Index

A
ACLs (Access Control Lists), 34
admin prohibited error, 60
AIDE (Advanced Intrusion Detection Environment), 13
amplification, 39
MITM attacks, 66
Apache, LMD integration, 96–97
ARP (Address Resolution Protocol),
Nping and, 53
attacks
Digital Attack Map tool, 45–46
Estonian DDoS attacks, 45–46
hardening and, 65–67
mapping, 45–46
MITM (man-in-the-middle), 66
password cracking, 106
wordlists, 106–107
phishing, 113
Ping of Death, 66
reflection, 38–40
SNMP, 41
reporting, 40–41
smurf, 66
SQLi, 113–114
launching, 118–120
auth category (NSE), 74
authentication, NSE, 77–78

B
BPC 38 (Best Current Practice 38), 43
broadcast category (NSE), 74
brute category (NSE), 74

C
CAPT (captured packet entries), 57
chaining commands in ncat, 30–31
CIDR (Classless Inter-DINameX1 Routing), 51
--clean command, 93–94
CLI (Command Line Interface), running LMD, 92
clone command, 117–118
cmd_timeout, 6
CMS (Content Management System), 115
commands
chaining, 30–31
--clean, 93–94
curse, 117–118
conptrack, 8
hashcat, 108–109
iptables, 61–63
--kill, 96
knock, 7
md5sum, 14
communications, netcat, 31–33
conptrack command, 8
cron job, LMD, 96
cryptography
hashes, 101–102
keyspace, 100–101
cudaHashcat, 110

D
DDoS (Distributed Denial of Service)
attacks, 37
Estonia, 44–45
Debian Jessie, config file, 3
default category (NSE), 74
Digital Attack Map tool, 45–46
discovery category (NSE), 74, 78–79
DNS (DoNameX1 Name System), 37
resolvers, 42–43
dos category (NSE), 74
DRARP (Dynamic RARP), 53
DROP response, 2

E
Echo mode, Nping, 54–57
Estonian DDoS attacks, 44–45
executables, netcat, 33–34
exploit category (NSE), 74
external category (NSE), 74
I

In file transfer, netcat, 29–30
filesystems
  knockd, 4
  LMD monitoring, 88
  security, 13
filters, Netfilter, 2
flushing iptables rules, 65
fuzzer category (NSE), 74

G

GitHub, clone command, 117–118
GUIs (graphical user interfaces),
  NSE, 81

H

hardening, ICMP broadcasts and, 65
Hashcat, 99
  attack modes, 109
  brute force attacks, 110
  capabilities, 103
  cudaHashcat, 110
  hashes, 101–103
    identifying, 104–105
  installation, 103–104
  oclHashcat, 110–111
  running, 107–110
  Shadow passwords, 104
hashcat command, 108–109
Hashcat-utils, 111
hashes, 101–103
  algorithms, 105
host scripts (NSE), 80
  host-based intrusion detection, 13

I

ICMP
  codes, 61
  iptables and, 61–63
  misconceptions, 59
  Nping and, 52–53
  Ping of Death, 66
ICMP Port Unreachable, 2
icmp_echo_ignore_broadcasts, 65
inbound connections, logging, 64–65
inotify-tools, 89
intrusive category (NSE), 75
invisibility of server, 7–8

iptables, 2
  flushing rules, 65
  iptables command, 61–63
  iptables-persistent package, 9
  rules, 9–10
  testing, 8–9

K

keyspace, 100–101
--kill command, 96
knock command, 7
knockd
  configuration, 5–6
  default settings, 3–4
  filesystems, location, 4
  installation, 2–4
    testing, 6–7
  network interface, default, 5
  packages, 3
  packets, 5–6
  starting, 5
  KoD (Kiss-o’-Death) packet, 38

--limit-burst option, 66
LMD (Linux Malware Detect), 85
  Apache, integration, 96–97
  --clean command, 93–94
  CLI options, 92
  cron job, 96
  definition updates, 85
  exclusions, 91–92
  features, 86–88
  filesystem monitoring, 88
  inotify-tools, 89
  installation, 88–90
  --kill command, 96
  maldet, 92
  Malware Hash Registry, 86
  monitoring, modes, 90–91
  quarantining, 93–94
  reporting, 92–93, 96
  scans, 94
    manual, 95
    stopping, 94–96
  threats, prevalent, 86–87
  updates, 94
  logging, inbound connections, 64–65
  --log-prefix option, 62–63
M
maldet, 92
malware. See also LMD (Linux Malware Detect)
malware category (NSE), 75
Malware Hash Registry, 86
mapping attacks, 45–46
md5deep, 16–17
md5sum command, 14
MD5sums, 14–16
MD5SUMS file, 14–15
MITM (man-in-the-middle) attacks, smurf attacks, 66
MTU (Maximum Transmission Unit), 59

N
NAT (Network Address Translation), 54–57
ncat, 26
command chaining, 30–31
installation packages, 27–29
ncat, 25, 27
ACLs (Access Control Lists), 34
communications, security, 31–33
executables, 33–34
file transfer, 29–30
options, 34–35
netcato, 27
netcat-openbsd, 27
netcat-traditional, 27
Netfilter, 2
Nmap, 1, 27–28
  Debian installation, 69
  port scanning, 69–71
  Red Hat installation, 69
nmap, 27
Nmap Project, 25
Nping, 49–50
ARP and, 53
  --debug, 58
  --delay 10, 57
Echo mode, 54–57
  --hide-sent, 57
ICMP and, 52–53
payload and, 53–54
  --rate 3, 57
TCP and, 50–51
  interpreting, 51
UDP and, 52
NSE (Nmap Scripting Engine), 71–73
  authentication checks, 77–78
  criteria, 75
  discovery, 78–79
GUIs, 81
regex (regular expressions), 80–81
scripts
  categorizing, 74–75
  host, 80
  postrule, 80
  prerule, 80
  service, 80
  updating, 79–80
security problems, 75–77
timing templates, 73
Zenmap, 81–82
NTP (Network Time Protocol), 37
OpenAccess servers, 37–38
reflection attacks, 38–40
RestrictedAccess servers, 37–38
O
oclHashcat, 110–111
Open Source Tripwire, 13
OpenAccess servers, 37–38
P
packages
  iptables-persistent, 9
  knockd, 3
packets, knockd, 5–6
password cracking, 99
attacks
  Hashcat numbers, 109
  mode, 106
  wordlists, 106–107
  hashes, 101–103
passwords, 99
  keystpace, 100–101
  security increase, 100
  Shadow passwords, 102–103
payload options, Nping and, 53–54
PDO (PHP Data Objects), 117
phishing attacks, 113
PHP, SQLi mitigation, 115–117
Ping of Death, 66
ping rules
  allowing to IP address, 64
  inbound, 64
  outbound, 64
port knocking, 1
  clients, 7
  security considerations, 10–11
sequences, 11–12
smartphone clients, 10
troubleshooting, 10
port mapping, 70
port scanners
  confusing, 2
  Nmap, 69–71
ports
  Nmap, 1
  probing, 1
postrule scripts (NSE), 80
prerule scripts (NSE), 80
probing ports, 1

Q
quarantine, LMD and, 93–94

R
rainbow tables, 107
RARP (Reverse ARP), 53
  DRARP (Dynamic RARP), 53
reflection attacks
  NTP, 38–40
  SNMP, preventing, 41
regex (regular expressions), NSE, 80–81
REJECT request, 2
reject-with tcp-reset, 2
reporting
  attacks, 40–41
  LMD and, 92–93, 96
RestrictedAccess servers, 37–38
Rootkit Hunter, 13, 17
  configuration, 19–21
  Debian and, 18
  design, 22–23
  false positives, 21–22
  Red Hat and, 18
rootkits, 13, 17
Round Trip Times, 56
RPM Package Managers, Red Hat and, 69
rsyslog, 62–63
rtt, 56

S
safe category (NSE), 75
SCANID, 92–93
scripting. See also NSE (Nmap Scripting Engine)
SCTP (Stream Control Transmission Protocol), 34–35
security, DDoS attacks, 37
sequences, port knocking, 11–12
servers, invisibility, 7–8
  iptable testing, 8–9
  iptables rules, 9–10
service scripts (NSE), 80
Shadow passwords, 102
  Hashcat, 104
Shadow Suite, 102–103
smartphones, port knocking, 10
smurf attacks, 66
SNMP (Simple Network Management Protocol), 40
  reflection attacks, preventing, 41
SQLi (SQL injection), 113, 114–115
attacks, launching, 118–120
mitigating, in PHP, 115–117
testing, 120–121
sqlmap, installation, 117–118
syslog, config file, creating, 63
syslog server, rsyslog, 62–63

T
TCP (Transmission Control Protocol), Nping and, 50–51
TCP RST packets, 1
tcpdump, 60–63
tcpflags, 5–6
templates, timing templates, 73
testing, SQLi, 120–121
timing templates, 73
Tripwire. See Open Source Tripwire
troubleshooting, port knocking, 10

U-V
UDP (User Datagram Protocol), Nping and, 52
utilities, Hashcat-utils, 111
version category (NSE), 75
vuln category (NSE), 75

W-Z
Web Scan Test, 120–121
wordlist attacks, 106–107
XOP (eXtended OPerations), 107–108
Zenmap, 81–82