Open Source Intelligence Techniques

This book will serve as a reference guide for anyone that is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials as they go. The search techniques offered will inspire analysts to "think outside the box" when scouring the internet for personal information. Much of the content of this book has never been discussed in any publication. Always thinking like a hacker, the author has identified new ways to use various technologies for an unintended purpose. This book will improve anyone's online investigative skills. Among other topics, you will learn how to locate: Hidden Social Network Content, Cell Phone Owner Information, Twitter GPS & Account Data, Hidden Photo GPS & Metadata, Deleted Website & Posts, Website Owner Information, Alias Social Network Profiles, Additional User Accounts, Sensitive Documents & Photos, Live Streaming Social Content, IP Addresses of Users, Newspaper Archives & Scans, Social Content by Location, Private Email Addresses, Historical Satellite Imagery, Duplicate Copies of Photos, Local Personal Radio Frequencies, Compromised Email Information, Wireless Routers by Location, Hidden Mapping Applications, Complete Facebook Data, Free Investigative Software, Alternative Search Engines, Stolen Items for Sale, Unlisted Addresses, Unlisted Phone Numbers, Public Government Records, Document Metadata, Rental Vehicle Contracts, Online Criminal Activity.

Open Source Intelligence Methods and Tools

Apply Open Source Intelligence (OSINT) techniques, methods, and tools to acquire information from publicly available online sources to support your intelligence analysis. Use the harvested data in different scenarios such as financial, crime, and terrorism investigations as well as performing business competition analysis and acquiring intelligence about individuals and other entities. This book will also improve your skills to acquire information online from both the regular Internet as well as the hidden web through its two sub-layers: the deep web and the dark web. The author includes an array of OSINT resources that can be used by intelligence agencies as well as by enterprises to monitor trends on a global level, identify risks, and gather competitor intelligence so more effective decisions can be made. You will discover techniques, methods, and tools that are equally used by hackers and penetration testers to gather intelligence about a specific target online. And you will be aware of how OSINT resources can be used in conducting social engineering attacks. Open Source Intelligence Methods and Tools takes a practical approach and lists hundreds of OSINT resources that can be used to gather intelligence from online public sources. The book also covers how to anonymize your digital identity online so you can conduct your search activities without revealing your identity. What You'll Learn Identify intelligence needs and leverage a broad range of tools and sources to improve data collection, analysis, and decision making in your organization Use OSINT resources to protect individuals and enterprises by discovering data that is online, exposed, and sensitive and hide the data before it is revealed by outside attackers Gather corporate intelligence about business competitors and predict future market directions Conduct advanced searches to gather intelligence from social media sites such as Facebook and Twitter Understand the different layers that make up the internet and how to search within the invisible web which contains both the deep and the dark webs Who This Book Is For Penetration testers, digital forensics investigators, intelligence services, military, law enforcement, UN agencies, and for-profit/non-profit enterprises.

Automating Open Source Intelligence

This book presents information on the gathering of information and extraction of actionable intelligence from openly available sources, including news broadcasts, public repositories, and more recently, social media. As OSINT has applications in crime fighting, state-based intelligence, and social research, this book provides recent advances in text mining, web crawling, and other algorithms that have led to advances in methods that can largely automate this process. The book is beneficial to both practitioners and academic researchers, with discussions of the latest advances in applications, a coherent set of methods and processes for automating OSINT, and interdisciplinary perspectives on the key problems identified within each discipline. Drawing upon years of practical experience and using numerous examples, editors Robert Layton, Paul Watters, and a distinguished list of contributors discuss Evidence Accumulation Strategies for OSINT, Named Entity Resolution in Social Media, Analyzing Social Media Campaigns for Group Size Estimation, Surveys and qualitative techniques in OSINT, and Geospatial reasoning of open data. Presents a coherent set of methods and processes for automating OSINT Focuses on algorithms and applications allowing the practitioner to get up and running quickly Includes fully developed case studies on the digital underground and predicting crime through OSINT Discusses the ethical considerations when using publicly available online data.

The Tao of Open Source Intelligence

This topical volume offers a comprehensive view into the newest methods for OSINT analytics and visualizations in combination with real-life case studies to showcase the application as well as the challenges of OSINT investigations across domains. Examples of OSINT range from information posted on social media as one of the most openly available means of accessing and gathering Open Source Intelligence to location data. This book is beneficial to both practitioners and academic researchers, provides recent advances in text mining, web crawling, and other algorithms that have led to advances in methods that can largely automate this process. The book is beneficial to both practitioners and academic researchers, with discussions of the latest advances in applications, a coherent set of methods and processes for automating OSINT, and interdisciplinary perspectives on the key problems identified within each discipline. Drawing upon years of practical experience and using numerous examples, editors Robert Layton, Paul Watters, and a distinguished list of contributors discuss Evidence Accumulation Strategies for OSINT, Named Entity Resolution in Social Media, Analyzing Social Media Campaigns for Group Size Estimation, Surveys and qualitative techniques in OSINT, and Geospatial reasoning of open data. Presents a coherent set of methods and processes for automating OSINT Focuses on algorithms and applications allowing the practitioner to get up and running quickly Includes fully developed case studies on the digital underground and predicting crime through OSINT Discusses the ethical considerations when using publicly available online data.

Open Source Intelligence Investigation

One of the most important aspects for a successful police operation is the ability for the police to obtain timely, reliable and actionable intelligence related to the investigation or incident at hand. Open Source Intelligence (OSINT) provides an invaluable avenue to access and collect such information in addition to traditional investigative techniques and information sources. This book offers an authoritative and accessible guide on how to conduct Open Source Intelligence investigations from data collection to analysis to the design and vetting of OSINT tools. In its pages the reader will find a comprehensive view into the newest methods for OSINT analytics and visualizations in combination with real-life case studies to showcase the application as well as the challenges of OSINT investigations across domains. Open Source Intelligence Investigation takes a practical approach and lists hundreds of OSINT resources that can be used to gather intelligence from online public sources. The book also covers how to anonymize your digital identity online so you can conduct your search activities without revealing your identity. What You’ll Learn Identify intelligence needs and leverage a broad range of tools and sources to improve data collection, analysis, and decision making in your organization Use OSINT resources to protect individuals and enterprises by discovering data that is online, exposed, and sensitive and hide the data before it is revealed by outside attackers Gather corporate intelligence about business competitors and predict future market directions Conduct advanced searches to gather intelligence from social media sites such as Facebook and Twitter Understand the different layers that make up the internet and how to search within the invisible web which contains both the deep and the dark webs Who This Book Is For Penetration testers, digital forensics investigators, intelligence services, military, law enforcement, UN agencies, and for-profit/non-profit enterprises.

Handbook of Intelligence Studies

This topical volume offers a comprehensive review of secret intelligence organizations and activities. Intelligence has been in the news consistently since 9/11
Internet Searches for Vetting, Investigations, and Open-Source Intelligence—Edward J. Appel 2016-04-19

In the information age, it is critical that we understand the implications and exposure of the activities and data documented on the Internet. Improved efficiencies and the added capabilities of instant communication, high-speed connectivity to browsers, search engines, websites, databases, indexing, searching and analytical applications have made information technology (IT) and the Internet a vital tool in understanding individuals, organizations, and enterprises. The downside is that this increased level of complexity and vulnerability presents a daunting challenge for enterprise and personal security. Internet Searches for Vetting, Investigations, and Open-Source Intelligence provides an understanding of the implications of the activities and data documented by individuals on the Internet. It delineates a much-needed framework for the responsible collection and use of the Internet for intelligence, investigation, vetting, and open-source information. This book makes a compelling case for action as well as the legal, policy, and procedural approaches needed. The book ends with more Case Studies and solutions for common problems encountered in Internet searching practice and information usage, from internal and external threats. The book is a valuable resource on how to utilize open-source, online sources to gather important information and screen and vet employees, prospective employees, corporate partners, and vendors.

Open Source Intelligence Investigation—Babak Akhgar 2016-12-17

One of the most important aspects for a successful police operation is the ability for the police to obtain timely, reliable, and actionable intelligence related to the investigation or incident at hand. Open Source Intelligence (OSINT) provides an invaluable avenue to access and collect such information in addition to traditional investigative techniques and information sources. This book provides a comprehensive guide on how to conduct and access open-source intelligence investigations from data collection to analysis to the design and vetting of OSINT tools. In its pages the reader will find a comprehensive view into the newest methods for OSINT analytics and visualizations in combination with real-life case studies to showcase the application as well as the challenges of OSINT investigations across domains.

Examples of OSINT range from information posted on social media as one of the most openly available means of accessing and gathering Open Source Intelligence to location data, OSINT obtained from the darkweb to combinations of OSINT with real-time analytical capabilities and closed sources. In addition it provides guidance on legal and ethical considerations making it relevant reading for practitioners as well as academics and students with a view to obtain thorough, first-hand knowledge from serving experts in the field.

Open Source Intelligence in the Twenty-First Century—Christopher Holmes 2014-05-09

This edited volume takes a fresh look at the subject of open source intelligence (OSINT), exploring both the opportunities and the challenges that this emergent area offers at the beginning of the twenty-first century. In particular, it explores the new methodologies and approaches that technological advances have engendered, while at the same time considering the risks associated with the pervasive nature of the Internet. Drawing on a diverse range of experience and expertise, the book begins with a number of chapters devoted to exploring the uses and value of OSINT in a general sense, identifying patterns, trends and key areas of debate. The focus of the book then turns to the role and influence of OSINT in three key areas of international security—nuclear proliferation; humanitarian crises; and terrorism. The book offers a timely discussion on the merits and failings of OSINT and provides readers with an insight into the latest and most original research being conducted in this area.

Counterterrorism and Open Source Intelligence—Uffe Wili 2011-06-27

Since the 9/11 terrorist attacks in the United States, serious concerns were raised on domestic and international security issues. Consequently, there has been considerable interest recently in technological strategies and resources to counter acts of terrorism. In this context, this book provides a state-of-the-art survey of the most recent advances in the field of counterterrorism and open source intelligence, demonstrating how various existing as well as novel tools and techniques can be applied in combating covert terrorist networks. A particular focus will be on future challenges of open source intelligence and perspectives on how to effectively operate in order to prevent terrorist activities.

Open Source Intelligence and Cyber Crime—Mohammad A. Tayebi 2020-09-01

This book shows how open source intelligence can be a powerful tool for combating crime by linking local and global patterns to help understand how criminal activities are connected. Readers will encounter the latest advances in cutting-edge data techniques such as forensics, malware analysis, and social engineering, and will learn how these tools can be used to prevent and investigate cyber crimes. The book also covers the legal and ethical implications of using open source intelligence in law enforcement, as well as the challenges and limitations of this approach. With its comprehensive coverage of open source intelligence in the field of cyber crime, this book is an essential resource for security professionals, law enforcement officers, and students interested in this rapidly evolving area of study.

Hacking Web Intelligence—Sudhanshu Chauban 2015-04-13

Open source intelligence (OSINT) and web reconnaissance are rich topics for infosec professionals looking for the best ways to sift through the abundance of information available online. In many cases, the first stage of any security assessment—that is, reconnaissance—is not given enough attention by security professionals, hackers, and penetration testers. Often, the information openly present is as critical as the confidential data. Hacking Web Intelligence shows you how to dig into the Web and uncover the information many don’t even know exists. The book takes a holistic approach that is not only about using tools to find information online but also how to link all the information and transform it into presentable and actionable intelligence. You will also learn how to secure your information online to prevent it being discovered by these reconnaissance methods. Hacking Web Intelligence is an in-depth technical reference covering the methods and techniques you need to unearth open source information from the Internet and utilize it for the purpose of targeted attack during a security assessment. This book will introduce you to many new and leading-edge reconnaissance, information gathering, and open source intelligence methods and techniques, including metadata extraction tools, advanced search engines, advanced browsers, powerful reconnaissance methods, online anonymity tools such as TOR and I2P, OSINT tools such as Maltego, Shodan, Creepy, SearchDiggity, Recon-ng, Social Network Analysis (SNA), Darkweb/Deepweb, data visualization, and much more. Provides a holistic approach to OSINT and Web recon, showing you how to fit all the data together into actionable intelligence focuses on hands-on tools such as TOR, I2P, Maltego, Shodan, Creepy, SearchDiggity, Recon-ng, FOCA, EXIF, Metagoofil, MAT, and many more. Discusses key technical topics such as metadata searching, advanced browsers and power searching, online anonymity, Darkweb / Deepweb, Social Network Analysis (SNA), and how to manage, analyze, and visualize the data you gather Includes hands-on technical examples and case studies, as well as a Python chapter that shows you how to create your own information-gathering tools and modify existing APIs.

Open Source Intelligence in a Networked World—Anthony Olcott 2012-05-17

The amount of publicly and often freely available information is staggering. Yet, the intelligence community still continues to collect and use information in the same manner as during WWII, when the OSS set out to learn as much as possible about Nazi Germany and Imperial Japan by scrutinizing encyclopedias, guide books, and short-wave radio. Today, the supply of information is greater than any possible demand, and anyone can provide information. In effect, intelligence analysts are drowning in information. The book explains how to navigate this rising flood and make best use of these new, rich sources of information. Written by a pioneer in the field, it explores the potential uses of digitized data and the impact of the new means of creating and transmitting data, recommending to the intelligence community new ways of collecting and processing information. This comprehensive overview of the world of open source intelligence will appeal not only to practitioners and students of intelligence, but also to anyone interested in communication and the challenges posed by the information age.
Open Source Intelligence Techniques—Michael Bazzell 2018-01-26 Completely Rewritten Sixth Edition Sheds New Light on Open Source Intelligence Collection and Analysis Author Michael Bazzell has been well known in government circles for his ability to locate personal information about any target through Open Source Intelligence (OSINT). In this book, he shares his methods in great detail. Each step of his process is explained throughout twenty-five chapters of specialized websites, software solutions, and creative search techniques. Over 250 resources are identified with narrative tutorials and screen captures. This book will serve as a reference guide for anyone that is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials as they go. The search techniques offered will inspire analysts to “think outside the box” when scouring the internet for personal information. Much of the content of this book has never been discussed in any publication. Always thinking like a hacker, the author has identified new ways to use various technologies for an unintended purpose. This book will greatly improve anyone’s online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network Content Cell Phone Subscriber Information Deleted Websites & Posts Missing Facebook Profile Data Full Twitter Account Data Alias Social Network Profiles Free Investigative Software Useful Browser Extensions Alternative Search Engine Results Website Owner Information Photo GPS & Metadata Live Streaming Social Content Social Content by Location IP Addresses of Users Additional User Accounts Sensitive Documents & Photos Private Email Addresses Duplicate Video Posts Mobile App Network Data Unlisted Addresses & # Public Government Records Document Metadata Rental Vehicle Contracts Online Criminal Activity Personal Radio Communications Compromised Email Information Automated Collection Solutions Linux Investigative Programs Dark Web Content (Tor) Restricted YouTube Content Hidden Website Details Website Registration Details

Sharing the Secrets—F. Holden-Rhodes 1997 This important work identifies the problems of counter-drug intelligence and points toward a remedy for the failed anti-drug policies in the United States through the effective use of open source intelligence.

Open Source Intelligence in the Twenty-First Century—C. Hobbs 2014-05-09 This edited book provides an insight into the new approaches, challenges and opportunities that characterise open source intelligence (OSINT) at the beginning of the twenty-first century. It does so by considering the impacts of OSINT on three important contemporary security issues: nuclear proliferation, humanitarian crimes and terrorism.

Open Source Intelligence Techniques—Michael Bazzell 2021 It is time to look at OSINT in a different way. For many years, and within the previous editions of this book, we have relied on external resources to supply our search tools, virtual environments, and investigation techniques. We have seen this process fail us when services shut down, websites disappear, and custom resources are dismantled due to outside pressures. This book aims to correct our dilemma. We will take control of our investigative resources and become self-reliant. There will be no more need for online search tools; we will make and host our own locally. We will no longer seek pre-built virtual machines; we will create and configure our own. This book puts the power back in your hands.

Defining Second Generation Open Source Intelligence (Osint) for the Defense Enterprise—Heather J. Williams 2018-05-17 This report describes the evolution of open source intelligence, defines open source information and the intelligence cycle, and parallels with other intelligence disciplines, along with methods used and challenges of using off-the-shelf technology.

Open Source Intelligence in a Networked World—Anthony Olcott 2012 “The amount of publicly and often freely available information is staggering. Yet, the intelligence community still continues to collect and use information in the same manner as during WWII, when the OSS set out to learn as much as possible about Nazi Germany and Imperial Japan by scrutinizing encyclopedias, guide books, and short-wave radio. Today, the supply of information is greater than any possible demand, and anyone can provide information. In effect, intelligence analysts are drowning in information. The book explains how to navigate this rising flood and make best use of these new, rich sources of information. Written by a pioneer in the field, it explores the potential uses of digitized data and the impact of the new means of creating and transmitting data, recommending to the intelligence community new ways of collecting and processing information. This comprehensive overview of the world of open source intelligence will appeal not only to practitioners and students of intelligence, but also to anyone interested in communication and the challenges posed by the information age.”—Bloomsbury Publishing.

Open Source Intelligence Tools and Resources Handbook—i-intelligence 2019-08-17 2018 version of the OSINT Tools and Resources Handbook. This version is almost three times the size of the last public release in 2016. It reflects the changing intelligence needs of our clients in both the public and private sector, as well as the many areas we have been active in over the past two years.

Critical Infrastructure Security and Resilience—Dimitris Gritzalis 2019-01-01 This book presents the latest trends in attacks and protection methods of Critical Infrastructures. It describes original research models and applied solutions for protecting major emerging threats in Critical Infrastructures and their underlying networks. It presents a number of emerging endeavors, from newly adopted technical expertise in industrial security to efficient design and implementation of attacks and relevant security measures in industrial control systems, including advancements in hardware and services security, interdependency networks, risk analysis, and control systems security along with their underlying protocols. Novel attacks against Critical Infrastructures (CI) demand novel security solutions. Simply adding more of what is done already (e.g. more thorough risk assessments, more expensive Intrusion Prevention/Detection Systems, more efficient firewalls, etc.) is simply not enough against threats and attacks that seem to have evolved beyond modern analyses and protection methods. The knowledge presented herein, will help Critical Infrastructure authorities, security officers, and SOC personnel and relevant researchers to (i) get acquainted with advancements in the field, (ii) integrate security research into their industrial or research work, (iii) evolve current practices in modeling and analyzing Critical Infrastructures, and (iv) moderate potential crises and emergencies influencing or emerging from Critical Infrastructures.

Hunting Cyber Criminals—Vinny Troia 2020-02-11 The skills and tools for collecting, verifying and correlating information from different types of systems is an essential skill when tracking down hackers. This book explores Open Source Intelligence Gathering (OSINT) outside out from multiple perspectives, including those of hackers and security experts. OSINT refers to the techniques and tools required to harvest publicly available data concerning a person or an organization. With several years of experience of tracking hackers with OSINT, the author whips up a classical plot-line involving a hunt for a threat actor. While taking the audience through the thrilling investigative drama, the author immerses the audience with in-depth knowledge of state-of-the-art OSINT tools and techniques. Technical users will want a basic understanding of the Linux command line in order to follow the examples. But a person with no Linux or programming experience can still gain a lot from this book through the commentaries. This book’s unique digital investigation proposition is a combination of story-telling, tutorials, and case studies. The book explores digital investigation from multiple angles: Through the eyes of the author who has several years of experience in the subject. Through the mind of the hacker who collects massive amounts of data from multiple online sources to identify targets as well as ways to hit the targets. Through the eyes of industry leaders. This book is ideal for: Investigation professionals, forensic analysts, and CISO/CIO and other executives wanting to understand the mindset of a hacker and how seemingly harmless information can be used to target their organization. Security analysts, forensic investigators, and SOC teams looking for new approaches on digital investigations from the perspective of collecting and parsing publicly available information. CISOs and defense teams will find this book useful because it takes the perspective of infiltrating an organization from the mindset of a hacker. The commentary provided by outside experts will also provide them with ideas to
further protect their organization’s data.

Clear Thinking—Sean S. Costigan 2012-10-28

Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism—Sari, Arif 2019-05-31 Interdisciplinary and multidisciplinary research is slowly yet steadily revolutionizing traditional education. However, multidisciplinary research can and will also improve the extent to which a country can protect its critical and vital assets. Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism is an essential scholarly publication that provides personnel directly working in the fields of intelligence, law enforcement, and science with the opportunity to understand the multidisciplinary nature of intelligence and science in order to improve current intelligence activities and contribute to the protection of the nation. Each chapter of the book discusses various components of science that should be applied to the intelligence arena. Featuring coverage on a range of topics including cybersecurity, economics, and political strategy, this book is ideal for law enforcement, intelligence and security practitioners, students, educators, and researchers.

Deep Learning with Python—Francois Chollet 2017-11-30 Summary Deep Learning with Python introduces the field of deep learning using the Python language and the powerful Keras library. Written by Keras creator and Google AI researcher François Chollet, this book builds your understanding through intuitive explanations and practical examples. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology Machine learning has made remarkable progress in recent years. We went from near-unusable speech and image recognition, to near-human accuracy. We went from machines that couldn't beat a serious Go player, to defeating a world champion. Behind this progress is deep learning—a combination of engineering advances, best practices, and theory that enables a wealth of previously impossible smart applications. About the Book Deep Learning with Python introduces the field of deep learning using the Python language and the powerful Keras library. Written by Keras creator and Google AI researcher François Chollet, this book builds your understanding through intuitive explanations and practical examples. You’ll explore challenging concepts and practice with applications in computer vision, natural-language processing, and generative models. By the time you finish, you’ll have the knowledge and hands-on skills to apply deep learning in your own projects. What’s Inside Deep learning from first principles Setting up your own deep learning environment Image-classification models Deep learning for text and sequences Neural style transfer, text generation, and image generation About the Reader Readers need intermediate Python skills. No previous experience with Keras, TensorFlow, or machine learning is required. About the Author François Chollet works on deep learning at Google in Mountain View, CA. He is the creator of the Keras deep-learning library, as well as a contributor to the TensorFlow machine-learning framework. He also does deep-learning research, with a focus on computer vision and the application of machine learning to formal reasoning. His papers have been published at major conferences in the field, including the Conference on Computer Vision and Pattern Recognition (CVPR), the Conference and Workshop on Neural Information Processing Systems (NIPS), the International Conference on Learning Representations (ICLR), and others. Table of Contents PART 1 - FUNDAMENTALS OF DEEP LEARNING What is deep learning? Before we begin: the mathematical building blocks of neural networks Getting started with deep neural networks Fundamentals of machine learning PART 2 - DEEP LEARNING IN PRACTICE Deep learning for computer vision Deep learning for text and sequences Advanced deep-learning best practices Generative deep learning Conclusions appendix A - Installing Keras and its dependencies on Ubuntu appendix B - Running Jupyter notebooks on an EC2 GPU instance

The Enterprise Big Data Lake—Alex Gorelik 2019-02-21 The data lake is a daring new approach for harnessing the power of big data technology and providing convenient self-service capabilities. But is it right for your company? This book is based on discussions with practitioners and executives from more than a hundred organizations such as Google, Microsoft, and Facebook, to governments and traditional corporate enterprises. You’ll learn what a data lake is, why enterprises need one, and how to build one successfully with the best practices in this book. Alex Gorelik, CTO and founder of Waterline Data, explains why old systems and processes can no longer support data needs in the enterprise. Then, in a collection of essays about data lake implementation, you’ll examine data lake initiatives, analytic projects, experiences, and best practices from data experts working in various industries. Get a succinct introduction to data warehousing, big data, and data science Learn various paths enterprises take to build a data lake Explore how to build a self-service model and best practices for providing analysts access to the data Use different methods for architecting your data lake Discover ways to implement a data lake from experts in different industries

Penetration Testing with Perl—Douglas Berdeaux 2015-01-05 If you are an expert Perl programmer interested in penetration testing or information security, this guide is designed for you. However, it will also be helpful for you even if you have little or no Linux shell experience.

Designing Distributed Systems—Brendan Burns 2018-02-20 In the race to compete in today's fast-moving markets, large enterprises are busily adopting new technologies for creating new products, processes, and business models. But one obstacle on the road to digital transformation is placing too much emphasis on technology, and not enough on the types of processes technology enables. What if different lines of business could build their own services and applications—and decision-making was distributed rather than centralized? This report explores the concept of a digital business platform as a way of empowering individual business segments to act on data in real time. Much innovation in a digital enterprise will increasingly happen at the edge, whether it involves business users (from marketers to data scientists) or IoT devices. To facilitate the process, your core IT team can provide these sectors with the digital tools they need to innovate quickly. This report explores: Key cultural and organizational changes for developing business capabilities through cross-functional product teams A platform for integrating applications, data sources, business partners, clients, mobile apps, social networks, and IoT devices Creating internal API programs for building innovative edge services in low-code or no-code environments Tools including Integration Platform as a Service, Application Platform as a Service, and Integration Software as a Service The challenge of integrating microservices and serverless architectures Event-driven architectures for processing and reacting to events in real time You’ll also learn about a complete pervasive integration solution as a core component of a digital business platform to serve every audience in your organization.

Using Open Source Platforms for Business Intelligence—Lyndsay Wise 2012-11-23 Open Source BI solutions have many advantages over traditional proprietary software, from offering lower initial costs to more flexible support and integration options; but, until now, there has been no comprehensive guide to the complete offerings of the OS BI market. Writing for IT managers and business analysts without bias toward any BI suite, industry insider Lyndsay Wise covers the benefits and challenges of all available open source BI systems and tools enabling readers to identify the solutions and technologies that best meet their business needs. Wise compares and contrasts types of OS BI and proprietary tools on the market, including Pentaho, Jaspersoft, RapidMiner, SpagoBI, BIRT, and many more. Real-world case studies and project templates clarify the steps involved in implementing open source BI, saving new users time and trouble of developing their own solutions from scratch. For business users who are hard pressed to identify the best Fit solutions to their company’s needs, this book provides a practical guide to evaluating the ROI of open source versus traditional BI deployments. The only book to provide complete coverage of all open source BI systems and tools specifically for business managers, without bias toward any OS BI suite A practical, step-by-step guide to implementing OS BI solutions that maximize ROI Comprehensive coverage of all open source systems and tools, including architectures, data integration, support, optimization, data mining, data warehousing, and interoperability Case studies and project templates enable readers to evaluate the benefits and tradeoffs of all OS BI options without having to spend time developing their own solutions from scratch.

How to Find Out Anything—Don MacLeod 2012-08-07 In How to Find Out Anything, master researcher Don MacLeod explains how to find what you’re looking for, quickly, efficiently, and accurately—and how to avoid the most common mistakes of the Google Age. Not your average research book, How to Find Out Anything shows you how to unveil nearly anything about anyone. From top CEO’s salaries to police records, you’ll learn little-known tricks for discovering the exact information you’re looking for. You’ll learn: • How to really tap the power of Google, and why Google is the best place to start a search, but never the best place to finish it. The scoop on
Down the Rabbit Hole an Osint Journey-Chris Kubecka 2017-06-29 Do you enjoy the reconnaissance part of a penetration testing? Want to discover issues on your network, assets or applications proactively? Would you like to learn some new OSINT based recon tools and techniques? Follow the rabbit hole and find exploitable critical vulnerabilities in the Panama Papers law firm and politics both American and international including Trump and the DNC. Analyze network and email configurations for entry points and exploits with FOCA, Maltego, Nmap/ZenMap, and Spiderfoot. Learn how to use advanced search engines, alternative search engines that don’t respect robots.txt., intel tools, and leak databases. Open source intelligence gathering (OSINT) and web-based reconnaissance is an important part of penetration testing and proactive defense. The more connected we are, the more information is held about everything. Yummy, juicy information for both a penetration tester or a malicious actor. Learning what sources of are available to start your search is an important first step in learning about reconnaissance and how the information could be utilized or resold. Both issues you or your client need to know. All of the tools and techniques in this book can be ninjafied with Python, Ruby or PowerShell. Initially, this book began as a presentation at the Cyber Senate Industrial Control Cybersecurity Nuclear Summit in Warrington, UK 2016. Originally, I intended to use some of the same techniques to target a nuclear power plant or someone in a nuclear regulatory capacity. After submitting my original talk idea. Daesh, otherwise known as ISIS, began publicly threatening the European nuclear industry. Due to the threats, we decided it wasn’t in anyone’s best interest to give a how to target nuclear installations and changed the repent instead to the law firm behind the Panama Papers fiasco. The project expanded to include additional targets with mostly a political slant. 2016 was a very tumultuous year in politics. Brexit, Trump, and the rise of the interesting politics and coups in Turkey, Netherlands, Germany, Russia, Bulgaria and the Philippines. It’s a lot more fun to learn about a topic in an empowering way. Also, only politicians like politicians. They make a fun target. Learning a new technique is easier when it’s fun. I chose targets and case studies which gave me a happy hacker smile. Publications Combined: Studies In Open Source Intelligence (OSINT) And Information-2019-03-23 Over 1,600 total pages ... CONTENTS: AN OPEN SOURCE APPROACH TO SOCIAL MEDIA DATA GATHERING Open Source Intelligence – Doctrine’s Neglected Child (Unclassified) Aggregation Techniques to Characterize Social Networks Open Source Intelligence (OSINT), Issues for Congress A BURNING NEED TO KNOW: THE USE OF OPEN SOURCE INTELLIGENCE IN THE FIRE SERVICE Balancing Social Media with Operations Security (OPSEC) in the 21st Century Sailing the Sea of OSINT in the Information Age Social Media. Valuable Tools in Today’s Operational Environment ENHANCING A WEB CRAWLER WITH ARABIC SEARCH CAPABILITY USING SOCIAL MEDIA TO FURTHER THE NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE THE WHO, WHAT AND HOW OF SOCIAL MEDIA EXPLOITATION FOR A COMBATANT COMMANDER Open Source Cybersecurity for the 21st Century UNAUTHORIZED DISCLOSURE: CAN BEHAVIORAL INDICATORS HELP PREDICT WHO WILL COMMIT UNAUTHORIZED DISCLOSURE OF CLASSIFIED NATIONAL SECURITY INFORMATION? ATP 2-22.9 Open-Source Intelligence NTTP 3-13.3M OPERATIONS SECURITY (OPSEC) FM 2-22.3 HUMAN INTELLIGENCE COLLECTOR OPERATIONS The War of the Worlds-H. G. Wells 2017-01-01 When a meteorite lands in Surrey, the locals don’t know what to make of it. But as Martians emerge and begin killing bystanders, it quickly becomes clear—England is under attack. Armed soldiers converge on the scene to ward off the invaders, but meanwhile, more Martian cylinders land on Earth, bringing reinforcements. As war breaks out across England, the locals must fight for their lives, but life on Earth will never be the same. This is an unbridled version of one of the first fictional accounts of extraterrestrial invasion. H. G. Wells’s military science fiction novel was first published in book form in 1898, and is considered a classic of English literature. Intelligence Collection-Robert M. Clark 2013-09-13 Intelligence Collection by Robert M. Clark—one of the foremost authorities in the field—offers systematic and analytic coverage of the “how and why” of intelligence collection across its three major stages: the front end (planning), collection, and the back-end (processing, exploitation, and dissemination). The book provides a fresh, logical, and easily understandable view of complex collection systems used worldwide. Its ground-breaking organizational approach facilitates understanding and cross-INT collaboration, highlighting the similarities and differences among the collection INTs. Part one explains how the literal INTs such as communications intelligence and cyber collection work. Part two focuses on nonliteral INTs including imagery, electronic intelligence, and MASINT. All chapters use a common format based on systems analysis methodology, detailing function, process, and structure of the collection disciplines. Examples throughout the book highlight topics as diverse as battlespace situational awareness, terrorism, weapons proliferation, criminal networks, treaty monitoring, and identity intelligence.

We Are Bellingcat-Eliot Higgins 2021-03-02 INTERNATIONAL BESTSELLER “Fascinating ... A powerful, exhortatory call to arms.”—New York Times Book Review “A David-and-Goliath story for the digital age ... Thrilling.”—Foreign Policy The page-turning inside story of the global team wielding the internet to fight for facts and combat autocracy—revealing the extraordinary ability of ordinary people to hold the powerful to account. In 2018, Russian exile Sergei Skripal and his daughter were nearly killed in an audacious poisoning attempt in Salisbury, England. Soon, the identity of one of the suspects was revealed: he was a Russian spy. This huge investigative coup wasn’t pulled off by an intelligence agency or a traditional news outlet. Instead, the scoop came from Bellingcat, the open-source investigative team that is redefining the way we think about news, politics, and the digital future. We Are Bellingcat tells the inspiring story of how a college dropout pioneered a new category of reporting and galvanized citizen journalists—working together from their computer screens around the globe—to crack major cases, at a time when fact-based journalism is under assault from authoritarian forces. Founder Eliot Higgins brought together tools available in the public domain and added analytics to help you pinpoint the location of an image, to an app that can nail down the time that photo was taken. This book digs deep into some of Bellingcat’s most important investigations—the downing of flight MH17 over Ukraine, Assad’s use of chemical weapons in Syria, the identities of alt-right protestors in Charlottesville-with the drama and gripping detail of a spy novel.

The Routledge International Handbook of Universities, Security and Intelligence Studies-Liam Francis Gearon 2019-10-23 In an era of intensified international terror, universities have been increasingly drawn into an arena of locating, monitoring and preventing such threats, forcing them into often covert relationships with the security and intelligence agencies. With case studies from across the world, the Routledge International Handbook of Universities, Security and Intelligence Studies provides a comparative, in-depth analysis of the historical and contemporary relationships between global universities, national security and intelligence agencies. Written by leading international experts and from multidisciplinary perspectives, the Routledge International Handbook of Universities, Security and Intelligence Studies provides theoretical, methodological and empirical definition to academic, scholarly and research enquiry at the interface of higher education, security and intelligence. The book comprehensively covers the following main themes as an intellectual frame for our understanding of the university-security-intelligence network: historical, contemporary and future-looking interactions from across the globe; accounts of individuals who represent the broader landscape between universities and the security and intelligence agencies; the reciprocal interplay of personnel from universities to the security and intelligence agencies and vice versa; the practical goals of scholarship, research and teaching of security and intelligence both from within universities and the agencies themselves; terrorism research as an important dimension of security and intelligence within and beyond universities; the implication of security and intelligence in diplomacy, journalism and as an element of public policy; the extent to which security and intelligence practice, research and study far exceeds the traditional remit of commonly held notions of security and intelligence. Bringing together a unique blend of leading academic and practitioner authorities on security and intelligence, the Routledge International Handbook of Universities, Security and Intelligence Studies is an essential and authoritative guide for researchers and policymakers looking to understand the relationship between universities, the security services and the intelligence community.
includes extended and revised versions of papers presented during the 2018 International Computer Symposium (ICS 2018), held in Yunlin, Republic of China (Taiwan), on December 20-22, 2018. The 86 papers presented were carefully reviewed and selected from 263 submissions from 11 countries. The variety of the topics include machine learning, sensor devices and platforms, sensor networks, robotics, embedded systems, networks, operating systems, software system structures, database design and models, multimedia and multimodal retrieval, object detection, image processing, image compression, mobile and wireless security.

Gray Hat Python - Justin Seitz 2009-04-15 Python is fast becoming the programming language of choice for hackers, reverse engineers, and software testers because it’s easy to write quickly, and it has the low-level support and libraries that make hackers happy. But until now, there has been no real manual on how to use Python for a variety of hacking tasks. You had to dig through forum posts and man pages, endlessly tweaking your own code to get everything working. Not anymore. Gray Hat Python explains the concepts behind hacking tools and techniques like debuggers, trojans, fuzzers, and emulators. But author Justin Seitz goes beyond theory, showing you how to harness existing Python-based security tools—and how to build your own when the pre-built ones won’t cut it. You’ll learn how to: – Automate tedious reversing and security tasks – Design and program your own debugger – Learn how to fuzz Windows drivers and create powerful fuzzers from scratch – Have fun with code and library injection, soft and hard hooking techniques, and other software trickery – Sniff secure traffic out of an encrypted web browser session – Use PyDBG, Immunity Debugger, Sulley, IDAPython, PyEMU, and more The world’s best hackers are using Python to do their handiwork. Shouldn’t you?

No More Secrets: Open Source Information and the Reshaping of U.S. Intelligence - Hamilton Bean Ph.D. 2011-05-18 This in-depth analysis shows how the high stakes contest surrounding open source information is forcing significant reform within the U.S. intelligence community, the homeland security sector, and among citizen activists. • Critique and commentary from intelligence officials and analysts regarding open source reforms within the intelligence community and homeland security sector • Three interrelated case studies through which post-9/11 U.S. intelligence reform is analyzed and critiqued • Examples of collateral, including official and unofficial photos, from the 2007 and 2008 Open Source Conferences sponsored by the Director of National Intelligence • A timeline of key open source developments, including the establishment of associated commissions and changes in organizational structures, policies, and cultures • Appendices containing excerpts of key open source legislation and policy documents • A bibliography of open source-related scholarship and commentary

Operator Handbook - Joshua Picolet 2020-03-18 The Operator Handbook takes three disciplines (Red Team, OSINT, Blue Team) and combines them into one complete reference guide. The book contains 123 individual cheat sheet references for many of the most frequently used tools and techniques by practitioners. Over 400 pages of content to assist the most seasoned cybersecurity veteran or someone just getting started in the career field. The goal of combining all disciplines into one book was to remove the artificial barriers that only certain knowledge exists within a “Team”. The reality is today’s complex digital landscape demands some level of knowledge in all areas. The “Operator” culture should mean a well-rounded team member no matter the “Team” you represent. All cybersecurity practitioners are Operators. The Blue Team should observe and understand Red Team tactics, Red Team should continually push collaboration with the Blue Team, and OSINT should continually work to peel back evidence of evil doers scattered across disparate data sources. In the spirit of having no separation, each reference is listed in alphabetical order. Not only does this remove those team separated notions, but it also aids in faster lookup. We’ve all had the same experience where we knew there was an “NMAP Cheat Sheet” but did it fall under Networking, Windows, or Tools? In the Operator Handbook it begins with “N” so flip to the N’s section. Also almost every topic is covered in “How to exploit X” and “How to defend X” perspectives. Tools and topics covered: Cloud (AWS, Azure, GCP), Windows, macOS, Linux, Android, DevOps (Docker, Kubernetes), OSINT, Ports, Forensics, Malware Resources, Defender tools, Attacker tools, OSINT tools, and various other supporting tools (Vim, iptables, nftables, etc....). This handbook was truly meant to be a single source for the most common tool and techniques an Operator can encounter while on the job. Search Copy Paste L33t.