

# Table of Contents

Preface .....	xxv
1. Introduction .....	xxv
2. Intended Audience and Organization .....	xxvi
3. Conventions .....	xxvi
4. Other Resources .....	xxviii
5. Request for Comments .....	xxviii
6. Acknowledgements .....	xxix
1. Getting Started with Nmap .....	1
1.1. Introduction .....	1
1.2. Nmap Overview and Demonstration .....	1
Avatar Online .....	1
Saving the Human Race .....	8
MadHat in Wonderland .....	10
1.3. Legal Issues .....	13
Is Unauthorized Port Scanning a Crime? .....	13
Can Port Scanning Crash the Target Computer/Networks? .....	18
Nmap Copyright .....	19
1.4. The History and Future of Nmap .....	20
2. Obtaining, Compiling, Installing, and Removing Nmap .....	25
2.1. Introduction .....	25
Testing Whether Nmap is Already Installed .....	25
Command-line and Graphical Interfaces .....	25
Downloading Nmap .....	28
Verifying the Integrity of Nmap Downloads .....	28
Obtaining Nmap from the Subversion (SVN) Repository .....	30
2.2. Unix Compilation and Installation from Source Code .....	31
Configure Directives .....	32
If You Encounter Compilation Problems .....	33
2.3. Linux Distributions .....	34
RPM-based Distributions (Red Hat, Mandrake, Suse, Fedora) .....	34
Updating Red Hat, Fedora, Mandrake, and Yellow Dog Linux with Yum .....	36
Debian Linux and Derivatives such as Ubuntu .....	37
Gentoo Linux .....	38
Other Linux Distributions .....	38
2.4. Windows .....	38
Windows Self-installer .....	39
Command-line Zip Binaries .....	39
Installing the Nmap zip binaries .....	40
Compile from Source Code .....	40
Executing Nmap on Windows .....	41
2.5. Sun Solaris .....	42
2.6. Apple Mac OS X .....	43
2.7. FreeBSD / OpenBSD / NetBSD .....	43



OpenBSD Binary Packages and Source Ports Instructions .....	44
FreeBSD Binary Package and Source Ports Instructions .....	44
Installation of the binary package .....	44
Installation using the source ports tree .....	45
NetBSD Binary Package Instructions .....	45
2.8. Amiga, HP-UX, IRIX, and Other Platforms .....	45
2.9. Removing Nmap .....	45
3. Host Discovery (“Ping Scanning”) .....	47
3.1. Introduction .....	47
3.2. Specifying Target Hosts and Networks .....	47
Input From List (-iL) .....	48
Choose Targets at Random (-iR <i>Numtargets</i> ) .....	48
Excluding Targets (--exclude, --excludefile <i>filename</i> ) .....	48
Practical Examples .....	49
3.3. DNS Resolution .....	49
Speeding DNS Resolution by Carefully Selecting DNS Servers .....	50
3.4. Host Discovery Controls .....	52
List Scan (-sL) .....	52
Ping Scan (-sP) .....	53
Disable Ping (-P0) .....	54
3.5. Host Discovery Techniques .....	55
TCP SYN Ping (-PS[portlist]) .....	56
TCP ACK Ping (-PA[portlist]) .....	57
UDP Ping (-PU[portlist]) .....	58
ICMP Ping Types (-PE, -PP, and -PM) .....	59
ARP Scan (-PR) .....	59
Default Combination (-PB) .....	60
3.6. Putting it All Together: Host Discovery Strategies .....	61
Related Options .....	61
Choosing and Combining Ping Options .....	63
TCP probe and port selection .....	63
UDP port selection .....	65
ICMP probe selection .....	65
Designing the ideal combinations of probes .....	65
3.7. Finding an Organization's IP addresses to Scan .....	67
3.8. Host Discovery Code Algorithms .....	67
4. Port Scanning Overview .....	69
4.1. Introduction to Port Scanning .....	69
What Exactly is a Port? .....	69
What is Port Scanning? .....	72
Why Scan Ports? .....	73
4.2. A Quick Port Scanning Tutorial .....	74
4.3. Command-line Flags .....	78
Selecting Scan Techniques .....	78
Selecting Ports to Scan .....	79
Timing-related Options .....	80



Output Format and Verbosity Options .....	81
Firewall and IDS Evasion Options .....	82
Specifying Targets .....	83
Miscellaneous Options .....	83
4.4. IPv6 Scanning [-6] .....	83
4.5. [RECIPE] Scanning a Large Network for a Certain Open TCP Port .....	84
Problem .....	84
Solution .....	84
Discussion .....	85
See Also .....	91
5. Port Scanning Techniques and Algorithms .....	93
5.1. Introduction .....	93
5.2. TCP SYN (Stealth) Scan (-sS) .....	95
5.3. TCP Connect Scan (-sT) .....	98
5.4. UDP Scan (-sU) .....	100
Disambiguating Open from Filtered UDP Ports .....	101
Speeding up UDP Scans .....	104
5.5. TCP FIN, NULL, and Xmas Scans (-sF, -sN, -sX) .....	105
5.6. Custom Scan Types with --scanflags .....	109
Custom SYN/FIN Scan .....	109
PSH Scan .....	110
5.7. TCP ACK Scan (-sA) .....	111
5.8. TCP Window Scan (-sW) .....	112
5.9. TCP Maimon Scan (-sM) .....	115
5.10. TCP Idle Scan (-sI) .....	115
Finding a Working Idle Scan Zombie Host .....	118
Executing an Idle Scan .....	118
Idle Scan Implementation Algorithms .....	119
5.11. IP Protocol Scan (-sO) .....	123
5.12. TCP FTP Bounce Scan (-b) .....	125
5.13. Scan Code and Algorithms .....	127
Network Condition Monitoring .....	127
Host and Port Parallelization .....	127
Round Trip Time Estimation .....	128
Congestion Control .....	128
Port Scan Pings .....	130
Inferred Neighbor Times .....	130
Adaptive Retransmission .....	130
Scan Delay .....	131
6. Optimizing Nmap Performance .....	133
6.1. Introduction .....	133
6.2. Scan Time Reduction Techniques .....	133
Omit Non-Critical Tests .....	134
Optimize Timing Parameters .....	135
Upgrade Nmap .....	135
Execute Concurrent Nmap Instances .....	135



Scan From a Favorable Network Location .....	136
Increase Available Bandwidth and CPU Time .....	136
6.3. Coping Strategies for Long Scans .....	137
Use a Multi-stage Approach .....	137
Estimate and plan for scan time .....	138
6.4. Low Level Timing Controls .....	138
Hostgroup Size (--min-hostgroup, --max-hostgroup) .....	139
Probe Parallelism (--min-parallelism, --max-parallelism) .....	139
Round Trip Time Timeouts (--min-rtt-timeout, --max-rtt-timeout, --initial-rtt-timeout) .....	140
Maximum Number of Retransmissions (--max-retries) .....	140
Host Timeout (--host-timeout) .....	141
Scan delay (--scan-delay, --max-scan-delay) .....	141
6.5. Timing Templates (-T) .....	141
6.6. Scanning 676,352 IP Addresses in 46 Hours .....	143
6.7. Scan Performance Examples .....	144
7. Service and Application Version Detection .....	145
7.1. Introduction .....	145
7.2. Usage and Examples .....	147
7.3. Technique Described .....	149
Cheats and Fallbacks .....	150
Probe Selection and Rarity .....	151
--version-intensity .....	152
--version-light .....	152
--version-all .....	152
7.4. Technique Demonstrated .....	153
7.5. Post-processors .....	155
Nmap Scripting Engine Integration .....	155
RPC Grinding .....	156
SSL Post-processor Notes .....	157
7.6. nmap-service-probes File Format .....	158
Exclude Directive .....	158
Probe Directive .....	159
match Directive .....	159
softmatch Directive .....	161
ports and sslports Directives .....	162
totalwaitms Directive .....	162
rarity Directive .....	163
fallback Directive .....	163
Putting it all together .....	163
7.7. Community Contributions .....	164
Submit Service Fingerprints .....	164
Submit Database Corrections .....	165
Submit New Probes .....	165
7.8. [RECIPE] Find All Servers Running an Insecure or Nonstandard Application Version .....	166
Problem .....	166



Solution .....	167
Discussion .....	167
7.9. [RECIPE] Hack Version Detection to Suit Custom Needs, such as Open Proxy Detection .....	168
Problem .....	168
Solution .....	169
Discussion .....	169
8. Remote OS Detection .....	171
8.1. Introduction .....	171
Reasons for OS Detection .....	171
Determining vulnerability of target hosts .....	171
Tailoring exploits .....	171
Network inventory and support .....	172
Detecting unauthorized and dangerous devices .....	172
Social engineering .....	172
8.2. Usage and Examples .....	172
8.3. TCP/IP Fingerprinting Methods Supported by Nmap .....	177
Probes Sent .....	180
Sequence generation (SEQ, OPS, WIN, and T1) .....	180
ICMP echo (IE) .....	181
TCP explicit congestion notification (ECN) .....	182
TCP (T2–T7) .....	182
UDP (U1) .....	182
Response Tests .....	183
TCP ISN greatest common denominator (GCD) .....	183
TCP ISN counter rate (ISR) .....	183
TCP ISN sequence predictability index (SP) .....	183
TCP IP ID sequence generation algorithm (TI) .....	184
ICMP IP ID sequence generation algorithm (II) .....	184
Shared IP ID sequence boolean (SS) .....	185
TCP timestamp option algorithm (TS) .....	185
TCP options (O, 01–06) .....	186
TCP initial window size (W, W1–W6) .....	186
Responsiveness (R) .....	187
IP don't fragment bit (DF) .....	187
Don't fragment (ICMP) (DFI) .....	187
IP initial time-to-live (T) .....	187
IP initial time-to-live guess (TG) .....	188
Explicit congestion notification (CC) .....	188
TCP miscellaneous quirks (Q) .....	188
TCP sequence number (S) .....	189
ICMP sequence number(SI) .....	189
TCP acknowledgment number (A) .....	189
TCP flags (F) .....	190
TCP RST data checksum (RD) .....	190
IP type of service (TOS) .....	190



IP type of service for ICMP responses (TOSI) .....	191
IP total length (IPL) .....	191
Unused port unreachable field nonzero (UN) .....	191
Returned probe IP total length value (RIPL) .....	191
Returned probe IP ID value (RID) .....	191
Integrity of returned probe IP checksum value (RIPCK) .....	191
Integrity of returned probe UDP length and checksum (RUL and RUCK) .....	192
Integrity of returned UDP data (RUD) .....	192
ICMP response code (CD) .....	192
IP data length for ICMP responses (DLI) .....	192
8.4. Fingerprinting Methods Avoided by Nmap .....	193
Passive Fingerprinting .....	193
Exploit Chronology .....	193
Retransmission Times .....	194
IP Fragmentation .....	194
8.5. Understanding an Nmap Fingerprint .....	194
Decoding the Subject Fingerprint Format .....	195
Decoding the SCAN line of a subject fingerprint .....	196
Decoding the Reference Fingerprint Format .....	197
Free-form OS description (Fingerprint line) .....	198
Device and OS classification (Class lines) .....	199
Test expressions .....	200
8.6. OS Matching Algorithms .....	201
8.7. Dealing with Misidentified and Unidentified Hosts .....	202
When Nmap Guesses Wrong .....	203
When Nmap Fails to Find a Match and Prints a Fingerprint .....	204
Modifying the nmap-os-db database Yourself .....	205
8.8. [RECIPE] Detect Rogue Wireless Access Points on an Enterprise Network .....	205
Problem .....	205
Solution .....	206
WAP Characteristics .....	206
9. Nmap Scripting Engine .....	209
9.1. Introduction .....	209
9.2. Usage and Examples .....	211
Script Categories .....	211
Arguments to Scripts .....	212
Command-line Arguments .....	212
Usage Examples .....	213
9.3. Script Format .....	214
id Field .....	214
description Field .....	214
author Field .....	214
license Field .....	214
runlevel Field .....	214
Port and Host Rules .....	214
Action .....	215



9.4. Script Language .....	215
Lua Base Language .....	215
9.5. Lua Extensions .....	216
Bitwise Logical Operations .....	216
Perl Compatible Regular Expressions .....	217
IP Operations .....	218
Short Portrules .....	219
Functional Programming Style List Operations .....	219
String Buffer Operations .....	220
URL Manipulation Functions .....	221
Buffered Network I/O Helper Functions .....	221
HTTP Functions .....	222
Data File Parsing Functions .....	222
Various Utility Functions .....	223
9.6. Nmap API .....	223
Information Passed to a Script .....	223
Target Information Retrieving by a Script .....	227
Various Utility Functions for Raw Packet Support .....	228
Network I/O API .....	228
Connect-style network I/O .....	228
Raw packet network I/O .....	231
Exception Handling .....	233
The Registry .....	234
9.7. Script Writing Tutorial .....	234
The Head .....	234
The Rule .....	235
The Mechanism .....	236
9.8. Version Detection using NSE .....	237
9.9. Example Scripts .....	239
Finger-Test Script .....	239
Service Owner Lookup via Identd .....	241
9.10. Implementation .....	242
Initialization Phase .....	243
Matching of Scripts to Targets .....	244
Running Scripts .....	245
Adding C Modules to Nselib .....	245
9.11. NSE Script License and Community Contributions .....	246
10. Detecting and Subverting Firewalls and Intrusion Detection Systems .....	247
10.1. Introduction .....	247
10.2. Why Would Whitehats Ever Do This? .....	247
10.3. Determining Firewall Rules .....	248
Standard SYN Scan .....	248
Sneaky firewalls that return RST .....	249
ACK Scan .....	249
IP ID Tricks .....	252
UDP Version Scanning .....	254



10.4. Bypassing Firewall Rules .....	255
Exotic Scan Flags .....	255
Source Port Manipulation .....	256
IPv6 Attacks .....	257
IP ID Idle Scanning .....	259
Multiple Ping Probes .....	259
Fragmentation .....	259
Proxies .....	260
Source Routing .....	260
FTP Bounce Scan .....	260
Take an Alternative Path .....	261
10.5. Subverting Intrusion Detection Systems .....	261
Intrusion Detection System Detection .....	262
Reverse probes .....	262
Sudden firewall changes and suspicious packets .....	263
Naming conventions .....	263
Unexplained TTL jumps .....	264
Avoiding Intrusion Detection Systems .....	264
Slow down .....	264
Scatter probes across networks rather than scanning hosts consecutively. ....	267
Fragment packets .....	267
Evade specific rules .....	268
Avoid easily detected Nmap features .....	269
Misleading Intrusion Detection Systems .....	269
Decoys .....	269
Port scan spoofing .....	271
MAC address spoofing .....	271
Idle scan .....	271
DNS proxying .....	271
DoS Attacks Against Reactive Systems .....	272
Exploiting Intrusion Detection Systems .....	272
Ignoring Intrusion Detection Systems .....	272
10.6. Detecting Packet Forgery by Firewall and Intrusion Detection Systems .....	273
Look for TTL Consistency .....	274
Look for IP ID and Sequence Number Consistency .....	275
The Bogus TCP Checksum trick .....	276
Round Trip Times .....	277
Close Analysis of Packet Headers and Contents .....	278
Unusual Network Uniformity .....	278
11. Defenses Against Nmap .....	279
11.1. Introduction .....	279
11.2. Proactive Scanning .....	279
11.3. Blocking and Slowing Nmap with Firewalls .....	280
11.4. Detecting Nmap Scans .....	281
11.5. Clever Trickery .....	282
Hiding Services on Obscure Ports .....	282



Port knocking .....	284
Honeypots and Honeynets .....	285
OS Spoofing .....	285
Tar Pits .....	287
Reactive Port Scan Detection .....	288
Escalating Arms Race .....	288
12. Zenmap GUI Users' Guide .....	289
12.1. Introduction .....	289
12.2. Scanning .....	289
Profiles .....	291
Scan tabs .....	291
12.3. Interpreting scan results .....	291
Scan results tabs .....	291
Sorting by host .....	296
Sorting by service .....	298
12.4. Saving and loading scan results .....	299
The recent scans database .....	300
12.5. The Nmap command constructor wizard .....	300
12.6. The profile editor .....	303
Creating a new profile .....	304
Profile meta-information .....	305
Editing a profile .....	305
Deriving a new profile from an old one .....	305
12.7. Searching through results .....	306
12.8. Comparing results .....	307
Graphical comparison .....	308
Text comparison .....	310
12.9. Location and purpose of Zenmap's configuration files .....	312
System configuration files .....	312
Per-user configuration files .....	313
12.10. Description of zenmap.conf .....	314
Sections of zenmap.conf .....	314
12.11. Command line options .....	316
Synopsis .....	316
Option summary .....	316
Output redirection and debugging .....	317
12.12. History .....	317
13. Nmap Output Formats .....	319
13.1. Introduction .....	319
13.2. Command-line Flags .....	320
Controlling Output Type .....	320
Controlling Verbosity of Output .....	321
Enabling Debugging Output .....	325
Enabling Packet Tracing .....	326
Resuming Aborted Scans .....	327
13.3. Interactive Output .....	327



13.4. Normal Output (-oN) .....	327
13.5. \$cRlP t klddI3 OuTPut (-oS) .....	328
13.6. XML Output (-oX) .....	329
Using XML Output .....	331
13.7. Manipulating XML Output with Perl .....	334
13.8. Output to a Database .....	336
13.9. Creating HTML Reports .....	337
13.10. Grepable Output (-oG) .....	337
Grepable Output Fields .....	338
Host field .....	338
Ports field .....	339
Protocols field .....	340
Ignored State field .....	340
OS field .....	341
Seq Index field .....	341
IP ID Seq field .....	341
Status field .....	341
Parsing Grepable Output on the Command Line .....	342
14. Understanding and Customizing Nmap Data Files .....	343
14.1. Introduction .....	343
14.2. Well Known Port List: nmap-services .....	343
14.3. Version Scanning DB: nmap-service-probes .....	345
14.4. SunRPC Numbers: nmap-rpc .....	346
14.5. Old Nmap OS Detection DB: nmap-os-fingerprints .....	347
14.6. Nmap OS Detection DB: nmap-os-db .....	348
14.7. MAC Address Vendor Prefixes: nmap-mac-prefixes .....	348
14.8. IP Protocol Number List: nmap-protocols .....	349
14.9. Using Customized Data Files .....	349
15. Nmap Reference Guide .....	353
15.1. Description .....	353
15.2. Options Summary .....	354
15.3. Target Specification .....	357
15.4. Host Discovery .....	358
15.5. Port Scanning Basics .....	364
15.6. Port Scanning Techniques .....	365
15.7. Port Specification and Scan Order .....	370
15.8. Service and Version Detection .....	371
15.9. OS Detection .....	373
15.10. Nmap Scripting Engine (NSE) .....	374
15.11. Timing and Performance .....	376
15.12. Firewall/IDS Evasion and Spoofing .....	380
15.13. Output .....	384
15.14. Miscellaneous Options .....	389
15.15. Runtime Interaction .....	391
15.16. Examples .....	391
15.17. Bugs .....	392



15.18. Author .....	393
15.19. Legal Notices .....	393
Nmap Copyright and Licensing .....	393
Creative Commons License for this Nmap Guide .....	394
Source Code Availability and Community Contributions .....	394
No Warranty .....	395
Inappropriate Usage .....	395
Third-Party Software .....	395
US Export Control Classification .....	396
A. Nmap XML Output DTD .....	397
A.1. Purpose .....	397
A.2. The Full DTD .....	397
Index .....	405





# List of Figures

1.1. Trinity begins her assault .....	8
1.2. Trinity scans the Matrix .....	9
1.3. Terminal-view of the hack .....	10
1.4. Strong opinions on port scanning legality and morality .....	14
2.1. NmapFE presents a simple graphical interface to Nmap .....	26
2.2. Zenmap is the newest and most advanced Nmap GUI .....	27
2.3. Executing Nmap from a Windows command shell .....	42
4.1. IPv4 header layout .....	69
4.2. TCP header layout .....	70
4.3. UDP header layout .....	70
5.1. ICMPv4 destination unreachable header layout .....	94
5.2. SYN scan of open port 22 .....	95
5.3. SYN scan of closed port 113 .....	96
5.4. SYN scan of filtered port 139 .....	97
5.5. Connect scan of open port 22 ( <b>nmap -sT -p22 scanme.nmap.org</b> ) .....	99
5.6. Idle scan technique (simplified) .....	116
5.7. Congestion window and threshold .....	129
5.8. Scan delay during a UDP scan .....	131
8.1. IPv4 header layout .....	178
8.2. TCP header layout .....	179
8.3. ICMP echo request or reply header layout .....	179
8.4. ICMP destination unreachable header layout .....	180
8.5. UDP header layout .....	180
10.1. BlackICE discovers an unusual intruder .....	263
10.2. An attacker masked by dozens of decoys .....	270
12.1. Zenmap's main window .....	290
12.2. Target and profile selection .....	290
12.3. Scan tabs .....	291
12.4. Host selection .....	297
12.5. Service selection .....	299
12.6. Choosing a profile .....	303
12.7. The profile editor .....	304
12.8. The search dialog .....	306
12.9. Search options .....	307
12.10. Comparison tool .....	308
12.11. Graphical comparison .....	309
12.12. Comparison colors .....	310
12.13. Text mode comparison .....	311
13.1. Reading XML in a web browser .....	333





# List of Tables

1. Formatting style conventions .....	xxviii
3.1. Valuable TCP probe ports, in descending order of accessibility .....	64
5.1. ICMP destination unreachable (type 3) code values .....	94
5.2. How Nmap interprets responses to a SYN probe .....	97
5.3. How Nmap interprets responses to a UDP probe .....	100
5.4. How Nmap interprets responses to a null, FIN, or Xmas scan probe .....	105
5.5. How Nmap interprets responses to an ACK scan probe .....	111
5.6. How Nmap interprets responses to a Window scan ACK probe .....	113
5.7. How Nmap interprets responses to a Maimon scan probe .....	115
5.8. How Nmap interprets responses to an IP protocol probe .....	124
6.1. Timing templates and their effects .....	142
7.1. <code>versioninfo</code> field formats and values .....	161
8.1. O test values .....	186
8.2. DFI test values .....	187
8.3. CC test values .....	188
8.4. S test values .....	189
8.5. SI test values .....	189
8.6. Ack test values .....	190
8.7. F test values .....	190
8.8. TOSI test values .....	191
8.9. CD test values .....	192
8.10. DLI test values .....	193
8.11. Reference fingerprint test expression operators .....	201
9.1. <code>port.version</code> values .....	226
12.1. Vulnerability icons .....	295
12.2. OS icons .....	298
12.3. Text diff character codes .....	312





# List of Examples

1. A typical Nmap scan .....	xxvii
1.1. Nmap list scan against Avatar Online IP addresses .....	3
1.2. Nmap results against an AO firewall .....	5
1.3. Another interesting AO machine .....	7
1.4. Nmap-diff typical output .....	12
1.5. Nmap-report execution .....	13
2.1. Checking for Nmap and determining its version number .....	25
2.2. Verifying the Nmap and Fyodor PGP Key Fingerprints .....	29
2.3. Verifying PGP Key Fingerprints (Successful) .....	29
2.4. Detecting a bogus file .....	29
2.5. A typical Nmap release digest file .....	30
2.6. Verifying Nmap hashes .....	30
2.7. Installing Nmap from binary RPMs .....	35
2.8. Building and installing Nmap from source RPMs .....	35
2.9. Installing Nmap from a system Yum repository .....	37
3.1. Enumerating hosts surrounding WWW.Stanford.Edu with list scan .....	53
3.2. Attempts to ping popular Internet hosts .....	56
3.3. Retry Host Discovery using port 80 SYN probes .....	57
3.4. Attempted ACK ping against Microsoft .....	58
3.5. Raw IP ping scan of an offline target .....	59
3.6. ARP ping scan of an offline target .....	60
3.7. Generating 50,000 IP Addresses, then ping scanning with default options .....	66
3.8. Repeating ping scan with extra probes .....	66
4.1. Viewing and increasing the ephemeral port range on Linux .....	71
4.2. Simple scan: <code>nmap scanme.nmap.org</code> .....	75
4.3. More complex: <code>nmap -p0- -v -A -T4 scanme.nmap.org</code> .....	77
4.4. A simple IPv6 scan .....	84
4.5. Discovering Playboy's IP space .....	86
4.6. Pinging Playboy's Web Server for a Latency Estimate .....	86
4.7. Digging through Playboy's DNS records .....	87
4.8. Pinging the MX servers .....	88
4.9. TCP Pinging the MX servers .....	88
4.10. Launching the scan .....	90
4.11. Egrep for open ports .....	90
5.1. A SYN Scan showing three port states .....	95
5.2. Using <code>--packet-trace</code> to understand a SYN scan .....	98
5.3. Connect scan example .....	100
5.4. UDP scan example .....	101
5.5. UDP scan example .....	101
5.6. Improving Felix's UDP scan results with version detection .....	102
5.7. Improving Scanme's UDP scan results with version detection .....	102
5.8. Attempting to disambiguate UDP ports with TTL discrepancies .....	103
5.9. Example FIN and Xmas scans .....	106



5.10. SYN scan of docsrv.caldera.com .....	107
5.11. FIN scan of docsrv.caldera.com .....	108
5.12. A SYN/FIN scan of Google .....	110
5.13. A custom PSH scan .....	110
5.14. A Typical ACK Scan .....	111
5.15. An ACK scan of Docsrv .....	112
5.16. Window scan of docsrv.caldera.com .....	114
5.17. A failed Maimon scan .....	115
5.18. An idle scan against the RIAA .....	119
5.19. IP protocol scan of a router and a typical Linux 2.4 box .....	125
5.20. Attempting an FTP bounce scan .....	126
5.21. Successful FTP bounce scan .....	126
6.1. Bandwidth usage over local 100Mbps ethernet network .....	137
6.2. Estimating scan time .....	138
7.1. Simple usage of version detection .....	146
7.2. Version detection against www.microsoft.com .....	147
7.3. Complex version detection .....	148
7.4. NULL Probe Cheat Example Output .....	151
7.5. Enumerating RPC services with rpcinfo .....	156
7.6. Nmap direct RPC scan .....	157
7.7. Version scanning through SSL .....	158
8.1. OS Detection with Verbosity (-O -v) .....	173
8.2. Using version scan to detect the OS .....	175
8.3. A typical subject fingerprint .....	195
8.4. A cleaned up subject fingerprint .....	196
8.5. A typical reference fingerprint .....	198
8.6. Some typical fingerprint descriptions and corresponding classifications .....	200
8.7. The MatchPoints structure .....	202
8.8. Scan results against a consumer WAP .....	207
9.1. Typical NSE Output .....	211
9.2. Exception handling example .....	233
9.3. Using local variables to save data. ....	244
10.1. Detection of closed and filtered TCP ports .....	248
10.2. ACK scan against Scanme .....	250
10.3. Contrasting SYN and ACK scans against Para .....	251
10.4. UDP scan against firewalled host .....	254
10.5. UDP version scan against firewalled host .....	255
10.6. FIN scan against stateless firewall .....	256
10.7. Bypassing Windows IPsec filter using source port 88 .....	257
10.8. Comparing IPv4 and IPv6 scans .....	258
10.9. Exploiting a printer with the FTP bounce scan .....	261
10.10. Host names can be deceiving .....	264
10.11. Noting TTL gaps with traceroute .....	264
10.12. Slow scan to bypass the default Snort 2.2.0 Flow-portscan fixed time scan detection method. ....	266
10.13. Default Snort rules referencing Nmap .....	268
10.14. Detection of closed and filtered TCP ports .....	275



10.15. Testing IP ID sequence number consistency .....	276
10.16. Finding a Firewall With Bad TCP Checksums .....	276
11.1. An all-tcp-port version scan .....	283
11.2. Deceiving Nmap with IP Personality .....	286
13.1. Scanrand output against a local network .....	319
13.2. Greping for verbosity conditionals .....	323
13.3. A comparison of interactive output with and without verbosity enabled. ....	324
13.4. Some representative debugging lines .....	325
13.5. Using <code>--packet-trace</code> to detail a ping scan of Scanme .....	326
13.6. A typical example of normal output .....	328
13.7. A typical example of <code>\$crIpt KiDDi3 OutPut</code> .....	329
13.8. An example of Nmap XML output .....	330
13.9. Nmap XML port elements .....	331
13.10. <code>Nmap::Parser</code> sample code .....	335
13.11. <code>Nmap::Scanner</code> sample code .....	336
13.12. A typical example of grepable output .....	338
13.13. Grepable output for IP protocol scan .....	340
13.14. Ping scan grepable output .....	342
13.15. List scan grepable output .....	342
13.16. Parsing grepable output on the command line .....	342
14.1. Excerpt from <code>nmap-services</code> .....	344
14.2. Excerpt from <code>nmap-service-probes</code> .....	345
14.3. Excerpt from <code>nmap-rpc</code> .....	346
14.4. Excerpt from <code>nmap-os-fingerprints</code> .....	347
14.5. Excerpt from <code>nmap-mac-prefixes</code> .....	348
14.6. Excerpt from <code>nmap-protocols</code> .....	349
15.1. A representative Nmap scan .....	354

