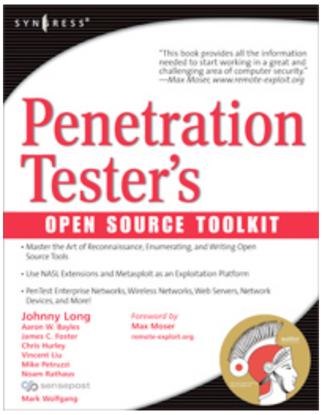
Daemon News Ezine BSD News BSD Mall BSD Support Forum BSD Advocacy BSD Updates

○ Web ○ daemonnews.org
Search

REVIEW: Penetration Tester's Open Source Toolkit

From Florian Khol



The book "Penetration Tester's Open Source Toolkit" (ISBN: 1597490210, available from Syngress Publishing) is a massive 750 page book accompanied by a bootable CD containing the Auditor Boot CD, a penetration testing Linux distro based on Knoppix.

The table of contents alone takes 12 pages. The list of authors is equally extensive, and reads like a yellow page listing for computer security, including but not limited to:

- Johnny Long, of "Google hacking" (also a Syngress publication) fame, and well known from talks and other publications.
- Aaron W. Bayles, CISSP, Senior Security Consultant at Sentigy Inc.
- James C. Foster, Executive Director of Global Product Development for Computer Sciences Corporation
- Chris Hurley, Senior Penetration Tester
and many more authors and contributors.

The Book approaches the art of penetration testing from an analytical viewpoint and contains tons of examples and actual hands on sessions.

The first few chapters all follow the same form:

Objectives, Approach, Core Technology, Open Source Tools and Case Studies - The Tools in Action

From the Table of Contents (only an excerpt):

Chapter 1 - Reconnaissance
Chapter 2 - Enumeration and Scanning
Chapter 3 - Introduction to Testing Databases
Chapter 4 - Web Server & Web Application Testing
Chapter 5 - Wireless Penetration Testing Using Auditor
Chapter 6 - Network Devices
Chapter 7 - Writing Open Source Security Tools
Chapter 8 - Nessus
...
Chapter 12 - Extending Metasploit I
Chapter 13 - Extending Metasploit II

Executive Summary

A great guideline for the newly interested in the covered topics, or even for experts looking for a handbook on extending their existing toolkits or techniques.

Sample Chapter

A sample chapter and the full Table of Contents are available at http://www.syngress.com/catalog/?pid=3330.

Detailed Review

The book covers all aspects of a penetration test, as one can see from the Table of Contents. In the Reconnaissance phase the reader is guided through intelligence gathering, e.g. getting a grasp of the organisational structure of the target, to footprinting IP addresses and DNS names, and double checking with such means as whois and traceroute if the IP address does belong to the target.

The Enumeration and Scanning chapter takes us through the basics of how scanning works to actually using nmap to do the scanning, and the commandline switches it takes. Issues that might crop up, like bandwidth

More Articles

- Book Review: Open Source Pen Testers Toolkit
- Daemon's Advocate
- BSDCan 2006 Friday Photos
- Installing BSD on IBM Netvista S40 - Part 3: DragonFly Installation
- BSDCan 2006 Photos
- AFS: network filesystem beyond NFS weaknesses
- Mastering FreeBSD and OpenBSD Security
- Installing BSD on IBM Netvista S40 - Part 2: FreeBSD Installation
- Interview with Diego Petteno, Gentoo/*BSD developer
- Installing BSD on IBM Netvista S40 - Part 1: FreeBSD Installation
- Interview with Jan Schaumann
- Interview with Theo de Raadt
- Book Review: Virtualization with VMware ESX Server
- Editorial: Not Quite Dead Yet
- The Design of OpenBGPd

constraints and timing problems, are equally covered as actually using the provided boot cd to do the hands on testing that is described. It covers banner grabbing and verifying as well as smb enumeration.

Testing databases educates the user from the ground up what databases are, what their use is, what the differences between major database vendor's solution are. It also explains the default users there are for most databases, and how to identify, asess, and exploit each given database.

Web Server and Web Application testing covers everything from forging cookie and form data with different opensource or free proxies, as well as actively scanning servers with such tools as nikto, wikto and nessus. It starts the reader off with a take on exploit basics, e.g. stack and heap based overflows. It goes on to actively showing the user an exploitable web application coded just for the purpose of demonstrating the bugs that web developers tend to miss. This chapter, I must say, is clearly my favorite, and it goes into great detail and explains on a very practical (hands on) basis the proceedings of finding the bug and exploiting it.

Wireless Penetration testing using Auditor does just what the packaging suggests. The user is taken from the theoretical weaknesses of wireless networks to the actual use of the well known tools such as kismet, wellenreiter and the likes of coWPAtty.

Chapter 6, Network Devices, takes us into the world of hacking networking gear, covering topics as Cisco IOS testing and SNMP loopholes.

Chapter 8 is an exemption, as it covers Nessus functionality and usage in very great detail.

Chapters 7 and 9-13 cover more advanced topics, taking the reader from actually coding security tools and basics of programming languages that can be used, to extending Nessus using NASL scripts and the like. The last two chapters take on the explanation and extension of the Metasploit Framework.

The expertise and detail enclosed in the book are well worth the price of having a bit of a mixed reading experience which comes with the multitude of contributors and authors covering such a mass of topics.

Recommendation:

I can heartily recommend the book to everyone inclined to learning their piece about penetration testing using open source tools, and to professionals that want a guidebook to pentesting and detailed extension handbook to Nessus and Metasploit.

Florian Kohl is a SysAdmin / NetworkAdmin / "it has buttons it uses electricity it's your job" kind of guy.

He's been a mac user since he could move a mouse, his first mac being a hand-me-down mac plus with an imagewriter attached to it. His first contact with Unix was OpenBSD, even before he touched a machine running windows.

BSD News

- PC-BSD 1.11 Released!
- Journaling UFS with gjournal.
- First Looks: A comparison of BSD live CDs
- Submit A News Item
- BSDCG: June Newsletter
- Roadmap Updated
- NetBSD Security Advisory: Sendmail malformed multipart MIME messages
- FreeBSD Security Advisory: Incorrect multipart message handling in Sendmail
- Macromedia Flash 7 plugin with Firefox