

Learn the secrets of protecting your network with
the world's most popular security program!

James "Professor" Messer

SECRETS OF NETWORK CARTOGRAPHY:

A Comprehensive Guide to Nmap

A  Professor Messer Publication

Secrets of Network Cartography: A Comprehensive Guide to Nmap

Second Edition, Revision 2

James "Professor" Messer

James@ProfessorMesser.com



A Professor Messer Publication

<http://www.ProfessorMesser.com>

Secrets of Network Cartography: A Comprehensive Guide to Nmap

Published by
Professor Messer, LLC
2910 Kerry Forest Parkway, #D4-230
Tallahassee, Florida 32309
<http://www.ProfessorMesser.com/>

Second Edition, Revision 2, March 2007

Copyright ©2007 by Professor Messer, LLC, Tallahassee, Florida

License Information for Ebook Version

GRANT OF LICENSE. You may use this Electronic Book with Acrobat Reader on any devices supported by that Reader or any other software capable of reading the Adobe Portable Document Format ("PDF"). You may not:

- 1) copy, install or use the Electronic Book except as permitted in this Agreement;
- 2) rent, lease, sublicense, assign or transfer your rights in the Electronic Book, or authorize all or any portion of the Electronic Book to be copied onto another user's computer except as may be expressly permitted herein. You may, however, transfer all your rights to use the Electronic Book to another person or legal entity provided that you transfer this Agreement, all copies of the software in all formats and all documentation to such person or entity and that you retain no copies, including copies stored on a computer, images stored in any application files, or stored on a backup device. All your rights under this license will then cease.
- 3) adapt or translate the Electronic Book;
- 4) extract all or any portion of the contents of the Electronic Book for use in any document or material for any purpose;
- 5) install all or any portions of the Electronic Book on any computer system on a public or private network where the contents of the Electronic Book might be accessible by individuals who are not licensed users of the Electronic Book;
- 6) export the Electronic Book in a manner contrary to U.S. export or administration laws or regulations.

PORTABLE OR HOME COMPUTER USE. The primary user of the computer on which the Electronic Book is installed may make a second copy of the Electronic Book for his or her exclusive use on either a portable Computer or a desktop Computer located at his or her home, provided the Electronic Book on the portable or home Computer is not used at the same time as the Electronic Book on the primary computer.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher and the author are not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Website is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Website may provide or recommendations it may make. Further, readers should be aware that Internet Websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products or service, or to obtain technical support, please contact Customer Care at <http://www.ProfessorMesser.com/helpdesk/>

Trademarks: Nmap is a registered trademark of Insecure.org, LLC. Linux is a registered trademark of Linus Torvalds. All other trademarks are the property of their respective owners.

Cover Photography: James Messer
Cover Design: John Henry, <http://www.studiojohnhenry.com/>

About the Author

James “Professor” Messer (James@ProfessorMesser.com) is the founder of ProfessorMesser.com and NetworkUptime.com, online resources for network and security professionals. His twenty years of experience in the computer and networking industry have taken him from liquid nitrogen-cooled supercomputers to enterprise network analysis and security solutions. He also maintains the comp.dcom.lans.ethernet and comp.dcom.lans.token-ring Frequently Asked Questions (FAQ) files.

James holds a Bachelor’s degree in Business Management from Florida State University, and his technology interests revolve around security, networking, and electronic privacy. James resides in Tallahassee, Florida, with his wife and three children.

To my wife, Judy, my daughter Katie, and my sons Ethan and Trey.

Table of Contents

INTRODUCTION.....	V
About This Book	vi
How This Book is Organized.....	vi
Conventions Used in This Book	ix
CHAPTER 1: THE BASICS	1
What is Nmap?	1
Windows Operating Systems and Nmap	2
Is Nmap Good or Evil?	3
Internet Protocol.....	5
Transmission Control Protocol (TCP)	6
User Datagram Protocol (UDP).....	8
Internet Control Message Protocol (ICMP).....	9
The Basics of Nmap.....	10
CHAPTER 2: SCANNING THE NETWORK	23
Nmap Scan Summary.....	24
TCP SYN Scan (-sS).....	25
TCP connect() Scan (-sT)	29
Stealth Scanning – The FIN Scan (-sF), Xmas Tree Scan (-sX), and Null Scan (-sN)	33
Ping Scan (-sP)	40
UDP Scan (-sU).....	43
IP Protocol Scan (-sO)	46
ACK Scan (-sA)	49
Window Scan (-sW)	52
RPC Scan (-sR)	55
List Scan (-sL)	58
Idlescan (-sI <zombie host:[probeport]>)	60
FTP Bounce Attack (-b <ftp_relay_host>).....	90
CHAPTER 3: THE SEARCH FOR HOSTS: NMAP'S PING OPTIONS.....	95
The Nmap Ping	95
ARP Ping (-PR)	96
ICMP Echo Request and TCP ACK Ping (-PB)	98
ICMP Echo Request Ping (-PE, -PI).....	100
TCP ACK Ping (-PA [portlist], -PT [portlist]).....	102
TCP SYN Ping (-PS [portlist]).....	106
UDP Ping (-PU [portlist]).....	109
ICMP Timestamp Ping (-PP)	111
ICMP Address Mask Ping (-PM).....	114
Don't Ping Before Scanning (-P0, -PN, -PD).....	117
Require Reverse DNS (-R).....	118
Disable Reverse DNS (-n)	120
Specify DNS Servers (--dns-servers).....	122
Use Non-Parallel DNS Lookups (--system-dns).....	124

CHAPTER 4: RECON SCANNING.....	125
Operating System Fingerprinting.....	125
Version Detection (-sV).....	141
Define IP Options Flags (--ip-options <option>).....	147
CHAPTER 5: HOST AND PORT OPTIONS	151
Exclude Targets (--exclude <host1 [,host2] [,host3]...>).....	151
Exclude Targets in File (--excludefile <exclude_file>).....	152
Read Targets from File (-iL <inputfilename>).....	152
No Random Ports (-r).....	153
Source Port (--source-port <portnumber>, -g <portnumber>).....	154
Specify Protocol or Port Numbers (-p <port_range>).....	154
Fast Scan Mode (-F).....	155
Interface (-e <interface>).....	155
List Interfaces (--iflist).....	156
Force Ethernet Frames (--send-eth).....	157
Force IP Frames (--send-ip).....	157
CHAPTER 6: RECORDING THE RESULTS: NMAP'S OUTPUT OPTIONS	159
Normal Format (-oN <logfilename>).....	159
XML Format (-oX <logfilename>).....	160
Script Kiddie Format (-oS <logfilename>).....	165
HTML Format (-oH).....	166
Resume Scan (--resume <logfilename>).....	166
Append Output (--append-output).....	167
Log Errors (--log-errors).....	167
Show Only Open Ports (--open).....	167
CHAPTER 7: INSTANT VISIBILITY: REAL-TIME INFORMATION.....	169
Verbose Mode (--verbose, -v).....	169
Version Trace (--version-trace).....	171
Packet Trace (--packet-trace).....	172
Debug Mode (--debug, -d).....	173
Interactive Mode (--interactive).....	175
Noninteractive Mode (--noninteractive).....	176
Run-Time Interactions.....	177
CHAPTER 8: NINJA SCANNING: TECHNIQUES FOR NETWORK INVISIBILITY	181
Ninja Scanning Techniques.....	181
Ninja Pinging.....	182
Ninja DNS Settings	183
Ninja Timing Options.....	183
Staying Invisible with Randomization.....	192
Ninja Decoys.....	194
Other Ninja Techniques.....	200

CHAPTER 9: WINDOWS AND NMAP	207
Choosing between Linux and Windows	207
WinPcap and Raw Socket Options	208
The History of Windows and Nmap	208
Operational Issues in Windows	209
The Downsides in Windows	210
Scanning localhost in Windows	210
CHAPTER 10: MISCELLANEOUS OPTIONS	213
Quick Reference Screen (--help, -h)	213
Nmap Version (--version, -v)	215
Data Directory (--datadir <directory_name>)	215
Quash Argument Vector (-q)	216
Define Custom Scan Flags (--scanflags <flagval>)	216
(Uriel) Maimon Scan (-sm)	217
IPv6 Support (-6)	218
Send Bad TCP or UDP Checksum (--badsum)	218
Force Privileged Mode (--privileged)	219
Force Unprivileged Mode (--unprivileged)	219
Release Accessible Memory (--release-memory)	219
Digital Salutations (--thc)	220
CHAPTER 11: USING NMAP IN THE "REAL WORLD"	221
Identifying the Remnants of a Virus Outbreak or Spyware Infestation	222
Vulnerability Assessments	224
Security Policy Compliance Testing	226
Asset Management	228
Firewall Auditing	230
Perpetual Network Auditing	232

Introduction

Networks are the Wild West of the modern age, and the network population is much like that of a frontier town. There's the usual local townsfolk who keep their head down and work amongst themselves, the occasional drifters who come into town and then disappear into the sunset, and there's always at least one black-hat-wearing bad guy who shows up to rob the bank, shoot-up the saloon, or cause a ruckus.

And then, there's the Sheriff. That's you.

In today's modern network, the Sheriff needs more than a pair of spurs and a six-shooter. Today's network professional requires an eclectic mix of network analyzers, security tools, and multi-functional gadgets. As with the Wild West, the Sheriff must always stay one step ahead of the bad guys.

Nmap is used every day by thousands of network professionals to keep their networks and systems secure. Nmap's documentation describes itself as a "network exploration tool and security scanner," and it has excelled at these complex capabilities. Nmap tracks down the Wild West town's citizens, identifies each person, and checks them over for potential security gaps. All of these scans are configured, launched, and recorded using Nmap's built-in capabilities. With Nmap, the Wild West's network becomes a safer and more comfortable place to live.

Nmap is an extremely powerful tool, and one of the most popular security utilities in the open source community. It's written and maintained by "Fyodor" from his web site at:



<http://insecure.org/>

The Nmap web page is a highly recommended read for its wealth of great security information.

About This Book

When I started writing this book, I thought it would be a quick twenty-page tutorial on how to use the most basic Nmap functions. As I began writing, I found Nmap's feature-rich functionality to be overwhelming. My two-week writing plans turned into months of Nmap network scans, megabytes of protocol decodes, and a complete immersion in Nmap's source code. This book is the culmination of years of work and research, and this updated edition contains details that I've discovered through hundreds of Nmap scans and conversations with the Nmap user community.

This book was written from the perspective of the security team, because it's the security team that is managing some of the largest technological responsibilities that our industry has ever experienced. As the first line of this book affirms, our networks really are a Wild West. The security group is always scrambling for new methods to combat these constantly increasing and evolving threats.

Nmap is a tool that has been available to network security professionals for years, but it's surprising how many haven't taken advantage of the most basic Nmap functions. It's my hope that this book will allow security teams to learn more about this incredibly powerful program and help them ultimately become better network security professionals.

This latest edition of this Nmap book focuses on the real-world aspects of Nmap. If the first rule of war is to understand your enemy, then this e-book will be a useful guide to fighting the good fight on the front lines of network security.

How This Book is Organized

This book consists of eleven chapters, with each chapter designed as a stand-alone set of related topics. If you are already familiar with the basic Nmap scans but you need more information about timing and tuning options, you can skip ahead without missing too much.

Professor Messer also offers the Nmap video training course "Nmap Secrets." This companion course enhances the material found in this book with live video tutorials of Nmap installations, live scanning techniques, and video feedback and cues that show you exactly what to expect from Nmap. If you've purchased this written book and you've not yet seen the videos, you're missing some examples that will bring the material in this book to life! You can learn more about "Nmap Secrets" at:



<http://www.NmapSecrets.com>

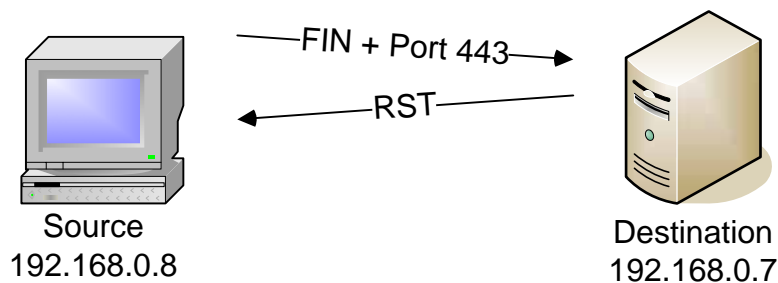
FIN, Xmas Tree, and Null Scan Operation

In the following examples, the graphical descriptions and trace files for the open and closed ports will look functionally identical, except that the bits in the TCP flags will be different in each scan type.

The FIN Scan (-sF)

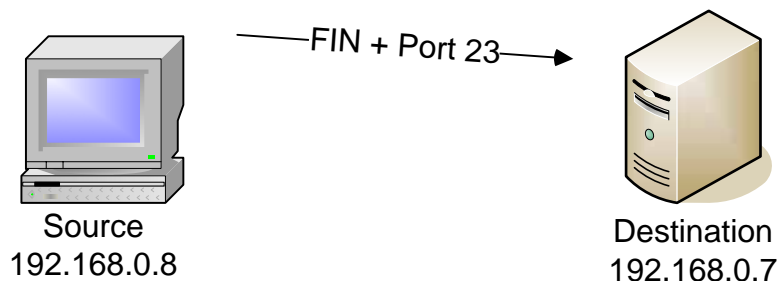
The FIN scan's "stealth" frames are unusual because they are sent to a device without first going through the normal TCP handshaking. If a TCP session isn't active, the session certainly can't be formally closed!

In this FIN scan, TCP port 443 is closed so the remote station sends a RST frame response to the FIN packet:



Source	Destination	Summary
[192.168.0.8]	[192.168.0.7]	TCP: D=443 S=62178 FIN SEQ=3532094343 LEN=0 WIN=2048
[192.168.0.7]	[192.168.0.8]	TCP: D=62178 S=443 RST ACK=3532094343 WIN=0

If a port is open on a remote device, no response is received to the FIN scan:



Source	Destination	Summary
[192.168.0.8]	[192.168.0.7]	TCP: D=23 S=62178 FIN SEQ=3532094343 LEN=0 WIN=2048

Chapter 3: The Search for Hosts: Nmap's Ping Options

Understanding Nmap's myriad scan types is only the beginning of harnessing its power. Nmap's additional options provide over fifty different choices of packet timings, ping options, output formats, and other customizable features! Although this considerable quantity of options seems overwhelming, it's this abundance of choices that provides Nmap with incredible flexibility in nearly any networking environment.

The Nmap Ping

Nmap always "pings" a remote station before initiating the scanning process. If the destination IP address is on the local subnet, Nmap sends an ARP request to verify availability. The default Nmap ping to a host on an external subnet consists of an ICMP echo request followed by a TCP ACK on port 80. If a station does not respond to either ping method, Nmap will continue to the next target. If the scan does not have any additional targets, the scan will end.

Networking purists consider the term "ping" as a reference to an ICMP echo request and the corresponding ICMP echo reply. However, Nmap's use of the word "ping" is more generic. In the Nmap world, a ping is any request that would prompt a remote station's response. Throughout this text, a ping will refer to Nmap's more relaxed definition.

The purpose of an Nmap ping is to provoke any kind of response from a remote station. Once a response is received from a remote device, Nmap identifies that device as active on the network and begins scanning it for detailed port information. Most of these ping options can be combined together to maximize the possibility of locating a device through firewalls or packet filters.

Nmap's pings can also be customized for the situation. For example, a firewall that blocks ICMP and ACK on port 80 might allow Nmap to ping through the firewall with a TCP SYN to port 135 or a UDP query to port 22. This customization could also be used as a filter that would only identify devices that fit certain profiles, such as routers or mail servers.

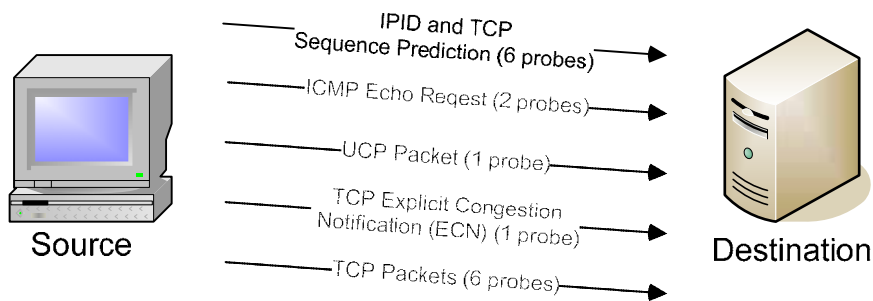
IPID and TCP Sequence Prediction Process

The first step of Nmap's operating system fingerprinting process begins with the IPID and TCP sequence prediction process. These six probes consist of TCP SYN frames, and look relatively normal when examined in a trace file.



The operating system fingerprinting process takes place in a different order than what's shown in the structure of the `nmap-os-db` fingerprint.

Remember, at this point Nmap has already completed a full port scan of the destination device. The operating system fingerprinting uses both open and closed ports to perform its testing.



Source	Destination	Summary
[192.168.0.5]	[192.168.0.9]	TCP: D=68 S=55117 SYN SEQ=1189513814 LEN=0 WIN=1
[192.168.0.9]	[192.168.0.5]	TCP: D=55117 S=68 SYN ACK=1189513815 SEQ=377390828 LEN=0
[192.168.0.5]	[192.168.0.9]	TCP: D=68 S=55117 RST ACK=0 SEQ=1189513815 LEN=0 WIN<<10=0
[192.168.0.5]	[192.168.0.9]	TCP: D=68 S=55118 SYN SEQ=1189513815 LEN=0 WIN=63
[192.168.0.9]	[192.168.0.5]	TCP: D=55118 S=68 SYN ACK=1189513816 SEQ=373392356 LEN=0
[192.168.0.5]	[192.168.0.9]	TCP: D=68 S=55118 RST ACK=0 SEQ=1189513816 LEN=0 WIN<<0=0
[192.168.0.5]	[192.168.0.9]	TCP: D=68 S=55119 SYN SEQ=1189513816 LEN=0 WIN=4
[192.168.0.9]	[192.168.0.5]	TCP: D=55119 S=68 SYN ACK=1189513817 SEQ=368399242 LEN=0
[192.168.0.5]	[192.168.0.9]	TCP: D=68 S=55119 RST ACK=0 SEQ=1189513817 LEN=0 WIN<<5=0
[192.168.0.5]	[192.168.0.9]	TCP: D=68 S=55120 SYN SEQ=1189513817 LEN=0 WIN=4
[192.168.0.9]	[192.168.0.5]	TCP: D=55120 S=68 SYN ACK=1189513818 SEQ=376262396 LEN=0
[192.168.0.5]	[192.168.0.9]	TCP: D=68 S=55120 RST ACK=0 SEQ=1189513818 LEN=0 WIN<<10=0
[192.168.0.5]	[192.168.0.9]	TCP: D=68 S=55121 SYN SEQ=1189513818 LEN=0 WIN=16
[192.168.0.9]	[192.168.0.5]	TCP: D=55121 S=68 SYN ACK=1189513819 SEQ=365535022 LEN=0
[192.168.0.5]	[192.168.0.9]	TCP: D=68 S=55121 RST ACK=0 SEQ=1189513819 LEN=0 WIN<<10=0
[192.168.0.5]	[192.168.0.9]	TCP: D=68 S=55122 SYN SEQ=1189513819 LEN=0 WIN=512
[192.168.0.9]	[192.168.0.5]	TCP: D=55122 S=68 SYN ACK=1189513820 SEQ=365856207 LEN=0
[192.168.0.5]	[192.168.0.9]	TCP: D=68 S=55122 RST ACK=0 SEQ=1189513820 LEN=0 WIN=0

Identifying the Remnants of a Virus Outbreak or Spyware Infestation

Viruses and spyware have different underlying technologies, but they have a common bond once they infest a system. Variants of MyDoom, Sasser, Beagle, NetBus, SubSeven, and other Trojan horses create open ports, providing backdoor communication conduits into infected systems.

This scan will show how the entire network can be easily scanned to locate a single spyware or virus remnant. This search will make use of unique ping methods, port searches, and reverse DNS lookup settings.

Identifying Virus, Spyware, and Trojan Horse Remnants

- **Nmap Ping type:** If ICMP is unfiltered in an organization's network, an ICMP ping (`-PE`) would be an efficient way of identifying an active system. If ICMP is actively filtered, a more applicable ping type should be considered. Since this scan will be working through a large number of IP addresses, an Nmap ping will be an important method of determining a remote device's availability. Disabling Nmap's ping option (`-P0`) should be used only as a last resort in a scan with a large number of IP addresses.
- **Nmap Scan Type:** Since this is a simple port availability test, a TCP SYN scan (`-sS`) or a UDP scan (`-sU`) would be an effective scan type. Different spyware remnants can open TCP ports or UDP ports, and occasionally both types will need to be specified. This example will assume that both types will be scanned.
- **IP Addresses:** The IP addresses for these types of scans will usually be a range of addresses, using Nmap's wildcards and naming conventions. For ease of use, these IP addresses should be listed in a file that can be included with the `-iL` option.
- **Port Ranges:** This particular scan will only need to scan a few ports from each device that are associated with a specific spyware infestation. If both TCP and UDP scan types are specified, then the `-p` option should include `U:<udpports>,T:<tcpports>`.

Index

6

-6, 218

A

-A, 139, 144
ACK scan, 49
additional, advanced, and aggressive, 139
address spoofing, 198
all output formats, 165
--allports, 145
append output, 167
--append-output, 167
ARP ping, 96
asset management, 228

B

-b, 90
bad checksum, 218
--badsum, 218
Bugtraq, 90

C

class, 129
Classless Inter-Domain Routing, 12
compliance testing, 226
custom scan flags, 216

D

-d, 173
-D, 195
--datadir, 215
--data-length, 205
--debug, 173
decoys, 195
delay, 189
disable reverse DNS, 120
--dns-servers, 122
don't ping, 117
don't exclude ports, 145

E

-e, 155
--exclude, 151
exclude targets, 151
--excludefile, 152

explicit congestion notification, 134

F

-f, 202
-F, 155
fast scan mode, 155
-ff, 202
FIN scan, 34
fingerprint, 128
firewall auditing, 230
force ethernet frames, 157
force IP frames, 157
force privileged mode, 219
force unprivileged mode, 219
fragmented IP packets, 202
FTP bounce attack, 90
ftpd, 93
--fuzzy, 138
Fyodor, v, 18, 89, 126, 139, 165

G

-g, 154
grep, 164
grepable format, 164

H

--help, 213
Hobbit, 90
--host-timeout, 184
HTML, 160
HTML format, 166

I

ICMP. See Internet Control Message Protocol
ICMP address mask ping, 114
ICMP echo request, 100, 132
ICMP timestamp ping, 111
idlescan, 60
--iflist, 156
-iL, 152
inetd.conf, 93
--initial-rtt-timeout, 186
Institute of Electrical and Electronics Engineers, 15
--interactive, 175
interface, 155
Internet Assigned Numbers Authority (IANA), 7, 21
Internet Control Message Protocol, 9
Internet Protocol, 5
internet timestamp, 148
IP. See Internet Protocol
IP options flags, 147
IP protocol scan, 46
IPID, 60, 64, 89
--ip-options, 147
IPv6, 218
-iR, 193

L

light version scan, 145
limit operating system scanning, 138
list interfaces, 156
list scan, 58
log errors, 167
--log-errors, 167
logs, 159
loose source routing, 150

M

Maimon scan, 217
--max-hostgroup, 187
maximum transmission unit, 205
--max-parallelism, 188
--max-rtt-timeout, 187
--max-scan-delay, 190
media access control, 15
--min-hostgroup, 188
--min-parallelism, 189
--min-rtt-timeout, 186
--mtu, 205

N

-n, 120
network auditing, 232
Nmap

basics, 10
command line, 12
NmapFE, 1
nmap-mac-prefixes, 15
nmap-os-db, 128, 137
nmap-os-fingerprints, 18, 128
nmap-protocols, 18, 46
nmap-rpc, 19
nmap-service-probes, 20, 141, 146
nmap-services, 20, 154
NMapWin, 1
no random ports, 153
--noninteractive, 176
non-parallel DNS lookups, 124
normal output format, 159
--no-stylesheet, 163
null scan, 37

O

-O, 17, 127
-O1, 137
-O2, 137
-oA, 165
-oG, 164
-oH, 166
-oN, 159
--open, 167
operating system fingerprinting, 125
OPS, 129
-oS, 165
--osscan-guess, 138
--osscan-limit, 138
-oX, 160

P

-p, 154
-P0, 117
-PA, 102
packet trace, 172
--packet-trace, 172
parallel host scanning, 187
parallel port scanning, 188
-PB, 98
-PD, 117
-PE, 100
-PI, 100
ping, 95
Ping scan, 40
-PM, 114
-PN, 117
port numbers, 154
-PP, 111
-PR, 96
--privileged, 219

privileged access, 13
proxy, 90
-PS, 106
-PT, 102
-PU, 109

Q

-q, 216
quash argument vector, 216

R

-r, 153
-R, 118
random targets, 193
--randomize-hosts, 193
raw sockets, 2
read targets from file, 152
real-time debugging levels, 179
real-time packet tracing, 180
real-time verbosity levels, 178
record route, 149
release accessible memory, 219
--release-memory, 219
require reverse DNS, 118
--resume, 166
resume scan, 166
-rH, 193
round trip time, 186
RPC scan, 55
RPCGrind, 55
run-time interactions, 177

S

-S, 198
-sA, 49
scan summary, 24
--scan-delay, 189
--scanflags, 216
script kiddie format, 165
--send-eth, 157
--send-ip, 157
SEQ, 129
-sF, 34
show only open ports, 167
-sI, 60
-sL, 58
-sM, 217
-sN, 37
-sO, 19, 46
source address, 198
source routing, 150
--source-port, 154
-sP, 40
specify DNS servers, 122

spoof, 60
--spoof, 175
spoof MAC address, 199
--spoof-mac, 199
spyware, 222
-sR, 19, 55
-sS, 25
-sT, 29
stealth scan, 33
strict source routing, 150
--stylesheet, 163
-sU, 43
subnet broadcast, 96
support files, 14
-sV, 20, 141
-sW, 52
-sX, 35
SYN flood, 196
--system-dns, 124

T

-T, 191
T:, 154
T1, 129
target specifications, 12
TCP. See Transmission Control Protocol
TCP ACK ping, 102
TCP connect() scan, 29
TCP Handshake, 7
TCP options, 130
TCP probe, 130, 135
TCP sequence prediction, 129
TCP SYN ping, 106
TCP SYN scan, 25
TCP window size, 130
TCP/IP, 5
 fundamentals, 5
--thc, 220
time to live, 200
--timing, 191
timing options, 183
timing policies, 191
Transmission Control Protocol, 6
 port, 6
Trojan horse, 222
--ttl, 200

U

- U:, 154
- UDP. See User Datagram Protocol
- UDP ping, 109
- UDP probe, 134
- UDP scan, 43
- unprivileged, 219
- Uriel Maimon, 217
- User Datagram Protocol, 8

V

- v, 169
- verbose, 169
- verbosity, 137
- version, 215
- version detection, 141
- version intensity, 145
- version-all, 145
- version-intensity, 145
- version-light, 145
- version-trace, 144, 171
- virus, 222
- vulnerability assessment, 224

W

- webxml, 163
- webXML, 163
- WIN, 129
- window scan, 52
- Windows
 - and Nmap, 2, 207
 - interfaces, 155
 - IP fragmentation, 205
 - raw sockets, 208
 - Service Pack 2, 2
 - stealth scanning, 33
 - support files, 14
- WinPcap, 208

X

- xmas tree scan, 35
- XML format, 160

Z

- zombie, 60, 64