
Index

A

- A switch, P0f, 205
- a switch, Tethereal, 141
- Abagnale Frank W., *Art of the Steal: How to Protect Yourself and Your Business from Fraud*, 421
- Absolute BSD: The Ultimate Guide to FreeBSD* (Lucas), 417
- Absolute OpenBSD: UNIX for the Practical Paranoid* (Lucas), 418
- Abuse of services, 16
- Access control in best practices, 350
- access-list command, 272
- Access lists, 249
- access violations phrase, 249
- Accessing
 - sensors, 98–99
 - console access, 99
 - in-band remote access, 100–101
 - out-of-band remote access, 101–102
 - zone traffic, 51
 - hubs, 52–56
 - inline devices, 76–84
 - SPAN ports, 56–63
 - summary, 84
 - taps. *See* Taps (test access ports)
- Accountability features in Sguil, 322
- Accounting, Cisco, 249–255
- "Achilles' Heel in Signature-Based IDS: Squealing False Positives in Snort" (Patton, Yurcik, and Doss), 733–734
- ACID interface, 318–319
- Active directory in Bro, 293
- Active field in Flow-cat, 231
- "Active Mapping: Registering NIDS Evasion Without Altering Traffic" (Shanker and Paxson), 735–736
- Active scanners, 653–654
- Add Expression command, 166
- additional field in Bro logs, 295
- Address Resolution Protocol (ARP)
 - headers, 666–668
 - in Packit, 523
 - traffic
 - with cable modem users, 355–356
 - filtering, 77–79, 356–358
 - tracking, 596
- adduser command, 287
- AFCERT (Air Force Computer Emergency Response Team), 753–754
- AFIWC (Air Force Information Warfare Center), 586–589
- Aimes, Aldrich, 634
- Air Force systems, 212
- Airtools, 93

INDEX

- alert.\$BROID file, 293
 Alert-centric intrusion detection papers
 "Achilles' Heel in Signature-Based IDS: Squealing
 False Positives in Snort", 733–734
 "Active Mapping: Registering NIDS Evasion
 Without Altering Traffic", 735–736
 "Application of Pattern Matching in Intrusion
 Detection", 718–719
 "Base-Rate Fallacy and Its Implications for the
 Difficulty of Intrusion Detection", 729–731
 "Bro: A System for Detecting Network Intruders
 in Real-Time", 722–723
 "Common Intrusion Detection Framework",
 727
 "Data Mining Approaches for Intrusion
 Detection", 727–728
 "EMERALD: Event Monitoring Enabling
 Responses to Anomalous Live
 Disturbances", 719–720
 "Enhancing Byte-Level Network Intrusion
 Detection Signatures with Context",
 736–739
 "GrIDS: A Graph-Based Intrusion Detection
 System for Large Networks", 719
 "IDES: The Enhanced Prototype: A Real-Time
 Intrusion-Detection Expert System",
 715–716
 "Implementing a Generalized Tool for Network
 Monitoring", 721–722
 "Insertion, Evasion, and Denial of Service:
 Eluding Network Intrusion Detection",
 723–726
 "NetSTAT: A Network-Based Intrusion Detection
 Approach", 728–729
 "Practical Automated Detection of Stealthy
 Portscans", 735
 "Real-Time Network-Based Anomaly Intrusion
 Detection", 733
 "Snort—Lightweight Intrusion Detection for
 Networks", 731–733
 "System for Distributed Intrusion Detection",
 717–718
 "Towards Detecting Intrusions in a Networked
 Environment", 716–717
 "Towards Faster String Matching for Intrusion
 Detection or Exceeding the Speed of Snort",
 734–735
- Alerts, 285
 in ACID, 319
 in Bro, 285–287
 BRA installation, 287–292
 capabilities and limitations, 297
 output files, 292–297
 in I&W process, 26–27
 in Prelude, 298
 capabilities and limitations, 313–315
 events in, 311–314
 installing, 299–307
 output files, 307–309
 PIWI installation, 309–311
 in real-time detection, 38–39
 SCAN FIN, 498–505
 in Sguil. *See* Sguil
 Truncated Tcp Options, 492–498
- Allen, Julia, "State of the Practice of Intrusion
 Detection Technologies", 686
- Amap tool, 411
- Ampersand character (&) in Snort, 153
- Analysis, 28
- Analysts
 in assessment process, 383–384
 attacks on, 647–648
 training for. *See* Training for analysts
- Anderson, Annelise, *FreeBSD: An Open-Source
 Operating System for Your Personal Computer*,
 417
- Anderson, James P.
 "Computer Security Technology Planning Study",
 687
 "Computer Security Threat Monitoring and
 Surveillance", 686–687
- Anderson, Ross J., *Security Engineering: A Guide to
 Building Dependable Distributed Systems*, 420
- Andrews, Chip, *SQL Server Security*, 413
- Anomalies, paper on, 714–715
- Anomaly-based IDSs, 369
- Anomaly detection, 757
 approaches, 759–760
 vs. explicit signature techniques, 762
 future of, 654–656
 general approach, 758–759
 implementation, 760–761
 introduction, 757–758
 warnings, 761

- Anonymity, 584
 client attacks for, 601–602
 decoys for, 640
 netblocks for, 597–600
 public intermediaries for, 602–603
 spoofed source addresses for, 589–597
 stepping-stone attacks for, 584–589
 trusted hosts for, 599
- Anti-Hacker Tool Kit* (Jones, Shema, and Johnson), 413
- Antivirus products, signature-based, 655
- Apisdorf, Joel, "OC3MON: Flexible, Affordable, High Performance Statistics Collection", 695–696
- Appearances in evading detection, 634–638
- "Application of Pattern Matching in Intrusion Detection" (Kumar and Spafford), 718–719
- Application relevance, 120
- Arbaugh, William A., *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*, 415
- Ardita, Julio Cesar, hacking by, 585–586
- Argus utility, 234–236
 as emergency NSM, 383
 reference for, 412
 for session data, 474–475
 Argus server, 236–237
 Ra client, 238–242
- Arkin, Ofir, Xprobe2 by, 558
- ARP (Address Resolution Protocol)
 headers, 666–668
 in Packit, 523
 traffic
 with cable modem users, 355–356
 filtering, 77–79, 356–358
 tracking, 596
- arp option, ifconfig, 51
- Art of Deception: Controlling the Human Element of Security* (Mitnick and Simon), 414
- Art of the Steal: How to Protect Yourself and Your Business from Fraud* (Abagnale), 421
- Ascher, David, *Learning Python*, 420
- ASCII mode in Snort, 152
- ASIM (Automated Security Incident Measurement) system, 212, 753–754
- Assembly language, 418–419
- Assessment, 5
 analyst feedback in, 383–384
 in best practices, 347–348
- Assets and asset value, 6
 in Polish Ministry of Defense case study, 10
 prioritization of, 396
 in risk equation, 9
- Astashonok, Slava, Fprobe for, 220
- Attacker classes, 45
- Attacks
 in reference intrusion model, 106–118
 tactics in, 583–584
 anonymity. *See* Anonymity
 degrading and denying collection, 639–647
 evading detection. *See* Evading detection
 normal appearance, 634–638
 self-inflicted NSM problems, 647–649
 tools for, 521
 Cisco IOS DOS attacks, 567–570
 Fragroute, 534–547
 IP Sorcery, 530–534
 LFT, 548–558
 Microsoft RPC exploitation, 575–581
 Packit, 521–530
 Solaris sadmind exploitation, 570–575
 Xprobe2, 558–566
- Attempted Unauthorized Access incident category, 373
- Auditing
 access control rules for, 350
 defensible networks, 21
 in in-house NSM solutions, 400
- Automated Incident Reporting project, 318
- Automated Security Incident Measurement (ASIM) system, 212, 753–754
- Axelsson, Stefan
 "Base-Rate Fallacy and Its Implications for the Difficulty of Intrusion Detection", 729–731
 "Intrusion Detection Systems: A Survey and Taxonomy", 686
- B**
- B/Pk field in Flow-cat, 231
- b switch
 Ifstat, 257
 Snort, 152, 545
 Tethereal, 141
- B switch, Ntop, 279
- Bace, Rebecca Gurley, *Intrusion Detection*, 686
- Back doors, 17–18

INDEX

- Background, Snort in, 153
 Backlog queues, 591
 Baker, Doris M., *Cryptography Decrypted*, 414
 Balupari, Ravindra, "Real-Time Network-Based Anomaly Intrusion Detection", 733
 Bandwidth
 Bmon for, 258–259
 network links, 56
 Bardwell, Joseph, *Troubleshooting Campus Networks: Practical Analysis of Cisco and LAN Protocols*, 415
 Barford, Paul
 "Characteristics of Network Traffic Flow Anomalies", 714
 home page for, 752
 "Signal Analysis of Network Traffic Anomalies", 714–715
 Barman, Scott, *Writing Information Security Policies*, 421
 "Base-Rate Fallacy and Its Implications for the Difficulty of Intrusion Detection" (Axelsson), 729–731
 Baselines for statistics, 248
 Batch analysis, 38
Beginning Databases with PostgreSQL (Stones and Matthew), 418
 Bejtlich, Richard, "Interpreting Network Traffic: An Intrusion Detector's Look at Suspicious Events", 709–710
 Bellovin, Steven M.
 "Packets Found on an Internet", 704–705
 TCP/IP stack weaknesses pointed out by, 591
 "There Be Dragons", 705
 Beowulf Project, 66
 Berkeley Packet Filter (BPF) interfaces, 97
 with Fragroute, 540–547
 paper on, 695
 with Tcpdump, 135–140
 Best practices, 347
 access control, 350
 assessment, 347–348, 383–384
 defined security policies, 348–349
 detection, 354–355
 collection phase, 355–360
 escalation phase, 377–380
 identification phase, 360–371
 validation phase, 371–377
 protection, 349–350
 proxies, 351–354
 response process, 380–383
 traffic scrubbing, 351
 Bevan, Matthew, attack by, 586
 BGP (Border Gateway Protocol), 597
 Big-endian conventions, 197–198, 200
 Binary mode in Snort, 152
 BIND
 exploits against, 466–471
 versions of, 465–466
 Bing, Matt, Tcpreplay by, 179
 Birkholz, Erik Pace, *Special Ops: Host and Network Security for Microsoft, UNIX, and Oracle*, 413
 BitTorrent system, 454
 Black Hat conference, 425
 Blaster worm, 576
 Blind TCP spoofing, 590
 Blinking red lights, 375
 Blocking web defacers, 616–617
 Bmon utility, 258–260
 Bogon addresses, 593–594
 Bomb threats, 647
 Bonding for virtual interfaces, 66–68
 Border Gateway Protocol (BGP), 597
 Border routers for scans, 638
 Bounds, Darren, Packit by, 521
 bourque for packet floods, 528–529
 BPF (Berkeley Packet Filter) interfaces, 97
 with Fragroute, 540–547
 paper on, 695
 with Tcpdump, 135–140
 BRA (Bro Reusable Architecture), 286–292
 Braden, Robert T., "NNStat: Internet Statistics Collection Package", 741–742
 brconfig command, 79–80
 Breach of services, 17
 Brentano, James, "System for Distributed Intrusion Detection", 717–718
 Bridges
 building, 79–81
 detecting, 77–79
 for inline devices, 76
 Pf with, 81–82
 testing, 82–83
 "Bro: A System for Detecting Network Intruders in Real-Time" (Paxson), 722–723

- bro_id keyword, 293
 Bro Reusable Architecture (BRA), 286–292
 Bro utility, 285–287
 BRA installation, 287–292
 capabilities and limitations, 297
 output files, 292–297
 Broadcasting events in Prelude, 313
 Browser limitations, 318
 Brute-force cracking techniques, 113
 BSD-Airtools tool, 411
 "BSD Packet Filter: A New Architecture for User-Level Packet Capture" (McCanne and Jacobson), 695
 Buffer-overflow attacks, 332–339
 Building filtering bridges, 79–81
Building Secure Software: How to Avoid Security Problems the Right Way (Viega and McGraw), 420
 Bullard, Carter
 Argus by, 234
 "Remote Packet Capture", 652
 Burch, Hal, Internet Mapping Project by, 611
 Burst traffic with taps, 73
 Bykova, Marina, "Detecting Network Intrusions via a Statistical Analysis of Network Packet Characteristics", 710–711
 Byte order
 big-endian and little-endian conventions, 197–202
 network, 204
- C**
C Primer Plus (Prata), 420
C++ Primer Plus (Prata), 420
 -c switch
 Argus, 236
 ping, 361–362
 Tcpcmdump, 127
 Tcpcflow, 183–184
 Tethereal, 144
 -C switch in Snort, 545
 Cable modems, ARP traffic with, 355–356
 Caceres, Ramon
 "Measurement and Analysis of IP Network Usage and Behavior", 697
 "Measurements of Wide Area Internet Traffic", 702–703
 Caged workstations, 77
 Cages, 77
 CAIDA (Cooperative Association for Internet Data Analysis), 372
 CanSecWest conference, 425
 Capture Options window, 162–163
 Capture performance, device polling for, 98
 Carrier Sense Multiple Access/Collision Detection (CSMA/CD), 54
 Castro, Simon, Covert Channel Tunneling Tool by, 513
 Categories for event incidents, 371–374
 CCEVS (Common Criteria Evaluation and Validation Scheme) Validation Body, 360
 CCTT (Covert Channel Tunneling Tool), 513
 Centralized analysis in NSM future, 652–653
 Certified Information Systems Security Professional (CISSP), 406
 Chained covert channels, 505–517
 Chan, Philip, home page for, 752
 Chaosreader program, 123
 "Characteristics of Network Traffic Flow Anomalies" (Barford and Plonka), 714
 Charter high schools, 409
 Checksum Fixer feature, 195–196
 Checksums
 in Netdude, 196
 in Tcpcmdump, 134
 Cheswick, Bill
 "Evening with Berferd in Which a Cracker Is Lured, Endured, and Studied", 742–743
 Internet Mapping Project by, 611
 CHM Plans case study, 105–118
 Cho, Kenjiro
 Tcpcmdstat by, 266
 Ttt by, 264
 Christy, Jim, on Rome Labs attack, 588
 CIS (COM Internet Services), 576
 Cisco accounting, 249–255
 Cisco IOS
 denial-of-service attacks on, 567–570
 HTTP authentication vulnerability, 657
 licenses for, 416–417
 Cisco Threat Response (CTR), 654
 CISSP (Certified Information Systems Security Professional), 406
 Citeseer Scientific Literature Digital Library, 685

INDEX

- Claffy, Kimberly, "OC3MON: Flexible, Affordable, High Performance Statistics Collection", 695–696
- Clarke, Arthur C., 35
- Client attacks, 601–602
- Clock adjustments in Editcap, 174
- cmdasp.asp script, 632
- Cmdwatch utility, 142
- CND (Computer Network Defense), 753
- CNT column in Sguil, 322
- Codes of Ethics, 406–407
- Coit, C. Jason, "Towards Faster String Matching for Intrusion Detection or Exceeding the Speed of Snort", 734–735
- Collateral damage packets, 749
- "Collect everything, then summarize" method, 213
- Collection, 28, 38
 - all traffic, 37
 - degrading and denying, 639
 - decoys in, 639–641
 - sensor attacks in, 643–647
 - separating analysts from consoles, 647
 - volume attacks in, 641–643
 - full content data. *See* Full content data separate, 68–71
- Collection phase in detection, 355–360
- Collectors for sessions data, 214
- Collisions
 - with half-duplex devices, 54–55
 - with hubs and taps, 72
- COM Internet Services (CIS), 576
- "Combining Cisco NetFlow Exports with Relational Database Technology for Usage Statistics, Intrusion Detection, and Network Forensics" (Navarro, Nickless, and Winkler), 713
- Combining tap outputs
 - with specialized hardware, 71–72
 - on switch SPAN ports, 71
- Combs, Gerald
 - Editcap and Mergecap by, 173
 - Ethereal by, 162
 - Tethereal by, 140
- Comer, Douglas E., "Probing TCP Implementations", 705–706
- Command line in Bro, 297
- Command-line packet summarization, 189–190
- Common Criteria Evaluation and Validation Scheme (CCEVS) Validation Body, 360
- Common Criteria for IDSs, 359
- "Common Intrusion Detection Framework" (Kahn, Porras, Staniford-Chen, and Tung), 727
- Common Reliable Accounting for Network Element (CRANE) protocol, 214
- Community strings in SNMP, 273–274
- Compiling Bro, 291
- Complete Guide to FreeBSD* (Lehey), 417
- Complimentary technologies papers
 - "1999 DARPA Off-Line Intrusion Detection Evaluation", 745–746
 - "Evening with Berferd in Which a Cracker Is Lured, Endured, and Studied", 742–743
 - "Experiences Benchmarking Intrusion Detection Systems", 750–751
 - "Inferring Internet Denial-of-Service Activity", 749
 - "Know Your Enemy: The Tools and Methodologies of the Script Kiddie", 746–747
 - "Methodology for Testing Intrusion Detection Systems", 743
 - "Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics", 748–749
 - "NNStat: Internet Statistics Collection Package", 741–742
 - "Passive Vulnerability Detection", 743–745
 - "Passive Vulnerability Scanning Introduction to NeVO", 752
 - "Security Holes: Who Cares?", 751–752
 - "Stalking the Wily Hacker", 739–741
- Comprehensive Perl Archive Network (CPAN) system, 287
- Compromise phases, 14–15
 - consolidation, 17
 - detection, 19
 - exploitation, 16–17
 - pillage, 18–19
 - reconnaissance, 15–16
 - reinforcement, 17
- Compromised systems
 - determining, 489–490
 - RPC exploitation against, 575–581
- Computer Crime and Security Survey, 32
- Computer crime laws, 585–586
- Computer Network Defense (CND), 753
- Computer science degrees, 408–409

- "Computer Security Technology Planning Study" (Anderson), 687
- "Computer Security Threat Monitoring and Surveillance" (Anderson), 686–687
- Conferences, security, 425
- config.pl file, 311
- Configuration files, PIWI, 311
- configure command for SPAN ports, 57
- Connection-oriented protocols, 211
- Connectionless protocols, 211, 593
- Consoles
 - for sensors, 99
 - separating analysts from, 647
 - for sessions data, 214
- Consolidation phase
 - in compromise, 17
 - in encryption, 631
 - intruder detection in, 19
- Containment, 9
- Context in I&W process, 26
- Contextual information, 653
- Contextual signatures, 738
- Conversation lists, 170
- Cooperating tools, 317
- Cooperative Association for Internet Data Analysis (CAIDA), 372
- Coordinated traceroutes, 607
- Correlation analysts, 649
- Cost of replacement, 9
- count field in NetFlow, 216
- Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses* (Skoudis), 413
- Countermeasures, 11
- Country of origin in attacks, 600–601
- Covert Channel Tunneling Tool (CCTT), 513
- Covert channels
 - chained, 505–517
 - in consolidation, 18
- CPAN (Comprehensive Perl Archive Network) system, 287
- CPUs for sensors, 94
- Cracker study, 742–743
- Cracking usernames and passwords, brute-force techniques for, 113
- CRANE (Common Reliable Accounting for Network Element) protocol, 214
- CRC (Cyclical Redundancy Check) values with taps, 75
- Crime laws, 585–586
- crontab for Bro, 291–292
- Crooks, LeRoy, 754
- Crusoe Correlated Intrusion Detection System, 318
- Cryptcat tool, retrieving, 631–632, 634
- Cryptography Decrypted* (Mel and Baker), 414
- CSMA/CD (Carrier Sense Multiple Access/Collision Detection), 54
- CTR (Cisco Threat Response), 654
- Curr, John, SANCIP project by, 320
- Currency in defensible networks, 23
- CyberRegs: A Business Guide to Web Property, Privacy, and Patents* (Zoellick), 421
- Cyclical Redundancy Check (CRC) values with taps, 75
- D**
- d switch
 - Argus, 236
 - Ipcad, 255
 - IPsumdump, 190
 - LFT, 550, 552
 - Ngrep, 188
 - P0f, 208
 - Tcpslice, 176
- D switch
 - IPsumdump, 190
 - LFT, 550
 - P0f, 208
 - Snort, 153
- DARPA, paper on, 746
- Data collection. *See* Collection
- "Data Mining Approaches for Intrusion Detection" (Lee and Stolfo), 727–728
- Database integrity, 6
- Datagrams vs. segments and packets, 125
- Datapipe tool, 338
- Datastream Cowboy, attack by, 586, 589
- date command
 - for Snort, 152
 - for timestamps, 132–133
- DCOM (Distributed Component Object Model) services, 575–576
- DCPhoneHome project, 352
- dd command, 180–181
 - across Internet, 607DDoS (distributed denial-of-service) attacks
 - in reference intrusion model, 114–117

INDEX

- Decision makers in escalation phase, 377
- Decisions, Sguil for, 329–331
- Decoys, 639–641
- Dedicated sensors, 482
- Defense Intelligence Agency (DIA), 27
- Defensible networks, 20
 - freedom to maneuver in, 21–22
 - monitoring, 20–21
 - number of services in, 23
 - patches in, 23–24
- Defensive tools, 412
- Deficiencies, 12
- Defined security policies, 348–349
- Degrading collection, 639
 - decoys in, 639–641
 - sensor attacks in, 643–647
 - separating analysts from consoles, 647
 - volume attacks in, 641–643
- Degrees for analysts, 408–409
- delay first option in Fragtest, 535
- Demilitarized zones (DMZs)
 - in in-house NSM solutions, 398–399
 - monitoring, 49–50
 - session data from, 475–479
- Denial-of-service attacks
 - backlog queues in, 591
 - on Cisco IOS, 567–570
 - distributed, 607
 - as validation category, 373
- Denning, Dorothy E.
 - on insider attacks, 33
 - "Intrusion-Detection Model", 689
 - "Requirements and Model for IDES---A Real-Time Intrusion-Detection Expert System", 43, 688
 - on security limitations, 43
- Denying collection, 639
 - decoys in, 639–641
 - sensor attacks in, 643–647
 - separating analysts from consoles, 647
 - volume attacks in, 641–643
- Department of Homeland Security (DHS) Advisory System, 8
- Deployment considerations, 45, 360
 - accessing zone traffic, 51
 - hubs, 52–56
 - inline devices, 76–84
 - SPAN ports, 56–63
 - summary, 84
 - taps, 63–76
 - monitoring zones and threat models, 45–51
 - sensor architecture, 93–98
 - sensor management, 98–102
 - wireless monitoring, 85–93
- Deraison, Renaud, "Passive Vulnerability Scanning Introduction to NeVO", 752
- Deri, Luca, 214
 - on device polling, 98
 - Ntop by, 278
- DeSchon, Annette L., "NNStat: Internet Statistics Collection Package", 741–742
- Descriptive statistics, 248
- Design, vulnerabilities from, 8
- "Design and Deployment of a Passive Monitoring Infrastructure" (Fraleigh), 697–698
- Detail in full content data
 - Tcpdump for, 134–135
 - Tethereal for, 146–149
- "Detecting Network Intrusions via a Statistical Analysis of Network Packet Characteristics" (Bykova, Ostermann, and Tjaden), 710–711
- Detection, 5, 29, 34–35
 - alert-centric. *See* Alert-centric intrusion detection papers
 - anomaly. *See* Anomaly detection
 - evading. *See* Evading detection
 - filtering bridges, 77–79
 - in I&W process, 26
 - of odd orders, 386–393
 - phases in, 354–355
 - collection, 355–360
 - escalation, 377–380
 - identification, 360–371
 - validation, 371–377
 - in phases of compromise, 19
 - real-time, 38–39
 - through sampling, 35–36
 - through traffic analysis, 36–37
- Deviations, statistics for, 248
- Device polling, 98
- Devious attacks against human targets, 648
- DHCP (Dynamic Host Configuration Protocol), 615
- DHS (Department of Homeland Security) Advisory System, 8
- DIA (Defense Intelligence Agency), 27

- Dif field in Flow-cat, 230
 - Digital communications standards, 56
 - Digital forensics, 41
 - Disgruntled employees, 33
 - Display Filters command, 166
 - Distributed attacks, 607–615
 - DDoS
 - across Internet, 607
 - in reference intrusion model, 114–117
 - Distributed Component Object Model (DCOM)
 - services, 575–576
 - Distributed Director tool, 457
 - Distributed John tool, 615
 - Distributed password-cracking programs, 615
 - Dittrich, Dave
 - on syn4k.c, 710
 - Tcpdstat by, 266
 - DMZs (demilitarized zones)
 - in in-house NSM solutions, 398–399
 - monitoring, 49–50
 - session data from, 475–479
 - DNS port 53 traffic, 433
 - malicious
 - TCP, 466–471
 - UDP, 459–466
 - normal
 - TCP, 442–448
 - UDP, 434–442
 - suspicious
 - TCP, 455–459
 - UDP, 448–455
 - dnsquery command, 443–444
 - Do-it-yourself taps, 75
 - dOctets field in NetFlow, 217
 - Doss, David, "Achilles' Heel in Signature-Based IDS: Squealing False Positives in Snort", 733–734
 - Downloaded files by intruders, 337–338
 - dPkts field in NetFlow, 217
 - Dragon system, 744
 - Drawbridge filtering bridge, 692
 - drop first option in Fragtest, 535
 - Dscan scanner, 607–610
 - Dscand agent, 607–609
 - Dshield IP Lookup option in Sguil, 326
 - dst_as field in NetFlow, 217
 - dst_mask field in NetFlow, 217
 - dstaddr field in NetFlow, 217
 - DstP field in Flow-cat, 230
 - dstport field in NetFlow, 217
 - Dual monitors, 348
 - DUMP Reply, 325
 - dup first option in Fragtest, 536
 - duration field in Bro logs, 295
 - Dynamic Host Configuration Protocol (DHCP), 615
- E**
- E-mail encryption, 618–624
 - e switch
 - Tcpdump, 134–135
 - Trafshow, 261
 - E switch in LFT, 557–558
 - ECN (Explicit Congestion Notification) option, 562
 - Edit Where Clause field, 327
 - Editcap utility, 123, 173–174
 - Edney, Jon, *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*, 415
 - Egress control, 47
 - Egress filters, 21, 593–595
 - 802.1x protocol, 22
 - Element of surprise in defense, 638
 - Elson, Jeremy, Tcpflow by, 182
 - "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances" (Porras and Neumann), 719–720
 - Emergency network security monitoring, 381–382, 386–393
 - EMERGENCY NSM, 382
 - Encryption
 - with chained covert channels, 511
 - e-mail, 618–621
 - stages in
 - consolidation, 631
 - exploitation, 624–628
 - pillage, 632–634
 - reconnaissance, 621–624
 - reinforcement, 628–631
 - WEP, 90–91
 - engine_id field in NetFlow, 216
 - engine_type field in NetFlow, 216
 - Engineer ethics code, 406–407
 - "Enhancing Byte-Level Network Intrusion Detection Signatures with Context" (Summer and Paxson), 736–739
 - Enterprise-class switch, 56

INDEX

- Enterprise hosts in perimeters, 48
 - Entry-level analysts, training for, 423–424
 - Escalated decisions in Sguil, 324, 330
 - Escalated Events tab, 330
 - Escalation phase in detection, 28–29, 377–380
 - ESSIDs (Extended Service Set Identifiers), 92
 - Etherape utility, 191–192
 - Ethereal option in Sguil, 324
 - Ethereal (force new) option in Sguil, 324
 - Ethereal utility, 162
 - basic usage, 162–163
 - for encrypted e-mail, 620–621
 - for full content data, 164–167
 - Protocol Hierarchy Statistics sequence in, 169–170
 - for rebuilding sessions, 167, 169, 338
 - reference for, 412
 - for sadmin exploitation, 571–572
 - for separate traffic collection, 68
 - for TCP traffic
 - malicious, 467–468
 - normal, 447
 - sequence numbers in, 677, 679
 - for Truncated Tcp Options alerts, 492–493
 - for UDP traffic
 - malicious, 463–464
 - normal, 438
 - for Unicode attacks, 625–628
 - Ethernet
 - channel bonding, 66
 - frames in, 664–665
 - in Packit, 523–524
 - Ethernet II frames, 664
 - Ethernet taps, ports for, 63–64
 - Ettercap tool, 411
 - Evading detection, 603
 - in anomaly detection techniques, 762
 - degrading and denying collection, 639
 - decoys in, 639–641
 - sensor attacks in, 643–647
 - separating analysts from consoles, 647
 - volume attacks in, 641–643
 - distributing attacks, 607–615
 - encryption for, 618–621
 - consolidation stage, 631
 - exploitation stage, 624–628
 - pillage stage, 632–634
 - reconnaissance stage, 621–624
 - reinforcement stage, 628–631
 - normal appearance for, 634–638
 - timing of attacks, 604–607
 - in web defacement attacks, 616–617
 - Evaluating managed security monitoring providers, 393–396
 - "Evening with Berferd in Which a Cracker Is Lured, Endured, and Studied" (Cheswick), 742–743
 - Event History option in Sguil, 324
 - Events
 - incident categories for, 371–374
 - in Prelude, 311–314
 - in real-time detection, 38
 - in Sguil, 329–330
 - Every Query results, 328
 - "Evolution of Intrusion Detection Systems" (Innella), 686
 - "Experiences Benchmarking Intrusion Detection Systems" (Ranum), 750–751
 - Explicit Congestion Notification (ECN) option, 562
 - Explicit signature techniques vs. anomaly detection, 762
 - Exploitation phase
 - in compromise, 16–17
 - in encryption, 624–628
 - intruder detection in, 19
 - Exploits, 8
 - Extended Service Set Identifiers (ESSIDs), 92
 - External intruders from wireless zones, 50
 - External segments, session data from, 488–490
- F**
- f switch, P0f, 208
 - F switch, Tethereal, 143
 - Failures, inevitability of, 13
 - False alarms, 730
 - Familiar netblocks, attacks from, 600
 - FCS (frame check sequence), 664
 - Feedback in assessment, 383–384
 - file command for raw trace files, 197
 - File Transfer Protocol (FTP)
 - in session data, 487
 - for tools retrieval, 629–630, 633
 - with Truncated Tcp Options alerts, 493–497
 - Files downloaded by intruders, 337–338

- Filtering bridges
 - building, 79–81
 - detecting, 77–79
 - for inline devices, 76
 - testing, 82–83
- Filters, 21
 - ARP, 77–79, 356–358
 - Berkeley Packet Filters, 97
 - with Fragroute, 540–547
 - paper on, 695
 - with Tcpdump, 135–140
 - in Ethereal, 166–167
 - in Tethereal, 143
- Find Packet command, 167
- Fingerprinting, 708–709
- Firewalls, 47
 - application-layer, 353
 - for inline devices, 76
 - Pf, 22
 - for scans, 638
- First field in NetFlow, 217
- Fl field in Flow-cat, 231
- flags field
 - in Bro logs, 295
 - in LFT, 554
- flipz, intrusions by, 616–617
- Flow-based monitoring papers
 - "Characteristics of Network Traffic Flow Anomalies", 714
 - "Combining Cisco NetFlow Exports with Relational Database Technology for Usage Statistics, Intrusion Detection, and Network Forensics", 713
 - "OSU Flow-tools Package and Cisco NetFlow Logs", 711–712
 - "Signal Analysis of Network Traffic Anomalies", 714–715
- Flow-capture program, 225–229
- Flow-cat utility, 229–232
- Flow-print utility, 229–232
- flow_sequence field in NetFlow, 216
- Flow-tools, 224–225
 - Flow-capture, 225–229
 - Flow-cat and Flow-print, 229–232
- flowctl command, 223
- Flowreplay utility, 182
- Flows, definition, 215
- Follow TCP Stream option, 493
- Forensics, 41
- Foundation papers, 686
 - "Computer Security Threat Monitoring and Surveillance", 686–687
 - "Network Security Model", 690–692
 - "Requirements and Model for IDES---A Real-Time Intrusion-Detection Expert System", 688
 - "TAMU Security Package: An Ongoing Response to Internet Intruders in an Academic Environment", 692–694
- Fprobe utility, 215, 220–221
- frag test, 534
- frag-new test, 534
- frag-old test, 534
- frag-timeout test, 534
- frag2 preprocessor, 545
- Fragmented packets, 22
 - with Fragroute, 540–547
 - in ICMP, 363–369
- Fragroute tool, 82–83, 534–547
- Fragrouter tool, 547
- Fragtest tool, 534–535
- Fraleigh, Chuck, "Design and Deployment of a Passive Monitoring Infrastructure", 697–698
- Frame check sequence (FCS), 664
- FreeBSD: An Open-Source Operating System for Your Personal Computer* (Anderson), 417
- FreeBSD monitoring
 - for channel binding, 66–68
 - for device polling, 98
 - for full content data, 120
 - for inline devices, 76
 - for sensors, 96–97
 - for session data, 474
 - for SPAN ports, 57–58
 - for taps, 64, 180
 - for TCP sequence numbers, 673–682
 - Tcpslice on, 175, 178
 - for wireless monitoring, 91
 - XMAS scan against, 635–636
- Freedom to maneuver in defensible networks, 21–22
- FreshPorts site, 221
- Fryxar, Tunnelshell by, 460

INDEX

- FTP (File Transfer Protocol)
 in session data, 487
 for tools retrieval, 629–630, 633
 with Truncated Tcp Options alerts, 493–497
 ftp.\$BROID file, 293
 FTP SITE overflow attempt alerts, 339–340
 Full content data, 119–121
 copying packets for, 652
 Etherape for, 162–171
 Libpcap for, 121–122
 options, 171–172
 vs. session, 212
 in Sguil, 324
 Snort for, 149–153
 Tcpdump for, 122–123, 125–132
 basic usage, 124
 with Berkeley Packet Filters, 135–140
 for detail, 134–135
 timestamps in, 132–134
 Tethereal for, 140
 basic usage, 140–141
 for detail, 146–149
 reading, 144–146
 storing, 141–144
 tools for
 Editcap and Mergecap, 173–174
 Etherape, 191–192
 IPsumdump, 189–190
 Netdude, 193–204
 Ngrep, 185–189
 POf, 205–209
 Tcpflow, 182–185
 Tcpreplay, 179–182
 Tcpslice for, 174–178
 Full disclosure, necessity of, 725
 Full-duplex links for taps, 75
 Fullmer, Mark
 Flow-tools by, 224
 "OSU Flow-tools Package and Cisco NetFlow
 Logs", 711–712
 Future of NSM, 651
 anomaly detection, 654–656
 integration of vulnerability assessment products,
 653–654
 paper on, 728
 remote packet capture and centralized analysis,
 652–653
 traffic leaving enterprises, 656–658
- Fyodor
 "Remote OS Detection via TCP/IP Stack
 Fingerprinting", 708–709
 tools poll by, 410
 Xprobe2 by, 558
- G**
 Garcia, Roberto, 753
 Gelber, Dan, on Rome Labs attack, 588
 Ghetta, Riccardo, Etherape by, 191
 GIAC (Global Incidents Analysis Center), 607
 Giant packets in statistics, 254
 GIGO principle, 40
 Global Incidents Analysis Center (GIAC), 607
 global load balancing systems, 457, 614
 Global Traffic Statistics screen, 281
 Gnucleus peer-to-peer client, 502–504
 Gnutella protocol, 499–504
 Goleniewski, Lillian, *Telecommunications Essentials*,
 415
 Government testing, 359
 Graf, Thomas, Bmon by, 258
 Granularity, 119
 Graphical packet utilities
 Etherape, 191–192
 Etherape, 162–171
 Netdude, 193–204
 Gray-World project, 352
 Green alerts in Prelude, 312
 "GrIDS: A Graph-Based Intrusion Detection System
 for Large Networks" (Staniford-Chen), 719
 Grindlay, Bill, *SQL Server Security*, 413
 Gspooof tool, 534
 GUI (graphical user interface), 164–165
 Gula, Ron
 on analyst attacks, 648
 on limiting access, 22
 on observed traffic, 355
 "Passive Vulnerability Detection", 743–745
 "Passive Vulnerability Scanning Introduction to
 NeVO", 752
- H**
 Hack back strategy, 589
 Hack backs for stepping-stone detection,
 586–588
*Hacker's Challenge: Test Your Incident Response
 Skills Using 20 Scenarios* (Schiffman), 414

- Hacker's Challenge 2: Test Your Network Security and Forensics Skills* (Schiffman), 414
- Hacking Exposed* series, 413
- Haines, Stephen, *Java 2 Primer Plus*, 420
- Half-duplex devices, 54
- Hall, Eric A., *Internet Core Protocols: The Definitive Reference*, 415
- Handley, Mark
- "Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics", 748–749
 - on scrubbing, 22
- Hanssen, Robert, 634
- Hard drives for sensors, 94
- Hardware, 94–96
- Hatch, Brian, *Hacking Exposed* series, 413
- Haugdahl, J. Scott, *Network Analysis and Troubleshooting*, 415
- Hawke Helicopter Supplies (HHS) case study, 385
- asset prioritization in, 396
 - emergency network security monitoring in, 386–393
 - evaluating managed security monitoring providers, 393–396
 - in-house NSM solutions in, 396–402
 - incident response in, 389–390
 - results in, 390–393
 - system administrators response in, 388–389
- Hayton, Todd, "Passive Vulnerability Scanning Introduction to NeVO", 752
- Heberlein, L. Todd
- home page for, 753
 - "Network Security Model", 690–692
 - Network Security Monitor by, 753
 - on Rome Labs attack, 586–587
 - "Tactical Operations and Strategic Intelligence: Sensor Purpose and Placement", 700–701
 - "Towards Detecting Intrusions in a Networked Environment", 716–717
- Hedgehog tool, 427–431
- Helicopter parts supplier. *See* Hawke Helicopter Supplies (HHS) case study
- Hess, David K., "TAMU Security Package: An Ongoing Response to Internet Intruders in an Academic Environment", 692–694
- History of NSM, 753–755
- Hitson, Bruce, "Knowledge-Based Monitoring and Control: An Approach to Understanding the Behavior of TCP/IP Network Protocols", 701–702
- Hoagland, James A., "Practical Automated Detection of Stealthy Portscans", 735
- Hobbs, Jeffrey, *Practical Programming in Tcl and Tk*, 420
- Hogan, Christine, *Practice of System and Network Administration*, 417
- Holistic intrusion detection, 39
- Home pages of researchers, 752–753
- Home users, 658
- Honeypots: Tracking Hackers* (Spitzner), 413
- host_#.ps graphs, 266
- Host-based audits, 400
- Host-based detection, 657
- host command for TCP traffic, 444–445
- Host names in Sguil, 321
- Host Traffic Stats screen, 283
- Hosts, Ntop for, 280
- hot_login function, 294
- Howard, Michael, *Writing Secure Code*, 420
- Hping program
- for filtering, 358
 - reference for, 411
- HTTP proxies, 352
- HTTPS sessions, 623, 626, 628
- HTTPTunnel tool, 352
- Hubs, 52–56
- advantages and disadvantages of, 84
 - and taps, 72
- Human targets, devious attacks against, 648
- I**
- i switch
 - Argus, 236
 - Ngrep, 186
 - Tcpdump, 124–125
 - I switch, Ngrep, 186
 - I&W (indications and warning), 25–28, 374
 - IATF (Information Assurance Technical Framework Forum), 359
 - ICMP protocol and packets, 362
 - for chained covert channels, 506–511, 514
 - in Flow-cat, 230
 - fragmented traffic in, 363–369
 - in Fragtest, 534

INDEX

- ICMP protocol and packets, *continued*
 header for, 670–671
 with LFT, 551, 554, 556
 with Nmap, 606
 normal traffic in, 361–363
 Tcpdump representation of, 127–128spoofing,
 593
 with Traceroute, 550
 in Xprobe2, 561, 563
 icmp.type filter, 166
 ICMPv4 header options in Packit, 522–523
 ICSA Labs, IDS testing criteria by, 359
 Identification phase in detection, 360–371
 Identifier field in ICMP Echo, 671
 Identities, intruder revelation of, 604–605
 "IDES: The Enhanced Prototype: A Real-Time
 Intrusion-Detection Expert System" (Lunt),
 715–716
 Idle hosts, 604
 Idle scans, 605
 IDMEF (Intrusion Detection Message Exchange
 Format), 298
 IDS Balancer device, 71
 IDSs
 for alerts, 285
 deployment failures in, 30–31, 39–40
 signature refinement in, 383
 testing criteria for, 359
 IEEE 802.3 headers, 665
 ifconfig command
 for filtering bridges, 80
 for NIC speed, 54
 for silent network interfaces, 51
 for virtual interface bonding, 67
 ifstat utility, 257–258
 Iftop utility, 263
 IGMP (Internet Group Management Protocol)
 statistics, 250
 IGRP (Interior Gateway Routing Protocol)
 statistics, 250
 IMAP (Internet Message Access Protocol), 618
 Impersonators, 634–635
 Implementation vulnerabilities, 8
 "Implementing a Generalized Tool for Network
 Monitoring" (Ranum), 721–722
 In-band remote access, 100–101
 In-house NSM solutions, 396–402
 Inbound traffic filtering, 21
Incident Response and Computer Forensics (Prorise,
 Mandia, and Pepe), 414
 Incident responses, 41
 in Argus, 236
 in case study, 389–390
 Incidents, 5
 attacks as, 361
 for events, 371–374
 Index page in MRTG, 276–277
 Indications, 25–28
 Indications and warning (I&W) concepts, 374
 Indicators, defined, 371–372
 Inferential statistics, 248
 "Inferring Internet Denial-of-Service Activity"
 (Moore, Voelker, and Savage), 749
 info.\$BROID file, 293
 Infoleak exploit, 466–468
 Information Assurance Technical Framework
 Forum (IATF), 359
Information Security Magazine, 426
 Information warriors, 7
 Ingress filters, 21, 594–595
 Initial response numbers (IRNs), 674
 Inline devices, 76–77
 advantages and disadvantages of, 84
 filtering bridges
 building, 79–81
 detecting, 77–79
 testing, 82–83
 Pf with bridging, 81–82
 InMon Agent, 233–234
 Innella, Paul, "Evolution of Intrusion Detection
 Systems", 686
 input field in NetFlow, 217
 Input queues, 567
 ins1der, RPC exploitation by, 575
 "Insertion, Evasion, and Denial of Service: Eluding
 Network Intrusion Detection" (Ptacek and
 Newsham), 723–726
 Insiders
 on intranets, 50
 vs. outsiders, 31–34
 Installing
 Bro and BRA, 287–292
 PIWI, 299, 309–311
 Prelude, 299–307

- Integration of vulnerability assessment products, 653–654
- Integrity of databases, 6
- Intel hardware for sensors, 94
- Intellectual history of NSM, 685–686
- alert-centric intrusion detection papers, 715–739
 - complimentary technologies papers, 739–752
 - flow-based monitoring papers, 711–715
 - foundation papers, 686–694
 - packet analysis papers, 701–711
 - researcher home pages, 752–753
 - sensor architecture papers, 694–701
- Intelligence of intruders, 12
- Intercept, Inc, odd traffic from, 614
- Interface statistics tools
- Bmon, 258–260
 - Ifstat, 257–258
 - Ipcad, 255–257
 - Trafshow, 260–264
- Interior Gateway Routing Protocol (IGRP) statistics, 250
- Internal networks in in-house NSM solutions, 399
- International computer crime laws, 585–586
- Internet Control Message Protocol. *See* ICMP protocol and packets
- Internet Core Protocols: The Definitive Reference* (Hall), 415
- Internet Group Management Protocol (IGMP) statistics, 250
- Internet Mapping Project, 611
- Internet Message Access Protocol (IMAP), 618
- Internet Protocol, header for, 668–670
- Internet Protocol Journal*, 427
- Internet Relay Chat (IRC) channels, 18, 602
- Internet Router Discovery Protocol (IRDP) statistics, 250
- Internet Security Threat Report, 600
- "Interpreting Network Traffic: An Intrusion Detector's Look at Suspicious Events" (Bejtlich), 709–710
- Interrupt request (IRQ) conflicts, 94–95
- Intranets, monitoring, 50–51
- Intruder-led incident responses, 383
- Intruders
- characteristics, 12–13
 - detecting. *See* Detection
 - identity revelation by, 604–605
- Intrusion Detection* (Bace), 686
- Intrusion Detection Message Exchange Format (IDMEF), 298
- "Intrusion-Detection Model" (Denning), 689
- "Intrusion Detection Systems: A Survey and Taxonomy" (Axelsson), 686
- Intrusion prevention systems (IPSs)
- vs. NSM, 41
 - purpose of, 349–350
- Intrusions, 5
- Inventory of defensible networks, 21
- ip accounting command, 249
- IP addresses
- in anonymity. *See* Anonymity with decoys, 640–641
 - Ntop, 280–281
 - in session data, 475–476
 - statistics for, 250
- ip_chaff dup option in Fragtest, 536
- IP Flow Information Export (IPFIX) system, 213
- ip_frag size option in Fragtest, 536
- IP header options in Packit, 523
- ip_opt lrr option in Fragtest, 536
- ip-opt test in Fragtest, 534–536
- ip-opt values, 535
- IP Sorcery tool, 530–534
- ip.src filter, 166
- ip switch, Argus, 236
- ip_tos tos option in Fragtest, 536
- ip_ttl ttl option in Fragtest, 536
- IP Version field in Packit packets, 532
- Ipcad tool, 255–257
- IPFilter firewalls, 76
- IPFIX (IP Flow Information Export) system, 213
- IPFW for inline devices, 76
- ipmagic file, 530
- IPMON system, paper on, 698
- IPSs (intrusion prevention systems)
- vs. NSM, 41
 - purpose of, 349–350
- IPsumdump utility, 189–190
- IRC (Internet Relay Chat) channels, 18, 602
- IRDP (Internet Router Discovery Protocol) statistics, 250
- IRNs (initial response numbers), 674
- IRQ (interrupt request) conflicts, 94–95
- iwpriv command, 87–88

INDEX

J

- Jacobson, Van
 - "BSD Packet Filter: A New Architecture for User-Level Packet Capture", 695
 - Libpcap by, 121
- Java 2 Primer Plus* (Haines and Potts), 420
- Johnson, Bradley C., *Anti-Hacker Tool Kit*, 413
- Jones, Keith J., *Anti-Hacker Tool Kit*, 413
- Jones, Ken, *Practical Programming in Tcl and Tk*, 420

K

- Kabay, Mitch, 4
- Kahn, Clifford, "Common Intrusion Detection Framework", 727
- Kay, Andrew, dscan by, 607
- keepstats option in Snort, 320, 328
- Kemmerer, Richard A.
 - "NetSTAT: A Network-Based Intrusion Detection Approach", 728–729
 - "Stateful Intrusion Detection for High-Speed Networks", 699–700
- keys.* files, 294
- Keystroke logs in Bro, 294
- Kismet tool
 - reference for, 411
 - vs. Snort-Wireless, 657
 - for wireless monitoring, 93
- Kline, Jeffrey, "Signal Analysis of Network Traffic Anomalies", 714–715
- Kluge, Martin, Cisco IOS DOS attacks by, 567
- Knittel, Brian, *Windows XP Under the Hood: Hardcore Windows Scripting and Command Line Power*, 420
- Knoppix distribution, 86–87, 91
- "Know Your Enemy: The Tools and Methodologies of the Script Kiddie" (Spitzner), 746–747
- "Knowledge-Based Monitoring and Control: An Approach to Understanding the Behavior of TCP/IP Network Protocols" (Hitson), 701–702
- Kochan, Stephen, *UNIX Shell Programming*, 420
- Kohler, Eddie, IPsumdump by, 189
- Kreibich, Christian
 - Netdude by, 193
 - "Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics", 748–749

- Kruegel, Christopher
 - home page for, 753
 - "Stateful Intrusion Detection for High-Speed Networks", 699–700
- Kuji, attack by, 586
- Kumar, Sandeep, "Application of Pattern Matching in Intrusion Detection", 718–719
- Kurtz, George, *Hacking Exposed* series, 413

L

- l switch
 - Snort, 152
 - Tcpdump, 126
 - Tcptrace, 244
- L switch, Tcpdump, 92
- L0 switch, Ra, 238
- Langille, Dan, 221
- Large-scale attacks, 719
- "Last analyst standing" security labs, 424–426
- Last field in NetFlow, 217
- Last Stage of Delirium (LSD) exploit, 466, 469–471
- Laws
 - international, 585–586
 - intrusion detection, 35
- Layer Four Traceroute (LFT) tool, 548–558
- LBM (load balancing manager), 457–458
- LBSs (load balancing systems), 458
- Learning Python* (Lutz and Ascher), 420
- LeBlanc, David C., *Writing Secure Code*, 420
- Lee, James, *Hacking Exposed* series, 413
- Lee, Wenke
 - "Data Mining Approaches for Intrusion Detection", 727–728
 - home page for, 753
- Lehey, Greg, *Complete Guide to FreeBSD*, 417
- Leres, Craig, Libpcap by, 121
- LFAP (Lightweight Flow Accounting Protocol), 214
- LFT (Layer Four Traceroute) tool, 548–558
- Libnetdude component, 193
- Libpcap tool
 - for full content data, 121–122
 - and Packit, 524–525
 - Tcpdstat for, 266–271
- Libpcapnav component, 193
- Libprelude utility, 299, 314
- Licenses for CISCO IOS, 416–417
- Lightweight Flow Accounting Protocol (LFAP), 214

- Limitations, 37–40
 Limoncelli, Thomas A., *Practice of System and Network Administration*, 417
 Lin, John C., "Probing TCP Implementations", 705–706
 Linux for wireless monitoring, 86–87, 91
 Lippmann, Richard, "1999 DARPA Off-Line Intrusion Detection Evaluation", 745–746
 Litchfield, David, *SQL Server Security*, 413
 Little-endian conventions, 201–202
 Live session data, Trafshow for, 260
 "Live Traffic Analysis of TCP/IP Gateways" (Porras and Valdes), 706–707
 Load balancing, global, 457, 614
 Load balancing manager (LBM), 457–458
 Load balancing systems (LBSs), 458
 LoadConfig function, 311
 local-addr field in Bro logs, 295
 local_IP element in Flow-capture, 225
 Lockhart, Andrew, Snort-Wireless project by, 657
 Log Monitoring Lackey, 299
 login_input_lines function, 294
 Logs
 in Bro, 293–295
 Tcpcdump, 126
 wiping, 647
 Long-term network usage statistics, 271–278
 LSD (Last Stage of Delirium) exploit, 466, 469–471
 lsof command, 289
 Lucas, Michael
 Absolute BSD: The Ultimate Guide to FreeBSD, 417
 Absolute OpenBSD: UNIX for the Practical Paranoid, 418
 Lunt, Teresa F., "IDES: The Enhanced Prototype: A Real-Time Intrusion-Detection Expert System", 715–716
 Lutz, Mark, *Learning Python*, 420
 Lyon, Barrett, for Opte Project, 612–613
- M**
- MAC (media access control) address for SPAN ports, 61
 Machine language, 418–419
 magic file, 530
 Magic numbers field, 201, 203–204
 make command for Bro, 291
 MAKEDEV script, 97
 Makefile file, 291
 Malicious traffic, 361
 port 53
 TCP, 466–471
 UDP, 459–466
Malware: Fighting Malicious Code (Skoudis and Zeltser), 413
 Managed security monitoring providers, evaluating, 393–396
 Managed security service providers (MSSPs), 40
 Management, analyst training program for, 421
 manager-adduser command, 304–305
 Manders, Chris, BRA by, 285
 Mandia, Kevin
 Incident Response and Computer Forensics, 414
 on incidents, 5
 Maneuverability in defensible networks, 21–22
 ManHunt IDS, 36
 Mask Request options in Packit, 523
 Masqueraders, 634–635
 Matthew, Neil, *Beginning Databases with PostgreSQL*, 418
 McAlerney, Joseph M.
 "Practical Automated Detection of Stealthy Portscans", 735
 "Towards Faster String Matching for Intrusion Detection or Exceeding the Speed of Snort", 734–735
 McCanne, Steven
 "BSD Packet Filter: A New Architecture for User-Level Packet Capture", 695
 Libpcap by, 121
 McCarthy, Nils, LFT for, 548
 McClure, Stuart, *Hacking Exposed* series, 413
 McGraw, Gary, *Building Secure Software: How to Avoid Security Problems the Right Way*, 420
 McIlroy, Doug, on UNIX philosophy, 317
 MDAC (Microsoft Data Access Components), vulnerability in, 616
 "Measurement and Analysis of IP Network Usage and Behavior" (Caceres), 697
 "Measurements of Wide Area Internet Traffic" (Caceres), 702–703
 Media access control (MAC) address for SPAN ports, 61
 Mel, H. X., *Cryptography Decrypted*, 414

INDEX

- Memory, storage conventions for, 198, 201
 Men & Mice, Inc, testing products from, 614
 Mergecap utility, 173–174
 for separate traffic collection, 68–70
 for taps, 65
 "Methodology for Testing Intrusion Detection Systems" (Puketza), 743
 Microsoft, RPC exploitation against, 575–581
 Microsoft Data Access Components (MDAC), vulnerability in, 616
 Microsoft Terminal Services, Tsgrinder on, 113–114
 Middleboxes, 353
 Minutes in Tcpslice timestamps, 177
 MISC MS Terminal Server Request alerts, 342–343
 Misconfigurations, 350
 Mitnick, Kevin D.
 Art of Deception: Controlling the Human Element of Security, 414
 spoofing attack by, 590–591
 Mitnick Attack, 590–591
 mod_ssl worm, 16
 Monitoring
 defensible networks, 20–21
 wireless networks, 85–93
 zones
 DMZ, 49–50
 intranets, 50–51
 perimeters, 48–49
 and threat models, 45–51
 wireless, 50
 Monitoring, Intrusion, Detection, and Administration System, 318
 Monitors, 348
 Months in Tcpslice timestamps, 177
 Moore, David, "Inferring Internet Denial-of-Service Activity", 749
 Moore, H. D., sadmin exploitation attempt by, 570
 Morris, Robert T., 591
 Motivation for IDS, 688
 MRTG (Multi Router Traffic Grapher) utility, 271–278
 MSSPs (managed security service providers), 40
 Mstream clients in reference intrusion model, 114–116
 Multi Router Traffic Grapher (MRTG) utility, 271–278
 Multiple destination ports with Packit, 529
 Multipurpose traffic analysis tools, 242–246
 Myrick, Paul, 212
 MySQL utility, 320
- N**
 N-code Filtering, 722
 -n switch
 Ngrep, 187
 Ntop, 279
 Ra, 238
 Snort, 150
 Tcpcdump, 124–125
 Traceroute, 548
 Trafshow, 261
 -N switch, P0f, 208
 Nachi worm, 508, 589
 NAT (network address translation), 21
 National Information Assurance Partnership (NIAP), 359
 National Society of Professional Engineers (NSPE) Code of Ethics, 406
 Navarro, John-Paul, "Combining Cisco NetFlow Exports with Relational Database Technology for Usage Statistics, Intrusion Detection, and Network Forensics", 713
 NBAR (Network-Based Application Recognition) features, 353–354
 Nbtscan tool, 411
 Nemesis tool, 411
 Nemeth, Evi, *UNIX System Administration Handbook*, 418
 Neohapsis IDS, 359
 Nessus tool, 411
 NetBIOS announcements, 58
 Netblocks, attacks from, 597–600
 NetBSD tool, 96
 Netcat tool
 for OpenSSH version, 622–623
 reference for, 411
 NetDetector tool, 212
 Netdude utility, 193
 for raw trace files, 196–204
 working with, 193–196
 NetFlow utility, 214–220
 Flow-tools, 224–232
 Fprobe, 220–221
 ng_netflow, 222–224
 for sessions, 213
 NetIntercept tool, 212

- Netsed utility, 204
- "NetSTAT: A Network-Based Intrusion Detection Approach" (Vigna and Kemmerer), 728–729
- netstat command for Sguil, 335
- Network address translation (NAT), 21
- Network Analysis and Troubleshooting* (Haugdahl), 415
- Network auditing and traffic analysis, 716–717
- access control rules for, 350
 - NetFlow for, 215
 - Ntop for, 278–283
 - path enumeration, 548–558
- Network-Based Application Recognition (NBAR)
- features, 353–354
- Network byte order, 204
- Network Computing* magazine, 426
- Network Flight Recorder, 721–722
- Network IDSs
- Bro utility, 285–287
 - BRA installation, 287–292
 - capabilities and limitations, 297
 - output files, 292–297
 - Prelude utility, 298
 - capabilities and limitations, 313–315
 - events in, 311–314
 - installing, 299–307
 - output files, 307–309
 - PIWI installation, 309–311
- Network infrastructure, 657
- "Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics" (Handley, Paxson, and Kreibich), 748–749
- Network Load link, 279
- Network Load Statistics screen, 279–280
- Network Magazine*, 426
- Network Monitoring and Analysis site, 231
- Network profiling in anomaly detection, 655–656
- "Network Security Model" (Heberlein), 690–692
- Network Security Monitor development, 753
- Network Sorcery site, 663
- Network Traffic screen, 282
- Neumann, Peter G.
- "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances", 719–720
 - "Requirements and Model for IDES—A Real-Time Intrusion-Detection Expert System", 43, 688
 - on security limitations, 43
- NeVO passive scanner
- modes in, 653–654
 - paper on, 752
- Newsgroups for attacks, 602
- Newsham, Timothy N., "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection", 723–726
- nextHop field in NetFlow, 217
- nFlow tool, 214
- ng_netflow utility, 222–225
- ngctl command, 67
- Ngrep utility
- with Fragroute, 541–542
 - for string matching, 185–189
- NIAP (National Information Assurance Partnership), 359
- Nickless, Bill, "Combining Cisco NetFlow Exports with Relational Database Technology for Usage Statistics, Intrusion Detection, and Network Forensics", 713
- NICs, speed of, 54
- Nikto tool, 411
- Nimda worms, 602
- "1999 DARPA Off-Line Intrusion Detection Evaluation" (Lippmann), 745–746
- Nmap tool
- for decoy scans, 639–641
 - for idle scans, 605
 - for operating system identification, 565–566
 - probe timing with, 604
 - reference for, 411
 - with spoofed addresses, 596
 - XMAS scan traffic, 637
- "NNStat: Internet Statistics Collection Package" (Braden and DeSchon), 741–742
- no keepalive option, Trafshow, 262
- Normal traffic, 361
- in ICMP, 361–363
 - port 53
 - TCP, 442–448
 - UDP, 434–442
- Normalization, 22
- nslookup command
- for TCP traffic, 444
 - for UDP traffic, 441
- NSPE (National Society of Professional Engineers) Code of Ethics, 406
- NSS Group IDS reviews, 359

INDEX

- Ntop utility, 224, 278–283
 Number of services in defensible networks, 23
 Nyberg, Claes M., Sadoor tool by, 510
 Nylon proxy, 351
- O**
- O switch, Ngrep, 188
 - o switch, P0f, 208
 - Observed traffic with sensors, 355
 - OC-3 standard, 56
 - OC-12 standard, 56
 - OC-48 standard, 56
 - OC-192 standard, 56
 - "OC3MON: Flexible, Affordable, High Performance Statistics Collection" (Apsidorf, Claffy, Thompson, and Wilder), 695–696
 - Odd orders, detection of, 386–393
 - Odd packets, paper on, 710–711
 - Oetiker, Tobias, MRTG by, 271
 - Offensive tools, 410–411
 - one2many system, 68
 - Open Security Evaluation Criteria (OSEC), 359
 - Open Shortest Path First (OSPF) protocol, 250
 - Open Source Security Information Management project, 318
 - OpenBSD
 - for filtering bridges, 79
 - for inline devices, 76
 - Pf firewall, 22
 - for sensors, 96
 - OpenSSH
 - versions of, 622–623, 625
 - vulnerability in, 11
 - Operating fishbowls, 77
 - Operating system identification
 - fingerprinting, 708–709
 - paper on, 706
 - sensor architecture, 96–98passive, 205–209
 - Xprobe2, 558–566
 - Oppenheimer, Priscilla, *Troubleshooting Campus Networks: Practical Analysis of Cisco and LAN Protocols*, 415
 - Opte Project, 612–613
 - order random option in Fragtest, 536
 - orig-bytes field in Bro logs, 295
 - Origination of attacks
 - by country, 600–601
 - internal vs. external, 32–34
 - OSEC (Open Security Evaluation Criteria), 359
 - OSPF (Open Shortest Path First) protocol, 250
 - Ostermann, Shawn
 - "Detecting Network Intrusions via a Statistical Analysis of Network Packet Characteristics", 710–711
 - home page for, 753
 - Tcptrace by, 242
 - "OSU Flow-tools Package and Cisco NetFlow Logs" (Fullmer and Romig), 711–712
 - OTH field in Bro states, 296
 - Out-of-band remote access, 101–102
 - Outbound filtering, 21
 - output field in NetFlow, 217
 - Outsiders vs. insiders, 31–34
- P**
- p switch
 - IPsundump, 189
 - P0f, 208
 - rpcinfo, 571
 - Tcpdump, 124
 - Xprobe2, 559
 - P switch, Traceroute, 548
 - p.ng switch, Ngrep, 186
 - P0 switch, Nmap, 596
 - P0f utility, 205–208, 320
 - Packet analysis papers, 701
 - "Detecting Network Intrusions via a Statistical Analysis of Network Packet Characteristics", 710–711
 - "Interpreting Network Traffic: An Intrusion Detector's Look at Suspicious Events", 709–710
 - "Knowledge-Based Monitoring and Control: An Approach to Understanding the Behavior of TCP/IP Network Protocols", 701–702
 - "Live Traffic Analysis of TCP/IP Gateways", 706–707
 - "Measurements of Wide Area Internet Traffic", 702–703
 - "Packets Found on an Internet", 704–705
 - "Probing TCP Implementations", 705–706
 - "Remote OS Detection via TCP/IP Stack Fingerprinting", 708–709
 - "TCP Packet Trace Analysis, 703–704
 - "There Be Dragons", 705

- Packet capture and analysis utilities
 - costs of, 707
 - Editcap and Mergecap, 173–174
 - Ethereal, 162–171
 - Libpcap, 121–122
 - Packit, 521–530
 - Snort, 149–153
 - Tcpdump, 122–123, 125–132
 - basic usage, 124
 - with Berkeley Packet Filters, 135–140
 - for detail, 134–135
 - timestamps in, 132–134
 - Tcpslice, 174–178
 - Tethereal, 140
 - basic usage, 140–141
 - for detail, 146–149
 - reading, 144–146
 - storing, 141–144
- Packet floods, 528
- Packet monkey analyses, 491
 - chained covert channels, 505–517
 - SCAN FIN alerts, 498–505
 - Truncated Tcp Options alerts, 492–498
- Packet Storm Security site, 427
- Packets
 - creating, 525–526
 - fragmentation, 22
 - with Fragroute, 540–547
 - in ICMP, 363–369
 - IP Sorcery for, 530–534
 - replay utility for, 179–182
 - scrubbers
 - with bridging, 82–83
 - for fragmentation, 545–546
 - vs. segments and datagrams, 125
- "Packets Found on an Internet" (Bellovin), 704–705
- Packit tool, 521–530
- pad 1 field in NetFlow, 217
- PAD/APM (protocol anomaly detection by application protocol modeling), 757
- pad2 field in NetFlow, 217
- Partners in in-house NSM solutions, 398
- Passive monitoring systems, 698
- Passive operating system identification systems, 205–209
- Passive taps, 75
- "Passive Vulnerability Detection" (Gula), 743–745
- "Passive Vulnerability Scanning Introduction to NeVO" (Deraison, Gula, and Hayton), 752
- Password-cracking
 - brute-force techniques, 113
 - distributed, 615
- Passwords
 - in in-house NSM solutions, 400
 - in Prelude, 304
- Patches in defensible networks, 23–24
- Pattern-based detection
 - in anomaly detection, 654–655
 - paper on, 734–735
- Patton, Samuel, "Achilles' Heel in Signature-Based IDS: Squealing False Positives in Snort", 733–734
- Paxson, Vern
 - "Active Mapping: Registering NIDS Evasion Without Altering Traffic", 735–736
 - "Bro: A System for Detecting Network Intruders in Real-Time", 722–723
 - Bro by, 285
 - "Enhancing Byte-Level Network Intrusion Detection Signatures with Context", 736–739
 - home page for, 753
 - intruder caught by, 170
 - "Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics", 748–749
 - on scrubbing, 22
 - Tcpslice by, 174
- Pepe, Matt, *Incident Response and Computer Forensics*, 414
- Perceived risk, 10
- Perception, 10
- Perimeters, monitoring, 48–49
- Periodicals for training programs, 426–427
- Perl by Example* (Quigley), 420
- Perl scripts in Argus, 242
- Pf program, 22
 - with bridging, 81–82
 - for fragmentation, 545–546
 - for inline devices, 76
- PFCs (Policy Feature Cards), 63
- Pfflowd probe, 224
- phric, IP Sorcery by, 530
- PHS (Protocol Hierarchy Statistics)
 - in Ethereal, 169–170
 - in Tethereal, 148

INDEX

- Pillage phase
 in compromise, 18–19
 in encryption, 632–634
 intruder detection in, 19
- PIM (Protocol Independent Multicasting) protocol
 statistics, 250
- ping command
 for Fragtest, 534
 for ICMP, 361–363
 for separate traffic collection, 69
 for Xprobe2, 561
- PIWI (Prelude IDS Web Interface), 298
 installing, 299, 309–311
 for Prelude events, 311–314
- Plonka, David
 "Characteristics of Network Traffic Flow
 Anomalies", 714
 "Signal Analysis of Network Traffic Anomalies",
 714–715
- Policies, security, 348–349
- Policy, training programs for, 421
- Policy Feature Cards (PFCs), 63
- Policy scripts in Bro, 297
- Polish Ministry of Defense case study, 9–12
- Polling
 devices, 98
 by MRTG, 272
- Polymorphism in anomaly detection, 762
- Poor design, vulnerabilities from, 8
- Poor Security Practice or Policy Violation incident
 category, 373
- POP (Post Office Protocol), 618–621
- Porras, Phillip A.
 "Common Intrusion Detection Framework", 727
 "EMERALD: Event Monitoring Enabling
 Responses to Anomalous Live
 Disturbances", 719–720
 home page for, 753
 "Live Traffic Analysis of TCP/IP Gateways",
 706–707
- Port 53 traffic
 malicious
 TCP, 466–471
 UDP, 459–466
 normal
 TCP, 442–448
 UDP, 434–442
 suspicious
 TCP, 455–459
 UDP, 448–455
- Port Aggregator tap, 72–74
- Port-based filters, 138
- Ports
 for Ethernet taps, 63–64
 mirroring, 56
 SPAN, 56–63, 84
 usage statistics, 281–282
- Post Office Protocol (POP), 618–621
- PostgreSQL database, 299–301
- Potts, Stephen, *Java 2 Primer Plus*, 420
- PPs (Protection Profiles), 359
- Pr field in Flow-cat, 231
- "Practical Automated Detection of Stealthy
 Portscans" (Staniford, Hoagland, and
 McAlerney), 735
- Practical Programming in Tcl and Tk* (Welch, Jones,
 and Hobbs), 420
- Practice of System and Network Administration*
 (Limoncelli and Hogan), 417
- Prata, Stephen
 C Primer Plus, 420
 C++ Primer Plus, 420
- Preambles in Ethernet frames, 664
- Predictability of intruders, 12
- Prelude IDS Web Interface (PIWI), 298
 installing, 299, 309–311
 for Prelude events, 311–314
- prelude.log file, 307
- Prelude-manager data processor, 299, 304–306
- prelude-manager-db-create.sh script, 301
- Prelude-NIDS IDS, 299, 305
- Prelude utility, 298
 capabilities and limitations, 313–315
 events in, 311–314
 installing, 299–307
 output files, 307–309
 PIWI installation, 309–311
- Prevention, 5, 13
- print option in Fragtest, 536
- Priority
 asset, 396
 Prelude alerts, 312
 in Snort, 321
- Privacy, paper on, 694, 712

- Privilege escalation, 632
 - Privmsg script, 170
 - Probes
 - incident category, 373–374
 - for sessions data, 214
 - timing, 604
 - "Probing TCP Implementations" (Comer and Lin), 705–706
 - Processes for escalation, 28–29
 - Products, 28
 - Profiler tool, 212
 - Profiles
 - Ntop for, 281
 - protection, 359
 - Programming, training program for, 418–420
 - Prorise, Chris
 - incident definition by, 5
 - Incident Response and Computer Forensics, 414
 - prot field in NetFlow, 217
 - Protection
 - in best practices, 349–350
 - in security process, 5
 - Protection Profiles (PPs), 359
 - proto_#.ps graphs, 266
 - proto syntax in Tcpdump, 138
 - Protocol analysis, 761
 - Protocol anomaly detection, 757
 - approaches to, 759–760
 - vs. explicit signature techniques, 762
 - general approach, 758–759
 - implementation, 760–761
 - introduction, 757–758
 - warnings, 761
 - Protocol anomaly detection by application protocol modeling (PAD/APM), 757
 - Protocol decode, 761
 - protocol field in Bro logs, 295
 - Protocol header references, 663
 - Address Resolution Protocol, 666–668
 - Ethernet frames, 664–665
 - IEEE 802.3, 665
 - Internet Control Message Protocol Echo, 670–671
 - Internet Protocol, 668–670
 - sub-network access protocol, 666
 - TCP sequence numbers, 673–682
 - Transmission Control Protocol, 672–673
 - User Datagram Protocol, 682–683
 - Protocol Hierarchy Statistics (PHS)
 - in Ethereal, 169–170
 - in Tethereal, 148
 - Protocol Independent Multicasting (PIM) protocol statistics, 250
 - Protocols in security policies, 349
 - Protocols (TCP/IP Illustrated, Volume 1)* (Stevens), 415
 - Proventia products, 653
 - Proxies, 351–354
 - Pryce, Richard, attack by, 586, 589
 - PsExec tool, 27
 - Ptacek, Thomas H., "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection", 723–726
 - Public intermediaries for anonymity, 602–603
 - Puketza, Nicholas J., "Methodology for Testing Intrusion Detection Systems", 743
- Q**
- q switch
 - Ngrep, 186
 - Traceroute, 548
 - Queries in Sguil, 327–330
 - Query Builder, 327, 343
 - Query Event Table option, 326
 - Query Sessions Table option, 326
 - Queues
 - in Cisco IOS devices, 567
 - in denial-of-service attack, 591
 - Quigley, Ellie, *Perl by Example*, 420
- R**
- r switch
 - date, 132–133
 - Ipcad, 255
 - Snort, 153
 - Tcpdump, 127
 - Tcpslice, 175–177
 - R switch
 - P0f, 205
 - Tcpslice, 175
 - Ra client, 238–242
 - Racount tool, 241
 - RADIOTAP extensions, 93

INDEX

- RAID (Recent Advances in Intrusion Detection)
 conference, 425
- RAM for sensors, 94
- Rand, Dave, MRTG by, 271
- Ranum, Marcus J.
 on anomaly detection, 655
 "Experiences Benchmarking Intrusion Detection Systems", 750–751
 "Implementing a Generalized Tool for Network Monitoring", 721–722
 on observed traffic, 355
 on uninteresting things, 35
- Rattray, Gregory J., *Strategic Warfare in Cyberspace*, 421
- Raw packets, access to, 652
- Raw trace files, 196–204
- RDS (Remote Data Services) vulnerability, 616
- Reading full content data
 Ethereal for, 164–167
 Snort for, 153
 Tethereal for, 144–146
- Real 802.11 Security: Wi-Fi Protected Access and 802.11i* (Edney and Arbaugh), 415
- Real-time capability, paper on, 691
- Real-time flow monitors (RTFMs), 234
- Real-time intrusion detection, 38–39
- Real-time intrusion detection export systems, 715–716
- Real-time Network Awareness (RNA) product, 653
- "Real-Time Network-Based Anomaly Intrusion Detection" (Balupari), 733
- RealTime Events tab, 321
- Rebuilding sessions, 167, 169, 338
- Recent Advances in Intrusion Detection (RAID) conference, 425
- Reconnaissance alerts
 response to, 638
 in Sguil, 321
- Reconnaissance phase
 in compromise, 15–16
 in encryption, 621–624
 intruder detection in, 19
- Reconnaissance/Probes/Scans incident category, 373–374
- Red alerts in Prelude, 312
- red.\$BROID file, 293
- Reference intrusion model, 105
 attacks in, 106–118
 scenario for, 105–106
 vs. Sguil, 331–343
- Reference sources
 for management and policy, 421
 for scripting and programming, 419–420
 for system administration, 416–418
 for telecommunications, 415
 for weapons and tactics, 412
- Regular expressions, 738
- Reinforcement phase
 in compromise, 17
 in encryption, 628–631
 intruder detection in, 19
- REJ field in Bro states, 296
- Remote access to sensors
 in-band, 100–101
 out-of-band, 101–102
- Remote Data Services (RDS) vulnerability, 616
- remote_IP element in Flow-capture, 225
- Remote Monitoring (RMON) Management Information Base (MIB), 171–172
- "Remote OS Detection via TCP/IP Stack Fingerprinting" (Fyodor), 708–709
- "Remote Packet Capture" (Bullard), 652
- Remote packet capture in future, 652–653
- Remote Procedure Call (RPC) services
 exploitation against Microsoft, 575–581
 vulnerabilities, 11
- Remote SPAN (RSPAN) technology, 62
- Replay packets, 179–182
- Replication in Prelude, 313
- "Requirements and Model for IDES---A Real-Time Intrusion-Detection Expert System" (Denning and Neumann), 43, 688
- Rescorla, Eric, "Security Holes: Who Cares?", 751–752
- Researcher home pages, 752–753
- resp-bytes field in Bro logs, 295
- Response process, 6, 29, 42–43
 in best practices, 380–383
 emergency network security monitoring, 381–382
 short-term incident containment, 381
- Results in case study, 390–393
- Reverse hacking, 587–588

- Risk, 6
 asset value in, 9
 in Polish Ministry of Defense case study, 9–12
 threats in, 6–8
 vulnerability in, 8
- Risk equation, 6
- Ritter, Jordan, Ngrep by, 185
- RMON (Remote Monitoring) Management Information Base (MIB), 171–172
- RNA (Real-time Network Awareness) product, 653
- Robertson, William, alert verification project by, 654
- Roesch, Martin
 on contextual information, 653
 "Snort---Lightweight Intrusion Detection for Networks", 731–733
 Snort by, 149
- Roles and responsibilities in training program, 422
- Rome Labs attack, 586–589
- Romig, Steve
 home page for, 753
 "OSU Flow-tools Package and Cisco NetFlow Logs", 711–712
- Ron, Amos, "Signal Analysis of Network Traffic Anomalies", 714–715
- Root access, 16
- Root accounts in trusted operating systems, 372
- Root passwords in in-house NSM solutions, 400
- rootdown.pl script, 570–574
- Roualland, Gael, Ifstat by, 257
- Round Robin Database Tool (RRDTool), 277
- RPC over HTTP, 576
- RPC (Remote Procedure Call) services
 exploitation against Microsoft, 575–581
 vulnerabilities, 11
- rpcinfo -p command, 571
- RRDTool (Round Robin Database Tool), 277
- RSPAN (Remote SPAN) technology, 62
- RST0 field in Bro states, 296
- RST+ACK test, 205, 207
- RSTOS0 field in Bro states, 296
- RSTR field in Bro states, 296
- RSTRH field in Bro states, 296
- RT status in Sguil, 322
- RTFMs (real-time flow monitors), 234
- Rule-based detection, 691
- ruleset directory, 309
- Runts in statistics, 254
- Russell, Ryan, *Stealing the Network: How to Own the Box*, 414
- S**
- s switch
 Ifstat, 258
 Ipcad, 255
 IPsumdump, 190
 Pof, 208
 ping, 362
 Tcpdump, 124
- S switch
 Ifstat, 257
 IPsumdump, 190
 Tcpdump, 127, 131–132
 Tethereal, 144
- S0 field in Bro states, 296
- S1 field in Bro states, 296
- S2 field in Bro states, 296
- S3 field in Bro states, 296
- sadmin exploitation, 570–575
- Sadoor tool, 510–512
- Safford, David R., "TAMU Security Package: An Ongoing Response to Internet Intruders in an Academic Environment", 692–694
- Sales offices in in-house NSM solutions, 398
- Sampling, detection through, 35–36
- sampling_interval field in NetFlow, 216
- SANCP project, 320
- SANS, GIAC established by, 607
- SANS Track 4 conference, 425
- Savage, Stefan, "Inferring Internet Denial-of-Service Activity", 749
- Save As feature in Netdude, 195
- SC Magazine, 426
- Scambray, Joel, *Hacking Exposed* series, 413
- SCAN FIN alerts, 498–505
- SCAN nmap TCP alerts, 340–342
- Scans incident category, 373–374
- Schales, Douglas Lee, "TAMU Security Package: An Ongoing Response to Internet Intruders in an Academic Environment", 692–694

INDEX

- Schiffman, Mike
 Hacker's Challenge: Test Your Incident Response Skills Using 20 Scenarios, 414
 Hacker's Challenge 2: Test Your Network Security and Forensics Skills, 414
- Schjolberg, Stein, law survey by, 585
- Schneier, Bruce, *Secrets and Lies: Digital Security in a Networked World*, 421
- Schultz, Eugene, on attack origins, 32–33
- Scoping process, 29
- SCP (Secure Copy), 17
- Script kiddies
 knowledge of, 12
 paper on, 746–747
- Scripting, training program for, 418–420
- Scrubbing traffic, 22, 351
- Secrets and Lies: Digital Security in a Networked World* (Schneier), 421
- Secure Copy (SCP), 17
- Secure Sockets Layer (SSL)
 in HTTPS session, 623
 support for, 618
 for Unicode attacks, 627–628
- Security
 conferences on, 425
 policies for, 348–349
 principles of
 compromise phases, 14–20
 defensible networks, 20–24
 detection, 34–37
 intruder characteristics, 12–13
 limitations, 37–40
 process, 4–6
Security Engineering: A Guide to Building Dependable Distributed Systems (Anderson), 420
 "Security Holes: Who Cares?" (Rescorla), 751–752
- Segments
 vs. packets and datagrams, 125
 session data from, 488–490
- Self-inflicted problems, 647–649
- sensor-adduser command, 305
- Sensors, 46
 architecture of, 93–94
 hardware, 94–96
 operating systems, 96–98
 attacks on, 643–647
 configuring, 51
 in DMZs, 49
 in full content collection, 652
 in hubs, 52
 managing, 98–99
 console access, 99
 in-band remote access, 100–101
 out-of-band remote access, 101–102
 observed traffic with, 355
 "BSD Packet Filter: A New Architecture for User-Level Packet Capture", 695papers on, 694
 "Design and Deployment of a Passive Monitoring Infrastructure", 697–698
 "Measurement and Analysis of IP Network Usage and Behavior", 697
 "OC3MON: Flexible, Affordable, High Performance Statistics Collection", 695–696
 "Stateful Intrusion Detection for High-Speed Networks", 699–700
 "Tactical Operations and Strategic Intelligence: Sensor Purpose and Placement", 700–701
 in perimeters, 49
 in Prelude, 298
 for session data, 482
 in Sguil, 322
 for wireless monitoring, 85
- Separating analysts from consoles, 647
- Sequence numbers
 in ICMP Echo, 671
 in LFT, 554, 557
 in TCP, 131, 591, 673–682
- Server Message Block (SMB) protocol, 273
- Service/Port Usage screen, 282
- Service Set Identifiers (SSIDs), 88
- Services in defensible networks, 23
- Session data, 211, 473
 Argus for, 234–236, 474–475
 Argus server, 236–237
 Ra client, 238–242
 from DMZ segments, 475–479
 from external segments, 488–490
 Flow-tools, 224–232
 forms of, 212–214
 Fprobe, 220–221
 NetFlow, 214–220
 ng_netflow, 222–224
 scenario for, 474–475

- sFLOW and sFLOW toolkit, 232–235
- Tcp replay, 226–228
- Tcp trace, 242–246
 - from VLANs, 479–488
 - from wireless segments, 475–476
- "Session first" method, 213
- Sessions, 211
 - identifiers for, 329
 - querying for, 327–328
 - rebuilding, 167, 169, 338
- SF field in Bro states, 296
- sFlow Probe tool, 215
- sFLOW toolkit, 232–234
- sFLOW utility, 232–235
- sFlowTest.awk script, 233–234
- Sguil, 317–318
 - alert handling in, 323–329
 - FTP SITE overflow attempts, 339–340
 - MISC MS Terminal Server Request, 342–343
 - SCAN FIN, 498–501
 - SCAN nmap TCP, 340–342
 - SHELLCODE x86 NOOP, 332–339
 - Truncated Tcp Options, 492–494
 - benefits, 318–319
 - for decisions, 329–331
 - development of, 755
 - events in, 39, 329–330
 - for full content packet data, 652
 - interface, 321–323
 - for POf, 209
 - vs. reference intrusion model, 331–343
 - for Tcpflow, 184
 - for UDP port 53 traffic
 - normal, 434–442
 - suspicious, 448–455
 - sguil.conf file, 321
 - SH field in Bro states, 296
- Shanker, Umesh, "Active Mapping: Registering NIDS Evasion Without Altering Traffic", 735–736
- Shaw, Mark, 457
- SHELLCODE x86 NOOP alerts, 332–339
- Shema, Mike
 - Anti-Hacker Tool Kit, 413
 - Hacking Exposed* series, 413
- Shepard, Timothy Jason, "TCP Packet Trace Analysis", 703–704
- Shimomura, Tsutomu, TCP sequence number predictions by, 590
- Short-term incident containment (STIC), 381
- show interface command, 252–254
- show interface accounting command, 254–255
- show interface ngeth0 command, 256–257
- show ip accounting command, 250, 256
- show ip cache flow command, 219
- show ip flow export command, 219
- show ip traffic command, 251–252
- Show Packet Data option, 323
- Show Rule option, 323
- show version command, 219
- SHR field in Bro states, 296
- Shrader, Larry, 753
- Siden tool, 610–611
- Sif field in Flow-cat, 230
- SIGINT for traffic analysis, 36
- "Signal Analysis of Network Traffic Anomalies" (Barford, Kline, Plonka, and Ron), 714–715
- Signal regeneration in taps, 75
- Signature feedback, 384
- Signature techniques
 - vs. anomaly detection, 762
 - antivirus products, 655
 - IDSs, 369
 - limitations of, 38
 - paper on, 707, 718–719
 - vs. rule-based, 691
- Silent network interfaces, 51
- SiLK (System for Internet-Level Knowledge)
 - NetFlow analysis project, 232
- Silver bullets, 4
- Simon, William L., *Art of Deception: Controlling the Human Element of Security*, 414
- Simple Mail Transfer Protocol (SMTP), 618–620, 623
- Simple Network Management Protocol (SNMP)
 - community strings in, 273–274
 - for RMON, 171
 - vulnerabilities, 10–11
- Simple Object Access Protocol (SOAP) over HTTP, 350
- Site Protector product, 653
- Skoudis, Ed
 - Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses, 413
 - Malware: Fighting Malicious Code, 413
 - Slurm utility, 263

INDEX

- Smart insiders, 50
- SMB (Server Message Block) protocol, 273
- Smirnof, Gleb, ng_netflow by, 222
- SMTP (Simple Mail Transfer Protocol), 618–620, 623
- Snare for in-house NSM solutions, 400
- SNMP (Simple Network Management Protocol)
 - community strings in, 273–274
 - for RMON, 171
 - vulnerabilities, 10–11
- SNMP-enabled network devices, MRTG polling by, 272
- Snoop program
 - data format in, 123
 - for raw trace files, 196–204
- snort.conf file, 161
- Snort IDS
 - for alerts, 39, 285, 320
 - basic usage, 149–152
 - for chained covert channels, 508
 - with Fragroute, 539–546
 - for full content data, 149–153, 652
 - reference for, 412
 - for specific packet parts, 159–161
 - for WAPs, 86
- Snort-inline, 77
- "Snort---Lightweight Intrusion Detection for Networks" (Roesch), 731–733
- snort.log.TIMESTAMP file, 160–162
- Snort.org documentation, 500
- Snort Personal Real-time Event GUI (SPREG), 754
- Snort-Wireless project, 657
- Snort-Wireless tool, 93
- SOAP (Simple Object Access Protocol) over HTTP, 350
- Softflowd probe, 224
- Solaris, sadmind exploitation attempt on, 570–575
- Song, Dug, Fragroute by, 534
- Source addresses, spoofed, 47, 589–597
- Sources of attacks
 - by country, 600–601
 - internal vs. external, 32–34
- Spafford, Eugene H., "Application of Pattern Matching in Intrusion Detection", 718–719
- SPAN (Switched Port Analyzer) ports, 56–63
 - advantages and disadvantages of, 84
 - for session data, 482
 - tap outputs on, 71
- SPARC hardware for sensors, 94
- Special Ops: Host and Network Security for Microsoft, UNIX, and Oracle* (Birkholz), 413
- Specific packet parts
 - Snort for, 159–161
 - Tcpdump for, 154–157
 - Tethereal for, 157–159
- Speed of NICs, 54
- Spice (Stealthy Probing and Intrusion Correlation Engine), 735
- Spitzner, Lance
 - Honeypots: Tracking Hackers, 413
 - "Know Your Enemy: The Tools and Methodologies of the Script Kiddie", 746–747
- Spoofed source addresses, 47, 589–597
- SPREG (Snort Personal Real-time Event GUI), 754
- SQL Server Security* (Andrews, Litchfield, and Grindlay), 413
- SQL Slammer worm, 309, 593
- Squid proxy, 351
- src_as field in NetFlow, 217
- src_mask field in NetFlow, 217
- srcaddr field in NetFlow, 217
- SrcP field in Flow-cat, 230
- srcport field in NetFlow, 217
- SSIDs (Service Set Identifiers), 88
- SSL (Secure Sockets Layer) protocol
 - in HTTPS session, 623
 - support for, 618
 - for Unicode attacks, 627–628
- Ssn ID column in Sguil, 329
- ST column in Sguil, 322
- Staff
 - in in-house NSM solutions, 401–402
 - training program roles and responsibilities, 422
- "Stalking the Wily Hacker" (Stoll), 739–741
- Staniford-Chen, Stuart
 - "Common Intrusion Detection Framework", 727
 - "GrIDS: A Graph-Based Intrusion Detection System for Large Networks", 719
 - "Practical Automated Detection of Stealthy Portscans", 735
 - on Rome Labs attack, 587
 - "Towards Faster String Matching for Intrusion Detection or Exceeding the Speed of Snort", 734–735
- start-time field in Bro logs, 295
- state field in Bro logs, 295

- "State of the Practice of Intrusion Detection Technologies" (Allen), 686
- Stateful inspection, 761
- "Stateful Intrusion Detection for High-Speed Networks" (Kruegel, Valeur, Vigna, and Kemmerer), 699–700
- Statistical data, 247–249
 - Bmon, 258–260
 - Cisco accounting, 249–255
 - Ifstat, 257–258
 - Ipcad, 255–257
 - MRTG, 271–278
 - Ntop, 278–283
 - paper on, 694
 - Tcpdstat, 266–271
 - Trafshow, 260–264
 - Ttt, 260–264
- Statistics command in Ethereal, 170
- Stats tab, Ntop, 279
- Status in Ipcad, 256
- Stealing the Network: How to Own the Box* (Russell), 414
- Stealth reconnaissance, 635
- Stealthy Probing and Intrusion Correlation Engine (Spice), 735
- Stegunnel application, 119
- Stepping-stones
 - attacks from, 584–589
 - availability of, 593
- Stevens, W. Richard, *Protocols (TCP/IP Illustrated, Volume 1)*, 415
- STIC (short-term incident containment), 381
- Stolfo, Salvatore J., "Data Mining Approaches for Intrusion Detection", 727–728
- Stoll, Clifford, "Stalking the Wily Hacker", 739–741
- Stones, Richard, *Beginning Databases with PostgreSQL*, 418
- Storing full content data
 - Snort for, 152–153
 - Tethereal for, 141–144
- Strategic Warfare in Cyberspace* (Rattray), 421
- String matching
 - in Fragroute, 541–542
 - in Ngrep, 185–189
- strings command, 185
- Structured threats, 7, 583
- Sub-network access protocol headers, 666
- Subversion, 16
- Successful Denial-of-Service Attack incident category, 373
- sudo utility, 401
- Summer, Robin, "Enhancing Byte-Level Network Intrusion Detection Signatures with Context", 736–739
- Suspicious traffic, 361
 - paper on, 704–705
 - port 53
 - TCP, 455–459
 - UDP, 448–455
- Switched Port Analyzer (SPAN) ports
 - advantages and disadvantages of, 84
 - for session data, 482
 - tap outputs on, 71
- SYN flag in LFT, 554
- SYN flooding, 515–517, 591–592
- Syn4k program, 515
- SYN+ACK test, 205–207
- Synk4 program, 515
- Sys Admin Magazine*, 427
- System administration
 - case study response by, 388–389
 - training program for, 415–418
- "System for Distributed Intrusion Detection" (Brentano), 717–718
- System for Internet-Level Knowledge (SiLK)
 - NetFlow analysis project, 232
- System messages in Sguil, 321
- SysUptime field in NetFlow, 216
- T**
- T-1 standard, 56
- T-3 standard, 56
- t switch
 - Ifstat, 257
 - IPsumdump, 189
 - Tcpslice, 176
- t ad switch, Tethereal, 144
- T paranoid switch, Nmap, 604
- "Tactical Operations and Strategic Intelligence: Sensor Purpose and Placement" (Heberlein), 700–701
- Tactics, 583–584
 - anonymity. *See* Anonymity
 - degrading and denying collection, 639
 - decoys in, 639–641
 - sensor attacks in, 643–647

INDEX

- Tactics, *continued*
- separating analysts from consoles, 647
 - volume attacks in, 641–643
 - evading detection. *See* Evading detection
 - normal appearance, 634–638
 - references for, 412
 - self-inflicted NSM problems, 647–649
 - tools for, 410–412
- "TAMU Security Package: An Ongoing Response to Internet Intruders in an Academic Environment" (Safford, Schales, and Hess), 692–694
- Tap interface, 180
- Taps (test access ports), 63–65
- advantages and disadvantages, 84
 - for combining outputs, 71–72
 - and hubs, 72
 - new, 72–76
 - for separate traffic collection, 68–71
 - virtual interface bonding, 66–68
- Tcl (Tool Command Language), 264, 319
- TCP (Transmission Control Protocol)
- for chained covert channels, 511
 - data reconstruction, 182–185
 - headers for, 672–673
 - packets in
 - for LFT, 548, 551–552
 - malicious, 466–471
 - normal, 442–448
 - Packit for, 527–528
 - suspicious, 455–459
 - in Xprobe2, 561
 - sequence numbers in, 673–682
 - in blind TCP spoofing, 590–591
 - with decoys, 640
 - in LFT, 554, 557
 - Tcpdump representation of, 128–130
 - tcp_chaff cksum option in Fragtest, 536
 - tcp filter with Tethereal, 143
 - tcp_flags field in NetFlow, 217
 - tcp.flags.urg filter in Ethereal, 166
 - TCP handshake, 565
 - tcp_opt mss option in Fragtest, 536
 - "TCP Packet Trace Analysis" (Shepard), 703–704
 - tcp_seg size option in Fragtest, 536
 - TCP/UDP header options in Packit, 522
 - Tcpdstat utility, 266–271
- Tcpdump utility, 122–123
- for ARP filters, 356–358
 - basic usage, 124
 - with decoys, 639–641
 - for denial-of-service attacks, 568–569
 - for filtering bridges, 80–81
 - with Fragroute, 538–541
 - for full content data, 125–132
 - for Berkeley Packet Filters, 135–140
 - for detail, 134–135
 - reading, 126–132
 - storing, 125–126
 - timestamps in, 132–134
 - for ICMP, 363
 - with LFT, 556
 - for NetFlow, 219
 - for ng_netflow, 223
 - with Packit, 529–530
 - for raw trace files, 198, 200–204
 - reference for, 412
 - for SCAN FIN alerts, 500
 - for sensor attacks, 645–646
 - for sensors, 97
 - for separate traffic collection, 69
 - for SPAN ports, 58
 - for specific packet parts, 154–157
 - with spoofed addresses, 596
 - for taps, 65
 - for TCP traffic, 446–447
 - with Tcpdstat, 271
 - with Tcpslice, 177–178
 - vs. Traceroute, 548–550
 - for virtual interface bonding, 67
 - vulnerabilities in, 99–100
 - for wireless monitoring, 92
 - for Xprobe2, 562
- Tcpdump-xploit.c code, 368
- Tcpflow utility
- for chained covert channels, 512–513
 - for data reconstruction, 182–185
 - for encrypted e-mail, 618–619
 - in Sguil, 320
- Tcpreplay utility
- for packet replay, 179–182
 - for session data, 226–228
- Tcpslice utility, 174–178
- Tcptrace utility, 242–246

- Teams in in-house NSM solutions, 400
- Telecommunications, training program for, 414–415
- Telecommunications Essentials* (Goleniewski), 415
- Teo, Lawrence, Siden by, 610–611
- Terminal Services, Tsgriinder on, 113–114
- Test access ports (taps), 63–65
 - advantages and disadvantages, 84
 - for combining outputs, 71–72
 - and hubs, 72
 - new, 72–76
 - for separate traffic collection, 68–71
 - virtual interface bonding, 66–68
- Testing
 - filtering bridges, 82–83
 - hub deployment, 55
 - IDSs, 359
 - paper on, 750–751
- Tethereal utility, 140
 - basic usage, 140–141
 - for full content data
 - detail, 146–149
 - reading, 144–146
 - stringing, 141–144
 - for Packit packets, 532–533
 - for RPC exploit, 577–578
 - for SPAN ports, 60–61
 - for specific packet parts, 157–159
 - with Xprobe2, 562–564
- TFTP (Trivial FTP) for tools retrieval, 629–630, 633–634
- "There Be Dragons" (Bellovin), 705
- Thomas, Rob, on spoofing, 593
- Thompson, Kevin, "OC3MON: Flexible, Affordable, High Performance Statistics Collection", 695–696
- Threat analysis, 8
- Threat conditions, 8
- Threat correlation, 26
- Threats and threat models, 7–8
 - in I&W process, 26
 - in Polish Ministry of Defense case study, 10
 - in risk equation, 6–8
 - for wireless monitoring, 85
 - and zone monitoring, 45–51
- Threshold-based IDSs, 369
- Throttles in statistics, 254
- Time out entries in Ra, 239
- Time Stamp Echo Reply (TSER) in Tethereal, 146
- Time Stamp Value (TSV) in Tethereal, 146
- Timestamp Request options in Packit, 523
- Timestamps
 - in Editcap, 174
 - in Ifstat, 257
 - memory storage conventions for, 201
 - for Snort, 152
 - in Tcpdump, 132–134
 - in Tcpslice, 175–177
- Timing of attacks, 604–607
- tip command, 218
- Tjaden, Brett, "Detecting Network Intrusions via a Statistical Analysis of Network Packet Characteristics", 710–711
- Tk toolkit, 264, 319
- TLS (Transport Layer Security), 618–620, 622
- Toledo, Juan, Etherape by, 191
- Toleration of intrusions, 6
- Tool Command Language (Tcl), 264, 319
- Tools
 - for attacking NSM. *See* Attacks
 - as intruder targets, 17, 628–631, 633–634
- Top talkers, Trafshow for, 261
- .torrent files, 452, 454–455, 463
- tos field in NetFlow, 217
- Total tab, Ntop, 280
- "Towards Detecting Intrusions in a Networked Environment" (Heberlein), 716–717
- "Towards Faster String Matching for Intrusion Detection or Exceeding the Speed of Snort" (Coit, Staniford, and McAlerney), 734–735
- trace.\$BROID directory, 294
- Traceroute tool, 548–550
- Traceroutes, coordinated, 607
- Traffic and traffic analysis
 - for chained covert channels, 505
 - detection through, 36–37
 - filtering, 21
 - graphing tools for, 260–264
 - normalizers, 748
 - scrubbing, 22, 351
- Traffic option, Ntop, 279
- Trafshow utility, 260–264
- Training for analysts, 405–407, 648
 - for management and policy, 421
 - paths to security field, 407–409

INDEX

- Training for analysts, *continued*
 periodicals and web sites for, 426–427
 process, 422–426
 for scripting and programming, 418–420
 special operators truths in, 407–409
 for system administration, 415–418
 for telecommunications, 414–415
 tool updating for, 427–431
 weapons and tactics for, 410–414
- Transaction signature (TSIG) handling code, 466–468
- Transcripts in Sguil, 324
- Transmission Control Protocol. *See* TCP (Transmission Control Protocol)
- Transparent bridges, inline, 77
- Transport Layer Security (TLS), 618–620, 622
- Trivial FTP (TFTP) for tools retrieval, 629–630, 633–634
- Troubleshooting Campus Networks: Practical Analysis of Cisco and LAN Protocols* (Oppenheimer and Bardwell), 415
- Truncated Tcp Options alerts, 492–498
- Trusted hosts for anonymity, 599
- Trusted operating systems
 in in-house NSM solutions, 400
 root accounts in, 372
- TS field in Flow-cat, 231
- TSER (Time Stamp Echo Reply) in Tethereal, 146
- Tsgrinder program, 113–114
- TSIG (transaction signature) handling code, 466–468
- TSV (Time Stamp Value) in Tethereal, 146
- tt switch, Tcpcdump, 132–134
- TTL values in LFT, 557
- Ttt tool, 260–264
- Tttprobe program, 266
- tttt switch, Tcpcdump, 132–133
- Tttview collector, 266
- Tung, Brian, "Common Intrusion Detection Framework", 727
- Tunnelshell program, 460–464
- Turner, Aaron, Tcpreplay by, 179
- U**
- U switch, Argus, 236
- u switch, Tcptrace, 244
- udp.dstport filter, 166
- UDP (User Datagram Protocol) protocol and datagrams
 creating with Packit, 526–527
 headers in, 682–683
 packets in
 malicious, 459–466 with LFT, 551
 normal, 434–442
 suspicious, 448–455
 with Traceroute, 550
 in Xprobe2, 561
 spoofing, 593
 Tcpcdump representation of, 127–128
- udp switch, Ngrep, 186
- UDP tab for Packit packets, 532
- Unauthorized Root-Admin Access incident category, 372–373
- Unauthorized User Access incident category, 373
- Unicode attacks, 625–629
- unicoder.pl script, 632
- unix_nsecs field in NetFlow, 216
- UNIX philosophy, cooperating tools in, 317
- unix_secs field in NetFlow, 216
- UNIX Shell Programming* (Kochan and Wood), 420
- UNIX System Administration Handbook* (Nemeth), 418
- Unpatched Solaris systems, sadmind exploitation on, 570–575
- Unpatched Windows systems, RPC exploitation against, 575–581
- Unstructured threats, 7, 15, 583
- USENIX Security conference, 425
- User Datagram Protocol. *See* UDP (User Datagram Protocol) protocol and datagrams
- User messages in Sguil, 321
- Usernames, cracking, 113
- V**
- v switch
 Snort, 149
 Tcpcdump, 134–135
 Xprobe2, 559
- V switch
 LFT, 552, 554
 Ngrep, 188
 Tethereal, 147–148
- VACLs (Virtual Access Control Lists), 62

- Valdes, Alfonso, "Live Traffic Analysis of TCP/IP Gateways", 706–707
- Valeur, Fredrik, "Stateful Intrusion Detection for High-Speed Networks", 699–700
- Validation phase in detection, 371–377
- Vandoorselaere, Yoanne, Prelude by, 298
- vBNS (very high speed Backbone Network Service) project, 696
- ve switch, Snort, 153
- Vendor questionnaires in case study, 394–396
- Verbosity level in Tcpdump, 134–135
- version field in NetFlow, 216
- Versions
 - BIND, 465–466
 - OpenSSH, 622–623, 625
- Very high speed Backbone Network Service (vBNS) project, 696
- Viega, John, *Building Secure Software: How to Avoid Security Problems the Right Way*, 420
- Vigna, Giovanni
 - home page for, 753
 - "NetSTAT: A Network-Based Intrusion Detection Approach", 728–729
 - "Stateful Intrusion Detection for High-Speed Networks", 699–700
- Virtual Access Control Lists (VACLs), 62
- Virtual interfaces, bonding for, 66–68
- Virtual local area networks (VLANs)
 - session data from, 479–488
 - with SPAN ports, 58–61
- Virus Infection incident category, 374
- Visscher, Robert "Bamm"
 - NSM Webcast by, 755
 - Sguil by, 319, 755
 - SPREG by, 754
- Visual Basic code, 429–430
- VLANs (virtual local area networks)
 - session data from, 479–488
 - with SPAN ports, 58–61
- Voelker, Geoffrey M., "Inferring Internet Denial-of-Service Activity", 749
- Volume attacks, 641–643
- Vorovyev, Vladimir, Trafshow by, 260
- Vulnerabilities
 - in I&W process, 26
 - in Polish Ministry of Defense case study, 10
 - in risk equation, 8–9
- SNMP, 10–11
- Tcpdump, 99–100
- Vulnerability assessment products, integration of, 653–654
- W**
- w command for Sguil, 335
- w switch
 - Argus, 236
 - Flow-capture, 225
 - Ntop, 279
 - P0f, 208
- Walkin, Lee, Ipcad by, 255
- WAPs (wireless access points), 85–86
- Warnings, 25–28
- Weapons
 - references for, 412
 - tools for, 410–412
- Web-based tools, limitations of, 318
- Web defacers, blocking, 616–617
- Web Server Folder Directory Traversal vulnerability, 624–628
- Web sites for training program, 426–427
- weird.\$BROID directory, 294
- Welch, Brent, *Practical Programming in Tcl and Tk*, 420
- Welchia worm, 508, 576, 589
- Well-defined security policies, 348
- WEP (Wireless Equivalent Privacy) encryption, 90–91
- WEP (Wireless Equivalent Privacy) keys, 86
- Whois database information, 321
- Wide area internet traffic, 702–703
- Wilder, Rick, "OC3MON: Flexible, Affordable, High Performance Statistics Collection", 695–696
- Windows systems
 - RPC exploitation against, 575–581
 - XMAS scan against, 635–637
- Windows XP Under the Hood: Hardcore Windows Scripting and Command Line Power* (Knittel), 420
- Windump tool
 - reference for, 412
 - for separate traffic collection, 70
- Winkler, Linda, "Combining Cisco NetFlow Exports with Relational Database Technology for Usage Statistics, Intrusion Detection, and Network Forensics", 713

INDEX

- Winpcap tool, 652
Wireless access points (WAPs), 85–86
Wireless Equivalent Privacy (WEP) encryption, 90–91
Wireless Equivalent Privacy (WEP) keys, 86
Wireless networks
 in in-house NSM solutions, 398–399
 infrastructure, 657
 monitoring, 50, 85–93
 platforms, 85
 session data from, 475–476
Wood, Patrick, *UNIX Shell Programming*, 420
Worms, 374
Writing Information Security Policies (Barman), 421
Writing Secure Code (Howard and LeBlanc), 420
- X**
- x switch
 - Ngrep, 186
 - P0f, 208
 - Tethereal, 146
 - X switch
 - Ngrep, 188
 - Snort, 150
 - Tcpdump, 134–135
- XMAS scan, 635–637
Xprobe tool, 411
Xprobe2 tool, 558–566
xscript.\$BROID directory, 294
- Y**
- Yarochkin, Fyodor
 "Remote OS Detection via TCP/IP Stack
 Fingerprinting", 708–709
 tools poll by, 410
 Xprobe2 by, 558
- Yellow alerts in Prelude, 312
Yurcik, William, "Achilles' Heel in Signature-Based
 IDS: Squealing False Positives in Snort",
 733–734
YXORP project, 354
- Z**
- z switch, Ifstat, 258
 - z io,phs switch, Tethereal, 148
- Zalewski, Michael
 Netsed by, 204
 P0f by, 205
 on TCP sequence numbers, 591
Zelikow, Phil, 344
Zeltser, Lenny, *Malware: Fighting Malicious Code*,
 413
Zero-day exploits, 12–13
Zhodiac, Tcpdump-xploit.c code by, 368
Ziese, Kevin, on Rome Labs attack, 587–588
Zoellick, Bill, *CyberRegs: A Business Guide to Web
 Property, Privacy, and Patents*, 421
- Zones
 accessing traffic in, 51
 hubs, 52–56
 inline devices, 76–84
 SPAN ports, 56–63
 summary, 84
 taps. *See* Taps (test access ports)
 monitoring, 45–51