INDEX

access control, 126
Advanced Persistent Threats (APTs), 81–82, 195–211
amplification attacks, 78–79
anycast DNS addressing, 113–118
  benefits, 114
caveats, 116
  configuration, 117–118
ANY queries, 75–76, 78, 143
authoritative poisoning attacks, 71–73, 169–186
  attack detection, 172–174
  attack forms, 170–172
defense mechanisms, 174–177
bogus query attacks, 65–66, 141
  mitigation approaches, 147–148
botnets, 2, 195–202
cache poisoning attacks
  attack forms, 69–72, 154–159
defense mechanisms, 160–167
detection, 159–160
DANE, 230–232
data exfiltration, 79–81, 188
DDoS, 65, 139–146
disaster risks
  defenses, 214
  DNS, 89–93, 98–102
DMZ, 89–93, 98–102
DNS
  domain hierarchy, 18–19
  hints file, 26
  Internationalized Domain Names (IDN), see IDNA
  localhost resolution, 27
  resolver configuration, 27–29
  zones and domains, 23–25
DNS block listing, 237
DNS classes, 41
DNS cookies, 146, 167
DNSCrypt, 168
DNS data sources, 4–6, 58, 60–61
DNS data sources and flows, 4
DNS deployment
  high availability, 86, 118
  lab deployment, 119
  sizing and scalability, 118–119
  vendor diversity, 118
DNS double flux, 202
DNS extensions (EDNS0), 44–48
DNS external service providers, 97–98, 171–172
DNS fast flux, 199
DNS firewall, 207–210
DNS fluxing, 198–202
DNS forwarding server, 21–23
DNS header opcode, 37
DNS hosting providers, 97, 171–172
DNS information trust model, 5–6, 49, 59–60
DNS load balancers, 119
DNS message format, 28
  additional section, 42
  answer section, 38, 42
  authority section, 42

© 2017 by The Institute of Electrical and Electronic Engineers, Inc. Published 2017 by John Wiley & Sons, Inc.

299
INDEX

DNS message format (Continued)
header, 35–38
labels, 31–32
question section, 38, 41
response codes, 38–40
DNS name resolution, 3, 18–23, 48–55
DNS QTYPEs, 41, 285–289
DNS rebinding attack, 77
DNS risks, 61–83
DNS role-specific defenses, 220–222
DNSSEC, 161–167, 176–186
algorithm rollover, 182–183
delegation signer, 171, 178, 180
digital signatures, 161–163
DNS root zone trust anchor, 163–165
hardware security modules, 183
key rollover, 179–183
key security, 183–185
key signing key (KSK), 171, 178–185
overview, 161–164
resolution process, 177–179
zone signing, 179
zone signing key (ZSK), 178–185
DNS security extensions, see DNSSEC
DNS security strategy, 213–228
DNS server hardening, 134–136
DNS service availability risks, 62
DNS service denial attacks, 63–67, 139–151
detection, 144–145
protection, 145–151
DNS trust sectors
external, 89, 91–98
extranet, 89, 98–99
internal, 90, 103–110
recursive, 90, 99–103
DNS trust zones, see DNS trust sectors
DNS tunneling attacks, 79–81
detection, 190–193
mitigation approaches, 193–194
DNS Update, 43–45
operations, 43
prerequisites, 43–45
DNS vulnerability mitigation summary, 214–219
Domain-based Message Authentication, Reporting and Conformance (DMARC), 245–246
domain generation algorithms (DGAs), 202
domain keys identified mail (DKIM), 242–244
domain name encoding, 31–35
domain registries, 170–171
EDNS0 options, 45–48
extended label types, 45
external DNS servers, 89, 91, 97
external namespace, 6, 89, 91, 97
external trust sector configuration
ISC BIND, 94
Knot DNS, 96–97
NLnet, 94–95
PowerDNS, 95–96
hardware/OS attacks, 63
hidden master DNS server, 89–93, 98–99, 104–105
human error risks
defense, 124, 220
hybrid authoritative/caching DNS servers, 111
ID guessing attack, 155
IDNA, 34
incident response, 131–134
information protection, 129
internal namespace, 6, 90, 98, 100, 104, 109–110
internal trust sector configuration
ISC BIND, 105–106
Knot DNS, 108
NLnet NSD, 106–107
PowerDNS, 107–108
Kaminsky attack, 71, 156–159
Kaminsky, Dan, 156
Kashpureff attack, 155–156
malware
detection, 202–206
extrication, 206–210
fast flux detection, 203–205
malware examples, 198
malware proliferation, 196–198
malware use of DNS, 62, 65, 74, 80–82, 198–203
man-in-the-middle attack, 74, 154–155, 163
Mirai malware, 65, 196–198
multi-tiered authoritative configurations, 109–110
name compression, 32
network reconnaissance attacks, 75–76, 129, 187–188
detection, 189
mitigation approaches, 193
NIST Cybersecurity Framework, 7
framework core, 7
framework implementation steps, 9
framework implementation tiers, 8
framework profile, 8
target profile and security planning, 13
passive DNS, 204–206
pseudorandom subdomain (PRSD) attacks, 67, 141–142
mitigation approaches, 148
public key infrastructure, 230–231
quagga, 117–118
query name case randomization, 161
recovery planning, 133
recursive DNS server, 3, 20
recursive trust sector configuration
ISC BIND, 102–103
Knot DNS, 103
NLnet Unbound, 103
PowerDNS, 103
reflector attacks, 78–79, 143–144
mitigation, 148–151
resolution data at rest, 127, 169–170
resolv.conf, 28–29
resolver, stub, 3, 27–29, 73–74
resolver redirection attacks, 73–75
resource record set (RRset), 23
resource record types
CERT-Certificate, 248
dHCID-Dynamic host config. ID, 246–247
IPSECKEY-IPSec public key, 248–249
KEY-Key, 249
KX-Key exchange, 250
MX-Mail exchange, 233–237
OPT-EDNS0 options, 45
SIG-Signature, 250
SSHFP-Secure shell fingerprint, 250–251
TA-Trust authority, 247
response policy zones, see DNS firewall
response rate limiting, 149–151
risk assessment, 11–13, 124–126
root DNS servers
internal, 90, 111–113
Sender Policy Framework (SPF), 238–242
macros, 241–242
mechanisms, 238–240
modifiers, 240–241
server hardware controls, 122–128
simple mail transfer protocol, 232–236
Smurf attack, 78
SOA mname field, 92, 104
stealth slave DNS servers, 111
stub resolver, see resolver, stub
tiered caching servers, 100–101
top level domain (TLD), 6, 18–22, 50–52, 54–55, 60–61, 97, 171, 202
UDP port randomization, 160–161
US-CERT, 125, 218
zone transfers, 25–26