Index

2X1 10/100 Regeneration Tap, 116–119
2X1 10/100 SPAN Regeneration Tap, 116–119
10/100 Port Aggregator Tap, 108

A
Acceptable use policies, 220
Access control, 33. See also Layer 3 access control.
Access control devices, 13
ACLs (access control lists), 156–157
Active FTP, 188–193
Active participation (on a wireless network), 107
Adaptation and evolution, 26
Alert data
definition, 15
extrusion detection, 96–104
generic IDS rules, 101
honeytokens, 103–104
outbound connection attempts, 98
outbound exploitation, 101–103
server replies to attacks, 98–101
tools, 23
Alerts, 11
Amap, 354–356
Analyzer tools, 18
Analyzing. See also Network forensics.
   NBE (network-based evidence)
      documenting activities, 267
      malicious traffic, 267
      methodologies, 268–273
      results validation, 266–267
      threats. See TTA (traffic threat assessment).
Anderson, James P., 81
Anomaly recognition, 352–358
Appliances
   converged, 322–323
   minimizing, 68–72
Application enumeration programs, 365–367
Application relevance, 13–14
Application scanners, 354–356
Applications, minimizing, 68–74
Arbor Networks PeakFlow, 96
Argus
   awk, parsing records with, 286–288
   collecting session data, 328–330
definition, 279–280
deploying, 279–280
INDEX

Argus, continued
full content data, 296–299
interpreting output, 282–286
session data, 279–280
Assessment (as part of the security process), 6.
See also TTA (traffic threat assessment).
Asset value, 8
Asset-based alerting, 345
Assets, 7
Audit systems, 13
awk, 286–288

B
Barros, Augusto Paes de, 103
Best evidence, 262
Blaster worm, 17
Blocking outbound traffic, 36–40
Books and publications
Computer Security Threat Monitoring and Surveillance, 81
“Extrusion Detection Systems: The Art of...Monitoring,” 85
A Guide to Forensics Testimony... , 245
“Honeytokens: The Other Honeypot,” 103–104
Incident Response, 299
The IRC Beginner’s Reference, 307
A Network Security Monitor, 81
Real Digital Forensics..., 219, 299
The Tao of Network Security..., 114–116
Wi-Foo: The Secrets of Wireless Hacking, 18
Bot nets, 89–90, 308. See also IRC bots.
Bot worms, 314–316
Brace, Rebecca Gurley, 245
Bro, 24
BullGuard, 86

C
CAR (Committed Access Rate), 157–159
CBP (Class Based Policing), 159–161
CCNA (Cisco Certified Network Associate), 275
CDP (Cisco Discovery Protocol), 68–73
CDPSniffer, 71
Centralized configurations, 347
Centralizing logs, 227
Certifications, 274–275
Chain of evidence, 266
CIFI (Certified Information Forensics Investigator), 274–275
Cisco NetFlow, 325–327
CISSP (Certified Information Systems Security Professional), 274
Clayton, Richard, 85
Collecting data. See also Network forensics;
TTA (traffic threat assessment).
distributed traffic, 126–130
full content data, 237–239
monitoring defensible networks, 28–29
network traffic, 228
session data
with Argus, 328–330
with Cisco NetFlow, 325–327
for incident response, 237–239
tools for, 18
TTA (traffic threat assessment), 181–187
Committed Access Rate (CAR), 157–159
Communication security, 221, 228–231
Computer Security Incident Response Team (CSIRT). See CSIRT (Computer Security Incident Response Team).
Computer Security Threat Monitoring and Surveillance, 81
Continuous scanning, 343–345
Control channels
bot nets, 311–314
identifying, 188–193
Controlled networks, 9
Controlling defensible networks. See also Layer 3 access control.
access control, 33
blocking outbound traffic, 36–40
containing extrusions, 34–36
examples, 38–40
filtering outbound traffic, 37
outside-in defense, 33–34
Pf (Packet Filter) firewall, 38–40
proxying outbound traffic, 43–54
replacing outbound traffic, 54–66
throttling outbound traffic, 40–43
Converged appliances, 322–323
Conversations. See Session data.
Cost of replacement, 8
Countermeasures, 8
See also Controlling defensible networks
See also Incident response
See also Internal intrusions, containing
See also Layer 3 access control
See also TTA (traffic threat assessment)
Credentials, 347
CSIRT (Computer Security Incident Response Team)
communication methods, 221, 228–231
communication security, 228–231
creating, 220
Customer contacts, incident response, 233–234

D
Daily scanning, 343–345
Data, network. See Network data.
Data analysis tools, 20–21
Data channels, identifying, 188–193
Data collection. See Collecting data; Network forensics.
DataSafe, 86
Decision makers, 11
Deep packet inspection (DPI) firewalls, 37
Defense strategies
See Defensible networks
See Extrusion detection
See Incident response
See Internal intrusions, containing
See Intrusion detection
See Layer 3 access control
See TTA (traffic threat assessment)
Defensible networks
adaptation and evolution, 26
characteristics of, 9–10
controlling
access control, 33
blocking outbound traffic, 36–40
containing extrusions, 34–36
definition, 9
elements, 38–40
filtering outbound traffic, 37
outside-in defense, 33–34
Pf (Packet Filter) firewall, 38–40
proxying outbound traffic, 43–54
replacing outbound traffic, 54–66
throttling outbound traffic, 40–43
definition, 9
keeping current, 9, 75–76
minimizing
appliances, 68–72
definition, 10
description, 66–75
element, 67
reducing applications, 68–74
resources, 74
services, 68–74
monitoring. See also Security, monitoring.
data collection, 28–29
definition, 9–10
pervasive network awareness, 27–33
risk reduction, 30
traffic visibility, 30–31
trusting results, 28
recognition, 26
recovery, 26
resistance, 26
survivability components, 26
Deficiencies, definition, 8
Defensive evidence, 263–265
Detection (as part of the security process), 6
See also Enumeration
See also Extrusion detection
See also Internal intrusions
Detection, continued
See also Intrusion detection
See also Monitoring
See also Network forensics
See also Traffic, accessing
See also TTA (traffic threat assessment)
Distributed traffic collection, 126–130
DMZs, taps, 125
DNS (Domain Name Servers), 213—216
Documenting
evidence collection, 258–259
incident response activities, 240
NBE (network-based evidence) collection, 267
Domain Name Servers (DNS), 213—216
DPI (deep packet inspection) firewalls, 37
Dual Port Aggregator Tap, 114–116
DuFresne, Ron, 85
Dup-to keyword, 126–130

E
E-mail, extrusion detection, 89
Encryption, collecting evidence, 253
End user contacts, incident response, 234
Enterprise sink holes, 144–147, 169–170
Enumeration, methods
asset-based alerting, 345
categories of scanners, 343–345
centralized configurations, 347
continuous scanning, 343–345
credentials, 347
daily scanning, 343–345
host agents, 347
instant scanning, 343–345
passive vulnerability discovery, 346–347
Enumeration, open source tools
Amap, 354–356
anomaly recognition, 352–358
application enumeration programs, 365–367
application scanners, 354–356
false positives, 353–354
host discovery, 350–352
identifying exposed services, 352–358
identifying live systems, 350–352
Nmap
application discovery, 357
identifying live systems, 350–352
OS identification, 358–359, 361–364
operating system identification, 358–364
Scanline, 350–352
service enumeration, 352–358
Superscan, 350–352
system ownership, 368
TCP port scan, 352–353
UDP port scan, 353–354
Windows enumeration, 365–367
Winfingerprint, 365–367
Xprobe2, 359–361
Escalation, 11
Evidence. See also Network forensics.
analyzing
documenting activities, 267
malicious traffic, 267
methodologies, 268–273
results validation, 266–267
collecting
automating the collection process, 258–259
collection weaknesses, 252–253
data volatility, 253
documenting the collection process, 258–259
encryption, 253
limiting access to sensors, 249–250
positioning sensors, 250
securing sensors, 248–249
sensor failure modes, 252
storage capacity, 253
tools and techniques, 253–258
verifying data collection, 251–252
visibility, 253
conclusions, 274–275
Daubert v. Merrell Dow Pharmaceuticals, Inc., 247
Federal Rules of Evidence, 247
general acceptance criteria, 247
governing documents, 247
Kumho Tire Company, Ltd. v. Patrick Carmichael, 247
NBE (network-based evidence)
documenting activities, 267
malicious traffic, 267
methodologies, 268–273
results validation, 266–267
preserving
best evidence, 262
chain of evidence, 266
copying to read-only media, 263
derivative evidence, 263–265
forms of evidence, 262
hash traces, 259–262
working copies, 262
relevance, 247
reliability, 247
rules for use, 247
Exploits, definition, 8
Extrusion detection
alert data, 96–104
bot nets, 89–90
definition, 4
description, 83–84
digital chat, 89
e-mail, 89
file transfer, 90–91
FTP (File Transfer Protocol), 90–91
full content data, 89–91
history of, 84–88
host profiling, 96
IM (instant messaging), 89
versus intrusion detection, 4–5
IRC (Internet Relay Chat), 89
malicious parties, 91–92
nonstandard protocols, 92
odd ports, 92
privacy aspects, 87
purpose of, 4–6
session data, 91–94
statistical data, 94–96
suspicious parties, 91–92
TFTP (Trivial File Transfer Protocol), 90–91
tools and utilities, 87
traffic, per time interval, 95–96
traffic mix, per time interval, 96
unauthorized parties, 91–92
unusual sessions, 92–94
Extrusion prevention, tools and utilities, 86
F
fakenet, 313
False positives, 80, 90–91, 353–354
FAX, security, 230
Fidelis Security Systems, 86, 88
Filtering outbound traffic, 37
Firewalls
DPI (deep packet inspection), 37
layer 7, 36
Pf (Packet Filter), 38–40
proxy, 43–45
remote administration, 60–61
First response. See also Incident response.
documenting activities, 240
full content data collection, 237–239
host-based live response, 239
intruder contact, limitations, 239–240
legal issues, 239–240
session data collection, 237–239
shutting down affected port, 234–237
Flows. See Session data.
Forensics, 246. See also Network forensics.
FTP (File Transfer Protocol)
active, 188–193
extrusion detection, 90–91
FTP, continued
   passive, 188–193
   transfers, omitting, 194–196
Full content data
   collecting, 237–239
   definition, 13–14
   extrusion detection, 89–91
   tools, 19
   TTA case study, 296–299

G
Gavrilenko, Konstantin V., 18
General incident response. See also Incident response.
   identifying and removing vulnerabilities, 243
   returning to service, 243–244
   scope of intrusion, 240–243
   verifying operations, 243–244
Granularity, 13
A Guide to Forensics Testimony..., 245

H
Hash traces, 259–262
Hashing, 259–260, 261
Heberlein, L. Todd, 81
Honeypots, 103
Honeytokens, 103–104
   “Honeytokens: The Other Honeypot,” 103–104
Host agents, 347
Host discovery, 350–352
Host inventory, 227–228
Host profiling, 96
Host-based live response, 239
Hub and spoke network, 138–139
Hubs, 106, 123

I
ICMP (Internet Control Message Protocol), 198
iController, 88
IDS (intrusion detection system), 101, 233
iGuard, 88
IM (instant messaging), extrusion detection, 89
Incident response
   CSIRT
      communication methods, 221, 228–231
      communication security, 228–231
      creating, 220
      customer contact, 233–234
      definition, 6, 219
      detection methods, 232–234
      end user contact, 234
      first response
         documenting activities, 240
         full content data collection, 237–239
         host-based live response, 239
         intruder contact, limitations, 239–240
         legal issues, 239–240
         session data collection, 237–239
         shutting down affected port, 234–237
      general incident response
         identifying and removing vulnerabilities, 243
         returning to service, 243–244
         scope of intrusion, 240–243
         verifying operations, 243–244
      IDS (intrusion detection systems), 233
      intruder profiles, 231–232
      law enforcement contact, 234
      log reviews, 233
      network performance data, 233
      peer contact, 234
      preparation
         acceptable use policies, 220
         centralizing logs, 227
         collecting network traffic, 228
         CSIRT, communication methods, 221
         CSIRT, creating, 220
         host inventory, 227–228
         IRP (Incident Response Plan), 220–221
         network maps, 227–228
security policies, 220

time synchronization, 221–227

secure communication

chat rooms, 231

communication methods, 221, 228–231

communication security, 228–231

FAX, 230

land line phones, 230

secure LAN, 230–231

voice mail, 230

structured threats, 231–232

TTA (traffic threat assessment), 233

unstructured threats, 232

vulnerability assessments, 233

Incident Response, 299

Incident Response Plan (IRP), 220–221

Incident response team. See CSIRT.

Incidents, definition, 6, 219

Indicators, definition, 11

Inline devices, 107

Inline matrix switches, 123–125

Instant messaging (IM), extrusion detection, 89

Instant scanning, 343–345

Intellectual property, tools and utilities, 86

Internal intrusions containing

ACLs (access control lists), 156–157

CAR (Committed Access Rate), 157–159

CBP (Class Based Policing), 159–161

overriding routing, 161–163

PBR (Policy-Based Routing) to Null0, 161–163

rate limiting, 157–161

stopping spoofed packets, 163–166

throttling, 157–161

traffic classes, 159–161

traffic policies, 159–161

uRPF (Unicast Reverse Path Forwarding), 163–166

identifying, 153–156. See also TTA (traffic threat assessment).

Internal network design, 137–141

Internet Control Message Protocol (ICMP), 198

Internet Relay Chat (IRC), 89. See also Chats.

Internet Security Association and Key Management Protocol (ISAKMP), 197–198

Intruder contact, limitations, 239–240, 252

Intruder profiles, 231–232

Intrusion detection

definition, 4

description, 80–83

versus extrusion detection, 4–5

privacy aspects, 87

Intrusion detection system (IDS), 101, 233

Intrusions, definition, 6

IPS (intrusion prevention systems), 36–37

IRC (Internet Relay Chat), 89. See also Chats.

The IRC Beginner’s Reference, 307

IRC bots. See also Bot nets.

a bot net admin, 316–319

bot worms, 314–316

common capabilities, 313

communication, 310

control channels, 311–314

fakenet, 313

identifying, 310

introduction, 308–309

LinkBot, 312–314

server channels, 311–314

IRP (Incident Response Plan), 220–221

WormRide, 315

ISAKMP (Internet Security Association and Key Management Protocol), 197–198

ISP sink holes, 141–143

J

Jones, Keith, 219, 299

K

Kuehl, Kirby, 350–352, 365–367
INDEX

L
Lanclope StealthWatch, 96
Land line phones, security, 230
LANs, secure communication, 230–231
Law enforcement contacts, incident response, 234
Layer 3 access control. See also Controlling defensible networks.
hub and spoke network, 138–139
internal intrusions, containing
ACLs (access control lists), 156–157
CAR (Committed Access Rate), 157–159
CBP (Class Based Policing), 159–161
overriding routings, 161–163
PBR (Policy-Based Routing) to Null0, 161–163
rate limiting, 157–161
stopping spoofed packets, 163–166
throttling, 157–161
traffic classes, 159–161
traffic policies, 159–161
uRPF (Unicast Reverse Path Forwarding), 163–166
internal network design, 137–141
sink holes
alternatives to, 170
configuration verification, 151–153
configuring, 149–150
definition, 141
disposing of traffic, 147–148
distribution layer summary, 152
disrupted enterprise, 144–147, 169–170
field notes, 169–170
internal intrusions, identifying, 153–156
ISPs (Internet Service Providers), 141–143
uRPF (Unicast Reverse Path Forwarding), 166–169
uses for, 170
three-tier network, 139–140
uRPF (Unicast Reverse Path Forwarding), 163–169
Layer 7 firewalls, 36
LDAP (Lightweight Directory Access Protocol), 200–201
Legal issues
evidence, 247–248
intruder contact, 239–240
prosecuting intruders, 246
terminating internal intruders, 246
Liebernam, Danny, 86–87
Link Aggregator Tap, 125
LinkBot, 312–314
Logs
centralizing, 227
reviews, incident response, 233
Lumeta, 350
M
Mandia, Kevin, 299
Marchand, Jean-Baptiste, 68
Matrix switches, 123–125
Mazu Profiler, 96
MD5 Message Digest Algorithm, 259
Md5deep, 261
Mikhailovsky, Andrei A., 18
Minimized networks, 10
Minimizing defensible networks
appliances, 68–72
description, 66–75
example, 67
reducing applications, 68–74
resources, 74
services, 68–74
Monitored networks, 9
Monitoring. See also Security, monitoring:
Traffic, accessing; TTA (traffic threat assessment).
defensible networks
data collection, 28–29
pervasive network awareness, 27–33
risk reduction, 30
traffic visibility, 30–31
trusting results, 28
on the WAP, 107
Moskowitz, Robert, 85
NADS (network anomaly detection system), 178–179
NBE (network-based evidence)
  documenting activities, 267
  malicious traffic, 267
  methodologies, 268–273
  results validation, 266–267
Network data, forms of
  alert
  definition, 15
  extrusion detection, 96–104
  generic IDS rules, 101
  honeypots, 103–104
  outbound connection attempts, 98
  outbound exploitation, 101–103
  server replies to attacks, 98–101
  tools, 23
full content
  collecting, 237–239
  definition, 13–14
  extrusion detection, 89–91
  tools, 19
  TTA case study, 296–299
  session. See also TTA (traffic threat assessment).
  collecting with Argus, 328–330
  collecting with Cisco NetFlow, 325–327
  definition, 14
  elements of, 179
  extrusion detection, 91–94
  limitations, 94
  malicious parties, 91–92
  nonstandard protocols, 92
  odd ports, 92
  session content, 92–94
  session duration, 92–94
  session frequency, 92–94
  suspicious parties, 91–92
  TTA case study, 279–280
  unauthorized parties, 91–92
statistical
  definition, 14–15
extrusion detection, 94–96
  tools, 23
Network forensics. See also Collecting data.
collecting evidence
  automating the collection process, 258–259
  collection weaknesses, 252–253
  data volatility, 253
  documenting the collection process, 258–259
  encryption, 253
  limiting access to sensors, 249–250
  positioning sensors, 250
  securing sensors, 248–249
  sensor failure modes, 252
  storage capacity, 253
  tools and techniques, 253–258
  verifying data collection, 251–252
  visibility, 253
conclusions, 274–275
definition, 6
forensics, definition, 246
governing documents, 247
NBE (network-based evidence)
  documenting activities, 267
  malicious traffic, 267
  methodologies, 268–273
  results validation, 266–267
preserving evidence
  best evidence, 262
  chain of evidence, 266
  copying to read-only media, 263
  derivative evidence, 263–265
  forms of evidence, 262
  hash traces, 259–262
  working copies, 262
  prosecuting intruders, 246
  terminating internal intruders, 246
Network maps, 227–228
A Network Security Monitor, 81
Network sniffing, 71
Nmap
application discovery, 357
identifying live systems, 350–352
OS identification, 358–359, 361–364
NSM (network security monitoring), 4, 10–13
NTP (Network Time Protocol), 196–197, 215

Omitting FTP transfers, 194–196
Operating system identification, 358–364
OSI model, intrusion conclusions, 274
Outbound traffic
blocking, 36–40
connection attempts, 98
exploitation, 101–103
filtering, 37
proxying, 43–54
replacing, 54–66
server replies to attacks, 98–101
throttling, 40–43
Outside-in defense, 33–34

Packet capture methods, 105–107
Packet Filter (Pf) firewall. See Pf (Packet Filter) firewall.
Passive FTP, 188–193
Passive inline taps, 112
Passive participation (on a wireless network), 107
Passive vulnerability discovery, 346–347
PBR (Policy-Based Routing) to Null0, 161–163
PCI Port Aggregator TAP, 107–114
Peer contacts, incident response, 234
Performance data, incident response, 233
Pervasive network awareness, 27–33
Pf (Packet Filter) firewall
distributed traffic collection, 126–130
dup-to keyword, 126–130
elements, 38–40
Policy-Based Routing (PBR) to Null0, 161–163
PortAuthority Technologies, 87
Ports
22 TCP, Secure Shell, 198–199
25 TCP, SMTP, 216
43 TCP, Whois, 199–200
80 TCP, HTTP, 126–130
123 UDP, NTP, 196–197
389 TCP, LDAP, 200–201
443 TCP, HTTPS, 130–135
445 TCP, SMB, 288–289
500 UDP, ISAKMP, 196–197
5003 to 9126, 201–209
44444 to 49993, 209–213
extrusion detection, 92
monitoring. See SPAN (Switched Port Analyzer).
scanning, 344
shutting down, 234–237
SPAN, 106, 116–119
test access. See Taps.
Prelude, 24
Prevention (as part of the security process), 6
See also Controlling defensible networks
See also Extrusion detection
See also Incident response
See also Internal intrusions, containing
See also Intrusion detection
See also Layer 3 access control
See also Sink holes
See also TTA (traffic threat assessment)
Privacy, 87
Probes, 18
Prosecuting intruders, 246
Prosise, Chris, 299
Protection, definition, 6
Protocols, extrusion detection, 92
Proxies, 43, 130–135
Proxy firewalls, 43–45
Proxy servers, 43–45
Proxying outbound traffic, 43–54
INDEX

Q
QoS (Quality of Service), 40–43

countermeasures, 8
defensible networks, 9–10
deficiencies, 8
definition, 6
detection, 6
exploits, 8
incident response, 6
incidents, 6
intrusions, 6
minimized networks, 10
monitored networks, 9
network forensics, 6
policies, 220
prevention, 6
principles, 8–10
process description, 6–8
process description, 6–8
protection, 6
reliability, 8
response, 6
risk, 7
structured threats, 7
threat analysis, 7
threat models, 7
threats, 7
unstructured threats, 7
vulnerability, 8

R
Ranum, Marcus, 43–45
Rate limiting, 157–161
Real Digital Forensics..., 219, 299
Recognition, 26
Reconnex, 88
Recovery, 26
Reliability, definition, 8
Replacing outbound traffic, 54–66
Resistance, 26
Responding to incidents. See Incident response.
Response, definition, 6
Restricting outbound traffic. See Throttling.
Returning to service, 243–244
Risk, definition, 7. See also TTA (traffic threat assessment).
Risk reduction, 30
Rivest, Ronald, 259
Robots. See Bot nets; IRC bots.
Rose, Curtis, 219, 299
Routing, overriding, 161–163

countermeasures, 8
defensible networks, 9–10
deficiencies, 8
definition, 6
detection, 6
exploits, 8
incident response, 6
incidents, 6
intrusions, 6
minimized networks, 10
monitored networks, 9
network forensics, 6
policies, 220
prevention, 6
principles, 8–10
process description, 6–8
protection, 6
reliability, 8
response, 6
risk, 7
structured threats, 7
threat analysis, 7
threat models, 7
threats, 7
unstructured threats, 7
vulnerability, 8

S
SANCP, 19
Sasser variant worm, 292
Sasser worm, 346
Scanline, 350–352
Scanners, categories of, 343–345
Scope of intrusion, 240–243
Scoping incidents, 11
Secure Shell, 180, 198–199
Security
assessment, 6. See also TTA (traffic threat assessment).
asset value, 8
assets, 7
controlled networks, 9
cost of replacement, 8

countermeasures, 8
defensible networks, 9–10
deficiencies, 8
definition, 6
detection, 6
exploits, 8
incident response, 6
incidents, 6
intrusions, 6
minimized networks, 10
monitored networks, 9
network forensics, 6
policies, 220
prevention, 6
principles, 8–10
process description, 6–8
protection, 6
reliability, 8
response, 6
risk, 7
structured threats, 7
threat analysis, 7
threat models, 7
threats, 7
unstructured threats, 7
vulnerability, 8

security, monitoring. See also Defensible networks, monitoring.
theory
access control devices, 13
alert data, 15
alerts, 11
application relevance, 13–14
audit systems, 13
currency, 9
decision makers, 11
escalation, 11
forms of network data, 13–18
full content data, 13–18
granularity, 13
indicators, 11
scoping incidents, 11
Security, monitoring, *continued*

- **theory, continued**
  - session data, 14
  - statistical data, 14–15
  - techniques, 13–18
  - theory, 10–13
  - warnings, 11
  - zero-day exploits, 10
- **tools**
  - alert data tools, 23
  - analyzers, 18
  - collectors, 18
  - data analysis, 20–21
  - full content data tools, 19
  - probes, 18
  - session data tools, 21–22
  - statistical data tools, 23
- **Server channels, bot nets**, 311–314
- **Service enumeration**, 352–358
- **Services, minimizing**, 68–74
- **Session data. See also TTA (traffic threat assessment).**
  - collecting
    - with Argus, 328–330
    - with Cisco NetFlow, 325–327
    - for incident response, 237–239
  - definition, 14
  - elements of, 179
  - extrusion detection, 91–94
  - limitations, 94
  - malicious parties, 91–92
  - nonstandard protocols, 92
  - odd ports, 92
  - session content, 92–94
  - session duration, 92–94
  - session frequency, 92–94
  - suspicious parties, 91–92
  - tools, 21–22
  - TTA case study, 279–280
  - unauthorized parties, 91–92
- **Session duration, 92–94**
- **Session frequency, 92–94**
- **SHA256, 259–260**
- **Simple Mail Transport Protocol (SMTP), 216**
- **Simple Object Access Protocol (SOAP), 36**
- **Sink holes. See also Layer 3 access control.**
  - alternatives to, 170
  - configuration verification, 151–153
  - configuring, 149–150
  - definition, 141
  - disposing of traffic, 147–148
  - distribution layer summary, 152
  - enterprise, 144–147, 169–170
  - field notes, 169–170
  - internal intrusions, identifying, 153–156
  - ISPs (Internet Service Providers), 141–143
  - uRPF (Unicast Reverse Path Forwarding), 166–169
  - uses for, 170
  - worms (detection), 153–163, 166–169
- **Slammer worm, 177**
- **Smith, Fred Chris, 245**
- **SMTP (Simple Mail Transport Protocol), 216**
- **Sniffing, 71**
- **Snort**
  - adding rules, 339–342
  - data interface tools, 19
  - description, 24
  - installation, Unix, 333–335
  - installation, Windows, 335–338
  - packet alterations, 59
- **SOAP (Simple Object Access Protocol), 36**
- **Sober worm, 215**
- **Spam detection, 85–86**
- **SPAN (Switched Port Analyzer), 106, 116–119**
- **SPAN matrix switches, 123–125**
- **SPAN ports, 106, 116–119**
- **Specialized machines, 321–322**
- **Spitzner, Lance, 103**
- **Spoofed packets, stopping, 163–166**
- **Squid, 51–54**
- **Squid SSL termination reverse proxy, 130–135**
- **Sguil, 19, 182**
Statistical data
  definition, 14–15
  extrusion detection, 94–96
  tools, 23
Streams. See Session data.
Structured threats, 7, 231–232
Sullivan, Tim, 86
Superscan, 350–352
Survivability components, 26
Switched Port Analyzer (SPAN), 106, 116–119
Synchronizing time, 221–227
System ownership, 368

T
  Tablus Content Alarm, 88
  *The Tao of Network Security*..., 114–116
  Taps
    2X1 10/100 Regeneration Tap, 116–119
    2X1 10/100 SPAN Regeneration Tap, 116–119
    10/100 Port Aggregator, 108
    definition, 106–107
    DMZs, 125
    Dual Port Aggregator, 114–116
    Ethernet networks, 116–119
    Link Aggregator Tap, 125
    passive inline, 112
    PCI Port Aggregator, 107–114
    SPAN ports, 116–119
    TCP port scan, 352–353
    Telephones, security, 230
    Telnet, 180
    10/100 Port Aggregator Tap, 108
    Terminating internal intruders, 246
    TFTP (Trivial File Transfer Protocol), 90–91
  Threat analysis, definition, 7. See also TTA (traffic threat assessment).
  Threat models, 7
  Threats, definition, 7
  Three-tier network, 139–140
  Throttling outbound traffic, 40–43, 157–161
  Time synchronization, 221–227
  Tools and utilities
    alert data tools, 23
    analyzers, 18
    Arbor Networks PeakFlow, 96
    Argus
      awk (parsing records with), 286–288
      definition, 279–280
      deploying, 279–280
      full content data, 296–299
      interpreting output, 282–286
      session data, 279–280
    Bro, 24
    BullGuard, 86
    CDPsNiffer, 71
    collecting evidence, 253–258
    collectors, 18
    data analysis, 20–21
    DataSafe, 86
    evidence integrity, 259, 261
    extrusion detection, 87
    extrusion prevention, 86
    full content data tools, 19
    hashing, 259–260, 261
    host profiling, 96
    iController, 88
    iGuard, 88
    Lancope StealthWatch, 96
    Mazu Profiler, 96
    MD5 Message Digest Algorithm, 259
    Md5deep, 261
    network sniffing, 71
    network visualization, 178–179
    Prelude, 24
    probes, 18
    Reconncex, 88
    session data tools, 21–22
    SHA256, 259–260
    Snort
      adding rules, 339–342
      data interface tools, 19
      description, 24
      installation, Unix, 333–335
INDEX

Tools and utilities, continued
Snort, continued
   installation, Windows, 335–338
   packet alterations, 59
Squid, 51–54
Sguil, 19
statistical data tools, 23
Tablus Content Alarm, 88
text processing, 286–288
thief of intellectual property, 86
U.S. Secure Hash Algorithm, 259
Traffic
   mix, per time interval, 96classes, 159–161
   outbound. See Outbound traffic.
   per time interval, 95–96
   policies, 159–161
   scope of normal patterns, 176–177
   threat assessment. See TTA (traffic threat
   assessment).
   undesirable, redirecting. See Sink holes.
   visibility, 30–31
Traffic, accessing
   active participation, 107
   distributed traffic collection, 126–130
   hubs, 106, 123
   inline devices, 107
   matrix switches, 123–125. See also SPAN ports.
   monitoring on the WAP, 107
   packet capture methods, 105–107
   passive participation, 107
   SPAN ports, 106, 116–119. See also Matrix
   switches.
   Squid SSL termination reverse proxy, 130–135
   taps
   2X1 10/100 Regeneration Tap, 116–119
   2X1 10/100 SPAN Regeneration Tap, 116–119
   10/100 Port Aggregator, 108
   definition, 106–107
   DMZs, 125
   Dual Port Aggregator, 114–116
   Ethernet networks, 116–119
   Link Aggregator Tap, 125
   passive inline, 112
   PCI Port Aggregator, 107–114
   SPAN ports, 116–119
   on WLANs, 107
Trends
   converged appliances, 322–323
   specialized machines, 321–322
   Trivial File Transfer Protocol (TFTP), 90–91
TTA (traffic threat assessment)
   batch analysis, 180
   DNS, 213–216
   elements of session data, 179
   gathering data, 181–187
   ICMP, 198
   incident response, 233
   ISAKMP, 197–198
   LDAP, 200–201
   manual inspection, 180
   NADS (network anomaly detection system), 178–179
   network visualization tools, 178–179
   NTP (Network Time Protocol), 196–197
   ports
   22 TCP, Secure Shell, 198–199
   25 TCP, SMTP, 216
   43 TCP, Whois, 199–200
   123 UDP, NTP, 196–197
   389 TCP, LDAP, 200–201
   500 UDP, ISAKMP, 196–197
   3003 to 9126, 201–209
   44444 to 49993, 209–213
   purpose of, 175–179
   scope of traffic patterns, 176–177
   Secure Shell, 180, 198–199
   SMTP (Simple Mail Transport Protocol), 216
   Sguil query components, 182
   suspicious traffic
   active FTP, 188–193
   identifying control and data channels, 188–193
omitting FTP transfers, 194–196
overview, 187–188
passive FTP, 188–193
Telnet, 180
Whois service, 199–200
TTA case study
Argus
awk (parsing records with), 286–288
definition, 279–280
deploying, 279–280
full content data, 296–299
interpreting output, 282–286
session data, 279–280
determining compromise, 289–292
identifying internal victims, 293–296
initial discovery, 279–282
live response data, 299–304
network evidence, 299–304
port 445 TCP traffic, 288–289
2X1 10/100 Regeneration Tap, 116–119
2X1 10/100 SPAN Regeneration Tap, 116–119

U
UCSD (University of California, San Diego), 11
UDP port scan, 353–354
Unstructured threats, 7, 232
uRPF (Unicast Reverse Path Forwarding), 163–169
U.S. Secure Hash Algorithm, 259

V
Verdasys, 87
Vericept, 88
Verifying operations, 243–244
Vidius, 87
Visibility, collecting evidence, 253
Vladimirov, Andrew, 18
Voice mail, secure communication, 230
Vulnerabilities
assessing, 233
definition, 8
detecting. See Enumeration.
identifying and removing, 243
incident response, 243

W
WAP, monitoring, 107
Warnings, definition, 11
Web bots. See Bot nets; IRC bots.
Whois, 199–200
Wi-Foo: The Secrets of Wireless Hacking, 18
Windows enumeration, 365–367
Winfingerprint, 365–367
WLANs, accessing traffic, 107
Working evidence copies, 262
WormRide, 315
Worms
Blaster, 17
Sasser, 346
Sasser variant, 292
sink holes, 153–163, 166–169
Slammer, 177
Sober, 215
Zotob, 89, 91

X
Xprobe2, 359–361

Z
Zero-day exploits, 10
Zotob worm, 89, 91