Index

OSI reference model
- overview, 2-3
- routers on, 4-2
OSPF (Open Shortest Path First), 4-4
Outsider threats, 8-3

P
- P2 Enterprise Shuttle, 2-41
- Packet marking, 5-14
- Packet-mistreating attacks, 4-5
- Pandora FMS, 3-49
- Paper mills, 9-11
- Parameter tampering, 3-5
- Paros, 3-29–3-30
- Patents, 9-23–9-25
- infringement, 9-24
- introduction, 9-23
- search for, 9-24
- types of, 9-23–9-24
- Patents (Amendment) Act (1999), 9-33
- Path identification (Pi) method, 5-15
- PC Inspector File Recovery, 11-5, 11-6
- Persistent attacks, 4-5
- Perverted Justice, 11-35
- Philippine laws, against child pornography, 11-26
- Phishing, 7-8, 7-17, 7-18
- Physical layer, of OSI model, 2-5
- Ping of death attacks, 5-2
- Plagiarism
- detection factors, 9-11–9-12
- detection tools, 9-12–9-23
- prevention steps, 9-11
- types of, 9-11
- PlagiarismDetect.com, 9-21, 9-22
- PLAGUE, 9-16–9-17
- POP3 (Post Office Protocol version 3), 7-3–7-4
- Post Office Protocol version 3 (POP3), 7-3–7-4
- PRAISE, 9-19, 9-20
- Presentation layer, of main protocols, 2-4–2-5
- Privatefirewall, 8-11–8-12
- Probabilistic packet monitoring (PPM), 5-14
- Process accounting, 1-18–1-19
- ProDiscover Investigator, 2-41, 2-42
- Profiling, 8-6
- Project Safe Childhood (PSC), 11-27
- Promiscuous attacks, 2-7
- Protocols, overview, 2-3–2-5
- Proxy servers, DNS poisoning on, 2-8, 2-9

Q
- Quid pro quo harassment, 10-3

R
- “Received” headers, 7-13
- Recover My Email for Microsoft Outlook, 7-22
- Reflected attacks, 5-4
- Reliance party, 9-10
- Remote logging, 1-9–1-10
- Report Child Porn, 11-37, 11-38
- Reveal, 11-12
- R-Mail, 7-20, 7-21
- Router Audit Tool (RAT), 4-16–4-17
- Router forensics
- definition of router, 4-2
- functions of a router, 4-2–4-4
- introduction, 4-2
- investigating router attacks, 4-6–4-16
- router attacks, 4-4–4-5
- router vulnerabilities, 4-4
- tools for, 4-16–4-18
- vs. traditional forensics, 4-5
- Router logs, 4-12–4-13
- Routing Information Protocol (RIP), 4-3–4-4
- Routing table, 4-3–4-4
- Routing table poisoning, 4-5

S
- SafeAssignment, 9-19, 9-20
- Sample complaint form, 10-12–10-14
- Samspade, 6-12
- Sawmill, 4-18
- Scottish laws, against child pornography, 11-25
- Scrawlr, 3-34
- Search warrants, 6-4–6-5, 7-8–7-9
- Security, for Web applications, 3-15
- Sequential change-point detection, 5-8
- Server Log Analysis (tool), 3-20
- Session layer, of main protocols, 2-4–2-5

Sexual harassment
- Australian laws on, 10-11–10-12
- Chinese laws on, 10-12
- complaint procedures, 10-7–10-8
- consequences of, 10-4
- defined, 10-2
- dos and don’ts for employees, 10-5
- employee responsibilities, 10-7
- German laws on, 10-12
- Indian laws on, 10-12
- introduction, 10-2
- investigation process, 10-9–10-10
- Malaysian penal code on, 10-12
- policies, 10-9
- preventive steps, 10-9–10-10
- stalking, 10-5–10-6
- stalking laws, 10-15
- statistics, 10-4
- supervisors responsibilities, 10-7
- types of, 10-2–10-4
- U.K. laws on, 10-12
- U.S. laws on, 10-10–10-11

Sherlock, 9-17, 9-19
- Show Traffic, 2-42
- Siemens Monitoring Center, 2-36–2-37
- Signature analysis, 8-6–8-7
- Simple Mail Transfer Protocol (SMTP), 7-3
- SIM (Software Similarity Tester), 9-16, 9-17
- SmartSniff, 2-21, 2-22
- SmartWhois, 3-44
- SMTP (Simple Mail Transfer Protocol), 7-3
- Smurf attacks, 5-3
- Sniff-O-Matic, 2-33, 2-34
- Sniphere, 2-29–2-30
- Snork attacks, 5-4
- Snort Intrusion Detection System, 2-43–2-44
- Socklog, 1-10–1-11
- SoftPerfect Network Protocol Analyzer, 2-15–2-16, 2-17
- South African laws
- against child pornography, 11-24–11-25
- for trademarks and copyright, 9-38
- South Korean laws, for trademarks and copyright, 9-39