Secrets of Network Cartography: A Comprehensive Guide to Nmap

Review by Jason Haddix, Security Aegis

Nmap is indispensable.

OK, that was obvious. There is no doubt that Fyodor and contributors have made the de-facto standard of network scanners, but when it comes down to learning the ins and outs and the power of Nmap, where should you put your hard earned cash?

Let’s neglect the support documentation (man pages) for a second, and assume you don’t really use Nmap on a day-to-day basis. Why? Over at http://www.professormesser.com/, James “Professor” Messer has put together a 232-page eBook proving that one doesn’t have to be a networking guru to learn how to use Nmap effectively in your organization.

But what about the $197 video companion to this $47 book? How does it stack up against Fyodor’s own book on Nmap (See EH-Net Review by JP Bourget)? Stick around my friends as the answers you seek are only minutes away.

del.icio.us

Discuss in Forums {mos_smf_discuss:Book Reviews}

Editor's Note: The reversion reviewed for this article is the 2nd edition R2.

Messer goes through eleven chapters of Nmap goodness starting from basic scans to more advanced “ninja” scans and provides helpful references to combine switches for maximum effect. Let’s go through them, shall we?

Chapters 1-3 of Secrets take you on a crash course of networking protocols including TCP, UDP, and ICMP, along with the basics of the well known functions of Nmap. Messer’s graphics and annotations are both easy to understand and helpful. The TCP three-way-handshake is described in adequate detail, and quite a few external links to Nmap related resources are also provided. You then explore the common scan types with descriptions, diagrams, packet captures, advantages, disadvantages, and when to use each particular type of scan. In fact, every function of Nmap described in this book follows that format. Finally in Chapter 3 the different Nmap host discovery methods/ping methods are ordered out, including ARP Ping, ICMP, TCP ACK Ping, TCP SYN Ping, and also how to suppress DNS and other functions in each scan type.

Chapters 4-7 kick off recon scanning, which is all about application fingerprinting, version detection, and IP Flag options. You review the different host and port options to fine tune your scans and bend them to your will. You also go through switches to exclude targets, input targets from a file, use random ports, specify source ports, force Ethernet frames, and force IP frames. Chapter 7 ends on output formats, which are insightful and pretty self-explanatory.

Chapters 8-11 go through “ninja” scanning: bringing everything together to achieve quiet and effective scan results. You learn to prioritize the noisiest scans and learn why they end up that way. This section covers the Nmap timing options, randomization, using decoys, fragmentation, and TTL. Nmap Secrets then takes a weird skip to “Nmap and Windows,” pros and cons, etc. Then it comes back to some negligible miscellaneous options. And finally it ends on real world Nmap scanning, cycling through scanning for malware, vulnerability assessments, policy compliance scanning, asset management, firewall auditing, and a small section on scanning an ever-evolving network called “Perpetual Network Auditing.”

Extras and Video Package: Messer’s book comes with a very handy Nmap cheat sheet and access to Messer’s webinars which have demonstrations of the most popular scans, very much like the video version of the course.

Quick Reference Guides

Webinar Screen Shot

Also note that the video is a play-by-play of every scan outlined in the book, with a brief packet capture in Wireshark for each scan as in the screen shot above. It is really nice to see the packets in action and the labs Messer has set up. It definitely helps get the concrete syntax engrained, but it comes at the cost of $197 versus $47.

Overview: Professor Messer’s Secrets of Network Cartography: A Comprehensive Guide to Nmap is a great resource for any information security professional. Clear graphics, notated packet captures, pros and cons for each scan, and practical applications of those scans all come together in a clear and easy to understand outline of Nmap.

What’s the catch?

Well, I’d hate to say it’s not up to date, because all the info is circa 2007, but Messer’s book is missing coverage of the newer features of Nmap like the NSE (Nmap Scripting Engine) and the new front end Zenmap GUI. This kind of omission is understandable for print versions of books. But being an eBook, I would have expected a faster update cycle.

And now for the burning questions:

Does Secrets of Network Cartography stack up to Fyodor’s book? In this reviewer’s opinion Messer’s book is second only to Fyodor’s Nmap Network Scanning. It has a range of education from absolute beginner to semi-advanced, and is well worth the price but, lacks the tiny bit extra that only the designer of the tool and (ethical) hacker can add. That being said, any IT shop would be wise to have them both.

Is the video companion worth the extra money? If you have the extra coin, I say go for it. But seeing as though times are tough and you do get free access to the webcast archives, penny pinchers can rest assured they’re not missing the boat by passing.

So overall, I’d give James “Professor” Messer’s Secrets of Network Cartography: A Comprehensive Guide to Nmap 4 out of 5 stars.

Jason Haddix is an IT Consultant and Security Blogger at http://www.securityaegis.com/. Jason has been working in information technology in one fashion or another for many years doing everything from admin work, component bench technician, and identity theft researcher. He is currently "in IT" at a Fortune 500 company. Jason is an auto-didactic polymath (constantly learning about everything he can) and has been reading, mapping, and planning out his future in IT security. Jason loves everything to do with (E)hacking, Social Engineering, the con community, et cetera. Jason's current projects include numberous reviews of current pentesting and incident handling teaching curriculums as well as his journey through the SANS certification paths.