BOOK Reviews

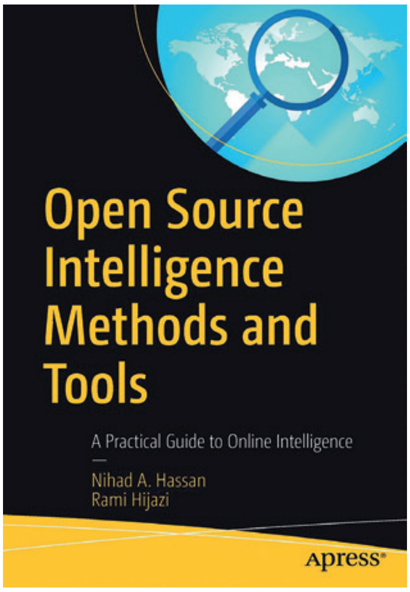
When I first received this book, my initial impression was one of concern that such a tome might be a hard read. What I found, however, was much to the contrary. It is a book packed with good content covering over 350 pages in a well laid out and logical manner. A must for any technical book.

With 'Threat Intelligence' (Threat Intelligence – The set of data collected, assessed and applied regarding security threats, threat actors, exploits, malware, vulnerabilities and compromise indicators – SANS Institute) receiving much attention these days as one of the tools in the armoury to get ahead of the game in cyber security terms, knowing how to gather, analyse and respond to Open Source Intelligence, is a 'Must Know' topic for anyone who is trying to establish such a capability within their organisation, or even just to protect themselves from what is out there on the public internet, especially important for celebrities or other individuals whose reputations maybe at stake.

The first chapter takes a look at the origination and development of Open Source Intelligence and lays out the basic information for what follows. Each chapter is packed full of resources to gather further information and chapter 1 is no different in this regard, though I do have a concern over the longevity of the source when using URLs. These unlike a report title, with author and date etc. that are often used when referencing papers in academic research are subject to change or loss as the Web refreshes itself or is removed. That being said technology moves quickly as we know and any source document or URL has a shelf life.

When I reached chapter 2 I was initially dismayed at the subject matter covered, however this soon changed as I got into the 73 pages (about a 5th of the book) that this chapter alone takes up of the total 354 pages of the book. This chapter is one of the most comprehensive compilations of online threats, advice on how to stay safe and undetected online and removal of your own digital traces when gathering data I have come across in a single chapter. I defy anyone not to learn something new from this chapter. Each chapter is stand alone and has its own summary allowing readers to concentrate on a single chapter or topic if they wish.

Chapter 3 takes us into the world of the Underground Internet and provides a good explanation of the various layers of the internet and how they work. No explanation of the underground internet would be complete without a reference to the TOR Onion Router, however the author has spent some time in explaining how to use TOR in some detail, but does not stop at TOR as the chapter also includes I2P and a comparison of the two. The authors also recommend the use of the Debian GNU/Linux security hardened OS, Tails, when entering the world of the underground internet and whilst I have no issue with the use of Tails, I do wonder how this might compare with using Cubes. A possible comparison project right there for the future. ▷



Open Source Intelligence Methods and Tools

A Practical Guide to Online Intelligence

Nihad A. Hassan
Rami Hijazi

Apress®

Open Source Intelligence Methods & Tools

Author(s)
Nihad A. Hassan & Rami Hijazi

Publisher
Apress

Date of Publishing
2018

ISBN
E-book: 978-1-4842-3213-2
Paperback: 978-1-4842-3212-5

Price
£24.99 / $34.99

Reviewer
Reem Naddar

●●●●○

We now enter the world of the search engine for Chapter 4 and how to create search terms that will gain you access to potentially sensitive information. The chapter goes on to compare search engines and to identify locations where specific types of data may reside. The chapter also includes information on Metadata search engines as well as how to search for code. One interesting aspect not often covered is the ability to search for and translate from other languages. Indeed why would we think that the web was only for English? Topically, the authors have included a section on Fake News advising significantly on not trusting the news until the source is verified and given a higher confidence level.

Social Media Intelligence is the focus for Chapter 5 and rightly so as it provides for a significantly rich seam of intelligence and information to be harvested. By classifying social media platforms the author has provided a mechanism whereby any social media site may be catalogued in your intelligence gathering. The chapter also provides information on how sites such as Facebook provide a semantic search engine (Graph Search) using Natural Language searches. What I also liked about this chapter is the inclusion and recognition of Psychological Analysis of Social Media content, a topic not often covered. The use of linguistic markers and analysis can tell you a lot as has been covered in a recent article in Issue 36 of the magazine.

Searching for information within Public Records when looking for intelligence on individuals is covered in Chapter 6 along with other resources for what are called 'People Search Engines'. Included is how to search for intelligence using Criminal and Court searches, property searches along with Tax and Financial records. I also liked the fact that the authors included Data Compromised Repository Websites that hold data regarding previous data breaches.

The authors next take us into the world of Maps and Geolocation information for Chapter 7. As the author points out "Most people do not care about the underlying technology responsible for delivering location-based services to them. People enter the address of the location they need to look up on the map, or they use the built-in feature available in smartphones to geotag digital files (such as images and videos) so they record the current location of images/ videos as a meta tag automatically". By again providing a rich list of resources and explanation the intelligence to be gained from geolocation data is not insignificant.

After having provided significant detail about where and how intelligence might be gathered, Chapter 8 turns to looking at how to 'recon' a targets own website, a practice referred to as Technical Footprinting. A significant amount of data may be gleaned from a targets website by using the tools and techniques identified in this chapter, even if you do not intend to do such work, it is important to know how this practice is carried out.

Having provided a comprehensive look at the world of OSINT and Intelligence gathering, the author concludes with Chapter 9 looking at the future of OSINT. Included, importantly to my mind is the OSINT Process; 5 clear steps on how to do OSINT and get the best out of what you gather. There is a touch of the future not included in the book that jumps out at you just because of the sheer scale of OSINT that this book provides and that is how to use Big Data and Computational Intelligence to analyse the raw data collected. The topic of another book for the author no doubt.

The final aspect of this book is a comprehensive Index allowing the reader to search and lookup particular aspects of interest ensuring that this book becomes a reference work for those involved in Threat Intelligence and OSINT gathering. If there was one downside and it is a very small one, I would like to see a greater resolution in the screenshots and images contained within.

Closing summary

A must read for anyone who wants to understand threat intelligence and OSINT gathering. A significant resource for those looking to establish a capability within an organization, or for those who want to establish a business, providing such a service to others. A comprehensive book recommended to both students and practitioners of threat intelligence gathering. •

When I first received this book, my initial impression was one of concern that such a tomb might be a hard read. What I found, however, was much to the contrary. It is a book packed with good content covering over 350 pages in a well laid out and logical manner. A must for any technical book.