 238
- Ethereal, 410-412
  - reading packet captures, 413-415
- Event Logs, 133-134, 298
  - auditing, 280
  - collecting entries, 170
  - dumping, 244-246
  - local incidents, 28
  - remote incidents, 31
- Event Viewer, 133
- EventComb MT, 245
- EventId.net, 437
- examples of incidents, 31
- Excel, hiding
  - data, 95
  - spreadsheets in Word documents, 101-102
- executable binders, 81
- executable files, analyzing, 246
  - with BinText, 247
  - with Dependency Walker, 250-251
  - with file version information (ver.pl), 248-249
  - with Microsoft Word documents, 252-254
  - with PDF documents, 254-255
  - with process memory dumps, 252
  - with strings.exe, 246
- executables, hiding data in, 104
- exploiting vulnerabilities, 51
- F**
- FBI2003.pdf, 255
- FDTE (File Date Time Extractor), 253-254
- file associations, viewing, 56
- file attributes
  - hiding date on live file systems, 56-60
  - malware, 58
- file binding, 81-83
- file client component, FSP, 373-377
- FILE command, 376
- File Date Time Extractor (FDTE), 253-254
- FILE keyword, 359
- file segmentation, 81
- File Selector dialog of file client component, 374
- file signatures, 62-63, 68
  - image files, 63
  - performing analysis of with Perl scripts, 64-67
- file systems
  - detecting changes in, 59
  - within a file, 101-102
- file times, 68-72, 74-76, 78-80, 225
  - modifying with touch.pl, 76-79
  - viewing, 68
- file version information
  - retrieving, 248
  - ver.pl, 248-249
- file-sharing programs, 269
- files
  - analyzing, 246
    - executable files*, 246-255
  - batch files, 287
  - collecting non-volatile information, 224, 226-227, 229-232
  - copying, 300-301
    - ensuring integrity of*, 229
    - with FSP*, 361
    - from a potentially compromised system*, 225
    - from systems*, 295
  - deleting, 299
  - footprints, 318, 320-321
    - tasks.pl, 324
  - getting off of servers, 294
  - researching, 291
  - searching for, 277
    - recently accessed files*, 320
  - tools for
    - examining files*, 258
    - obtaining information about*, 257
- FILETIME structure, 225
  - Registry keys, LastWrite times, 238
- firewalls, perimeter devices, 109

## 452 First Responder Utility (FRU)

- First Responder Utility (FRU), 324
- first responders, 310
- footprints, 317
  - files and directories, 318-321
    - Perl script*, 324
  - open ports, 328-329
  - processes, 327-328
  - Registry keys, 325-327
  - services, 329-331
- Forensic Acquisition Utilities, 439
- forensic audit, 3
- Forensic Server, 303
- Forensic Server Project. *See* FSP
- forensics, 3
- Forensics.nl, 439
- Forever worm, 141
- FoundStone, 438
- fport, 209
- fport, collecting network
  - information and connections, 209-210
- fport.exe, 284
- free port scanners, 32
- freeware, 179
- freeware tools, 389
- FRU (First Responder Utility), 324, 361-363, 378
  - Perl scripts to parse the output of tlist, pslist, and openports, 380-383
  - running, 366, 369-373
  - setting up, 367-369
- fru.pl, 361
- FSP (Forensic Server Project), 324, 358-362
  - case management
    - component, 365
  - client components, 360
  - collecting data, 362
    - file client component*, 373-377
    - launching FSP*, 363-366
    - running FRU*, 366, 369-373
  - copying files, 361
  - correlating and analyzing data, 377-378
  - compromised Windows 2000 systems*, 385
  - infected Windows 2003 systems*, 378-380
  - rootkits on Windows 2000 systems*, 380, 384-385
  - file client component, 373-377
  - future of, 385-386
  - initial configuration dialog
    - for, 364
  - launching, 363
  - Perl, 361
  - setting up, 364
- fsw.pl, 138-140
- FTP site properties, 131
- FTP traffic capture, 443-444
  - Ethereal, 413
- ftype command, 56
- functions
  - ConnectIPC(), 49
  - EnumAccountPrivileges(), 125
  - GetTimeZoneInformation(), 95
  - Parent import, 251
- G**
- Garner, Jr., George M., 439
- GatSlag, 317
- Geschonneck, Alexander, 440
- GetLocalTime(), 184
- GetSystemTime(), 184
- GetTimeZoneInformation(), 95
- GNU GPL (General Public License), 390
- Google, 436
- GoToMyPC, 18
- GPList, 220
- GPOs (group policy objects), 117, 220
- GPResult.exe, 220-222
- Group Policies, 117-118
- group policy information,
  - collecting volatile information, 220, 223
  - Protected Storage, 223
- group policy objects (GPOs), 117, 220
- GUI tools, 180
  - BinText, 247
- H**
- Handle.exe, 194
- hardening, 2
- hash.pl, 229-231
- hashes, 360
- help, PPM commands, 418
- Heyne, Frank, 439
- HFS (Hierarchical File System), 83
- hidden attribute, 60-62
- hiding
  - data
    - in executables*, 104
    - in Office document*, 95-101
    - in Registry*, 92, 94-95
    - steganography*, 102-104
  - date on live file systems
    - file attributes*, 56-60
    - file binding*, 81-83
    - file segmentation*, 81
    - file signatures*, 62-63, 68
    - file times*, 68-72, 74-76, 78-80
    - hidden attribute*, 60, 62
    - NTFS ADS*, 83-84, 86, 88-90
  - Word documents in Excel spreadsheets, 101-102
- Hierarchical File Systems (HFS), 83
- high-speed connections,
  - pervasiveness of, 10
- Hoglund, Greg, 332, 439
- host configuration, 111
  - NTFS file system, 111-112
  - SCM, 112-116
- Hydan, 104
- I**
- IDE (integrated development environment), 422
- IIS (Internet Information Server), 128
  - Application Configuration dialog, 129
- IIS traffic capture, 445
  - Ethereal, 414
- image files, file signatures, 63
- incident preparation, 106
  - anti-virus solutions, 147
  - audit settings, 133-134
  - Event Logs, 133-134
  - Group Policies, 117-118
  - host configuration. *See* host configuration
  - monitoring. *See* monitoring
  - patch management, 145-146
  - perimeter devices. *See* perimeter devices

- permissions, 132-133
- restricting services, 128-132
- user rights, 118-122, 126-128
- WFP, 134-137
  - and ADSs, 144-145*
  - Registry values, 140-144*
  - Windows 2000 SP2, 143*
- incident response policies, 285-288
  - investigating systems, 286
- incident response tools, 179
- incidents, 2, 23
  - Administrator passwords, 35
  - automatic incidents, 35
  - characteristics of, 25
  - Code Red II, 141
  - Code Red worm, 36
  - ease of attacks, 37-38, 50-52
  - examples of, 31
  - Forever worm, 141
  - investigating, 309-314
  - local incidents, 25-29
  - manual incidents, 34
  - policies, 37
  - programming errors, 36
  - real-life incidents, 16-19
  - reasons for occurring, 35, 37
  - remote incidents, 30-34
- InControl5, 299, 321
  - files added by `afx_example.exe`
    - installation, 335
- infection vectors, 314-316
  - limiting, 331
- INFO2, 233
- information
  - non-volatile information. *See* non-volatile information
  - volatile information. *See* volatile information
- initial configuration dialog for FSP, 364
- InPEct, 82
- Insecure.org, 438
- install, PPM commands, 419
- installation
  - of malware, preventing, 331
  - of rootkits, preventing, 353-354
- installing
  - Perl, 418-422
    - for use with this book, 426-430*
  - Perl modules, 420-422
  - WinPcap drivers, 403
- integrated development environment (IDE), 422
- integrity of files, ensuring, 229
- Internet Information Server. *See* IIS
- Internet Relay Chat (IRC), 2
- Internetwork Operating System (IOS), 108
- investigating
  - IP addresses, 263-268
  - systems, 286
  - unusual traffic, 263-268
- investigations
  - litigious investigations, 307
  - overview of, 309-314
- IOS (Internetwork Operating System), 108
- IP addresses, investigating, 263-268
- Ipconfig, collecting network information and connections, 205-206
- IRC (Internet Relay Chat), 2
- IRC bots, 224
- J-K**
- jdbgmgr.exe, 135
- Jiang, Juju, 18
- KartOO, 436
- Kaspersky Labs, 437
- KB (KnowledgeBase), 436
- kbAlertz.com, 436
- kernal-mode rootkits, 332
- keywords, 359
- KnowledgeBase (KB), 436
  - article 174073, 28
  - article 328691 MIRC Trojan
    - Realted Attack Detection and Repair, 315
  - article Q222192, 141
  - article Q230206, 27
  - article Q832017 Port Requirements for the Microsoft Windows Server System (*s/b ital*), 109
- Kwbot worm, 316
- L**
- LastWrite times, 238, 240
- launching
  - FSP, 363
  - netcat listener, 313
- LDAP (Lightweight Directory Access Protocol), 396
- liability, 284
- licensing issues, 179, 390
- Lightweight Directory Access Protocol (LDAP), 396
- limiting infection vectors, 331
- ListDLLs, 194
- listdlls.exe, 336
- LISTENING, 390-391
- listing
  - scheduled tasks, 324-325
  - sessions on local systems, 188
- listings
  - Batch file for configuring systems, 172, 174-177
  - Contnets of an example .dat file, 375
  - di.pl Perl script for retrieving drive information, 430-431
  - EliteWrap script for binding Notepad.exe and Sol.exe (Solitaire), 82
  - Example output of winapimac.pl, 74
  - Excerpt of case log file from file copy, 376
  - Fsw.pl Perl script for implementing a file system monitor, 138-139
  - Hash.pl, a Perl script that computes MD5 and SHA-1 hashes for a file, 229-230
  - Mdmscan.pl Perl script for locating modems, 156-158
  - Meta.pl Perl script for retrieving metadata from Microsoft Word documents, 96-98
  - null.pl Perl script, 38-40, 42-49
  - Output of commands run to determine the current date and time on the system, 183
  - Output of di.pl Perl script, 432
  - Output of dir /ah command, 233

## 454 listings

- Output of dir /ta command, 69
  - Output of gpresult.exe on a Windows 2000 system logged into a domain, 221-222
  - Output of pslist -t run on a Windows XP system, 193
  - Output of pslist run on a Windows XP system, 192
  - Output of pulist run on a Windows XP system, 190
  - Output of rifiuti command, 234
  - Output of rkd.pl Perl script when run against an AFX Rootkit 2003 infected system, 351-352
  - Output of tlist -c run on a Windows XP system, 197-198
  - Output of tlist -s run on a Windows XP system, 196
  - Pdfmeta.pl Perl script for retrieving metadata from PDF files, 254
  - Perl code excerpt for retrieving file MAC times, 69
  - Perl code listing for svelst.pl, 218
  - Perl script for performing file signature analysis, 64-67
  - Perl script for retrieving the MAC times of a file using Perl's stat() function, 226
  - Perl script tasks.pl for listing scheduled tasks, 324-325
  - Perl script that lists session on the local system, 188
  - Perl script to dump contents of the Clipboard, 215
  - Perl script to enumerate Registry key LastWrite times, 238
  - Perl script to parse the output of tlist, pslist, and openports from the FRU, 380-383
  - Perl script ver.pl, 297
  - Priv.pl Perl script to list user privileges, 124-125
  - Priv2.pl Perl script for retrieving users with a specific user right, 148-150
  - Result of pd.pl run on Windows 2000 system infected with a rootkit, 384
  - Rkd.pl Perl script for performing local and remote rootkit detection, 338-348
  - Runchk.pl Perl script for retrieving contents of Run key, 160-162
  - Sniffscan.pl Perl script for locating WinPcap drivers, 152-155
  - Touch.pl Perl script to demonstrate modifying a file's MAC times, 76-79
  - Tz.pl Perl script demonstrating how to retrieve time zone information, 93-94
  - Useraudit.pl Perl script for retrieving user information, 164-169
  - Users.pl, a Perl script to list the user accounts on a system, their last logon date, the number of times they've logged in, and the groups each account is a member of, 242
  - Ver.pl Perl script used to retrieve file version information, 248
  - Wfpgget.pl Perl Script to retrieve contents of specific Registry keys, 236
  - Winapimac.pl Perl script to demonstrate using the Win32 API to retrieve file times, 70-74
  - Wksdump.pl Perl script for dumping a list of workstations from the PDC, 150-151
  - litigious investigations, 307
  - Lloyd, Timothy, 17
  - local incidents, 25-29
  - Local Security Policy, Windows XP, 114
  - local systems, listing sessions, 188
  - locating
    - backdoors as services, 330
    - modems, 156-159
    - WinPcap drivers, 152-155
  - LOG, 359
  - log files, 289
  - logged on users, collecting
    - volatile information, 185
    - with net session command, 186
    - with netusers.exe, 186
    - with psloggedon.exe, 186, 189
  - logic bombs, 17
  - logon rights, Windows XP, 126-128
- ## M
- m, 227
  - MAC (media access control), 206
  - MAC times, 68, 227
    - Perl code excerpt for retrieving, 69
    - preserving, 226
  - mac.pl, 226
  - MACS (Microsoft Audit Collection System), 170
  - malicious software. *See* malware
  - malware, 2
    - file attributes, changing, 58
    - fingerprints, 317
      - file and directories, 318, 320-321, 324
      - open ports, 328-329
      - processes, 327-328
      - Registry keys, 325-327
      - services, 329-331
    - infection vectors, 314-316
    - local incidents, 26
    - persistency, 317
    - preventing installations, 331
  - managing patches, 145-146
  - manual incidents, 34
  - Map List, 439
  - mapping processes to ports, 278
  - Master File Table (MFT), 83
  - MBSA (Microsoft Baseline Security Analyzer), 145-146, 291
  - md5deep.exe, 229-231
  - MDF message digest, 360
  - mdmscan.pl, 156-159
  - media access control (MAC), 206
  - memory
    - process memory, collecting volatile information, 202-205
    - process memory dumps, 252
  - Merge Streams, 101



- meta.pl, retrieving metadata from Microsoft Word documents, 96-98
- metadata  
retrieving from PDF files, 254  
Word documents, 99-100
- methodologies, 310-311  
for incident response, 285-288  
*investigating systems*, 286  
investigating unusual traffic, 263-268
- MFT (Master File Table), 83
- Microsoft Audit Collection System (MACS), 170
- Microsoft Baseline Security Analyzer (MBSA), 145
- Microsoft Excel, hiding data, 95  
documents in Word documents, 101-102
- Microsoft Installer (MSI) file, 417
- Microsoft Internet Information Server. *See* IIS
- Microsoft KnowledgeBase (KB), 436
- Microsoft Management Console. *See* MMC
- Microsoft Office documents, hiding data, 95-97, 99-101
- Microsoft Resource Kits, 15
- Microsoft Security Bulletin MS02-24, DebPloit, 27
- Microsoft Systems Management Server (SMS), 404
- Microsoft Windows Application Programming Interface (API), 417
- Microsoft Word  
hiding data, 95  
*documents in Excel spreadsheets*, 101-102  
metadata, 99-100  
Microsoft Word documents, analyzing executable files, 252  
FDTE, 253-254  
WordDumper, 252  
Microsoft.com, 436
- MMC (Microsoft Management Console), 112  
SCM, 112  
Security Options settings, 113  
snap-ins, 118  
Windows XP MMC, Security Configuration and Analysis snap-in, 115
- modems, locating, 156-159
- modifying file MAC times with touch.pl, 76-79
- modules, Perl, 417-419  
CPAN, 420  
installing, 420-422  
Win32::API::Prototype, 428  
Win32::DriveInfo, 429  
Win32::File::Ver, 427  
Win32::FileOp, 429  
Win32::GUI, 428  
Win32::IPCConfig, 432  
Win32::Lanman, 426  
Win32::Perms, 428  
Win32::TaskScheduler, 426  
Win32::TieRegistry, 236
- monitoring, 147-148  
collecting Event Log entries, 170  
mdmscan.pl, 157-159  
*locating modems*, 156-158  
perimeter devices, 110  
Port Reporter, 171  
priv2.pl, 149-150  
*retrieving users with specific user rights*, 148
- runchk.pl, retrieving contents of Run key, 160-162
- sniffscan.pl, 153-155  
*locating WinPcap drivers*, 152-154
- useraudit.pl, retrieving user information, 164-169
- wksdump.pl, 151  
*dumping lists of workstations from the PDC*, 150
- Morris, Robert T., 16
- MS03-26, 19
- MSI (Microsoft Installer) file, 417
- MWC, Inc., Red Button, 50
- MZ file signature, 62
- N**
- nbtstat, collecting network information and connections, 209
- net file command, 213
- net session command, 186, 213
- net start command, 217
- net.exe, 279  
network information and connections, collecting, 212, 215
- netcap, 404-405
- netcat, 58, 294  
copying files, 301  
port scanners, 392-394
- netcat listener, launching, 313
- netcat traffic capture, 444  
Ethereal, 413
- netmon (Network Monitor), 404
- netstat, collecting network information and connections, 207-208
- netstat -ano, 208
- netusers.exe, 186
- network information and connections, 205  
fport, 209-210  
ipconfig, 205-206  
nbtstat, 209  
net.exe, 212, 215  
netstat, 207-208  
openports, 211  
promiscdetect, 206
- network interface card NIC, 206, 403
- network interface status, 206
- Network Monitor, 404
- network protocol analyzers. *See* sniffers
- network sniffers. *See* sniffers
- NIC (network interface card), 206, 403
- nmap, port scanners, 396-403  
nmap traffic capture, 446  
Ethereal, 415
- non-volatile information, 182  
collecting, 224  
*contents for the Recycle Bin*, 232-234

**456 non-volatile information**

- dumping Event Logs, 244-246*
- files, 224, 226-227, 229-232*
- Registry keys, 235-237, 240*
- scheduled tasks, 241*
- user information, 241-243*
- tools for retrieving, 257
- notes, 276
- NSA XP, workstation.inf security
  - template, 116
- NTFS, ADS, 83-86, 88-90
- NTFS file system, host
  - configuration, 111-112
- NTFS.com, 437
- NTRootkit, 352
- NTSecurity.nu, 438
- NTSecurity.nu sute,
  - pmdump.exe, 202
- null session connections, 38, 50
- null session traffic capture, 445
  - Ethereal, 414
- null.pl Perl script, 38-49
- O**
- Office documents, hiding data,
  - 95-97, 99-101
- OLE structured storage, 101-102
- open ports
  - detecting with port scanners. *See* port scanners
  - port scanners
  - footprints, 328-329
- openfiles, 214
- opening Scheduled Tasks applet, 62
- openports, collecting network information and connections, 211
- openports.exe, 348
- OWA (Outlook Web Access), 107
- P**
- P2P (peer-to-peer) file-sharing
  - programs, 24
- packet captures, Analyzer, 410
- PacketStorm Security, 439
- Panda Software Virus
  - Encyclopedia, 437
- Parent Import (PI) Function
  - View, 251
- passwords, 266
  - Administrator passwords, 35
- patch management, 145-146
- pd.pl, 384
- PDF documents, analyzing
  - executable files, 254-255
- PDF files, retrieving metadata
  - from, 254
- pdfmeta.pl, 254
- peer-to-peer (P2P) file-sharing
  - programs, 24
- performing rootkit detection, 338-351
- perimeter devices, 107
  - configuration of, 108-109
  - monitoring, 110
- Perl, 4, 180, 417
  - code excerpt for retrieving file
    - MAC times, 69
  - editors, 422-423
  - FSP. *See* FSP
  - installing, 418-419, 421-422
  - modules, 417
  - programming websites, 440-441
  - running scripts, 423-425
  - scripts, 418
    - di.pl*, 430-432
    - null.pl*, 38-40, 42-50
  - setting up for use with this book, 426-430
  - text files, 417
- Perl modules
  - CPAN, 420
  - installing, 420, 422
  - Win32::API::Prototype, 428
  - Win32::DriveInfo, 429
  - Win32::File::Ver, 427
  - Win32::FileOp, 429
  - Win32::GUI, 428
  - Win32::IPCConfig, 432
  - Win32::Lanman, 426
  - Win32::Perms, 228, 428
  - Win32::TaskScheduler, 426
- Perl Monks website, 441
- Perl Package Manager (PPM), 418
- Perl scripts
  - to enumerate Registry key
    - LastWrite times, 238
  - fru.pl, 361
  - fsw.pl, 138-140
  - hash.pl, 229-231
  - mac.pl, 226
- mdmscan.pl, 156-159
- meta, pl, 96-98
- null.pl, 38-49
- pd.pl, 384
- pdfmeta.pl, 254
- performing file signature
  - analysis, 64-67
- priv.pl, 124-126
- priv2.pl, 148-150
- for retrieving MAC times of a
  - file, 226
- rkd.pl, 338-352
- runchk.pl, 160-163
- sess.pl, 188
- sniffscan.pl, 152-155
- svclst.pl, 218
- systeme.pl, 184-185
- tasks.pl, 324-325
- tz.pl, 93-94
- useraudit.pl, 164-169
- users.pl, 242-243
- ver.pl, 248, 297
- vperms.pl, 229
- wfpget.pl, 236
- wksdump.pl, 150-151
- permissions, 132-133
  - setting, 133
- persistence, 182, 317
- pervasiveness
  - of easy-to-use tools, 11
  - of high-speed connections, 10
  - of Windows systems, 8-10
- PIDs (process identifiers), 279, 349
- plist -t, 193
- pmdump.exe, 202
- policies, security policies, 309
- polices, 2, 37
- Port Reporter, 171
- port scanners, 389-391
  - netcat, 392-394
  - nmap, 396-403
  - portqry.exe, 394-396
  - TCP connect() scanners, 391
- PortExplorer toolkit,
  - openports, 211
- portqry.exe, port scanners, 394-396
- ports, 181
  - mapping processes to, 278



- open ports
  - detecting with port scanners.*
  - See port scanners*
  - footprints, 328-329*
- PPM (Perl Package Manager), 418-419
- PPM commands, 418-419
- ppm query Win32, 418
- PR-Initial-.log, 171
- PR-PIDS-.log, 171
- PR-Ports-.log, 171
- preparing for incidents. *See* incident preparation
- preserving MAC times, 226
- preventing
  - changes to file attributes, 59
  - malware installations, 331
  - rootkit installations, 353-354
- Principle of Least Privilege, 30, 107, 129
- priv.pl, 124-126
- priv2.pl, 148-150
- privilege escalation, local incidents, 26
- privilege levels, 30
- process enumeration
  - checked, 352
- process identifier (PID), 279
- process information, collecting, 189-190
  - with cmdline.exe, 201-202
  - with Handle, 194
  - with ListDLLs, 194
  - with ps.exe, 199
  - with pslist.exe, 191-194
  - with pulist.exe, 190-191
  - with Tlist, 195-199
- process memory, 202-205
- process memory dumps, 252
- Process Tracking, 280
- process-to-port mapper, 211
- processes, 181
  - footprints, 327-328
  - mapping to ports, 278
- program websites, 438-439
- programming errors, 36
- programs
  - file-sharing programs, 269
  - Perl, 4
- promiscdetect, collecting
  - network information and connections, 206
- prosecution, 260
- Protected Storage, 223
- ps.exe, 199
- pslist.exe, 191-194
- psloggedon.exe, 186, 189
- pstoreview.exe, 223
- public newsgroups, posting to, 271
- pulist.exe, 190-191
- purpose of this book, 11-14
- Q-R**
- query, PPM commands, 418
- Ramdane, Amine Moulay, 137
- RAS (remote access servers), 107
- RCA (root cause analysis), 260
- reading packet captures (Ethereal), 413-415
- real-life incidents, 16-19
- Recycle Bin, collecting non-volatile information, 232-234
- Red Button, 50
- redirecting output of commands to a file, 277
- reg.exe, 235
- Registry, 92-95
- Registry keys, 159
  - collecting non-volatile information, 235-237, 240
  - footprints, 325-327
  - LastWrite time, 238-240
  - retrieving specific contents of, 236
- Registry values, WFP, 140-144
- reinstalling systems, 273
  - drawbacks of, 259-260
- remote access servers (RAS), 107
- remote incidents, 30-32, 34
  - banner grabbing, 33
  - defending against, 34
  - Event Logs, 31
- Remote Procedure Call (RPC), 128, 394
- removing unnecessary resources, 292
- researching files, 291
- resources for more information, 20-21
- response teams, composition of, 309
- restricting services, 128-132
- retrieving
  - contents of Run key, 160-163
  - contents of specific Registry keys, 236
  - drive information with di.pl Perl script, 430-431
  - file MAC times, Perl code excerpt for, 69
  - file times with winapimac.pl, 70-72, 74
  - file version information, 248
  - MAC times from files using Perl's stat() function, 226
  - metadata from Microsoft Word documents with meta.pl, 96-98
  - metadata from PDF files, 254
  - user information, 164-169
  - users with specific user rights, 148-150
- returning banners from other ports, 393
- rifiuti command, 234
- Rivest, Ronald L., 360
- rkd.pl, 338-352
- root cause analysis. *See* RCA
- Rootkit.com, 439
- rootkits, 331
  - AFX Rootkit 2003, 353
  - detecting, 337-351, 353
  - kernel-mode rootkits, 332
  - preventing installation of, 353-354
  - user-mode rootkits, 332
    - AFX Windows Rootkit 2003, 332-337
- Roth, David, 228
  - Perl modules, 419
- RPC (Remote Procedure Call), 128, 394
- Run keys
  - retrieving contents of, 160-163
  - rootkits, 353
- runchk.pl, 160-163

**458**      **running**

- running
  - FRU, 366, 369-370, 372-373
  - Perl scripts, 423-425
- S**
- s switch, *tlist*, 195
- S-Tools, 103
- SACLs (system access control lists), 132
- SANS InfoSec Reading Room, 442
- SB 1386 (California state law), 261
- scanners
  - free port scanners, 32
  - port scanners. *See* port scanners
- Scheduled Task Wizard, 321, 426
- scheduled tasks, 321-323
  - collecting non-volatile information, 241
  - creating on Windows XP, 322-323
  - listing, 324-325
- Scheduled Tasks applet,
  - opening, 62
- schtasks.exe, 323
- SCM (Security Configuration Manager), 112
  - configuring systems, 112-116
  - MMC, 112
- SCM (Service Control Manager), 330, 349
- script mappings, disabling, 130
- scripts, Perl scripts. *See* Perl, scripts
- search, PPM commands, 419
- searching
  - for files, 277
  - for recently accessed files, 320
  - websites, 436
- Secure Hash Algorithm 1 (SHA-1), 360
- SecuriTeam, 440
- Security Configuration and Analysis snap-in, Windows XP MMC, 115
- Security Configuration Manager. *See* SCM
- security information websites, 439
- security policies, 309
- SecurityFocus.com, 441
- servers, getting files from, 294
- Service Control Manager (SCM), 330
- service level agreements (SLAs), 260
- services
  - collecting volatile information, 217-220
  - footprints, 329-331
  - restricting, 128-129, 131-132
- sess.pl, 188
- sessions, listing on local systems, 188
- SFC (System File Checker), 136
- SFCD11CacheDir, 140
- SFCDisable, 141-142, 144
- SFCQuota, 140
- SFCScan, 140
- SFCShowProgress, 140
- SHA-1 (Secure Hash Algorithm), 360
- shwobinarymfr.exe, 232
- /si switch, 220
- Siedsma, Christine, 440
- Simple Mail Transfer Protocol (SMTP), 108
- Simple Network Management Protocol (SNMP), 36, 109
- Slammer worm, 17
- SLAs (service level agreements), 260
- SlashDot, 441
- Smith, Richard M., 252
- SMS (Systems Management Server), 404
- SMTP (Simple Mail Transfer Protocol), 108
- sniffers, 389, 403-404
  - Analyzer, 407-408, 410
  - Ethereal, 410, 412
    - reading packet captures*, 413-415
  - netcap, 404-405
  - netmon, 404
  - Windump, 405-407
- sniffscan.pl, 152-155
- SNMP (Simple Network Management Protocol), 36, 109
- Somarsoft Utilities,
  - netusers.exe, 186
- Sophos, 437
- speculation, 24
- spyware, 24, 269, 271
- standard output (STDOUT), 180
- STDOUT (standard output), 180
- steganography, 102-104
- Stoll, Clifford, 16
- Storm Watch, 439
- streams.exe, 84
- strings.exe, 246
- SubSeven, 329
- SVChost, 200
- svclst.pl, 218
- Swinton, Ernest, 261
- switches, 26
- Symantec,
  - SecurityFocus.com, 441
- Symantec Security Response Center, 437
- Symantec Security Response site, 328
- SYN packet, 398
- SYN scan, 398
- SysInternals
  - Autoruns, 319
  - handle.exe, 194
  - ListDLLs, 194
  - psloggedon.exe, 186, 189
- SysInternals.com, 438
- system access control lists (SACLs), 132
- System File Checker (SFC), 136
- system hardening, 2
- system time, 183-185
- systems
  - copying files from, 295
  - investigating, 286
  - reinstalling, 273
    - drawbacks of reinstalling*, 259-260
- systemtime.pl, 184-185
- T**
- /t switch, *dir* command, 226
- tables
  - List of tools for examining various types of files, 258
  - List of tools used for obtaining information about files, 257

- List of tools used to retrieve non-volatile information, 257
- List of tools used to retrieve volatile information, 256
- TaoSecurity, 441
- Task Manager, 276, 328, 336
  - Windows XP Professional, 16
- Task Scheduler, 62
- tasklist/svc, 197
- tasks.pl, 324-325
- TaskScheduler module, 426
- TCP (Transmission Control Protocol), 181, 390
- TCP connect() scanners, 391
- TCP handshake, 391
- TCP/IP, 360
- Teddy Bear virus hoax, 135
- text files, Perl, 417
- The Ultimate Collection Of Forensics Software (TUCOFS), 438
- time, 7
- time zone information
  - Registry, 92-95
  - retrieving, 93-94
- timestamps, 296
- Tlist, 195-199
- tlist.exe, 348
- tools
  - command line tools, 180
  - on compromised systems, 283
  - for examining various types of files, 258
  - freeware tools, 389
  - GUI tools, 180
  - for obtaining information about files, 257
  - pervasiveness of easy-to-use tools, 11
  - for retrieving non-volatile information, 257
  - for retrieving volatile information, 256
- Toptygin, Alexey, 427
- touch.exe, 76
- touch.pl, modifying file MAC times, 76-79
- traffic
  - FTP traffic capture, 443-444
  - IIS traffic capture, 445
  - investigating unusual traffic, 263, 265-268
  - netcat traffic capture, 444
  - nmap traffic capture, 446
  - null session traffic capture, 445
- traffic captures, Ethereal, 413-415
- Transmission Control Protocol (TCP), 181, 390
- Trojans, 200, 317
  - Registry keys, 325-327
- troubleshooting Active Directory with portqry, 395
- TUCOFS (The Ultimate Collection Of Forensics Software), 438
- /tw switch, 226
- type argument, 227
- tz.pl, retrieving time zone information, 93-94
- U**
- ubiquitous Run key, 159
- UDP (User Datagram Protocol), 181
- The Ultimate Collection Of Forensics Software (TUCOFS), 438
- UltraEdit, 423
- Unicode strings, 246
- US Computer Emergency Response Team, 440
- use lib, 424
- User Datagram Protocol (UDP), 181
- user information
  - collecting non-volatile information, 241-243
  - retrieving, 164-169
- user privileges, Windows XP, 119-122
- user rights, 118-120, 122
  - Windows XP logon rights, 126-128
- user-mode rootkits, 332
  - AFX Windows Rootkit 2003, 332-337
- useraudit.pl, 164-169
- users.pl, 241-243
- UTC (Coordinated Universal Time), 184
- utilities
  - auditpol.exe, 134
  - whoami.exe, 123
- V**
- /v switch, 220
- ver.pl, 248-249, 297
- verifying digital signatures, 143
- viewing
  - file associations, 56
  - file times, 68
- virtual private networks (VPNs), 109
- viruses
  - Teddy Bear virus hoax, 135
  - W2K.Stream, 90-91
- VirusList.com, 437
- volatile information, 181, 308
  - collecting, 182, 358
    - clipboard contents, 215-216
    - command history, 216-217
    - with FSP. *See* FSP
    - group policy information, 220, 223
    - logged on users, 185-186, 189
    - network information and connections, 205-212, 215
    - process information, 189-192, 194-195, 197, 199, 201-202
    - process memory, 202-205
    - services and drivers, 217-220
    - system time, 183-185
  - tools for retrieving, 256
- vperms.pl, 229
- VPNs (virtual private networks), 109
- vulnerabilities, exploiting, 51
- W-X-Y-Z**
- W32.AimVen. Worm, 316
- W32.HLLW.LyndEgg worm, 318
- web servers, log files, 289
- websites
  - Aaron's Homepage, 438
  - anti-virus sites, 437-438
  - CERT Coordination Center, 440
  - DiamondCS, 438
  - E-evidence Info, 440
  - EventId.net, 437
  - for searching, 436

**460**      **websites**

- Forensic Acquisition
  - Utilities, 439
- Forensics.nl, 439
- FoundStone, 438
- Google, 436
- Insecure.org, 438
- KartOO, 436
- kbAlertz.com, 436
- Kaspersky Labs, 437
- Microsoft.com, 436
- NTFS.com, 437
- NTSecurity.nu, 438
- PacketStorm Security, 439
- Panda Software, 437
- Perl Monks, 441
- Perl programming sites, 440-441
- program sites, 438-439
- Rootkit.com, 439
- SANS InfoSec Reading
  - Room, 442
- SecuriTeam, 440
- security information sites, 439
- SecurityFocus.com, 441
- SlashDot, 441
- Sophos, 437
- Symantec Security Response
  - Center, 437
- SysInternals.com, 438
- TaoSecurity, 441
- TUCOFS, 438
- US Computer Emergency
  - Response Team, 440
- VirusList.com, 437
- WFP (Windows File Protection),
  - 83-85, 134-138
  - and ADSs, 144-145
  - collecting non-volatile
    - information, 231
  - disabling, 141-144
  - Registry values, 140-144
  - Windows 2000 SP2, 143
- wfpget.pl, 236
- whoami.exe, 123
- WhoIsConnected, 51
- Win32 API, retrieving file times
  - with winapimac.pl, 70-72, 74
- Win32::AdvNotify module, 137
- Win32::API::Prototype, 428
- Win32::DriveInfo, 429
- Win32::File::Ver, 427
- Win32::FileOp, 429
- Win32::GUI, 428
- Win32::IPConfig, 432
- Win32::Lanman, 426
- Win32::Lanman module, 421
- Win32::Perms, 228, 428
- Win32::TaskScheduler, 426
- Win32::TieRegistry module, 236
- winapimac.pl
  - example output of, 74
  - using Win32 API to retrieve file
    - times, 70-72, 74
- Windows 2000
  - DebPloit, 27
  - net session command, 187
- Windows 2000 Resource Kit
  - utility, auditpol.exe, 134
- Windows 2000 SP2, 143
- Windows 2000 systems
  - compromised systems, analyzing
    - data with FSP, 385
  - rootkits, analyzing data with FSP,
    - 380, 384-385
- Windows 2003 systems, infected
  - systems (analyzing data with
    - FSP), 378-380
- Windows File Protection
  - (WFP), 83
- Windows Management Interface
  - (WMI), 245
- Windows NT, SCM, 112
- Windows systems
  - nmap, 400
  - pervasiveness of, 8-10
- Windows XP
  - ListDLLs, 194
  - Local Security Policy, 114
  - logon rights, 126-128
  - netstat -ano, 208
  - pslist, 191-194
  - pulist, 190-191
  - scheduled tasks, creating,
    - 322-323
  - Tlist, 195-199
  - user privileges, 119-120, 122
- Windows XP MMC with Security
  - Configuration and Analysis
    - snap-in, 115
- Windows XP Professional
  - command prompt, 15
  - Task Manager, 16
- Windows XP Professional,
  - command prompt, 15
- Windump, 405-407
- WinPcap drivers
  - installing, 403
  - locating, 152-155
- wizards, Scheduled Task
  - Wizard, 321, 426
- wksdump.pl, 150-151
- WMI (Windows Management
  - Interface), 245
- Word, hiding
  - data, 95
  - documents in Excel
    - spreadsheets, 101-102
- Word documents, metadata,
  - 99-100
- WordDumper, 252
- worms, 52, 315
  - buffer overflow
    - vulnerabilities, 316
  - Code Red worm, 36
  - Forever worm, 141
  - Kwbot, 316
  - W32.AimVen. Worm, 316
  - W32.HLLW.LyndEgg, 318

