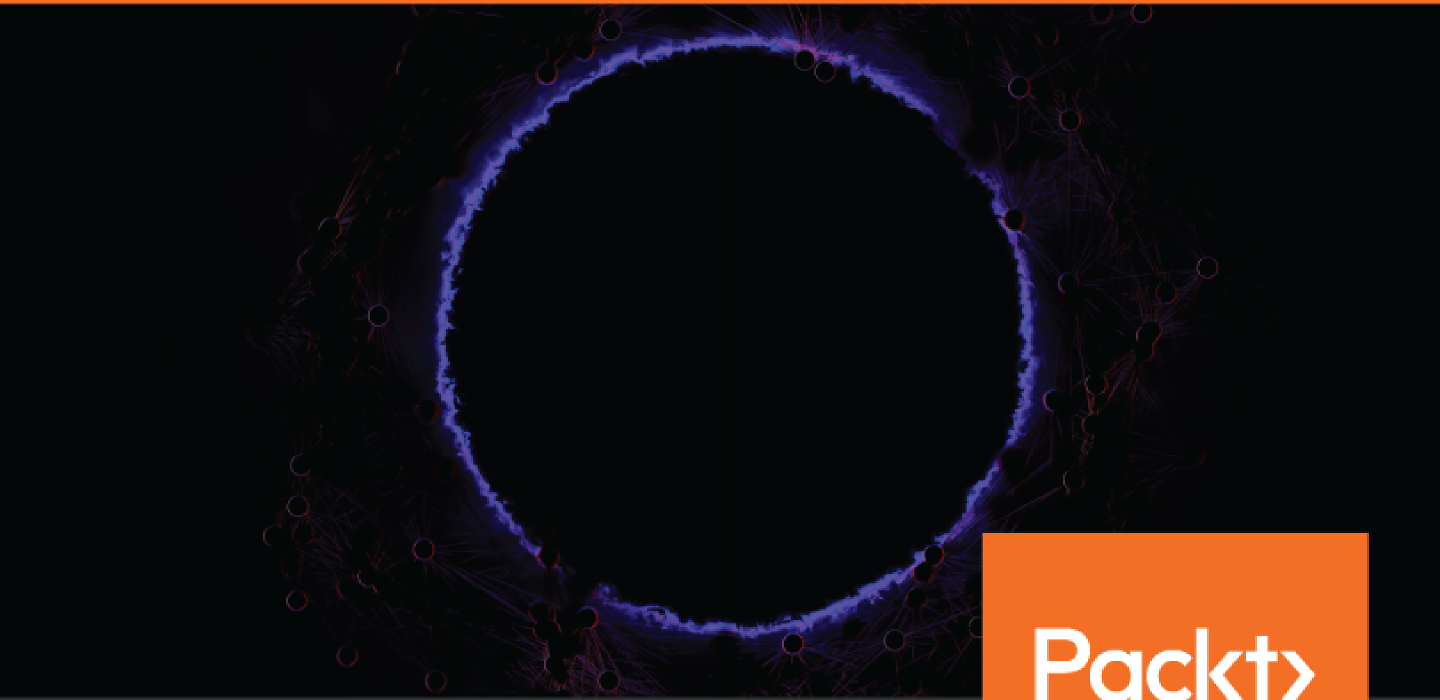
Hands-On Dark Web Analysis

Learn what goes on in the Dark Web, and how to work with it



Sion Retzkin

Packt
www.packt.com

Hands-On Dark Web Analysis

Learn what goes on in the Dark Web, and how to work with it

Sion Retzkin

Packt

BIRMINGHAM - MUMBAI

Hands-On Dark Web Analysis

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 or its dealers and distributors, will be held liable for any damages caused or alleged to have been 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.

Commissioning Editor: Gebin George
Acquisition Editor: Heramb Bhavsar
Content Development Editor: Ronn Kurien
Technical Editor: Prachi Sawant
Copy Editor: Safis Editing
Project Coordinator: Jagdish Prabhu
Proofreader: Safis Editing
Indexer: Rekha Nair
Graphics: Tom Scaria
Production Coordinator: Jyoti Chauhan

First published: December 2018

Production reference: 1241218

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

ISBN 978-1-78913-336-3

`www.packtpub.com`

Contributors

About the author

Sion Retzkin is an IT and security professional with over 20 years' experience in various technical and business roles. Sion was born in New York City, and has lived, studied, and worked internationally. Sion also delivers training to other professionals on the topics he's mastered, sharing his passion for security, ethical hacking, and information systems. With multiple certifications under his belt, Sion feels comfortable both in the boardroom, meeting customers, and working hands-on.

Today, he works at Pcysys, as director of customer success, which allows him to continue to do what he loves.

> *I would like to thank Meytal, my wife and love of my life, for putting up with long nights of writing and thinking (sometimes out loud) how I can make this book effective and interesting. To my sons, who loaned their father to this book, and for whom I wrote it, I love you. Also, thanks to my reviewer Rishalin Pillay for helping me, and to my editors in Packt, who offered ideas, improvements and encouragement, during my writing.*

About the reviewer

Rishalin Pillay, with in excess of 11 years of cybersecurity experience, has acquired a vast number of skills consulting for Fortune 500 companies while participating in projects performing tasks in network security design, implementation, and vulnerability analysis. He holds many certifications that demonstrate his knowledge and expertise in the cybersecurity field, such as CISSP, CCNP Security, CCSPA, MCSE, MCT, A+ and Network+

Rishalin currently works at a large-scale software company as a senior cybersecurity engineer.

Packt is searching for authors like you

If you're interested in becoming an author for Packt, please visit `authors.packtpub.com` and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Table of Contents

Preface

The World Wide Web is divided into three areas: the Surface Web, the Deep Web, and the Dark Web. The Deep Web and Dark Web are the two areas that are not accessible through general search engines or browsers. This provides several advantages, such as anonymity and privacy, but it also provides people performing illicit, illegal, or nefarious activities with the same benefits. IT and security professionals also gain benefits by accessing these areas.

This book will initially introduce you to the concept of the Deep Web and the Dark Web and will examine their significance. Then, we will deep dive into the recommended ways to access them, by using various operating systems and tools such as the Tor browser. We will also discuss what data can be obtained there, best practices for using the tools for the best effect, and who uses the Deep Web and the Dark Web.

By the end of this book, you will have hands-on experience of working with the Deep Web and the Dark Web.

Who this book is for

This book is aimed at IT and security professionals, security analysts, and any stakeholder interested in learning the concepts of the Deep Web and the Dark Web. Some technical acumen is necessary for the hands-on parts of this book, such as internet browsing, the concept and use of virtual machines, and installing operating systems. The book includes step-by-step instructions, with screenshots of all the hands-on chapters.

What this book covers

`Chapter 1`, *Understanding the Deep and Dark Web*, starts by looking at where it all started, and we will talk about the terminology—what is the Deep Web? What is the Dark Web? We will also talk about the difference between the Deep Web and the Dark Web, and examine the reason behind the names and what can be done there.

`Chapter 2`, *Working with the Deep Web*, discusses using the Deep Web and the Dark Web. For example, how to access the Deep Web and the Dark Web, and what really goes on there? How can there be so many sites out there? In this chapter, we'll discuss how the Deep Web and Dark Web are used.

`Chapter 3`, *The Future of the Dark Web*, covers the usage trends in the Dark Web. We will also talk about how it is used today and where will it go from here. We will learn about what to expect in the future from the Deep Web and the Dark Web. We will learn about the future benefits (or dangers) we can gain from the uncharted territory of the Dark Web.

`Chapter 4`, *Installing a Linux Virtual Machine (VM)*, explains how to install a Linux virtual machine.

`Chapter 5`, *Accessing the Dark Web with the Tor Browser*, will help you to learn about, install, and configure the Tor browser on a Linux distribution.

`Chapter 6`, *Installing Tails OS*, outlines another operating system that is useful for accessing the Deep Web—Tails OS. It is a live operating system that you can start on almost any computer from a USB stick or a DVD. In this chapter, we'll focus on installing Tails OS and accessing the Dark Web with it.

`Chapter 7`, *Installing Whonix*, covers another operating system that's worth mentioning: Whonix. Whonix is designed for advanced security and privacy. It's a heavily reconfigured Linux Debian that runs inside multiple virtual machines, providing a substantial layer of protection from malware and IP address leaks. Whonix is the only operating system designed to be run inside a VM and paired with Tor. In this chapter, we'll learn how to install and use Whonix to browse the Dark Web.

`Chapter 8`, *Installing Qubes OS*, covers a Xen-based operating system that is also considered extremely secure: Qubes OS, which will be the focus of this chapter. Qubes OS operates under the assumption that it has already been breached, so every application is run in its own virtual environment. In this chapter, we will learn how to install and use Qubes OS to access the Deep Web.

`Chapter 9`, *What Goes on in the Dark Web – Case Studies*, provides several examples of how the Dark Web is used in order to outline the dangers (and benefits) of going there. Anyone can access the Dark Web and, in this chapter, we will break down the types of people who access it, and why.

`Chapter 10`, *The Dangers of the Dark Web*, discusses the things that are lurking in the Dark Web. What are the dangers? How do we avoid them? These are probably the type of questions you've asked yourself when contemplating the Dark Web. Many people view the Dark Web as an evil place, teeming with malicious hooded hackers, just waiting for us to enter. In this chapter, we'll learn what the risks are in the Dark Web, and how to avoid them.

Chapter 11, *Using the Dark Web for Your Business*, moves on from who uses the Deep Web and Dark Web, and why. Now, let's learn how we can use them ourselves, to help us perform tasks, to help in our career, and more.

To get the most out of this book

You should have a USB stick and a computer you are willing to format, or a computer with enough resources to create virtual machines.

Download the color images

We also provide a PDF file that has color images of the screenshots/diagrams used in this book. You can download it here: https://www.packtpub.com/sites/default/files/downloads/9781789133363_ColorImages.pdf.

Conventions used

There are a number of text conventions used throughout this book.

CodeInText: Indicates code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles. Here is an example: "Double-click on the Start-tor-browser.desktop file to launch Tor Browser"

A block of code is set as follows:

```
html, body, #map {
 height: 100%;
 margin: 0;
 padding: 0
}
```

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

```
sudo apt install gnupg
```

Bold: Indicates a new term, an important word, or words that you see onscreen. For example, words in menus or dialog boxes appear in the text like this. Here is an example: "Now, plug in the second USB stick, go to **Applications** | **Tails** | **Tails Installer** (in Tails OS), and install Tails on it."

Warnings or important notes appear like this.

Tips and tricks appear like this.

Get in touch

Feedback from our readers is always welcome.

General feedback: If you have questions about any aspect of this book, mention the book title in the subject of your message and email us at `customercare@packtpub.com`.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you would report this to us. Please visit `www.packt.com/submit-errata`, selecting your book, clicking on the Errata Submission Form link, and entering the details.

Piracy: If you come across any illegal copies of our works in any form on the Internet, we would be grateful if you would provide us with the location address or website name. Please contact us at `copyright@packt.com` with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit `authors.packtpub.com`.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions, we at Packt can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about Packt, please visit `packt.com`.

Disclaimer

The information within this book is intended to be used only in an ethical manner. Do not use any information from the book if you do not have written permission from the owner of the equipment. If you perform illegal actions, you are likely to be arrested and prosecuted to the full extent of the law. Packt Publishing does not take any responsibility if you misuse any of the information contained within the book. The information herein must only be used while testing environments with proper written authorizations from appropriate persons responsible.