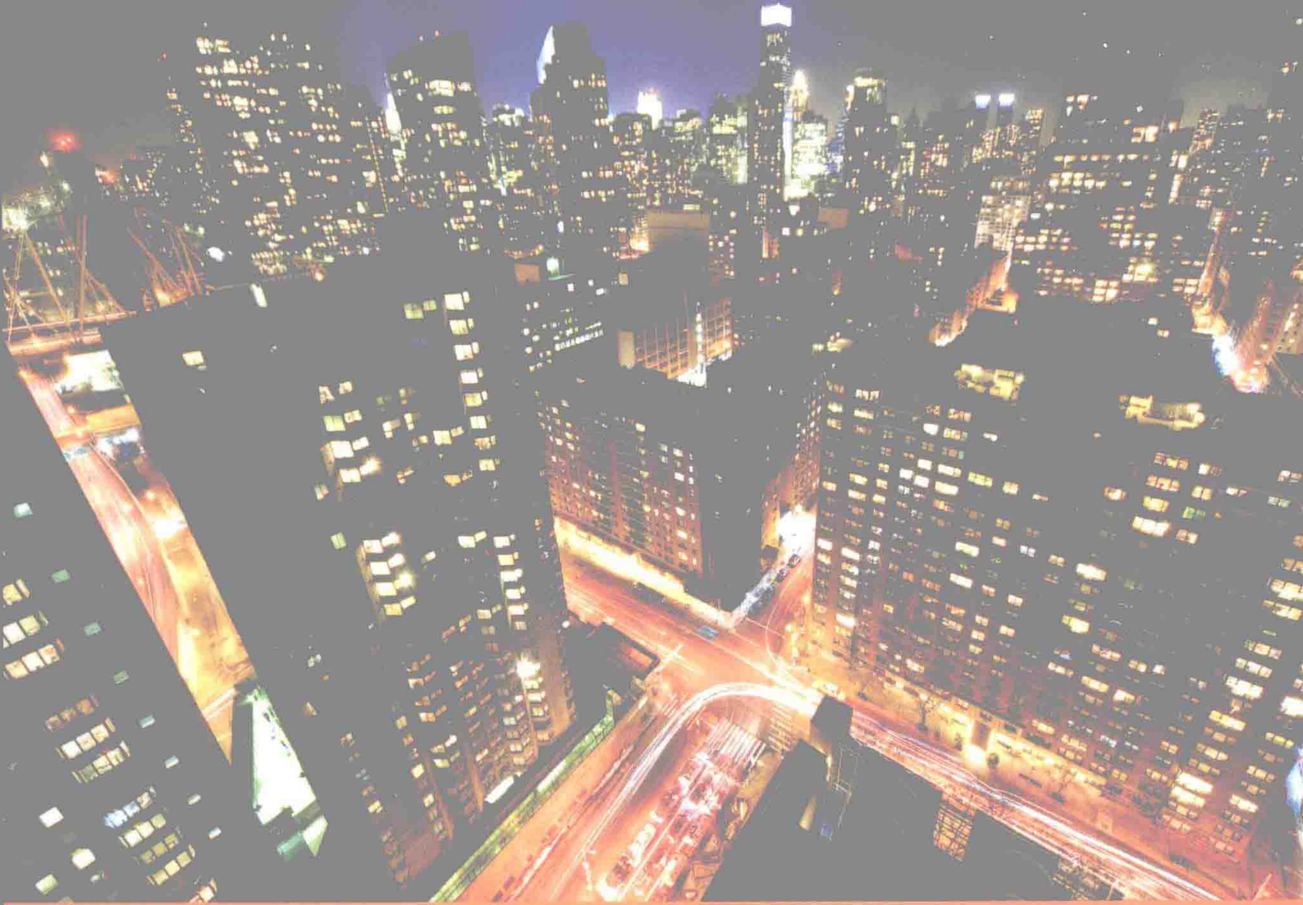

Community Experience Distilled

Building Virtual Pentesting Labs for Advanced Penetration Testing

Build intricate virtual architecture to practice any penetration testing technique virtually

Kevin Cardwell

[PACKT] open source*
community experience distilled
PUBLISHING

Building Virtual Pentesting Labs for Advanced Penetration Testing

Build intricate virtual architecture to practice any penetration testing technique virtually

Kevin Cardwell

[PUBLISHING] open source
community experience distilled

BIRMINGHAM - MUMBAI

Building Virtual Pentesting Labs for Advanced Penetration Testing

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing, and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

First published: June 2014

Production reference: 1130614

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.

ISBN 978-1-78328-477-1

www.packtpub.com

Cover image by Tony Shi (shihe99@hotmail.com)

Credits

Author
Kevin Cardwell

Reviewers
Praveen Darshanam
Steven McElrea
Sachin Raste
Abhinav Singh
Aaron M. Woody

Commissioning Editor
Kartikey Pandey

Acquisition Editor
Subho Gupta

Content Development Editor
Mohammed Fahad

Technical Editors
Tanvi Bhatt
Monica John

Copy Editors
Sayanee Mukherjee
Deepa Nambiar
Karuna Narayanan

Project Coordinator
Wendell Palmer

Proofreaders
Simran Bhogal
Maria Gould
Ameesha Green
Paul Hindle

Indexers
Hemangini Bari
Mariammal Chettiyar

Graphics
Abhinash Sahu

Production Coordinators
Aparna Bhagat
Nitesh Thakur

Cover Work
Aparna Bhagat

About the Author

Kevin Cardwell currently works as a freelance consultant and provides consulting services for companies all over the world. He developed the Strategy and Training Development Plan for the first Government CERT in the country of Oman and developed the team to man the first Commercial Security Operations Center there. He has worked extensively with banks and financial institutions throughout the Middle East, Africa, Europe, and the UK. He currently provides consultancy services to commercial companies, governments, major banks, and financial institutions across the globe. He is the author of the book *Backtrack – Testing Wireless Network Security, Packt Publishing.*

This book is dedicated to Loredana for her support during the countless long hours; Aspen, for the enjoyment she has provided as she became a young lady; my mother, Sally, for instilling in me the importance of reading; and my father, Darrell, for showing me an incredible work ethic. Without all of them, this book would not have been possible.

About the Reviewers

Praveen Darshanam has over seven years of experience in Information Security with companies such as McAfee, Cisco Systems, and iPolicy Networks. His core expertise and passions are Vulnerability Research, Application Security and Malware Analysis, Signature Development, Snort, and much more. He pursued a Bachelor of Technology degree in Electrical Engineering and a Master of Engineering degree in Control and Instrumentation from one of the premier institutes of India. He holds industry certifications such as CHFI, CEH, and ECSA. He is a known Ethical Hacking trainer in India. He also blogs at `http://blog.disects.com/`.

> I would like to thank my parents, sister, brother, wife, and son for their everlasting love, encouragement, and support.

Steven McElrea has been working in IT for over 10 years as a Microsoft Windows and Exchange Server administrator. Having been bitten by the security bug, he's been playing around and learning about InfoSec for several years now. He has a nice little blog (`www.kioptrix.com`) that does its best to show and teach newcomers the basic principles of information security. He is currently working in security professionally and he loves it. The switch to InfoSec is the best career move he has made.

> I would like to thank everyone around me for putting up with me over the years. Big thanks to Aaron Woody (`@shaisaint`) for all the great Twitter conversations over the last few months. A special thanks goes out to my parents; without them, I wouldn't be the person I am today.

Sachin Raste is a leading security expert with over 18 years of experience in the field of Network Management and Information Security. With his team, he has designed, streamlined, and integrated networks, applications, and IT processes for some of the big business houses in India, and has successfully helped them achieve Business Continuity. He has also reviewed the book *Metasploit Penetration Testing Cookbook, Packt Publishing*. He can be followed on twitter at `@essachin`.

> First and foremost, I'd like to thank my wife, my son, and my close group of friends, without whom everything in this world would have seemed impossible.
>
> I would also like to thank everyone at MalwareMustDie NPO, a group of White hat security researchers who tackle malware, for their immense inspiration and support.

Abhinav Singh is a young information security specialist from India. He has a keen interest in the field of Information Security and has adopted it as his full-time profession. His core work areas include malware analysis, network security, and system and enterprise security. He is also the author of the books *Metasploit Penetration Testing Cookbook* and *Instant Wireshark* published by Packt Publishing.

Abhinav's work has been quoted in several Infosec magazines and portals. He shares his day-to-day security encounters on `www.securitycalculus.com`. Currently, he is working as a cyber security engineer for JP Morgan.

You can contact him at `abhinavbom@gmail.com`. His Twitter ID is `@abhinavbom`.

Aaron M. Woody is a security consultant specializing in penetration testing, security operations development, and security architecture. He is a speaker and instructor and teaches hacking and security concepts. He is currently pursuing the OSCP certification to add to his more than 16 years of experience in teaching. Aaron is the author of the book *Enterprise Security – A Data-Centric Approach to Securing the Enterprise, Packt Publishing*.

He also maintains a blog at `www.datacentricsec.com`. He can be followed on Twitter at `@shaisaint`.

Table of Contents

Preface

This book will provide you with a systematic process to follow when building a virtual environment to practice penetration testing. Throughout the book, network architectures will be created that allow for the testing of virtually any production environment.

What this book covers

Chapter 1, Introducing Penetration Testing, provides an introduction to what pentesting is and an explanation that pentesting is a component of professional security testing, and it is a validation of vulnerabilities. This means "exploitation", and in most cases, in a contracted pentest, the client does not have a clear understanding of this.

Chapter 2, Choosing the Virtual Environment, discusses the different virtual environment platforms there are to choose from. We also look at most of the main virtual technology platforms that exist.

Chapter 3, Planning a Range, explains what is required to plan a test environment. We also discuss the process of searching and finding vulnerabilities to test and creating a lab environment to test a type of vulnerability.

Chapter 4, Identifying Range Architecture, defines the composition of the range and the process of creating the network structure. Following this, a number of different components are introduced and then connected to the structure.

Chapter 5, Identifying a Methodology, explores a sample group of a number of testing methodologies. The format and steps of this sample set will be presented so that as a tester, you can make a comparison and adapt a methodology.

Chapter 6, Creating an External Attack Architecture, builds a layered architecture and performs a systematic process and methodology for conducting an external test. Additionally, you will learn how to deploy protection measures and carry out testing to see how effective the protection measures are.

Chapter 7, Assessment of Devices, presents the challenges of testing devices. This section includes the techniques for testing weak filtering as well as the methods of penetrating the various defenses when possible.

Chapter 8, Architecting an IDS/IPS Range, investigates the deployment of the Snort IDS and a number of host-based security protections. Once deployed, a number of evasion techniques are explored to evade the IDS.

Chapter 9, Assessment of Web Servers and Web Applications, explores the installation of web servers and applications. You will follow a testing strategy to evaluate the servers and their applications.

Chapter 10, Testing Flat and Internal Networks, explores the process for testing flat and internal networks. The use of vulnerability scanners is explored and scanning with or without credentials is compared.

Chapter 11, Attacking Servers, identifies the methods we use to attack services and servers. The most common attack vector we will see is the web applications that are running on a web server.

Chapter 12, Exploring Client-side Attack Vectors, presents the main vectors of attack against the network, and that is from the client side. You will explore the methods that can be used to trick a client into accessing a malicious site.

Chapter 13, Building a Complete Cyber Range, is where you put all of the concepts together and create a range for testing. Throughout the chapter, you will deploy decoys and practice against them.

What you need for this book

The examples in the book use VMWare Workstation and Kali Linux predominantly. These are the minimum requirements needed. Additional software is introduced and references to obtain the software are provided.

Who this book is for

This book is for anyone who is working as or who wants to work as a professional security tester. The book teaches a foundation and systematic process of building a virtual lab environment that allows for the virtual testing of any environment that you may encounter in pentesting.

Conventions

In this book, you will find a number of styles of text that distinguish between different kinds of information. Here are some examples of these styles, and an explanation of their meaning.

Code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles are shown as follows: "In the metasploitable virtual machine, enter `sudo route add default gw 10.3.0.10` to add the route to the table."

A block of code is set as follows:

```
<IMG SRC="http://10.2.0.132/WebGoat/attack?Screen=52&menu=
900&transferFunds=4000"width="1" height="1"/>
```

Any command-line input or output is written as follows:

```
ip access-group External in
```

New terms and **important words** are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "Go to the Serversniff page and navigate to **IP Tools** | **TCP Traceroute**."

> Warnings or important notes appear in a box like this.

> Tips and tricks appear like this.

Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book—what you liked or may have disliked. Reader feedback is important for us to develop titles that you really get the most out of.

To send us general feedback, simply send an e-mail to `feedback@packtpub.com`, and mention the book title via the subject of your message.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide on `www.packtpub.com/authors`.