

Assessment

Chapter 1: Understanding the Deep and Dark Web

1. Surface Web, Deep Web, Dark Web
2. Search engines
3. True
4. Private databases, News headlines, Academic journals
5. Darknets, Overlay networks, Content accessible using specialized software
6. Journalism, Sale of an exploit tool you have developed
7. Bypassing country censorships, Buying counterfeit money

Chapter 2: Working with the Deep Web

1. The privacy and anonymity are defined as follows:
 - **Privacy** can be defined as a state in which a person (or a corporate entity) can hide information about themselves from others. This can be done for various reasons, which ultimately don't matter. The idea is that it's possible, or at least should be. This is becoming enforced by laws, such as GDPR, or any number of privacy acts and laws
 - **Anonymity**, can be described as hiding a persons true identity from others without hiding or censoring their activities.
2. The three main cryptocurrency transaction methods are as follows:
 - **Finalize Early**: Is a payment method, in which a vendor requires receipt of payment before dispatching the purchased goods. The risk is on the buyer's end, but it also expedites the transaction due to little or no risk on the vendor's side (this method is the least secure for the buyer)
 - **Escrow**: Is a payment method in which a Dark Web market will generate a bitcoin address to which the buyer transfers the payment. The market holds the buyer's money and pay's the vendor only after the buyer marks the order as complete. (Moderately Secure)

- **Multiple Signature Escrow:** Also called multisig, this payment method generates multiple keys for the bitcoin transaction and payment release process. The multisig can be either 2 out of 2 or 2 out of 3, where 2 of 3 provides the most security for three keys - the market's key, the vendor's key and the buyer's key. The keys are:
 - **2-of-2 Multisig:** Market public key, vendor public key
 - **2-of-3 Multisig:** Market public key, vendor public key + customer public key
3. The Dark Web search websites are as follows:
- Ahmia
 - Torch
 - DuckDuckGo
4. Almost everything you might do on the Surface Web (including Browsing, Email, Blogging, Forums, Financial Transacting)

Chapter 3: The Future of the Dark Web

1. Three improvements in Tor are:
 - Host websites anonymously and privately.
 - Onion domain names will include more characters.
 - The network will randomly assign the relays that each onion service contacts.
2. Dark Web markets are:
 - Hansa
 - Agora
 - OpenBazaar
 - Silk Road
3. Main proposed future changes in the Dark Web are:
 - The UI of applications designed to access the Dark Web, such as Tor, are becoming more user friendly
 - Enhanced security, privacy and anonymity
 - Making the Dark Web more mainstream

Chapter 4: Installing a Linux Virtual Machine (VM)

1. An open source, free OS, with an emphasis on relatively easy customization and security (among other features).
2. A distro (or distribution) is a version or flavor of Linux. The differences in distros mainly revolve around desktop interfaces, included software and technology, intended use, and other aspects. There is no best distro, but rather the best distro for you. Remember to try out several until you find the one that best fits your requirements and temperament.
3. Linus Torvalds

Chapter 5: Accessing the Dark Web with Tor Browser

1. Four recommendations for safe use of Tor Browser are:
 - Don't torrent over Tor.
 - Don't enable or install browser plugins.
 - Use HTTPS versions of websites.
 - Don't open documents downloaded through Tor while online.
2. Tor Browser is based on Firefox browser.
3. The following is the command:

```
./start-tor-browser.desktop
```

Chapter 6: Installing Tails OS

1. The Linux software installation requirements for Tails OS are as follows:
 - Debian 9 and higher
 - Ubuntu 16.04 and higher
 - Linux Mint 18 and higher
2. The Terminal command that starts the Tails Installer application is:

```
sudo apt install tails-installer
```

3. The Tails OS hardware installation requirements are as follows:
 - A 64-bit x86-64 compatible processor (except for PowerPC or ARM)
 - 2 GB of RAM
 - A way to boot either from a DVD or USB flash drive

Chapter 7: Installing Whonix

1. The other operating system is designed to work with Whonix are as follows:
 - Qubes OS
 - Windows
 - Ubuntu Linux
 - Tails
2. Whonix is unique as:
 - Its architecture consist of two virtual machines, one acting as the secure and anonymous gateway, while the other functions as the user's desktop OS.
 - All traffic is routed through Tor, by default.
 - Whonix comes with anonymity and privacy focused applications installed by default.

Chapter 8: Installing Qubes OS

1. Qubes is unique as, it is based on the concept of isolation, where each application, hardware and session exist in different virtual machines, hence isolating them from one another, but still providing the user with a smooth, unified interface.
2. Each qube has its own window, and the windows have different color borders, to display the different level of security, and qube, being used.
3. The hypervisor platform that allows Qubes to create its qubes is: Xen

Chapter 9: What Goes on in the Dark Web - Case Studies

1. The Silk Road
2. General Data Protection Regulation
3. Dr. Fernando Caudevilla
4. Pulitzer

Chapter 10: The Dangers of the Dark Web

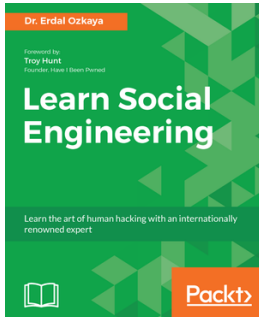
1. Malware and Tor botnets
2. NASA
3. Following are the metrics you should use to verify to make sure a Dark Web market is legitimate:
 - Multisig, Escrow, Finalize early
 - Anonymity and security
 - Reviews
 - Help and support
 - Uptime Status

Chapter 11: Using the Dark Web for Your Business

1. Operation Bayonet
2. Threat Intelligence
3. All A, B, C

Another Book You May Enjoy

If you enjoyed this book, you may be interested in these another book by Packt:



Learn Social Engineering Erdal Ozkaya

ISBN: 978-1-78883-792-7

- Learn to implement information security using social engineering
- Learn social engineering for IT security
- Understand the role of social media in social engineering
- Get acquainted with Practical Human hacking skills
- Learn to think like a social engineer
- Learn to beat a social engineer

Leave a review - let other readers know what you think

Please share your thoughts on this book with others by leaving a review on the site that you bought it from. If you purchased the book from Amazon, please leave us an honest review on this book's Amazon page. This is vital so that other potential readers can see and use your unbiased opinion to make purchasing decisions, we can understand what our customers think about our products, and our authors can see your feedback on the title that they have worked with Packt to create. It will only take a few minutes of your time, but is valuable to other potential customers, our authors, and Packt. Thank you!

Index

2

2-of-2 Multisig 30

2-of-3 Multisig 30

5

51% attack 30

A

active instances directory
reference 17

Ahmia 33

B

Bitcoin

used, for performing illegal sales on Dark Web
147, 148

Bitmessage Mail Gateway 37

block reward 30

business companies examples

Academic Index 173

DeepDyve 172

JSTOR 176

Law Library of Congress 175

PubMed 174

C

criminals

about 18

counterfeit goods 20, 21

drugs and illegal substances 18

hackers 22, 23

stolen information 21

cryptocurrency transaction methods, Dark Web

about 29, 33, 36

Escrow 30

Finalize Early (FE) 29

Multiple Signature Escrow 29

CryptoDog 38

D

Dark Web market

risk, minimizing 161

Dark Web search engines

Candle 92

Grams 92

Haystak 92

Not Evil 92

Tor Onionland 92

Torch 92

Dark Web

about 15, 17

accessing, with Qubes OS 131

advantages 133

browsing, considerations 31

criminals 18

dangers 162, 164, 166

disadvantages 134

forums sites 39

illegal sales, using Bitcoin 147, 148

journalism 17

law enforcement 17

markets 46, 47, 49, 51, 53

privacy 18

privacy, maintaining 26, 27

public interest 56, 57

Silk Road 149

terrorism 150

TOR Project 53, 54

transacting on 28

Deep Web

about 12, 14

currency 44

- future 43, 44
- DeepDotWeb 39
- Drug Enforcement Administration (DEA) 178
- DuckDuckGo 34

E

- European Economic Area (EEA) 143
- European Union (EU) 143

F

- features, Tails OS
 - AppArmor confinement 95
 - HTTPS Encryption 95
 - Torbutton 95

G

- GNOME Disks 99
- GNU Privacy Guard (GPG) 80

H

- Hypertext Transfer Protocol (HTTP) 10

I

- internet of Things (IoT) 10
- Internet Service Providers (ISPs) 170
- internet
 - origin 7, 9, 10, 12
- Intrusion Detection Systems (IDS) 165
- Invisible Internet Project (I2P) network 15, 47

K

- kill switch 63

L

- Linux VM
 - executing, from USB flash drive 74, 75
 - installing 63, 66, 72
 - tasks 73
 - using 63, 64, 66, 68, 69, 70
- Linux
 - advantages 61
 - overview 61
 - Tails OS, downloading 97
 - Tor, installing 79

- Logical Volume Management (LVM) 69

M

- miners 30
- multisig 30

N

- Network Access Control systems (NACs) 170
- Network Control Protocol (NCP) 9
- notEvil 33

O

- Onion Mail 38
- onion websites
 - Adland website 136
 - Energy Control website 142
 - EU GDPR website 144
 - Facebook onion site 135
 - Global Voices website 138
 - Hidden Answers website 146
 - Human Rights website 138
 - Rising Voices website 141
 - SecureDrop website 141
 - WikiLeaks website 145
- online scams
 - about 153, 157, 159
 - Evolution Marketplace 158, 161
 - fake IDs 155
 - Hidden Wiki 154
- Operation Onymous 149
- orphaned blocks 30

P

- Personal Package Archive (PPA) 101
- Personally Identifiable Information (PII) 162

Q

- qubes 123
- Qubes OS
 - about 123
 - hardware requisites 126
 - installation process 127, 129, 130
 - installing, reference 125
 - label 124

used, for accessing Dark Web 131

R

Rufus

reference 126

RVI

reference 111

S

Scriptmail 36

security domain 124

SoylentNews 40

T

Tails OS

about 94

downloading 97

downloading, in Linux 97

downloading, in Windows 97

installation prerequisites 96

installing 98

installing, from command line 101, 103, 104, 107

installing, in Fedora 99

installing, in Red Hat 99

installing, on Windows 98

Tails

about 31

reference 97

The Amnesic Incognito Live System (Tails) 94

Tor (The Onion Router)

about 78

and I2P comparison, reference 15

installing, entirely via Terminal 88

installing, on Linux 79, 80, 82, 83, 85, 87

installing, via Terminal 87

reference 79

Tor bridge relay

reference 89

Tor Browser

using, with Whonix 120, 121

Tor Links 35

Tor Project

about 53

recommendations 91

reference 89

Transport Control Protocol/Internet Protocol (TCP/IP) 7

tumblers 28

U

Ubuntu Desktop Edition

reference 63

Uniform Resource Locators (URLs) 10

USB flash drive

Linux VM, executing from 74, 75

users, Dark Web

business companies 171

cybersecurity professionals 179

IT professionals 170

law enforcement agencies 176, 177

military organizations 178

V

Virtual Private Network (VPN) 89

VirtualBox

download link 112

W

Whonix

about 109

benefits 110

download link 112

installation 111, 112, 115, 117, 118

prerequisites 111

Tor Browser, using with 120, 121

Wikileaks 40

Windows

Tails OS, downloading 97

Tails OS, installing 98

World Wide Web 10

Z

zero-day attacks 123