

Mastering Open Source Threat Analysis Strategies

*Strategic approaches, practical insights,
and case studies for effective cyber security*

Vishal Rai



www.bpbonline.com

First Edition 2024

Copyright © BPB Publications, India

ISBN: 978-93-55516-398

All Rights Reserved. No part of this publication may be reproduced, distributed or transmitted in any form or by any means or stored in a database or retrieval system, without the prior written permission of the publisher with the exception to the program listings which may be entered, stored and executed in a computer system, but they can not be reproduced by the means of publication, photocopy, recording, or by any electronic and mechanical means.

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

To View Complete
BPB Publications Catalogue
Scan the QR Code:



www.bpbonline.com

Dedicated to

*The unwavering support of my family and
the invaluable contributions of the publications support team*

About the Author

Vishal Rai has done B.Sc. and Masters in Mathematics, A-Level, MCA, Cyber Law (Symbiosis, Pune), AWS Solutions Architect and multiple certifications related to database and networking. He has worked as a Jr. Consultant (Incident Response)/Sr. System Administrator/Project Associate/Trainer in Govt./Private organizations. He also has more than 10 years of experience in various domains like Mathematics, Database, Networking, Cyber Security and Virtualization etc. Along with this, he deployed the Lab for Cyber Security Training using Virtualization, and trained Govt. Employee of various organizations related to cyber security.

The author has experience in the area of Information Security, System administration and process advocacy, along with live experience in maintenance/implementation of various organizational level policies, and network administration of more than 600 nodes. He has worked in the field of lab designing, information security policies designing/implementation, making presentation to the big audience.

Vishal is well versed with most of the latest software productions in the field of virtualization, setting up various organization level information network setups, guides. His work expertise also includes Deployed Moodle Server (E-Learning) & Integrate with BigBlueButton with the help of programming team (Video Conferencing System). Alongwith this, he has designed, installed and configured VMware ESXi, with vSphere 5.x/6.x environments with Virtual Center management, Consolidated Backup, DRS, HA, vMotion and VMware Data. He has previously authored “Expert Linux Administrator Guide” published by BPB Publications.

About the Reviewer

Ayushi Shukla is a Senior Cybersecurity professional with over seven years of experience in Threat Intelligence, OSINT Investigation, Vulnerability Assessment and Cybersecurity Product Solutioning. Ayushi started her journey with the Offensive Security domain and then navigated to the Defensive Security. Her experience includes working closely with the stakeholders, advising them on advanced threat mitigation strategies, and security best practices while conducting security assessments and investigations. Ayushi, an advisory board member for the GIAC, holds a bachelor's degree in Computer Science and Engineering and has several professional certifications to her credit like CISSP, GCTI, ISO 27001 and CEH. Ayushi is an avid reader and often engages herself in mentoring upcoming grads in the field of cybersecurity. When she is not being the guardian of the digital realm, you may find her seeking pleasure in nature and music.

Acknowledgement

I am deeply thankful to my family for their unwavering encouragement throughout the book-writing journey. Gratitude extends to the educational course and supportive companies that facilitated my learning of web scraping tools, with a special acknowledgment for the behind-the-scenes support. Furthermore, my appreciation goes to the BPB Publications team for their steadfast support, providing both time and flexibility to complete and publish the book. This approach proved crucial in delving into the diverse problem classes within image processing without overwhelming the content with excessive volume.

Finally, I extend my thanks to my brother who has supported me to complete the research work directly or indirectly.

Preface

There is a rising trend in cyberspace where cyber criminals are trying to contact vulnerable people, causing a sense of threat or fear. The impact of cybercrime can be as severe as physical offenses, even though the cyber criminal is not physically visible and their location may be unknown. Internet and intranet exploitations can result in extortion, lottery scams, credit card scams, etc. This is due to the lack of proper organizational structure to counter cyber threats effectively. Therefore, law enforcement agencies, citizens, and educational institutions, should keep updating themselves with new technologies. This will help them understand the possibilities that may be created by criminals and how they can be used as tools for fighting cyber crime.

To handle the increasing volume of cyber crimes and its complexity, it is necessary that corporates, police, judiciary and people be sensitized about cyber crime related problems. On the other hand, cyber forensics is also important in terms of evidence gathering, creation and presentation purposes to solve cyber crime cases. Internationally, cyber law has evolved into a distinct legal field aimed at addressing cybercrime, enhancing the capabilities of cyber experts and investigators in effectively combating cybercriminal activities.

In this book, we have discussed various cyber crimes with the help of examples, along with discussing the I.T Act. We have also explained how to setup cyber lab using open source softwares. Furthermore, this book will provide you with some critical aspects of cyber crime and investigation processes.

Chapter 1: Setting up OSINT Environment – Open Source Intelligence (OSINT) is a technique used to describe the search, collection, analysis, and use of information from open sources, about a particular target. The target may be cyber criminal/cyber terrorist/public enemy. In other words, OSINT refers to all the information that is available to the general public. The investigation through OSINT requires proxy identity, hence, in this chapter, we have given an introduction and showed how to setup OSINT lab for investigation.

Chapter 2: Secure Browsers – Concealing digital identity is essential for investigations using OSINT. There are multiple techniques available in OSINT to hide a person's digital identity. Keeping this in view, Chapter 2 explains how to secure the web browser using ad-ons and in-built feature of web browser. It will also equip you with hiding digital identity, such IP address, geo-location etc.

Chapter 3: Exploring OS Security – Operating system is the core part for communication devices. Without it, you cannot share data globally or locally. OS security means protecting the OS from threats, viruses, worms, malware or remote hacker intrusions. This chapter discusses OS security, encompassing all preventive-control techniques which safeguard any computer assets capable of being stolen, edited or deleted if OS security is compromised.

Chapter 4: Online Privacy and Security – Privacy is very important when you are working as an OSINT investigator. Most companies are selling user data to advertisers, making it very likely that your data will fall into the wrong hands at some point. However, there is no one best tool for privacy. This chapter will cover the best way to boost your online privacy, i.e., using a combination of tools.

Chapter 5: Tail OS in Use – According to Tail OS community, Tails is a portable operating system that protects against surveillance and censorship. In other words, Tail OS can be used to access the internet while keeping your identity anonymous. In this chapter, we have explained how to use Tail OS for tracing cyber criminal footprint.

Chapter 6: Using Tor Browser – Torbrowser is used to hide the user's IP address. It is a useful tool for a cyber investigator to track the presence of a cyber criminal on various social media platforms. This is also used by hackers and cyber criminal to access the dark web. In this chapter, we have explained how to use Torbrowser and its features.

Chapter 7: Advanced Search Tools – The pages that belong to the dark web cannot be discovered by a simple search. The number of pages on these websites continually changes according to many factors, hence, Google and other search engines cannot index the entire web. Therefore, the user must know how to use advanced searching technique by using OSINT which is discussed in this chapter.

Chapter 8: Sock Puppet Accounts – Sock puppets are fake social media accounts used for OSINT investigation. This account can be used by law enforcement agencies, police, and even hackers. The objective of creating sock puppets account is to hide the digital identity of users such as real name and geo-location. In this chapter, we have explained how to create sock puppets accounts for OSINT investigation.

Chapter 9: Exploring Footprinting – Digital footprints include user logins identity such as IP address, geolocation, and visited website. An example of a digital footprint may be browsing history, likes, text messages, search history, tagged photos, and videos, basically anything that leaves a digital trace that may be linked back to users. You can review digital footprint by using privacy setting of the web browser. The digital foot print is also known as digital shadow and is unique. In this chapter, we have explained footprinting based on scenarios such as private networks and public networks to clear the fundamentals. We have also described how to use OSINT tools to gather information about the remote target.

Chapter 10: Investigating E-mails – In this chapter, we have explained how to analyze e-mail headers in technical and non-technical ways. We have described phishing e-mail on the basis of OSINT tools. We have also explained how the law enforcement agency gathers the information from ISPs as well as the role of CERT-IN which is the apex agency of Govt. of India, working in the field of cyber security.

Chapter 11: Utilizing Social Media – In this chapter, we have explained how to create an anonymous social media account and then use the same to locate a target on available social media platforms using OSINT tools. We have also explained how to fetch the social media ID along with its date of creation.

Chapter 12: Tracking Family and Friends – In this chapter, we have explained how to search a person using OSINT tools. Some search engines explained in this chapter work better in some countries like the USA, UK, and more. Do check if your country supports the tool, before buying a paid subscription.

Chapter 13: Mobile Identity Search – Mobile identity is related to data from mobile network operators, such as a subscriber's mobile phone number, name and addresses. When you forensically examine the suspicious digital device, such as mobile phone, it will provide a lot of information related to suspect such as the geo-location of suspect at the time of crime etc. We can say that mobile identity is a digital identity. In this chapter, we have explained how to search for a person using OSINT tools.

Chapter 14: Mining Online Communities – The online or internet community is a group of people with a shared interest or purpose who communicate with each other digitally. Online communities have their own set of guidelines. The primary difference between an online community and social media is that the online community caters to an audience with a specific objective and social media is related to broad audiences. Some online communities are not indexed by search engines. Hence, it may be used by cyber criminals to pass the information. In this chapter, we have explained all these things using OSINT.

Chapter 15: Investigating Domain and IP – In layman’s language, the website is also known as a domain name. DNS and IP Address collectively can tell us about subscriber’s information such as IP address, geo-location and payment details. In case of threatening e-mails, we have to investigate DNS and IP addresses to determine who is behind the illegal act. In order to retrieve an IP address from some Internet Service Providers (ISP) it will require warrant, or court order of the company for information. In this chapter, we have explained from scratch to the advanced level, how the domain name works and what IP address works behind a specific domain name, registrar, registrant, and IP Address providers.

Chapter 16: Detection of Data Leaks – Data leaks can cause companies to lose millions of dollars and their reputation. In this chapter, we have explained various OSINT tools to detect the data leaks. We have also discussed how to find data breaches using social medial platforms.

Chapter 17: Understanding Encryption and Digital Certificates – The learning objective for this chapter is to understand the fundamentals of encryption, symmetric, asymmetric, hashers, SSL, TLS, certificates, SSL stripping, and the weaknesses inherent in encryption. The objective of this chapter is to explain digital certificates along with its security risk and how to mitigate it.

Chapter 18: Access Fake News – In this chapter, we have discussed how to detect fake news. We have also explained topics like, what is fake news, how to identify it, why detect fake news and the efforts of various organisations towards tackling the issues of fake news.

Chapter 19: Reverse Image Search – Reverse image search is a technology that takes an image file as input and returns an output related to the image. Search engines that offer reverse image capability include Google, TinEye, Bing, Yandex, Baidu etc. In this chapter, we have explained cropped reverse image searching. After reading this chapter, you will be able to detect the differences between morphed and real images.

Chapter 20: Geo-location – In this chapter, we have explained how to use online maps such as google, yandex, bing , mapillary and many more. The aerial maps are helpful when you are trying to know about the street or other location. This is useful when law enforcement agencies want to move in a particular street/location for investigation purposes.

Chapter 21: Identify Real Images – In this chapter, we have explained how to detect websites for sharing photo and reveal the meta data of the photo such as longitude, latitude etc. We have also explained the default extension used by cameras when you capture the objects.

Chapter 22: Use of Aadhaar and Social Security Number – With the crime rates increasing day-by-day, governments have assigned a unique identification to each citizen that can help law enforcement agency track criminals. and cyber criminals. In this chapter, we have discussed the use of Aadhar, and Social Security Number.

Chapter 23: Tracking Fraud SMS – SMS services are used by various organizations to promote their product. Schools/colleges are also using SMS to provide information related to students' enrolment/examinations. This is the positive use of SMS services. In this chapter, we will understand how law enforcement agencies find who is behind a cyber crime by tracking a fraudster/ malicious user's SMS sent to victims.

Coloured Images

Please follow the link to download the
Coloured Images of the book:

<https://rebrand.ly/fcw7v2n>

We have code bundles from our rich catalogue of books and videos available at **<https://github.com/bpbpublications>**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Did you know that BPB offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.bpbonline.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at :

business@bpbonline.com for more details.

At **www.bpbonline.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 BPB books and eBooks.

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 **business@bpbonline.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 **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights 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.

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 BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

<https://discord.bpbonline.com>



Table of Contents

1. Setting up OSINT Environment.....	1
Introduction.....	1
Structure.....	1
Objectives.....	1
Introduction to OSINT	1
Setting up the virtual lab for OSINT.....	2
Creating snapshots for VMs.....	6
Introduction to Linux command line.....	10
<i>About console.....</i>	<i>11</i>
<i>webHTTrack website copier</i>	<i>12</i>
<i>Metagoofil</i>	<i>13</i>
<i>SpiderFoot.....</i>	<i>15</i>
<i>theHarvester</i>	<i>18</i>
Antivirus	19
VPN and its uses.....	19
Lab using Proton VPN	19
Conclusion.....	21
Multiple choice questions.....	22
Answers	22
2. Secure Browsers	23
Introduction.....	23
Structure.....	23
Objectives.....	23
Introduction to privacy	24
Security versus privacy.....	24
Introduction to web browsers.....	25
Configuring web browser.....	25
Choice of browser for OSINT.....	30
Installation of extensions for browsers.....	30
Overview of extensions	31
<i>uBlock origin.....</i>	<i>31</i>
<i>Firefox containers</i>	<i>38</i>
<i>Installation process of multi-containers</i>	<i>39</i>

Copy selected links	43
Scenario for social media account	45
Solution using Trace Lab	45
Bulk Media Downloader	46
EXIF Viewer	46
Using TraceLab	47
User-agent switcher	49
Security	52
Conclusion	52
Multiple choice questions	53
Answers	53
3. Exploring OS Security	55
Introduction	55
Structure	55
Objectives	55
Operating system to OSINT	55
OS hardening	56
Disable Distributed Link Tracking	57
Disabling account information access for apps	58
Verification of results	67
User Account Control	67
Disable unnecessary services	68
Disabling IP helper	69
BIOS security	70
Disabling system booting from USB/DVD/CD or any external devices	70
Protecting the Grub	71
OS updates from trusted sources	72
Stopping/disabling unnecessary services in Linux	73
Closing the open ports	74
Securing Secure shell	74
Enabling SELinux	74
Disabling the IPv6	75
Disabling tracking in Linux	75
Privacy and tracking	75
Conclusion	78
Multiple choice questions	78
Answers	79
References	79

4. Online Privacy and Security	81
Introduction	81
Structure	81
Objectives	81
Introduction to VPN	81
<i>Configuring Windows for VPN</i>	<i>82</i>
<i>OpenVPN</i>	<i>84</i>
<i>Probabilistic approach to choose VPN</i>	<i>84</i>
Configuring web browsers	84
<i>Updating the Chrome browser</i>	<i>86</i>
<i>Disable/remove the unwanted extensions</i>	<i>86</i>
<i>Disable/remove the unwanted apps</i>	<i>87</i>
<i>Cleaning the browsing history</i>	<i>88</i>
<i>Securing the site settings such as camera location</i>	<i>89</i>
<i>Chrome internals</i>	<i>92</i>
<i>About iknowwhatyoudownload.com</i>	<i>97</i>
<i>Finding the torrent activity in an organization</i>	<i>99</i>
<i>Gathering information from various ISPs</i>	<i>99</i>
<i>Information gathering steps</i>	<i>100</i>
Configuring uBlock Origin	100
Introduction to containerization	102
Password manager	104
Conclusion	106
Multiple choice questions	107
Answers	107
5. Tail OS in Use	109
Introduction	109
Structure	109
Objectives	109
Introduction to Tail OS	110
Installation requirement for Tail OS	110
<i>Downloading Tails OS</i>	<i>110</i>
Installing Tail OS	111
<i>Tails OS on VirtualBox</i>	<i>112</i>
Overview of Tails OS tools	117
Tor Browser	118

<i>Metadata cleaner</i>	120
<i>Image viewer</i>	123
<i>GtkHash</i>	124
<i>GUI of GtkHash</i>	126
<i>KeePassXC</i>	128
OnionShare	133
<i>Receiving files using OnionShare</i>	137
HTTPS Everywhere	139
Thunderbird	143
Electrum wallets	148
Using Tail OS.....	148
Uninstalling Tails OS.....	148
Uncensored and anonymous internet	149
Conclusion.....	150
Multiple choice questions.....	150
Answers	151
6. Using Tor Browser	153
Introduction.....	153
Structure.....	153
Objectives.....	154
Introduction to Tor Project	154
How Tor works	154
Tor features	155
Configuring Tor Browser	155
Tor node list	159
<i>Displaying guard node</i>	162
<i>Investigation point of view</i>	162
Introduction to deep web	163
Introduction to dark web.....	163
<i>Investigation point of view</i>	167
Deep web versus dark web	168
Steps to access the dark web	169
Tor over VPN.....	169
VPN over Tor.....	170
Tor versus VPN	170
Proton Mail	171
Verifying IP related to TOR.....	172

Conclusion	172
Multiple choice questions.....	172
Answers	173
7. Advanced Search Tools.....	175
Introduction.....	175
Structure.....	175
Objectives.....	175
Introduction to search engines.....	176
Google searching methods	176
<i>File type search operator</i>	177
<i>Hyphen search operator</i>	178
<i>InURL operator</i>	179
<i>Google alert in investigation</i>	179
<i>Google Image</i>	180
About DuckDuckGo.....	181
Google versus DuckDuckGo.....	182
Searches using Tor	182
Torrent sites and searches.....	183
Private search engines.....	184
<i>I Search From</i>	185
<i>Keywordtool.io</i>	186
Yandex and its operators	187
<i>Plus operator</i>	187
<i>Minus operator</i>	187
<i>Quotation marks operator</i>	188
<i>URL operator</i>	188
<i>Site operator</i>	188
<i>Host operator</i>	189
<i>Title operator</i>	189
Conditions to trust on search results	189
<i>Facts about Tor configuration file</i>	192
<i>Verification of assigned country codes/IP address</i>	192
FTP searches	193
<i>FTP connection modes</i>	193
Bing	196
Conclusion	196
Multiple choice questions.....	196

Answers	197
References	197
8. Sock Puppet Accounts	199
Introduction	199
Structure	199
Objectives	199
Introduction to sock puppets	199
Purpose of sock puppets	200
Procedure to create sockpuppets	200
<i>About the websites receive-sms-online.info</i>	<i>202</i>
Searching people using sockpuppets	203
<i>Approach to finding the suspects using foreign virtual numbers</i>	<i>203</i>
<i>Detecting fake Facebook profiles using sock puppet</i>	<i>204</i>
Investigating the suspect's profile	205
Conclusion	205
Multiple choice questions	205
Answers	206
References	206
9. Exploring Footprinting	207
Introduction	207
Structure	207
Objectives	207
Introduction to footprinting	208
Robots.txt file	213
website mirroring tools	213
<i>Website Copier tools</i>	<i>216</i>
<i>Analysis of fraudulent websites</i>	<i>220</i>
Extracting links from website	223
Checking hidden link of websites	225
Checking the technology used in website	226
<i>OpenCorporates</i>	<i>227</i>
website certificate information	232
Checking malicious websites	236
Checking defaced websites	237
Netcraft	238
Conclusion	239

Multiple choice questions.....	239
Answers	240
References	240
10. Investigating E-mails	241
Introduction.....	241
Structure.....	241
Objectives.....	241
Introduction to e-mail	242
Common e-mail protocols	242
Introduction to open relay servers	242
Introduction to phishing and spoofing.....	244
<i>Phishing techniques</i>	244
<i>Objective behind phishing</i>	244
<i>Technical terms used as per Indian Cyber Law</i>	245
<i>Types of phishing</i>	246
<i>Detecting phishing e-mails</i>	246
Introduction to e-mail header	246
<i>Analysis of e-mail header</i>	247
<i>Case 1: e-mail sent using VPN</i>	255
<i>E-mail header analysis using online tools</i>	265
<i>Time overview</i>	267
<i>Description</i>	268
<i>Received details</i>	268
<i>List of public IP addresses</i>	269
Scenario for e-mail phishing	270
Procedure for getting registrant information	276
The simplest ways to identify a fraudulent e-mail	276
Role of the Indian Computer Emergency Response Team	277
Guidelines for intermediary.....	277
E-mail usage policy and responsibilities.....	277
Precautions for e-mails.....	278
Conclusion	278
Multiple choice questions.....	279
Answers	279
11. Utilizing Social Media	281
Introduction.....	281

Structure.....	281
Objectives.....	281
Introduction to social media	281
<i>Facebook tricks</i>	282
<i>Facebook profile searching</i>	284
<i>Searching Facebook ID and its date</i>	285
<i>Extraction of friend list from Facebook</i>	285
OSINT tools for X and WhatsApp	288
OSINT tools for other social media platforms.....	298
How Law Enforcement Agency works	299
Securing social media account.....	303
Conclusion.....	303
Multiple choice questions.....	303
Answer	304
12. Tracking Family and Friends.....	305
Introduction.....	305
Structure.....	305
Objectives.....	305
Introduction to people's search engine	305
<i>TruthFinder</i>	307
<i>True People Search</i>	307
<i>Fast People Search</i>	308
<i>FamilySearch</i>	308
<i>Spytox</i>	308
<i>Family tree</i>	308
<i>Spokeo</i>	309
<i>Whitepages</i>	309
Step-by-step data collection and analysis using OSINT	309
Conclusion.....	314
Multiple choice questions.....	314
Answers	314
13. Mobile Identity Search.....	315
Introduction.....	315
Structure.....	315
Objectives.....	315
OSINT for phone numbers.....	315

<i>Truecaller</i>	318
<i>Phone validator</i>	319
<i>Spy Dialer</i>	319
<i>PhoneInfoga</i>	319
Central Equipment Identity Register	326
<i>Steps to block stolen mobile numbers using CEIR</i>	327
<i>Steps to unblock mobile numbers using CEIR</i>	328
<i>Steps for IMEI verification</i>	329
Websites for telephone numbers	330
FCC ID search	331
Conclusion	332
Multiple choice questions	332
Answers	333
14. Mining Online Communities	335
Introduction	335
Structure	335
Objectives	335
Introduction to online communities	336
Types of online communities	336
Reddit	338
Hacker news	342
websites	343
Types of investigation	346
e-Auction	349
FakeSpot	349
Pinterest	350
Conclusion	351
Multiple choice questions	351
Answers	352
References	352
15. Investigating Domain and IP	353
Introduction	353
Structure	353
Objectives	353
Introduction to domain name	353
<i>Root domain</i>	354

<i>Top-level domain</i>	354
<i>Second level domain</i>	354
How DNS works	354
<i>DNS zones</i>	355
<i>Web-based tools for DNS lookup</i>	358
Introduction to public IP address	363
<i>Public IP address verses private IP address</i>	363
<i>Registrar, registrant, registry, ISP, and NetNames</i>	366
Whois history and reverse Whois	367
<i>Reverse name server lookup</i>	371
<i>IP address to geolocation</i>	372
DNS spy	372
DNS leaks	373
Additional OSINT tools for DNS	374
<i>Dnslytics</i>	377
<i>Domainiq</i>	378
Conclusion	378
Multiple choice questions	379
Answers	379
16. Detection of Data Leaks	381
Introduction	381
Structure	381
Objectives	381
Introduction to data leaks and breaches	381
Data breaches versus data leaks	390
OSINT tools to detect data leaks	390
Online tools related to data leaks	396
Data leakage prevention	397
<i>Leaked credential</i>	397
Conclusion	398
Multiple choice questions	398
Answers	399
References	399
17. Understanding Encryption and Digital Certificates	401
Introduction	401
Structure	401

Objectives.....	401
Introduction to encryption	402
Types of encryptions	403
Introduction to the hash function.....	405
Digital signature	405
<i>E-mail communication</i>	406
<i>Document signing</i>	406
<i>Online transactions</i>	406
Digital certificate.....	410
Secure Sockets Layer certificates	411
The function of the certification authority	412
<i>Root Secure Sockets Layer certificates</i>	412
<i>Intermediate certificate</i>	413
Introduction to SSL and TLS	416
Introduction to HTTP and HTTPS	416
Introduction to steganography	417
Scenario for steganography.....	419
OSINT for Secure Socket Layer server test	421
Certificate fingerprint.....	421
Conclusion	422
Multiple choice questions.....	422
Answer	423
18. Access Fake News	425
Introduction.....	425
Structure.....	425
Objectives.....	425
Introduction to fake news.....	425
Fake news and its related areas	426
Detecting fake news	426
Social media fact check addresses	430
Conclusion	431
Multiple choice questions.....	431
Answers	432
19. Reverse Image Search	433
Introduction.....	433
Structure	433

Objectives.....	433
Objectives of reverse image searching.....	433
Reverse image searching using scenario.....	434
Reverse image searching using Google.....	435
Yandex reverse image searching.....	436
Cropped image searching.....	439
Steps to download bulk images.....	441
Conclusion.....	443
Multiple choice questions.....	443
Answer	444
20. Geo-location.....	445
Introduction.....	445
Structure.....	445
Objectives.....	445
Google Maps.....	445
Location using GPS coordinates.....	448
How to use Zoom Earth.....	451
<i>Bing Maps</i>	451
Land Viewer	453
Wikimapia.....	454
Zillow	455
Mapbox	455
Flightradar24 Map.....	456
Submarine Cable Map.....	460
Conclusion.....	461
Multiple choice questions.....	461
Answers	462
21. Identify Real Images	463
Introduction.....	463
Structure.....	463
Objectives.....	463
Google Images.....	464
Bing Images	465
Yandex Images	466
TinEye.....	466
EXIF data.....	468

EXIF viewer	470
Forensically	472
Difference checker	475
Downloading videos from different channels.....	478
Searching video on the basis of text.....	479
Bypassing age and country restrictions.....	480
Conclusion	481
Multiple choice questions.....	482
Answers	482
22. Use of Aadhaar and Social Security Number.....	483
Introduction.....	483
Structure.....	483
Objectives.....	483
Introduction to Aadhaar	484
Linking Aadhaar to mobile number	485
How to check fake Aadhaar numbers	486
Aadhaar helpline to complain about fake Aadhaar number	487
Locking/ unlocking of Aadhaar numbers	488
Social security number.....	489
Conclusion	490
Multiple choice questions.....	490
Answers	491
23. Tracking Fraud SMS.....	493
Introduction.....	493
Structure.....	493
Objectives.....	493
Fundamentals of Short Message Service	493
Telecom Regulatory Authority of India guidelines	495
Steps to trace the SMS providers	496
Conclusion	499
Multiple choice questions.....	499
Answers	500
Index.....	501-508

CHAPTER 1

Setting up OSINT Environment

Introduction

Open-source Intelligence (OSINT) is a technique to describe the search, collection, analysis, and use of information from open sources about a particular target. The target may be a cyber-criminal, a cyber-terrorist, or a public enemy. In other words, OSINT refers to all the information that is available to the general public. This information can be used for intelligence gathering. The investigation through OSINT requires an anonymous identity. Hence, in this chapter, we have explained the introduction as well as how to set up an OSINT lab for investigation.

Structure

In this chapter, we will cover the following topics:

- Introduction to OSINT
- Setting up a virtual lab for OSINT
- Creating snapshots for VMs
- Introduction to Linux command line
- Antivirus
- VPN and its uses
- Lab using proton VPN

Objectives

After reading this chapter, the reader will be able to understand the open-source intelligence tools and techniques and learn about setting up a lab using an open-source operating system, basic operating system commands, and its file system, along with the lab using a virtualization platform (virtual box).

Introduction to OSINT

OSINT is the collection and analysis of data gathered from open sources, that is, publicly available sources (the sources may be websites/newspapers/others) to produce meaningful/actionable intelligence. The intelligence agencies use OSINT to track events, for example, weapons systems, public enemies, terrorists, cybercriminals, war-like situations, and so on. These are the targets of interest. Hence, OSINT is low-risk, cheap, and often highly effective. OSINT is completely legal because it only uses publicly available information through open sources. In

other words, it does not include information that is stored within an organization's database. A hacker uses OSINT to gather information before launching an attack on the target. Some of the OSINT sources are as follows:

- News and media
- Literature
- Social media
- Court filings
- Arrest records
- Public surveys
- Telephone directories
- Census data
- System vulnerability data
- Dark web
- Deep web

Online media and search engines make OSINT faster and easier, and social media is the most effective medium for gathering information about individuals/organizations. The OSINT investigator must have strong searching skills. Today, you can find most of the data on social media platforms using advanced searching techniques. The hackers and intelligence agencies view social media profiles on sites such as LinkedIn, Facebook, and Instagram and then take decisions accordingly based on the intelligence they have collected.

Setting up the virtual lab for OSINT

In the following section, the documentation part is taken from the open-source virtual box website <https://www.virtualbox.org>. The *VirtualBox* provides the virtualization environment to set up the lab. The step-by-step process is given as follows:

The hardware/software requirements to set up the OSINT lab process are as follows:

- **Recommended hardware for Oracle VirtualBox**
 - o **Memory:** 1.5 GB or 4 GB with Oracle XE
 - o **Processor Type:** 32bit or 64-bit
 - o **Processor speed:** 1.83 GHz
 - o **Hard disk:** 5 GB
- **Recommended hardware for Linux-based operating system**
 - o If hardware is running a 64-bit processor with virtualization capability (Intel VT-x or AMD-V*) and at least 3 GB of memory and 50 GB of disk space, then we can run two virtual machines, each with one GB RAM and one GB for the host machine.

The user can perform the lab by using open-source software “VirtualBox” for Windows/Linux. You can download the 64-bit or 32-bit VBox, depending on the processor architecture. The virtual box is a virtualization platform where users can install multiple operating systems on a single host. It is also known as hosted virtualization. The step-by-step process is as follows:

1. Open the web browser and access <https://www.virtualbox.org/wiki/Downloads>. Then, select **Windows hosts** if you want to install it on the Windows operating system.
2. Double-click on **downloaded exe**. This would display *Figure 1.1*. Click on the **Next** button:

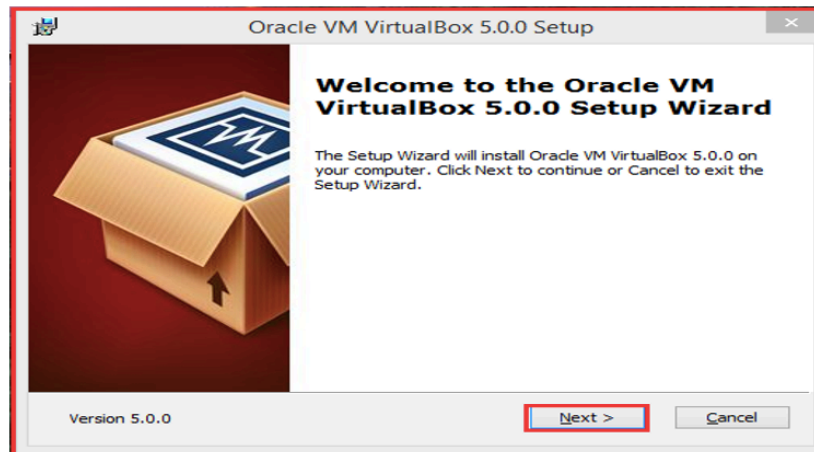


Figure 1.1: Welcome wizard

3. This would display the location where your VBox file would be installed. You can change the file location by using the **Browse** button. Then, click on the **Next** button, as shown in Figure 1.2:

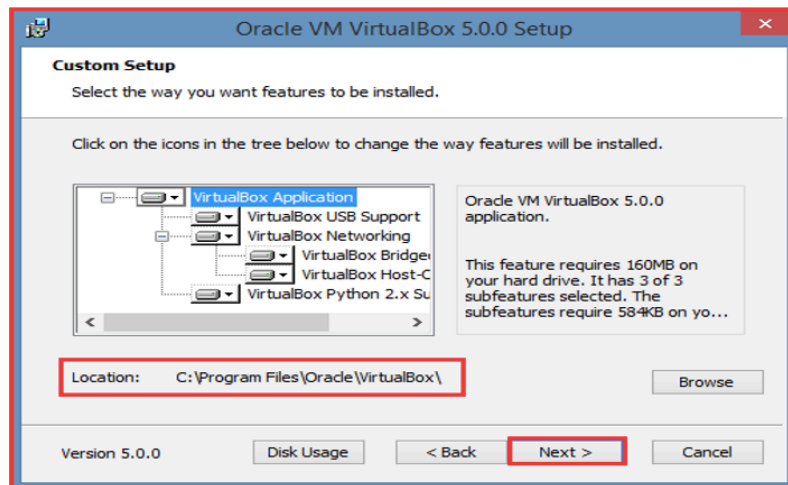


Figure 1.2: Location selection for installation

4. Now, click on the **Next** button, as shown in Figure 1.3:

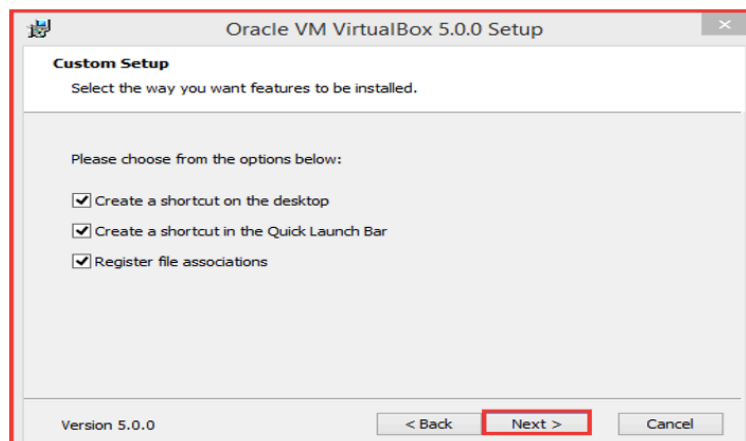


Figure 1.3: Selecting options

5. This will reset the network connection temporarily and will install the **Network interface card** for VBox. Click on the **Yes** button, as shown in Figure 1.4:



Figure 1.4: Network connection resetting wizard

6. Click on the **Install** button, as shown in Figure 1.5:

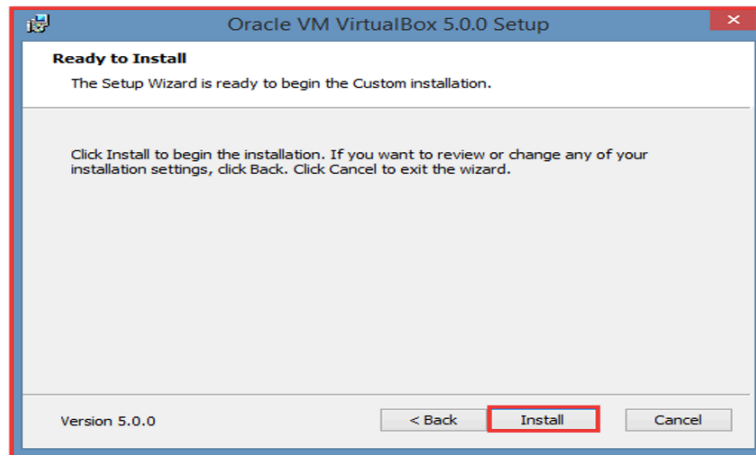


Figure 1.5: Installation wizard

7. Now, the installation process will start. Refer to Figure 1.6:

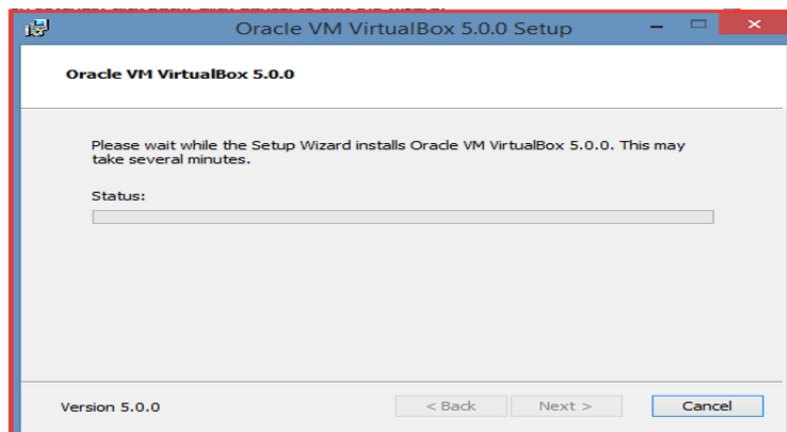


Figure 1.6: Installing software

8. A user access control window would be displayed. Click on the **Yes** button to allow the VBox. Then click on the **Install** button, as shown in Figure 1.7:

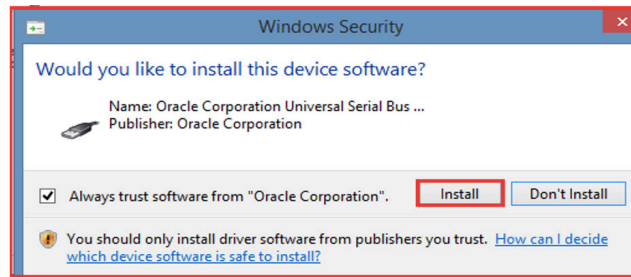


Figure 1.7: Installing device

9. Click on the **Finish** button, as shown in Figure 1.8:



Figure 1.8: Installation complete wizard

10. In Figure 1.9, we can see that VBox is installed:

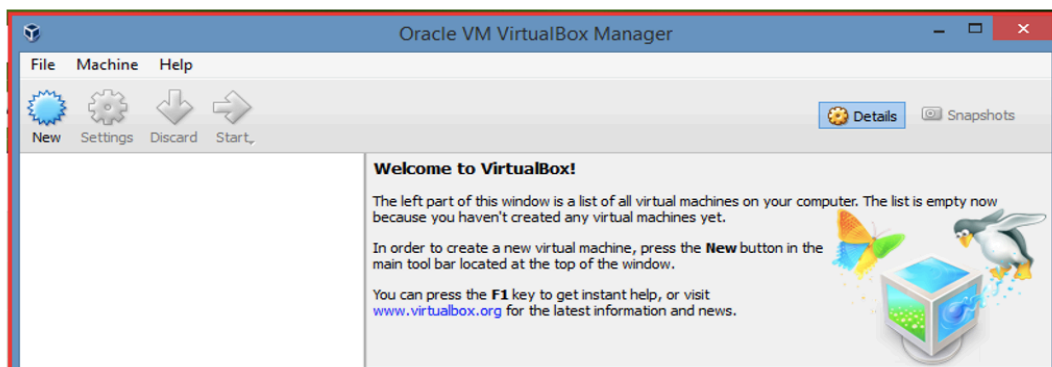


Figure 1.9: Displaying virtual box in default mode

11. Now download the virtual machine for OSINT using the website <https://www.tracelabs.org/initiatives/osint-vm> and then import the OVA file on the virtual box, as shown in Figure 1.10:

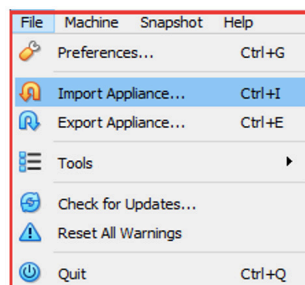


Figure 1.10: Importing appliances