

Nmap Network Scanning

Review by JP Bourget, CISSP, MCSE, MS

Once again, my company had acquired some new networks for us to take over, and of course, the documentation was from 3 years ago. As part of our due diligence, I had to quickly and accurately figure out everything on the network. How did I accomplish this? With a network mapping utility; and the de facto standard in this area is Nmap! Nmap by Gordon Lyon AKA Fyodor not only saves you time, but, if you really know how to unleash it's power, it can be your friend for network audit's, discovering new devices, and even part of the network reconnaissance phase of a Pen Test. Another cool use I just learned from the Fyodor /. Interview was that the Chinese use it to scan for open proxies to bypass the Great Firewall of China. With that kind of flexibility, it is clearly the right tool for this job and many others. But what's the quickest way to get that power working in my favor?

Info on getting half the book for free is available below.

The obvious choice would be an in-depth tome from the author himself, but, after over 10 years in use around the globe, such a book didn't exist. But after seeing Fyodor's talk at Defcon 16 in August of 2008 and seeing an actual pre-release copy of his forthcoming book, I couldn't wait to get my hands on it. Fast forward to January of 2009 when Fyodor sent me a review copy of what is one of the most well written reference books I have had the chance to use to date. Before you even get to chapter one, you get a comprehensive table of contents followed by a list of tables and examples. Every book should do this! It's also important to note that this book is filled with out-of-the-box command line examples that should be in any pen tester's toolkit.

del.icio.us

Discuss in Forums {mos_smf_discuss:Book Reviews}

"About half of the content is available in the free online edition. Chapters exclusive to the print edition include 'Detecting and Subverting Firewalls and Intrusion Detection Systems', 'Optimizing Nmap Performance', 'Port Scanning Techniques and Algorithms', 'Host Discovery (Ping Scanning)', and more. The solution selections which provide detailed instructions on the best way to solve common networking tasks are also exclusive to the printed book."

- Quoted from Fyodor <http://nmap.org/book/>

Chapter 1 starts out with a quick intro to Nmap, as well as a history to help the reader understand why and how it has evolved to where it is today. Fyodor gives the reader some insight on the legal issues of using Nmap (don't scan the White House for example) and using Nmap responsibly. He shows us where they used Nmap in the Matrix (without his permission) and tells us where Nmap is going (ndiff, network topology mapping, etc.). Fyodor also does a good job at clearly defining his writing style, with bits of humor and robust organization, a trend which continues throughout the book.

Chapter 2 goes on to explain all of the options for installing, compiling and removing Nmap, and some tricks to keep things current. Also provided are suggestions on how to get the latest version with the newest features that may not be in the 'stable' release.

Once you dive into Chapter 3, you start to learn about one of the primary functions of Nmap: Host Discovery. This was my main area of previous experience with Nmap. As Fyodor explains the more common options, he also gives good examples of when and why to use each option, something you won't find in the man pages. For example, doing a ping scan with Nmap is pretty simple:

Nmap –sP –T4 www.yournetwork.com

I use these ping scans, followed by a port scan whenever I have a new network assigned to me. Fyodor also explains to us in Chapter 3 how to do SYN and ACK pings (-PS –PA options) as well as ARP scans (-PR). He also explains when to use all the available options and their effect on your network.

Chapter 4 continues your discovery process with port scanning. Fyodor's most important point in this chapter is how to use custom port lists to change the default behavior of Nmap during port scanning. As mentioned in his talk at Defcon 16, custom port lists can drastically increase the speed of your scans. For example, before I hit a new site I may want to know if they are running any web or smtp services. I would run the following command:

```
Nmap -PN -p80,443,25 -max-rtt-timeout 200 --initial-rtt-timeout 150 172.16.10.0/23
```

This will not only scan these ports but also reduce the timeout dramatically, so we only need to wait 3 minutes for our scan to complete. I would also replace the 172.16.10.0 with the target network range. I could also define a set of custom ports that I may want to scan. Very handy tips for the busy network administrator. Chapter 5 shows, and more importantly explains, all of the advanced scans available with Nmap. Most of these are based off sending raw IP packets, which requires not only root access but a detailed understanding of how they work to prevent any unintended effects on the target network. There is also a robust explanation of the algorithms behind these scans and what has and hasn't worked in the past. For example, if I wanted to figure out what machines may be in my target network with open ports that don't respond to pings, I might use a TCP SYN scan, using the --sS option, or a connect scan, using the --sT, or finally a UDP scan --sU. We also learn that you can create your own custom Scan types with --scanflags parameter. You can even set everything: --scanflags URGACKPSHRSTSYNFIN or a subset of all available scans.

In Chapter 6, Fyodor gives some excellent strategies on how to enhance the performance of your port scan, which can save you precious time during scans of larger networks. We learn not to run multiple instances of Nmap at once, as well as some strategies for planning out large scans. He also goes over the --T (T0-T5, T5 being the most aggressive) options, called timing templates. This can be beneficial when scanning large ranges, because you can reduce the default timeout and other key timing settings like delay and rate.

Chapters 7 and 8 moves us into service and operating system fingerprinting and introduced some of the post processors available, such as the Nmap Scripting Engine and others, to interrogate the services we may find running on a network. Fyodor also does an excellent job of showing how Nmap fingerprints Operating Systems, and actually explains how fingerprinting works under the hood.

Chapter 9 goes in-depth into the Nmap Scripting Engine (NSE). This chapter could have its own review, and teaches how to run many of the pre-written scripts available, as well as techniques to writing your own. You can get a full list of all the Nmap scripts at <http://Nmap.org/nsedoc/>. Some of the NSE scripts I use the most are: nbstat.nse, and sniffer-detect.nse. Here's some sample code to try them out:

```
Nmap -sU -script nbstat.nse --p137
```

```
Nmap -script sniffer-detect.nse 10.10.10/24
```

Chapter 10 shows us how to identify and evade firewalls and intrusion detection systems, as well as how to avoid being detected while scanning these devices. On the other side of that equation, Chapter 11 gives guidance on how to detect when your network is being interrogated by tools and techniques such as Nmap, honeypots, and blocking and/or slowing Nmap scans. The views of the offensive and defensive sides proved to be very useful from testing and incident response angles, as both are vital in today's organizations.

Chapter 12 brings us to ZeNmap, the GUI version of Nmap with viz technologies. There are many profiles such as intense scan, regular scan, OS Detection, quick scan, and more. ZeNmap can also aggregate results from multiple scans into a single view called "network inventory." I use this where I work and do weekly scans to see what has entered and left my network in the past week. When your scan is done, you get the output window with a few pretty useful tabs. The one I use the most (after skimming through the Nmap output tab) is the topology tab. See Figure 1. It shows us the topology of the network in hops using rings. Other tabs provide us some quick sorting abilities such as by port or hosts.

Figure 1: The "Topology Tab" (From <http://Nmap.org/book/zeNmap-results.html#zeNmap-tab-topology>)

Next up is Chapter 13, Nmap Output Formats. Fyodor goes into great detail on how to control what Nmap prints to the screen and output files. There are many options such as XML, populating a database, as well as grepable output. He even shares tricks to formatting the output for more usable results.

Chapter 14 wraps things up with info on how to customize how Nmap runs each time by editing the Nmap config files such as Nmap-services and Nmap-service-protocols. I really like the ability to define a set of ports or services you want to scan. I could create a custom Nmap-services file that defines the ports to scan, such as a port of a known Trojan or worm that's in the wild. Once I have my custom file, I can pass it to Nmap at runtime using - -servicedb option. I sometimes use this in order to check my networks in China for new worms that their network may have had exposure to. I also use this ability when doing initial reconnaissance on a pen test to quickly find potential holes leading to a full Nmap scan for further investigation.

"Nmap Network Scanning" is an informing read straight through, and Fyodor has done an excellent job of shaping this work into a reference book, one that any network pro or pen tester should have on his desk. I learned more about TCP scanning and how to "stretch" the TCP protocol than I did from comprehensive books on the subject. Another thing done very well in Nmap Network Scanning is the real world examples to help you understand what is trying to be accomplished with each command line. Fyodor also does a good job in entertaining as his sense of humor seen during his live presentations coming through on the written page. Finally, the in-depth explanations of why certain features work in certain ways goes a long way in understanding the how's and why's of network scanning. Many of the more obscure details of several network protocols will help any network admin realize how much information they can have readily available. I would recommend this as a must-have book for any network or security professional, as well as anyone wanting to learn more about TCP/IP.

References:

<http://interviews.slashdot.org/article.pl?sid=03/05/30/1148235&startat=&threshold=4&mode=nocomment&commentsort=3&op=Change>

<http://insecure.org/>

http://en.wikipedia.org/wiki/Gordon_Lyon

Jean Paul (JP) Bourget, BS IT, RIT 2005; MS Computer Security and Information Assurance, RIT 2008; CISSP; MCSE, CSSA. JP has five years experience in computer networking, system administration, and information security. During the day JP is responsible for Network and Security Management for a medium size global company based in the US. JP is also adjunct faculty at Rochester Institute of Technology where he teaches Networking and Security undergraduate classes. JP also performs pen testing and security audits for local companies in Rochester, NY. In his spare time, JP snowboards, rides motorcycles, mountain bikes and enjoys fixing up older homes.