



INDEX

Note: Page numbers followed by *f* and *t* indicate figures and tables, respectively.

A

ACID, for data storage, 298, 336, 336*f*

Active countermeasures, risk in using, 136–138

Activity capture. *See* Data capture

adb(1), for jail monitoring, 190

Address Resolution Protocol (ARP), for MAC identifiers, 151–152, 152*f*

ADMmutate, 61, 274–275

Aggressive character, in Specter behavior settings, 114, 121–122, 123*f*

Alert(s)

by Alert Mail, 130–131, 131*f*

archiving, 314–315

in BackOfficer Friendly, 100–101, 100*f*, 101*f*

reviewing, 107, 107*f*

saving, 101–102, 107, 108*f*, 399–405

vs. Specter, 113

value of, 92–93

critical content of, 311, 312*f*

in data control, 248–249, 249*f*

in detection, 310, 352–353, 353*f*

from firewalls, 354, 354*f*

in honeynets, 248–249, 249*f*

logging, 350–352

in GenI honeynets

from firewalls, 248–249, 249*f*

from Intrusion Detection Systems, 251–252

in high-interaction Honeypots, 326–327

in Honeyd, 164–165

in honeynets, 248–249, 249*f*, 364,

423–427 (*See also* GenI honeynets)

in Honeypots goals, 343

from IDS gateway, 266–267, 267*f*

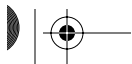
from Intrusion Detection Systems, 222–223, 251–252

from log server, 352, 363

logging, 350–352

in maintenance, 310

in ManTrap, 215–218, 216*f*



INDEX

- Alert(s) *continued*
- in ManTrap cages, 209–210, 209f
 - misconfiguration and, 284–285
 - for outbound traffic, 248–249, 249f
 - prioritizing, 312–314, 313f, 315f
 - redundancy in, 310–311
 - reliability of, 310–311
 - in research Honeypots, 310
 - in response Honeypots, 310, 353
 - reviewing, 107, 107f
 - saving, 101–102, 107, 108f, 399–405
 - by Short Mail, 129, 130f
 - simplicity of, 310
 - in Specter
 - by Alert Mail, 130–131, 131f
 - configuration of, 126–127
 - by Short Mail, 129, 130f
 - value of, 113
 - Alert Mail, in Specter, 130, 131f
 - Al-Qaeda, hacking threats and, 28
 - Ann Arbor Networks, blackhole
 - monitoring by, 144
 - Application(s), in ManTrap, 196, 199–200
 - Application layer
 - data capture at, in ManTrap, 220–221
 - emulation of, in Honeyd, 156–157, 156f
 - purpose of, 148f, 149
 - Application logs
 - data aggregation with, 61
 - for information gathering, in Specter, 133
 - in jails, 189
 - Arkin, Ofir, 334
 - ARP (Address Resolution Protocol), for
 - MAC identifiers, 151–152, 152f
 - ARP proxy, in Honeyd, 153–154, 154f, 159
 - ARP spoofing
 - definition of, 148
 - in Honeyd, 152–153
 - risk in, 165
 - ARP table, 150–152, 150f
 - Arpd utility, 148, 152, 162
 - Attack(s)
 - on BackOfficer Friendly, 105–106, 106f
 - on detection Honeypots, 357–358
 - on GenI honeynets, example of, 265–274, 273f
 - on honeynets, analysis of, 365–366
 - information sharing after, 236–237
 - against log servers, 253
 - modifying, 259
 - motives for, 27–29, 69
 - netcat utility in, 331
 - on networks, 359, 360f
 - on response Honeypots, 356–357
 - scripts for, 366
 - steps in, 14, 15
 - throttling, 259
 - Attackers. *See* Hacker(s)
 - identifying, with file recovery, 221–222
 - IRC used by, 1–2
 - learning about, 8
 - luring *vs.* capturing, 44
 - motives of, 27–29, 69
 - privacy protection for, 373, 376
 - skill levels of, 11–12, 14, 75–76, 269
 - threats from, 12–13
 - tracking, 34–35, 64–65
 - traditional defense against, 4
 - types of, 11–12
 - Authentication, 56, 152
 - Automated tools. *See* Auto-rooters
 - Auto-rooters. *See also* Luckroot
 - capture of, 69, 361
 - detection of, port monitors for, 170–171
 - evolution of, studying, 234–235
 - FTP attack with, 365

- interchangeability in, 18–19
 - vs. mass-rooters, 19
 - method of, 15–16
 - randomness of, 16–17
 - risk posed by, 29
- B**
- Back Orifice, 88–90, 89f
 - Backdoors, rootkits for creating, 2
 - BackOfficer Friendly (BOF)
 - advantages and disadvantages of, 103t
 - alerts in, 100–101, 100f, 101f
 - reviewing, 107, 107f
 - saving, 101–102, 107, 108f, 399–405
 - vs. Specter, 113
 - attack on, 105–106, 106f
 - configuration of, 95–98, 96f, 97f, 104, 104f
 - description of, 83
 - example using, 74–75, 74f
 - fingerprinting of, 102
 - information gathering in, 100–101
 - installation of, 95, 96f, 104
 - logging in, 101–102, 399–405
 - management of, 98–99
 - operation of, 93–95
 - original use of, 90–91
 - overview of, 87–91
 - release of, 38
 - and remote management, 98–99
 - for response, 279
 - risk associated with, 102
 - service emulation in, 98
 - vs. Specter, 92–93, 110
 - tutorial for, 103–108
 - value of, 91–93
 - Banners, consent, 376–379, 378f
 - bash, modified version of, for remote data capture, 254, 272–273, 273f
 - BIND8 service, jails for, 187–188
 - Blackhat(s), advanced
 - definition of, 12
 - meritocratic nature of, 28
 - studying, with research Honeypots, 395–396
 - targets of, 25–27
 - tools of, 25–26, 68
 - trail of, 25–26
 - Blackhat(s), low-level, 11–12, 14
 - Blackholing
 - definition of, 144–145
 - deployment of, 163
 - in Honeyd, 144–147
 - intent of, 145
 - risk in, 165
 - Block option, in Honeyd configuration, 160
 - BOF. *See* BackOfficer Friendly
 - BO2K Trojan, in Specter configuration, 125
 - BOTs, 1–2, 27
 - Bragging rights, as motive for attack, 28
 - BUTTplugs, for Back Orifice, 88–90
- C**
- CAIDA (Cooperative Association for Internet Data Analysis), blackhole monitoring analysis by, 145
 - CDE Subprocess Control Service (dtspcd), exploit for, 39
 - CERT, statistics released by, 13
 - CGM (Content Generation Module), in ManTrap, 207–208
 - Character, in Specter, configuration of, 121–123, 122f, 123f
 - chroot. *See* Jail(s)
 - chroot command, for ManTrap cage customization, 210, 211f

INDEX

- Chuvakin, Anton, on jail breaking, 190–191
- CodeRed II worm
capture and analysis of, 39, 173–174
release of, 21–22, 23*f*
- CodeRed worm, 19–21, 21*f*
- Commercial Honeypots
vs. homemade Honeypots, 344, 345
selection of, 280, 282–283, 361
increase in, 390–391
- Compromised systems
and Back Orifice, 90
as currency, 28
data control in, 350
evidence gathered from, 65–66
forensic analysis of, 332
liability issues with, 381–383
monitoring, real-time, 364
patching, 66
- Configuration
and alerts, 284–285
of BackOfficer Friendly, 95–98, 96*f*,
97*f*, 104, 104*f*
of high-interaction Honeypots, 82
of Honeyd, 158–162, 159*f*
of jails, 187–188
by level of interaction, 77, 77*f*
of low-interaction Honeypots, 78
of ManTrap, 205–211
of medium-interaction Honeypots, 81
of Specter, 119, 120*f*
testing, scripts for, 161, 161*f*
- Consent banners, 376–379, 378*f*
- Consent, federal law exceptions for,
376–379
- Constitution, U.S., privacy under,
372–374
- Content Generation Module (CGM), in
ManTrap, 207–208
- Contraband, Honeypot storage of, 382–383
- Cooperative Association for Internet
Data Analysis (CAIDA), blackhole
monitoring analysis by, 145
- Corporate espionage, as motive for
attack, 28
- Countermeasures, active, risk in using,
137–138
- CPU cycles, as motive for attack, 28
- Credit cards, as motive for attack, 28
- The Cuckoo's Egg* (Stoll), 34–35
- Cult of the Dead Cow, Back Orifice
released by, 88
- CyberCop Sting, 5, 36–37
- D**
- Data
storage of, 241, 250, 298, 336, 336*f*
transactional, under Wiretap Act and
Pen/Trap statute, 375
value of, in Honeypots, 49–51
- Data aggregation. *See also* Data capture
for data analysis, 335–336
database for, 335
definition of, 59
management of, 295–298
problem of, 61
production Honeypots and, 62, 63
value in, 296
- Data analysis
data aggregation for, 335–336
for detection Honeypots, 358
with high-interaction Honeypots,
325
in Honeypot maintenance, 320
keystroke capture for, 329
with low-interaction Honeypots,
320–325, 321*f*, 323*f*, 324*f*
passive, 332–335, 334*f*, 335*f*
preparation for, in deployment, 337

- Data capture. *See also* Keystroke capture;
- Log(s)
 - archiving, 241
 - definition of, 416
 - and deployment, 263–264, 362
 - and encryption, 198, 202, 255–256, 260
 - firewalls for, 250, 251*f*, 363
 - in GenI honeynets, 255–256
 - in GenII honeynets, 260
 - in honeynets
 - definition of, 239
 - and deployment, 263–264, 362
 - and encryption, 255–256, 260
 - firewalls for, 250, 251*f*, 363
 - Intrusion Detection Systems for, 250–253, 252*f*
 - log server for, 253, 266, 266*f*, 273
 - purpose of, 240–241
 - remote, 253–254, 272–273, 273*f*
 - requirements for, 241
 - Snort for, 266
 - storage of, 241, 250
 - in Honeybots, 291–295, 352–356
 - Intrusion Detection Systems for, 250–253, 252*f*
 - IP addresses *vs.* resolved names in, 295
 - kernel in, 201–202, 260
 - log server for
 - in honeynets, 253, 266, 266*f*, 273
 - for Honeybots, 352–356
 - in ManTrap
 - at application layer, 220–221
 - and encryption, 198, 202
 - kernel in, 201–202
 - reviewing, 217–218, 219*f*
 - value of, 198
 - maximizing, 291–293
 - redundancy in, 293–295
 - remote, 253–254, 272–273, 273*f*
 - requirements for, 241, 417–418
 - reviewing, 217–218, 219*f*
 - Snort for, 266
 - standards for, 419
 - storage of, 241, 250, 298
 - ECPA and, 374
- Data collection
- definition of, 416
 - with GenII honeynets, 260–261
 - with honeynets
 - definition of, 239
 - and deployment, 264
 - elements of, 242
 - purpose of, 241–242
 - integrity in, 261
 - legal issues with, 375–376
 - requirements for, 418
 - standardized format for, 261
 - standards for, 419–421
- Data control
- alerts for, 248–249, 249*f*
 - automating, 240
 - bypassing, 274–275
 - for compromised systems, 350
 - definition of, 416
 - and deployment, 263–264, 362
 - and due diligence, 382
 - firewalls for, 363
 - in GenI honeynets, 243–249, 250*f*, 255
 - in GenII honeynets, 256–260
 - in honeynets (*See also* Outbound traffic)
 - alerts for, 248–249, 249*f*
 - automating, 240
 - bypassing, 274–275
 - definition of, 239
 - and deployment, 263–264, 362
 - firewalls for, 363
 - layers of, 248

INDEX

- Data control *continued*
 - purpose of, 239–240
 - requirements for, 240
 - Honeypot location and, 290–291
 - requirements for, 240, 416–417
 - in response procedures, 319
 - for risk mitigation, 304–305
 - and updating, 365
- Database
 - for data aggregation, 335
 - for log storage, 298
- Deception
 - with BackOfficer Friendly, 91
 - detection of Honeypots in, by
 - attackers, 305–306
 - example of, 57–58
 - with honeynets, value of, 231
 - Honeypots for, 278
 - jails for, 184–185
 - with ManTrap, value in, 195–196
 - for prevention, 56–57
 - with Specter, 112, 114
- Deception Toolkit (DTK), 5, 36
- Demarc, for data storage, 298
- Demilitarized Zone. *See* DMZ
- Denial of Service (DoS), as motive for
 - attack, 27
- Deployment
 - data analysis preparation in, 337
 - effectiveness and, 348
 - of high-interaction Honeypots, 82
 - of Honeyd, 162–163
 - of honeynets, 263–265
 - for research, 362–364, 363f
 - of jails, 188
 - by level of interaction, 77, 77f
 - locations for, 286
 - of low-interaction Honeypots, 78
 - of ManTrap, 211–214
 - of medium-interaction Honeypots, 81
 - of Specter, 127
- Detection. *See also* Alert(s)
 - alerts in, 310, 352–353, 353f
 - in BackOfficer Friendly, 91–93, 92f
 - in Honeyd, and service emulation, 143
 - with honeynets, value of, 231
 - of Honeypots, 305–306, 349–350
 - Honeypots for, 278
 - alerts from, 352–353, 353f
 - attack on, 357–358
 - deployment of, 346, 347f
 - effectiveness of, optimizing, 348–349
 - goal of, 343
 - location of, 287f, 288–289
 - response procedure for, 317, 355, 357–358
 - Intrusion Detection System (IDS) for, 59
 - jails for, 185
 - level of interaction and, 344
 - with low-interaction Honeypots, 78
 - with ManTrap, value in, 196–197
 - with port monitors, 170–172, 172f
 - problems in (*See* Data aggregation;
False negatives; False positives)
 - production Honeypots and, 61–63, 63f
 - purpose of, 58
- Deterrence
 - with BackOfficer Friendly, 91
 - detection of Honeypots in, by
 - attackers, 305–306
 - Honeypots for, 278
 - with ManTrap, value in, 195–196
 - for prevention, 56–57
 - with Specter, 112, 114–115
- Dittrich, David, 370
- DMZ (Demilitarized Zone)
 - incident response in, 66, 67f
 - monitoring, 42, 43f, 62–63, 63f

- DNS (Domain Name Service). *See also*
 BIND8 service
 jails for, 182–183, 186–187
 in Specter, 125, 136
- Domain names, for honeynets, 262–263
- DoS (Denial of Service), as motive for
 attack, 27
- DTK (Deception Toolkit), 5, 36
- dtspcd (CDE Subprocess Control
 Service), exploit for, 39
- E**
- Early warning mechanisms
 data analysis in, 335
 honeynets as, 235
 research Honeypots as, 69, 394
- Electronic Communications Privacy Act
 (ECPA), 372, 374
- Emulation
 of application layer, in Honeyd,
 156–157, 156f
 of IP addresses, in Honeyd
 ARP proxy for, 153–154, 154f
 operation of, 146
 overview of, 142
 value of, 144–145
 of IP stack
 in Honeyd, 143, 156–157, 156f, 159
 and Specter, 118–119, 138
 of networks, 37
 of operating systems
 in Honeyd, 143, 155–157, 156f
 in medium-interaction Honeypot, 80
 in Specter, 111–112, 115–118, 116f,
 117f, 120–121, 138
 of services
 in BackOfficer Friendly, 98, 102
 in Honeyd, 156–157, 156f
 configuration of, 159–160
 customization of, 142
 and detection, 143
 operation of, 145–146
 for response, 154–155
 value of, 143–144
 with port monitors, 180–181
 in Specter, 110–111, 111f, 123–124, 125f
 of vulnerabilities, in Specter, 110, 111f,
 114
- EnCase, for forensic analysis, 332
- Encryption
 activity capture and, in ManTrap, 198,
 202
 data capture and
 in GenII honeynets, 260
 and log servers, 273
 and network captures, 272
 for prevention, 56
 use of, 29
- Entrapment, legal issues with, 380–381
- Ethereal, for network analysis, 331–332,
 333f
- Ethernet, in link layer, 149–151
- "An Evening with Berferd in Which a
 Cracker Is Lured, Endured, and
 Studied" (Cheswick), 34, 35–36, 184
- Event Log, for information gathering, in
 Specter, 134, 134f
- Evidence, from Honeypots, 64–66
- Exploits
 automatic, 15–16
 capture of
 port monitors in, 172–173
 unknown, 39, 69, 232–233, 233f,
 234f, 235
 development of, 14
 downloading, via FTP, 331
 interchangeability of, in auto-routers,
 18–19

INDEX

- Exploits *continued*
 launching, 14
 point-and-click, 15, 16*f*
 unknown
 capture of, 39, 69, 232–233, 233*f*,
 234*f*, 235
 identification of, 396
- F**
- Failing* character, in Specter behavior
 settings, 122
- False negatives
 definition of, 59
 eliminating, 396
 problem of, 60–61
 production Honeyd and, 61–64
 reduction of, with IDS integration, 392
- False positives
 definition of, 59
 eliminating, 396
 in honeynets, 235
 problem of, 59–60
 production Honeyd and, 61, 62–63
 reduction of, 127, 392
- Federal Aviation Administration (FAA),
 information sharing by, 236–237
- Federal Wiretap Act (Title III), privacy
 under, 372, 374–380
- File recovery
 in Ethereal, 332
 in honeynets, 271–272
 in ManTrap, 221–222
- File system, in ManTrap, 202–204, 203*f*
- File Transfer Protocol. *See* FTP
- FINGER, in Specter
 configuration of, 124
 for information gathering, 136
- Fingerprinting
 of BackOfficer Friendly, 102
 of Honeyd, 155–156
 of honeynets, 255
 of Honeyd, 54–55
 ICMP for, 118, 333–335, 335*f*
 mitigating, 305–307
 passive
 for data analysis, 332–335, 334*f*, 335*f*
 in Honeyd appliances, 390
 of Specter, 112, 118–119
- Firewall(s)
 adoption of technology, 388–389
 alerts from, 354, 354*f*
 in honeynets, 248–249, 249*f*
 logging, 350–352
 for data capture, 250, 251*f*, 294–295,
 294*f*, 363
 for data control, 248–249, 249*f*, 265,
 350, 363
 failure of, 58
 for GenI honeynets, 244–245
 GUI for, 389, 390*f*
 in high-interaction Honeyd, 82
 for Honeyd, 163
 for honeynets, 244–245, 362, 363, 365
 and Honeyd location, 286
 integration of, with Honeyd, 392
 internal connections and, 359
 and Intrusion Detection Systems,
 combining, 256
 maintaining, 264
 for ManTrap, 225–226
 misconfiguration of, 390
 for outbound traffic, 6
 for prevention, 56
 resource exhaustion and, 51
 return on investment in, 52
 rulebase for
 for compromised systems, 350
 for honeynets, 246–247, 247*f*

- misconfiguration of, 390
 - reviewing, 359
 - use of, 40–41
 - FireWall-1, 246, 389, 390*f*
 - Forensic analysis, of compromised systems, 332
 - Fourth Amendment, 372–374
 - FTP (File Transfer Protocol)
 - auto-rooter attack against, 365
 - in BackOfficer Friendly, 94, 97
 - in Specter, configuration of, 110, 111*f*, 123
 - for tools download, 331
 - FTP banner, in Specter, for information gathering, 136
- G**
- gdb(1), for jail monitoring, 190
 - GenI honeynets
 - alerts in, 248–249, 249*f*, 251–252
 - architecture of, 243
 - capabilities of, 243
 - data capture in, 255–256
 - data control in, 243–249, 250*f*, 255
 - deployment of, 265, 266*f*
 - example attack on, 265–274, 273*f*
 - firewalls for, 244–245, 265, 266*f*
 - rulebase for, 246–247, 247*f*
 - vs. GenII honeynets, 261, 362
 - outbound traffic in, 244–248
 - overview of, 242–243
 - risk in, 255
 - routers for, 248
 - GenII honeynets
 - data capture in, 260
 - data collection in, 260–261
 - data control in, 256–260
 - vs. GenI honeynets, 261, 362
 - honeynet sensor in, 256–257
 - Intrusion Detection Systems gateways
 - in, 257–259
 - network diagram of, 258*f*
 - overview of, 256–261
 - in production networks, 257, 258*f*
 - response in, 259
 - GFORCE, hacking threats from, 28
 - Granick, Jennifer, 370
 - Graphical user interfaces (GUI), and ease of use, 389–390, 390*f*
 - Guest books, link from, 348–349
- H**
- Hacked computers. *See* Compromised systems
 - Hacker(s). *See* Attackers
 - h4x0r, 3, 76
 - Hacking. *See* Attack(s)
 - Hard drive, wiping, for deployment, 337
 - Hardware requirements, for ManTrap, 206
 - High-interaction Honeypots
 - alerts in, 326–327
 - capabilities of, 75–76, 76*f*, 81–82
 - data analysis with, 325
 - definition of, 75
 - due diligence for, 382
 - example of, 325–326, 326*f*
 - vs. low-interaction Honeypots, 344, 345
 - privacy issues with, 371
 - risk from, mitigating, 350
 - Hogwash IDS gateway, 259–260
 - Home networks, scanning of, statistics for, 13
 - Homemade Honeypots. *See also* Jail; Port monitors
 - advantages of using, 167
 - vs. commercial Honeypots, 344, 345
 - selection of, 280, 282–283, 361

INDEX

- Homemade Honeyd. *continued*
- description of, 84
 - interfaces of, 282
 - overview of, 168–169
 - uses of, 168
 - variety of, 168
- Honey cards, use of, 395–396
- Honeyd
- advantages and disadvantages of, 166*f*
 - alerts in, 164–165
 - ARP proxy in, 153–154, 154*f*, 159
 - ARP spoofing in, 152–153
 - ARP table in, 152, 153
 - blackholing in, 144–147
 - configuration of, 158–162, 159*f*
 - deployment of, 162–163
 - description of, 84
 - fingerprinting of, 155–156
 - firewalls for, 163
 - information gathering with, 163–165
 - initialization of, 157–158
 - installation of, 157
 - IP emulation in
 - ARP proxy for, 153–154, 154*f*
 - operation of, 146
 - overview of, 142
 - value of, 144–145
 - IP monitoring in
 - operation of, 145–146
 - overview of, 142
 - value of, 144
 - IP stack emulation in
 - configuration of, 159
 - overview of, 143
 - level of interaction of, modification of, 143–144
 - logging with, 163, 164*f*
 - maintenance of, 162–163
 - misconfiguration of, and risk, 165
 - network traffic forwarded to, 146–147, 147*f* (*See also* ARP spoofing)
 - operating systems emulation in, 143, 155
 - operation of, 145–157
 - overview of, 142–143
 - proxying in, 159*f*, 161–162
 - response in, 154–157
 - risk in using, 165
 - scripts in, 160–161, 161*f*
 - service emulation in
 - configuration of, 159–160
 - customization of, 142
 - operation of, 145–146
 - for response, 154–155
 - scripts for, 160–161
 - value of, 143–144
 - and sniffers, 164
 - value of, 143–145
 - virtual networks in, 162
- Honeynet(s). *See also* GenI honeynets; GenII honeynets
- activity on, generating, 263
 - advantages and disadvantages of, 265, 275*t*
 - alerts in, 423–427
 - as architecture, 238–239
 - attacks on, analysis of, 365–366
 - complexity of, risk from, 274
 - comprehensiveness of, 237–238
 - definitions for, 416
 - deployment of, 263–265, 266*f*
 - for research, 362–364, 363*f*
 - description of, 85–86
 - distributed, 392–393
 - domain names for, 262–263
 - as early warning system, 235
 - example attack on, 265–274, 273*f*
 - expected activity captured by, 274–275

- false positives in, 235
- flexibility of, 265
- history of, 229–230
- information gathering with, 268
- level of interaction of, 229, 274
- maintenance of, 263–265, 364–365
- management of, networks for, 362
- monitoring, 264–265
- operation of, 238–242
- overview of, 229–231
- prevention with, value of, 231
- as production Honeypots, value of, 231
- production systems in, 229
- requirements for, 416–418
- as research Honeypots, 231–232, 278, 362
 - deployment of, 362–364, 363*f*
 - for response development, 236–238
 - response procedures for, 364
 - risks with, 274–275
 - standards for, 419–421
 - as targets of choice, 262–263
 - as test beds, 238, 364
 - tool evolution and, 234–235
 - trend analysis with, 235–236
 - unknown exploits captured with, 232–233, 233*f*, 234*f*
 - updating, 365
 - value of, 231–238
 - virtual, 261–262
- Honeynet Project
 - data collection by, 50, 336, 336*f*, 366, 394
 - formation of, 38, 230
 - mission statement of, 230
- Honeynet Research Alliance, 230–231, 392–393
- Honeynet sensor, 256–259
- Honeyp.com, overview of, 341–342
- Honeyp.edu, overview of, 360
- Honeypots. *See also* Production Honeypots; Research Honeypots
 - advantages of, 49–53
 - as appliances, 390–391
 - auto-router capture with, selection for, 361
 - behavior of, modifying, 306
 - blending into organization, 306–307
 - compromise statistics for, 12–13
 - concept of, 3–4, 41
 - consent banners for, 376–379, 378*f*
 - contraband storage on, 382–383
 - cost of, 52, 282, 285
 - customized, 42–44, 43*f*, 350
 - for data capture, in honeynets, 253
 - data value in, 49–51, 50*f*
 - definition of, 40, 387–388
 - detection of, by attackers, 54, 349–350
 - disadvantages of, 53–55
 - for DMZ monitoring, 42, 43*f*
 - failures of, 8
 - field of view of, 53–54
 - fingerprinting of, 54–55, 305–307
 - first documented, 35
 - flexible use of, 41
 - goals for, 277–280, 343–346, 361–362
 - government use of, 394
 - in honeynets, 253
 - HTTP links to, 348–349
 - integration of, with other technologies, 391–392
 - legality of (*See* Legal issues)
 - level of interaction of
 - for detection, 343–344
 - selection of, 280–282, 361
 - location of, 286, 287*f*, 346–347, 347*f*
 - maintenance of, 352–356, 389–390
 - management of
 - ease of, improving, 389–390

INDEX

- Honeypots. *continued*
- network for, 296–298, 297*f*, 350–352, 351*f*
 - and number, 286
 - misconceptions about, 9, 44, 388
 - misconfiguration of, 284–285, 389–390
 - mistakes in, 54
 - number of, determining, 285–286, 346–347, 347*f*
 - operating systems for, selection of, 280, 283–285, 361
 - organizational limits on, 368–369
 - port forwarding to, NAT for, 301–302, 303*f*
 - prepackaged, increase in, 390–391
 - prioritizing, for alerts, 313
 - vs. production systems, 40
 - realism in, 307
 - resource exhaustion and, 51–52
 - return on investment in, 52–53
 - risk posed by, 55, 302–305
 - in security policy, 70
 - selecting, 280–285, 361–362
 - simplicity of, 52
 - with sniffers, 292, 292*f*
 - specialization of, 392–393
 - timeline of, 33–34
 - tool download with, 331
 - unknown exploits captured by, 39
 - updating, 338–339, 355–356
 - value of, 359
 - worm capture with, selection for, 281, 361
- HTTP (Hyper-Text Transfer Protocol)
- automated attacks against, and port monitors, 171–172, 172*f*
 - in BackOfficer Friendly, 94, 97
 - in Specter, configuration of, 124
 - vulnerabilities in, 365
- HTTP document, in Specter, 136
- HTTP server head, in Specter, 136
- Huger, Alfred, 5
- I**
- iButton, 198–199, 207, 223
- ICMP packets
- for fingerprinting, 118, 333–335, 335*f*
 - in Honeyd, 144, 163, 164*f*
- IIS (Microsoft Internet Information Server)
- CodeRed and, 19–21
- IMAP (Internet Message Access Protocol), in BackOfficer Friendly, 98
- IMAP4 (Internet Message Access Protocol), in Specter, 125
- Implementation, for data capture, 291–295
- Incident response
- alerts in, 310
 - BackOfficer Friendly for, value in, 91
 - data control in, 319
 - developing, honeynets for, 236–238
 - in DMZ, 66
 - evidence collection in, 64–65
 - in GenII honeynets, 259
 - in Honeyd, 154–157
 - Honeypots for, 278
 - alerts from, and production services, 353
 - attacks on, 356–357
 - deployment of, 346–347, 347*f*
 - effectiveness of, optimizing, 348–349
 - location of, 287*f*, 289
 - purpose of, 344–345
 - response procedure for, 317, 355
 - selecting, 279
 - and information sharing, 237
 - with jails, 185
 - level of interaction and, 345

- ManTrap for, 198, 345–346
 - preparation for, 67–68
 - procedures for
 - active value of, 316–317
 - development of, 355
 - documenting, 318–319
 - for honeynets, 364
 - options for, 315–316
 - passive, 317
 - in production Honeypots, 66
 - purpose of, 64
 - remote access in, 319
 - roles in, 318
- Incidents.org, 179, 366, 394
- Information gathering. *See also* Data entries
- with BackOfficer Friendly, 100–101
 - with high-interaction Honeypots, 82
 - with Honeyd, 163–165
 - with honeynets, 268
 - with jails, 189–190
 - by level of interaction, 77, 77*t*
 - with low-interaction Honeypots, 79
 - in ManTrap, 214–215
 - with medium-interaction Honeypots, 81
 - with Specter, 112–113, 124–126, 129, 134–138
- Installation
- of BackOfficer Friendly, 95, 96*f*, 104
 - of high-interaction Honeypots, 82
 - of Honeyd, 157
 - of jails, 187–188
 - by level of interaction, 77, 77*f*
 - of low-interaction Honeypots, 78
 - of ManTrap, 205–211
 - of medium-interaction Honeypots, 81
 - of Specter, 119
- Intelligence Gathering, in Specter, 135–137
- Internal network
- connection from, 358–359
 - monitoring of, 42–44, 43*f*
- Internet Chat Relay. *See* IRC
- Internet Message Access Protocol. *See* IMAP
- Intrusion Detection System (IDS)
- adoption of technology, 388
 - alerts from, 222–223
 - data aggregation with, 61
 - data capture by, 250–253, 252*f*
 - deployment and, 362
 - for detection, 59
 - evasion of, 61
 - false negatives in, 60–61
 - false positives in, 59–60
 - and firewalls, combining, 256
 - for honeynets, and deployment, 362
 - integration of, with Honeypots, 392
 - interface of, 250–251
 - method used by, 60
 - remote logging with, 253
 - resource exhaustion and, 51
 - role of, 251
 - as sniffers, 222–223
 - Specter as, 112
 - in trend analysis, 235
 - updating, 365
 - use of, 41
- Intrusion Detection Systems gateway. *See also* Hogwash IDS gateway
- advantages of, 257–259
 - alerts from, 266–267, 267*f*
 - in GenII honeynets, 257
 - maintaining, 264
 - signature database of, 257
- IP addresses
- aliased, 51
 - binding (*See* ARP proxy)

INDEX

- IP addresses *continued*
- emulation of, in Honeyd
 - ARP proxy for, 153–154, 154f
 - operation of, 146
 - overview of, 142
 - value of, 144–145
 - logging, with Snort, 328
 - and MAC identifiers, association of,
 - 150, 150f
 - monitoring, with Honeyd
 - operation of, 145–146
 - overview of, 142
 - value of, 144
 - in network layer, 149
 - vs. resolved names, in data capture, 295
 - source, analysis of, 320–324, 321f, 323f, 324f
 - translation of, NAT for, 298
- IP protocols, 411–413
- IP stack, emulation of
- in Honeyd, 143, 156–157, 156f, 159
 - and Specter, 118–119, 138
- IPTables firewall, for GenI honeynets, 246
- IRC (Internet Chat Relay)
- capture of, 377, 379
 - definition of, 1
 - in DoS attacks, 27
 - as exploit resource, 15
 - in hacking community, 1–2
- J**
- Jail(s). *See also* Homemade Honeypots;
- ManTrap cages
 - vs. chroot, 184
 - concept of, 169
 - configuration of, 187–188
 - customizable, 183
 - deception with, 184–185
 - definition of, 36
 - deployment of, 188
 - description of, 182
 - for detection, 185
 - detection of, by attackers, 190
 - disadvantages of, 186
 - flexibility of, 184–186
 - information gathering with, 189–190
 - installation of, 187–188
 - level of interaction in, 184
 - logging in, 189
 - maintenance of, 188
 - in medium-interaction Honeypot, 80
 - monitoring, 189–190, 189f
 - operating systems for, 184
 - operation of, 186–187
 - original use of, 182–183
 - vs. port monitors, 169
 - as research Honeypots, 185–186
 - for response, 185
 - risk with, 55, 190–191
 - value of, 184–186
- Jail breaking, risk of, 190–191, 226–227
- K**
- Kernel
- for data capture, 260
 - definition of, 201
 - in ManTrap, 201–202, 214–215
 - rootkits for, 271
- Kernel modification, use of, 30
- Keystroke capture
- for data analysis, 329, 358
 - for data collection, 268–269
 - with GenII honeynets, 260
 - with Intrusion Detection Systems, 251
 - in ManTrap, reviewing, 219–220, 220f
 - remote forwarding of, 254, 254f
 - in security policy, 368–369
- Keystroke reply, in ManTrap, 224–225, 224f

- Know Your Enemy* (HoneyNet Project),
38, 230
- L**
- LaBrea Tarpit, for internal network
monitoring, 43
- Leaves worm, capture and analysis of,
38–39, 178–181
- Legal issues, with HoneyNets
consent and, 376–379
data collection and, 375–376
entrapment and, 380–381
liability and, 381–383
organizational, 368–369
precedent in, 369–371
privacy and, 371–374
Service Provider Protection exception
and, 379–380
variables in, 367–368
- Level of interaction
definition of, 73
guidelines for, 281–282
in Honeyd, modification of, 143–144
in honeynets, 229, 274, 345
in HoneyNets
for detection, 343–344
selection of, 280–282, 361
in jails, 184
in ManTrap, 193
risk in, 281, 303–304
tradeoffs between, 74, 76–77, 77*t*
- Liability, legal issues of, 381–383
- Link layer, purpose of, 148*f*, 149
- localhost, for HoneyPot attack, 105
- Log(s)
aggregation of, 295–298
in BackOfficer Friendly, 101–102,
399–405
by firewalls, 250, 251*f*
integrity of, and iButton, 223
by Intrusion Detection Systems,
250–251
of IP addresses, 328
by jails, 189
by low-interaction HoneyNets, in
trend analysis, 324–325
by ManTrap cages
configuration of, 209–210, 209*f*
location of, 214–215
by ManTrap, reviewing, 217–218, 219*f*
network for, 296–298, 297*f*, 350–352,
351*f*
protection of, with iButton, 199
remote (*See* Remote logging)
by Snort, for data analysis, 327–329,
328*f*, 329*f*, 332, 333*f*
by Specter, 132–138
storage of, 298
- Log Analyzer, for information gathering,
in Specter, 132, 132*f*
- Log server
alerts from, 352
attacks against, 253
for data capture
analysis of, 356–357
for honeynets, 253, 266, 266*f*, 273, 363
for HoneyNets, 352–356
maximizing, 293
encryption and, 273
- Loopback, use of, 202–204
- Low-interaction HoneyPot
advantages and disadvantages of, 79
capabilities of, 74–75, 78–79
data analysis with, 320–324, 321*f*, 323*f*,
324*f*
definition of, 74
due diligence for, 382
example of, 74–75, 74*f*, 78–79

INDEX

- Low-interaction Honeypot *continued*
 vs. high-interaction Honeypots, 344, 345
 improvement of, future, 393
 logs of, for trend analysis, 324–325
- Luckgo, 17
- Luckroot, 17–19, 18f
- Luckscan, 17
- Luckstatdx, 17
- M**
- MAC (modify, access, change), 65, 269
- MAC (Media Access Control) identifiers
 composition of, 149–150
 in Ethernet, 149–151
 and IP addresses, association of, 150,
 150f
 in ManTrap, 206
 unknown, finding, 151f, 152–153
- Maintenance
 alerts in, 310
 data analysis in, 320
 ease of, improving, 389–390
 of high-interaction Honeypots, 82
 of Honeyd, 162–163
 of honeynets, 263–265, 364–365
 of Honeypots, 352–356
 of jails, 188
 by level of interaction, 77, 77f
 of low-interaction Honeypots, 78
 of ManTrap, 213–214
 of medium-interaction Honeypots, 81
 of Specter, 127–128
- Management
 of BackOfficer Friendly, 98–99
 ease of, improving, 389–390
 of honeynets, networks for, 362
 of Honeypots, network for, 296–298,
 297f, 350–352, 351f
 and number of Honeypots, 286
- ManTrap. *See also* iButton
 activity capture with
 at application level, 220–221
 reviewing, 217–218, 219f
 value of, 198
 advantages and disadvantages of, 227t
 alerts in, 215–218, 216f
 cages in (*See* ManTrap cages)
 CGM in, 207–208
 complexity of, risk with, 226
 configuration of, 205–211, 208f
 data integrity in, 223
 deployment of, 211–214
 description of, 85
 detection with, value in, 196–197
 file recovery in, 221–222
 file system in, 202–204, 203f
 firewalls for, 225–226
 hardware requirements of, 206
 host system in (*See* ManTrap host
 system)
 information gathering in, 214–215
 installation of, 205–211
 jail breaking in, 226–227
 kernel in, 201–202, 214–215
 keystroke capture in, reviewing,
 219–220, 220f
 keystroke reply in, 224–225, 224f
 level of interaction of, 193
 limitations of, 194–195, 199–200
 logging in, reviewing, 217–218, 219f
 MAC identifiers in, 206
 operating system requirements of,
 194–195, 199, 205–206
 operation of, 200, 200f
 overview of, 193–195
 prevention with, value of, 195–196
 process log in, alerts from, 217–218
 as research Honeypot, 198–199, 278

- for response, 345–346
 - response with, 198, 278, 279
 - risk with, 225–227
 - security testing with, 199
 - services in, value of, 197
 - sniffers and, 222–223
 - alerts from, 217
 - value of, 196–197
 - vulnerabilities in, 195–196
- ManTrap cages. *See also* Jail(s)
- alerting in, 209–210, 209f
 - compromising, 193, 195–196
 - configuration of, 207, 208f, 209–210, 209f
 - customization of, 207–208, 210–211
 - deployment of, 211–212, 212f
 - file capture from, 221–222
 - file system in, 202–204, 203f, 204f
 - flexibility of, 194
 - host file system in, 202–204, 203f
 - identification of, by attackers, 205, 226
 - kernel sharing by, 201–202
 - limitations in, 205
 - logging in, 209–210, 209f, 214–215
 - operation of, 200, 200f, 204–205, 205f
 - overview of, 194
- ManTrap host system
- building, 206–207
 - configuration of, 207, 208f
 - customization of, 207
 - deployment of, 212–213, 213f
 - file system in, 202–204, 203f
 - kernel sharing by, 201–202
 - operation of, 200, 200f
- Mass-rooters, 19, 20f, 232–233, 233f, 234f
- MD5 checksum, as data analysis preparation, 337
- Media Access Control identifiers. *See* MAC identifiers
- Medium-interaction Honeypot, 80–81, 393
- MEECES (Money, Ego, Entertainment, Cause, Entrance), 27
- Memory, worms residing in, 38, 173
- MICE (Money, Ideology, Compromise, Ego), 27
- Microsoft Internet Information Server (IIS), CodeRed and, 19–21
- modify, access, change (MAC), 65, 269
- Motives, for attacks, 27–29, 69
- N**
- NAT (Network Address Translation), 298–301, 300f, 301f, 349
- National Infrastructure Protection Center (NIPC), 39, 181
- NETBUS, in Specter, configuration of, 124
- netcat utility
- and expected behaviors, 176–177, 179
 - for port listening, in attacks, 331
 - for port monitoring, 174–177, 175f, 176f, 177f
 - for remote connections, 179–180
- NetFacade, 37
- NetForensics, for data storage, 298
- NetSec, 84
- netstat command, listening ports identified with
- and BackOfficer Friendly, 94–95, 94f, 105, 105f
 - and Specter, 115
- Network(s). *See also* DMZ; Internal network
- analysis of, Ethernet for, 331–332
 - attack on, 359, 360f
 - diagrams of, notation for, xxii
 - under ECPA, 374
 - emulation of, 37
 - for honeynet management, 362

INDEX

- Network(s). *continued*
 for Honeypot management, 296–298,
 297*f*, 350–352, 351*f*
 for logging, 296–298, 297*f*, 350–352, 351*f*
 notation for, 141–142
 privacy on, 371
 virtual, in Honeyd, 162
- Network Address Translation (NAT),
 298–301, 300*f*, 301*f*, 349
- Network capture
 and encryption, 272
 for file recovery, 271–272
 in honeynets, 267, 268*f*, 269–272, 270*f*
 in ManTrap, 214
- Network Flight Recorder, 83
- Network Intrusion Detection System. *See*
 Intrusion Detection System
- Network layer, purpose of, 148*f*, 149
- Network sweeps, covert, 50–51, 50*f*
- Network traffic
 forwarding
 future solutions for, 392
 to Honeyd, 146–147, 147*f* (*See also*
 ARP spoofing)
 with NAT, 301–302, 303*f*
 monitoring, and encryption, 29–30
- Network Voice Protocol, as backdoor,
 232–233, 233*f*, 234*f*
- Nimda worm, 22–24
- NIPC (National Infrastructure
 Protection Center), 39, 181
- Nmap, for fingerprinting, 118, 143, 155,
 157, 158*f*
- O**
- Open* character, in Specter behavior
 settings, 121, 122*f*
- Open option, for service emulation, in
 Honeyd configuration, 160
- Open sockets. *See* Port listeners
- OpenSource, definition of, 142
- Operating systems
 configuration of, and familiarity, 284
 emulation of
 in Honeyd, 143, 155, 156–157, 156*f*
 in medium-interaction Honeypot, 80
 in Specter, 111–112, 115–118, 116*f*,
 117*f*, 120–121, 138
- fingerprinting of
 for data analysis, 332–335, 334*f*, 335*f*
 and Honeyd, 155–156
 for Honeyd, 344, 345
 selection of, 280, 283–285, 361
 and ManTrap, 193–195, 199, 205–206
 risk to, 137–138, 181–182
 securing, for risk mitigation, 304, 357
 updating, 338, 365
- Outbound traffic. *See also* Data control
 alerts for, 248–249, 249*f*
 prioritizing, 312–313, 313*f*
 allowing, 8
 controlling with routers, 248
 firewall for, 6
 in GenI honeynets, 244–248
 honeynet sensor and, 258–259
 in honeynets, 363–364
 limiting, 245–246, 363–364
 necessity of, 245
 risk of, 225–226, 255
- P**
- Packeting, as motive for attack, 27
- Palisade Systems, 391
- Passive OS fingerprinting
 for data analysis, 332–335, 334*f*, 335*f*
 and Honeyd, 155–156
 in Honeyd appliances, 390
- Password(s), failure of, 59

- Password files, downloading, 110, 114, 117–118
 - configuration for, 125–126
 - Pen Register/Trap and Trace Statute (Pen/Trap), privacy under, 372, 374–380
 - Platform. *See* Operating systems
 - Political motives, for attacking, 28
 - POP3
 - in BackOfficer Friendly, 94, 98
 - in Specter, configuration of, 124
 - Port forwarding, NAT for, 301–302
 - Port listeners
 - in BackOfficer Friendly, 93–94
 - netcat for, in attacks, 331
 - in Specter, 113
 - for worm capture, selection for, 281–282
 - Port misconfiguration, 357
 - Port monitors. *See also* Homemade Honeypots; netcat utility
 - capture with, 172–173, 181
 - definition of, 168
 - detection with, 170–172, 172*f*
 - emulation capabilities in, 177–181
 - vs.* jails, 169
 - overview of, 169–170
 - as research Honeypots, 170, 181
 - risk associated with, 181–182
 - service emulation in, 180–181
 - value of, 170–173
 - Portscan, in Specter, for information gathering, 136
 - Prevention. *See also* Deception; Deterrence
 - with BackOfficer Friendly, 91
 - definition of, 56
 - Honeypots for, 278, 287–288, 287*f*
 - with ManTrap, value of, 195–196
 - production Honeypots in, 56–58
 - Privacy, in Honeypot legal issues, 371–374
 - Private addressing (RFC 1918), definition of, 298–299
 - Process log, alerts from, 217–218, 219*f*
 - Production Honeypots. *See also* Detection; Incident response; Prevention
 - detection problems addressed by, 61–62
 - for DMZ monitoring, 62–63, 63*f*
 - for evidence collection, 66
 - field of view of, 64
 - Honeyd as, 142
 - honeynets as, 231
 - incident response in, 66, 67*f*
 - jails as, 184
 - location of, 286
 - number of, determining, 285
 - in prevention, 56–58
 - purpose of, 44–45, 55
 - vs.* research Honeypots, 46
 - role of, defining, 278–279
 - specialization of, 392–393
 - use of, 69
 - value of, 278
 - Production networks
 - GenII honeynets in, 257, 258*f*
 - Honeyd deployment on, 163
 - Production systems
 - in honeynets, 229
 - and Honeypots, 40, 348
 - retiring, as Honeypots, 42, 43*f*
 - spoofed attacks from, 54
 - Propagation, and multiple vulnerability scans, 22–24
 - Provos, Niels, 84, 142
 - Proxying, in Honeyd, 159*f*, 161–162
- R**
- rain forest puppy, Windows Web Server emulation script by, 161

INDEX

- Random* character, in Specter behavior settings, 123
 - Ranum, Marcus, 38, 83
 - Recourse, 85
 - Red Hat Linux, 6, 7f, 12
 - Remote alerts, in Specter, 113
 - Remote connections, 179–180, 319, 331
 - Remote logging, 253, 266
 - Remote management
 - and BackOfficer Friendly, 98–99
 - of ManTrap, 213–214, 213f
 - of Specter, 127, 128f
 - Research Honeypots
 - advanced blackhats studied with, 395–396
 - alerts in, 310
 - BackOfficer Friendly as, 91–92
 - commercial use of, 394
 - in distributed environments, 396–397
 - for early warning and detection, 69, 394
 - fingerprinting of, 54
 - honey cards used in, 395–396
 - Honeyd as, 142
 - honeynets as, 231–232, 362
 - Honeypots for, 278
 - jails as, 185–186
 - location of, 286, 287f, 290–291
 - ManTrap as, 198–199
 - number of, determining, 285
 - port monitors as, 170, 181
 - vs. production Honeypots, 46
 - purpose of, 44–46, 68
 - response procedure for, 317, 327
 - role of, defining, 279
 - specialization of, 392–393
 - Specter as, 112–113, 134
 - trend analysis with, 235
 - unknown exploits identified with, 396
 - uses of, 69–70
 - value of, 278
 - Reset option, for service emulation, 160
 - Resolved names, vs. IP addresses, in data capture, 295
 - Resource exhaustion, Honeypots and, 51–52
 - Response. *See* Incident response
 - Return on investment, in Honeypots, 52–53
 - Risk
 - from auto-rooters, 29
 - and BackOfficer Friendly, 102
 - with high-interaction Honeypots, 82
 - and Honeyd, 165
 - with honeynets, 274–275
 - with Honeypots, 55
 - with Honeypots, mitigating, 302–305, 349–350
 - identification of, with BackOfficer Friendly, 92–93
 - with jails, 55, 190–191
 - and level of interaction, 77, 77f, 281
 - with low-interaction Honeypots, 78
 - with ManTrap, 225–227
 - with medium-interaction Honeypots, 81
 - and Specter, 137–138
 - updating and, 338
 - Roesch, Marty, 37
 - Rootkits, 2, 271
 - Routers, 248, 294
 - rpc.statd exploit, 2, 17
 - RST packets, closing connection with, 98, 99f
 - Russell, Ryan, 174
- S**
- Salgado, Richard, 370–371
 - Scanning, 13, 21–22
 - Screen shots, remote forwarding of, 254

- Script(s)
 - for attacks, 366
 - in Honeyd, 160–161, 161*f*
 - for ManTrap cage customization, 210
- Script kiddies, 11–12, 14
- Script option, for service emulation, 160
- Secure character, in Specter behavior settings, 121
- Secure Shell (SSH), 125, 365
- Security policy, 70, 316, 368–369
- Security testing, with ManTrap, 199
- SecurityFocus.com, 174, 366, 394
- Sendmail Honeypot, 169
- September 11, 2001, hacking after, 28
- Service Provider Protection exception, 379–380
- Services
 - emulation of
 - in BackOfficer Friendly, 98, 102
 - in Honeyd (*See* Honeyd, service emulation in)
 - with port monitors, 180–181
 - in Specter, 110–111, 123–124, 125*f*
 - in ManTrap, value of, 197
 - vulnerable, 14, 182–183
- SESSION files, for keystroke capture, 329–330, 330*f*
- Short Mail, 129, 130, 130*f*
- Signatures
 - in Honeypot detection, 349–350
 - in Intrusion Detection Systems gateway, 257, 264
 - in jail identification, 190
- Silk Rope, for Back Orifice, 89
- Simple Mail Transfer Protocol. *See* SMTP
- Smoke Detector Honeypot appliance, 391
- SMTP (Simple Mail Transfer Protocol)
 - in BackOfficer Friendly, 94, 97
 - in Specter, configuration of, 123
 - SMTP banner, in Specter, for information gathering, 136
- Sniffers. *See also* Snort
 - and Honeyd, 164
 - with Honeyd, 292, 292*f*
 - Intrusion Detection Systems as, 222–223
 - for jails, 189, 189*f*
 - ManTrap and, 196–197, 217, 222–223
 - syslog information capture with, 293
- Snort. *See also* Hogwash IDS gateway
 - configuration file for, 329, 407–409
 - for data capture, 266, 267, 267*f*
 - development of, 37
 - as honeynet Intrusion Detection System, 252–253
 - with Honeyd, 292, 292*f*
 - for jails, 189, 189*f*
 - keystroke capture with, 329–330, 330*f*
 - log capture of, for data analysis, 327–329, 328*f*, 329*f*, 332, 333*f*
 - packet payload from, 329
 - timestamping in, 330
- Song, Dug, on blackholing, 144–145
- Specter
 - advantages and disadvantages of, 138*t*
 - alerts in, 113, 126–127, 129–131, 130*f*, 131*f*
 - vs. BackOfficer Friendly, 110
 - behavior setting in, 114–115
 - character in, configuration of, 121–123, 122*f*, 123*f*
 - configuration of, 119, 120*f*
 - for alerts, 126–127
 - character in, 121–123, 122*f*, 123*f*
 - information gathering in, 124–126
 - operating system emulation in, 120–121
 - password files in, 125–126

INDEX

Specter continued

- service emulation in, 123–124, 125f
- traps in, 124–125
- customizing, 112, 350
- deception with, 112, 114
- description of, 84
- deterrence with, 112, 114–115
- effectiveness of, optimizing, 348–349
- fingerprinting of, 112, 118–119
- flexibility of, 112
- information gathering with, 112–113,
129, 133–137
 - configuration of, 124–126
 - risk in using, 136–138
- initialization of, 127
- installation of, 119
- IP stack emulation and, 118–119, 138
- level of interaction of, 110
- operating system emulation in,
111–112, 115–118, 116f, 117f
 - configuration of, 120–121
 - risk in, 138
- operation of, 115–119
- overview of, 109–112
- password files in, 110, 117–118,
125–126
- port listeners in, 113, 115–118
- prevention with, 278
- remote management of, 127, 128f
- as research Honeypot, 112–113, 132
- risk from using, 137–138
- service emulation in, 110–111, 111f,
123–124, 125f
- system requirements for, 109
- traps in, 111, 124–125
- updating, 339
- value of, 112–115
- vulnerability emulation in, 110, 111f,
114

Spoofing. *See specific types*

- SSH (Secure Shell), 125, 365
- State law, consent under, 377
- Stoll, Clifford, hacker tracking by, 34–35
- strace(1), for jail monitoring, 190
- Strange* character, in Specter behavior
settings, 114, 122
- Sub7 Trojan
 - and Leaves worms, 38–39, 178–181
 - overview of, 178, 179f
 - in Specter configuration, 125
- SUN-RPC, in Specter configuration, 125
- Swatch, for syslog monitoring, 164–165,
352
- Syslog/syslogd
 - disabling, 253
 - in Honeyd, 163–165, 164f
 - maximizing, 293
 - and sniffers, 293
 - in Specter, 135, 135f
- System, 6, 14
- System, compromised. *See Compromised
systems*
- System logs
 - data aggregation with, 61
 - maintaining, 264
 - reviewing, 267, 267f, 356–357, 358
- System processes, in ManTrap cages,
204–205, 205f

T

- Targets of choice
 - deception and deterrence and, 57
 - GenI technologies and, 243
 - hacking, 25–27
 - honeynets as, 262–263
- Targets of opportunity. *See also*
Auto-rooters; Worm(s)
 - deception and deterrence and, 57

- GenI technologies and, 243
 - hacking, steps in, 14–15
 - TASK, for forensic analysis, 332
 - TCP/IP protocol suite, layers of, 148–152, 148*f*
 - Telnet, 97, 123
 - Telnet banner, in Specter, 136
 - Templates, in Honeyd configuration, 158, 159*f*
 - Test beds, honeynets as, 238, 364
 - Testing, for risk mitigation, 305
 - Time zones, in data capture, 241
 - Timestamp, in Snort logs, 330
 - Tiny Honeypot, 169
 - "To Build a Honeypot," 230
 - Tracer, for information gathering, 136
 - Traceroute, for information gathering, 136
 - Transactional data, under Wiretap Act and Pen/Trap statute, 375
 - Transport layer, purpose of, 148*f*, 149
 - Traps, 111, 124–125
 - Trend analysis
 - alerts archive in, 314–315
 - data analysis in, 335
 - with honeynets, 235–236
 - with low-interaction Honeypot logs, 324–325
 - Tripwire, for MD5 checksum, 337
 - truss(1), for jail monitoring, 190
 - TTY Watcher, for remote data capture, in honeynets, 253–254
- U**
- UDP services, in Honeyd, 143–144
 - Ullrich, Johannes B., 180–181
 - Updates, 338–339, 355–356, 365
 - Uptime, spoofing, in Honeyd, 162
 - U.S. Constitution, privacy under, 372–374
 - U.S. Patriot Act, privacy and, 380
 - User Mode Linux (UML), for virtual honeynets, 262
 - "Using Chroot Security" (Chuvakin), on jail breaking, 190–191
- V**
- Virtual honeynets, 261–262
 - Virtual operating systems
 - in Honeyd, 143, 155, 156–157, 156*f*
 - in medium-interaction Honeypot, 80
 - in Specter, 111–112, 115–118, 116*f*, 117*f*, 120–121, 138
 - VMWare, for virtual honeynets, 262
 - Vulnerabilities
 - attack on, analysis of, 365–366
 - emulation of, in Specter, 110, 111*f*, 114
 - identification of, 14
 - jails for, 182–183
 - in ManTrap, 195–196, 216
 - patches for, 25
 - scanning for multiple, 22
 - updates for, 338–339
- W**
- Whois, in Specter, for information gathering, 136
 - Wiretap Act (Title III), privacy under, 372, 374–380
 - Worm(s)
 - capture of, 38, 69
 - Honeypot selection for, 281, 361
 - with netcat, 174–177, 175*f*, 176*f*, 177*f*
 - with port monitors, 172–173
 - capture statistics for, 13
 - for CPU cycle takeover, 28
 - definition of, 19
 - devastation of, 19–21
 - growth in, 38
 - mutation of, 29



INDEX

wwwhack, 16f
method of, 15

X
X, for fingerprinting, 118, 155

Z
Zero0, 271

