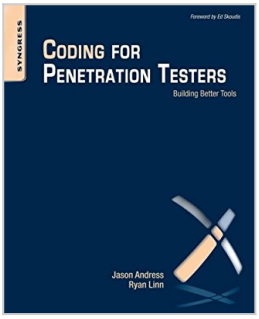

Coding for Penetration Testers: Building Better Tools

By Jason Andress, Ryan Linn

Coding for Penetration Testers: Building Better Tools By Jason Andress, Ryan Linn

Coding for Penetration Testers discusses the use of various scripting languages in penetration testing. The book presents step-by-step instructions on how to build customized penetration testing tools using Perl, Ruby, Python, and other languages. It also provides a primer on scripting including, but not limited to, Web scripting, scanner scripting, and exploitation scripting. It guides the student through specific examples of custom tool development that can be incorporated into a tester's toolkit as well as real-world scenarios where such tools might be used. This book is divided into 10 chapters that explores topics such as command shell scripting; Python, Perl, and Ruby; Web scripting with PHP; manipulating Windows with PowerShell; scanner scripting; information gathering; exploitation scripting; and post-exploitation scripting. This book will appeal to penetration testers, information security practitioners, and network and system administrators.

- Discusses the use of various scripting languages in penetration testing
- Presents step-by-step instructions on how to build customized penetration testing tools using Perl, Ruby, Python, and other languages
- Provides a primer on scripting including, but not limited to, Web scripting, scanner scripting, and exploitation scripting

Coding for Penetration Testers: Building Better Tools

By Jason Andress, Ryan Linn

Coding for Penetration Testers: Building Better Tools By Jason Andress, Ryan Linn

Coding for Penetration Testers discusses the use of various scripting languages in penetration testing. The book presents step-by-step instructions on how to build customized penetration testing tools using Perl, Ruby, Python, and other languages. It also provides a primer on scripting including, but not limited to, Web scripting, scanner scripting, and exploitation scripting. It guides the student through specific examples of custom tool development that can be incorporated into a tester's toolkit as well as real-world scenarios where such tools might be used. This book is divided into 10 chapters that explores topics such as command shell scripting; Python, Perl, and Ruby; Web scripting with PHP; manipulating Windows with PowerShell; scanner scripting; information gathering; exploitation scripting; and post-exploitation scripting. This book will appeal to penetration testers, information security practitioners, and network and system administrators.

- Discusses the use of various scripting languages in penetration testing
- Presents step-by-step instructions on how to build customized penetration testing tools using Perl, Ruby, Python, and other languages
- Provides a primer on scripting including, but not limited to, Web scripting, scanner scripting, and exploitation scripting

Coding for Penetration Testers: Building Better Tools By Jason Andress, Ryan Linn Bibliography

- Sales Rank: #949824 in Books
- Published on: 2011-10-07
- Released on: 2011-09-23
- Original language: English
- Number of items: 1
- Dimensions: 9.25" h x .73" w x 7.50" l, 1.35 pounds
- Binding: Paperback
- 320 pages

Editorial Review

Review

"This book is definitely not for rookie coders, but rather a good starting point for people with a medium level of programming experience. It is also not suited well as a reference to quickly look things up in. But if what you're looking for is a very practical guide with tons of pointers to further (and recommended) reading material and exercises Coding for Penetration Testers delivers what it promises."**--Computers and Security**

"Penetration testing is a profession that requires the mastery of dozens of tools; every job poses challenges that require these tools to be mixed, matched, and automated. The master penetration tester not only excels at using his or her toolbox, but also expands it with custom scripts and unique programs to solve the challenge of the day. This book provides a solid introduction to custom scripting and tool development, using multiple languages, with a penetration tester's goals in mind. This background can transform penetration testing from a manual, often repetitive task, to an efficient process that is not just faster, but also more accurate and consistent across large engagements."--**HD Moore, Metasploit Founder and CSO of Rapid7**

"Penetration testing requires that the tester understand the target as much as possible, and know how to perform various attacks while being as efficient as possible. Having the skill set to create and use a variety of scripts increases the penetration tester's efficiency and elevates him or her from the script kiddie to the professional realm. Ryan Linn and Jason Andress have created a guide that explores and introduces the techniques that are necessary to build the scripts used during a test. No matter the platform, this book provides the information required to learn scripting and become a world-class penetration tester. This is definitely a book that will remain close at hand for every test I perform!"--**Kevin Johnson, Senior Consultant, Secure Ideas**

"At 175 pages, the book does not kill many trees, but does give the reader an overview of all of the key principles around information security…For those looking to get their feet wet in the deep waters of information security, The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice is a great place to start."--**RSAConference.com**

"Overall this is an excellent book, which offers some clear and effective tutorials on the different languages and on efficient and effective penetration testing. It's highly recommended for any testers who want to broaden their skills and move to the next level."**--BCS.org**

From the Back Cover

Tools used for penetration testing are often purchased or downloaded from the Internet. Each tool is based on a programming language such as Perl, Python, or Ruby. If a penetration tester wants to extend, augment, or change the functionality of a tool to perform a test differently than the default configuration, the tester must know the basics of coding for the related programming language. ***Coding for Penetration Testers*** provides the reader with an understanding of the scripting languages that are commonly used when developing tools for penetration testing. It also guides the reader through specific examples of custom tool development and the situations where such tools might be used. While developing a better understanding of each language, the reader is guided through real-world scenarios and tool development that can be incorporated into a tester's toolkit.

About the Author
Jason Andress (CISSP, ISSAP, CISM, GPEN) is a seasoned security professional with a depth of experience in both the academic and business worlds. Presently he carries out information security oversight duties, performing penetration testing, risk assessment, and compliance functions to ensure that critical assets are protected. Jason has taught undergraduate and graduate security courses since 2005 and holds a doctorate in computer science, researching in the area of data protection. He has authored several publications and books, writing on topics including data security, network security, penetration testing, and digital forensics.

Ryan Linn (OSCE, GPEN, GWAPT) is a penetration tester, an author, a developer, and an educator. He comes from a systems administation and Web application development background, with many years of IT security experience. Ryan currently works as a full-time penetration tester and is a regular contributor to open source projects including Metasploit, The Browser Exploitation Framework, and the Dradis Framework. He has spoken at numerous security conferences and events, including ISSA, DEF CON, SecTor, and CarolinaCon.

Users Review

From reader reviews:

Morris Whitfield:

Playing with family in a park, coming to see the marine world or hanging out with buddies is thing that usually you may have done when you have spare time, after that why you don't try factor that really opposite from that. 1 activity that make you not experiencing tired but still relaxing, trilling like on roller coaster you already been ride on and with addition of information. Even you love Coding for Penetration Testers: Building Better Tools, you could enjoy both. It is good combination right, you still need to miss it? What kind of hangout type is it? Oh come on its mind hangout people. What? Still don't get it, oh come on its named reading friends.

Shelia Lopez:

You may get this Coding for Penetration Testers: Building Better Tools by go to the bookstore or Mall. Just simply viewing or reviewing it may to be your solve trouble if you get difficulties for the knowledge. Kinds of this guide are various. Not only by written or printed but can you enjoy this book by simply e-book. In the modern era including now, you just looking by your local mobile phone and searching what your problem. Right now, choose your own ways to get more information about your e-book. It is most important to arrange you to ultimately make your knowledge are still upgrade. Let's try to choose appropriate ways for you.

Elizabeth Daugherty:

Publication is one of source of expertise. We can add our information from it. Not only for students but additionally native or citizen want book to know the revise information of year for you to year. As we know those textbooks have many advantages. Beside we add our knowledge, can also bring us to around the world. Through the book Coding for Penetration Testers: Building Better Tools we can get more advantage. Don't someone to be creative people? To become creative person must choose to read a book. Only choose the best book that acceptable with your aim. Don't become doubt to change your life at this book Coding for

Penetration Testers: Building Better Tools. You can more desirable than now.

Marianne Button:

A lot of people said that they feel fed up when they reading a e-book. They are directly felt it when they get a half areas of the book. You can choose typically the book Coding for Penetration Testers: Building Better Tools to make your current reading is interesting. Your own skill of reading ability is developing when you such as reading. Try to choose simple book to make you enjoy to study it and mingle the feeling about book and reading through especially. It is to be initial opinion for you to like to open a book and read it. Beside that the book Coding for Penetration Testers: Building Better Tools can to be your new friend when you're experience alone and confuse using what must you're doing of these time.

Read Coding for Penetration Testers: Building Better Tools By Jason Andress, Ryan Linn for online ebook

Coding for Penetration Testers: Building Better Tools By Jason Andress, Ryan Linn Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Coding for Penetration Testers: Building Better Tools By Jason Andress, Ryan Linn books to read online.

Online Coding for Penetration Testers: Building Better Tools By Jason Andress, Ryan Linn ebook PDF download

Coding for Penetration Testers: Building Better Tools By Jason Andress, Ryan Linn Doc

Coding for Penetration Testers: Building Better Tools By Jason Andress, Ryan Linn Mobipocket

Coding for Penetration Testers: Building Better Tools By Jason Andress, Ryan Linn EPub

FNDV3RP095Z: Coding for Penetration Testers: Building Better Tools By Jason Andress, Ryan Linn