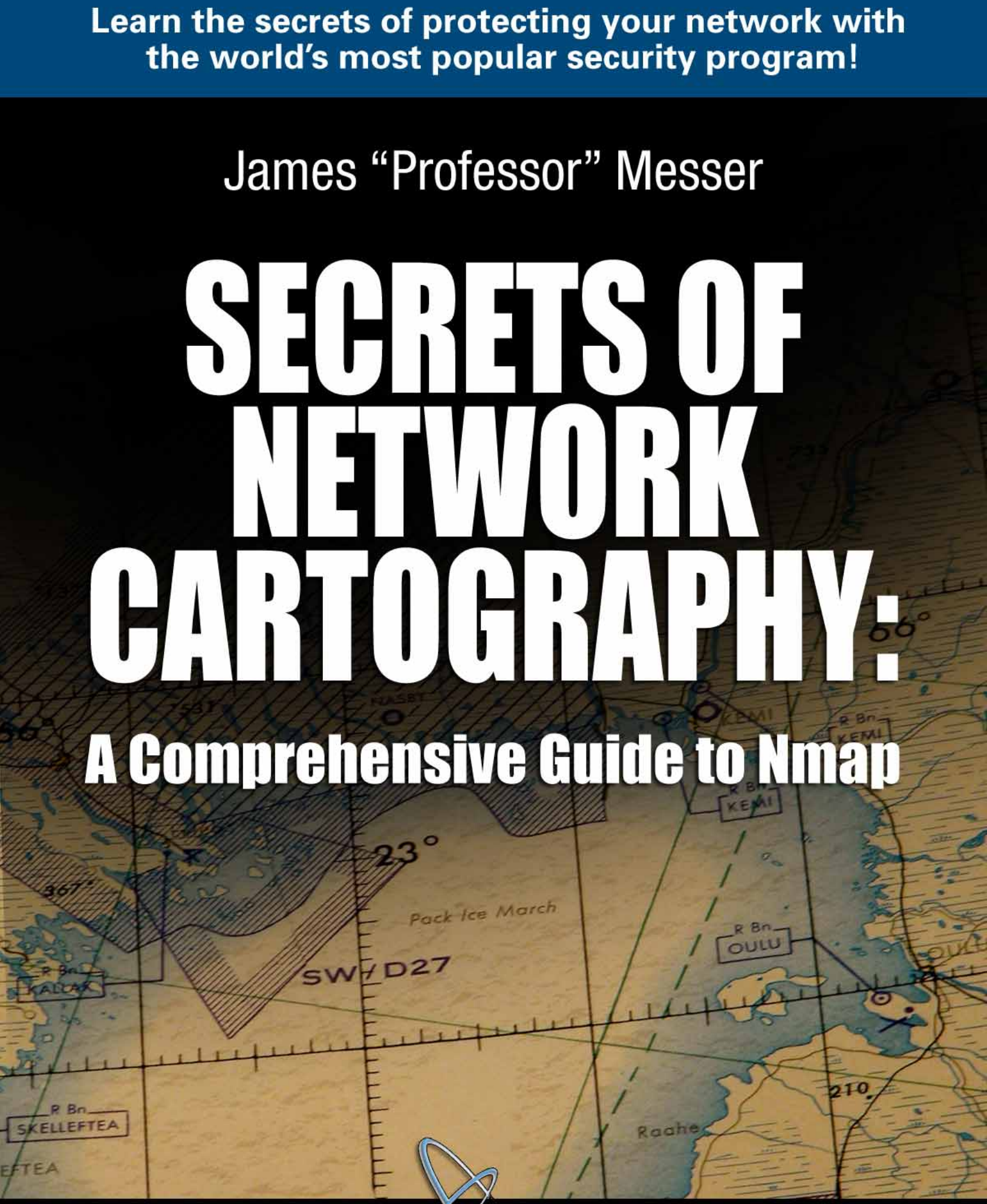
Learn the secrets of protecting your network with the world's most popular security program!

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

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

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

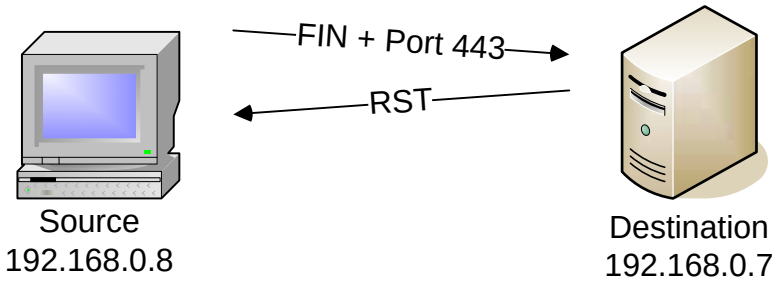
FIN, Xmas Tree, and Null Scan Operation

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)

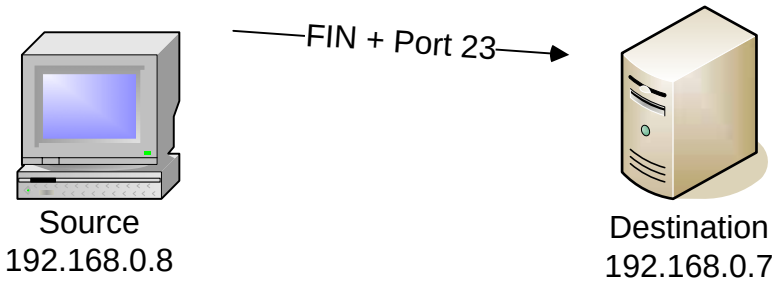
The FIN scan's "stealth" frames are unusual because they are sent to a device without first going through the normal TCP handshaking. If a TCP session isn't active, the session certainly can't be formally closed!

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.

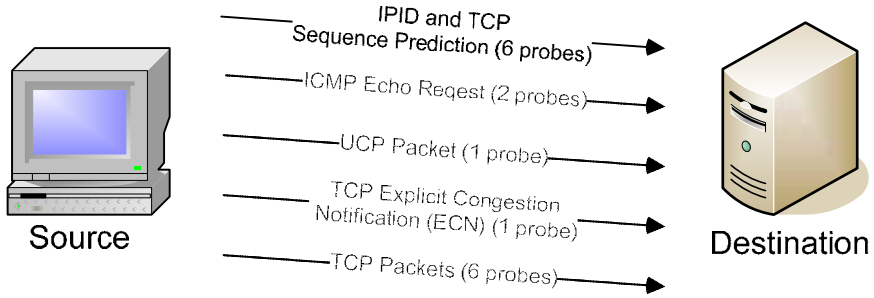
Nmap's pings can also be customized for the situation. For example, a firewall that blocks ICMP and ACK on port 80 might allow Nmap to ping through the firewall with a TCP SYN to port 135 or a UDP query to port 22. This customization could also be used as a filter that would only identify devices that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

Q

R

S

T

U

V

W

X

Z