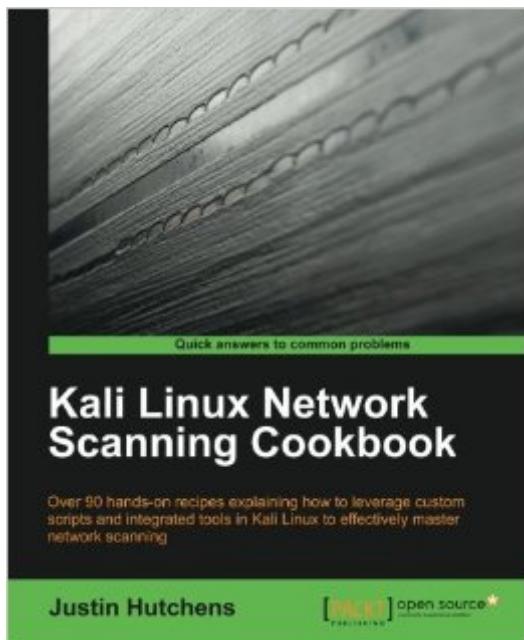


The book was found

Kali Linux Network Scanning Cookbook



Synopsis

Over 90 hands-on recipes explaining how to leverage custom scripts and integrated tools in Kali Linux to effectively master network scanning

About This Book Learn the fundamentals behind commonly used scanning techniques Deploy powerful scanning tools that are integrated into the Kali Linux testing platform A step-by-step guide, full of recipes that will help you use integrated scanning tools in Kali Linux, and develop custom scripts for making new and unique tools of your own

Who This Book Is For"Kali Linux Network Scanning Cookbook" is intended for information security professionals and casual security enthusiasts alike. It will provide the foundational principles for the novice reader but will also introduce scripting techniques and in-depth analysis for the more advanced audience. Whether you are brand new to Kali Linux or a seasoned veteran, this book will aid in both understanding and ultimately mastering many of the most powerful and useful scanning techniques in the industry. It is assumed that the reader has some basic security testing experience.

What You Will Learn Develop a network-testing environment that can be used to test scanning tools and techniques Understand the underlying principles of network scanning technologies by building custom scripts and tools Perform comprehensive scans to identify listening on TCP and UDP sockets Examine remote services to identify type of service, vendor, and version Evaluate denial of service threats and develop an understanding of how common denial of service attacks are performed Identify distinct vulnerabilities in both web applications and remote services and understand the techniques that are used to exploit them

In DetailKali Linux Network Scanning Cookbook will introduce you to critical scanning concepts. You will be shown techniques associated with a wide range of network scanning tasks that include discovery scanning, port scanning, service enumeration, operating system identification, vulnerability mapping, and validation of identified findings. You will learn how to utilize the arsenal of tools available in Kali Linux to conquer any network environment. You will also be shown how to identify remote services, how to assess security risks, and how various attacks are performed. This immersive guide will also encourage the creation of personally scripted tools and the development of skills required to create them.

Book Information

Paperback: 400 pages

Publisher: Packt Publishing - ebooks Account (August 26, 2014)

Language: English

ISBN-10: 1783982144

ISBN-13: 978-1783982141

Product Dimensions: 7.5 x 1 x 9.2 inches

Shipping Weight: 2.1 pounds (View shipping rates and policies)

Average Customer Review: 4.8 out of 5 stars See all reviews (15 customer reviews)

Best Sellers Rank: #129,846 in Books (See Top 100 in Books) #46 in Books > Computers & Technology > Operating Systems > Linux > Networking & System Administration #146 in Books > Computers & Technology > Networking & Cloud Computing > Network Security #401 in Books > Computers & Technology > Security & Encryption

Customer Reviews

Chapter 1: Getting StartedGood detailed coverage of setting up VMWare Player (Windows) or VMWare Fusion (Mac OS X). I would have seen the author at least cover VirtualBox as it works on Windows, OS X and Linux. The discussion on having vulnerable targets to work with covers Metasploitable which is an excellent choice. I am glad the point was stressed to not expose a Metasploitable system to any untrusted network. While I appreciate learning on Windows XP I would have expected a cook book to focus on either the latest Windows OS (8.1) or the most used Windows OS (Windows 7).
Chapter 2: DiscoveryFor some IT professionals the review of the OSI model is potentially redundant, but for many it is essential to truly understand the process of scanning a network. The discussion on layer 2 vs layer 3 vs layer 4 discovery was very clear and effective. I like the depth given for each of the chosen tools (Scapy, ARPing, Nmap, NetDiscover, Metasploit, ICMP ping, fping, and hping3). I have not made much use of Scapy, but I think I will be adding it to my tool bag due to the excellent python examples given making use of it.
Chapter 3: Port ScanningThis chapter was well done with coverage of Scapy, Nmap, Metasploit, Hping3, Dmitry and Netcat. Nmap is always a favorite of mine, but I was particularly impressed by the coverage of Scapy scripts used for scanning for zombies.
Chapter 4: FingerprintingThe tools covered in this chapter are Netcat, Python sockets, Dmitry, Nmap NSE, Amap, xProbe2, pOf, Onesixtyone and SNMPwalk. I think the best part about this chapter is the explanation of how the various programs identify (fingerprint) the target.

With the advent of the constantly connected computers (not only the Internet) the attack surface has increased immensely. At the same time the user machines became as powerful as the servers were. However, there was very little done to educate computer professionals to detect, prevent and cope intrusions or penetration attacks. Kali Linux Network Scanning Cookbook can serve very well as one to close the gap. A little on Kali Linux: it is a specialized distribution for penetration testing

and forensics purposes. It got a lot of traction lately in the penn-testing and security pros circles. As one of the less subtle features, it runs always under the super user rights and typically is installed as a VM guest OS.Let me tell, I was shocked the book counted 450 + pages! This is how much insight and tooling actually was created to harden your computing infrastructure (jargon used by security pros, meaning making your systems less vulnerable). It is hard to imagine an average practitioner would harness each in oneâ™s daily use, but I would to strive to. And I advocate looking in details into every applicable offering. Besides, the book uses a lot of Python code, thus the reader shall make sure one is familiar and feels comfortable performing some coding as well using basic text editors as Nano and VI. If the reader ever decides to prepare for the book I would recommend a good book on Learning Python and another from Packt on VI â“ Hacking VIM.Justin being a very experienced professional delivers the material at a very detailed level, in depth, with a lot of examples and in a very digestible format. If I am not mistaken several dozens of tools are covered in his book. I think this is unprecedented!

[Download to continue reading...](#)

Kali Linux Network Scanning Cookbook Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning Linux: Linux Command Line - A Complete Introduction To The Linux Operating System And Command Line (With Pics) (Unix, Linux kernel, Linux command line, ... CSS, C++, Java, PHP, Excel, code) (Volume 1) Kali Mantra Magick: Summoning The Dark Powers of Kali Ma (Mantra Magick Series) (Volume 2) LINUX: Easy Linux For Beginners, Your Step-By-Step Guide To Learning The Linux Operating System And Command Line (Linux Series) 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) Kali Linux: Windows Penetration Testing Kali Linux: Wireless Penetration Testing Beginner's Guide Setting Up A Linux Internet Server Visual Black Book: A Visual Guide to Using Linux as an Internet Server on a Global Network Linux For Beginners: The Ultimate Guide To The Linux Operating System & Linux Linux Administration: The Linux Operating System and Command Line Guide for Linux Administrators 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) Network Marketing For Introverts: Guide To Success For The Shy Network Marketer (network marketing, multi level marketing, mlm, direct sales) Network Marketing : How To Recruit Prospect Step By Step From Newbies To Professional in network marketing: network marketing, multiple marketing, MLM, ... Step from Newbies to Professional Book 5) CompTIA Linux+ Powered by Linux Professional Institute Study Guide: Exam

LX0-103 and Exam LX0-104 (Comptia Linux + Study Guide) Swim Through the Darkness: My Search for Craig Smith and the Mystery of Maitreya Kali Tantric Kali: Secret Practices and Rituals Kali Kaula - A Manual of Tantric Magick Twenty-Four Aspects of Mother Kali Design for 3D Printing: Scanning, Creating, Editing, Remixing, and Making in Three Dimensions

[Dmca](#)