



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\*  
PUBLISHING community experience distilled

# 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

Copyright © 2014 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

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](http://www.packtpub.com)

Cover image by Tony Shi ([shihe99@hotmail.com](mailto:shihe99@hotmail.com))

# Credits

**Author**

Kevin Cardwell

**Project Coordinator**

Wendell Palmer

**Reviewers**

Praveen Darshanam

Steven McElrea

Sachin Raste

Abhinav Singh

Aaron M. Woody

**Proofreaders**

Simran Bhogal

Maria Gould

Ameesha Green

Paul Hindle

**Commissioning Editor**

Kartikey Pandey

**Indexers**

Hemangini Bari

Mariammal Chettiyar

**Acquisition Editor**

Subho Gupta

**Graphics**

Abhinash Sahu

**Content Development Editor**

Mohammed Fahad

**Production Coordinators**

Aparna Bhagat

Nitesh Thakur

**Technical Editors**

Tanvi Bhatt

Monica John

**Cover Work**

Aparna Bhagat

**Copy Editors**

Sayanee Mukherjee

Deepa Nambiar

Karuna Narayanan

# 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](http://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](http://www.securitycalculus.com). Currently, he is working as a cyber security engineer for JP Morgan.

You can contact him at [abhinavbom@gmail.com](mailto: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](http://www.datacentricsec.com). He can be followed on Twitter at @shaisaint.

# www.PacktPub.com

## Support files, eBooks, discount offers, and more

You might want to visit [www.PacktPub.com](http://www.PacktPub.com) for support files and downloads related to your book.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at [www.PacktPub.com](http://www.PacktPub.com) and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at [service@packtpub.com](mailto:service@packtpub.com) for more details.

At [www.PacktPub.com](http://www.PacktPub.com), you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.



<http://PacktLib.PacktPub.com>

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can access, read and search across Packt's entire library of books.

## Why subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print and bookmark content
- On demand and accessible via web browser

## Free access for Packt account holders

If you have an account with Packt at [www.PacktPub.com](http://www.PacktPub.com), you can use this to access PacktLib today and view nine entirely free books. Simply use your login credentials for immediate access.



# Table of Contents

<b>Preface</b>	<b>1</b>
<b>Chapter 1: Introducing Penetration Testing</b>	<b>5</b>
<b>Security testing</b>	<b>5</b>
Authentication	6
Authorization	6
Confidentiality	6
Integrity	7
Availability	7
Non-repudiation	7
<b>Abstract testing methodology</b>	<b>8</b>
Planning	8
Nonintrusive target search	9
Intrusive target search	14
Data analysis	21
Reporting	22
<b>Myths and misconceptions of pen testing</b>	<b>23</b>
<b>Summary</b>	<b>23</b>
<b>Chapter 2: Choosing the Virtual Environment</b>	<b>25</b>
<b>Open source and free environments</b>	<b>27</b>
VMware Player	27
VirtualBox	28
Xen	31
Hyper-V	32
vSphere Hypervisor	36
<b>Commercial environments</b>	<b>37</b>
vSphere	37
VMware Player Plus	38

XenServer	39
VMware Workstation	39
<b>Image conversion</b>	<b>47</b>
<b>Converting from a physical to virtual environment</b>	<b>49</b>
<b>Summary</b>	<b>50</b>
<b>Chapter 3: Planning a Range</b>	<b>51</b>
<b>Planning</b>	<b>51</b>
What are we trying to accomplish?	51
By when do we have to accomplish it?	52
<b>Identifying vulnerabilities</b>	<b>54</b>
Vulnerability sites	56
Vendor sites	76
<b>Summary</b>	<b>80</b>
<b>Chapter 4: Identifying Range Architecture</b>	<b>81</b>
<b>Building the machines</b>	<b>81</b>
Building new machines	82
Conversion	83
Cloning a virtual machine	83
<b>Selecting network connections</b>	<b>86</b>
The bridged setting	86
Network Address Translation	87
The host-only switch	89
The custom settings	90
<b>Choosing range components</b>	<b>93</b>
The attacker machine	93
Router	96
Firewall	107
Web server	114
<b>Summary</b>	<b>115</b>
<b>Chapter 5: Identifying a Methodology</b>	<b>117</b>
<b>The OSSTMM</b>	<b>117</b>
The Posture Review	121
Logistics	122
Active detection verification	122
Visibility Audit	122
Access verification	123
Trust verification	123
Control verification	124
Process verification	124

---

Configuration verification	124
Property validation	125
Segregation review	125
Exposure verification	125
Competitive intelligence scouting	126
Quarantine verification	126
Privileges audit	126
Survivability validation	127
Alert and log review	127
<b>CHECK</b>	<b>127</b>
<b>NIST SP-800-115</b>	<b>131</b>
The information security assessment methodology	134
Technical assessment techniques	135
Comparing tests and examinations	135
Testing viewpoints	136
Overt and covert	136
Offensive Security	141
Other methodologies	143
Customization	144
<b>Summary</b>	<b>145</b>
<b>Chapter 6: Creating an External Attack Architecture</b>	<b>147</b>
<b>Establishing layered architectures</b>	<b>147</b>
<b>Configuring firewall architectures</b>	<b>162</b>
<b>iptables</b>	<b>164</b>
Deploying IDS/IPS and load balancers	170
Intrusion Detection System (IDS)	171
Intrusion Prevention System (IPS)	178
Load balancers	179
Integrating web application firewalls	180
<b>Summary</b>	<b>184</b>
<b>Chapter 7: Assessment of Devices</b>	<b>185</b>
<b>Assessing routers</b>	<b>185</b>
<b>Evaluating switches</b>	<b>206</b>
MAC attacks	207
VLAN hopping attacks	208
GARP attacks	208
<b>Attacking the firewall</b>	<b>209</b>
<b>Identifying the firewall rules</b>	<b>213</b>
<b>Tricks to penetrate filters</b>	<b>221</b>
<b>Summary</b>	<b>228</b>

---

<b>Chapter 8: Architecting an IDS/IPS Range</b>	<b>229</b>
<b>Deploying a network-based IDS</b>	<b>230</b>
<b>Implementing the host-based IDS and endpoint security</b>	<b>239</b>
<b>Working with virtual switches</b>	<b>245</b>
<b>Evasion</b>	<b>248</b>
Determining thresholds	248
Stress testing	249
Shell code obfuscation	249
<b>Summary</b>	<b>252</b>
<b>Chapter 9: Assessment of Web Servers and Web Applications</b>	<b>253</b>
<b>Analyzing the OWASP Top Ten attacks</b>	<b>253</b>
Injection flaws	255
Broken authentication and session management	259
Cross-Site Scripting	263
Insecure direct object references	266
Security misconfiguration	270
Sensitive data exposure	270
Missing function-level access control	271
Cross-Site Request Forgery	272
Using known vulnerable components	274
Invalidated redirects and forwards	274
<b>Identifying web application firewalls</b>	<b>274</b>
<b>Penetrating web application firewalls</b>	<b>277</b>
<b>Tools</b>	<b>282</b>
<b>Summary</b>	<b>283</b>
<b>Chapter 10: Testing Flat and Internal Networks</b>	<b>285</b>
<b>The role of Vulnerability Scanners</b>	<b>286</b>
Microsoft Baseline Security Analyzer	286
Open Vulnerability Assessment Language	289
Scanning without credentials	293
Nessus	296
Scanning with credentials	299
<b>Dealing with host protection</b>	<b>304</b>
User Account Control	304
The host firewall	308
Endpoint protection	313
Enhanced Mitigation Experience Toolkit	313
<b>Summary</b>	<b>316</b>

---

<b>Chapter 11: Attacking Servers</b>	<b>317</b>
<b>Common protocols and applications for servers</b>	<b>317</b>
Web	318
File Transfer Protocol	318
Protocol research	320
Secure Shell	324
Mail	330
<b>Database assessment</b>	<b>333</b>
MSSQL	333
MySQL	339
Oracle	342
<b>OS platform specifics</b>	<b>344</b>
Windows legacy	344
Windows Server 2008 and 2012	345
Unix	345
Linux	346
MAC	347
<b>Summary</b>	<b>347</b>
<b>Chapter 12: Exploring Client-side Attack Vectors</b>	<b>349</b>
<b>Client-side attack methods</b>	<b>350</b>
Bait	350
Lure	350
<b>Pilfering data from the client</b>	<b>355</b>
<b>Using the client as a pivot point</b>	<b>359</b>
Pivoting	360
Proxy exploitation	365
Leveraging the client configuration	365
<b>Client-side exploitation</b>	<b>369</b>
<b>Binary payloads</b>	<b>376</b>
<b>Malicious PDF files</b>	<b>378</b>
<b>Bypassing antivirus and other protection tools</b>	<b>379</b>
<b>Obfuscation and encoding</b>	<b>381</b>
<b>Summary</b>	<b>384</b>
<b>Chapter 13: Building a Complete Cyber Range</b>	<b>385</b>
<b>Creating the layered architecture</b>	<b>385</b>
Architecting the switching	385
Segmenting the architecture	386
<b>Integrating decoys and honeypots</b>	<b>390</b>

---

<b>Attacking the cyber range</b>	<b>399</b>
<b>Recording the attack data for further training and analysis</b>	<b>400</b>
<b>Summary</b>	<b>401</b>
<b>Index</b>	<b>403</b>

---

# 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](mailto: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](http://www.packtpub.com/authors).