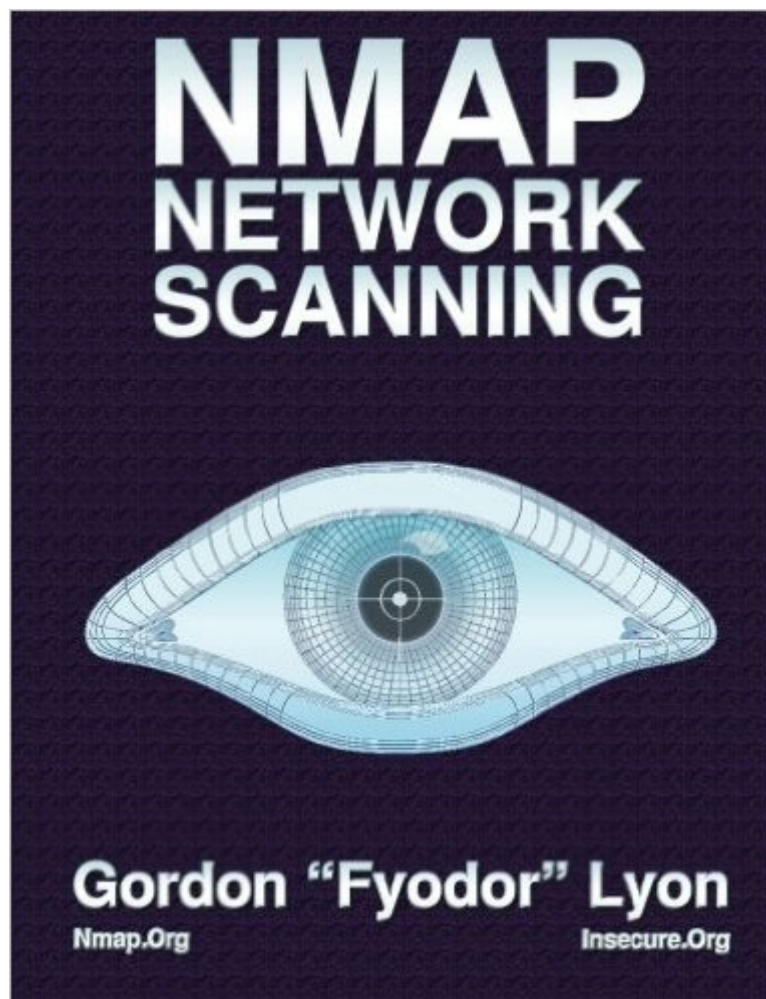# Nmap Network Scanning: The Official Nmap Project Guide To Network Discovery And Security Scanning

Synopsis

Nmap Network Scanning is the official guide to the Nmap Security Scanner, a free and open source utility used by millions of people for network discovery, administration, and security auditing. From explaining port scanning basics for novices to detailing low-level packet crafting methods used by advanced hackers, this book by Nmap's original author suits all levels of security and networking professionals. The reference guide documents every Nmap feature and option, while the remainder demonstrates how to apply them to quickly solve real-world tasks. Examples and diagrams show actual communication on the wire. Topics include subverting firewalls and intrusion detection systems, optimizing Nmap performance, and automating common networking tasks with the Nmap Scripting Engine. Visit http://nmap.org/book for more information and sample chapters.

Book Information

Paperback: 464 pages

Publisher: Nmap Project; 12.2.2008 edition (January 1, 2009)

Language: English

ISBN-10: 0979958717

ISBN-13: 978-0979958717

Product Dimensions: 7.4 x 1 x 9.7 inches

Shipping Weight: 2.2 pounds (View shipping rates and policies)

Average Customer Review: 4.8 out of 5 starsÂ Â See all reviewsÂ (77 customer reviews)

Best Sellers Rank: #20,731 in Books (See Top 100 in Books)   #11 inÂ Books > Computers & Technology > Certification > CompTIA   #16 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Administration   #22 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security

Customer Reviews

Earlier this year Fyodor sent me a pre-publication review copy of his new self-published book, Nmap Network Scanning (NNS). I had heard of Fyodor's book when I wrote my 3 star review of Nmap in the Enterprise in June, but I wasn't consciously considering what could be in Fyodor's version compared to the Syngress title. Although the copy I read was labelled "Pre-Release Beta Version," I was very impressed by this book. Now that I have the final copy (available from) in my hands, I am really pleased with the product. In short, if you are looking for *the* book on Nmap, the search is over: NNS is a winner.I've reviewed dedicated "tool" books before, including titles about Snort, Nessus, and Nagios. NNS dives into the internals of Nmap unlike any other title I've read. Without

Nmap author Fyodor as the author, I think any competitor would need to have thoroughly read the source code of the application to have a chance at duplicating the level of detail Fyodor includes in NNS.Instead of just describing how to use Nmap, Fyodor explains how Nmap works. Going even further, he describes the algorithms used to implement various tests, and why he chose those approaches. The "Idle Scan Implementation Algorithsm" section in Ch 5 is a great example of this sort of material. I will probably just refer students of my TCP/IP Weapons School class to this part of NNS when we discuss the technique!One of the best parts of NNS, mentioned but explained in no other text, is the Nmap Scripting Engine (NSE). Ch 9 is all about NSE, with a brief intro to Lua and excellent documentation of using and building upon NSE. Beyond this groundbreaking material readers will find many examples of Nmap case studies from users.

The 1962 song Wipe Out, with its energetic drum solo started, was the impetus for many people to take up playing the drums. Similarly, Nmap, the legendary network scanner, likely interested many in the art of hacking, and for some, started a career for security professionals and hackers. Nmap and its creator Fyodor need no introduction to anyone on Slashdot. With that, Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning, is a most useful guide to anyone interested in fully utilizing Nmap.One may ask, why spend $50 on this book, when the Nmap Reference Guide provides a significant amount of the basic information needed to use the tool, especially since the reference guide is both free, and well written. The reference guide is included in the book in chapter 15, and takes up 41 pages. And for those that are cash strapped, the free reference guide is the way to go.In addition, the web site for the book notes that about half of the content is available in the free online edition. The most useful information is in the book in chapters exclusive to the print edition, which includes Detecting and Subverting Firewalls and Intrusion Detection System, Optimizing Nmap Performance, Port Scanning Techniques and Algorithms, Host Discovery, and troubleshooting.The main benefit of the buying the book is that it has the collected wisdom of Fyodor's, in addition to numerous real-world scenarios, and Nmap commands not documented elsewhere. At over 400 pages, the books 15 chapters provide the reader with everything they need to know about using Nmap to the fullest.Chapter 1 starts with an overview of the history of Nmap and how it came to be.

I could summarize this book review by saying this is THE nmap reference book, what in itself would be an obvious conclusion I already expected before reading a single page, just by looking at the author name. Fyodor is the creator of nmap, a tool he has carefully fed and taken care of during all

these years, and slightly knowing him from the Honeynet project, I couldn't expect less."Nmap Network Scanning" is a masterpiece that teaches the reader the Art of Network Mapping and Scanning, and definitely, one of the best books I've read in years. Honestly, there are only a few minor things regarding network scanning you cannot accomplish with a single tool, the current nmap version. The book takes advantage of it.The official nmap reference guide is simply included on chapter 15, while the rest of the book steers the reader through the nifty art of network mapping and scanning. It disects the network scanning phases and techniques, describing the different options and tool arguments available throughout practical examples and real-world usage tips, here and there, that will improve all your scanning techniques. This is a never-ending book that took Fyodor 5 years to write, and it clearly spreads his experience testing and analyzing networks. This is specially true in the "Solution" section at the end of some chapters, where real-world scenarios are efficiently solved.Additionally, the book clearly pinpoints the limitations for the multiple platforms (eg. Windows vs Linux) and scenarios (eg. privileged vs non-privileged user) nmap can run on. Besides that, it summarizes most nmap internals without requiring you to dive deep into the source code, what is a challenge in itself.

<u>Download to continue reading...</u>

Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning Social Security & Medicare Facts 2016: Social Security Coverage, Maximization Strategies for Social Security Benefits, Medicare/Medicaid, Social Security Taxes, Retirement & Disability, Ser Project Management Using Microsoft Project 2013: A Training and Reference Guide for Project Managers Using Standard, Professional, Server, Web Application and Project Online Project Management: Secrets Successful Project Managers Know And What You Can Learn From Them: A Beginner's Guide To Project Management With Tips On Learning ... Project Management Body of Knowledge) Agile Project Management: Box Set - Agile Project Management QuickStart Guide & Agile Project Management Mastery (Agile Project Management, Agile Software Development, Agile Development, Scrum) Project Management: 26 Game-Changing Project Management Tools (Project Management, PMP, Project Management Body of Knowledge) Agile Project Management: An Inclusive Walkthrough of Agile Project Management (Agile Project Management, Agile Software Developement, Scrum, Project Management) Network Marketing Success Blueprint: Go Pro in Network Marketing: Build Your Team, Serve Others and Create the Life of Your Dreams (Network Marketing ... Scam Free Network Marketing) (Volume 1) CompTIA Security+ Guide to Network Security Fundamentals (with CertBlaster Printed Access Card) Agile Project Management: QuickStart Guide - The Simplified Beginners Guide To Agile Project

Management (Agile Project Management, Agile Software Development, Agile Development, Scrum) Agile Project Management: & Scrum Box Set - Agile Project Management QuickStart Guide & Scrum QuickStart Guide (Agile Project Management, Agile Software ... Scrum, Scrum Agile, Scrum Master) Agile Project Management: QuickStart Guide - The Complete Beginners Guide To Mastering Agile Project Management! (Scrum, Project Management, Agile Development) Kali Linux Network Scanning Cookbook Project Management: A Quick Start Beginner's Guide For The Serious Project Manager To Managing Any Project Easily Agile Project Management: Mastery - An Advanced Guide To Agile Project Management (Agile Project Management, Agile Software Development, Agile Development, Scrum) Project Management: A Quick Start Beginners Guide For The Serious Project Manager To Managing Any Project Easily! Network Marketing For Introverts: Guide To Success For The Shy Network Marketer (network marketing, multi level marketing, mlm, direct sales) Agile Project Management: For Beginners - A Brief Introduction to Learning the Basics of Agile Project Management (Agile Project Management, Agile Software Development, Scrum) Microsoft Project 2013, ConfiguraciÃƒÂ n: Configura bien el Project, evita contratiempos (Administrando Proyectos con Microsoft Project) (Spanish Edition) Network Marketing: Network Marketing Recruiting for Facebook: How to Find People to Talk to and What to Say When You Do (MLM Recruiting, Direct Sales, Network Marketing, Home Business)